SECOND EDITION

CEH™ v11

CERTIFIED ETHICAL HACKER VERSION 11

PRACTICE TESTS

RIC MESSIER

Provides 5 complete, unique practice tests covering all sections of the CEH v11.

Complements the *Sybex CEH v11: Certified Ethical Hacker Version 11 Study Guide*.

SYBEX®
A Wiley Brand

CEH™ v11

Certified Ethical Hacker

Version 11

Practice Tests

Second Edition

Ric Messier

SYBEX®
A Wiley Brand

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

Published simultaneously in Canada.

978-1-119-82451-0
978-1-119-82513-5 (ebk.)
978-1-119-82452-7 (ebk.)

Library of Congress Control Number: 2021943988

Cover Image: © Getty Images Inc./Jeremy Woodhouse
Cover Design: Wiley

For my best friend, partner, and the best support and cheerleader I could ask for, Robin.

Acknowledgments

Thanks to my agent, Carole, for always looking out for me, and thanks to Robin for always supporting me and keeping me going as I worked through this process. Thanks as well to the Wiley staff, Tom Dinse, and Jim Minatel for their support through the editing of this book.

The publisher wishes to acknowledge the work of Raymond Blockmon, the author of the previous Sybex book *CEH v9: Certified Ethical Hacker Version 9 Practice Tests*. Although this new book, *CEH v11: Certified Ethical Hacker Version 11 Practice Tests*, is heavily updated with new and revised questions, Raymond's work on the CEH v9 book laid the foundation that made this new CEH v11 book possible.

About the Author

Ric Messier got started in information security in the early 1980s by discovering a privilege escalation vulnerability on an IBM mainframe that opened the door to the worldwide network of the BITNET for him. Since that time, he has been a programmer, system administrator, network engineer, security consultant, instructor, program director, and penetration tester as well as having led a security engineering team at a global Internet service provider (the company that built the ARPAnet). He has developed many training courses as well as having developed graduate degree programs for two colleges. Additionally, he's taught courses at Brandeis University, Champlain College, University of Colorado at Boulder, and Harvard University. He holds CEH, CCSP, GCIH, GSEC, and CISSP certifications and has previously held CCNA, MCSE, and MCP+I certifications. Additionally, he has a Master of Science degree in Digital forensic science. He is currently a Principal Consultant with Mandiant, a world leader in incident response and security consulting.

About the Technical Editor

Kenneth Tanner is an IT professional with 25+ years of extensive hands-on experience in networking, telecommunications, and systems administration, and the security thereof. He is currently a Senior Technical Instructor at FireEye/Mandiant where he provides instruction on incident response. He has also worked for Hughes Training, The University of Alabama System, and various private companies as a consultant and/or instructor. Kenneth attended the University of Alabama at Birmingham (UAB) in Birmingham, Alabama where he received both a Bachelor and Master of Science degree in Electrical Engineering. He currently holds the following certifications: $(ISC)^2$ CISSP, EC-Council CEH, CND and CHFI, CompTIA CASP, PenTest+, CySA+, Security+, and Network+, Cisco CCNA Route and Switch, CCNA Security, CCNA Voice, CCNA CyberOps, and CCDA, Axelos ITIL, Metasploit Pro Certified Specialist, and Nexpose Certified Administrator. He has taught many of the certifications he holds. Kenneth lives in Colorado with his wife, Nadean, and their two children Shelby and Gavin.

Contents

Introduction *vi*

Chapter 1 Practice Test 1 1

Chapter 2 Practice Test 2 27

Chapter 3 Practice Test 3 55

Chapter 4 Practice Test 4 81

Chapter 5 Practice Test 5 107

Appendix Answers to Practice Tests 133

Chapter 1: Practice Test 1 134
Chapter 2: Practice Test 2 145
Chapter 3: Practice Test 3 157
Chapter 4: Practice Test 4 169
Chapter 5: Practice Test 5 180

Index *191*

Introduction

This exam book is designed to give the CEH candidate a realistic idea of what the CEH exam will look like. As a candidate, you should be familiar with Wireshark, Nmap, and other tools. To get the most out of these exams, you should consider constructing a virtual lab and practicing with the tools to become familiar with viewing the logs that are generated. In preparing for the CEH exam, you will benefit greatly by using YouTube. YouTube is a goldmine of information—and it's free. It is also recommended that you keep up with the latest malware and cybersecurity news provided online. Most cybersecurity-related websites provide insight on the latest vulnerabilities and exploits that are in the wild. Keeping up-to-date with this information will only add value to your CEH knowledge and will help solidify your understanding even more.

