

# Inhaltsverzeichnis

Über den Autor	7
<b>Einführung</b>	<b>21</b>
Wer sollte dieses Buch lesen?	21
Über dieses Buch	22
Wie Sie dieses Buch verwenden	22
Was Sie nicht lesen müssen	23
Törichte Annahmen über den Leser	23
Wie dieses Buch aufgebaut ist	23
Teil I: Den Grundstock für das ethischen Hacken legen	23
Teil II: Mit dem ethischen Hacken loslegen	24
Teil III: Ein Netzwerk hacken	24
Teil IV: Betriebssysteme hacken	24
Teil V: Anwendungen hacken	24
Teil VI: Nacharbeiten	24
Teil VII: Der Top-Ten-Teil	25
Symbole, die in diesem Buch verwendet werden	25
Wie es weiter geht	25
Eine nicht unwichtige Besonderheit	26
<b>Teil I</b>	
<b>Den Grundstock für das ethischen Hacken legen</b>	<b>27</b>
<b>Kapitel 1</b>	
<b>Eine Einführung in das ethische Hacken</b>	<b>29</b>
Die Terminologie verständlich machen	29
Den Begriff »Hacker« definieren	30
Den Begriff »böswilliger Benutzer« definieren	30
Wie böswillige Angreifer ethische Hacker zeugen	31
Ethisches Hacken im Vergleich zur Auditierung	31
Überlegungen zu Richtlinien	32
Befolgung von Regeln und regulatorische Dinge	32
Warum die eigenen Systeme hacken?	32
Die Gefahren verstehen, mit denen Ihre Systeme konfrontiert werden	33
Nicht technische Angriffe	34
Angriffe auf die Infrastruktur von Netzwerken	34
Angriffe auf das Betriebssystem	34
Angriffe auf Anwendungen und Funktionen	35
Die Gebote des ethischen Hackens	35
Die Privatsphäre respektieren	35
Bringen Sie keine Systeme zum Absturz	36

Die Arbeitsabläufe des ethischen Hackens	36
Den Plan formulieren	36
Werkzeuge auswählen	38
Den Plan ausführen	40
Ergebnisse auswerten	41
Wie es weitergeht	41

## ***Kapitel 2 Die Denkweise von Hackern knacken***

Gegen wen Sie vorgehen	43
Wer in Computersysteme einbricht	46
Warum sie das tun	47
Angriffe planen und ausführen	50
Anonym bleiben	51

## ***Kapitel 3 Einen Plan für das ethische Hacken entwickeln***

Eine Zielrichtung vorgeben	53
Festlegen, welche Systeme gehackt werden sollen	55
Teststandards erstellen	58
Zeitliche Planung	58
Tests gezielt ablaufen lassen	59
Blinde oder Überprüfung mit Kenntnissen	60
Den Standort wählen	61
Auf die Schwachstellen reagieren, die Sie finden	61
Törichte Annahmen	61
Werkzeuge für eine Sicherheitsüberprüfung auswählen	62

## ***Kapitel 4 Die Methodik des Hackens***

Die Bühne für das Testen vorbereiten	63
Sehen, was andere sehen	65
Öffentlich zugängliche Informationen beschaffen	65
Das Netzwerk kartografieren	68
Systeme scannen	70
Hosts	71
Offene Ports	71
Feststellen, was auf offenen Ports läuft	71
Schwachstellen bewerten	74
In das System eindringen	76

