

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 L0phcrack.....	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	fEvol	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 verwant.....	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: <i>Rechnung.pdf.exe</i>	368
17.3.2	Experiment 2: <i>bild-07.jpg.com</i>	370
17.4	Drive-by-Downloads.....	373
17.5	Schutz vor (un)bekannten Schädlingen aus dem Netz.....	378
17.5.1	Mailprogramm und Webbrower 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 Tcpcdump	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 POf	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