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.

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 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.

Further Resources

Finally, this exam book should not be the only resource you use to prepare. You should use other exam books and study guides as well. The more diverse the exposure in terms of reading and preparation material, the better. Take your time studying; invest at least one hour per day prior to your exam date.

If you have not already read *CEHv11: Certified Ethical Hacker Version 11 Study Guide* (Sybex, 2021) and you're not seeing passing grades on these practice tests, it is an excellent resource to master any CEH topics causing problems. The study guide maps every official exam objective to the corresponding chapter in the book to help track your exam preparation objective by objective. There are also challenging review questions in each chapter to prepare for exam day and online test prep materials including flashcards and additional practice tests.

How to Register for the Online Testbanks

All the questions in this book are also available in Sybex's online practice test tool. To get access to this online learning environment, go to `www.wiley.com/go/sybextestprep` and start by registering your book. You'll receive a PIN code and instructions on where to create an online test bank account. Once you have access, you can use the online version to create your own sets of practice tests from the book questions and practice in a timed and graded setting.

Chapter

1

Practice Test 1

1. Which of the following is considered a passive reconnaissance action?
   - **A.** Searching through the local paper
   - **B.** Calling Human Resources
   - **C.** Using the `nmap -sT` command
   - **D.** Conducting a man-in-the-middle attack

2. Which encryption was selected by NIST as the principal method for providing confidentiality after the DES algorithm?
   - **A.** 3DES
   - **B.** Twofish
   - **C.** RC4
   - **D.** AES

3. What cloud service would you be most likely to use if you wanted to share documents with another person?
   - **A.** Software as a Service
   - **B.** Platform as a Service
   - **C.** Storage as a Service
   - **D.** Infrastructure as a Service

4. What is the difference between a traditional firewall and an IPS?
   - **A.** Firewalls don't generate logs.
   - **B.** An IPS cannot drop packets.
   - **C.** An IPS does not follow rules.
   - **D.** An IPS can inspect and drop packets.

5. What is one of the advantages of IPv6 over IPv4 from a security perspective?
   - **A.** IPv4 has a smaller address space.
   - **B.** IPv6 allows for header authentication.
   - **C.** IPv6 is more flexible about extensions.
   - **D.** IPv6 is typically represented in hexadecimal.

6. You are the senior manager in the IT department for your company. What is the most cost-effective way to prevent social engineering attacks?
   - **A.** Install HIDS.
   - **B.** Ensure that all patches are up-to-date.
   - **C.** Monitor and control all email activity.
   - **D.** Implement security awareness training.

7. In which phase within the ethical hacking framework do you alter or delete log information?
   - **A.** Scanning and enumeration
   - **B.** Gaining access
   - **C.** Reconnaissance
   - **D.** Covering tracks

8. An attacker is conducting the following on the target workstation: `nmap -sT 192.33.10.5`. The attacker is in which phase?

A. Covering tracks

B. Enumeration

C. Scanning and enumeration

D. Gaining access

9. Which encryption algorithm is a symmetric stream cipher?

A. AES

B. ECC

C. RC4

D. PGP

10. What is the most important part of conducting a penetration test?

A. Receiving a formal written agreement

B. Documenting all actions and activities

C. Remediating serious threats immediately

D. Maintaining proper handoff with the information assurance team

11. You are a CISO for a giant tech company. You are charged with implementing an encryption cipher for your new mobile devices that will be introduced in 2022. What encryption standard will you most likely choose?

