

# Auf einen Blick

---

<b>Über den Autor</b> .....	<b>9</b>
<b>Einführung</b> .....	<b>23</b>
<b>Teil I: Den Grundstock für Sicherheitstests legen</b> .....	<b>27</b>
<b>Kapitel 1:</b> Einführung in Schwachstellen- und Penetrationstests .....	29
<b>Kapitel 2:</b> Die Denkweise von Hackern nachvollziehen .....	45
<b>Kapitel 3:</b> Einen Plan für Ihre Sicherheitstests entwickeln .....	57
<b>Kapitel 4:</b> Die Methodik des Hackens .....	69
<b>Teil II: Erste Sicherheitstests durchführen</b> .....	<b>79</b>
<b>Kapitel 5:</b> Daten sammeln .....	81
<b>Kapitel 6:</b> Social Engineering .....	87
<b>Kapitel 7:</b> Physische Sicherheit .....	103
<b>Kapitel 8:</b> Kennwörter .....	115
<b>Teil III: Netzwerkhosts hacken</b> .....	<b>143</b>
<b>Kapitel 9:</b> Netzwerkinfrastruktur .....	145
<b>Kapitel 10:</b> Drahtlose Netzwerke .....	177
<b>Kapitel 11:</b> Mobilgeräte .....	205
<b>Teil IV: Betriebssysteme hacken</b> .....	<b>219</b>
<b>Kapitel 12:</b> Windows .....	221
<b>Kapitel 13:</b> Linux und macOS .....	247
<b>Teil V: Anwendungen hacken</b> .....	<b>269</b>
<b>Kapitel 14:</b> Kommunikations- und Benachrichtigungssysteme .....	271
<b>Kapitel 15:</b> Webanwendungen und Apps für Mobilgeräte .....	295
<b>Kapitel 16:</b> Datenbanken und Speichersysteme .....	321
<b>Teil VI: Aufgaben nach den Sicherheitstests</b> .....	<b>333</b>
<b>Kapitel 17:</b> Die Ergebnisse präsentieren .....	335
<b>Kapitel 18:</b> Sicherheitslücken beseitigen .....	341
<b>Kapitel 19:</b> Sicherheitsprozesse verwalten .....	347

<b>Teil VII: Der Top-Ten-Teil</b> .....	<b>355</b>
<b>Kapitel 20:</b> Zehn Tipps für die Unterstützung der Geschäftsleitung .....	357
<b>Kapitel 21:</b> Zehn Gründe, warum nur Hacken effektive Tests ermöglicht .....	363
<b>Kapitel 22:</b> Zehn tödliche Fehler .....	367
 <b>Anhang: Werkzeuge und Ressourcen</b> .....	 <b>371</b>
<b>Stichwortverzeichnis</b> .....	<b>385</b>

# Inhaltsverzeichnis

---

<b>Über den Autor</b> .....	<b>9</b>
<b>Einführung</b> .....	<b>23</b>
Über dieses Buch. ....	23
Törichte Annahmen über den Leser. ....	24
Symbole, die in diesem Buch verwendet werden. ....	25
Wie es weitergeht .....	25
 <b>TEIL I</b>	
<b>DEN GRUNDSTOCK FÜR SICHERHEITSTESTS LEGEN</b> .....	<b>27</b>
 <b>Kapitel 1</b>	
<b>Einführung in Schwachstellen- und Penetrationstests</b> .....	<b>29</b>
Begriffserklärungen. ....	29
»Hacker« .....	30
»Böswillige Benutzer« .....	31
Wie aus arglistigen Angreifern ethische Hacker werden. ....	31
Ethisches Hacken im Vergleich zur Auditierung .....	32
Betrachtungen zu Richtlinien .....	32
Compliance und regulatorische Aspekte .....	33
Warum eigene Systeme hacken? .....	33
Die Gefahren verstehen, denen Ihre Systeme ausgesetzt sind .....	34
Nicht-technische Angriffe .....	35
Angriffe auf Netzwerkinfrastrukturen. ....	35
Angriffe auf Betriebssysteme. ....	35
Angriffe auf Anwendungen und spezielle Funktionen .....	36
Prinzipien bei Sicherheitsbewertungen .....	36
Ethisch arbeiten .....	37
Die Privatsphäre respektieren .....	37
Bringen Sie Ihre Systeme nicht zum Absturz. ....	37
Die Arbeitsabläufe bei Schwachstellen- und Penetrationstests .....	38
Die Planformulierung .....	38
Die Auswahl von Werkzeugen .....	40
Planumsetzung. ....	42
Ergebnisauswertung .....	43
Wie es weitergeht. ....	43

