

Jürgen Ebner

Einstieg in Ethical Hacking

Penetration Testing & Hacking-Tools
für die IT-Security



Hinweis des Verlages zum Urheberrecht und Digitalen Rechtemanagement (DRM)

Liebe Leserinnen und Leser,

dieses E-Book, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Mit dem Kauf räumen wir Ihnen das Recht ein, die Inhalte im Rahmen des geltenden Urheberrechts zu nutzen. Jede Verwertung außerhalb dieser Grenzen ist ohne unsere Zustimmung unzulässig und strafbar. Das gilt besonders für Vervielfältigungen, Übersetzungen sowie Einspeicherung und Verarbeitung in elektronischen Systemen.

Je nachdem wo Sie Ihr E-Book gekauft haben, kann dieser Shop das E-Book vor Missbrauch durch ein digitales Rechtemanagement schützen. Häufig erfolgt dies in Form eines nicht sichtbaren digitalen Wasserzeichens, das dann individuell pro Nutzer signiert ist. Angaben zu diesem DRM finden Sie auf den Seiten der jeweiligen Anbieter.

Beim Kauf des E-Books in unserem Verlagsshop ist Ihr E-Book DRM-frei.

Viele Grüße und viel Spaß beim Lesen,

Ihr mitp-Verlagsteam



Jürgen Ebner

Einstieg in Ethical Hacking

Penetration Testing & Hacking-Tools für die IT-Security



Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-7475-0692-9

1. Auflage 2024

www.mitp.de

E-Mail: mitp-verlag@sigloch.de

Telefon: +49 7953 / 7189 - 079

Telefax: +49 7953 / 7189 - 082

© 2024 mitp Verlags GmbH & Co. KG, Frechen

Dieses Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Lektorat: Janina Vervost

Sprachkorrektur: Petra Heubach-Erdmann

Covergestaltung: Christian Kalkert

Bildnachweis: © Ruben Chase / stock.adobe.com

Satz: III-satz, Kiel, www.drei-satz.de

Inhaltsverzeichnis

	Einleitung.....	13
Teil 1	Grundlagen des Ethical Hackings	17
1	Was ist (Ethical) Hacking?	19
1.1	Begriffserklärung.....	19
1.2	Was ist ein Hacker?.....	20
1.3	Hackertypen und deren Motivation.....	21
1.3.1	Black Hats.....	22
1.3.2	White Hats oder Ethical Hacker.....	22
1.3.3	Grey Hats.....	22
1.3.4	Script Kiddies.....	22
1.3.5	Blue Team & Red Team.....	23
1.4	Die Rolle des Ethical Hackers.....	23
1.4.1	Hacker-Ethik.....	26
1.4.2	Ethical Hacking vs. Auditierung.....	27
1.5	Wie werde ich ein Hacker oder eine Hackerin?.....	28
1.6	Informationen zu den Tools sammeln.....	29
1.7	Richtlinien, Compliance und regulatorische Aspekte.....	30
1.8	Warum sich selbst hacken?.....	31
1.9	Vorgehensweise und Methodik im Ethical Hacking.....	32
1.10	Gefahren verstehen.....	34
1.10.1	Nicht-technische Angriffe.....	35
1.10.2	Angriffe auf das Netzwerk.....	35
1.10.3	Angriffe auf Betriebssysteme.....	35
1.11	Zusammenfassung.....	36
2	Betriebssysteme für Hacker	37
2.1	Kali Linux.....	37
2.2	Backbox.....	37
2.3	Parrot OS.....	38
2.4	BlackArch.....	39
2.5	Deft Linux.....	40
2.6	Pentoo Linux.....	40
2.7	CAINE.....	41
2.8	Fedora Security Spin.....	42
2.9	Zusammenfassung.....	43

3	Vorbereitung des Betriebssystems	45
3.1	Kali-Linux-Installation	45
	3.1.1 Herunterladen des ISO-Images.	45
	3.1.2 Kopieren des Images auf ein bootfähiges Medium	46
3.2	Stand-Alone-Installation	50
	3.2.1 Partitionierung der Festplatte	56
	3.2.2 Konfigurieren des Package Managers (apt)	59
	3.2.3 GRUB-Bootloader installieren	61
	3.2.4 Installation abschließen und neu starten	63
3.3	Kali Linux als virtuelle Maschine	63
	3.3.1 Installation von VirtualBox	63
	3.3.2 Kali Linux als virtuelle Maschine.	65
4	(Kali-)Linux-Grundlagen	71
4.1	Was ist Linux?	71
4.2	Hardwaresteuerung	73
4.3	Vereinheitlichtes Dateisystem.	74
4.4	Prozessverwaltung	75
4.5	Die Kommandozeile (Command Line)	76
	4.5.1 Wie komme ich zur Kommandozeile?	76
	4.5.2 Verzeichnisbaum durchsuchen und Dateien verwalten	77
	4.5.3 Umgebungsvariablen	79
4.6	Das Dateisystem von Kali	79
	4.6.1 Dateisystem-Hierarchie-Standard	79
	4.6.2 Das Home-Verzeichnis des Anwenders	80
4.7	Rechtmanagement	81
	4.7.1 Benutzerkategorien und Rechte	82
	4.7.2 Rechte verwalten	83
4.8	Hilfreiche Befehle für die Kommandozeile	85
	4.8.1 Anzeigen und Ändern von Text-Dateien.	85
	4.8.2 Suche nach Dateien und innerhalb von Dateien	86
	4.8.3 Prozesse verwalten	86
	4.8.4 Systeminformationen und Logs aufrufen.	87
	4.8.5 Hardware erkennen	88
4.9	Dienste	89
	4.9.1 Init-Systeme	89
	4.9.2 Starten und Beenden von Diensten.	89
	4.9.3 Auffinden und Ablegen von Diensten	90
	4.9.4 Deaktivieren von Diensten.	90
4.10	Zusammenfassung	90

5	Erste Schritte & Hacking-Labor einrichten mit Kali Linux.	91
5.1	Erste Schritte mit Kali Linux.	91
	5.1.1 Verwalten von Diensten in Kali Linux	91
	5.1.2 Übung macht den Meister: Hacking-Labor einrichten	94
5.2	Installation von Tools und Updates	97
	5.2.1 (Kali) Linux updaten.	97
	5.2.2 OpenVAS zur Schwachstellenanalyse.	97
	5.2.3 Dns2proxy.	101
6	Einführung in Security-Assessments.	103
6.1	Was bedeutet »Sicherheit« im Umgang mit Informationssystemen?	103
6.2	Arten von Assessments.	105
	6.2.1 Schwachstellenanalyse	107
	6.2.2 Compliance-Test.	112
	6.2.3 Traditioneller Penetrationstest	113
	6.2.4 Applikations-Assessment.	115
6.3	Normierung der Assessments	117
6.4	Arten von Attacks	118
	6.4.1 Denial of Service (DoS)	118
	6.4.2 Speicherbeschädigungen	119
	6.4.3 Schwachstellen von Webseiten	120
	6.4.4 Passwort-Attacks	121
	6.4.5 Clientseitige Angriffe	121
6.5	Zusammenfassung	122
7	Einführung in Programmierung & Shell-Skripte	125
7.1	Programmiersprachen für Ethical Hacking	125
7.2	Programmieren mit Python	127
	7.2.1 Erste Befehle	128
	7.2.2 Datentypen und Variablen.	129
	7.2.3 Bedingte Anweisungen (Verzweigungen)	132
	7.2.4 Schleifen	133
7.3	Bash-Skripte	135
	7.3.1 Skript ausführbar und verfügbar machen	137
	7.3.2 Ausgaben und Variablen	138
	7.3.3 Schleifen in Skripten	139
7.4	Zusammenfassung	141

