

CEHTM v12

CERTIFIED ETHICAL HACKER

STUDY GUIDE

Includes interactive online learning environment and study tools:

750 practice questions

100 electronic flashcards

Searchable key term glossary

RIC MESSIER, CEH, GSEC, CISSP

 **SYBEX**
A Wiley Brand

Table of Contents

[Cover](#)

[Title Page](#)

[Copyright](#)

[About the Authors](#)

[About the Technical Editor](#)

[Introduction](#)

[What Is a CEH?](#)

[About EC-Council](#)

[Using This Book](#)

[Objective Map](#)

[Let's Get Started!](#)

[How to Contact the Publisher](#)

[Assessment Test](#)

[Answers to Assessment Test](#)

[Chapter 1: Ethical Hacking](#)

[Overview of Ethics](#)

[Overview of Ethical Hacking](#)

[Attack Modeling](#)

[Methodology of Ethical Hacking](#)

[Summary](#)

[Chapter 2: Networking Foundations](#)

[Communications Models](#)

[Topologies](#)

[Physical Networking](#)

[IP](#)

[TCP](#)

[UDP](#)

[Internet Control Message Protocol](#)

[Network Architectures](#)

[Cloud Computing](#)

[Summary](#)

[Review Questions](#)

[Chapter 3: Security Foundations](#)

[The Triad](#)

[Information Assurance and Risk](#)

[Policies, Standards, and Procedures](#)

[Organizing Your Protections](#)

[Security Technology](#)

[Being Prepared](#)

[Summary](#)

[Review Questions](#)

[Chapter 4: Footprinting and Reconnaissance](#)

[Open Source Intelligence](#)

[Domain Name System](#)

[Passive Reconnaissance](#)

[Website Intelligence](#)

[Technology Intelligence](#)

[Summary](#)

[Review Questions](#)

[Chapter 5: Scanning Networks](#)

[Ping Sweeps](#)

[Port Scanning](#)

[Vulnerability Scanning](#)

[Packet Crafting and Manipulation](#)

[Evasion Techniques](#)

[Protecting and Detecting](#)

[Summary](#)

[Review Questions](#)

[Chapter 6: Enumeration](#)

[Service Enumeration](#)

[Remote Procedure Calls](#)

[Server Message Block](#)

[Simple Network Management Protocol](#)

[Simple Mail Transfer Protocol](#)

[Web-Based Enumeration](#)

[Summary](#)

[Review Questions](#)

[Chapter 7: System Hacking](#)

[Searching for Exploits](#)

[System Compromise](#)

[Gathering Passwords](#)

[Password Cracking](#)

[Client-Side Vulnerabilities](#)

[Living Off the Land](#)

[Fuzzing](#)

[Post Exploitation](#)

[Summary](#)

[Review Questions](#)

[Chapter 8: Malware](#)

[Malware Types](#)

[Malware Analysis](#)

[Creating Malware](#)

[Malware Infrastructure](#)

[Antivirus Solutions](#)

[Persistence](#)

[Summary](#)

[Review Questions](#)

[Chapter 9: Sniffing](#)

[Packet Capture](#)

[Detecting Sniffers](#)

[Packet Analysis](#)

[Spoofing Attacks](#)

[Summary](#)

[Review Questions](#)

[Chapter 10: Social Engineering](#)

[Social Engineering](#)

[Physical Social Engineering](#)

[Phishing Attacks](#)

[Social Engineering for Social Networking](#)

[Website Attacks](#)

[Wireless Social Engineering](#)

[Automating Social Engineering](#)

[Summary](#)

[Review Questions](#)

[Chapter 11: Wireless Security](#)

[Wi-Fi](#)

[Bluetooth](#)

[Mobile Devices](#)

[Summary](#)

[Review Questions](#)

[Chapter 12: Attack and Defense](#)

[Web Application Attacks](#)

[Denial-of-Service Attacks](#)

[Application Exploitation](#)

[Lateral Movement](#)

[Defense in Depth/Defense in Breadth](#)

[Defensible Network Architecture](#)

