

Dr. Peter Kraft/Andreas Weyert

3. überarbeitete Auflage

Network Hacking

Professionelle Angriffs- und Verteidigungstechniken gegen Hacker und Datendiebe

Mit 412 Abbildungen

Inhaltsverzeichnis

Teil I: Tools – Werkzeuge für Angriff und Verteidigung	19
1 Keylogger – Spionage par excellence	21
1.1 Logkeys	22
1.2 Elite Keylogger	23
1.3 Ardamax Keylogger	24
1.4 Stealth Recorder Pro	25
1.5 Advanced Keylogger	26
1.6 Hardware-Keylogger	27
1.7 Abwehr – generelle Tipps	28
2 Passwortknacker: Wo ein Wille ist, ist auch ein Weg	31
2.1 CMOSPwd	31
2.2 Hydra	32
2.3 Medusa	34
2.4 Ncrack (Nmap-Suite)	36
2.5 VNCrack	37
2.6 PWDUMP (in unterschiedlichen Versionen bis PWDUMP 7.1)	38
2.7 John the Ripper	39
2.8 oclHashcat-plus	40
2.9 Ophcrack	41
2.10 SAMInside	42
2.11 Cain & Abel	43
2.12 L0phtcrack	44
2.13 Distributed Password Recovery	45
2.14 Offline NT Password & Registry Editor	46
2.15 PW-Inspector (Hydra-Suite)	46
2.16 Abwehr – generelle Tipps	47
3 An den Toren rütteln: Portscanner & Co.	49
3.1 Nmap	51
3.2 Lanspy	53
3.3 Essential NetTools	54

3.4	Winfingerprint	55
3.5	Xprobe2	56
3.6	p0f	58
3.7	Abwehr – generelle Tipps	61
4	Proxy & Socks	63
4.1	ProxyCap	64
4.2	Proxy Finder	65
4.3	Abwehr – generelle Tipps	66
5	Remote Access Tools (RAT) – Anleitung für Zombie-Macher	67
5.1	Atelier Web Remote Commander	67
5.2	Poison Ivy	68
5.3	Turkojan	69
5.4	Optix Pro	70
5.5	Cybergate 2.3.0 Public	71
5.6	Abwehr – generelle Tipps	72
6	Rootkits – Malware stealthen	73
6.1	Oddysee_Rootkit	74
6.2	Hacker_Defender	75
6.3	TDSS alias TDL-4	76
6.4	Abwehr – generelle Tipps	77
7	Security-/Vulnerability-Scanner	79
7.1	X-NetStat Professional	79
7.2	GFI LANguard N.S.S.	80
7.3	Nessus	81
7.4	Open Vulnerability Assessment System/OpenVAS	82
7.5	Nikto2	84
7.6	Abwehr – generelle Tipps	85
8	Sniffer: Die Schnüffler im Netzwerk	87
8.1	dsniff (dsniff-Suite)	88
8.2	mailsnarf (dsniff-Suite)	89
8.3	urlsnarf (dsniff-Suite)	91
8.4	arpspoof (dsniff-Suite)	92
8.5	PHoss	93
8.6	Driftnet	94

8.7	Ettercap/Ettercap NG	95
8.8	tcpdump	96
8.9	Wireshark	97
8.10	Abwehr – generelle Tipps	98
9	Sonstige Hackertools	99
9.1	Metasploit Framework (MSF)	99
9.2	USB DUMPER 2	100
9.3	USB Switchblade/7zBlade	101
9.4	Net Tools 5.0	102
9.5	Troll Downloader	103
9.6	H.O.I.C – High Orbit Ion Cannon	104
9.7	Phoenix Exploit's Kit	105
9.8	fEviol	106
9.9	Ox333shadow	106
9.10	Logcleaner-NG	108
9.11	NakedBind	109
9.12	Ncat (Nmap-Suite)	110
9.13	GNU MAC Changer (macchanger)	111
9.14	Volatility Framework	112
9.15	Abwehr – generelle Tipps	113
10	Wireless Hacking	115
10.1	Kismet-Newcore	116
10.2	Aircrack-NG (Aircrack-NG-Suite)	117
10.3	Aireplay-NG (Aircrack-NG-Suite)	118
10.4	Airodump-NG (Aircrack-NG-Suite)	119
10.5	Airbase-NG (Aircrack-NG-Suite)	120
10.6	coWPAtty	121
10.7	Reaver	122
10.8	Wash (Reaver-Suite)	124
10.9	Pyrit	125
10.10	MDK3	126
10.11	Vistumbler	127
10.12	Abwehr – generelle Tipps	129

