EC-COUNCIL CERTIFIED ETHICAL HACKER (CEH) CERTIFICATION PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://eccouncilceh.examzify.com

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 of the following are spoofing methods?

A. ARP spoofing

B. DNS spoofing

C. IP spoofing

D. All of the above

2. Which technique involves adding random bits of data to a password before it is stored as a hash?

A. Hashing without salt

B. Encryption

C. Key stretching

D. Password salting

3. Which tool is suitable for OS fingerprinting by analyzing network traffic?

A. Nmap results

B. P0f OS fingerprinting

C. Wireshark capture

D. Netstat

4. In vulnerability assessment, which phase focuses on identifying externally visible services on a target with limited information?

A. Wireless auditing

B. External penetration testing

C. Internal vulnerability scanning

D. Social engineering assessment

5. What describes a session ID?

A. A unique token that a server assigns for the duration of a client's communications with the server

B. An identifying user name

C. A session cookie used after login

D. A cryptographic nonce for each request

6. **Implementing emergency lighting that operates on protected power and activates automatically when main power fails is an example of which physical security objective?**

A. Data confidentiality

B. Employee and visitor safety

C. Access control

D. Availability

7. **Which tool uses rainbow tables to crack Windows login passwords?**

A. Hashcat

B. Ophcrack

C. John the Ripper

D. Cain and Abel

8. **A person discovers a vulnerability on a system without permission, anonymously alerts the owner, and instructs how to secure it. What type of hacker is this?**

A. Black hat

B. White hat

C. Gray hat

D. Script kiddie

9. **What does malware provide to the attacker on a compromised device?**

A. An access point to the attacker.

B. A firewall

C. A VPN

D. A honeypot

10. **In User-Mode Linux, which device represents the guest's virtual hard disk?**

A. /dev/sda

B. /dev/null

C. /dev/vda

D. /dev/ubd*

Answers

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

Explanations

1. Which of the following are spoofing methods?

A. ARP spoofing

B. DNS spoofing

C. IP spoofing

D. All of the above

Spoofing is about deceiving a system or user by pretending to be someone or something else, often to intercept traffic, misdirect requests, or evade detection. ARP spoofing works on the local network by sending forged ARP messages that link the attacker's MAC address to the IP address of another device (like the gateway or a victim). This lets the attacker intercept or modify traffic between devices on the same LAN, creating a man-in-the-middle position. DNS spoofing involves deceiving name resolution so that a domain name resolves to a fraudulent IP address. This can be done by poisoning a DNS cache or by crafting forged DNS responses so users end up at attacker-controlled sites when they think they're visiting a legitimate one. IP spoofing is when the source IP address in packets is forged to appear as though it came from a different machine. This is used to impersonate another host, evade traceability, or facilitate certain attack techniques like reflection or amplification. Because each technique involves falsifying information to impersonate or mislead a part of the network, all of these are spoofing methods.

2. Which technique involves adding random bits of data to a password before it is stored as a hash?

A. Hashing without salt

B. Encryption

C. Key stretching

D. Password salting

Adding random data to a password before hashing is known as salting. The random value, called a salt, is unique for each password and is stored alongside the resulting hash. This ensures that even if two users have the same password, their hashes will be different, so precomputed rainbow tables can't be reused. Because each password-hash pair uses its own salt, an attacker would have to compute hashes separately for every possible password with every salt, which greatly increases the effort required. Encryption isn't used for password storage because it's reversible, whereas hashing (with a salt) aims to store a one-way representation. Hashing without a salt leaves you vulnerable to rainbow table attacks. Key stretching, while related in practice to slowing down attackers by increasing computation (and often involving a salt), is a separate technique focused on making hash computations intentionally slower. The technique described here is specifically salting.

3. Which tool is suitable for OS fingerprinting by analyzing network traffic?

A. Nmap results

B. P0f OS fingerprinting

C. Wireshark capture

D. Netstat

Passive OS fingerprinting focuses on the information already present in network traffic rather than sending probes. P0f is built for this approach: it passively monitors captured traffic, analyzes characteristics of the remote host's TCP/IP stack (such as TTL, window size, IPID behavior, TCP options, and timing patterns), and matches those fingerprints against a database to infer the operating system. This makes it the best fit for OS fingerprinting by analyzing network traffic because it does not generate additional traffic or detectable probes, reducing impact on the target and remaining covert. By contrast, the other tools have different primary roles: a packet analyzer like Wireshark captures and lets you inspect traffic, but it doesn't automatically map those observations to an OS; a netstat command shows current connections and ports rather than fingerprinting the host; and active scanners that produce results, like Nmap, rely on sending crafted probes to elicit responses, which is not analyzing existing traffic.

4. In vulnerability assessment, which phase focuses on identifying externally visible services on a target with limited information?