[Summary](#)

[Review Questions](#)

[Chapter 13: Cryptography](#)

[Basic Encryption](#)

[Symmetric Key Cryptography](#)

[Asymmetric Key Cryptography](#)

[Certificate Authorities and Key Management](#)

[Cryptographic Hashing](#)

[PGP and S/MIME](#)

[Disk and File Encryption](#)

[Summary](#)

[Review Questions](#)

[Chapter 14: Security Architecture and Design](#)

[Data Classification](#)

[Security Models](#)

[Application Architecture](#)

[Security Architecture](#)

[Summary](#)

[Review Questions](#)

[Chapter 15: Cloud Computing and the Internet of Things](#)

[Cloud Computing Overview](#)

[Cloud Architectures and Deployment](#)

[Common Cloud Threats](#)

[Internet of Things](#)

[Operational Technology](#)

[Summary](#)

[Review Questions](#)

[Appendix: Answers to Review Questions](#)

[Chapter 2: Networking Foundations](#)

[Chapter 3: Security Foundations](#)

[Chapter 4: Footprinting and Reconnaissance](#)

[Chapter 5: Scanning Networks](#)

[Chapter 6: Enumeration](#)

[Chapter 7: System Hacking](#)

[Chapter 8: Malware](#)

[Chapter 9: Sniffing](#)

[Chapter 10: Social Engineering](#)

[Chapter 11: Wireless Security](#)

[Chapter 12: Attack and Defense](#)

[Chapter 13: Cryptography](#)

[Chapter 14: Security Architecture and Design](#)

[Chapter 15: Cloud Computing and the Internet of Things](#)

[Index](#)

[End User License Agreement](#)

List of Tables

Introduction

[Table 1.1 Objective Map](#)

Chapter 14

[Table 14.1 Governmental Data Classifications](#)

[Table 14.2 Simple Data Classification](#)

List of Illustrations

Chapter 1

[Figure 1.1 Cyber kill chain](#)

[Figure 1.2 Attack life cycle](#)

Chapter 2

[Figure 2.1 Network headers](#)

[Figure 2.2 The seven layers of the OSI model](#)

[Figure 2.3 The TCP/IP architecture layers](#)

[Figure 2.4 Bus network](#)

[Figure 2.5 Star network](#)

[Figure 2.6 Ring network](#)

[Figure 2.7 Mesh network](#)

[Figure 2.8 Full mesh network](#)

[Figure 2.9 IP headers](#)

[Figure 2.10 TCP headers](#)

[Figure 2.11 Three-way handshake](#)

[Figure 2.12 UDP headers](#)

[Figure 2.13 DMZ network](#)

[Figure 2.14 Google Drive](#)

[Figure 2.15 Amazon Web Services](#)

[Figure 2.16 AWS marketplace images](#)

[Figure 2.17 Azure Marketplace images](#)

Chapter 3

[Figure 3.1 The CIA triad](#)

[Figure 3.2 An error message about an apparently invalid certificate](#)

[Figure 3.3 Network diagram showing IDS placement](#)

[Figure 3.4 Network diagram showing IPS placement](#)

[Figure 3.5 Google Rapid Response system](#)

[Figure 3.6 Kibana interface to the Elastic Stack](#)

[Figure 3.7 Defense-in-depth network design](#)

[Figure 3.8 Event Viewer](#)

[Figure 3.9 Audit Policy in Windows](#)

Chapter 4

[Figure 4.1 EDGAR site](#)

[Figure 4.2 Portion of Schedule 14A for Microsoft](#)

[Figure 4.3 PeekYou output](#)

[Figure 4.4 www.weknowwhatyouredoing.com](#)

[Figure 4.5 Facebook Graph API](#)

[Figure 4.6 John Wiley & Sons information](#)

[Figure 4.7 Facebook permissions settings](#)

[Figure 4.8 LinkedIn job statistics](#)

[Figure 4.9 Job requirements for a network security engineer](#)

[Figure 4.10 Twitter keys and access tokens](#)

[Figure 4.11 Maltego graph from Twitter](#)