## Kapitel 2

<b>Die Denkweise von Hackern nachvollziehen</b>	<b>45</b>
Ihre Gegenspieler	45
Wer in Computersysteme einbricht	48
Hacker mit unterschiedlichen Fähigkeiten	48
Die Motivation der Hacker	49
Warum machen sie das?	50
Angriffe planen und ausführen	53
Anonymität wahren	54

## Kapitel 3

<b>Einen Plan für Ihre Sicherheitstests entwickeln</b>	<b>57</b>
Zielsetzungen festlegen	57
Festlegen, welche Systeme getestet werden sollen	60
Teststandards formulieren	62
Zeitpläne für Ihre Tests festlegen	63
Spezifische Tests ausführen	63
Tests blind oder mit Hintergrundwissen durchführen	64
Standortauswahl	65
Auf entdeckte Schwachstellen reagieren	66
Törichte Annahmen	66
Werkzeuge für Sicherheitsgutachten auswählen	66

## Kapitel 4

<b>Die Methodik des Hackens</b>	<b>69</b>
Die Bühne für das Testen vorbereiten	69
Sehen, was andere sehen	71
Systeme scannen	72
Hosts	72
Offene Ports	73
Feststellen, was über offene Ports läuft	73
Schwachstellen bewerten	76
In das System eindringen	77

## TEIL II

<b>ERSTE SICHERHEITSTESTS DURCHFÜHREN</b>	<b>79</b>
---	-----------

## Kapitel 5

<b>Daten sammeln</b>	<b>81</b>
Öffentlich verfügbare Daten sammeln	81
Soziale Medien	81
Suche im Web	82
Webcrawler	83
Websites	84
Netzwerkstrukturen abbilden	84
Whois	84
Datenschutzrichtlinien	86

<b>Kapitel 6</b>	
<b>Social Engineering</b>	<b>87</b>
Eine Einführung in Social Engineering	87
Erste Tests im Social Engineering	88
Warum Social Engineering für Angriffe genutzt wird	89
Die Auswirkungen verstehen	90
Vertrauen aufbauen	91
Die Beziehung ausnutzen	91
Social-Engineering-Angriffe durchführen	94
Ein Ziel festlegen	94
Informationen suchen	95
Maßnahmen gegen Social Engineering	98
Richtlinien	98
Aufmerksamkeit und Schulung der Nutzer	100
 <b>Kapitel 7</b>	
<b>Physische Sicherheit</b>	<b>103</b>
Grundlegende physische Sicherheitsschwachstellen identifizieren	103
Physische Schwachstellen in eigenen Büros aufspüren	105
Gebäudeinfrastruktur	105
Versorgung	106
Raumgestaltung und Nutzung der Büros	108
Netzwerkkomponenten und Computer	110
 <b>Kapitel 8</b>	
<b>Kennwörter</b>	<b>115</b>
Schwachstellen bei Kennwörtern verstehen	116
Organisatorische Schwachstellen von Kennwörtern	116
Technische Schwachstellen bei Kennwörtern	117
Kennwörter knacken	118
Kennwörter auf herkömmliche Weise knacken	118
Kennwörter technisch anspruchsvoll ermitteln	121
Kennwortgeschützte Dateien knacken	130
Weitere Optionen, an Kennwörter zu gelangen	131
Mit schlechten Kennwörtern ins Unheil	135
Allgemeine Gegenmaßnahmen beim Knacken von Kennwörtern	136
Kennwörter speichern	137
Kennwortrichtlinien erstellen	137
Andere Gegenmaßnahmen ergreifen	139
Betriebssysteme sichern	140
Windows	140
Linux und Unix	141

