

Auf einen Blick

Über den Autor	9
Einführung	23
Teil I: Den Grundstock für Sicherheitstests legen	27
Kapitel 1: Einführung in Schwachstellen- und Penetrationstests	29
Kapitel 2: Die Denkweise von Hackern nachvollziehen	45
Kapitel 3: Einen Plan für Ihre Sicherheitstests entwickeln	57
Kapitel 4: Die Methodik des Hackens	69
Teil II: Erste Sicherheitstests durchführen	79
Kapitel 5: Daten sammeln	81
Kapitel 6: Social Engineering	87
Kapitel 7: Physische Sicherheit	103
Kapitel 8: Kennwörter	115
Teil III: Netzwerkhosts hacken	143
Kapitel 9: Netzwerkinfrastruktur	145
Kapitel 10: Drahtlose Netzwerke	179
Kapitel 11: Mobilgeräte	207
Teil IV: Betriebssysteme hacken	221
Kapitel 12: Windows	223
Kapitel 13: Linux und macOS	249
Teil V: Anwendungen hacken	271
Kapitel 14: Kommunikations- und Benachrichtigungssysteme	273
Kapitel 15: Webanwendungen und Apps für Mobilgeräte	299
Kapitel 16: Datenbanken und Speichersysteme	325
Teil VI: Aufgaben nach den Sicherheitstests	337
Kapitel 17: Die Ergebnisse präsentieren	339
Kapitel 18: Sicherheitslücken beseitigen	345
Kapitel 19: Sicherheitsprozesse verwalten	351
Teil VII: Der Top-Ten-Teil	359
Kapitel 20: Zehn Tipps für die Unterstützung der Geschäftsleitung	361
Kapitel 21: Zehn Gründe, warum nur Hacken effektive Tests ermöglicht	367
Kapitel 22: Zehn tödliche Fehler	371
Kapitel 23: Anhang: Werkzeuge und Ressourcen	375
Stichwortverzeichnis	389



Inhaltsverzeichnis

Über den Autor	9
Einführung	23
Über dieses Buch	24
Törichte Annahmen über den Leser	24
Symbole, die in diesem Buch verwendet werden	25
Wie es weitergeht	25
TEIL I	
DEN GRUNDSTOCK FÜR SICHERHEITSTESTS LEGEN	27
Kapitel 1	
Einführung in Schwachstellen- und Penetrationstests	29
Begriffserklärungen	29
»Hacker«	30
»Böswillige Benutzer«	31
Wie aus arglistigen Angreifern ethische Hacker werden	32
Ethisches Hacken im Vergleich zur Auditierung	32
Betrachtungen zu Richtlinien	33
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	36
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	38
Die Arbeitsabläufe bei Schwachstellen- und Penetrationstests	38
Die Planformulierung	39
Die Auswahl von Werkzeugen	41
Planumsetzung	43
Ergebnisauswertung	43
Wie es weitergeht	44
Kapitel 2	
Die Denkweise von Hackern nachvollziehen	45
Ihre Gegenspieler	45
Wer in Computersysteme einbricht	48

14 Inhaltsverzeichnis

Hacker mit unterschiedlichen Fähigkeiten	48
Die Motivation der Hacker	49
Warum machen sie das?	50
Angriffe planen und ausführen	53
Anonymität wahren	55
Kapitel 3	
Einen Plan für Ihre Sicherheitstests entwickeln	57
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	65
Standortauswahl	65
Auf entdeckte Schwachstellen reagieren	66
Törichte Annahmen	66
Werkzeuge für Sicherheitsgutachten auswählen	67
Kapitel 4	
Die Methodik des Hackens	69
Die Bühne für das Testen vorbereiten	69
Sehen, was andere sehen	71
Systeme scannen	72
Hosts	73
Offene Ports	73
Feststellen, was über offene Ports läuft	74
Schwachstellen bewerten	76
In das System eindringen	78
TEIL II	
ERSTE SICHERHEITSTESTS DURCHFÜHREN	79
Kapitel 5	
Daten sammeln	81
Öffentlich verfügbare Daten sammeln	81
Soziale Medien	81
Suche im Web	82
Webcrawler	83
Websites	84
Netzwerkstrukturen abbilden	84
Whois	85
Datenschutzrichtlinien	86
Kapitel 6	
Social Engineering	87
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	92
Social-Engineering-Angriffe durchführen	94
Ein Ziel festlegen	95
Informationen suchen	95
Maßnahmen gegen Social Engineering	99
Richtlinien	99
Aufmerksamkeit und Schulung der Nutzer	100

