



Eigenes  
Hacking-Labor

Alle Beispiele sind  
legal mit kostenlosen  
Programmen  
durchführbar

Dr. Patrick  
Engebretson

# Hacking Handbuch

Penetrationstests planen und durchführen

Seien Sie schneller als die Hacker und nutzen Sie deren Techniken und Tools: Kali Linux, Metasploit, Armitage, Wireshark, JtR, Rootkits, Netcat, Meterpreter und mehr.

Dr. Patrick  
Engbretson

# **Hacking Handbuch**

Dr. Patrick  
Engebretson

# Hacking Handbuch

Penetrationstests planen und durchführen

Seien Sie schneller als die Hacker und nutzen Sie deren Techniken und Tools: Kali Linux, Metasploit, Armitage, Wireshark, JtR, Rootkits, Netcat, Meterpreter und mehr.

## Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Alle Angaben in diesem Buch wurden vom Autor mit größter Sorgfalt erarbeitet bzw. zusammengestellt und unter Einschaltung wirksamer Kontrollmaßnahmen reproduziert. Trotzdem sind Fehler nicht ganz auszuschließen. Der Verlag und der Autor sehen sich deshalb gezwungen, darauf hinzuweisen, dass sie weder eine Garantie noch die juristische Verantwortung oder irgendeine Haftung für Folgen, die auf fehlerhafte Angaben zurückgehen, übernehmen können. Für die Mitteilung etwaiger Fehler sind Verlag und Autor jederzeit dankbar. Internetadressen oder Versionsnummern stellen den bei Redaktionsschluss verfügbaren Informationsstand dar. Verlag und Autor übernehmen keinerlei Verantwortung oder Haftung für Veränderungen, die sich aus nicht von ihnen zu vertretenden Umständen ergeben. Evtl. beigefügte oder zum Download angebotene Dateien und Informationen dienen ausschließlich der nicht gewerblichen Nutzung. Eine gewerbliche Nutzung ist nur mit Zustimmung des Lizenzinhabers möglich.

This edition of **The Basics of Hacking and Penetration Testing** by Patrick Engebretson is published by arrangement with **ELSEVIER INC.**, a Delaware corporation having its principal place of business at 360 Park Avenue South, New York, NY 10010, USA

ISBN der englischen Originalausgabe: 978-0124116443

© 2015 Franzis Verlag GmbH, 85540 Haar bei München

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Das Erstellen und Verbreiten von Kopien auf Papier, auf Datenträgern oder im Internet, insbesondere als PDF, ist nur mit ausdrücklicher Genehmigung des Verlags gestattet und wird widrigenfalls strafrechtlich verfolgt.

Die meisten Produktbezeichnungen von Hard- und Software sowie Firmennamen und Firmenlogos, die in diesem Werk genannt werden, sind in der Regel gleichzeitig auch eingetragene Warenzeichen und sollten als solche betrachtet werden. Der Verlag folgt bei den Produktbezeichnungen im Wesentlichen den Schreibweisen der Hersteller.

**Programmleitung:** Dr. Markus Stäuble

**Satz und Übersetzung:** G&U Language & Publishing Services GmbH

**art & design:** [www.ideehoch2.de](http://www.ideehoch2.de)

**Druck:** C.H. Beck, Nördlingen

Printed in Germany

ISBN 978-3-645-60417-8

# Inhaltsverzeichnis

Danksagung.....	11
Der Autor .....	13
Einleitung .....	15
<b>1 Penetrationstests – was ist das?.....</b>	<b>25</b>
1.1 Einführung.....	25
1.2 Vorbereitungen.....	26
1.3 Einführung in Kali Linux: »Werkzeuge. Jede Menge Werkzeuge.«.....	30
1.4 Arbeiten auf dem Angriffscomputer: Die Engine starten.....	36
1.5 Ein Hacker-Labor einrichten und nutzen .....	40
1.6 Die Phasen eines Penetrationstests .....	43
1.7 Wie geht es weiter? .....	50
1.8 Zusammenfassung .....	51
<b>2 Aufklärung .....</b>	<b>53</b>
2.1 Einführung.....	53
2.2 HTTrack: Ein Website-Kopierer.....	59
2.3 Google-Direktiven: Üben Sie sich in Google-Fu!.....	64
2.4 Harvester: E-Mail-Adressen aufspüren und ausnutzen.....	73
2.5 Whois .....	77
2.6 Der Befehl host.....	83
2.7 Informationen von DNS-Servern abrufen.....	84