## TEIL III NETZWERKHOSTS HACKEN..... 143

### Kapitel 9 Netzwerkinfrastruktur ..... 145

Schwachstellen der Netzwerkinfrastruktur .....	146
Werkzeuge auswählen .....	147
Scanner und Analysatoren .....	147
Schwachstellenbestimmung .....	148
Das Netzwerk scannen und durchwühlen .....	148
Portscans .....	149
SNMP scannen .....	154
Banner-Grabbing .....	156
Firewall-Regeln testen .....	158
Netzwerkdaten untersuchen .....	159
Der Angriff auf die MAC-Adresse .....	166
Denial-of-Service-Angriffe testen .....	172
Bekannte Schwachstellen von Routern, Switches und Firewalls erkennen .....	174
Unsichere Schnittstellen ermitteln .....	175
Aspekte der Preisgabe von Daten durch SSL und TLS .....	175
Einen allgemeinen Netzwerkverteidigungswall einrichten .....	175

### Kapitel 10 Drahtlose Netzwerke ..... 177

Die Folgen von WLAN-Schwachstellen verstehen .....	177
Die Auswahl Ihrer Werkzeuge .....	178
Drahtlose Netzwerke aufspüren .....	179
Sie werden weltweit erkannt .....	180
Lokale Funkwellen absuchen .....	181
Angriffe auf WLANs erkennen und Gegenmaßnahmen ergreifen .....	182
Verschlüsselter Datenverkehr .....	184
Wi-Fi Protected Setup .....	189
Die drahtlosen Geräte von Schurken .....	192
MAC-Spoofing .....	197
Physische Sicherheitsprobleme .....	201
Angreifbare WLAN-Arbeitsstationen .....	201

### Kapitel 11 Mobilgeräte ..... 205

Schwachstellen von Mobilgeräten abschätzen .....	205
Kennwörter von Laptops knacken .....	206
Auswahl der Werkzeuge .....	206
Gegenmaßnahmen anwenden .....	211
Telefone, Smartphones und Tablets knacken .....	211
iOS-Kennwörter knacken .....	213
Display-Sperre bei Android-Geräten einrichten .....	216
Maßnahmen gegen das Knacken von Kennwörtern .....	217

## TEIL IV BETRIEBSSYSTEME HACKEN ..... 219

### Kapitel 12 Windows ..... 221

Windows-Schwachstellen .....	222
Werkzeugauswahl .....	222
Kostenlose Microsoft-Werkzeuge .....	223
Komplettlösungen .....	224
Aufgabenspezifische Werkzeuge .....	224
Daten über Ihre Windows-Systemschwachstellen sammeln .....	225
Das System untersuchen .....	225
NetBIOS .....	228
Null Sessions entdecken .....	231
Zuordnung, auch Mapping oder Einhängen .....	231
Informationen sammeln .....	232
Maßnahmen gegen Null-Session-Hacks .....	233
Freigabeberechtigungen überprüfen .....	234
Windows-Vorgaben .....	235
Testen .....	235
Fehlende Patches nutzen .....	236
Metasploit verwenden .....	238
Maßnahmen gegen das Ausnutzen fehlender Patches .....	243
Authentifizierte Scans ablaufen lassen .....	244

### Kapitel 13 Linux und macOS ..... 247

Linux-Schwachstellen verstehen .....	248
Werkzeugauswahl .....	248
Daten über Ihre System-Schwachstellen unter Linux und macOS sammeln .....	249
Das System durchsuchen .....	249
Maßnahmen gegen das Scannen des Systems .....	251
Nicht benötigte und unsichere Dienste ermitteln .....	253
Suchläufe .....	254
Maßnahmen gegen Angriffe auf nicht benötigte Dienste .....	255
Die Dateien .rhosts und hosts.equiv schützen .....	258
Hacks, die die Dateien hosts.equiv und .rhosts verwenden .....	258
Maßnahmen gegen Angriffe auf die Dateien .rhosts und hosts.equiv .....	259
Die Sicherheit von NFS überprüfen .....	260
NFS-Hacks .....	261
Maßnahmen gegen Angriffe auf NFS .....	261
Dateiberechtigungen überprüfen .....	261
Das Hacken von Dateiberechtigungen .....	262
Maßnahmen gegen Angriffe auf Dateiberechtigungen .....	262