Kapitel 7
Physische Sicherheit..... 103

Grundlegende physische Sicherheitsschwachstellen identifizieren	104
Physische Schwachstellen in den eigenen Büros aufspüren	105
Gebäudeinfrastruktur	105
Versorgung	107
Raumgestaltung und Nutzung der Büros	108
Netzwerkkomponenten und Computer	110

Kapitel 8
Kennwörter 115

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	132
Mit schlechten Kennwörtern ins Unheil	136
Allgemeine Gegenmaßnahmen beim Knacken von Kennwörtern	137
Kennwörter speichern	138
Kennwortrichtlinien erstellen	138
Andere Gegenmaßnahmen ergreifen	140
Betriebssysteme sichern	141
Windows	141
Linux und Unix	142

TEIL III
NETZWERKHOSTS HACKEN..... 143

Kapitel 9
Netzwerkinfrastruktur 145

Schwachstellen der Netzwerkinfrastruktur	146
Werkzeuge auswählen	147

16 Inhaltsverzeichnis

Scanner und Analysatoren	147
Schwachstellenbestimmung	148
Das Netzwerk scannen und durchwühlen	148
Portscans	149
SNMP scannen	155
Banner-Grabbing	157
Firewall-Regeln testen	158
Netzwerkdaten untersuchen	160
Der Angriff auf die MAC-Adresse	166
Denial-of-Service-Angriffe testen	173
Bekannte Schwachstellen von Routern, Switches und Firewalls erkennen	175
Unsichere Schnittstellen ermitteln	175
Aspekte der Preisgabe von Daten durch SSL und TLS	176
Einen allgemeinen Netzwerkverteidigungswall einrichten	176
Kapitel 10	
Drahtlose Netzwerke	179
Die Folgen von WLAN-Schwachstellen verstehen	180
Die Auswahl Ihrer Werkzeuge	180
Drahtlose Netzwerke aufspüren	182
Sie werden weltweit erkannt	182
Lokale Funkwellen absuchen	183
Angriffe auf WLANs erkennen und Gegenmaßnahmen ergreifen	185
Verschlüsselter Datenverkehr	187
Wi-Fi Protected Setup	193
Die drahtlosen Geräte von Schurken	195
MAC-Spoofing	200
Physische Sicherheitsprobleme	204
Angreifbare WLAN-Arbeitsstationen	205
Kapitel 11	
Mobilgeräte	207
Schwachstellen von Mobilgeräten abschätzen	207
Kennwörter von Laptops knacken	208
Auswahl der Werkzeuge	208
Gegenmaßnahmen anwenden	213
Telefone, Smartphones und Tablets knacken	214
iOS-Kennwörter knacken	215
Display-Sperre bei Android-Geräten einrichten	219
Maßnahmen gegen das Knacken von Kennwörtern	219
TEIL IV	
BETRIEBSSYSTEME HACKEN	221
Kapitel 12	
Windows	223
Windows-Schwachstellen	224

- Werkzeugauswahl 225
 - Kostenlose Microsoft-Werkzeuge 225
 - Komplettlösungen 226
 - Aufgabenspezifische Werkzeuge 226
- Daten über Ihre Windows-Systemschwachstellen sammeln 227
 - Das System untersuchen 227
 - NetBIOS 230
- Null-Sessions entdecken 233
 - Zuordnung, auch Mapping oder Einhängen 233
 - Informationen sammeln 234
 - Maßnahmen gegen Null-Session-Hacks 236
- Freigabeberechtigungen überprüfen 237
 - Windows-Vorgaben 237
 - Testen 238
- Fehlende Patches nutzen 239
 - Metasploit verwenden 241
 - Maßnahmen gegen das Ausnutzen fehlender Patches 245
- Authentifizierte Scans ablaufen lassen 247

