CEH™ v11

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™ v11

Certified Ethical Hacker

Study Guide

CEH™ v11

Certified Ethical Hacker

Study Guide

Ric Messier,

CEH, GSEC, CISSP

SYBEX®
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

ISBN: 978-1-119-80028-6
ISBN: 978-1-119-80029-3 (ebk)
ISBN: 978-1-119-80030-9 (ebk)

Library of Congress Control Number: 2021939941

Cover image: © Getty Images Inc./Jeremy Woodhouse

Cover design: Wiley

For Robin, the inspirational light in my life.

About the Author

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 FireEye Mandiant and occasionally teaches courses at Harvard University.

About the Technical Editor

Erin O'Brien is currently a security consultant at Mandiant, where she focuses on incident response and threat intelligence. She has over 7 years of experience in the information technology industry, with specialties in vulnerability management, security engineering, and data loss prevention.

Contents at a Glance

Contents

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 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 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 v11 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 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://www.vue.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. 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 (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 there is a set of known standards. 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 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.

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
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

Objective	Chapter
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.

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. 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. The Python interpreter is slow.

B. The 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