[Figure 4.12 Job listing with technologies](#)

[Figure 4.13 DNS name resolution](#)

[Figure 4.14 Recon with Recon](#)

[Figure 4.15 Netcraft hosting history](#)

[Figure 4.16 Wappalyzer for technology](#)

[Figure 4.17 Chrome developer tools](#)

[Figure 4.18 Google hacking results](#)

[Figure 4.19 Google Hacking Database](#)

[Figure 4.20 Shodan search for DNP3](#)

[Figure 4.21 Shodan results](#)

Chapter 5

[Figure 5.1 MegaPing IP Scanner](#)

[Figure 5.2 UDP scan from Wireshark](#)

[Figure 5.3 Zenmap scan types](#)

[Figure 5.4 Zenmap service output](#)

[Figure 5.5 MegaPing scan types](#)

[Figure 5.6 MegaPing scan report](#)

[Figure 5.7 Greenbone Security Assistant](#)

[Figure 5.8 Creating a target in OpenVAS](#)

[Figure 5.9 Creating credentials in OpenVAS](#)

[Figure 5.10 OpenVAS scan configs](#)

[Figure 5.11 OpenVAS NVT families](#)

[Figure 5.12 OpenVAS NVT selections](#)

[Figure 5.13 OpenVAS tasks](#)

[Figure 5.14 OpenVAS task creation](#)

[Figure 5.15 OpenVAS Scans dashboard](#)

[Figure 5.16 OpenVAS Results list](#)

[Figure 5.17 Setting an override](#)

[Figure 5.18 Scan policies in Nessus](#)

[Figure 5.19 Scan configuration settings](#)

[Figure 5.20 Credentials configuration settings](#)

[Figure 5.21 Scan results list](#)

[Figure 5.22 Finding details](#)

[Figure 5.23 Remediations list](#)

[Figure 5.24 Plugins Rules settings](#)

[Figure 5.25 packETH interface](#)

[Figure 5.26 Data pattern fill](#)

[Figure 5.27 Network layer data fill](#)

Chapter 6

[Figure 6.1 NetBIOS Enumerator](#)

Chapter 7

[Figure 7.1 Remote Exploits list at \[www.exploit-db.com\]\(http://www.exploit-db.com\)](#)

[Figure 7.2 Exploit-DB search results](#)

[Figure 7.3 Kerberos authentication](#)

[Figure 7.4 Temporary Chrome Internet files in Windows](#)

[Figure 7.5 Using alternate data streams in Windows](#)

Chapter 8

[Figure 8.1 AV-TEST Institute malware statistics](#)

[Figure 8.2 WannaCry ransom demand](#)

[Figure 8.3 Overview of PE in Cutter](#)

[Figure 8.4 Portable executable sections](#)

[Figure 8.5 Looking for packers](#)

[Figure 8.6 Entry point for malware](#)

[Figure 8.7 Program disassembly in Cutter](#)

[Figure 8.8 Properties on executable](#)

[Figure 8.9 VirusTotal results](#)

[Figure 8.10 VirusTotal details](#)

[Figure 8.11 Ghidra analysis](#)

[Figure 8.12 Executable file details](#)

[Figure 8.13 Cuckoo Sandbox details](#)

[Figure 8.14 Cuckoo Sandbox options](#)

[Figure 8.15 Cuckoo Sandbox results](#)

[Figure 8.16 New IDA session](#)

[Figure 8.17 IDA view](#)

[Figure 8.18 OllyDbg view](#)

[Figure 8.19 Call stack](#)

[Figure 8.20 Using capa on a malware sample](#)

[Figure 8.21 Command-and-control infrastructure](#)

Chapter 9

[Figure 9.1 Wireshark frames list](#)

[Figure 9.2 Protocol details](#)

[Figure 9.3 TLS information](#)

[Figure 9.4 RSA keys preferences](#)

[Figure 9.5 Wireshark home screen](#)

[Figure 9.6 Capture filter in Wireshark](#)

[Figure 9.7 Packet analysis](#)

