

Auf einen Blick

von Dr. rer. oec. Barbara Schödl, Lehrstuhl für Wirtschaftsinformatik

Über den Autor	9
Einleitung	19
Teil I: Die ersten Schritte	23
Kapitel 1: Die Rolle von Pentests in der IT-Sicherheit.	25
Kapitel 2: Pentesting im Überblick	41
Kapitel 3: Das Werkzeug zusammensuchen	57
Teil II: Angriffe und was man damit macht	71
Kapitel 4: Penetration und Exploit.	73
Kapitel 5: Identitätsdiebstahl: der Mann in der Mitte und seine finsternen Freunde.	91
Kapitel 6: Überschwemmen und lahmlegen: DoS/DDoS.	101
Kapitel 7: Malware für Destroy Attacks.	115
Kapitel 8: Die Kontrollen umgehen: subversive Angriffe	125
Teil III: Es geht los: Vorbereiten und testen	137
Kapitel 9: Einen Pentest vorbereiten.	139
Kapitel 10: Einen Penetrationstest durchführen.	151
Teil IV: Der Pentest-Report	169
Kapitel 11: Reporting	171
Kapitel 12: Empfehlungen geben.	183
Kapitel 13: Retesting	203
Teil V: Der Top-Ten-Teil	213
Kapitel 14: Zehn falsche Pentest-Mythen.	215
Kapitel 15: Zehn Tipps, wie Sie ein noch besserer Pentester werden	223
Kapitel 16: Zehn Websites, auf denen Sie noch mehr über Pentesting erfahren.	231
Abbildungsverzeichnis	239
Stichwortverzeichnis	245

Über den Autor	9
Widmung.....	9
Danksagung	9
Einleitung	19
Über dieses Buch.....	19
Törichte Annahmen über Sie	20
Symbole in diesem Buch	20
Was (und wie) Sie nicht lesen müssen	20
Wie es jetzt weitergeht	21
TEIL I	
DIE ERSTEN SCHRITTE	23
Kapitel 1	
Die Rolle von Pentests in der IT-Sicherheit	25
Die Rolle von Penetrationstests.....	26
Crowdsourcing	26
Firmeneigene Sicherheitsprofis	27
Security Consultants	28
Zertifizierungen	28
Wie Sie sich die Grundlagen aneignen	28
Basic Networking	30
Allgemeine Sicherheitstechnologie	32
Systeminfrastruktur und Applikationen	33
Mobile Systeme und die Cloud	34
Cyberkriminalität	34
Was Sie brauchen, um anfangen zu können	36
Pentest – wie und wann?	38
Die ersten Schritte	39
Kapitel 2	
Pentesting im Überblick	41
Die Ziele der Pentester	41
Werte schützen.....	42
Risiken aufdecken	42
Sicherheitslücken aufdecken	45
Scannen und bewerten.....	46
Security-Operationen	47
Auf Vorfälle reagieren	47
Scanning im Alltag	49
Exclusions und Ping Sweeps.....	49
Patches	50

14 Inhaltsverzeichnis

- Antivirus und Co. 51
- Compliance 52
- Wer die Hacker sind 53
 - Hacktivisten..... 54
 - Vom Script-Kiddie zur Hacker-Elite 54
 - White Hat..... 54
 - Grey Hat..... 55
 - Black Hat 55
- Wie Hacker an Informationen kommen..... 55

- Kapitel 3**
- Das Werkzeug zusammensuchen 57**
 - Worauf Sie achten sollten..... 57
 - Nessus..... 58
 - Wireshark 61
 - Kali Linux..... 64
 - Nmap..... 68

TEIL II
ANGRIFFE UND WAS MAN DAMIT MACHT 71

- Kapitel 4**
- Penetration und Exploit 73**
 - Vektoren und die Kunst des Hackens..... 74
 - Typen von Penetrationsangriffen 75
 - Social Engineering 75
 - Client- und Server-seitige Angriffe..... 80
 - Passwörter knacken..... 82
 - Kryptografie und Verschlüsselung 84
 - SSL/TLS..... 85
 - SSH..... 85
 - IPsec..... 86
 - Metasploit..... 86

- Kapitel 5**
- Identitätsdiebstahl: der Mann in der Mitte und seine finsternen Freunde 91**
 - Ihr Toolkit 92
 - Burp Suite 92
 - Wireshark 94
 - Hineinhorchen, um Daten zu sammeln 96
 - Adressen fälschen 96
 - Der große Lauschangriff..... 97
 - Datenpakete sammeln und analysieren..... 98
 - Key Logger..... 99
 - Karten-Skimmer..... 99
 - USB-Sticks 100

Kapitel 6

Überschwemmen und lahmlegen: DoS/DDoS	101
Grundlegendes zum Toolkit	102
Kali	102
Der Kali T50 Mixed Packet Injector	104
Denial of Service (DoS) verstehen	105
Buffer Overflow	107
Fragmentation Attacks	110
Angriff der Killerschlümpfe	110
Tiny Packet Attacks	112
Offensive Weihnachtsbäume	113

Kapitel 7

Malware für Destroy Attacks	115
Was das Toolkit hier bietet	116
Antivirus-Software und andere Tools	116
Nessus	116
Malware	119
Ransomware	121
Andere Formen von Destroy Attacks	123