Schwachstellen für Pufferüberläufe finden .....	263
Angriffe .....	263
Maßnahmen gegen Buffer-Overflow-Angriffe .....	263
Physische Sicherheitsmaßnahmen überprüfen .....	264
Physische Hacks .....	264
Maßnahmen gegen physische Angriffe auf die Sicherheit .....	264
Allgemeine Sicherheitstests durchführen .....	265
Sicherheitsaktualisierungen für Linux .....	267
Aktualisierungen der Distributionen .....	267
Update-Manager für mehrere Plattformen .....	267

## TEIL V ANWENDUNGEN HACKEN ..... 269

### Kapitel 14 Kommunikations- und Benachrichtigungssysteme ..... 271

Grundlagen der Schwachstellen bei Messaging-Systemen .....	271
Erkennung und Abwehr von E-Mail-Angriffen .....	272
E-Mail-Bomben .....	272
Banner .....	276
SMTP-Angriffe .....	278
Die besten Verfahren, Risiken bei E-Mails zu minimieren .....	287
Voice over IP verstehen .....	289
VoIP-Schwachstellen .....	289
Maßnahmen gegen VoIP-Schwachstellen .....	294

### Kapitel 15 Webanwendungen und Apps für Mobilgeräte ..... 295

Die Werkzeuge für Webanwendungen auswählen .....	296
Web-Schwachstellen auffinden .....	297
Verzeichnis traversieren .....	297
Maßnahmen gegen Directory Traversals .....	300
Eingabe-Filter-Angriffe .....	301
Maßnahmen gegen Eingabeangriffe .....	308
Angriffe auf Standardskripte .....	309
Maßnahmen gegen Angriffe auf Standardskripte .....	311
Unsichere Anmeldeverfahren .....	311
Maßnahmen gegen unsichere Anmeldesysteme .....	314
Allgemeine Sicherheitsscans bei Webanwendungen durchführen .....	316
Risiken bei der Websicherheit minimieren .....	316
Sicherheit durch Obskürität .....	317
Firewalls einrichten .....	318
Quellcode analysieren .....	318
Schwachstellen von Apps für Mobilgeräte aufspüren .....	319



**Kapitel 16****Datenbanken und Speichersysteme..... 321**

Datenbanken untersuchen .....	321
Werkzeuge wählen.....	322
Datenbanken im Netzwerk finden.....	322
Datenbankkennwörter knacken .....	323
Datenbanken nach Schwachstellen durchsuchen.....	325
Bewährte Vorkehrungen zur Minimierung der Sicherheitsrisiken bei Datenbanken .....	325
Sicherheit für Speichersysteme.....	326
Werkzeuge wählen.....	327
Speichersysteme im Netzwerk finden.....	327
Sensiblen Text in Netzwerkdateien aufspüren .....	328
Bewährte Vorgehensweisen zur Minimierung von Sicherheitsrisiken bei der Datenspeicherung .....	331

**TEIL VI****AUFGABEN NACH DEN SICHERHEITSTESTS..... 333****Kapitel 17****Die Ergebnisse präsentieren..... 335**

Die Ergebnisse zusammenführen.....	335
Schwachstellen Prioritäten zuweisen .....	336
Berichterstellung .....	338

**Kapitel 18****Sicherheitslücken beseitigen..... 341**

Berichte zu Maßnahmen werden lassen .....	341
Patchen für Perfektionisten .....	342
Patch-Verwaltung.....	343
Patch-Automatisierung .....	343
Systeme härten .....	344
Die Sicherheitsinfrastrukturen prüfen .....	345

**Kapitel 19****Sicherheitsprozesse verwalten..... 347**

Den Prozess der Sicherheitsbestimmung automatisieren .....	347
Bösartige Nutzung überwachen .....	348
Sicherheitsprüfungen auslagern.....	350
Die sicherheitsbewusste Einstellung .....	352
Auch andere Sicherheitsmaßnahmen nicht vernachlässigen.....	353

