

Inhaltsverzeichnis

Danksagung.....	11
Der Autor	13
Einleitung	15
1 Penetrationstests – was ist das?	25
1.1 Einführung.....	25
1.2 Vorbereitungen.....	26
1.3 Einführung in Kali Linux: »Werkzeuge. Jede Menge Werkzeuge.«.....	30
1.4 Arbeiten auf dem Angriffscomputer: Die Engine starten.....	36
1.5 Ein Hacker-Labor einrichten und nutzen	40
1.6 Die Phasen eines Penetrationstests	43
1.7 Wie geht es weiter?	50
1.8 Zusammenfassung	51
2 Aufklärung	53
2.1 Einführung.....	53
2.2 HTTrack: Ein Website-Kopierer.....	59
2.3 Google-Direktiven: Üben Sie sich in Google-Fu!.....	64
2.4 Harvester: E-Mail-Adressen aufspüren und ausnutzen.....	73
2.5 Whois	77
2.6 Der Befehl host.....	83
2.7 Informationen von DNS-Servern abrufen.....	84

2.8	NSLookup.....	86
2.9	Dig.....	89
2.10	Fierce: Wenn eine Zonenübertragung nicht möglich ist.....	90
2.11	Informationen von E-Mail-Servern gewinnen.....	92
2.12	MetaGooFil.....	93
2.13	ThreatAgent: Drohnenangriff.....	95
2.14	Social Engineering.....	97
2.15	Die Informationen nach angreifbaren Zielen durchsuchen.....	99
2.16	Wie übe ich diesen Schritt?.....	101
2.17	Wie geht es weiter?	101
2.18	Zusammenfassung	103
3	Scan.....	105
3.1	Einführung.....	105
3.2	Pings und Ping-Folgen	111
3.3	Portscans	114
3.4	Der Drei-Wege-Handshake	117
3.5	TCP-Verbindungscans mit Nmap	117
3.6	SYN-Scans mit Nmap	120
3.7	UDP-Scans mit Nmap	122
3.8	Weihnachtsbaumscans mit Nmap.....	126
3.9	NUL-Scans mit Nmap	128
3.10	Die Nmap-Script-Engine: Von der Raupe zum Schmetterling	129
3.11	Portscans: Zusammenfassung.....	132
3.12	Schwachstellen-Scan.....	133
3.13	Wie übe ich diesen Schritt?.....	141
3.14	Wie geht es weiter?	143
3.15	Zusammenfassung	144

4	Eindringen	145
4.1	Einführung.....	145
4.2	Medusa: Zugriff auf Remotedienste gewinnen	148
4.3	Metasploit: Hacking im Hugh-Jackman-Stil.....	154
4.4	JtR: König der Passwortcracker.....	172
4.5	Lokales Passwortcracking	176
4.6	Knacken von Passwörtern über das Netzwerk	186
4.7	Knacken von Linux-Passwörtern	187
4.8	Passwörter zurücksetzen: Die Abrissbirnen-Technik....	189
4.9	Sniffing: Netzwerkdatenverkehr ausspähen	193
4.9.1	Macof: Aus einem Switch einen Hub machen	196
4.9.2	Wireshark: Der Hai im Datenmeer.....	197
4.10	Armitage: Hacking wie mit dem Maschinengewehr	201
4.11	Warum fünf Werkzeuge lernen, wenn doch eines reicht?	205
4.12	Wie übe ich diesen Schritt?.....	209
4.13	Wie geht es weiter?	213
4.14	Zusammenfassung	216
5	Social Engineering	219
5.1	Einführung.....	219
5.2	Die Grundlagen von SET	220
5.3	Websites als Angriffswege.....	224
5.4	Credential Harvester.....	232
5.5	Weitere Optionen in SET	234
5.6	Zusammenfassung	237
6	Webgestützte Eindringversuche	239
6.1	Einführung.....	239
6.2	Grundlagen des Webhacking	241
6.3	Nikto: Abfragen von Webservern	243

6.4	W3af: Mehr als nur eine hübsche Oberfläche	245
6.5	Spider: Die Zielwebsite analysieren.....	249
6.6	Anforderungen mit WebScarab abfangen	254
6.7	Codeinjektion	257
6.8	XSS-Angriffe: Wenn Browser Websites vertrauen.....	263
6.9	Zed Attack Proxy: Alles unter einem Dach.....	267
6.10	Informationen mit ZAP abfangen	269
6.11	Spiderangriffe mit ZAP.....	271
6.12	Scannen mit ZAP.....	272
6.13	Wie übe ich diesen Schritt?.....	273
6.14	Wie geht es weiter?	275
6.15	Weitere Quellen.....	275
6.16	Zusammenfassung	276
7	Nacharbeiten und Erhaltung des Zugriffs mit Hintertüren, Rootkits und Meterpreter.....	279
7.1	Einführung.....	279
7.2	Netcat: Das Schweizer Messer.....	281
7.3	Netcats kryptischer Vetter: Cryptcat	289
7.4	Rootkits	290
7.5	Hacker Defender: Nicht das, wofür Sie es halten.....	292
7.6	Rootkits erkennen und abwehren	298
7.7	Meterpreter: Der Hammer, der aus allem einen Nagel macht.....	300

7.8	Wie übe ich diesen Schritt?.....	304
7.9	Wie geht es weiter?	306
7.10	Zusammenfassung	307
8	Der Abschluss eines Penetrationstests.....	309
8.1	Einführung.....	309
8.2	Den Testbericht schreiben	310
8.3	Die Zusammenfassung für die Geschäftsführung	312
8.4	Der ausführliche Bericht.....	312
8.5	Die Rohausgaben	315
8.6	Sie müssen nicht nach Hause gehen, aber hierbleiben können Sie auch nicht.....	320
8.7	Wie geht es weiter?	323
8.8	Schlusswort.....	325
8.9	Der Kreislauf des Lebens	326
8.10	Zusammenfassung	327
	Stichwortverzeichnis	329