Teil II: Angriffsszenarien und Abwehrmechanismen	131
11 Die Angreifer und ihre Motive	133
11.1 Die Motive	133
11.1.1 Rache	133
11.1.2 Geltungssucht	134
11.1.3 Furcht	134
11.1.4 Materielle Interessen	134
11.1.5 Neugierde	135
11.2 Die Angreifer	136
11.2.1 Hacker	136
11.2.2 Script-Kiddies	137
11.2.3 IT-Professionals	138
11.2.4 Normalanwender und PC-Freaks	139
12 Szenario I: Datenklau vor Ort	141
12.1 Zugriff auf Windows-PCs	141
12.1.1 Erkunden von Sicherheitsmechanismen	141
12.1.2 Überwinden der CMOS-Hürde	142
12.1.3 Das Admin-Konto erobern	144
12.2 Zugriff auf Linux-Rechner	153
12.2.1 Starten von Linux im Single-User-Mode	153
12.2.2 Starten von einem Linux-Boot-Medium	157
12.2.3 Einbinden der zu kompromittierenden Festplatte in ein Fremdsystem	158
12.3 Abwehrmaßnahmen gegen einen physischen Angriff von außen	159
12.4 2-Faktoren-Authentifizierung	161
12.4.1 iKey 2032 von SafeNet	162
12.4.2 Chipdrive Smartcard Office	165
12.4.3 Security Suite	169
13 Szenario II: Der PC ist verwandt	173
13.1 Software-Keylogger	175
13.1.1 Ausforschen von Sicherheitseinstellungen	175
13.1.2 Festlegen des Überwachungsumfangs	175
13.1.3 Installation des Keyloggers	176
13.1.4 Sichten, Bewerten und Ausnutzen der gewonnenen Daten	179
13.1.5 Die Audiowanze	179

13.2	Big Brother im Büro	181
13.3	Abwehrmaßnahmen gegen Keylogger & Co.	183
14	Szenario III: Spurensucher im Netz	191
14.1	Google-Hacking	192
14.1.1	Angriffe	192
14.1.2	Abwehrmaßnahmen	202
14.2	Portscanning, Fingerprinting und Enumeration	205
14.2.1	Portscanning	205
14.2.2	Fingerprinting und Enumeration	221
14.2.3	Security-Scanner	225
14.3	Abwehrmaßnahmen gegen Portscanner & Co.	231
15	Szenario IV: Web Attack	239
15.1	Defacements	239
15.2	XSS-Angriffe	240
15.3	Angriff der Würmer	241
15.4	DoS-, DDoS- und andere Attacken	241
15.5	Ultima Ratio – Social Engineering oder Brute Force?	250
15.6	Sicherheitslücken systematisch erforschen	253
15.6.1	AccessDiver	253
15.6.2	Spuren verwischen mit ProxyHunter	255
15.6.3	Passwortlisten konfigurieren	259
15.6.4	Wortlisten im Eigenbau	261
15.6.5	Websecurity-Scanner: Paros	264
15.6.6	Websecurity-Scanner: WVS	266
15.6.7	Websecurity-Scanner: Wikto	270
15.7	Abwehrmöglichkeiten gegen Webattacken	277
15.7.1	.htaccess schützt vor unbefugtem Zugriff	277
16	Szenario V: WLAN-Attacke	281
16.1	Aufspüren von Funknetzen	283
16.1.1	Hardwareausstattung für Wardriving	283
16.1.2	Vistumbler für Windows	285
16.1.3	Kismet-Newcore für Linux	290
16.2	Kartografierung von Funknetzen	304
16.2.1	Kartografierung von Funknetzen mit Google Maps oder OpenStreetMap	305

