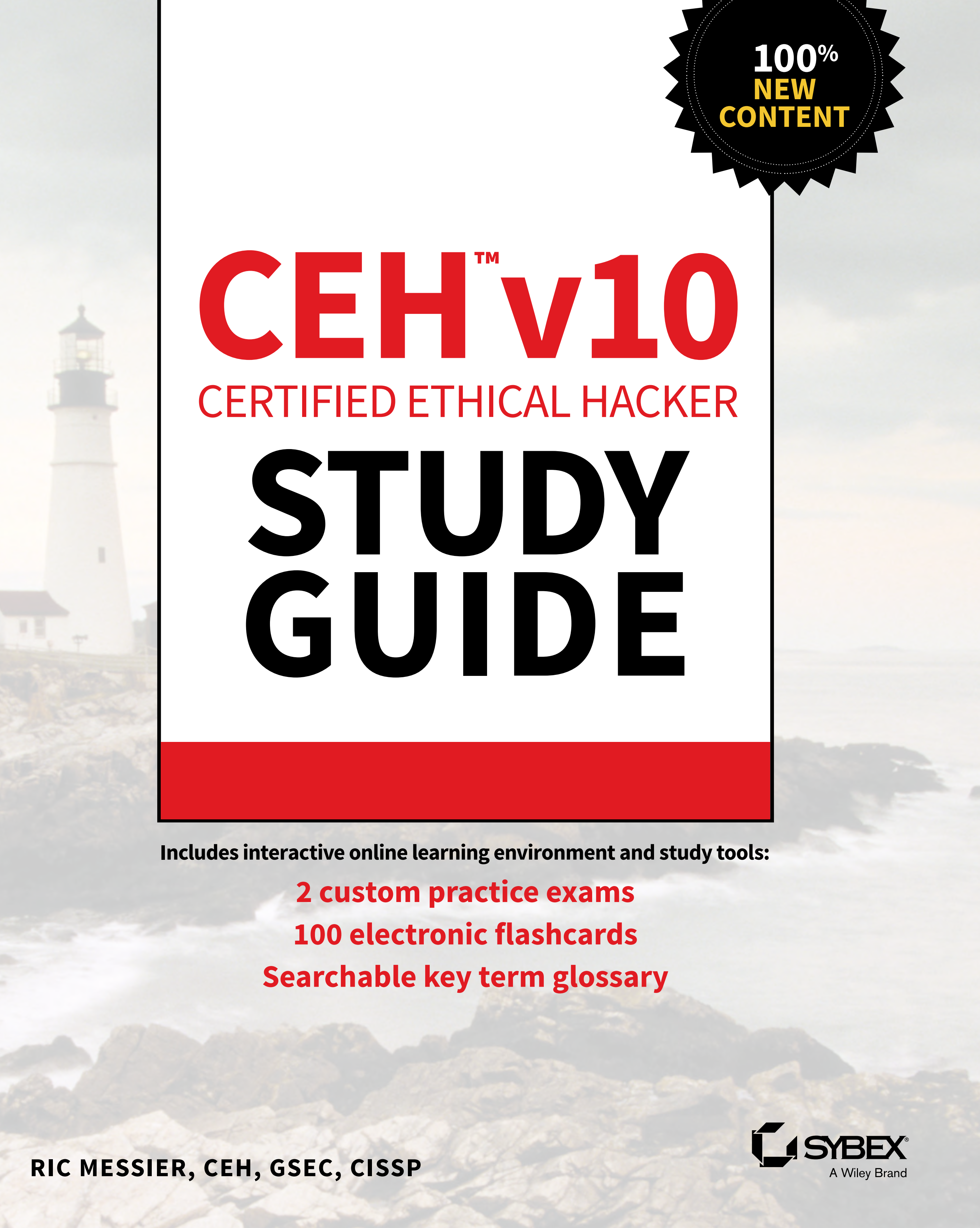

100% NEW CONTENT

CEH™ v10

CERTIFIED ETHICAL HACKER

STUDY GUIDE

Includes interactive online learning environment and study tools:

2 custom practice exams

100 electronic flashcards

Searchable key term glossary

RIC MESSIER, CEH, GSEC, CISSP

SYBEX®
A Wiley Brand

CEH™ v10

Study Guide

CEH™ v10

Certified Ethical Hacker

Study Guide

Ric Messier,

CEH, GCIH, GSEC, CISSP

SYBEX®
A Wiley Brand

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

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

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

10 9 8 7 6 5 4 3 2 1

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

Introduction *xvii*

Assessment 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

Appendix Answers to Review Questions 501

Index *531*

Contents

Introduction *xvii*

Assessment 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

Website Intelligence 120
Technology Intelligence 124
Google Hacking 125
Internet of Things (IoT) 126
Summary 128
Review Questions 130

Chapter 5 Scanning Networks 135

Ping Sweeps 137
Using fping 137
Using MegaPing 139
Port Scanning 141
Nmap 142
masscan 155
MegaPing 157
Vulnerability Scanning 159
OpenVAS 160
Nessus 171
Packet Crafting and Manipulation 177
hping 178
packETH 180
fragroute 183
Evasion Techniques 185
Summary 187
Review Questions 189

Chapter 6 Enumeration 193

Service Enumeration 195
Remote Procedure Calls 198
SunRPC 198
Remote Method Invocation 200
Server Message Block 204
Built-In Utilities 205
Nmap Scripts 207
Metasploit 209
Other Utilities 212
Simple Network Management Protocol 215
Simple Mail Transfer Protocol 217
Web-Based Enumeration 220
Summary 226
Review Questions 228

Chapter 7 System Hacking 233

Searching for Exploits 234
System Compromise 239
  Metasploit Modules 239
  Exploit-DB 243
Gathering Passwords 245
Password Cracking 248
  John the Ripper 248
  Rainbow Tables 250
Client-Side Vulnerabilities 253
Post Exploitation 255
  Privilege Escalation 255
  Pivoting 260
  Persistence 262
  Covering Tracks 265
Summary 272
Review Questions 274

Chapter 8 Malware 279

Malware Types 281
  Virus 281
  Worm 282
  Trojan 284
  Botnet 284
  Ransomware 285
  Dropper 286
Malware Analysis 287
  Static Analysis 288
  Dynamic Analysis 296
Creating Malware 305
  Writing Your Own 305
  Using Metasploit 308
Malware Infrastructure 311
Antivirus Solutions 314
Summary 314
Review Questions 316

Chapter 9 Sniffing 321

Packet Capture 322
  tcpdump 323
  tshark 329
  Wireshark 331
  Berkeley Packet Filter (BPF) 335
  Port Mirroring/Spanning 336

Packet Analysis 337
Spoofing Attacks 342
ARP Spoofing 342
DNS Spoofing 346
sslstrip 348
Summary 350
Review Questions 352

Chapter 10 Social Engineering 357

Social Engineering 358
Pretexting 360
Social Engineering Vectors 362
Physical Social Engineering 362
Badge Access 363
Man Traps 364
Biometrics 365
Phone Calls 366
Baiting 367
Phishing Attacks 368
Website Attacks 371
Cloning 371
Rogue Attacks 374
Wireless Social Engineering 375
Automating Social Engineering 379
Summary 381
Review Questions 383

Chapter 11 Wireless Security 387

Wi-Fi 388
Wi-Fi Network Types 390
Wi-Fi Authentication 392
Wi-Fi Encryption 393
Bring Your Own Device (BYOD) 397
Wi-Fi Attacks 398
Bluetooth 407
Scanning 408
Bluejacking 409
Bluesnarfing 410
Bluebugging 410
Mobile Devices 411
Mobile Device Attacks 412
Summary 414
Review Questions 416

Chapter 12 Attack and Defense 419

Web Application Attacks 420
XML External Entity Processing 422
Cross-Site Scripting (XSS) 423
SQL Injection 425
Command Injection 427
Denial of Service Attacks 428
Bandwidth Attacks 428
Slow Attacks 431
Legacy 432
Application Exploitation 433
Buffer Overflow 433
Heap Spraying 436
Lateral Movement 436
Defense in Depth/Defense in Breadth 438
Defensible Network Architecture 440
Summary 441
Review Questions 443

