

ALL ■ IN ■ ONE

# CEH Certified Ethical Hacker

EXAM GUIDE

Matt Walker



New York • Chicago • San Francisco • Lisbon  
London • Madrid • Mexico City • Milan • New Delhi  
San Juan • Seoul • Singapore • Sydney • Toronto

McGraw-Hill is an independent entity from the International Council of E-Commerce Consultants® (EC-Council) and is not affiliated with EC-Council in any manner. This study/training guide and/or material is not sponsored by, endorsed by, or affiliated with EC-Council in any manner. This publication and CD may be used in assisting students to prepare for The Certified Ethical Hacker (CEH™) exam. Neither EC-Council nor McGraw-Hill warrant that use of this publication and CD will ensure passing any exam. CEH is a trademark or registered trademark of EC-Council in the United States and certain other countries. All other trademarks are trademarks of their respective owners.

Cataloging-in-Publication Data is on file with the Library of Congress

McGraw-Hill books are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. To contact a representative, please e-mail us at [bulksales@mcgraw-hill.com](mailto:bulksales@mcgraw-hill.com).

### CEH™ Certified Ethical Hacker All-in-One Exam Guide

Copyright © 2012 by The McGraw-Hill Companies. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

All trademarks or copyrights mentioned herein are the possession of their respective owners and McGraw-Hill makes no claim of ownership by the mention of products that contain these marks.

1234567890 QFR QFR10987654321

ISBN: Book p/n 978-0-07-177230-3 and CD p/n 978-0-07-177231-0  
of set 978-0-07-177229-7

MHID: Book p/n 0-07-177230 8 and CD p/n 0-07-177231-6  
of set 0-07-177229-4

**Sponsoring Editor**

Timothy Green

**Technical Editor**

Brad Horton

**Production Supervisor**

James Kussow

**Editorial Supervisor**

Jody McKenzie

**Copy Editor**

Bart Reed

**Composition**

Apollo Publishing Services

**Project Editor**

Emilia Thiuri, Fortuitous Publishing  
Services

**Proofreader**

Louise Watson

**Illustration**

Lyssa Wald

**Acquisitions Coordinator**

Stephanie Evans

**Indexer**

Jack Lewis

**Art Director, Cover**

Jeff Weeks

The views and opinions expressed in all portions of this publication belong solely to the author and/or editor and do not necessarily state or reflect those of the Department of Defense or the United States Government. References within this publication to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, do not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government.

Some glossary terms included in this book may be considered public information as designated by The National Institute of Standards and Technology (NIST). NIST is an agency of the U.S. Department of Commerce. Please visit [www.nist.gov](http://www.nist.gov) for more information.

Information has been obtained by McGraw-Hill from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill, or others, McGraw-Hill does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

This book is dedicated to my children:  
Faith, Hope, Christian, and Charity.  
They are the world to me.

---

## ABOUT THE AUTHOR

**Matt Walker**, an IT Security and Education professional for over 20 years, has served as the Director of the Network Training Center and the Curriculum Lead/Senior Instructor for the local Cisco Networking Academy on Ramstein AB, Germany. After leaving the U.S. Air Force, Matt served as a Network Engineer for NASA's Secure Network Systems (NSS), designing and maintaining secured data, voice, and video networking for the Agency. Soon thereafter, Matt took a position as Instructor Supervisor and Senior Instructor at Dynetics, Inc., in Huntsville, Alabama, providing onsite certification awarding classes for ISC2, Cisco, and CompTIA, and after two years came right back to NASA as the IT Security Manager for UNITeS, SAIC, at Marshall Space Flight Center. He has written and contributed to numerous technical training books for NASA, Air Education and Training Command, the U.S. Air Force, as well as commercially, and he continues to train and write certification and college-level IT and IA Security courses. Matt holds numerous commercial certifications, including CEHv7, CPTS, CNDA, CCNA, and MCSE. Matt is currently the IT Security Manager for Lockheed Martin at Kennedy Space Center.

### **About the Technical Editor**

**Brad Horton** currently works as an Information Security Specialist with the U.S. Department of Defense. Brad has worked as a security engineer, commercial security consultant, penetration tester, and information systems researcher in both the private and public sectors.