16.2.2	Kartografierung von Funknetzen mit Google Earth und Vistumbler	309
16.2.3	Kartografierung von Funknetzen mit Google Earth und Kismet-Newcore	311
16.3	Angriffe auf Funknetze	313
16.3.1	Zugriff auf ein offenes WLAN	314
16.3.2	Zugriff auf ein WLAN, dessen Hotspot keine SSID sendet	315
16.3.3	Zugriff auf ein WLAN, das keinen DHCP-Dienst anbietet	318
16.3.4	Zugriff auf ein mit MAC-Filter gesichertes WLAN	323
16.3.5	Zugriff auf ein WEP-verschlüsseltes WLAN	328
16.3.6	Zugriff auf ein WPA2-verschlüsseltes WLAN	342
16.3.7	Zugriff auf ein WPA2-verschlüsseltes WLAN durch die WPS-Schwäche	355
16.3.8	Zugriff auf ein WPA2-verschlüsseltes WLAN durch Softwareschwächen	362
16.3.9	WLAN, mon amour – Freu(n)de durch Funkwellen	363
16.4	Sicherheitsmaßnahmen bei Wireless LAN	373
17	Szenario VI: Malware-Attacke aus dem Internet	377
17.1	Angriffe via E-Mail	378
17.1.1	Absendeadresse fälschen	378
17.1.2	Phishen nach Aufmerksamkeit	382
17.1.3	Der Payload oder Malware aus dem Baukasten	386
17.1.4	Massenattacken und Spam-Schleudern	391
17.1.5	Office-Attacken	393
17.1.6	Kampf der Firewall	396
17.2	Rootkits	402
17.2.1	Test-Rootkit Unreal	404
17.2.2	AFX-Rootkit	406
17.3	Die Infektion	409
17.3.1	Experiment 1: <i>rechnung.pdf.exe</i>	409
17.3.2	Experiment 2: <i>bild-07_jpg.com</i>	412
17.4	Drive-by-Downloads	415
17.5	Schutz vor (un)bekannten Schädlingen aus dem Netz	421
17.5.1	Mailprogramm und Webbrowser absichern	423
17.5.2	Pflicht: Malware- und Antivirens Scanner	424
17.5.3	Malware-Abwehr mit Sandboxie	427
17.5.4	Allzweckwaffe Behavior Blocker & HIPS	429

18	Szenario VII: Netzwerkarbten: Wenn der Feind innen hackt	433
18.1	Der Feind im eigenen Netzwerk	433
18.2	Zugriff auf das LAN	434
18.3	Passives Mitlesen im LAN: Sniffing	436
18.3.1	Tcpdump	438
18.3.2	Wireshark	442
18.3.3	Ettercap NG	445
18.3.4	DSniff-Suite	455
18.3.5	Driftnet	466
18.3.6	Pof	466
18.3.7	ARPSpoof	469
18.4	Scanning: »Full Contact« mit dem LAN	472
18.4.1	Xprobe2	473
18.4.2	Nmap	476
18.4.3	Open Vulnerability Assessment System/OpenVAS	484
18.5	Der Tritt vors Schienbein: Exploits	494
18.5.1	wunderbar_emporium	495
18.5.2	2009-lsa.zip/Samba < 3.0.20 heap overflow	501
18.5.3	Metasploit Framework	505
18.6	Hurra, ich bin root – und nun?	534
18.7	Windows-Rechner kontrollieren	534
18.7.1	Integration von Schadsoftware	541
18.8	Linux unter Kontrolle: Rootkits installieren	543
18.8.1	evilbs	545
18.8.2	Mood-NT	549
18.8.3	eNYeLKM	553
18.9	Linux unter Kontrolle: Spuren verwischen mit Logfile- Cleaner	559
18.10	Linux unter Kontrolle: Keylogger	564
18.11	Linux unter Kontrolle: Password-Cracking	566
18.11.1	John the Ripper	567
18.11.2	ophcrack	567
18.11.3	Medusa	570
18.11.4	Hydra	572
18.12	Schutz vor Scannern, Exploits, Sniffen & Co.	574

Teil III: Prävention und Prophylaxe	577
19 Private Networking	579
19.1 Sicherheitsstatus mit MBSA überprüfen	579
19.2 Überflüssige Dienste	585
19.3 Vor »Dienstschluss« Abhängigkeiten überprüfen	587
19.4 Alle Dienste mit dem Process Explorer im Blick	588
19.5 Externer Security-Check tut Not	590
19.6 Malware-Check	592
19.7 Risiko: Mehrbenutzer-PCs und Netzwerksharing	605
19.8 Schadensbegrenzung: Intrusion Detection & Prevention	613
20 Company Networking	619
20.1 Basiselemente zur Unternehmenssicherheit	623
20.2 Teilbereich Infrastruktur und Organisation	624
20.3 Teilbereich Personal	626
20.4 Teilbereich Technik	630
Stichwortverzeichnis	635