[Figure 9.8 Relative sequence numbers](#)

[Figure 9.9 Follow TCP Stream dialog box](#)

[Figure 9.10 Protocol Hierarchy Statistics](#)

[Figure 9.11 Conversations statistics](#)

[Figure 9.12 Expert Information](#)

[Figure 9.13 Ettercap host list](#)

[Figure 9.14 MitM Menu in Ettercap](#)

[Figure 9.15 DHCP starvation attack](#)

Chapter 10

[Figure 10.1 I Love You virus](#)

[Figure 10.2 RFID-based badge](#)

[Figure 10.3 Phishing email](#)

[Figure 10.4 Wells Fargo phishing email](#)

[Figure 10.5 Phishing email with attachment](#)

[Figure 10.6 LinkedIn message](#)

[Figure 10.7 WinHTTrack options](#)

[Figure 10.8 Site cloning with WinHTTrack](#)

[Figure 10.9 List of Wi-Fi networks](#)

[Figure 10.10 wifiphisher SSID selection](#)

[Figure 10.11 wifiphisher attack template selection](#)

Chapter 11

[Figure 11.1 Wireless ad hoc network](#)

[Figure 11.2 Wireless infrastructure network](#)

[Figure 11.3 Wireshark capture of radio traffic](#)

[Figure 11.4 Multiple BSSIDs for a single SSID](#)

[Figure 11.5 Authentication and association steps](#)

[Figure 11.6 Four-way handshake for WPA2](#)

[Figure 11.7 Wireless configuration under Linux](#)

[Figure 11.8 Probe request in Wireshark](#)

[Figure 11.9 Radio headers in Wireshark](#)

[Figure 11.10 Apple App Store](#)

[Figure 11.11 Smishing message](#)

Chapter 12

[Figure 12.1 Model/view/controller design](#)

[Figure 12.2 SQL injection attack outcome](#)

[Figure 12.3 Command-line injection attack output](#)

[Figure 12.4 Smurf amplifier registry](#)

[Figure 12.5 Low Orbit Ion Cannon](#)

[Figure 12.6 Stack frame](#)

[Figure 12.7 Buffer overflow](#)

[Figure 12.8 Defense-in-depth network design](#)

Chapter 13

[Figure 13.1 English letter normal distribution](#)

[Figure 13.2 Vigenère square](#)

[Figure 13.3 Diffie-Hellman process](#)

[Figure 13.4 Elliptic curve](#)

[Figure 13.5 Simple Authority CA creation](#)

[Figure 13.6 Certificate creation](#)

[Figure 13.7 Certificate details](#)

[Figure 13.8 Certificate error](#)

[Figure 13.9 List of PGP keys](#)

[Figure 13.10 Encrypting a PDF on macOS](#)

[Figure 13.11 FileVault encryption](#)

[Figure 13.12 BitLocker control panel](#)

Chapter 14

[Figure 14.1 Basic state machine](#)

[Figure 14.2 Multitier application design](#)

[Figure 14.3 IIS application server](#)

[Figure 14.4 Entity-relationship diagram](#)

[Figure 14.5 Service-oriented architecture](#)

[Figure 14.6 AWS service offerings](#)

[Figure 14.7 AWS serverless architecture](#)

[Figure 14.8 NoSQL database offerings with Azure](#)

[Figure 14.9 NIST's five functions](#)

[Figure 14.10 Attack life cycle](#)

[Figure 14.11 Cloud-based business communications](#)

Chapter 15

[Figure 15.1 IBM System/360 mainframe](#)

[Figure 15.2 Nine-track magnetic tape](#)

[Figure 15.3 Amazon Web Services EC2 instance selection](#)

[Figure 15.4 Microsoft Azure .NET server selection](#)

[Figure 15.5 Lucidchart web interface](#)

[Figure 15.6 OneDrive application](#)

[Figure 15.7 S3 bucket configuration](#)

[Figure 15.8 Active Directory federation](#)

[Figure 15.9 Creating a function app in Azure](#)

[Figure 15.10 Creating a function app in Azure](#)