<b>TEIL VII</b>	
<b>DER TOP-TEN-TEIL</b>	<b>355</b>

## Kapitel 20

### Zehn Tipps für die Unterstützung der

<b>Geschäftsleitung</b>	<b>357</b>
Sorgen Sie für Verbündete und Geldgeber	357
Geben Sie nicht den Aufschneider	357
Zeigen Sie, warum es sich das Unternehmen nicht leisten kann, gehackt zu werden	357
Betonen Sie allgemeine Vorteile der Sicherheitstests	358
Zeigen Sie, wie insbesondere Sicherheitstests Ihrem Unternehmen helfen.	359
Engagieren Sie sich für das Unternehmen	359
Zeigen Sie sich glaubwürdig	360
Reden Sie wie ein Manager	360
Demonstrieren Sie den Wert Ihrer Anstrengungen	360
Seien Sie flexibel und anpassungsfähig	361

## Kapitel 21

### Zehn Gründe, warum nur Hacken effektive Tests

<b>ermöglicht</b>	<b>363</b>
Die Schurken hegen böse Absichten, nutzen beste Werkzeuge und entwickeln neue Methoden	363
Einhaltung von Vorschriften und Regeln bedeutet in der IT mehr als Prüfungen mit anspruchsvollen Checklisten	363
Schwachstellen- und Penetrationstests ergänzen Audits und Sicherheitsbewertungen.	364
Kunden und Partner interessiert die Sicherheit Ihrer Systeme	364
Das Gesetz des Durchschnitts arbeitet gegen Ihr Unternehmen.	364
Sicherheitsprüfungen verbessern das Verständnis für geschäftliche Bedrohungen	365
Bei Einbrüchen können Sie auf etwas zurückgreifen.	365
Intensive Tests enthüllen die schlechten Seiten Ihrer Systeme	365
Sie sind auf die Vorteile kombinierter Schwachstellen- und Penetrationstests angewiesen.	366
Sorgfältiges Testen kann Schwachstellen aufdecken, die ansonsten vielleicht lange übersehen worden wären.	366

## Kapitel 22

### Zehn tödliche Fehler

	<b>367</b>
Keine Genehmigung vorab einholen	367
Davon ausgehen, dass im Testverlauf alle Schwachstellen gefunden werden	367
Anzunehmen, alle Sicherheitslöcher beseitigen zu können	368
Tests nur einmal ausführen	368
Glauben, alles zu wissen.	368
Tests nicht aus der Sicht von Hackern betrachten	369
Die falschen Systeme testen	369

Nicht die richtigen Werkzeuge verwenden .....	369
Sich zur falschen Zeit mit Produktivsystemen befassen .....	370
Tests Dritten überlassen und sich dann nicht weiter darum kümmern .....	370

## **Anhang: Werkzeuge und Ressourcen .....371**

Allgemeine Hilfen. ....	371
Anspruchsvolle Malware. ....	372
Bluetooth .....	372
Datenbanken .....	372
DoS-Schutz (Denial of Service) .....	372
Drahtlose Netzwerke. ....	373
Exploits .....	373
Gesetze und Vorschriften. ....	373
Hacker-Zeugs .....	374
Kennwörter knacken. ....	374
Keylogger .....	375
Linux .....	375
Live-Toolkits .....	375
Messaging. ....	376
Mobil .....	376
Netzwerke. ....	376
Patch-Management. ....	378
Protokollanalyse .....	378
Quellcode-Analyse. ....	378
Schwachstellendatenbanken. ....	379
Social Engineering und Phishing. ....	379
Speicherung .....	379
Systeme härten .....	379
Verschiedenes .....	380
Voice over IP .....	380
Wachsamkeit der Benutzer .....	380
Websites und Webanwendungen .....	380
Windows .....	381
WLAN. ....	382
Wörterbuchdateien und Wortlisten .....	382
Zertifizierungen .....	383

## **Stichwortverzeichnis..... 385**

