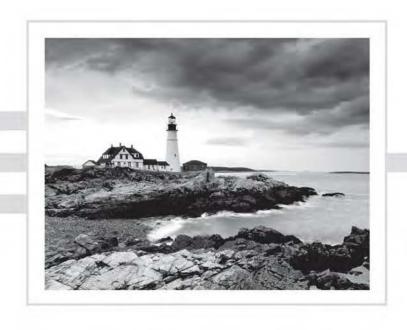
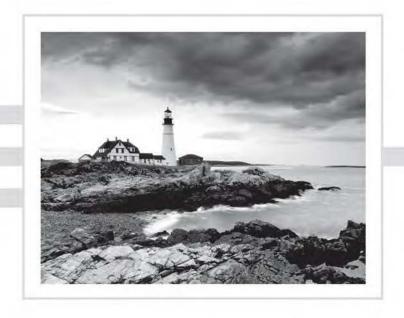
# CEH<sup>™</sup> v10 Study Guide



# CEH™ v10

# **Certified Ethical Hacker**

**Study Guide** 



Ric Messier, CEH, GCIH, GSEC, CISSP



Development Editor: Kim Wimpsett

Technical Editors: Russ Christy and Megan Daudelin Senior Production Editor: Christine O'Connor

Copy Editor: Judy Flynn

Editorial Manager: Pete Gaughan Production Manager: Kathleen Wisor Associate Publisher: Jim Minatel

Book Designers: Judy Fung and Bill Gibson

Proofreader: Louise Watson, Word One New York

Indexer: Johnna VanHoose Dinse

Project Coordinator, Cover: Brent Savage

Cover Designer: Wiley

Cover Image: Getty Images Inc. / Jeremy Woodhouse

Copyright © 2019 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-53319-1 ISBN: 978-1-119-53325-2 (ebk.) ISBN: 978-1-119-53326-9 (ebk.)

Manufactured in the United States of America

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

#### Library of Congress Control Number: 2019940400

TRADEMARKS: Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. CEH is a trademark of EC-Council. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

### About the Author

Ric Messier, GCIH, GSEC, CEH, CISSP, MS, has entirely too many letters after his name, as though he spends time gathering up strays that follow him home at the end of the day. His interest in information security began in high school but was cemented when he was a freshman at the University of Maine, Orono, when he took advantage of a vulnerability in a jailed environment to break out of the jail and gain elevated privileges on an IBM mainframe in the early 1980s. His first experience with Unix was in the mid-1980s and with Linux in the mid-1990s. Ric is an author, trainer, educator, and security professional with multiple decades of experience. He is currently a Senior Information Security Consultant with FireEye Mandiant and occasionally teaches courses at Harvard University and the University of Colorado Boulder.

## Contents at a Glance

Introduct	ion		xvii
Assessme	nt Test		xxiv
Chapter	1	Ethical Hacking	1
Chapter	2	Networking Foundations	9
Chapter	3	Security Foundations	49
Chapter	4	Footprinting and Reconnaissance	83
Chapter	5	Scanning Networks	135
Chapter	6	Enumeration	193
Chapter	7	System Hacking	233
Chapter	8	Malware	279
Chapter	9	Sniffing	321
Chapter	10	Social Engineering	357
Chapter	11	Wireless Security	387
Chapter	12	Attack and Defense	419
Chapter	13	Cryptography	447
Chapter	14	Security Architecture and Design	475
Appendi	K	Answers to Review Questions	501
Index			531

## Contents

Introduction			xvii	
Assessment	t Test		xxiv	
Chapter	1	Ethical Hacking	1	
		Overview of Ethics	2	
		Overview of Ethical Hacking	4	
		Methodology of Ethical Hacking	5	
		Reconnaissance and Footprinting	6	
		Scanning and Enumeration	6	
		Gaining Access	7	
		Maintaining Access	7	
		Covering Tracks	8	
		Summary	8	
Chapter	2	Networking Foundations	9	
		Communications Models	11	
		Open Systems Interconnection	12	
		TCP/IP Architecture	15	
		Topologies	16	
		Bus Network	16	
		Star Network	17	
		Ring Network	18	
		Mesh Network	19	
		Hybrid	20	
		Physical Networking	21	
		Addressing	21	
		Switching	22	
		IP	23	
		Headers	23	
		Addressing	25	
		Subnets	26	
		TCP	28	
		UDP	31	
		Internet Control Message Protocol	32	
		Network Architectures	33	
		Network Types	34	
		Isolation	35	
		Remote Access	36	

		Cloud Computing	36
		Storage as a Service	37
		Infrastructure as a Service	39
		Platform as a Service	40
		Software as a Service	42
		Internet of Things	43
		Summary	44
		Review Questions	46
Chapter	3	Security Foundations	49
		The Triad	51
		Confidentiality	51
		Integrity	53
		Availability	54
		Parkerian Hexad	55
		Risk	56
		Policies, Standards, and Procedures	58
		Security Policies	58
		Security Standards	59
		Procedures	60
		Guidelines	60
		Security Technology	61
		Firewalls	61
		Intrusion Detection Systems	65
		Intrusion Prevention Systems	68
		Security Information and Event Management	69
		Being Prepared	70
		Defense in Depth	71
		Defense in Breadth	73
		Logging	74
		Auditing	76
		Summary	78
		Review Questions	79
Chapter	4	Footprinting and Reconnaissance	83
		Open-Source Intelligence	85
		Companies	85
		People	93
		Social Networking	97
		Domain Name System	108
		Name Lookups	109
		Zone Transfers	115
		Passive Reconnaissance	117