[Figure 15.11 Microservices design](#)

[Figure 15.12 AWS CloudFormation Designer](#)

[Figure 15.13 Burp Suite testing RESTful application](#)

[Figure 15.14 Burp Suite Intruder](#)

[Figure 15.15 Payload options](#)

[Figure 15.16 Force browse in ZAP](#)

[Figure 15.17 Google IAM](#)

[Figure 15.18 S3 bucket configuration](#)

[Figure 15.19 Phishing message](#)

[Figure 15.20 Internet-enabled light switch](#)

[Figure 15.21 Shodan website](#)

[Figure 15.22 Postman sending POST request](#)

[Figure 15.23 IoT services with Microsoft Azure](#)

[Figure 15.24 ICS design](#)

[Figure 15.25 Purdue Enterprise Reference Architecture](#)

[*OceanofPDF.com*](#)

CEH™ v12

Certified Ethical Hacker Study Guide



Ric Messier, CEH, GSEC, CISSP



OceanofPDF.com

Copyright © 2023 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBN: 978-1-394-18692-1

ISBN: 978-1-394-18687-7 (ebk.)

ISBN: 978-1-394-18691-4 (ebk.)

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 Section 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, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. 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 www.wiley.com/go/permission.

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.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Control Number: 2023932588

Cover image: © Getty Images Inc./Jeremy Woodhouse

Cover design: Wiley

OceanofPDF.com

About the Authors

Ric Messier, GCIH, CCSP, 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 Principal Consultant with Mandiant and has developed graduate programs and courses in information security at different colleges and universities.

About the Technical Editor

James Michael Stewart, CISSP, CEH, CHFI, ECSA, CND, ECIH, CySA+, PenTest+, CASP+, Security+, Network+, A+, CISM, and CFR, has been writing and training for more than 25 years, with a current focus on security. He has been teaching CISSP training courses since 2002, not to mention other courses on internet security and ethical hacking/penetration testing. He is the author of and contributor to more than 75 books on security certification, Microsoft topics, and network administration, including *CompTIA Security+ Review Guide*. More information about Michael can be found at his website, www.impactonline.com.

OceanofPDF.com

Introduction

You're thinking about becoming a Certified Ethical Hacker (CEH). No matter what variation of security testing you are performing—ethical hacking, penetration testing, red teaming, or application assessment—the skills and knowledge necessary to achieve this certification are in demand. Even the idea of security testing and ethical hacking is evolving as businesses and organizations begin to have a better understanding of the adversaries they are facing. It's no longer the so-called script kiddies that businesses felt they were fending off for so long. Today's adversary is organized, well-funded, and determined. This means testing requires different tactics.

Depending on who you are listening to, 80–90 percent of attacks today use social engineering. The old technique of looking for technical vulnerabilities in network services is simply not how attackers are getting into networks. Networks that are focused on applying a defense-in-depth approach, hardening the outside, may end up being susceptible to attacks from the inside, which is what happens when desktop systems are compromised. The skills needed to identify vulnerabilities and recommend remediations are evolving, along with the tactics and techniques used by attackers.

This book is written to help you understand the breadth of content you will need to know to obtain the CEH certification. You will find a lot of concepts to provide you with a foundation that can be applied to the skills required for the certification. While you can read this book cover to cover, for a substantial chunk of the subjects, getting hands-on experience is essential. The concepts are often demonstrated through the use of tools. Following along with these demonstrations and using the tools yourself will help you understand the tools and how to use them. Many of the demonstrations are done in Kali Linux, though many of the tools have Windows analogs if you are more comfortable there.

We can't get through this without talking about ethics, though you will find it mentioned in several places throughout the book. This is serious, and not only because it's a huge part of the basis for the certification. It's also

essential for protecting yourself and the people you are working for. The short version is do not do anything that would cause damage to systems or your employer. There is much more to it than that, which you'll read more about in [Chapter 1](#), “Ethical Hacking,” as a starting point. It's necessary to start wrapping your head around the ethics involved in this exam and profession. You will have to sign an agreement as part of achieving your certification.