Chapter 13 Cryptography 447

Basic Encryption 449
Substitution Ciphers 449
Diffie-Hellman 452
Symmetric Key Cryptography 453
Data Encryption Standard (DES) 453
Advanced Encryption Standard (AES) 454
Asymmetric Key Cryptography 456
Hybrid Cryptosystem 456
Non-Repudiation 457
Elliptic Curve Cryptography 457
Certificate Authorities and Key Management 459
Certificate Authority 459
Trusted Third Party 462
Self-Signed Certificates 463
Cryptographic Hashing 465
PGP and S/MIME 467
Summary 469
Review Questions 471

Chapter 14 Security Architecture and Design 475

Data Classification 476
Security Models 478
State Machine 478
Biba 479
Bell-LaPadula 480
Clark-Wilson Integrity Model 480
Application Architecture 481
n-tier Application Design 482
Service-Oriented Architecture 485
Cloud-Based Applications 487
Database Considerations 489
Security Architecture 492
Summary 495
Review Questions 497

Appendix Answers to Review Questions 501

Chapter 2: Networking Foundations 502
Chapter 3: Security Foundations 503
Chapter 4: Footprinting and Reconnaissance 506
Chapter 5: Scanning Networks 508
Chapter 6: Enumeration 511
Chapter 7: System Hacking 513
Chapter 8: Malware 515
Chapter 9: Sniffing 518
Chapter 10: Social Engineering 519
Chapter 11: Wireless Security 522
Chapter 12: Attack and Defense 524
Chapter 13: Cryptography 526
Chapter 14: Security Architecture and Design 528

Index 531

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 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 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 very short version of it 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 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 (CEH) 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 in order 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 v10 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 Hacking
- Cloud Computing
- Cryptography

As you can see, the range of subjects is very 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 above, 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.

Should you wish 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.

In order to pass the exam, you will have to correctly answer questions, though the actual number of questions you have to answer correctly 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 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. CEH certification (or exam?) 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 non-refundable 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

In order 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.

About EC-Council

The International Council of Electronic Commerce Consultants is more commonly known as the EC-Council. It was created after the airplane attacks that happened against the United States on 9/11/01. 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. They operate in 145 countries and have certified more than 200,000 people. In addition to the CEH, the EC-Council also administers a number of other IT-related certifications. They manage the following certifications:

- Certified Network Defender (CND)
- Certified Ethical Hacker (CEH)
- 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 that there is a set of known standards. In order to obtain the certification, you will need to have met at least the minimal standard. 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 hopefully 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 to. 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 to.

Objective Map

Table I.1 contains an objective map to show you at a glance where 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 I.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

Objective	Chapter
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

On the Day of the Exam

Plan to arrive at your test center at least 30 minutes before your exam start time. To check in, you'll need to:

- Show two (2) valid, unexpired forms of personal ID (examples include: government issued IDs, passport, etc.). Both must have your signature, and one of the two must have your photo. For more information about acceptable IDs please visit: `https://www.isc2.org/Register-for-Exam`, and look under the What You Need to Bring to the Test Center tab for more information.
- Provide your signature.
- Submit to a palm vein scan (unless it's prohibited by law).
- Have your photo taken. Hats, scarves, and coats may not be worn for your photo. You also can't wear these items in the test room.

The Test Administrator (TA) will give you a short orientation. If you have already arranged for special accommodations for your testing, and (ISC)2 and Pearson VUE have approved them, be sure to go over these with the TA. Then, the TA will escort you to a computer terminal.

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 how you can make the best use of this book.

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

   D. Jailbreaking

4. What protocol is used to take a destination IP address and get a packet to a destination on the local network?

   A. DHCP

   B. ARP

   C. DNS

   D. RARP

5. What would be the result of sending the string AAAAAAAAAAAAAAAA into a variable that has been allocated space for 8 bytes?

   A. Heap spraying

   B. SQL injection

   C. Buffer overflow

   D. Slowloris attack

6. If you were to see the subnet mask 255.255.248.0, what CIDR notation (prefix) would you use to indicate the same thing?