A. Wireless auditing

B. External penetration testing

C. Internal vulnerability scanning

D. Social engineering assessment

From an outside-in perspective, the goal is to map the attack surface that an external attacker could reach with limited starting information. The phase that focuses on identifying externally visible services on a target in this way is external penetration testing. It involves simulating an attacker coming from outside the organization, with minimal intel, and using network discovery to determine what is exposed—from which hosts to which ports and services are reachable, and what versions or configurations might be vulnerable. This helps establish what an attacker could actually exploit from the internet and guides what needs to be secured or patched. If you think about the other options, wireless auditing targets Wi Fi security, not the internet-facing services; internal vulnerability scanning looks at assets inside the network after access is gained; and social engineering assesses human factors rather than technical exposure.

5. What describes a session ID?

A. A unique token that a server assigns for the duration of a client's communications with the server

B. An identifying user name

C. A session cookie used after login

D. A cryptographic nonce for each request

A session ID is a unique token that the server creates to identify a specific user's session for the duration of their interaction with the application. HTTP is stateless, so the server wouldn't know who you are from one request to the next. It generates a random, hard-to-guess identifier and associates any session data (like login status, shopping cart contents, preferences) with that ID on the server. The client then presents this token with subsequent requests (typically via a cookie), and the server uses it to fetch the correct session data and continue where you left off. This concept is different from a user name, which identifies the user themselves, and it's not a per-request nonce. A session cookie is a common transport method for the ID, but what matters is the server-issued token that links requests to a particular session.

6. Implementing emergency lighting that operates on protected power and activates automatically when main power fails is an example of which physical security objective?

A. Data confidentiality

B. Employee and visitor safety

C. Access control

D. Availability

The main idea is protecting people's safety during emergencies. Emergency lighting that runs on protected power and automatically activates when main power fails ensures that exits are clearly visible, guiding employees and visitors to safety even in a blackout. This focus on preserving life and enabling safe evacuation is why it's best categorized as protecting employee and visitor safety. It doesn't directly address protecting data, restricting access, or keeping IT services running, whereas the immediate priority in this scenario is the safe movement of people during a power loss.

7. Which tool uses rainbow tables to crack Windows login passwords?

A. Hashcat

B. Ophcrack

C. John the Ripper

D. Cain and Abel

Rainbow tables are precomputed mappings of hashes to plaintext passwords, allowing quick reversal of hash values without trying every possible password. Windows login credentials are stored as hashes (NTLM/LM), so cracking involves reversing those hashes offline. Ophcrack is built to crack Windows passwords by loading rainbow tables and using them to map the captured NTLM/LM hashes back to the original passwords. This makes it especially fast for common Windows passwords compared to brute-force or dictionary methods. The other tools are versatile crackers that rely on dictionaries, rules, or brute force rather than precomputed tables, so they aren't based on rainbow-table attacks.

8. A person discovers a vulnerability on a system without permission, anonymously alerts the owner, and instructs how to secure it. What type of hacker is this?

A. Black hat

B. White hat

C. Gray hat

D. Script kiddie

Disclosing a vulnerability without official permission but providing a fix or guidance shows crossing a testing boundary without authorization, yet aiming to improve security. That combination is characteristic of a gray hat hacker: they don't have formal authorization to test the system, but their actions are meant to help by alerting the owner and offering steps to secure the flaw. White hats operate with explicit authorization and usually follow a formal process or program; black hats exploit or cause harm for gain; script kiddies rely on ready-made tools with little understanding. Anonymous notification can fit gray hat behavior because the intent is protective, even if the method doesn't follow sanctioned testing rules.

9. What does malware provide to the attacker on a compromised device?

A. An access point to the attacker.

B. A firewall

C. A VPN

D. A honeypot

When malware infects a device, its primary aim is to give the attacker a foothold and remote control over that system. It does this by creating a backdoor or remote access mechanism, effectively turning the compromised device into an access point that the attacker can use to issue commands, exfiltrate data, or pivot to other machines. That's why this option best describes what malware provides to the attacker: ongoing access and control through a direct connection into the victim. The other concepts are defensive or decoy in nature and don't originate from malware: a firewall is meant to block or limit access, not provide it; a VPN is a legitimate secure tunnel for privacy or remote access but isn't something malware "provides" to attackers; and a honeypot is a decoy system used to lure attackers, not something malware delivers to enable attacker access.

10. In User-Mode Linux, which device represents the guest's virtual hard disk?

A. /dev/sda

B. /dev/null

C. /dev/vda

D. /dev/ubd*

User-Mode Linux presents the guest's disk through a user-space block device. Inside the UML guest, the virtual hard disk appears as a block device named /dev/ubdN (for example, /dev/ubd0 or /dev/ubd1). This /dev/ubd interface is provided by the UML user-space block driver, mapping a host file to a guest block device. That's why the correct choice is the one referencing /dev/ubd*, rather than /dev/sda (typical in other VM setups), /dev/vda (KVM/virtio), or the non-disk device /dev/null.*

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!