Kapitel 13
Linux und macOS 249

- Linux-Schwachstellen verstehen 250
- Werkzeugauswahl 250
- Daten über Ihre System-Schwachstellen unter Linux und macOS sammeln 251
 - Das System durchsuchen 251
 - Maßnahmen gegen das Scannen des Systems 255
- Nicht benötigte und unsichere Dienste ermitteln 256
 - Suchläufe 256
 - Maßnahmen gegen Angriffe auf nicht benötigte Dienste 258
- Die Dateien .rhosts und hosts.equiv schützen 260
 - Hacks, die die Dateien hosts.equiv und .rhosts verwenden 261
 - Maßnahmen gegen Angriffe auf die Dateien .rhosts und hosts.equiv 262
- Die Sicherheit von NFS überprüfen 263
 - NFS-Hacks 263
 - Maßnahmen gegen Angriffe auf NFS 264
- Dateiberechtigungen überprüfen 264
 - Das Hacken von Dateiberechtigungen 264
 - Maßnahmen gegen Angriffe auf Dateiberechtigungen 265
- Schwachstellen für Pufferüberläufe finden 266
 - Angriffe 266
 - Maßnahmen gegen Buffer-Overflow-Angriffe 266
- Physische Sicherheitsmaßnahmen überprüfen 267
 - Physische Hacks 267
 - Maßnahmen gegen physische Angriffe auf die Sicherheit 267
- Allgemeine Sicherheitstests durchführen 268
- Sicherheitsaktualisierungen für Linux 269
 - Aktualisierungen der Distributionen 270
 - Update-Manager für mehrere Plattformen 270

TEIL V ANWENDUNGEN HACKEN 271

Kapitel 14 Kommunikations- und Benachrichtigungssysteme 273

Grundlagen der Schwachstellen bei Messaging-Systemen.....	273
Erkennung und Abwehr von E-Mail-Angriffen.....	274
E-Mail-Bomben.....	274
Banner.....	278
SMTP-Angriffe.....	280
Die besten Verfahren, Risiken bei E-Mails zu minimieren.....	290
Voice over IP verstehen.....	292
VoIP-Schwachstellen.....	292
Maßnahmen gegen VoIP-Schwachstellen.....	296

Kapitel 15 Webanwendungen und Apps für Mobilgeräte 299

Die Werkzeuge für Webanwendungen auswählen.....	300
Web-Schwachstellen auffinden.....	301
Verzeichnis traversieren.....	301
Maßnahmen gegen Directory Traversals.....	305
Eingabe-Filter-Angriffe.....	305
Maßnahmen gegen Eingabeangriffe.....	313
Angriffe auf Standardskripte.....	314
Maßnahmen gegen Angriffe auf Standardskripte.....	315
Unsichere Anmeldeverfahren.....	316
Maßnahmen gegen unsichere Anmeldesysteme.....	319
Allgemeine Sicherheitsscans bei Webanwendungen durchführen.....	320
Risiken bei der Websicherheit minimieren.....	321
Sicherheit durch Obskurität.....	321
Firewalls einrichten.....	322
Quellcode analysieren.....	323
Schwachstellen von Apps für Mobilgeräte aufspüren.....	323

Kapitel 16 Datenbanken und Speichersysteme 325

Datenbanken untersuchen.....	325
Werkzeuge wählen.....	326
Datenbanken im Netzwerk finden.....	326
Datenbankkennwörter knacken.....	327
Datenbanken nach Schwachstellen durchsuchen.....	329
Bewährte Vorkehrungen zur Minimierung der Sicherheitsrisiken bei Datenbanken.....	329
Sicherheit für Speichersysteme.....	330
Werkzeuge wählen.....	331
Speichersysteme im Netzwerk finden.....	331
Sensiblen Text in Netzwerkdateien aufspüren.....	332

Bewährte Vorgehensweisen zur Minimierung von Sicherheitsrisiken
bei der Datenspeicherung 335

**TEIL VI
AUFGABEN NACH DEN SICHERHEITSTESTS..... 337**

**Kapitel 17
Die Ergebnisse präsentieren 339**
 Die Ergebnisse zusammenführen 339
 Schwachstellen Prioritäten zuweisen 341
 Berichterstellung 342