At the end of each chapter, you will find a set of questions. This will help you to demonstrate to yourself that you understand the content. Most of the questions are multiple choice, which is the question format used for the CEH exam. These questions, along with the hands-on experience you take advantage of, will be good preparation for taking the exam.

What Is a CEH?

The Certified Ethical Hacker exam is to validate that those holding the certification understand the broad range of subject matter that is required for someone to be an effective ethical hacker. The reality is that most days, if you are paying attention to the news, you will see a news story about a company that has been compromised and had data stolen, a government that has been attacked, or even enormous denial-of-service attacks, making it difficult for users to gain access to business resources.

The CEH is a certification that recognizes the importance of identifying security issues to get them remediated. This is one way companies can protect themselves against attacks—by getting there before the attackers do. It requires someone who knows how to follow techniques that attackers would normally use. Just running scans using automated tools is insufficient because as good as security scanners may be, they will identify false positives—cases where the scanner indicates an issue that isn't really an issue. Additionally, they will miss a lot of vulnerabilities—false negatives—for a variety of reasons, including the fact that the vulnerability or attack may not be known.

Because companies need to understand where they are vulnerable to attack, they need people who are able to identify those vulnerabilities, which can be very complex. Scanners are a good start, but being able to find holes in

complex networks can take the creative intelligence that humans offer. This is why we need ethical hackers. These are people who can take extensive knowledge of a broad range of technical subjects and use it to identify vulnerabilities that can be exploited.

The important part of that two-word phrase, by the way, is “ethical.” Companies have protections in place because they have resources they don't want stolen or damaged. When they bring in someone who is looking for vulnerabilities to exploit, they need to be certain that nothing will be stolen or damaged. They also need to be certain that anything that may be seen or reviewed isn't shared with anyone else. This is especially true when it comes to any vulnerabilities that have been identified.

The CEH exam, then, has a dual purpose. It not only tests deeply technical knowledge but also binds anyone who is a certification holder to a code of conduct. Not only will you be expected to know the content and expectations of that code of conduct, you will be expected to live by that code. When companies hire or contract to people who have their CEH certification, they can be assured they have brought on someone with discretion who can keep their secrets and provide them with professional service in order to help improve their security posture and keep their important resources protected.

The Subject Matter

If you were to take the CEH v12 training, you would have to go through the following modules:

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing

- Social Engineering
- Denial of Service
- Session Hijacking
- Evading IDSs, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT and OT Hacking
- Cloud Computing
- Cryptography

As you can see, the range of subjects is broad. Beyond knowing the concepts associated with these topics, you will be expected to know about various tools that may be used to perform the actions associated with the concepts you are learning. You will need to know tools like nmap for port scanning, for example. You may need to know proxy-based web application attack tools. For wireless network attacks, you may need to know about the aircrack-ng suite of tools. For every module listed, there are potentially dozens of tools that may be used.

The subject matter of the CEH exam is very technical. This is not a field in which you can get by with theoretical knowledge. You will need to have had experience with the methods and tools that are covered within the subject matter for the CEH exam. What you may also have noticed here is that the modules all fall within the different stages mentioned earlier. While you may not necessarily be asked for a specific methodology, you will find that the contents of the exam do generally follow the methodology that the EC-Council believes to be a standard approach.

About the Exam

The CEH exam has much the same parameters as other professional certification exams. You will take a computerized, proctored exam. You will have 4 hours to complete 125 questions. That means you will have, on average, roughly 2 minutes per question. The questions are all multiple choice. The exam can be taken through the ECC Exam Center or at a Pearson VUE center. For details about VUE, please visit <https://home.pearsonvue.com/eccouncil>.

Should you want to take your certification even further, you could go after the CEH Practical exam. For this exam you must perform an actual penetration test and write a report at the end of it. This demonstrates that in addition to knowing the body of material covered by the exam, you can put that knowledge to use in a practical way. You will be expected to know how to compromise systems and identify vulnerabilities.