A. RC4

B. MD5

C. AES

D. Skipjack

12. What does a SYN scan accomplish?

A. It establishes a full TCP connection.

B. It establishes only a "half open" connection.

C. It opens an ACK connection with the target.

D. It detects all closed ports on the target system.

13. What is the major vulnerability for an ARP request?

A. It sends out an address request to all the hosts on the LAN.

B. The address is returned with a username and password in cleartext.

C. The address request can cause a DoS.

D. The address request can be spoofed with the attacker's MAC address.

14. You are the CISO for a popular social website. Your engineers are telling you they are seeing multiple authentication failures but with multiple usernames, none of them ever repeated. What type of attack are you seeing?

A. Brute force password attack

B. Authentication failure attack

C. Denial-of-service attack

D. Credential stuffing attack

15. What is the purpose of a man-in-the-middle attack?

A. Gaining access

B. Maintaining access

C. Hijacking a session

D. Covering tracks

16. What method of exploitation might allow the adversary to pass arbitrary SQL queries within the URL?

A. SQL injection

B. XSS

C. Spear phishing

D. Ruby on Rails injection method

17. What is the default TTL value for Microsoft Windows 10 OS?

A. 64

B. 128

C. 255

D. 256

18. Which input value would you utilize in order to evaluate and test for SQL injection vulnerabilities?

A. SQL test

B. admin and password

C. `|| or |!`

D. `1=1'`

19. What is the advantage of using SSH for command-line traffic?

A. SSH encrypts the traffic and credentials.

B. You cannot see what the adversary is doing.

C. Data is sent in the clear.

D. A and B.

20. What year did the Ping of Death first appear?

A. 1992

B. 1989

C. 1990

D. 1996

21. Which type of malware is likely the most impactful?

A. Worm

B. Dropper

C. Ransomware

D. Virus

22. You are part of the help desk team. You receive a ticket from one of your users that their computer is periodically slow. The user also states that from time to time, documents have either disappeared or have been moved from their original location to another. You remote desktop to the user's computer and investigate. Where is the most likely place to see if any new processes have started?

A. The Processes tab in Task Manager

B. `C:\Temp`

C. The Logs tab in Task Manager

D. `C:\Windows\System32\User`

23. Your security team notifies you that they are seeing the same SSID being advertised in your vicinity, but the BSSID is different from ones they are aware of. What type of attack is this?

A. Deauthentication attack

B. Wardriving

C. MAC spoofing

D. Evil twin

24. What does a checksum indicate?

A. That the data has made it to its destination

B. That the three-way TCP/IP handshake finished

C. That there were changes to the data during transit or at rest

D. The size of the data after storage

25. Out of the following, which is one of RSA's registered key strengths?

A. 1,024 bits

B. 256 bits

C. 128 bits

D. 512 bits

26. To provide non-repudiation for email, which algorithm would you choose to implement?

- **A.** AES
- **B.** DSA
- **C.** 3DES
- **D.** Skipjack

27. Which of the following describes a race condition?

- **A.** Where two conditions occur at the same time and there is a chance that arbitrary commands can be executed with a user's elevated permissions, which can then be used by the adversary
- **B.** Where two conditions cancel one another out and arbitrary commands can be used based on the user privilege level
- **C.** Where two conditions are executed under the same user account
- **D.** Where two conditions are executed simultaneously with elevated user privileges

28. Your end clients report that they cannot reach any website on the external network. As the network administrator, you decide to conduct some fact finding. Upon your investigation, you determine that you are able to ping outside of the LAN to external websites using their IP address. Pinging websites with their domain name resolution does not work. What is most likely causing the issue?

- **A.** The firewall is blocking DNS resolution.
- **B.** The DNS server is not functioning correctly.
- **C.** The external websites are not responding.
- **D.** An HTTP GET request is being dropped at the firewall, preventing it from going out.

29. You are the security administration for your local city. You just installed a new IPS. Other than plugging it in and applying some basic IPS rules, no other configuration has been made. You come in the next morning, and you discover that there was so much activity generated by the IPS in the logs that it is too time-consuming to view. What most likely caused the huge influx of logs from the IPS?

