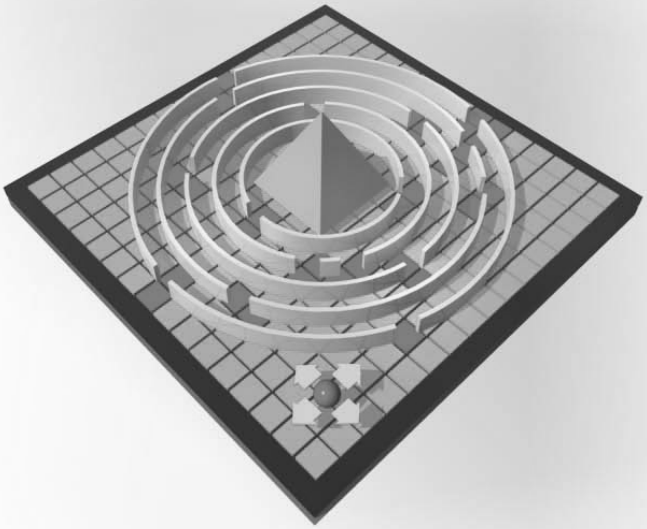
Computer & Literatur Verlag GmbH

Die Kunst des Penetration Testing

Marc Ruef



Deutsche Nationalbibliothek – CIP-Einheitsaufnahme
Bibliografische Information der Deutschen Nationalbibliothek

Ein Titeldatensatz für diese Publikation ist bei
der Deutschen Nationalbibliothek erhältlich und im Internet über
http://dnb.ddb.de abrufbar.

1. Auflage 2007

Zavelsteiner Straße 20, 71034 Böblingen
E-Mail: info@cul.de
WWW: http://www.cul.de

Coverdesign: Hawa & Nöh, Neu-Eichenberg
Satz: C&L-Verlag
Druck: PUT i RB DROGOWIEC
Printed in Poland

Dieses Buch wurde auf chlorfrei gebleichtem Papier gedruckt

ISBN: 978-3-936546-49-1

Inhalt

Kapitel 4
Reconnaissance – Zielnetzwerk auswerten
Seite 103

Kapitel 5
Mapping – Aktive Systeme erkennen
Seite 201

Kapitel 6
Portscanning – Dienste ermitteln
Seite 315

Kapitel 7
Application Mapping – Dienste ermitteln
Seite 395

Kapitel 8
OS Fingerprinting – Betriebssystemerkennung
Seite 439

Kapitel 9
Application Fingerprinting – Anwendungen ermitteln
Seite 491

Kapitel 10
Denial of Service – Destruktive Attacken
Seite 547

Kapitel 11
Firewall-Systeme – Auswertung und Angriffe
Seite 585

Kapitel 12
Debugging – Systematische Fehlersuche
Seite 665

Kapitel 13
Exploits – Schwachstellen ausnutzen
Seite 725