<b>Teil II</b>	
<b>Mit dem ethischen Hacken loslegen</b>	<b>77</b>
<b>Kapitel 5</b>	
<b>Social Engineering</b>	<b>79</b>
Eine Einführung in Social Engineering	79
Erste Tests in Social Engineering	80
Warum Angreifer Social Engineering verwenden	82
Die Auswirkungen verstehen	83
Social-Engineering-Angriffe durchführen	84
Informationen abgreifen	84
Vertrauen bilden	87
Die Beziehung ausnutzen	88
Maßnahmen gegen Social Engineering	90
Richtlinien	91
Das Bewusstsein der Benutzer und Benutzerschulung	91
<b>Kapitel 6</b>	
<b>Physische Sicherheitseinrichtungen</b>	<b>95</b>
Erste physische Sicherheitslöcher identifizieren	95
Schwachstellen im Büro lokalisieren	97
Die Infrastruktur eines Gebäudes	98
Versorgung	99
Gestaltung und Nutzung von Büros	100
Netzwerkkomponenten und Computer	102
<b>Kapitel 7</b>	
<b>Kennwörter</b>	<b>105</b>
Schwachstellen bei Kennwörtern	105
Organisatorische Schwachstellen bei Kennwörtern	107
Technische Schwachstellen bei Kennwörtern	108
Kennwörter knacken	109
Kennwörter auf die herkömmliche Art knacken	109
Kennwörter »profimäßig« knacken	112
Kennwortgeschützte Dateien knacken	119
Weitere Wege, um am Kennwörter zu gelangen	121
<b>Teil III</b>	
<b>Netzwerkhosts hacken</b>	<b>125</b>
<b>Kapitel 8</b>	
<b>Die Infrastruktur des Netzwerks</b>	<b>127</b>
Schwachstellen an der Infrastruktur von Netzwerken	128
Werkzeuge wählen	129

Scanner und Analysatoren	130
Schwachstellenprüfung	130
Das Netzwerk scannen und in ihm herumstochern	131
Ports scannen	131
SNMP scannen	137
Banner-Grabbing	138
Firewall-Regeln testen	139
Netzwerkdaten untersuchen	142
Der Angriff auf die MAC-Adresse	147
Denial-of-Service-Angriffe testen	152
Mit bekannten Schwachstellen bei Router, Switch und Firewall umgehen	154
Unsichere Schnittstellen	154
IKE-Schwächen ausnutzen	155
Einen allgemeinen Verteidigungswall für das Netzwerk einrichten	156

***Kapitel 9******Drahtlose Netzwerke*****157**

Die Folgen von Schwachstellen bei drahtlosen Netzwerken verstehen	157
Die Werkzeuge wählen	159
Drahtlose Netzwerke entdecken	160
Sie werden weltweit erkannt	160
Die lokalen Funkwellen scannen	162
Angriffe auf drahtlose Netzwerke erkennen und Gegenmaßnahmen ergreifen	163
Verschlüsselter Verkehr	165
Maßnahmen gegen Angriffe auf verschlüsselten Verkehr	169
WiFi Protected Setup	170
Maßnahmen gegen Schwächen beim WPS-PIN	172
Gefährliche drahtlose Geräte	172
Maßnahmen gegen gefährliche drahtlose Geräte	175
MAC-Spoofing	176
Maßnahmen gegen MAC-Spoofing	180
Physische Sicherheitslöcher	180
Maßnahmen gegen physische Schwachstellen bei der Sicherheit drahtloser Netzwerke	180
Verwundbare drahtlose Arbeitsstationen	181
Maßnahmen gegen Schwachstellen bei drahtlosen Arbeitsstationen	181

***Kapitel 10******Mobile Geräte*****183**

Mobile Schwachstellen einschätzen	183
Kennwörter von Laptops knacken	183
Die Werkzeuge wählen	184
Gegenmaßnahmen	187
Telefone und Tablets knacken	188
iOS-Kennwörter knacken	189
Maßnahmen gegen das Knacken von Kennwörtern	192