Teil 2 Durchführung von Penetrationstests 143

8	Der Penetrationstest	145
8.1	Umfang des Penetrationstests (Scope)	149
8.1.1	Umfang des Projekts definieren	150
8.1.2	Metriken für die Zeitschätzung	151
8.1.3	Zusätzlicher Support und Scope Creep	152
8.2	Fragen zur Erhebung des Umfangs des Penetrationstests	153
8.2.1	Netzwerk-Penetrationstest	153
8.2.2	Penetrationstest für Webanwendungen	154
8.2.3	Wireless-Netzwerk-Penetrationstests	154
8.2.4	Physischer Penetrationstest	155
8.2.5	Social Engineering	156
8.2.6	Fragen an den Abteilungs-/Geschäftsstellenleiter	156
8.2.7	Fragen an Systemadministratoren	156
8.3	Ziele	157
8.3.1	Primär	157
8.3.2	Sekundär	157
8.4	Geschäftsanalyse	157
8.5	Angeben von IP-Bereichen und Domänen	158
8.6	Umgang mit Dritten	158
8.6.1	Cloud-Dienste	159
8.6.2	Internetdienstanbieter (ISP)	159
8.6.3	Managed Security Service Provider (MSSPs)	159
8.6.4	Länder, in denen Server gehostet werden	160
8.7	Definition akzeptabler Social-Engineering-Vorwände	160
8.8	DoS-Tests	160
8.9	Zahlungsbedingungen	160
8.10	Kommunikationswege einrichten	161
8.10.1	Kontaktinformationen für Notfälle	161
8.10.2	Incident-Reporting-Prozess	162
8.10.3	Definition von Vorfällen	162
8.10.4	Häufigkeit von Statusberichten	163
8.10.5	Verschlüsselung und Alternativen	163
8.11	Regeln für den Auftrag	164
8.11.1	Zeitleiste	164
8.11.2	Orte	164
8.11.3	Sensible Informationen schützen	164
8.11.4	Umgang mit Beweismitteln	165
8.11.5	Regelmäßige Statusbesprechungen	165
8.11.6	Uhrzeit zum Testen	166

8.11.7	Berechtigung zum Testen	166
8.11.8	Rechtliche Überlegungen	166
8.12	Vorhandene Funktionen und Technologien	166
8.13	Zusammenfassung	167
9	Informationen sammeln (Aufklärung)	169
9.1	Einführung.	169
9.2	Die Recherche	171
9.3	Identifikation von Zielen	172
9.4	Passives Scannen vs. aktives Scannen	173
9.5	Tools zum Sammeln von Informationen	173
9.5.1	HTTrack – Website als Offline-Kopie.	174
9.5.2	Google Dork – Hacking mit Suchanfragen	176
9.5.3	Newsgroups, Hilfeforen und Co. als Informationsquelle . . .	180
9.5.4	Social Media als Informationsquelle.	181
9.5.5	TheHarvester – E-Mail-Adressen aufspüren und ausnutzen	182
9.5.6	Domäne als Informationsquelle	184
9.5.7	Informationen von DNS-Servern abrufen	186
9.5.8	fierce – Falls Zonentransfer nicht möglich ist.	189
9.5.9	Informationen von E-Mail-Servern gewinnen	189
9.5.10	MetaGooFil – Metadaten extrahieren	190
9.5.11	Maltego – Gesammelte Daten in Beziehung setzen	191
9.5.12	Sherlock – Der Detektiv fürs soziale Netz	193
9.5.13	Social Engineering – Menschliche Schwachstellen ausnutzen	195
9.6	Auswertung der Informationen und nach Zielen suchen	196
9.7	Wie kann man diese Schritte üben?	197
9.8	Zusammenfassung	199
10	Aktives Scannen.	201
10.1	Einführung.	201
10.1.1	Ermitteln der aktiven Hosts mittels Ping	201
10.1.2	Portscan.	202
10.1.3	Untersuchung der Ergebnisse mittels NSE	203
10.1.4	Schwachstellen-Scan mit OpenVAS	203
10.2	Aktive Hosts mittels Ping aufspüren	204
10.3	Portscan	206
10.3.1	Scannen mit Nmap	207
10.3.2	Nmap Script Engine – Transformation eines Tools	215
10.3.3	Portscan abschließen	217
10.4	Automation bei der Informationsbeschaffung mit legion	219

10.5	Schwachstellen-Scan	221
10.5.1	Arten von Schwachstellen-Scans und des Erkennens von Schwachstellen.	221
10.5.2	Was bewirken Schwachstellen-Scan-Tools?	222
10.5.3	Welche Schwachstellen-Scanner gibt es?	223
10.5.4	Scan-Ergebnisse auswerten mit Schwachstellendatenbanken	224
10.5.5	OpenVAS – Sicherheitslücken aufdecken	226
10.6	Siege – Performance Test von Webseiten	231
10.6.1	Konfiguration	232
10.7	Wie kann man diese Schritte üben?	233
10.8	Was sind die nächsten Schritte?	233
10.9	Zusammenfassung	234
11	Eindringen über das lokale Netzwerk.	235
11.1	Zugriff auf Remotedienste	237
11.1.1	Medusa	237
11.2	Übernahme von Systemen	240
11.2.1	Metasploit	241
11.2.2	Meterpreter	249
11.3	Passwörter hacken	250
11.3.1	Lokales Passwort-Cracking.	252
11.3.2	Passwort-Cracking über das Netzwerk	255
11.3.3	JtR – Passwort-Cracking.	256
11.3.4	Knacken von Linux-Passwörtern	259
11.3.5	Abrissbirnen-Technik – Passwörter zurücksetzen.	260
11.4	Passwörter aus dem Active Directory	263
11.4.1	LLMNR Poisoning	263
11.4.2	SMB Relay	265
11.5	Netzwerkverkehr ausspähen (Sniffing)	267
11.5.1	Wie kann man den Netzwerkdatenverkehr abhören?	267
11.5.2	dsniff – Sammlung von Werkzeugen zum Ausspionieren von Netzwerkdatenverkehr	269
11.5.3	macof – Aus einem Switch einen Hub machen.	270
11.5.4	WireShark – Der Hai im Datenmeer	271
11.5.5	Ettercap – Datenverkehr abfangen und manipulieren.	274
11.6	Armitage – Hacking mit dem »Maschinengewehr«	276
11.7	Wie kann man diesen Schritt üben?	280
11.8	Was sind die nächsten Schritte?	281
11.9	Zusammenfassung	283