**Kapitel 18
Sicherheitslücken beseitigen 345**
 Berichte zu Maßnahmen werden lassen 345
 Patchen für Perfektionisten 346
 Patch-Verwaltung 347
 Patch-Automatisierung 347
 Systeme härten 348
 Die Sicherheitsinfrastrukturen prüfen 349

**Kapitel 19
Sicherheitsprozesse verwalten 351**
 Den Prozess der Sicherheitsbestimmung automatisieren 351
 Böartige Nutzung überwachen 352
 Sicherheitsprüfungen auslagern 354
 Die sicherheitsbewusste Einstellung 356
 Auch andere Sicherheitsmaßnahmen nicht vernachlässigen 357

**TEIL VII
DER TOP-TEN-TEIL..... 359**

**Kapitel 20
Zehn Tipps für die Unterstützung der Geschäftsleitung..... 361**
 Sorgen Sie für Verbündete und Geldgeber 361
 Geben Sie nicht den Aufschneider 361
 Zeigen Sie, warum es sich das Unternehmen nicht leisten kann,
gehackt zu werden 362
 Betonen Sie allgemeine Vorteile der Sicherheitstests 363
 Zeigen Sie, wie insbesondere Sicherheitstests Ihrem
Unternehmen helfen. 363
 Engagieren Sie sich für das Unternehmen 364
 Zeigen Sie sich glaubwürdig. 364
 Reden Sie wie ein Manager 364
 Demonstrieren Sie den Wert Ihrer Anstrengungen 365
 Seien Sie flexibel und anpassungsfähig 365

Kapitel 21	
Zehn Gründe, warum nur Hacken effektive Tests ermöglicht	367
Die Schurken hegen böse Absichten, nutzen beste Werkzeuge und entwickeln neue Methoden	367
Einhaltung von Vorschriften und Regeln bedeutet in der IT mehr als Prüfungen mit anspruchsvollen Checklisten	367
Schwachstellen- und Penetrationstests ergänzen Audits und Sicherheitsbewertungen	368
Kunden und Partner interessiert die Sicherheit Ihrer Systeme	368
Das Gesetz des Durchschnitts arbeitet gegen Ihr Unternehmen	368
Sicherheitsprüfungen verbessern das Verständnis für geschäftliche Bedrohungen	369
Bei Einbrüchen können Sie auf etwas zurückgreifen	369
Intensive Tests enthüllen die schlechten Seiten Ihrer Systeme	370
Sie sind auf die Vorteile kombinierter Schwachstellen- und Penetrationstests angewiesen	370
Sorgfältiges Testen kann Schwachstellen aufdecken, die ansonsten vielleicht lange übersehen worden wären	370
Kapitel 22	
Zehn tödliche Fehler	371
Keine Genehmigung vorab einholen	371
Davon ausgehen, dass im Testverlauf alle Schwachstellen gefunden werden ..	371
Anzunehmen, alle Sicherheitslöcher beseitigen zu können	372
Tests nur einmal ausführen	372
Glauben, alles zu wissen	372
Tests nicht aus der Sicht von Hackern betrachten	373
Die falschen Systeme testen	373
Nicht die richtigen Werkzeuge verwenden	373
Sich zur falschen Zeit mit Produktivsystemen befassen	374
Tests Dritten überlassen und sich dann nicht weiter darum kümmern	374
Kapitel 23	
Anhang: Werkzeuge und Ressourcen	375
Allgemeine Hilfen	375
Anspruchsvolle Malware	376
Bluetooth	376
Datenbanken	376
DoS-Schutz (Denial of Service)	377
Drahtlose Netzwerke	377
Exploits	378
Gesetze und Vorschriften	378
Hacker-Zeugs	378
Kennwörter knacken	378
Keylogger	379

Linux	379
Live-Toolkits	380
Messaging	380
Mobil	380
Netzwerke	381
Patch-Management	382
Protokollanalyse	383
Quellcode-Analyse	383
Schwachstellendatenbanken	383
Social Engineering und Phishing	384
Speicherung	384
Systeme härten	384
Verschiedenes	384
Voice over IP	385
Wachsamkeit der Benutzer	385
Websites und Webanwendungen	385
Windows	386
WLAN	386
Wörterbuchdateien und Wortlisten	387
Zertifizierungen	388

Stichwortverzeichnis 389

