Eric Amberg | Daniel Schmid

Hacking

Der umfassende Praxis-Guide

Inkl. Prüfungsvorbereitung zum CEHv12

3. Auflage

mitp

Eric Amberg, Daniel Schmid

Hacking

Der umfassende Praxis-Guide

Inkl. Prüfungsvorbereitung zum CEHv12

mitp

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.

Bei der Herstellung des Werkes haben wir uns zukunftsbewusst für umweltverträgliche und wiederverwertbare Materialien entschieden.
Der Inhalt ist auf elementar chlorfreiem Papier gedruckt.

ISBN 978-3-7475-0872-5
3. Auflage 2024

www.mitp.de
E-Mail: mitp-verlag@sigloch.de
Telefon: +49 7953 / 7189 - 079
Telefax: +49 7953 / 7189 - 082

Lektorat: Sabine Schulz, Nicole Winkel
Sprachkorrektorat: Petra Heubach-Erdmann
Covergestaltung: Christian Kalkert
Bildnachweis: © ZayNyi / stock.adobe.com
Satz: III-satz, Husby, www.drei-satz.de

Inhaltsverzeichnis

Einleitung

Sie suchen nach einem strukturierten, umfassenden Praxishandbuch zum Thema »Ethical Hacking und Penetration Testing«? Prima, dann sind Sie hier genau richtig! In diesem Buch lernen Sie die Vorgehensweisen und Techniken professioneller Hacker und Penetration-Tester kennen und erlernen das Handwerk von der Pike auf. Durch viele Schritt-für-Schritt-Anleitungen, die Sie selbst in Ihrem Hacking-Labor nachvollziehen können, erleben Sie die Hacking-Techniken quasi live und in der Praxis. Hier ist Mitmachen angesagt!

Dieses Buch versteht sich zum einen als Praxisleitfaden für einen fundierten Einstieg in die Welt der Hacker und Penetration-Tester. Zum anderen sind die Inhalte an das Curriculum des Certified-Ethical-Hacker-Examens (CEHv12) des EC-Council angelehnt, sodass Sie dieses Werk als zusätzliche Ressource für die Prüfungsvorbereitung nutzen können. Bitte beachten Sie hierzu, dass es bestimmte Voraussetzungen für die Prüfungszulassung gibt, die wir Ihnen im ersten Kapitel erläutern.

Das CEH-Examen unterliegt ständigen Aktualisierungen, die naturgemäß nicht im bereits gedruckten Buch berücksichtigt werden können. Im Buch-Memberbereich auf `www.hacking-akademie.de/buch/member` versuchen wir aber, immer zeitnah aktualisierte Informationen bereitzustellen. Die Zugangsdaten zum Memberbereich finden Sie am Ende dieser Einleitung.

Für wen ist dieses Buch geeignet?

Dieses Buch ist für Sie geeignet, wenn Sie sich praxisorientiert und umfassend mit den Themen Hacking und Penetration Testing beschäftigen möchten. Die Zielgruppe umfasst insbesondere:

- Angehende Ethical Hacker und Penetration-Tester
- System- und Netzwerkadministratoren mit Fokus auf IT-Sicherheit
- Verantwortliche im Bereich IT-Security
- Interessierte Power-User

Auch wenn Sie sich durch einfaches Durchlesen des Buches bereits einen guten Überblick über das Thema verschaffen können, ist der Inhalt eher dazu konzipiert, tief in die Materie einzutauchen, und fordert Sie mit konkreten praktischen Beispielen zum Mitmachen auf. Dies erfordert bei Ihnen auf diesem Level auch ein ordentliches Maß an Engagement und Eigeninitiative. Aber genau so lernen Sie die Methoden nicht nur in der Theorie, sondern direkt in der praktischen Umsetzung.

Die Inhalte bauen an einigen Stellen aufeinander auf, sodass das Buch für ein umfassendes Verständnis Kapitel für Kapitel durchgearbeitet werden sollte. Natürlich eignet es sich darüber hinaus auch als Nachschlagewerk, da zu allen Inhalten, die für das Verständnis eines Themas benötigt werden, entsprechende Verweise zu den jeweiligen Stellen im Buch vorhanden sind.

