

Inhaltsverzeichnis

Vorwort	9
Über den Autor	11
Einführung	23
Wer sollte dieses Buch lesen?	24
Über dieses Buch	24
Wie Sie dieses Buch verwenden	25
Was Sie nicht lesen müssen	25
Törichte Annahmen über den Leser	25
Wie dieses Buch aufgebaut ist	25
Teil I: Grundlagen für Sicherheitstests schaffen	26
Teil II: Sicherheitstests praktisch nutzen	26
Teil III: Netzwerkhosts hacken	26
Teil IV: Betriebssysteme hacken	26
Teil V: Anwendungen hacken	26
Teil VI: Aufgaben nach den Sicherheitstests	27
Teil VII: Der Top-Ten-Teil	27
Symbole, die in diesem Buch verwendet werden	27
Wie es weiter geht	28
Eine nicht unwichtige Besonderheit	28
 Teil I	
Den Grundstock für Sicherheitstests legen	29
 Kapitel 1	
Einführung in das ethische Hacken	31
Begriffserklärungen	31
Den Begriff »Hacker« definieren	32
Den Begriff »böswilliger Benutzer« definieren	33
Wie aus arglistigen Angreifern ethische Hacker werden	33
Ethisches Hacken im Vergleich zur Auditierung	34
Betrachtungen zu Richtlinien	34
Compliance und regulatorische Aspekte	34
Warum eigene Systeme hacken?	35
Die Gefahren verstehen, denen Ihre Systeme ausgesetzt sind	36
Nicht-technische Angriffe	36
Angriffe auf Netzwerkinfrastrukturen	37
Angriffe auf Betriebssysteme	37
Angriffe auf Anwendungen und spezielle Funktionen	37

Die Gebote des ethischen Hackens befolgen	38
Ethisch arbeiten	38
Die Achtung der Privatsphäre	38
Bringen Sie keine Systeme zum Absturz	39
Die Arbeitsabläufe beim ethischen Hacken	39
Die Planformulierung	40
Werkzeugwahl	41
Planumsetzung	43
Ergebnisauswertung	44
Wie es weitergeht	44

Kapitel 2

Die Denkweise von Hackern nachvollziehen **45**

Ihre Gegenspieler	45
Wer in Computersysteme einbricht	48
Warum sie das tun	49
Angriffe planen und ausführen	52
Anonymität wahren	54

Kapitel 3

Einen Plan für das ethische Hacken entwickeln **55**

Zielsetzungen festlegen	55
Festlegen, welche Systeme gehackt werden sollen	57
Teststandards formulieren	60
Zeitplanung	60
Spezifische Tests ausführen	61
Tests mit oder ohne Hintergrundwissen	62
Standortauswahl	62
Auf entdeckte Schwachstellen reagieren	63
Törichte Annahmen	63
Werkzeuge für Sicherheitsgutachten auswählen	63

Kapitel 4

Die Methodik des Hackens **65**

Die Bühne für das Testen vorbereiten	65
Sehen, was andere sehen	67
Öffentliche Informationen sammeln	67
Systeme scannen	68
Hosts	68
Offene Ports	69
Feststellen, was über offene Ports läuft	69
Schwachstellen bewerten	72
In das System eindringen	73

Teil II**Mit den Sicherheitstests loslegen** **75****Kapitel 5****Daten sammeln** **77**

Öffentlich verfügbare Daten sammeln	77
Soziale Medien	77
Suche im Web	78
Webcrawler	79
Websites	79
Netzwerkstrukturen abbilden	80
Whois	80
Google Groups	81
Datenschutzrichtlinien	82

Kapitel 6**Social Engineering** **83**

Eine Einführung in Social Engineering	83
Erste Tests im Social Engineering	84
Warum Social Engineering für Angriffe genutzt wird	85
Die Auswirkungen verstehen	86
Vertrauen aufbauen	87
Die Beziehung ausnutzen	87
Social-Engineering-Angriffe durchführen	90
Informationen suchen	90
Maßnahmen gegen Social Engineering	93
Richtlinien	93
Training und Schulung der Nutzer	94

