EC-Council Certified Ethical Hacker (CEH) Certification Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here’s how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don’t just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **Which statement best describes a rootkit?**

   A. Can modify the network interface only

   B. Can modify the operating system and the utilities of the target system

   C. Is a form of antivirus software

   D. Only hides files on the disk

2. **Which item is included in the scope of work for a merger penetration test?**

   A. IT budgets

   B. Office leases

   C. Marketing slogans

   D. Company culture

3. **Which information sharing policy addresses the sharing of critical information in press releases, annual reports, product catalogs, and marketing materials?**

   A. A printed materials policy

   B. Data breach notification policy

   C. Incident response policy

   D. Acceptable use policy

4. **In OS fingerprinting, which attributes of a response are commonly analyzed to guess the target OS?**

   A. IP address and DNS records

   B. Port numbers and service banners

   C. Time To Live (TTL) and window size

   D. MAC address and vendor ID

5. **In packet analysis, what does filtering for a specific host typically accomplish?**

   A. It captures only traffic to or from that host.

   B. It captures only inbound.

   C. It captures only outbound.

   D. It captures all traffic.

6. Which type of vulnerability research focuses on application flaws in software during security testing?

A. Network scanning

B. Firmware analysis

C. Social engineering

D. Application flaws

7. Which term describes registering a domain name that closely resembles a cloud provider to deceive users?

A. Phishing

B. DNS Spoofing

C. Cybersquatting

D. Man-in-the-middle

8. Which tool is commonly used to inspect network traffic and can be deployed inline for protection?

A. Snort inline

B. Nmap

C. Burp Suite

D. Wireshark

9. Which statement correctly describes the difference between proximity cards and smart cards?

A. Proximity cards communicate more information than smart cards.

B. Proximity cards are designed to only communicate the card's ID, while smart cards can communicate more information.

C. Proximity cards require physical contact to read the ID, while smart cards are contactless.

D. Proximity cards operate at 13.56 MHz, while smart cards operate at 125 kHz.

10. During a penetration test with limited information, what type of engagement is being performed if only the target's IP address and hostname are known?

A. Internal

B. External

C. Blind

D. Targeted

Answers

1. B
2. D
3. A
4. C
5. A
6. D
7. C
8. A
9. B
10. B

Explanations

1. Which statement best describes a rootkit?

A. Can modify the network interface only

B. Can modify the operating system and the utilities of the target system

C. Is a form of antivirus software

D. Only hides files on the disk

Rootkits are stealthy malware that gain high privileges and hide themselves by tampering with the operating system and its essential utilities. By integrating with the OS—often at the kernel level—and by altering or replacing system binaries, drivers, and utilities, they can intercept system calls and conceal processes, files, registry entries, network connections, and other artifacts, all while maintaining persistence and control over the system. This breadth of capability is what makes the description that a rootkit can modify the operating system and the utilities of the target system the best fit. In contrast, limiting modification to the network interface is too narrow, since rootkits can affect many parts of the system beyond the network. They are not antivirus software; rootkits are designed to evade detection and grant control, not protect the host. And while hiding files can be part of what they do, rootkits go further by concealing processes, memory, network connections, and by altering the behavior of system utilities to avoid detection.

2. Which item is included in the scope of work for a merger penetration test?

A. IT budgets

B. Office leases

C. Marketing slogans

D. Company culture

In merger penetration testing, the scope isn't limited to technical systems; it includes organizational and human factors that shape security. Company culture matters because it influences how employees follow security policies, respond to suspicious activity, and adopt security practices during integration. When two organizations merge, differences in training, awareness, and collaboration can create security gaps that technical scans alone might miss. By evaluating culture, you assess social engineering risk, insider threat potential, and the overall willingness to enforce and sustain security measures across the new entity. The other items—IT budgets, office leases, and marketing slogans—are business or logistical concerns and don't directly reflect how people behave or how security controls are applied, which is what the test aims to gauge.

3. Which information sharing policy addresses the sharing of critical information in press releases, annual reports, product catalogs, and marketing materials?

A. A printed materials policy

B. Data breach notification policy

C. Incident response policy

D. Acceptable use policy

External communications and public disclosures rely on controls that govern what information can be shared and how it is presented. The printed materials policy is designed to manage the creation and distribution of physical materials such as press releases, annual reports, product catalogs, and marketing materials. It addresses what information may be disclosed, who must approve content, and how branding and confidentiality considerations are applied, ensuring accuracy and regulatory compliance in outward-facing documents. The other policies focus on different areas: data breach notification deals with informing about security incidents, incident response covers the steps to handle security events, and acceptable use focuses on the proper use of company IT resources rather than the content of external communications.

4. In OS fingerprinting, which attributes of a response are commonly analyzed to guess the target OS?

A. IP address and DNS records

B. Port numbers and service banners

C. Time To Live (TTL) and window size

D. MAC address and vendor ID

OS fingerprinting hinges on how a target's TCP/IP stack responds to crafted probes, with certain response attributes serving as telltale signs of the operating system. The most informative are the Time To Live (TTL) value and the TCP window size. TTL is set by the sending OS and each hop reduces it by one; different OS families tend to use characteristic initial TTL values (for example 64, 128, or 255). By observing the TTL in replies, you can estimate how many hops were traversed and which OS family is likely. The TCP window size reveals how the sender's stack configures flow control for connections; default window sizes and subsequent scaling behavior vary across OS implementations, producing distinctive fingerprints in responses to probes. When you combine TTL and window size, you get a reliable signal about the target's stack. Other options don't map as directly to the OS. IP address and DNS records show where a host is or what name it uses, not what it's running. Ports and service banners indicate what services are active, but many OSes can run the same services. MAC address and vendor ID identify the network interface hardware and are typically visible only within the local network; they don't reliably indicate the operating system on distant hosts.