Für wen ist dieses Buch nicht geeignet?

Auch wenn Sie in diesem Buch sehr viele Hacking-Tools kennenlernen werden, so möchten wir an dieser Stelle doch klar betonen, dass das Buch nicht für Scriptkiddies gedacht ist, die mit ein paar wenigen Klicks coole Hacks zaubern und ihre Freunde beeindrucken wollen. Leser, die ohne viel Hintergrundwissen und Engagement ein paar oberflächliche Tricks lernen wollen, finden sicher andere Literatur interessanter.

Andersherum geht es hier auch nicht darum, versierten Profis, die bereits tief in den Themen stecken, den letzten Schliff zu geben. Zu jedem Thema, das das Buch aufgreift, lassen sich eigene Bücher schreiben. Auch wenn die Seitenzahl sehr groß ist, können wir zu vielen Themen nicht mehr als einen fundierten, praxisnahen Einstieg bieten.

Was werden Sie hier lernen?

In diesem Buch geht es um Ethical Hacking und Penetration Testing. Wir werden diese Begriffe noch detaillierter beschreiben. Vom Grundsatz handelt es sich darum, die Perspektive des Angreifers einzunehmen, um die Schwachstellen von Computersystemen und -netzwerken aufzudecken. Dabei haben wir unter dem Strich das Ziel, die IT-Systeme sicherer zu machen. Es geht also nicht darum, die gefundenen Schwachstellen für die eigene Bereicherung zu nutzen, sondern darum, dem Auftraggeber die Möglichkeit zu geben, diese zu beseitigen. Anders ausgedrückt, bilden wir Sie hier zu einem »gutartigen« Hacker aus. Die Vorgehensweise, Technologien und eingesetzten Tools sind jedoch weitgehend dieselben, wie sie von bösartigen Hackern verwendet werden. Diese lernen Sie damit also ebenfalls kennen. Es ist wie so oft: Nicht die Werkzeuge bestimmen darüber, ob sie etwas verbessern oder Schaden anrichten, sondern derjenige, der sich diese Werkzeuge zunutze macht und einsetzt.

Hacking ist einerseits sehr kreativ und individuell, andererseits gibt es aber auch eine sinnvolle Vorgehensweise mit verschiedenen Phasen, die in fast jedem professionellen Hacking-Angriff enthalten sind. Sie erfahren, welche das sind und wie die einzelnen Phasen ablaufen. Viele Hacking-Tätigkeiten bauen aufeinander auf, andere kommen nur in bestimmten Szenarien zum Tragen. Wir haben in diesem Buch fast alle relevanten und gängigen Bereiche abgedeckt: angefangen vom simplen Passwort-Hacking über diverse Web-Hacking-Szenarien bis hin zu Mobile- und IoT-Hacking. Für alle Angriffsformen werden effektive Verteidigungsmaßnahmen aufgelistet, so dass Sie Ihre Kunden dabei unterstützen können, die gefundenen Schwachstellen zu beheben.

Der Fokus in diesem Buch liegt allerdings auf den Angriffstechniken. Sie erhalten zum einen fundierte Hintergrundinformationen zur Vorgehensweise und zu den Hacking-Techniken und zum anderen viele Praxisszenarien, in denen Sie Ihr neues Wissen praktisch einsetzen können. Nachdem Sie dieses Buch durchgearbeitet und die Szenarien praktisch nachvollzogen haben, sind Sie auf dem besten Weg zu einem fähigen Ethical Hacker und Penetration-Tester. Im Anschluss sind Sie in der Lage, Ihre Fähigkeiten eigenständig weiterzuentwickeln und mit zusätzlichen Informationsquellen Ihr Know-how zu vertiefen. Zudem erhalten Sie eine wertvolle Ressource für die Vorbereitung auf das CEHv12-Examen, mit dem Sie Ihre Karriere als Ethical Hacker effektiv voranbringen können.