Kapitel 7**Physische Sicherheit** **97**

Erste physische Sicherheitslücken identifizieren	97
Schwachstellen im Büro aufspüren	98
Gebäudeinfrastruktur	99
Versorgung	100
Raumgestaltung und Nutzung der Büros	101
Netzwerkkomponenten und Computer	103

Kapitel 8**Kennwörter 107**

Schwachstellen bei Kennwörtern	108
Organisatorische Schwachstellen von Kennwörtern	108
Technische Schwachstellen bei Kennwörtern	109
Kennwörter knacken	109
Kennwörter auf herkömmliche Weise knacken	110
Kennwörter technisch anspruchsvoll ermitteln	113
Kennwortgeschützte Dateien knacken	121
Weitere Optionen, an Kennwörter zu gelangen	122
Allgemeine Gegenmaßnahmen beim Knacken von Kennwörtern	127
Kennwörter speichern	127
Kennwortrichtlinien erstellen	128
Andere Gegenmaßnahmen ergreifen	129
Betriebssysteme sichern	131
Windows	131
Linux und UNIX	132

Teil III**Netzwerkhosts hacken 133****Kapitel 9****Netzwerkinfrastruktur 135**

Schwachstellen der Netzwerkinfrastruktur	135
Werkzeuge wählen	137
Scanner und Analysatoren	137
Schwachstellenbestimmung	137
Das Netzwerk scannen und in ihm herumwühlen	138
Portscans	138
SNMP scannen	144
Banner-Grabbing	146
Firewall-Regeln testen	147
Netzwerkdaten untersuchen	150
Der Angriff auf die MAC-Adresse	156
Denial-of-Service-Angriffe testen	163
Bekannte Schwachstellen von Routern, Switches und Firewalls erkennen	165
Unsichere Schnittstellen ermitteln	165
IKE-Schwächen ausnutzen	165
Aspekte der Preisgabe von Daten durch SSL und TLS	166
Einen allgemeinen Netzwerkverteidigungswall einrichten	167

Kapitel 10**Drahtlose Netzwerke** **169**

Die Folgen von WLAN-Schwachstellen verstehen	169
Die Werkzeugauswahl	170
Funknetze entdecken	171
Sie werden weltweit erkannt	171
Lokale Funkwellen absuchen	173
Angriffe auf WLANs erkennen und Gegenmaßnahmen ergreifen	174
Verschlüsselter Datenverkehr	175
Wi-Fi Protected Setup	182
Die drahtlosen Geräte von Schurken	184
MAC-Spoofing	189
Physische Sicherheitslücken	193
Angreifbare WLAN-Arbeitsstationen	193

Kapitel 11**Mobilgeräte** **195**

Schwachstellen von Mobilgeräten beurteilen	195
Kennwörter von Laptops knacken	196
Auswahl der Werkzeuge	196
Gegenmaßnahmen	199
Telefone, Smartphones und Tablets knacken	201
iOS-Kennwörter knacken	202
Displaysperre bei Android-Geräten einrichten	205
Maßnahmen gegen das Knacken von Kennwörtern	205

Teil IV**Betriebssysteme hacken** **207****Kapitel 12****Windows** **209**

Windows-Schwachstellen	210
Werkzeuge wählen	210
Kostenlose Microsoft-Werkzeuge	211
Komplettlösungen	211
Aufgabenspezifische Werkzeuge	212
Daten für Windows-Systemschwachstellen sammeln	212
Das System untersuchen	213
NetBIOS	215
Null Sessions entdecken	218
Zuordnung, auch Mapping oder Einhängen	218
Informationen sammeln	219
Maßnahmen gegen Null-Session-Hacks	221

Freigabeberechtigungen überprüfen	222
Windows-Standards	222
Testen	222
Fehlende Patches nutzen	223
Metasploit verwenden	225
Maßnahmen gegen das Ausnutzen fehlender Patches	230
Authentifizierte Scans ablaufen lassen	230