- **A.** The clipping level was established.
- **B.** A developer had local admin rights.
- **C.** The LAN experienced a switching loop.
- **D.** The new rules were poorly designed.

30. Which method would be targeting the client in a web-based communication?

- **A.** Cross-site scripting (XSS)
- **B.** SQL injection
- **C.** XML external entity
- **D.** Command injection

31. As a penetration tester, only you and a few key selected individuals from the company will know of the targeted network that will be tested. You also have zero knowledge of your target other than the name and location of the company. What type of assessment is this called?

A. Gray box testing

B. White box testing

C. Black box testing

D. Blue box testing

32. As an attacker, you are searching social media sites as well as job listings. What phase of the attack are you in?

A. Casing the target

B. Gaining access

C. Maintaining access

D. Reconnaissance

33. Which scanning tool is more likely going to yield accurate and useful results during reconnaissance and enumeration?

A. ncat

B. Nmap

C. ping

D. nslookup

34. Why would an attacker conduct an open TCP connection scan using Nmap?

A. The attacker does not want to attack the system.

B. The attacker made a mistake by not selecting a SYN scan function.

C. The attacker is trying to connect to network services.

D. The attacker is trying to make the scan look like normal traffic.

35. Why would an attacker want to avoid tapping into a fiber-optic line?

A. It costs a lot of money to tap into a fiber line.

B. If done wrong, it could cause the entire connection signal to drop, therefore bringing unwanted attention from the targeted organization.

C. The network traffic would slow down significantly.

D. Tapping the line could alert an IPS/IDS.

36. You are an attacker who has successfully infiltrated your target's web server. You performed a web defacement on the targeted organization's website, and you were able to create your own credential with administrative privileges. Before conducting data exfiltration, what is the next move?

A. Log into the new user account that you created.

B. Go back and delete or edit the logs.

C. Ensure that you log out of the session.

D. Ensure that you migrate to a different session and log out.

37. What is a common attack type of the Kerberos protocol that can look like legitimate traffic?

A. Kerberoasting

B. Javaroasting

C. Man-in-the-middle

D. Ticket granting compromise

38. Where is the password file located on a Windows system?

A. `C:\Windows\temp`

B. `C:\Win\system\config`

C. `C:\Windows\accounts\config`

D. `C:\Windows\system32\config`

39. Which response would the adversary receive on closed ports if they conducted an XMAS scan?

A. RST

B. RST/ACK

C. No Response

D. FIN/ACK

40. Why would the adversary encode their payload before sending it to the target victim?

A. Encoding the payload will not provide any additional benefit.

B. By encoding the payload, the adversary actually encrypts the payload.

C. The encoded payload can bypass the firewall because there is no port associated with the payload.

D. Encoding the payload may bypass IPS/IDS detection because it changes the signature.

41. Which password is more secure?

A. keepyourpasswordsecuretoyourself

B. pass123!!

C. P@$$w0rD

D. KeepY0urPasswordSafe!

42. Which of the following best describes DNS poisoning?

A. The adversary intercepts and replaces the victim's MAC address with their own.

B. The adversary replaces their malicious IP address with the victim's IP address for the domain name.

C. The adversary replaces the legitimate domain name with the malicious domain name.

D. The adversary replaces the legitimate IP address that is mapped to the fully qualified domain name with the malicious IP address.

43. Which of the following allows the adversary to forge certificates for authentication?

A. Wireshark

B. Ettercap

C. Cain & Abel

D. Ncat

44. Which encryption standard is used in WEP?

A. AES

B. RC5

C. MD5

D. RC4

45. You are sitting inside of your office, and you notice a strange person in the parking lot with what appears to be a tall antenna connected to a laptop. What is the stranger most likely doing?

A. Brute-forcing their personal electronic device

B. Wardriving

C. Warflying

D. Bluesnarfing

46. If a web application is using a RESTful API, NoSQL databases, and microservices in containers, what style of design is it likely using?