   A. /23

   B. /22

   C. /21

   D. /20

7. What is the primary difference between a worm and a virus?

A. A worm uses polymorphic code

B. A virus uses polymorphic code

C. A worm can self-propagate

D. A virus can self-propagate

8. How would you calculate risk?

A. Probability * loss

B. Probability * mitigation factor

C. (Loss + mitigation factor) * (loss/probability)

D. Probability * mitigation factor

9. How does an evil twin attack work?

A. Phishing users for credentials

B. Spoofing an SSID

C. Changing an SSID

D. Injecting four-way handshakes

10. In order to remove malware in the network before it gets to the endpoint, you would use which of the following?

A. Antivirus

B. Application layer gateway

C. Unified threat management appliance

D. Stateful firewall

11. What is the purpose of a security policy?

A. Providing high-level guidance on the role of security

B. Providing specific direction to security workers

C. Increasing the bottom line of a company

D. Aligning standards and practices

12. What has been done to the following string? %3Cscript%3Ealert('wubble');%3C/script%3E

A. Base64 encoding

B. URL encoding

C. Encryption

D. Cryptographic hashing

13. What would you get from running the command `dig ns domain.com`?

A. Mail exchanger records for domain.com

B. Name server records for domain.com

C. Caching name server for domain.com

D. IP address for the hostname ns

14. What technique would you ideally use to get all of the hostnames associated with a domain?

A. DNS query

B. Zone copy

C. Zone transfer

D. Recursive request

15. If you were to notice operating system commands inside a DNS request while looking at a packet capture, what might you be looking at?

A. Tunneling attack

B. DNS amplification

C. DNS recursion

D. XML entity injection

16. What would be the purpose of running a ping sweep?

A. You want to identify responsive hosts without a port scan.

B. You want to use something that is light on network traffic.

C. You want to use a protocol that may be allowed through the firewall.

D. All of the above.

17. How many functions are specified by NIST's cybersecurity framework?

A. 0

B. 3

C. 5

D. 4

18. What would be one reason not to write malware in Python?

A. Python interpreter is slow.

B. Python interpreter may not be available.

C. There is inadequate library support.

D. Python is a hard language to learn.

19. If you saw the following command line, what would you be capturing?

```
tcpdump -i eth2 host 192.168.10.5
```

A. Traffic just from 192.168.10.5

B. Traffic to and from 192.168.10.5

C. Traffic just to 192.168.10.5

D. All traffic other than from 192.168.86.5

20. What is Diffie-Hellman used for?
    - A. Key management
    - B. Key isolation
    - C. Key exchange
    - D. Key revocation

21. Which social engineering principle may allow a phony call from the help desk to be effective?
    - A. Social proof
    - B. Imitation
    - C. Scarcity
    - D. Authority

22. How do you authenticate with SNMPv1?
    - A. Username/password
    - B. Hash
    - C. Public string
    - D. Community string

23. What is the process Java programs identify themselves to if they are sharing procedures over the network?
    - A. RMI registry
    - B. RMI mapper
    - C. RMI database
    - D. RMI process

24. What do we call an ARP response without a corresponding ARP request?
    - A. Is-at response
    - B. Who-has ARP
    - C. Gratuitous ARP
    - D. IP response

25. What are the three times that are typically stored as part of file metadata?
    - A. Moves, adds, changes
    - B. Modified, accessed, deleted
    - C. Moved, accessed, changed
    - D. Modified, accessed, created

26. Which of these is a reason to use an exploit against a local vulnerability?
    - A. Pivoting
    - B. Log manipulation
    - C. Privilege escalation
    - D. Password collection

27. What principle is used to demonstrate that a signed message came from the owner of the key that signed it?
    - A. Non-repudiation
    - B. Non-verifiability
    - C. Integrity
    - D. Authority

28. What is a viable approach to protecting against tailgaiting?
    - A. Biometrics
    - B. Badge access
    - C. Phone verification
    - D. Man traps

29. Why is bluesnarfing potentially more dangerous than bluejacking?
    - A. Bluejacking sends while bluesnarfing receives.
    - B. Bluejacking receives while bluesnarfing sends.
    - C. Bluejacking installs keyloggers.
    - D. Bluesnarfing installs keyloggers.

30. Which of the security triad properties does the Biba security model relate to?
    - A. Confidentiality
    - B. Integrity
    - C. Availability
    - D. All of them