5. In packet analysis, what does filtering for a specific host typically accomplish?

A. It captures only traffic to or from that host.

B. It captures only inbound.

C. It captures only outbound.

D. It captures all traffic.

Filtering for a specific host focuses the capture on the communications that involve that host's IP address. This means you'll see packets where the host is either the source or the destination, giving a complete view of both inbound and outbound traffic for that host. It narrows down what you're analyzing to just that host's activity, rather than everything on the network. If you want only inbound or only outbound traffic, you'd apply a directional filter (for example, filtering only packets where the host is the destination or only where it is the source).

6. Which type of vulnerability research focuses on application flaws in software during security testing?

A. Network scanning

B. Firmware analysis

C. Social engineering

D. Application flaws

Focusing vulnerability research on applications means scrutinizing software for weaknesses in how it processes input, enforces authentication and authorization, manages sessions, and implements its logic during security testing. This targets flaws inside the software itself, such as insecure input handling or broken access control. Network scanning, by comparison, looks at exposed services and hosts on a network rather than the internal flaws of the software. Firmware analysis examines embedded device firmware, not application software. Social engineering targets people and processes rather than technical flaws in software. Because the question highlights finding weaknesses inside software during testing, the best fit is application flaws.

7. Which term describes registering a domain name that closely resembles a cloud provider to deceive users?

A. Phishing

B. DNS Spoofing

C. Cybersquatting

D. Man-in-the-middle

Registering a domain name that closely imitates a legitimate cloud provider to deceive users is cybersquatting. This tactic hinges on capturing trust by making the site look real enough that users think they're visiting the genuine provider. The attacker can lure victims into clicking, entering credentials, or downloading malware, all by exploiting the familiar brand name and design cues. Phishing describes the broader goal of tricking people into divulging sensitive information and can be carried out using cybersquatted domains, but the specific act of acquiring a near-copy domain is cybersquatting. DNS spoofing and man-in-the-middle describe different attack methods that don't hinge on registering a confusingly similar domain.

8. Which tool is commonly used to inspect network traffic and can be deployed inline for protection?

A. Snort inline

B. Nmap

C. Burp Suite

D. Wireshark

Snort in inline mode is designed to inspect every packet as it traverses the network and enforce protections based on its rule set. When placed inline, Snort acts as an intrusion prevention system: it analyzes traffic against signatures and policies, and it can drop, reject, or reset connections that match malicious patterns, effectively stopping attacks in real time while providing alerts. This capability is why it's commonly used for protection in addition to detection. Other tools serve different purposes: Nmap is a network scanner used to map hosts and services, not to inspect and block traffic; Burp Suite is a web application testing proxy for analyzing and manipulating web traffic, not a general network IPS; Wireshark is a packet analyzer for passive visibility and troubleshooting, not something that blocks traffic in real time.

9. Which statement correctly describes the difference between proximity cards and smart cards?

A. Proximity cards communicate more information than smart cards.

B. Proximity cards are designed to only communicate the card's ID, while smart cards can communicate more information.

C. Proximity cards require physical contact to read the ID, while smart cards are contactless.

D. Proximity cards operate at 13.56 MHz, while smart cards operate at 125 kHz.

The key idea here is what each type of card is capable of communicating and processing. Proximity cards are designed to simply transmit the card's identifier when they're in a reader's field. They are usually passive devices with little to no ability to store or process information themselves. Smart cards, on the other hand, have an embedded microprocessor and memory, so they can store multiple data items, perform cryptographic operations, run authentication checks, and handle more complex interactions with a reader. That combination of data storage and on-card processing means smart cards can convey or verify much more than just a single ID. So, the statement that proximity cards primarily communicate the card's ID while smart cards can communicate more information accurately captures the practical difference between them. The other descriptions don't fit: proximity cards aren't defined by requiring physical contact (they're typically contactless), and the frequency used is not the defining factor—the real distinction is the processing capability and the amount of information that can be exchanged.

10. During a penetration test with limited information, what type of engagement is being performed if only the target's IP address and hostname are known?

A. Internal

B. External

C. Blind

D. Targeted

The key idea here is distinguishing how a penetration test is scoped and where the tester operates. An external engagement means testing from outside the target's network, focusing on assets exposed to the internet. Knowing only the target's IP address and hostname fits this, because you're starting with publicly reachable identifiers and are attempting to assess external defense without internal access or detailed internal knowledge. Internal would require access inside the network or credentials. Blind would imply almost no information about the target, or that you must discover everything without hints, which isn't the case when an IP and hostname are already known. Targeted implies a highly collaborative scenario with more contextual information provided to the tester.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://eccouncilceh.examzify.com

We wish you the very best on your exam journey. You've got this!