This has included work with several defense contractors, including General Dynamics C4S, SAIC, and Dynetics, Inc. Mr. Horton currently holds CISSP, CEH, CISA, and CCNA trade certifications. Brad holds a bachelor's degree in Commerce and Business Administration from the University of Alabama, a master's degree in Management of Information Systems from the University of Alabama in Huntsville (UAH), and a graduate certificate in Information Assurance from UAH. When not hacking, Brad can be found at home with his family or on a local golf course.

The views and opinions expressed in all portions of this publication belong solely to the author and/or editor and do not necessarily state or reflect those of the Department of Defense or the United States Government. References within this publication to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, do not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government.

## **About the Contributing Editor**

**Angie Walker** is currently an Information Systems Security Engineer for Harris Corporation, located in Melbourne, Florida. Among the many positions she has filled over the course of her 20-plus years in Information Technology and Information Assurance are Chief Information Security Officer for the University of North Alabama, Manager of the Information Systems Security (ISS) office for the Missile Defense Agency (MDS) South, and lead for the MDA Alternate Computer Emergency Response Team (ACERT). She served as Superintendent of the United States Air Forces in Europe (USAFE) Communications and Information Training Center, Superintendent of the 385 Communications Squadron on Ali Al Saleem AB, Kuwait, and Senior Information Security Analyst for Army Aviation Unmanned Aircraft Systems. Angie holds several industry certifications, including CISSP, Network+ and Security+, and a master's degree in Information Systems Management. She has developed and taught courseware worldwide for the U.S. Air Force, as well as several computer science courses for the University of Alabama in Huntsville and Kaplan University in Fort Lauderdale, Florida.

---

# CONTENTS AT A GLANCE

<b>Chapter 1</b>	Ethical Hacking Basics .....	1
<b>Chapter 2</b>	Cryptography 101 .....	27
<b>Chapter 3</b>	Reconnaissance: Information Gathering for the Ethical Hacker ...	53
<b>Chapter 4</b>	Scanning and Enumeration .....	85
<b>Chapter 5</b>	Hacking Through the Network: Sniffers and Evasion .....	121
<b>Chapter 6</b>	Attacking a System .....	155
<b>Chapter 7</b>	Low Tech: Social Engineering and Physical Security .....	193
<b>Chapter 8</b>	Web-Based Hacking: Servers and Applications .....	219
<b>Chapter 9</b>	Wireless Network Hacking .....	251
<b>Chapter 10</b>	Trojans and Other Attacks .....	283
<b>Chapter 11</b>	The Pen Test: Putting It All Together .....	311
<b>Appendix A</b>	Tool, Sites, and References .....	325
<b>Appendix B</b>	About the CD .....	337
<b>Glossary</b>	.....	339
<b>Index</b>	.....	373

---

# CONTENTS

	Acknowledgments .....	xvii
	Introduction .....	xix
<b>Chapter 1</b>	Ethical Hacking Basics .....	1
	Introduction to Ethical Hacking .....	2
	Security Basics: CIA .....	2
	Defining the Ethical Hacker .....	5
	Hacking Terminology and Attacks .....	11
	Legal Hacking: Laws and Guidelines You Need to Know .....	14
	U.S. Cyber Crime Laws .....	15
	International Cyber Crime Laws .....	18
	Chapter Review .....	20
	Questions .....	22
	Answers .....	24
<b>Chapter 2</b>	Cryptography 101 .....	27
	Cryptography and Encryption Overview .....	28
	Encryption Algorithms and Techniques .....	28
	PKI, the Digital Certificate, and Digital Signatures .....	38
	The PKI System .....	39
	Digital Certificates .....	40
	Digital Signatures .....	43
	Encrypted Communication and Cryptography Attacks .....	44
	Data Encryption: At Rest and While Communicating .....	44
	Cryptography Attacks .....	46
	Chapter Review .....	47
	Questions .....	49
	Answers .....	51
<b>Chapter 3</b>	Reconnaissance: Information Gathering for the Ethical Hacker ...	53
	Vulnerability Research .....	54
	Footprinting .....	58
	Footprinting with DNS .....	62
	Determining Network Range .....	71
	Google Hacking .....	74
	Other Tips and Tools .....	77
	Chapter Review .....	78
	Questions .....	81
	Answers .....	83