<b>Teil IV</b>	
<b>Betriebssysteme hacken</b>	<b>193</b>
<b>Kapitel 11</b>	
<b>Windows</b>	<b>195</b>
Windows-Schwachstellen	196
Werkzeuge wählen	196
Kostenlose Microsoft-Werkzeuge	197
Komplettlösungen	197
Aufgabenspezifische Werkzeuge	198
Informationen über die Schwachstellen Ihres Windows-Systems sammeln	198
Das System untersuchen	199
NetBIOS	201
Null Sessions entdecken	204
Zuordnung, auch Mapping genannt	204
Informationen sammeln	205
Maßnahmen gegen Null-Session-Hacks	207
Freigabeberechtigungen überprüfen	208
Windows-Standards	208
Testen	209
Fehlende sicherheitstechnische Programmaktualisierungen ausnutzen	210
Metasploit verwenden	212
Maßnahmen gegen das Ausnutzen fehlender Programmaktualisierungen	218
Authentifizierte Scans ablaufen lassen	219
<b>Kapitel 12</b>	
<b>Linux</b>	<b>221</b>
Schwachstellen bei Linux verstehen	222
Werkzeuge wählen	222
Informationen über die Schwachstellen Ihrer Linux-Systeme sammeln	223
Das System absuchen	223
Maßnahmen gegen das Scannen des Systems	226
Ungenutzte und unsichere Dienste finden	227
Suchen	227
Maßnahmen gegen Angriffe auf ungenutzte Dienste	229
Die Dateien »rhosts« und »hosts.equiv« schützen	232
Hacks, die die Dateien »rhosts« und »hosts.equiv« verwenden	232
Maßnahmen gegen Angriffe auf die Dateien »rhosts« und »hosts.equiv«	233
Die Sicherheit von NFS überprüfen	234
NFS-Hacks	234
Maßnahmen gegen Angriffe auf das NFS	235
Dateiberechtigungen überprüfen	235
Das Hacken von Dateiberechtigungen	235
Maßnahmen gegen Angriffe auf Dateiberechtigungen	235

Für Buffer-Overflow empfängliche Schwachstellen finden	236
Angriffe	237
Maßnahmen gegen Buffer-Overflow-Angriffe	237
Physische Sicherheitsmaßnahmen überprüfen	237
Physische Hacks	237
Maßnahmen gegen physische Angriffe auf die Sicherheit	238
Allgemeine Sicherheitstests durchführen	239
Sicherheitsaktualisierungen für Linux	240
Aktualisierungen der Distributionen	240
Update-Manager für mehrere Plattformen	241

**Teil V****Anwendungen hacken** 243**Kapitel 13****Kommunikations- und Benachrichtigungssysteme** 245

Eine Einführung in Schwachstellen bei Benachrichtigungssystemen	245
Angriffe auf E-Mail erkennen und ihnen begegnen	246
E-Mail-Bomben	246
Banner	250
SMTP	251
Die besten Methoden, um Risiken bei E-Mails zu minimieren	261
Voice over IP verstehen	263
Schwachstellen von VoIP	263
Maßnahmen gegen Schwachstellen bei VoIP	269

**Kapitel 14****Websites und Webanwendungen** 271

Die Werkzeuge für Webanwendungen auswählen	272
Mit dem Web zusammenhängende Schwachstellen suchen	274
Directory Traversal	274
Maßnahmen gegen Directory Traversals	276
Angriffe über das Filtern von Eingaben	277
Maßnahmen gegen Angriffe über Eingaben	286
Angriffe auf Standardskripte	287
Maßnahmen gegen Angriffe auf Standardskripte	288
Unsichere Anmeldemechanismen	288
Maßnahmen gegen unsichere Anmeldesysteme	291
Allgemeine Sicherheitsscans bei Webanwendungen durchführen	293
Risiken bei der Websicherheit minimieren	293
Sicherheit durch Verbergen	293
Firewalls errichten	294
Quellcode analysieren	294