12	Webgestütztes Eindringen	285
12.1	Grundlagen des Webhackings	285
12.1.1	Anforderungen abfangen, die vom Browser ausgehen	286
12.1.2	Webseiten, Verzeichnisse und sonstige Dateien finden, die für die Webanwendung notwendig sind	286
12.1.3	Antworten von Webanwendungen analysieren und auf Schwachstellen durchsuchen	287
12.2	Schwachstellen in Webapplikationen finden	288
12.2.1	Nikto – Aufspüren von Schwachstellen auf Webservern ...	288
12.2.2	watobo – Mehr als nur eine hübsche Oberfläche.	289
12.3	WebScarab – Webseiten analysieren (Spider)	295
12.3.1	Konfiguration und Spiderangriff.	296
12.3.2	Anforderungen abfangen.	298
12.4	Code-Injection	300
12.5	Wenn Browser Webseiten vertrauen – XSS-Angriffe.	304
12.6	ZAP – Zed Attack Proxy, das All-in-one-Tool	307
12.6.1	ZAP als Proxy	307
12.6.2	Informationen abfangen	307
12.6.3	Informationen sammeln (Spiderangriff) mit ZAP	309
12.6.4	Schwachstellen-Scan mit ZAP.	310
12.7	Wie kann man diesen Schritt üben?	310
12.8	Was sind die nächsten Schritte?	312
12.9	Zusammenfassung	313
13	Social Engineering	315
13.1	Grundlagen von SET	315
13.2	Spear-Phishing.	317
13.3	Webseite als Angriffsweg	317
13.4	Credential Harvester	323
13.5	Weitere Optionen in SET	324
13.6	Zusammenfassung	327
14	Nachbearbeitung & Erhaltung des Zugriffs	329
14.1	Netcat – Das Schweizer Taschenmesser	330
14.2	Cryptcat – Ein kryptischer Vetter von Netcat.	336
14.3	Rootkits.	337
14.3.1	Rootkits erkennen und abwehren	339
14.4	Meterpreter – Der Hammer, der aus allem einen Nagel macht ...	341
14.5	Wie kann man diesen Schritt üben?	344
14.6	Was sind die nächsten Schritte?	345
14.7	Zusammenfassung	346

15	Abschluss eines Penetrationstests	347
15.1	Tools für den Report	348
	15.1.1 Cutycapt	348
	15.1.2 Faraday-IDE	350
	15.1.3 Pipal	354
	15.1.4 RecordMyDesktop	354
15.2	Testbericht schreiben	355
	15.2.1 Zusammenfassung für die Geschäftsführung	356
	15.2.2 Rohausgaben	356
	15.2.3 Abschluss und Übermittlung des Berichts	357
15.3	Was sind die nächsten Schritte?	359
15.4	Zusammenfassung	361
A	Nachwort	363
	Stichwortverzeichnis	367



Einleitung

Es ist noch nicht lange her, dass Hacking eher ein Tabu war, und es gab auch keine Schulungen dazu. Aber inzwischen hat sich die Erkenntnis breitgemacht, dass auch ein offensiver Ansatz einen Mehrwert für die IT-Sicherheit liefert. Diese neue Herangehensweise wird von vielen Organisationen aller Größen und Branchen begrüßt: Staatliche Stellen machen inzwischen Ernst mit offensiver Sicherheit, Regierungen geben auch offiziell zu, dass sie daran arbeiten.

Für das Sicherheitskonzept einer Organisation spielen vor allem Penetrationstests eine wichtige Rolle. Richtlinien, Risikobewertungen, Notfallpläne und die Wiederherstellung nach Katastrophen sind zu unverzichtbaren Maßnahmen zum Erhalt der IT-Sicherheit geworden und genauso müssen auch Penetrationstests in die Gesamtplanung für die Sicherheit aufgenommen werden. Mit solchen Tests können Sie erkennen, wie Sie vom Feind wahrgenommen werden. Das kann zu vielen überraschenden Entdeckungen führen und Ihnen kostbare Zeit geben, um Ihre Systeme zu verbessern, bevor es einen echten Angriff gibt.

Für das Hacking stehen heutzutage viele gute Werkzeuge zur Verfügung. Viele davon sind nicht einfach nur »da«, sondern laufen aufgrund der langjährigen Entwicklungszeit auch sehr stabil. Noch wichtiger ist für viele die Tatsache, dass die meisten dieser Tools kostenlos erhältlich sind.

Das ist zwar schön, aber Sie müssen diese Werkzeuge erst einmal finden, kompilieren und installieren, bevor auch nur der einfachste Penetrationstest durchgeführt werden kann. Auf den modernen Linux-Betriebssystemen geht das zwar relativ einfach, aber für Neulinge kann es immer noch eine abschreckende Aufgabe sein. Auch für Fortgeschrittene ist es mühsam, alle Tools erst mal zusammenzusuchen und zu installieren.

Die Security-Community ist glücklicherweise eine sehr aktive und freigiebige Gruppe. Mehrere Organisationen haben unermüdlich daran gearbeitet, verschiedene Linux-Distributionen für Hacking und Penetrationstests zu erstellen. Eine Distribution (kurz Distro) ist eine Variante von Linux. Für Hacking und Penetrationstests gibt es Linux-Distros wie

- Parrot Security OS
- BlackBox
- BlackArch
- Fedora Security Spin

- Samurai Web Testing Framework
- Pentoo Linux
- DEFT Linux
- Caine
- Network Security Toolkit (NST)
- Kali Linux

Die bekannteste Distro für Penetrationstests ist Kali Linux. Wir werden in diesem Buch deshalb auch Kali Linux verwenden, um die verschiedenen Tools fürs Hacking zu nutzen, die aber auch in allen anderen Linux-Distributionen und teilweise sogar unter Windows verwendet werden können. Mit Kali Linux, aber auch den anderen Betriebssystemen für das Hacking, erhalten angehende Sicherheitsexperten, Pentester und IT-Verantwortliche eine umfangreiche Plattform, um digitale Attacken zu planen und durchzuführen.

Warum sollte man das tun wollen?

Einerseits, um sich mit potenziellen Angriffen auf die eigenen Systeme auseinanderzusetzen, und andererseits, um interne und externe Schwachstellen besser zu verstehen.

Ein »Hacker-Betriebssystem« wie Kali Linux & Co. ist standardmäßig schon voller Tools, die Sicherheitsexperten und IT-Verantwortlichen entweder den Schlaf rauben oder ihre Augen glitzern lassen.

Die Hacker-Betriebssysteme enthalten eigentlich nichts Exklusives – man kann sich jedes Tool, jede Software und jedes Skript auf jedem beliebigen Linux (teilweise auch Windows) installieren –, dennoch greifen viele Sicherheitsforscher auf eine Distribution wie Kali zurück.

Der Grund, warum gerne Distributionen wie Kali & Co. verwendet werden, ist, dass die meisten Programme samt den passenden Einstellungen bereits mit der Installation der Distribution mitgeliefert werden oder einfach aus den Repositorien installiert werden können. Ein weiterer Grund ist, dass Kali sich sehr gut als isolierte Umgebung betreiben lässt. Sollte doch mal etwas schiefgehen, kann das System rasch neu installiert werden und man kann von vorne anfangen – das ist natürlich um vieles besser, als sich eine Produktivumgebung komplett zu zerschießen.

Vorsicht

Die falsche Anwendung von Security-Tools in Ihrem Netzwerk – vor allem ohne Erlaubnis – kann irreparablen Schaden mit erheblichen Folgen anrichten. Testen bzw. greifen Sie nie Systeme ohne Erlaubnis an.