<b>Chapter 4</b>	Scanning and Enumeration .....	<b>85</b>
	Scanning for Targets .....	86
	Identifying Active Machines .....	87
	Port Scanning .....	91
	Other Scanning Tips and Tools .....	105
	Enumeration .....	107
	Windows Security Basics .....	108
	Enumeration Techniques .....	110
	Chapter Review .....	113
	Questions .....	117
	Answers .....	119
<b>Chapter 5</b>	Hacking Through the Network: Sniffers and Evasion .....	<b>121</b>
	Sniffing .....	122
	Communications Basics .....	122
	Sniffing Techniques and Tools .....	127
	Network Roadblocks .....	136
	Intrusion Detection .....	136
	Firewalls and Honeypots .....	144
	Chapter Review .....	149
	Questions .....	151
	Answers .....	153
<b>Chapter 6</b>	Attacking a System .....	<b>155</b>
	Windows System Hacking .....	156
	Password Cracking .....	156
	Escalating Privileges and Maintaining Stealth .....	168
	Linux Hacking .....	177
	Linux Essentials .....	177
	Hardening a Linux Machine .....	184
	Chapter Review .....	187
	Questions .....	189
	Answers .....	192
<b>Chapter 7</b>	Low Tech: Social Engineering and Physical Security .....	<b>193</b>
	Social Engineering .....	194
	Human-Based Attacks .....	195
	Computer-Based Attacks .....	197
	Physical Security .....	202
	Physical Security 101 .....	202
	Chapter Review .....	213
	Questions .....	214
	Answers .....	217



<b>Chapter 8</b>	Web-Based Hacking: Servers and Applications	219
	Attacking Web Servers	220
	Web Services Architecture	220
	Web Attacks	225
	Web Applications	230
	Application Attacks	230
	Protecting Your Web Resources	240
	Chapter Review	244
	Questions	246
	Answers	249
<b>Chapter 9</b>	Wireless Network Hacking	251
	Wireless 101	252
	Network Architecture and Standards	252
	Finding and Identifying Wireless Networks	259
	Wireless Hacking	265
	Wireless Attacks	265
	Bluetooth Attacks	273
	Chapter Review	274
	Questions	279
	Answers	282
<b>Chapter 10</b>	Trojans and Other Attacks	283
	The “Malware” Attacks	284
	Trojans, Backdoors, Viruses, and Worms	284
	Remaining Attacks	295
	Denial of Service	295
	Session Hijacking	298
	Chapter Review	301
	Questions	306
	Answers	308
<b>Chapter 11</b>	The Pen Test: Putting It All Together	311
	Methodology and Steps	312
	The Security Assessments	312
	Security Assessment Deliverables	318
	Chapter Review	319
	Questions	321
	Answers	323
<b>Appendix A</b>	Tool, Sites, and References	325
	Vulnerability Research Sites	325
	Footprinting Tools	326
	Website Research Tools	326

DNS and WHOIS Tools .....	326
Traceroute Tools and Links .....	326
Website Mirroring Tools and Sites .....	327
E-mail Tracking .....	327
Google Hacking .....	327
Scanning and Enumeration Tools .....	327
Ping Sweep .....	327
Scanning Tools .....	328
War Dialing .....	328
Banner Grabbing .....	328
Vulnerability Scanning .....	328
Proxy, Anonymizer, and Tunneling .....	329
Enumeration .....	329
System Hacking Tools .....	330
Password Hacking Tools .....	330
Sniffing .....	330
Keyloggers and Screen Capture .....	330
Covering Tracks .....	331
Packet Crafting/Spoofing .....	331
Session Hijacking .....	331
Cryptography and Encryption .....	331
Encryption Tools .....	331
Hash Tools .....	332
Steganography .....	332
Cryptanalysis .....	332
Sniffing .....	332
Packet Capture .....	332
Wireless .....	333
MAC Flooding/Spoofing .....	333
ARP Poisoning .....	333
Trojans and Malware .....	333
Wrappers .....	333
Monitoring Tools .....	333
Attack Tools .....	334
IDS .....	334
Evasion Tools .....	334
Wireless .....	334
Web Attacks .....	335
SQL Injection .....	335
Miscellaneous .....	336
Pen Test Suites .....	336
Extras .....	336
Linux Distributions .....	336
Tools, Sites, and References Disclaimer .....	336