To pass the exam, you will have to correctly answer a certain number of questions, though the actual number will vary. The passing grade varies depending on the difficulty of the questions asked. The harder the questions that are asked out of the complete pool of questions, the fewer questions you need to get right to pass the exam. If you get easier questions, you will need to get more of the questions right to pass. There are some sources of information that will tell you that you need to get 70 percent of the questions right, and that may be okay for general guidance and preparation as a rough low-end marker. However, keep in mind that when you sit down to take the actual test at the testing center, the passing grade will vary. The score you will need to achieve will range from 60 to 85 percent.

The good news is that you will know whether you passed before you leave the testing center. You will get your score when you finish the exam, and you will also get a piece of paper indicating the details of your grade. You will get feedback associated with the different scoring areas and how you performed in each of them.

Who Is Eligible

Not everyone is eligible to sit for the CEH exam. Before you go too far down the road, you should check your qualifications. Just as a starting point, you have to be at least 18 years of age. The other eligibility standards are as follows:

- Anyone who has versions 1–7 of the CEH certification. The CEH certification is ANSI certified now, but early versions of the exam were available before the certification. Anyone who wants to take the ANSI-accredited certification who has the early version of the CEH certification can take the exam.
- Minimum of two years of related work experience. Anyone who has the experience will have to pay a nonrefundable application fee of \$100.
- Have taken an EC-Council training.

If you meet these qualification standards, you can apply for the certification, along with paying the fee if it is applicable to you (if you take one of the EC-Council trainings, the fee is included). The application will be valid for three months.

Exam Cost

To take the certification exam, you need to pay for a Pearson VUE exam voucher. The cost of this is \$1,199. You could also obtain an EC-Council voucher for \$950, but that requires that you have taken EC-Council training and can provide a Certificate of Attendance.



EC-Council may change their eligibility, pricing, or exam policies from time to time. We highly encourage you to check for updated policies at the EC-Council website (<https://cert.eccouncil.org/certified-ethical-hacker.html>) when you begin studying for this book and again when you register for this exam.

About EC-Council

The International Council of Electronic Commerce Consultants is more commonly known as the EC-Council (www.eccouncil.org). It was created

after the airplane attacks that happened against the United States on September 11, 2001. The founder, Jay Bavisi, wondered what would happen if the perpetrators of the attack decided to move from the kinetic world to the digital world. Even beyond that particular set of attackers, the Internet has become a host to a large number of people who are interested in causing damage or stealing information. The economics of the Internet, meaning the low cost of entry into the business, encourage criminals to use it as a means of stealing information, ransoming data, or other malicious acts.

The EC-Council is considered to be one of the largest certifying bodies in the world. It operates in 145 countries and has certified more than 200,000 people. In addition to the CEH, the EC-Council administers a number of other IT-related certifications:

- Certified Network Defender (CND)
- Certified Ethical Hacker Practical
- EC-Council Certified Security Analyst (ECSA)
- EC-Council Certified Security Analyst Practical
- Licensed Penetration Tester (LPT)
- Computer Hacking Forensic Investigator (CHFI)
- Certified Chief Information Security Officer (CCISO)

One advantage to holding a certification from the EC-Council is that the organization has been accredited by the American National Standards Institute (ANSI). Additionally, and perhaps more importantly for potential certification holders, the certifications from EC-Council are recognized worldwide and have been endorsed by governmental agencies like the National Security Agency (NSA). The Department of Defense Directive 8570 includes the CEH certification. This is important because having the CEH certification means that you could be quickly qualified for a number of positions with the United States government.

The CEH certification provides a bar. This means there is a set of known standards. To obtain the certification, you will need to have met at least the minimal standards. These standards can be relied on consistently. This is why someone with the CEH certification can be trusted. They have

demonstrated that they have met known and accepted standards of both knowledge and professional conduct.