Über dieses Buch

Dieses Buch ist ein praktischer Leitfaden für alle, die sich für das Thema Ethical Hacking und Penetration Testing interessieren. Es richtet sich sowohl an Einsteiger als auch an Fortgeschrittene, die ihre Fähigkeiten im Bereich der IT-Sicherheit erweitern wollen. Das Buch erklärt die Grundlagen des Ethical Hacking, die rechtlichen und ethischen Aspekte, sowie die wichtigsten Methoden und Werkzeuge, die Hacker verwenden, um Schwachstellen in Netzwerken und Systemen zu finden und auszunutzen. Anhand von zahlreichen Beispielen lernen Sie, wie Sie selbst Sicherheitstests durchführen können.

Ich habe das Buch so aufgebaut, dass Sie es auch verwenden können, wenn Sie noch keine Erfahrungen mit Security-Assessments haben bzw. noch nicht mit Linux gearbeitet haben. Wenn Sie das Buch gelesen haben, sollten Sie als Penetrationstester – auch wenn Sie ein Anfänger sind – Security-Assessments erfolgreich durchführen können.

Im ersten Teil des Buches finden Sie alle Grundlagen, die Sie für das Ethical Hacking brauchen, insbesondere eine kurze Einführung in Kali Linux, die Einrichtung Ihres Hacking-Labors sowie die wichtigsten Linux-Grundlagen, damit Sie, falls Sie Linux-Anfänger sind, keine Probleme haben, den Anleitungen im Buch zu folgen. Sie erfahren, welche Arten von Security-Assessments es gibt und welche Rolle das Penetration Testing dabei spielt. Weiterhin erhalten Sie einen Überblick über die Funktionsweise der Programmiersprache Python sowie BASH-Skripte, die für die Anpassung bestehender Hacking-Tools bzw. die Automatisierung nützlich sind.

Der zweite Teil des Buches konzentriert sich auf die Planung und Durchführung von Penetrationstests. Sie lernen die verschiedenen Testphasen sowie eine Vielzahl von Attacken und passender Hacking-Tools im Detail kennen und erfahren, welche Richtlinien Sie bei der Durchführung Ihrer Tests einhalten sollten, um sicher und ethisch zu hacken.

Weitere Infos

Um Interessierte über die aktuellen Security-Themen und Änderungen in meinen Büchern auf dem Laufenden zu halten, habe ich eine Homepage (<https://www.jurgenebner.com/>) eingerichtet. Hier können Sie mir auch Feedback zu meinen Büchern geben, damit wir weitere Auflagen verbessern können.

Teil 1

Grundlagen des Ethical Hackings

In diesem Teil des Buches erfahren Sie alles, was Sie brauchen, um mit dem Ethical Hacking zu beginnen. Wir betrachten die Unterschiede zwischen den Zielen ethischer Hacker und bösartiger Angreifer. Außerdem schauen wir uns an, wie das ethische Hacken entstanden ist und sich entwickelt hat.

In diesem Buch werden wir zwar mit Kali-Linux arbeiten, aber es ist nicht für jeden das geeignete Tool, deshalb werden wir uns auch anschauen, welche Alternativen es zu Kali Linux gibt, damit Sie wenn nötig darauf zurückgreifen können.

Bevor Sie mit dem Hacking starten können, müssen Sie sich noch das System einrichten. Für dieses Buch haben wir uns für einen schnellen Start entschieden, deshalb werden wir das Image für Virtual Box verwenden. Daneben wird auch die allgemeine Installation von Kali Linux beschrieben.

In diesem Teil:

- **Kapitel 1**
Was ist (Ethical) Hacking?19
- **Kapitel 2**
Betriebssysteme für Hacker37
- **Kapitel 3**
Vorbereitung des Betriebssystems45
- **Kapitel 4**
(Kali-)Linux-Grundlagen71
- **Kapitel 5**
Erste Schritte & Hacking-Labor einrichten
mit Kali Linux.....91
- **Kapitel 6**
Einführung in Security-Assessments103
- **Kapitel 7**
Einführung in Programmierung & Shell-Skripte ..125

Was ist (Ethical) Hacking?

Mit diesem Buch sollten Sie in der Lage sein, Schwachstellen auf Ihren Computer und in Ihrem Netzwerk aufzuspüren und gefundene Schwachstellen zu beseitigen, bevor Cyber-Kriminelle die Möglichkeit haben, diese auszunutzen.

Da der Begriff »Ethik« häufig missverständlich gebraucht wird, schauen wir uns einmal an, wie der Begriff in Wörterbüchern definiert ist:

Gesamtheit sittlicher Normen und Maximen, die einer [verantwortungsbewussten] Einstellung zugrunde liegen.

Diese Definition passt auch sehr gut zu diesem Buch und den hier behandelten professionellen Sicherheitstests und -techniken. Fachleute aus IT- und Datensicherheit sind verpflichtet, die hier vorgestellten Techniken ehrlich und nur dann durchzuführen, wenn sie **die ausdrückliche Erlaubnis der Inhaber der Systeme erhalten haben**.

1.1 Begriffserklärung

Wenn man die Medienberichte verfolgt, ist klar, dass viele bereits die Folgen von Cyber-Angriffen zu spüren bekommen. Deshalb haben viele sicher schon von Hackern und böswilligen Anwendern gehört. Aber um wen handelt es sich bei den Leuten? Was sollten Sie über diese wissen?

Um Missverständnissen in diesem Buch vorzubeugen, definieren wir hier folgende Begriffe:

- **Hacker:** Hier versucht ein externer Angreifer, Computer und sensible Daten anzugreifen, um ein illegales Ziel zu erreichen. Es werden dabei beinahe alle Systeme angegriffen, die als Angriffsziel lohnend sein können.
- **Böswillige Anwender:** Dabei handelt es sich um interne Angreifer, die als berechtigte und »vertrauenswürdige« Anwender von innen heraus Computer und sensible Daten angreifen. Ein böswilliger Anwender greift die Systeme meistens an, um sich zu rächen, aber in einigen Fällen verfolgt er auch illegale Ziele.

Angreifer können zugleich Hacker als auch böswillige Anwender sein. Es ist einfacher, beide als Hacker zu bezeichnen und ich werde nur dann einen Unterschied zwischen beiden Begriffen machen, wenn wir uns intensiver mit deren Werkzeugen, Techniken und Denkweisen beschäftigen müssen.

- **Ethische Hacker:** Hier handelt es sich um die »Guten«, die Systeme hacken, um ihre Schwachstellen aufzudecken, um Schutzmaßnahmen gegen unberechtigte Zugriffe aufbauen zu können. Zu diesen können IT-Security-Berater als auch internes Personal zählen.

1.2 Was ist ein Hacker?

Wenn wir an einen Hacker denken, dann fällt vielen der typische Computer-Nerd im Kapuzenpullover ein. Doch was ist ein Hacker wirklich?

Die beste Beschreibung, die ich bisher gehört habe, die aber wenig mit Computern zu tun hat, lautet: Ein Hacker ist eine Person, die auf kreative Art und Weise ein Problem löst.

