

# Auf einen Blick

---

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



# Inhaltsverzeichnis

---

<b>Über den Autor</b> .....	<b>9</b>
Widmung .....	9
Danksagung .....	9
<b>Einleitung</b> .....	<b>19</b>
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
<b>TEIL I</b>	
<b>DIE ERSTEN SCHRITTE</b> .....	<b>23</b>
<b>Kapitel 1</b>	
<b>Die Rolle von Pentests in der IT-Sicherheit</b> .....	<b>25</b>
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
<b>Kapitel 2</b>	
<b>Pentesting im Überblick</b> .....	<b>41</b>
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
Haktivisten. ....	54
Vom Script-Kiddie zur Hacker-Elite .....	54
White Hat. ....	54
Grey Hat. ....	55
Black Hat .....	55
Wie Hacker an Informationen kommen. ....	55
<b>Kapitel 3</b>	
<b>Das Werkzeug zusammensuchen .....</b>	<b>57</b>
Worauf Sie achten sollten. ....	57
Nessus. ....	58
Wireshark .....	61
Kali Linux. ....	64
Nmap. ....	68
<b>TEIL II</b>	
<b>ANGRIFFE UND WAS MAN DAMIT MACHT .....</b>	<b>71</b>
<b>Kapitel 4</b>	
<b>Penetration und Exploit .....</b>	<b>73</b>
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
<b>Kapitel 5</b>	
<b>Identitätsdiebstahl: der Mann in der Mitte und seine finsternen Freunde .....</b>	<b>91</b>
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

<b>TEIL V</b>	
<b>DER TOP-TEN-TEIL</b> .....	<b>213</b>
<b>Kapitel 14</b>	
<b>Zehn falsche Pentest-Mythen</b> .....	<b>215</b>
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
<b>Kapitel 15</b>	
<b>Zehn Tipps, wie Sie ein noch besserer Pentester werden</b> ....	<b>223</b>
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
<b>Kapitel 16</b>	
<b>Zehn Websites, auf denen Sie noch mehr über</b>	
<b>Pentesting erfahren</b> .....	<b>231</b>
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
<b>Abbildungsverzeichnis</b> .....	<b>239</b>
<b>Stichwortverzeichnis</b> .....	<b>245</b>