A. Model-view-controller

B. Cloud-native design

C. Traditional architecture

D. NoSQL design

47. Which is the best example of a denial-of-service (DoS) attack?

A. A victim's computer is infected with a virus.

B. A misconfigured switch is in a switching loop.

C. An adversary is forging a certificate.

D. An adversary is consuming all available memory of a target system by opening as many "half-open" connections on a web server as possible.

48. In the Windows SAM file, what security identifier would indicate to the adversary that a given account is an administrator account?

A. 500

B. 1001

C. ADM

D. ADMIN_500

49. Which regional Internet registry is responsible for North and South America?

A. RIPE

B. AMERNIC

C. LACNIC

D. ARIN

50. Which of following actions is the last step in scanning a target?

A. Scan for vulnerabilities

B. Identify live systems

C. Discover open ports

D. Identify the OS and servers

51. Which of the following best describes the ICMP Type 8 code?

A. Device is being filtered

B. Network route is incorrect or missing

C. Echo request

D. Destination unreachable

52. Which of the following port ranges will show you the ports requiring administrative access?

A. 0 to 1023

B. 0 to 255

C. 1024 to 49151

D. 1 to 128

53. What is the length of an IPv6 address?

A. 64 bits

B. 128 bits

C. 256 bits

D. 32 bits

54. Which of the following switches for the Nmap command does nothing but fingerprinting an operating system?

A. `-O`

B. `-sFRU`

C. `-sA`

D. `-sX`

55. What command would the adversary use to show all the systems within the domain using the command-line interface in Windows?

A. `netstat -R /domain`

B. `net view /<domain_name>:domain`

C. `net view /domain:<domain_name>`

D. `netstat /domain:<domain_name>`

56. You are a passenger in an airport terminal. You glance across the terminal and notice a man peering over the shoulder of a young woman as she uses her tablet. What do you think he is doing?

A. Wardriving

B. Shoulder surfing

C. War shouldering

D. Shoulder jacking

57. What type of attack is being used if you were to see `<!ENTITY xxe SYSTEM "file:///etc/passwd">` in your web server logs?

A. SQL injection

B. XSS

C. Command injection

D. XXE

58. Which option describes the concept of injecting code into a portion of data in memory that allows for arbitrary commands to be executed?

A. Buffer overflow

B. Crash

C. Heap spraying

D. Format string

59. Of the following methods, which one acts as a middleman between an external network and the private network by initiating and establishing the connection?

A. Proxy server

B. Firewall

C. Router

D. Switch

60. As an attacker, you successfully exploited your target using a service that should have been disabled. The service had vulnerabilities that you were able to exploit with ease. There appeared to be a large cache of readily accessible information. What may be the issue here?

A. The administrator did not apply the correct patches.

B. The web server was improperly configured.

C. You are dealing with a honeypot.

D. The firewall was not configured correctly.

61. Where is the logfile that is associated with the activities of the last user that signed in within a Linux system?

A. `/var/log/user_log`

B. `/var/log/messages`

C. `/var/log/lastlog`

D. `/var/log/last_user`

62. What default TCP port does SSH utilize?

A. Port 22

B. Port 21

C. Port 443

D. Port 25

63. As a pen tester, you are hired to conduct an assessment on a group of systems for your client. You are provided with a list of critical assets, a list of domain controllers, and a list of virtual share drives. Nothing else was provided. What type of test are you conducting?

A. White hat testing

B. Gray hat testing

C. Gray box testing

D. Red hat testing

64. Which type of firewall would you use if you wanted to have the firewall check for malware as it passed through the firewall?

A. Web application firewall

B. Stateful firewall

C. Next-generation firewall

D. Stateless firewall

65. Which tool can be used to conduct layer 4 scanning and enumeration?

A. Cain & Abel

B. John the Ripper

C. Ping-eater

D. Nmap

66. What port number or numbers is/are associated with the IP protocol?

A. 0 to 65535

B. No ports

C. 53

D. 80