In der ursprünglichen Bedeutung war es noch ein Tüftler im Kontext einer verspielten, selbstbezogenen Hingabe im Umgang mit Technik und einem besonderen Sinn für Kreativität. Jedoch ist der Begriff heute meist negativ behaftet und wir verstehen darunter eine Person, die illegal in Computersysteme eindringt. Diese Person hat Spaß daran, programmierbare Systeme zu erforschen, und geht dabei bis an die Grenzen ihrer Fähigkeiten. Sie liebt die intellektuelle Herausforderung, Hindernisse auf kreative Art und Weise zu überwinden und zu umgehen. Hier versucht die Person mit dem Wissen über technische Geräte sowie das Internet, die Technik zu überlisten, zweckzuentfremden oder zu modifizieren.

Was unterscheidet Programmierer oder Informatiker von Hackern? Es ist nicht leicht, diese Frage zu beantworten, da es keine feste Definition gibt. Programmierer(in) ist ein normaler Job, den man erlernen kann, ohne automatisch ein Hacker oder eine Hackerin zu sein.

Es gibt aber einige Punkte, die Hacker von Programmierern unterscheiden: Hacker probieren neue Dinge aus. Dinge, die nicht dokumentiert sind. Sie experimentieren und testen Software oder Hardware. Sie wissen nicht unbedingt, wie alles funktioniert, und versuchen, die Software oder Hardware über ihre Tests zu verstehen. Programmierer und Programmiererinnen bleiben bei den Systemen, die sie kennen. Hacker versuchen, die Software zu einem Verhalten zu bringen, das ihrem Zweck dient. Sie versuchen, die Ecken zu finden, die nicht dokumentiert sind, was oft Trial-and-Error bedeutet. Hacker haben Freude daran, was bei anderen normalerweise Frust hervorruft. In der Regel fühlen sie sich davon herausgefordert und ruhen selten, bevor sie nicht verstanden haben, was gerade passiert.

Hacker(innen) teilen ihre Erkenntnisse häufig mit der Community, um damit für besseres Verständnis zu sorgen. Sie dokumentieren ihre Schritte, um auch andere auf diesen Punkt zu bringen. Das hilft ihnen dabei, auch über ihre Fähigkeiten hinauszukommen.

Sie können die Hacker aufgrund ihrer Tätigkeit unterschiedlichen Szenen zuordnen: Hardware Hacker, Open Source Software, Security, Hacktivismus, File Sharing und Cracking-Szene. Die Aufzählung ist bestimmt nicht vollzählig. Man hat in der Szene versucht, die illegalen Tätigkeiten von den »guten« Hackern zu trennen. Aus diesem Grund wurde versucht, den Begriff »Cracker« zu etablieren. Aber leider hat er sich nicht durchgesetzt, deshalb müssen wir akzeptieren, dass das Wort »Hacker« ein Sammelbegriff für viele Beschreibungen geworden sind.

Heutzutage wird die Bezeichnung »Hacker« meist missverstanden. Sie klingt in der allgemeinen Sprache negativ, meint aber eigentlich hochversierte Computerfreaks. Es handelt sich um Menschen, die sich mit Computersystemen beschäftigen und zugleich besonders neugierig sind. Es sind Menschen, die Herausforderungen lieben und gerne Neues erlernen. Den Hacker zeichnet es aus, kreativ zu sein, eigene Ideen zu entwickeln, Neues zu schaffen und die eigenen Fertigkeiten möglichst kreativ einzusetzen. Hacker sind bereit, harte Arbeit zu leisten, um ihre Ziele zu erreichen, und teilen ihr Wissen mit ihresgleichen. Das sind eigentlich alles positive Eigenschaften, die sich viele Unternehmen von ihren Mitarbeitern wünschen.

Wie überall gibt es auch unter den Hackern schwarze Schafe. Diese spezielle Gruppierung der Hacker sind die kriminellen Cracker: Es sind jene Freaks, die für das negative Image der Hacker verantwortlich sind. Sie dringen in Netzwerke und Computersysteme ein, stehlen Daten und knacken Passwörter.

1.3 Hackertypen und deren Motivation

Unter dem Begriff »Hacker« werden die guten Hacker in dieselbe Schublade wie die heimlich operierenden Hacker gesteckt. Aus diesem Grund spricht man auch oft von »White Hat«- und »Black Hat«-Hackern. Diese Einteilung stammt aus alten Western-Filmen, in denen die Guten immer weiße und die Bösen immer schwarze Hüte getragen haben. Trotzdem verbinden heutzutage die meisten Menschen etwas Negatives mit dem Begriff »Hacker«.

Hinweis

Viele bösartigen Hacker behaupten, es zum Wohle der Gesellschaft machen und keinen schädigen zu wollen. Achten Sie darauf, einen Sicherheitsbeauftragten nicht mit einem kriminellen Hacker zu verwechseln. Der Sicherheitsbeauftragte hackt in ehrlichen Interessen und entwickelt auch jene Werkzeuge, die uns bei der Arbeit unterstützen. Sie sind sich ihrer Verantwortung bewusst und sorgen dafür, dass ihre Ergebnisse und die Quelltexte ihrer Programme veröffentlicht werden.

1.3.1 Black Hats

Black Hats sind die bösen Hacker. Sie nutzen ihre Fähigkeiten mit krimineller und destruktiver Absicht. Sie dringen illegal in Systeme ein und stehlen Daten oder verschlüsseln diese. Sie erpressen Unternehmen, stehlen Geld oder richten Schaden an. Black Hats verändern auch fremde Software, um einen Kopierschutz aufzuheben oder unbemerkt eine Schadsoftware anzuhängen. Sie stehlen digitale Identitäten, um sich selbst Vorteile zu verschaffen, und stören zudem die Verfügbarkeit von Diensten mittels Denial-of-Service-Angriffen.

1.3.2 White Hats oder Ethical Hacker

White Hats nutzen ihre Fähigkeiten für die Verteidigung von Systemen. Es handelt sich dabei häufig um unabhängige Security-Consultants, die Sicherheitsmaßnahmen und Systeme analysieren und Maßnahmen zur Verbesserung der Sicherheit vorschlagen.

White Hats haben Freude am Hacken von Webseiten, Apps und Programmen. Sie helfen Unternehmen und Personen, alle möglichen Fehler, Schwachstellen und Bugs in ihrer Software zu finden.

1.3.3 Grey Hats

Gray Hats veröffentlichen (un)absichtlich ihre gefundenen Schwachstellen aus bekannten Betriebssystemen und Software im Internet. Die Schwachstellen können von allen, auch den Black Hats, ausgenutzt werden. Für die Unternehmen läuft die Zeit, sie müssen die Schwachstelle rasch schließen, um das Risiko eines erfolgreichen Angriffs zu reduzieren.

Gray Hats sind der Meinung, dass Software- und Hardwarehersteller für die Sicherheit der eigenen Produkte verantwortlich sind, und überlassen es dem Schicksal, ob die von ihnen veröffentlichten Informationen für gute oder schlechte Zwecke eingesetzt werden.

1.3.4 Script Kiddies

Bei den Script Kiddies handelt es sich um Jugendliche, die ein Tool im Netz finden, mit dem sie Unternehmen oder eine Privatperson angreifen und ihre Opfer gezielt zur Weißglut bringen. Selten ist hier das Ziel, Geld zu machen, sondern es geht darum, die eigenen Fähigkeiten auszutesten und das Ziel zu ärgern.

Diese Gruppe war vor allem in den frühen Jahren des Hackings noch weit verbreitet, bildet aber nur noch einen kleinen Teil der Angreifer.

