

# Inhaltsverzeichnis

Danksagungen.....	15
Der Autor .....	17
Einleitung .....	19
Überblick und Lernschwerpunkte .....	19
Zielpublikum.....	19
Der Aufbau dieses Buches.....	20
Schlusswort.....	23
<b>1. Das Handwerkszeug .....</b>	<b>25</b>
1.1 Einführung .....	25
1.2 Ziele .....	26
1.3 Vorgehensweise.....	26
1.4 Grundlegende Technologien .....	28
1.4.1 Live-CDs.....	28
1.4.2 ISO-Images .....	30
1.4.3 Bootfähige USB-Laufwerke .....	31
1.4.4 Eine persistente Live-CD erstellen.....	33
1.5 Open-Source-Werkzeuge .....	34
1.5.1 Tools zum Erstellen von Live-CDs .....	35
1.5.2 Werkzeugsätze für Penetrationstests.....	39
1.5.3 Ziele für Penetrationstests .....	47
1.6 Fallstudie: Die Werkzeuge im Einsatz.....	50
1.7 Praktische Übung.....	57
1.7.1 Zusammenfassung.....	58

<b>2. Aufklärung.....</b>	<b>59</b>
2.1 Einführung .....	59
2.2 Ziele .....	60
2.3 Eine Methodik für die Aufklärung.....	63
2.4 Informationsgewinnung aus öffentlichen Quellen.....	65
2.4.1 Grundlegende Technologien .....	65
2.4.2 Vorgehensweise.....	67
2.4.3 Open-Source-Werkzeuge .....	74
2.4.4 Informationsgewinnung aus öffentlichen Quellen: Zusammenfassung ....	87
2.5 Footprinting .....	87
2.5.1 Grundlegende Technologien .....	88
2.5.2 Vorgehensweise.....	95
2.5.3 Open-Source-Werkzeuge .....	100
2.5.4 Footprinting: Zusammenfassung .....	112
2.6 Informationsbeschaffung über Personen .....	112
2.6.1 Grundlegende Technologien .....	113
2.6.2 Beziehungen .....	113
2.6.3 Open-Source-Werkzeuge .....	117
2.6.4 Informationsbeschaffung über Personen: Zusammenfassung .....	121
2.7 Verifizierung.....	121
2.7.1 Grundlegende Technologien .....	121
2.7.2 Vorgehensweise.....	123
2.7.3 Open-Source-Werkzeuge .....	131
2.7.4 Verifizierung – Zusammenfassung .....	135
2.8 Fallstudie: Die Werkzeuge im Einsatz.....	135
2.8.1 Informationsgewinnung aus öffentlichen Quellen, Footprinting und Verifizierung für ein mit dem Internet verbundenes Netzwerk.....	135
2.8.2 Footprinting .....	141
2.8.3 Zusammenfassung der Fallstudie.....	145

2.9	Praktische Übung.....	145
2.10	Zusammenfassung.....	146
<b>3.</b>	<b>Scan und Auflistung .....</b>	<b>147</b>
3.1	Einführung .....	147
3.2	Ziele.....	147
3.2.1	Bevor Sie beginnen.....	148
3.2.2	Scans und Auflistungen – wozu?.....	149
3.3	Scans .....	150
3.3.1	Vorgehensweisen.....	150
3.3.2	Grundlegende Technologien .....	151
3.3.3	Open-Source-Werkzeuge .....	155
3.4	Auflistung .....	166
3.4.1	Vorgehensweise.....	166
3.4.2	Grundlegende Technologien .....	167
3.4.3	Open-Source-Werkzeuge .....	172
3.5	Fallstudien: Die Werkzeuge im Einsatz.....	187
3.5.1	Extern .....	187
3.5.2	Intern .....	188
3.5.3	Heimliche Vorgehensweise .....	191
3.5.4	Lauter IDS-Test .....	193
3.6	Praktische Übung.....	195
3.7	Zusammenfassung.....	196
<b>4.</b>	<b>Netzwerkgeräte .....</b>	<b>197</b>
4.1	Ziele.....	197
4.2	Vorgehensweise.....	198
4.3	Grundlegende Technologien .....	199
4.3.1	Switches .....	200

4.3.2	Router.....	202
4.3.3	Firewalls.....	203
4.3.4	IPv6.....	204
4.4	Open-Source-Werkzeuge .....	206
4.4.1	Footprinting-Werkzeuge.....	206
4.4.2	Scanwerkzeuge.....	209
4.4.3	Auflistungswerkzeuge.....	213
4.4.4	Exploit-Werkzeuge .....	214
4.5	Fallstudie: Die Werkzeuge im Einsatz.....	221
4.6	Praktische Übung.....	226
4.7	Zusammenfassung.....	227
<b>5.</b>	<b>Webanwendungen und -dienste .....</b>	<b>229</b>
5.1	Einführung .....	229
5.2	Ziel.....	230
5.2.1	Schwachstellen von Webservern: Geschichtlicher Abriss.....	230
5.2.2	Webanwendungen: Die neue Herausforderung.....	231
5.3	Vorgehensweise.....	232
5.3.1	Testen des Webservers .....	233
5.3.2	Testen von CGIs und Standardseiten.....	234
5.3.3	Testen von Webanwendungen.....	235
5.4	Grundlegende Technologien .....	236
5.4.1	Grundlagen der Ausnutzung von Webservern .....	236
5.4.2	Ausnutzung von CGIs und Standardseiten .....	240
5.4.3	Ausnutzung von Webanwendungen .....	241
5.5	Open-Source-Werkzeuge .....	245
5.6	Fallstudie: Die Werkzeuge im Einsatz.....	257
5.7	Praktische Übung.....	264
5.8	Zusammenfassung.....	265