Using This Book

This book is structured in a way that foundational material is up front. With this approach, you can make your way in an orderly fashion through the book, one chapter at a time. Technical books can be dry and difficult to get through sometimes, but it's always my goal to try to make them easy to read and I hope entertaining along the way. If you already have a lot of experience, you don't need to take the direct route from beginning to end. You can skip around as you need. No chapter relies on any other. They all stand alone with respect to the content. However, if you don't have the foundation and try to jump to a later chapter, you may find yourself getting lost or confused by the material. All you need to do is jump back to some of the foundational chapters.

Beyond the foundational materials, the book generally follows a fairly standard methodology when it comes to performing security testing. This methodology will be further explained in [Chapter 1](#). As a result, you can follow along with the steps of a penetration test/ethical hacking engagement. Understanding the outline and reason for the methodology will also be helpful to you. Again, though, if you know the material, you can move around as you need.

Additional Study Tools

This book is accompanied by an online learning environment that provides several additional elements. The following items are available among these companion files:

Practice tests All of the questions in this book appear in our proprietary digital test engine—including the 30-question assessment test at the end of this introduction and the 100+ questions that make up the review question sections at the end of each chapter. In addition, there are four bonus exams, each 125 questions.

Electronic “flashcards” The digital companion files include more than 100 questions in flashcard format (a question followed by a single

correct answer). You can use these to review your knowledge of the exam objectives.

Glossary The key terms from this book, and their definitions, are available as a fully searchable PDF.

Interactive Online Learning Environment and Test Bank

To start using additional online materials that accompany this book to study for the Certified Ethical Hacker exam, go to www.wiley.com/go/sybextestprep and click the link “Click here to register a product” to receive your unique PIN. Once you have the PIN, return to www.wiley.com/go/sybextestprep, find your book and click Register or Login, and follow the link to create a new account or add this book to an existing account.



Like all exams, the CEH certification from EC-Council is updated periodically and may eventually be retired or replaced. At some point after EC-Council is no longer offering this exam, the old editions of our books and online tools will be retired. If you have purchased this book after the exam was retired, or are attempting to register in the Sybex online learning environment after the exam was retired, please know that we make no guarantees that this exam's online Sybex tools will be available once the exam is no longer available.

Objective Map

[Table 1.1](#) contains an objective map to show you at a glance where in the book you can find each objective covered. While there are chapters listed

for all of these, there are some objectives that are scattered throughout the book. Specifically, tools, systems, and programs get at least touched on in most of the chapters.

TABLE 1.1 Objective Map

Objective	Chapter
Tasks	
1.1 Systems development and management	7 , 14
1.2 Systems analysis and audits	4 , 5 , 6 , 7
1.3 Security testing and vulnerabilities	7 , 8
1.4 Reporting	1 , 7
1.5 Mitigation	7 , 8
1.6 Ethics	1
Knowledge	
2.1 Background	2 , 3
2.2 Analysis/assessment	2 , 11
2.3 Security	3 , 13 , 14
2.4 Tools, systems, programs	4 , 5 , 6 , 7
2.5 Procedures/methodology	1 , 4 , 5 , 6 , 7 , 14
2.6 Regulation/policy	1 , 14
2.7 Ethics	1

Let's Get Started!

This book is structured in a way that you will be led through foundational concepts and then through a general methodology for ethical hacking. You can feel free to select your own pathway through the book. Remember, wherever possible, get your hands dirty. Get some experience with tools, tactics, and procedures that you are less familiar with. It will help you a lot.

Take the self-assessment. It may help you get a better idea of how you can make the best use of this book.

How to Contact the Publisher

If you believe you've found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

In order to submit your possible errata, please email it to our Customer Service Team at wileysupport@wiley.com with the subject line "Possible Book Errata Submission."

Assessment Test

1. Which header field is used to reassemble fragmented IP packets?
 - A. Destination address
 - B. IP identification
 - C. Don't fragment bit
 - D. ToS field
2. If you were to see the following in a packet capture, what would you expect was happening?
' or 1=1;
 - A. Cross-site scripting
 - B. Command injection
 - C. SQL injection
 - D. XML external entity injection
3. What method might you use to successfully get malware onto a mobile device?
 - A. Through the Apple Store or Google Play Store
 - B. External storage on an Android
 - C. Third-party app store