1.3.5 Blue Team & Red Team

Hier handelt es sich um die zwei Seiten der Medaille für den Schutz von IT-Systemen.

Beim Red Team handelt es sich um Penetration Tester, die nach Schwachstellen in den Systemen suchen und so versuchen, in die Systeme einzudringen. Hierzu zählen auch die »Bug-Bounty-Hunter«. Diese Gruppe sucht nach Schwachstellen für Unternehmen im Rahmen eines Bug-Bounty-Programms. Viele Unternehmen, vor allem Software-Hersteller wie Microsoft, Google, Amazon, Twitter & Co., haben Bug-Bounty-Programme, die es erlauben, die Programme auf Schwachstellen zu prüfen.

Das Blue Team bilden die Cyber-Security-Analysten, die die Systeme gegen die Angriffe schützen. Es gibt auch Wettbewerbe, bei denen Blue Teams einen Server mit Demodaten vor dem Red Team schützen. Die Red Teams versuchen dabei, unbemerkt in die Systeme einzudringen.

1.4 Die Rolle des Ethical Hackers

Die Rolle des Ethical Hackers, auch als White Hat Hacker oder Sicherheitsexperte bezeichnet, ist von entscheidender Bedeutung, wenn es um die Sicherheit von IT-Systemen und Netzwerken geht. Im Gegensatz zu böswilligen Hackern, die Schwachstellen ausnutzen, um unbefugten Zugriff zu erlangen und Schaden anzurichten, hat der Ethical Hacker eine völlig andere Zielsetzung. Ethisches Hacken erfolgt in einem professionellen Umfeld mit der Genehmigung der »Opfer«. Seine Hauptaufgabe besteht darin, Sicherheitslücken und Schwachstellen in einem System zu identifizieren, bevor diese von Angreifern ausgenutzt werden können.

Der Ethical Hacker geht dabei in der Regel methodisch vor und es besteht eine gute Chance, die Auswirkungen bössartiger Angriffe bereits im Testbetrieb auszuwerten, mit dem Ziel, noch vor der Produktivstellung neuer Software oder Änderungen in der Netzwerkkonfiguration einen höheren Sicherheitsgrad zu erreichen.

Ein ethischer Hacker stellt im Rahmen eines sogenannten Audits folgende Fragen:

- Was kann ein Angreifer auf dem Zielsystem sehen?
- Welche Server und Geräte sind für ihn sichtbar?
- Welche dieser Geräte sind für ihn erreichbar?
- Wie kann der Angreifer die gewonnenen Informationen gegen das Unternehmen einsetzen?
- Sind seine Versuche und Erfolge in den Systemen nachvollziehbar?
- Welche Systeme sind im Unternehmen zu schützen?

- Gegen wen oder was muss geschützt werden?
- Welche Maßnahmen sind jeweils angemessen?
- Wie hoch ist das Budget, das das Unternehmen für einen ausreichenden Schutz bereitstellen kann?

Es ist die Aufgabe des ethischen Hackers, die Systeme von Unternehmen hinsichtlich der bekannten Cyber-Attacken abzusichern. Da es, wie bekannt ist, keinen 100%igen Schutz gibt, sind Ethical Hacker bemüht, Detect-, Alert- und Log-Mechanismen zu installieren, um eventuelle Angriffe bis zum Angreifer zurück nachvollziehen zu können.

Statt sich auf die Sicherheitsmechanismen von eingekauften Standardsystemen zu verlassen, dringt der Ethical Hacker im Auftrag des Unternehmens in dessen IT-Infrastruktur ein. Genauso hartnäckig wie ein böswilliger Angreifer penetriert der ethische Hacker das Unternehmensnetzwerk und sucht eine Lücke, über die er eindringen kann. Er scannt alle von außen und innen erreichbaren Geräte und versucht, die darauf installierten Betriebssysteme und Dienste zu ermitteln. Sobald er eine Sicherheitslücke gefunden hat, verschafft er sich einen Zugriff zu dem betroffenen System und hinterlässt dort als Beweis eine Nachricht für den Auftraggeber.

Bei diesem Vorgehen, das man auch als »Penetrationstest« bezeichnet, arbeitet der ethische Hacker vorsichtig und achtet darauf, produktiv laufende Dienste nicht zu beeinträchtigen. Angriffe, die auf die Abschaltung bestimmter Dienste abzielen, werden dabei nicht auf produktiven Systemen, sondern ausschließlich auf Testsystemen durchgeführt. Buffer-Overflows-, Denial-of-Service-(Dos-)Angriffe oder Wurmattaken werden dabei in einem abgeschotteten Testnetzwerk durchgeführt. Um aber die gleichen Bedingungen zu schaffen wie auf den produktiven Systemen, muss die gleiche Hardware und Netzwerkkonfiguration eingesetzt werden; das betrifft Firewalls, Router, Switches, Datenbanken, Webserver, Mail-Server, FTP-Server und vieles mehr.

Darüber hinaus hat ein Ethical Hacker folgende Aufgaben:

■ **Autorisierte Sicherheitstests**

Der Ethical Hacker führt Sicherheitstests nur mit ausdrücklicher Erlaubnis des Eigentümers oder Verwalters des Systems oder Netzwerks durch. Bevor ein Sicherheitstest durchgeführt wird, muss der Ethical Hacker einen schriftlichen Auftrag erhalten, der die Ziele, den Umfang und die Bedingungen des Tests festlegt. Die Autorisierung gewährleistet, dass der Ethical Hacker rechtmäßig handelt und keine rechtlichen Konsequenzen befürchten muss.

■ **Identifizierung von Schwachstellen**

Die Hauptaufgabe des Ethical Hackers besteht darin, Schwachstellen und Sicherheitslücken in einem System oder Netzwerk zu identifizieren. Hierbei

setzt er verschiedene Methoden und Techniken ein, wie zum Beispiel Penetrationstests, Vulnerability Scans und Code Reviews. Durch die Identifizierung von Schwachstellen kann der Ethical Hacker dem Unternehmen dabei helfen, proaktiv auf potenzielle Bedrohungen zu reagieren und entsprechende Sicherheitsmaßnahmen zu ergreifen.

■ Vermeidung von Sicherheitsvorfällen

Indem der Ethical Hacker Sicherheitslücken aufdeckt, trägt er maßgeblich dazu bei, Sicherheitsvorfälle zu verhindern. Durch die Behebung von Schwachstellen, bevor sie von böswilligen Hackern ausgenutzt werden können, schützt der Ethical Hacker das Unternehmen vor finanziellen Verlusten, Reputationsrisiken und rechtlichen Konsequenzen.

■ Beratung und Empfehlungen

Nach Abschluss eines Sicherheitstests erstellt der Ethical Hacker einen detaillierten Bericht mit den identifizierten Schwachstellen und Sicherheitslücken. Dieser Bericht enthält auch Empfehlungen und Vorschläge, wie die Sicherheit des Systems verbessert werden kann. Der Ethical Hacker fungiert somit als Berater für das Unternehmen und unterstützt es dabei, eine effektive Sicherheitsstrategie zu entwickeln und umzusetzen.

■ Sensibilisierung und Schulung

Der Ethical Hacker trägt auch zur Sensibilisierung und Schulung der Mitarbeiter bei. Durch Schulungen und Workshops können die Mitarbeiter für die Bedeutung der IT-Sicherheit sensibilisiert werden und lernen, wie sie sich vor Phishing-Angriffen, Social Engineering und anderen Sicherheitsbedrohungen schützen können.