Kapitel 13

Linux

233

Linux-Schwachstellen verstehen	234
Werkzeugauswahl	234
Daten über Schwachstellen von Linux-Systemen sammeln	235
Das System durchsuchen	235
Maßnahmen gegen das Scannen des Systems	239
Nicht benötigte und unsichere Dienste ermitteln	239
Suchläufe	239
Maßnahmen gegen Angriffe auf nicht benötigte Dienste	241
Die Dateien »rhosts« und »hosts.equiv« schützen	243
Hacks, die die Dateien »rhosts« und »hosts.equiv« verwenden	243
Maßnahmen gegen Angriffe auf die Dateien »rhosts« und »hosts.equiv«	244
Die Sicherheit von NFS überprüfen	246
NFS-Hacks	246
Maßnahmen gegen Angriffe auf NFS	246
Dateiberechtigungen überprüfen	247
Das Hacken von Dateiberechtigungen	247
Maßnahmen gegen Angriffe auf Dateiberechtigungen	247
Schwachstellen für Pufferüberläufe finden	248
Angriffe	248
Maßnahmen gegen Buffer-Overflow-Angriffe	249
Physische Sicherheitsmaßnahmen überprüfen	249
Physische Hacks	249
Maßnahmen gegen physische Angriffe auf die Sicherheit	250
Allgemeine Sicherheitstests durchführen	251
Sicherheitsaktualisierungen für Linux	252
Aktualisierungen der Distributionen	252
Update-Manager für mehrere Plattformen	253

Teil V**Anwendungen hacken****255****Kapitel 14****Kommunikations- und Benachrichtigungssysteme****257**

Grundlagen der Schwachstellen bei Messaging-Systemen	257
Erkennung und Abwehr von E-Mail-Angriffen	258
E-Mail-Bomben	258
Banner	262
SMTP-Angriffe	263
Die besten Verfahren, Risiken bei E-Mails zu minimieren	272
Voice over IP verstehen	274
VoIP-Schwachstellen	274
Maßnahmen gegen VoIP-Schwachstellen	278

Kapitel 15**Websites und Webanwendungen****279**

Die Werkzeuge für Webanwendungen auswählen	280
Mit dem Web zusammenhängende Schwachstellen suchen	280
Verzeichnis traversieren	281
Maßnahmen gegen Directory Traversals	284
Eingabe-Filter-Angriffe	284
Maßnahmen gegen Angriffe durch arglistige Eingaben	292
Angriffe auf Standardskripte	292
Maßnahmen gegen Angriffe auf Standardskripte	294
Unsichere Anmeldeverfahren	294
Maßnahmen gegen unsichere Anmeldesysteme	297
Allgemeine Sicherheitsscans bei Webanwendungen durchführen	299
Risiken bei der Websicherheit minimieren	299
Sicherheit durch Obskurität	299
Firewalls einrichten	300
Quellcode analysieren	301
Schwachstellen von Apps für Mobilgeräte aufspüren	303

Kapitel 16**Datenbanken und Speichersysteme****305**

In Datenbanken abtauchen	305
Werkzeuge wählen	305
Datenbanken im Netzwerk finden	306
Datenbankkennwörter knacken	307
Datenbanken nach Schwachstellen durchsuchen	308
Bewährte Vorkehrungen zur Minimierung der Sicherheitsrisiken bei Datenbanken	308

Sicherheit für Speichersysteme	309
Werkzeuge wählen	310
Speichersysteme im Netzwerk finden	310
Sensiblen Text in Netzwerkdateien aufspüren	311
Bewährte Vorgehensweisen zur Minimierung von Sicherheitsrisiken bei der Datenspeicherung	313

Teil VI

Aufgaben nach den Sicherheitstests 315

Kapitel 17

Die Ergebnisse präsentieren 317

Die Ergebnisse zusammenführen	317
Schwachstellen Prioritäten zuweisen	318
Berichte erstellen	320