<b>6. Datenbankdienste hacken.....</b>	<b>267</b>
6.1 Ziel.....	267
6.2 Grundlegende Technologien .....	268
6.2.1 Grundlegende Terminologie.....	268
6.2.2 Datenbankinstallation.....	270
6.2.3 Kommunikation.....	272
6.2.4 Ressourcen und Überwachung.....	272
6.3 Microsoft SQL Server .....	273
6.3.1 Benutzer .....	273
6.3.2 Richtlinien zum Erstellen von Passwörtern.....	274
6.3.3 Rollen und Berechtigungen.....	274
6.3.4 Gespeicherte Prozeduren.....	275
6.3.5 Open-Source-Werkzeuge .....	276
6.4 Oracle .....	281
6.4.1 Benutzer .....	281
6.4.2 Rollen und Rechte .....	282
6.4.3 Gespeicherte Prozeduren.....	283
6.4.4 Open-Source-Werkzeuge .....	283
6.5 Fallstudie: Die Werkzeuge im Einsatz.....	291
6.6 Praktische Übung.....	294
6.7 Zusammenfassung.....	295
<b>7. Unternehmensanwendungen testen .....</b>	<b>297</b>
7.1 Ziel.....	297
7.2 Grundlegende Technologien .....	298
7.2.1 Was sind Unternehmensanwendungen? .....	298
7.2.2 Mehrschichtige Architektur.....	300
7.2.3 Integration .....	301
7.3 Vorgehensweise.....	304

7.4	Open-Source-Werkzeuge .....	307
7.5	Fallstudie: Die Werkzeuge im Einsatz .....	322
7.6	Praktische Übung.....	325
7.7	Zusammenfassung.....	326
<b>8.</b>	<b>Clientseitige Angriffe und Social Engineering .....</b>	<b>327</b>
8.1	Ziel.....	327
8.2	Phishing.....	328
8.2.1	Vorgehensweisen.....	329
8.2.2	Walfang.....	332
8.2.3	Grundlegende Technologien .....	334
8.2.4	Open-Source-Werkzeuge .....	338
8.3	Angriffe in sozialen Medien.....	345
8.3.1	Vorgehensweise.....	345
8.3.2	Grundlegende Technologien .....	347
8.3.3	Open-Source-Werkzeuge .....	351
8.4	Maßgeschneiderte Malware.....	357
8.4.1	Vorgehensweise.....	357
8.4.2	Grundlegende Technologien .....	359
8.4.3	Open-Source-Werkzeuge .....	363
8.5	Fallstudie: Die Werkzeuge im Einsatz.....	368
8.6	Praktische Übung.....	375
8.7	Zusammenfassung.....	375
<b>9.</b>	<b>Penetrationstests in drahtlosen Netzwerken.....</b>	<b>377</b>
9.1	Ziel.....	378
9.2	Vorgehensweise.....	378
9.3	Grundlegende Technologien .....	379
9.3.1	Schwachstellen in WLANs .....	379

9.3.2	Die Entwicklung von WLAN-Schwachstellen.....	380
9.3.3	Werkzeuge für Penetrationstests in drahtlosen Netzwerken .....	383
9.4	Open-Source-Werkzeuge .....	392
9.4.1	Werkzeuge zur Informationsbeschaffung.....	392
9.4.2	Footprinting-Werkzeuge.....	398
9.4.3	Auflistungswerkzeuge.....	401
9.4.4	Werkzeuge zur Überprüfung auf Schwachstellen .....	402
9.4.5	Exploit-Werkzeuge .....	402
9.4.6	Bluetooth-Schwachstellen .....	420
9.4.7	Bluetooth-Schwachstellen ausnutzen.....	428
9.4.8	Gefahren von Bluetooth .....	430
9.5	Fallstudie: Die Werkzeuge im Einsatz.....	430
9.6	Praktische Übung.....	432
9.7	Zusammenfassung.....	433
<b>10.</b>	<b>Ein Labor für Penetrationstests einrichten .....</b>	<b>435</b>
10.1	Ziele.....	436
10.2	Vorgehensweise.....	436
10.2.1	Das Labor entwerfen.....	437
10.2.2	Das Labor aufbauen.....	450
10.2.3	Der Betrieb des Labors.....	454
10.3	Grundlegende Technologien .....	456
10.3.1	Was ist Virtualisierung?.....	457
10.3.2	Virtualisierung im Zusammenhang mit Penetrationstests.....	457
10.3.3	Virtualisierungsarchitektur .....	458
10.4	Open-Source-Werkzeuge .....	460
10.4.1	Xen.....	460
10.4.2	VirtualBox.....	461
10.4.3	GNS3, Dynagen und Dynamips .....	462
10.4.4	Weitere Werkzeuge .....	463

10.5	Fallstudie: Die Werkzeuge im Einsatz.....	463
10.6	Praktische Übung.....	465
10.7	Zusammenfassung.....	466
	<b>Stichwortverzeichnis .....</b>	<b>468</b>