■ Gesetzliche Aspekte und Ethik

Der Ethical Hacker muss sich strikt an ethische Richtlinien und gesetzliche Bestimmungen halten. Er darf nur autorisierte Tests durchführen und muss sicherstellen, dass seine Aktivitäten den geltenden Gesetzen und Vorschriften entsprechen. Der Ethical Hacker hat eine ethische Verpflichtung, die Privatsphäre und die Daten des Unternehmens zu respektieren und vertrauliche Informationen vertraulich zu behandeln.

Zusammenfassend lässt sich sagen, dass die Rolle des Ethical Hackers von großer Bedeutung für die Sicherheit von IT-Systemen und Netzwerken ist. Durch die Identifizierung von Schwachstellen und Sicherheitslücken trägt der Ethical Hacker maßgeblich dazu bei, Sicherheitsvorfälle zu verhindern und das Unternehmen vor finanziellen Schäden und Rufverlust zu schützen. Die enge Zusammenarbeit zwischen dem Ethical Hacker und dem Unternehmen ist unerlässlich, um eine effektive Sicherheitsstrategie zu entwickeln und umfassende Schutzmaßnahmen umzusetzen. Ethical Hacking ist somit ein unverzichtbarer Bestandteil eines ganzheitlichen Sicherheitskonzepts.

Es ist also durchaus möglich, dass Hacking ethisch ist!

Für viele mag es nach einem Widerspruch klingen, aber es ist eine ausgezeichnete Methode, sich gegen bösartige Angriffe abzusichern. Es schafft eine solide Basis für mehr Sicherheit, wenn man sich nicht auf die Funktionen der eingekauften Systeme verlässt, sondern die eigene Infrastruktur hinterfragt und ausreichend testet. Angreifer interessieren sich meistens nicht für das Netzwerk eines bestimmten Unternehmens, auf das sie es abgesehen haben: Sie scannen das Internet nach ihnen bekannten Schwachstellen ab und greifen dort an, wo ein schneller Erfolg mit wenig Aufwand möglich ist.

Der beste Weg, sein Netzwerk vor Hackern zu schützen, ist, selbst wie ein Hacker zu denken.

1.4.1 Hacker-Ethik

Ein Hacker, der mit einem ausdrücklichen Auftrag der Verantwortlichen eines Unternehmens arbeitet, um das Unternehmen vor Angriffen zu schützen, hat sich ethisch korrekt zu verhalten. Das bedeutet, er schadet dem Unternehmen nicht und stiehlt auch keine Informationen. Sein Anliegen ist es, die Integrität und Vertrauenswürdigkeit der Systeme eines Unternehmens zu festigen.

Bei der professionellen Durchführung von Sicherheitstests müssen ethische Hacker daher die folgenden Regeln einhalten.

Ethisch arbeiten

Das bedeutet vor allem, sich an professionellen Moralvorstellungen und Prinzipien zu orientieren, unabhängig davon, ob es sich um Tests an eigenen Systemen oder Auftragsarbeiten handelt. Die Unternehmensziele müssen dabei unterstützt werden. Dazu zählt vor allem, dass Ergebnisse immer rückhaltlos vorgelegt werden, auch wenn es für Sie ein Nachteil sein kann.

Der oberste Grundsatz lautet immer Vertrauenswürdigkeit. Diese stellt auch die beste Möglichkeit dar, um Mitarbeiter auf Dauer vom Sicherheitsprogramm zu überzeugen. Ein Datenmissbrauch ist ein absolutes No-Go. So würden nur Black-Hat-Hacker agieren.

Achtung der Privatsphäre

Sie müssen die gesammelten Daten mit allergrößtem Respekt behandeln. Alles, was Sie bei Ihren Tests erfahren, muss privat bleiben. Dazu zählen Protokolldateien von Webanwendungen, Kennwörter im Klartext, aber auch persönliche Daten. Schnüffeln Sie niemals in vertraulichen Firmendaten oder im Privatleben der Mitarbeiter des getesteten Unternehmens herum.

Tipp

Binden Sie immer andere in den Prozess mit ein und sorgen Sie für Zeugen. Wenn Sie selbst beaufsichtigt werden, sorgt das vor allem für mehr Vertrauen.

Bringen Sie keine Systeme zum Absturz

Der größte Fehler, der beim Hacken von Systemen auftritt, besteht darin, Systeme, die eigentlich geschützt werden sollten, versehentlich zum Absturz zu bringen. Das passiert vor allem bei schlechter Planung. Häufig werden die Möglichkeiten und Grenzen sowie der Nutzen der verwendeten Werkzeuge und Techniken nicht gut genug verstanden.

Die Wahrscheinlichkeit ist nicht hoch, aber durch das Testen können für die Systeme DoS-Bedingungen entstehen. Das geschieht vor allem dann, wenn zu viele und zu schnell Tests ausgeführt werden. Es kann dann zu Systemausfällen, Beschädigung von Daten, Systemneustarts und Ähnlichem kommen. Häufig kommt es beim Testen von Webseiten und -anwendungen vor.

Es kann auch passieren, dass Sie Konten versehentlich dauerhaft oder vorübergehend sperren, indem Sie jemanden veranlassen, Passwörter zu ändern, ohne dass dieser die Konsequenzen derartiger Situationen erkennt. Seien Sie immer vorsichtig und gehen Sie mit gesundem Menschenverstand an Ihre Aufgabe heran.

1.4.2 Ethical Hacking vs. Auditierung

Häufig wird Ethical Hacking mit einer Sicherheitsüberprüfung (Auditierung) verwechselt, aber es gibt hierbei Unterschiede. Bei einem Audit vergleicht man Sicherheitsrichtlinien eines Unternehmens mit den aktuell gültigen Standards. Ein Audit wird durchgeführt, um zu überprüfen, dass es Sicherheitskontrollen gibt, dabei wird üblicherweise ein risikobasierter Ansatz verfolgt, das heißt, dass Sie sich mit allen Risiken der Systeme auseinandersetzen und diese entsprechend bewerten. Bei Sicherheitsaudits werden oft auch Geschäftsabläufe überdacht, wobei die Abläufe nicht unbedingt technisch ausgerichtet sein müssen, sondern einfach nur auf Sicherheitsfragen basieren.

Beim Ethical Hacking konzentriert man sich auf potenziell nutzbare Schwachstellen. Dabei wird geprüft, ob Sicherheitskontrollen effektiv sind oder zumindest überhaupt existieren. Ethical Hacking kann einerseits sehr technisch sein, andererseits auch auf niedrigem technischem Niveau ablaufen. Auch wenn hier formale Vorgehensweisen verfolgt werden, sind diese tendenziell weniger strukturiert als bei formalen Sicherheitsaudits. Bei Unternehmensaudits (z.B. für die Zertifizierung ISP 9001 oder 27001) sollten Sie darüber nachdenken, die hier vorgestellten Techniken des Ethical Hacking auch im Auditierungsprozess einzubinden.