<b>Kapitel 15</b>	
<b>Datenbanken und Speichersysteme</b>	<b>297</b>
In Datenbanken eintauchen	297
Werkzeuge wählen	297
Datenbanken im Netzwerk finden	299
Datenbankkennwörter knacken	300
Datenbanken nach Schwachstellen absuchen	301
Bewährten Vorgehensweisen folgen, um Sicherheitsrisiken bei Datenbanken zu minimieren	302
Speichersysteme	303
Werkzeuge wählen	303
Speichersysteme im Netzwerk finden	303
Sensiblen Text in Netzwerkdateien ausgraben	304
Bewährten Vorgehensweisen folgen, um Sicherheitsrisiken bei der Datenspeicherung zu minimieren	306
<b>Teil VI</b>	
<b>Die Ernte des ethischen Hackens</b>	<b>309</b>
<b>Kapitel 16</b>	
<b>Die Ergebnisse präsentieren</b>	<b>311</b>
Die Ergebnisse zusammenführen	311
Schwachstellen mit Prioritäten versehen	312
Berichte erstellen	314
<b>Kapitel 17</b>	
<b>Sicherheitslöcher stopfen.</b>	<b>317</b>
Berichte in Aktionen verwandeln	317
Patchen für die Perfektion	318
Patch-Verwaltung	318
Patch-Automatisierung	319
Systeme dicht machen	320
Die Infrastruktur der Sicherheitseinrichtungen überprüfen	320
<b>Kapitel 18</b>	
<b>Sicherheitsverfahren umsetzen</b>	<b>323</b>
Die Abläufe des ethischen Hackens automatisieren	323
Bösartigkeit überwachen	324
Ethisches Hacken an Dritte vergeben	326
Für eine auf Sicherheit gerichtete Einstellung sorgen	328
Auch bei anderen Sicherheitsanstrengungen nicht nachlassen	328

<b>Teil VII</b>	
<b>Der Top-Ten-Teil</b>	<b>331</b>
<b>Kapitel 19</b>	
<b>Zehn Tipps, um die Unterstützung der Geschäftsführung zu erlangen</b>	<b>333</b>
Sorgen Sie für einen Verbündeten und einen Geldgeber	333
Seien Sie kein Aufschneider	333
Zeigen Sie, warum es sich das Unternehmen nicht leisten kann, gehackt zu werden	333
Heben Sie die allgemeinen Vorteile des ethischen Hackens hervor	334
Zeigen Sie, wie ethisches Hacken gerade Ihrem Unternehmen helfen kann	334
Kümmern Sie sich um das Unternehmen	335
Seien Sie glaubwürdig	335
Reden Sie wie ein Manager	335
Zeigen Sie, wie wertvoll Ihre Anstrengungen sind	336
Seien Sie flexibel und anpassungsfähig	336
<b>Kapitel 20</b>	
<b>Zehn Gründe, warum Hacken das einzig sinnvolle Testen ist</b>	<b>337</b>
Die Bösen denken Böses, verwenden gute Werkzeuge und entwickeln neue Methoden	337
Gesetze und die Einhaltung von Regeln bedeuten in der IT immer noch mehr als hochwertige Prüflisten	337
Ethisches Hacken ergänzt Prüfverfahren und Einschätzungen der Sicherheitsstandards	337
Kunden und Partner fragen: »Wie sicher sind Ihre Systeme?«	337
Das Gesetz des Durchschnitts arbeitet gegen Ihr Unternehmen	338
Das ethische Hacken verbessert das Verständnis für Bedrohungen des Unternehmens	338
Wenn es zu einem Einbruch kommt, müssen Sie auf etwas zurückgreifen können	338
Ethisches Hacken fördert das Übelste Ihrer Systeme ans Tageslicht	338
Ethisches Hacken verbindet das Beste der Tests auf Eindringen mit dem Prüfen auf Schwachstellen	339
Ethisches Hacken kann Schwächen aufdecken, die ansonsten vielleicht jahrelang übersehen worden wären	339
<b>Kapitel 21</b>	
<b>Zehn tödliche Fehler</b>	<b>341</b>
Im Vorfeld keine Genehmigung einholen	341
Davon ausgehen, dass Sie im Verlauf Ihrer Tests alle Schwachstellen finden	341
Davon ausgehen, alle Sicherheitslöcher beseitigen zu können	341
Tests nur einmal ausführen	342
Glauben, alles zu wissen	342
Tests nicht aus der Sicht eines Hackers betrachten	342

Die falschen Systeme testen	342
Nicht die richtigen Werkzeuge verwenden	343
Sich zur falschen Zeit mit produktiven Systemen abgeben	343
Tests an Dritte vergeben und sich dann um nichts kümmern	343

<i>Stichwortverzeichnis</i>	<b>345</b>
-----------------------------	------------