Kapitel 18

Sicherheitslücken beseitigen 323

Berichte zu Maßnahmen werden lassen	323
Patchen für Perfektionisten	324
Patch-Verwaltung	325
Patch-Automatisierung	325
Systeme härten	326
Die Sicherheitsinfrastrukturen prüfen	328

Kapitel 19

Sicherheitsprozesse verwalten 329

Den Prozess des ethischen Hackens automatisieren	329
Bösartige Nutzung überwachen	330
Sicherheitsprüfungen auslagern	332
Die sicherheitsbewusste Einstellung	334
Auch andere Sicherheitsmaßnahmen nicht vernachlässigen	334

Teil VII

Der Top-Ten-Teil 337

Kapitel 20

Zehn Tipps für die Unterstützung der Geschäftsleitung 339

Sorgen Sie für Verbündete und Geldgeber	339
Geben Sie nicht den Aufschneider	339

Zeigen Sie, warum es sich das Unternehmen nicht leisten kann, gehackt zu werden	339
Heben Sie allgemeine Vorteile des ethischen Hackens hervor	340
Zeigen Sie, wie insbesondere ethisches Hacken Ihrem Unternehmen helfen kann	340
Engagieren Sie sich für das Unternehmen	341
Zeigen Sie sich glaubwürdig	341
Reden Sie wie ein Manager	342
Demonstrieren Sie den Wert Ihrer Anstrengungen	342
Seien Sie flexibel und anpassungsfähig	342

Kapitel 21

Zehn Gründe, warum einzig Hacken effektive Tests ermöglicht **343**

Die Schurken hegen böse Gedanken, nutzen gute Werkzeuge und entwickeln neue Methoden	343
Vorschriften und Regeleinhaltung bedeuten in der IT mehr als Prüfungen mit anspruchsvollen Checklisten	343
Ethisches Hacken ergänzt Prüfverfahren und Sicherheitsbewertungen	344
Kunden und Partner interessieren sich für die Sicherheit Ihrer Systeme	344
Die Wahrscheinlichkeit arbeitet gegen Ihr Unternehmen	344
Sicherheitsprüfungen verbessern das Verständnis für geschäftliche Bedrohungen	344
Bei Einbrüchen können Sie auf etwas zurückgreifen	345
Intensive Tests enthüllen die schlechten Seiten Ihrer Systeme	345
Ethisches Hacken kombiniert die Vorteile von Penetrationstests und Schwachstellenprüfung	345
Sorgfältiges Testen kann Schwachstellen erkennen, die ansonsten vielleicht lange übersehen worden wären	345

Kapitel 22

Zehn tödliche Fehler **347**

Keine Genehmigung vorab einholen	347
Davon ausgehen, dass im Testverlauf alle Schwachstellen gefunden werden	347
Anzunehmen, alle Sicherheitslöcher beseitigen zu können	348
Tests nur einmal ausführen	348
Glauben, alles zu wissen	348
Tests nicht aus der Sicht von Hackern betrachten	349
Die falschen Systeme testen	349
Nicht die richtigen Werkzeuge verwenden	349
Sich zur falschen Zeit mit Produktivsystemen befassen	350
Tests Dritten überlassen und sich dann nicht weiter darum kümmern	350

Anhang Werkzeuge und Ressourcen	351
Allgemeine Suchwerkzeuge	351
Anspruchsvolle Malware	352
Bluetooth	352
Datenbanken	352
Drahtlose Netzwerke	353
Exploits	353
Hacker-Zeugs	354
Kennwörter knacken	354
Keyloggers	355
Linux	355
Live-Toolkits	356
Messaging	356
Mobil	356
Netzwerke	357
Patch-Management	358
Protokollanalyse	359
Quellcode-Analyse	359
Schwachstellendatenbanken	359
Social Engineering und Phishing	359
Speicherung	359
Systeme härten	360
Verschiedenes	360
Voice over IP	360
Wachsamkeit der Benutzer	361
Websites und Webanwendungen	361
Windows	362
Wörterbuchdateien und Wortlisten	362
Zertifizierungen	363
 Stichwortverzeichnis	 365