Kapitel 8

Die Kontrollen umgehen: subversive Angriffe	125
Aus dem Toolkit geplaudert	125
Antivirus-Software und andere Tools	126
Nmap	126
Angriffsvektoren	131
Phishing	133
Spoofing	133
Malware	134
Mit Malware ins System	134
Antivirus-Software umgehen	135

TEIL III

ES GEHT LOS: VORBEREITEN UND TESTEN	137
--	------------

Kapitel 9

Einen Pentest vorbereiten	139
Logistik im Vorfeld	139
Wir müssen reden	139
Die Erlaubnis einholen	142
Change Control	143
Backups, Backups, Backups	143
Dokumentationen	143
Das Benötigte zusammensuchen	144
Frühere Testergebnisse	144
Das Risk Register befragen	145

16 Inhaltsverzeichnis

Einen Plan haben	146
Einen Projekt- oder Scan-Typ auswählen	147
Die Tools auswählen	147
Plan B.	149

Kapitel 10

Einen Penetrationstest durchführen 151

Attacke!	152
Infiltration	153
Penetration	155
Exploit	156
APT	156
Exfiltration (Erfolg!)	157
Die nächsten Schritte.	157
Pentests von innerhalb des Systems	158
Dokumentieren Sie jeden Schritt!	159
Die Netzwerk-Map	159
Das Risk Register aktuell halten	161
Wahren Sie die Balance.	161
Weitere Methoden und Vektoren	161
Bewerten der Ergebnisse	162
Infiltration	162
Penetration	162
Exploit	163
Exfiltration	163
Prävention	164
Hardening	164
Aktives Monitoring	165
Retesting	165
Lessons learned: Entwickeln Sie Best Practices.	165

TEIL IV

DER PENTEST-REPORT 169

Kapitel 11

Reporting 171

Die Struktur eines Pentest-Reports.	171
Executive Summary	173
Tools, Methoden und Vektoren	174
Ihre Funde im Detail	175
Zusammenfassung	176
Empfehlungen	177
Anhang	177
Wie Sie einen professionellen Report verfassen.	178
Seien Sie professionell.	178
Bleiben Sie fokussiert	178
Vermeiden Sie falsch positive Aussagen.	178

Kategorisieren Sie Ihre Daten.	179
Fördern Sie das Sicherheitsbewusstsein	179
Den Report präsentieren	179
Update des Risk Registers	180

Kapitel 12

Empfehlungen geben 183

Warum Empfehlungen so wichtig sind.	183
Wie aus Bewertungen Empfehlungen werden	184
Netzwerke.	186
Network Hardening	187
Netzwerksegmentierung.	188
Interne Netzwerke	189
Verkabelt oder drahtlos?.	190
Externe Netze	190
Systeme.	190
Server.	192
Client-seitige Angriffe	192
Infrastruktur	193
Mobile Systeme	194
Cloud	195
Empfehlungen für alle Systeme.	195
Ports.	195
Nicht benötigte Dienste.	195
Ein Patch-Programm	196
Firewalls.	196
AV-Software.	196
Ressourcen teilen.	197
Verschlüsselung	198
Weitere Empfehlungen.	199
Segmentation und Virtualisierung.	199
Access Control	199
Backups	200
Die Logs sichern	200
Achtsamkeit und Social Engineering.	201

Kapitel 13

Retesting 203

Die Vorteile des Retestings.	204
Die sich wiederholende Natur von Pentesting und Retesting	204
Wann ist ein Retest fällig?.	206
Was der Retest testet	207
Ihre Dokumentation befragen	207
Den Report noch einmal lesen.	208
Noch einmal ins Risk Register schauen	209
Einen Pen-Retest durchführen	210

TEIL V

DER TOP-TEN-TEIL 213

Kapitel 14

Zehn falsche Pentest-Mythen..... 215

Ethical Hacking ist immer das Gleiche	215
Wir können uns keinen Pentester leisten	216
Wir können einem Pentester nicht wirklich trauen	217
Wir trauen den Tools nicht.	217
Pentests braucht man nicht oft zu machen.	219
Pentests betreffen nur technische Systeme	220
Externe können keine guten Pentests machen.	220
Pentest-Toolkits müssen standardisiert werden	221
Pentesting ist selbst nur ein Mythos.	221
Ein guter Pentester braucht nichts mehr zu lernen	222

Kapitel 15

Zehn Tipps, wie Sie ein noch besserer Pentester werden 223

Hören Sie nie auf zu lernen	223
Stellen Sie sich Ihr persönliches Toolkit zusammen.	224
Denken Sie über den Tellerrand hinaus.	225
Denken Sie wie ein Hacker.	225
Bringen Sie sich ein	226
Benutzen Sie eine Lab-Umgebung	227
Bleiben Sie informiert	228
Verfolgen Sie die technische Entwicklung	228
Machen Sie sich einen Namen.	229
Kümmern Sie sich auch um die physische Security	229

Kapitel 16

Zehn Websites, auf denen Sie noch mehr über

Pentesting erfahren 231

SANS Institute.	231
GIAC Certifications.	232
Software Engineering Institute	233
Ein Kessel Legal Penetration Sites.	233
Open Web Application Security Project	234
Tenable	235
Nmap	235
Wireshark	236
Dark Reading	236
Offensive Security	237

Abbildungsverzeichnis..... 239

Stichwortverzeichnis 245