1.5 Wie werde ich ein Hacker oder eine Hackerin?

Um diese Frage hier im Buch auch beantworten zu können, habe ich sie in unterschiedliche Suchmaschinen eingegeben. Bei der Suche stellten sich immer drei Hauptthemen heraus:

- Grundlegende Fertigkeiten des Hackens erwerben
- Wie ein Hacker denken
- Respekt verdienen

Der erste Punkt ist leicht abzuhandeln, es ist das Grundwissen, das man sich aneignen muss. Hierbei handelt es sich vor allem um IT-Grundlagen. Dieses Wissen lässt sich auch abseits der bekannten Wege wie Ausbildung erlangen. Es ist ein wichtiger Bestandteil dieses Buches: Wie bekomme ich dieses Wissen aus dem Internet?

Ein Teil dieser Grundlagen sind:

- Verstehen, wie der Computer funktioniert
- Betriebssysteme verstehen
- Ein gutes Betriebssystem beherrschen – in der Regel Linux
- Verstehen, wie logische Abläufe funktionieren
- Programmabläufe verstehen
- Programmieren lernen
- Verstehen, wie man mit verschiedenen Datenstrukturen umgeht
- Datenbanken verstehen
- Wissen, wie Netzwerke funktionieren
- Wissen, wie das Internet funktioniert

Beim Thema, wie ein Hacker zu denken, wird es schwieriger. Es geht hierbei oft darum, sich kreative Lösungen zu überlegen oder Dinge zu verbinden, die nicht offensichtlich zusammengehören. Diese Fertigkeit steigt erst mit den technischen Fähigkeiten.

Der dritte Punkt »Respekt verdienen« ist schwerer zu erklären. Es ist hiermit nicht gemeint, ein möglichst cooler Hacker zu sein, wie es im Script-Kiddie-Bereich durchaus üblich ist. Es geht nicht um den Hack selbst, sondern um Sie als Person. Aufrichtig sein, zuhören und lernen, Empathie und Hilfe anbieten, andere respektieren und sich deren Respekt verdienen. Dabei handelt es sich um keine Einbahnstraße.

Dieses Buch, das Internet und andere Hacker und Hackerinnen sind ein guter Startpunkt, um Wissen zu sammeln, herauszufinden, was Sie besonders interessiert, und etwas damit anzufangen.

Ich möchte Sie darauf hinweisen, dass die meisten Dokumentationen auf Englisch verfasst sind, daher ist es empfehlenswert, Englisch zu können. Einzelne Fachbegriffe sind schnell nachgeschlagen, aber ohne technischen Wortschatz wird es fast unmöglich.

Tipp

Sollten Sie darüber nachdenken, für Ihre Kunden ethisch zu hacken und Tests durchzuführen, oder wenn Sie Ihre Referenzen und Leistungsnachweise um ein zusätzliches Zertifikat erweitern wollen, können Sie im Rahmen des EC-Council¹ den Certified Ethical Hacker (C|EH) erwerben oder bei Offensive Security² eine Zertifizierung, z.B. OSCP, machen.

1.6 Informationen zu den Tools sammeln

Grundlagen sind sehr wichtig, um das gesamte Zusammenspiel der Komponenten zu verstehen, seien es nun die Netzwerkkomponenten innerhalb der zu testenden Infrastruktur oder die der eingesetzten Tools. Generell ist die IT-Welt sehr komplex, darum spezialisieren sich viele auf einzelne Themenbereiche. Beim Hacken ist es sinnvoll, ein Generalist zu sein und ein breites Spektrum zu erlernen, aber nur, so weit es auch benötigt wird. Beim Hacking werden aber auch ganz andere Fähigkeiten notwendig. Es ist wichtig, dass Sie Informationen schnell finden sowie abstrakte oder neue Konzepte schnell verstehen und umsetzen können. Glücklicherweise haben wir das Internet zur Verfügung.

Zwei der wichtigsten Werkzeuge sind ein Browser und eine Suchmaschine. Dabei ist es egal, welche Suchmaschine benutzt wird, datenschutzfreundliche Alternativen wie DuckDuckGo liefern ähnliche Ergebnisse wie Google. Welche Suchmaschine Sie nutzen, ist das Ergebnis des Abwägens Ihrer persönlichen Wünsche.

Da viele Suchergebnisse, die wir uns erarbeitet haben, früher oder später nicht mehr erreichbar sind, empfiehlt es sich, eine persönliche Wissensdatenbank anzulegen. Das bedeutet, Sie speichern sich gute Erklärvideos, Artikel oder PDFs offline ab. Gute Artikel, Schaubilder oder Texte kopiere ich entweder direkt heraus oder drucke mir die Webseite als PDF aus. Die Druckansicht ist meistens auch schöner, übersichtlicher und ohne Werbung.

Da nicht bekannt ist, wie lange URLs noch existieren, werde ich in diesem Buch darauf verzichten, diese mit Ihnen zu teilen. Aber egal, nach welchen Begriffen ich gesucht habe, ich habe immer die gleichen oder ähnliche Inhalte gefunden.

¹ <https://www.eccouncil.org/>

² <https://www.offensive-security.com/>

Es gibt viele Blogartikel im Internet, die einzelne Themen gut erklären, aber die besten Quellen sind häufig die offiziellen Dokumentationen oder Spezifikationen, danach kommen die Wikis und Stackoverflows. Sie können sich dort gerne die eine oder andere Idee anschauen, aber Sie sollten sie immer noch einmal überprüfen, bevor Sie etwas übernehmen.

Es gibt viele Fachbücher als Open-Book-Projekt zum Herunterladen. Diese sind zum Nachschlagen auch passend, aber nur eine praktische Anleitung erklärt Ihnen die Zusammenhänge. Solche Anwendungsbeispiele lassen sich als »how to« oder »tutorial« finden.

Wenn Sie sich für ein Tool entschieden haben, können Sie auch speziell nach Bedienungsanleitungen, Blogposts und Tutorials für dieses Tool suchen, die Sie dann für Ihren Lernprozess ebenfalls dokumentieren und speichern sollten. Es gibt neben den größeren Dokumentationen häufig auch Programm-Cheat-Sheets, nach denen Sie suchen können. Dabei handelt es sich um kleine Spickzettel, die oft benutzte Beispiele oder Funktionen dokumentieren. Sie können sich auch eigene Cheat Sheets anlegen, falls es keine oder keine guten gibt, die Ihren Bedürfnissen entsprechen.

Um einen schnellen Einstieg in ein Thema zu haben, gehe ich immer gleich vor:

- Einen groben Überblick über das Thema verschaffen
- Dokumentationen lesen
- Beispiele suchen
- Prototypen entwickeln bzw. testen/üben

1.7 Richtlinien, Compliance und regulatorische Aspekte

Sollte ethisches Hacken ein Bestandteil Ihres IT-Risikomanagements werden, dann benötigen Sie unbedingt schriftliche Richtlinien für Ihre Sicherheitstests. Diese Richtlinien beschreiben,

- welche Art von ethischem Hacken ausgeführt wird,
- welche Systeme (Server, Webanwendungen, Laptops und so weiter) berücksichtigt werden und
- wie oft die Prüfung vorgenommen wird.

Sie sollten auch darüber nachdenken, eine Dokumentation der jeweils verwendeten Testwerkzeuge anzulegen, in der diese beschrieben und die Termine für die regelmäßigen Tests Ihrer Systeme vorgegeben werden. So können Sie z.B. vorgeben, dass externe Systeme vierteljährlich und interne Systeme halbjährlich getestet werden müssen.