EC-COUNCIL CERTIFIED ETHICAL HACKER (CEH) V13 (312-50V13) PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://eccouncil31250v13.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. Who first presented the meet-in-the-middle attack for cryptanalysis?

A. Diffie and Hellman.

B. Rivest and Shamir.

C. NIST researchers.

D. Lamport and Deffie.

2. Which statements about a zone transfer are correct?

A. A zone transfer is accomplished with DNS, passes all zone information that a DNS server maintains, and can be prevented by blocking all inbound TCP port 53 connections.

B. A zone transfer uses UDP only and cannot be blocked by firewalls.

C. Zone transfers share only a portion of zone data and are hard to block.

D. Zone transfers occur without any DNS involvement.

3. What is the purpose of performing service and OS discovery during vulnerability scanning?

A. To investigate the network topology.

B. To enumerate open ports and identify the operating system on target systems.

C. To patch all known vulnerabilities automatically.

D. To monitor user login activity.

4. Blocking inbound TCP port 53 connections serves to prevent unauthorized zone transfers.

A. To prevent unauthorized zone transfers.

B. To prevent DNS cache poisoning.

C. To block all DNS queries from external networks.

D. To stop remote code execution on the DNS server.

5. What is a common characteristic of phishing scams claiming to be from financial institutions?

A. Generic email addresses not belonging to official representatives.

B. Use of official email domain in all emails.

C. Always includes a security badge.

D. Only targets high-net-worth individuals.

6. In risk management, which concept represents the monetary loss expected from a single incident?

A. Annual Rate of Occurrence

B. Security Loss Expectancy

C. Single Loss Expectancy

D. Single Loss Event

7. What is the significance of the SOA record version in DNS?

A. It indicates the TTL value of zone records.

B. It specifies the mail exchange server.

C. It lists the authoritative servers.

D. It indicates the version of the zone file and helps in managing DNS records.

8. If '/bin/sh' is found in the ASCII output of a network IDS entry, what does this imply?

A. The traffic shows a benign shell command.

B. The attacker is attempting to launch a command-line shell.

C. The IDS signature is misconfigured.

D. The data indicates a file transfer over SSH.

9. Tripwire is primarily used to detect unauthorized changes to what?

A. Network traffic

B. System files and web content

C. User accounts

D. DNS records

10. What is the role of the application server in the recommended architecture?

A. To operate on the internal network and process application logic

B. To face the Internet and handle incoming web requests

C. To store and manage data

D. To route traffic between networks

Answers

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

Explanations

1. Who first presented the meet-in-the-middle attack for cryptanalysis?

A. Diffie and Hellman.

B. Rivest and Shamir.

C. NIST researchers.

D. Lamport and Deffie.

Meet-in-the-middle attacks split a two-stage process, like double encryption, into two halves and look for a match in the middle. You precompute all possible results from the first stage and store them, then work from the second stage and try to match those intermediates with the second-key outcomes. When a match is found, you've effectively identified the two keys with far less effort than trying every possible pair from start to finish. This trade of memory for time is what makes the technique so powerful for breaking two-key schemes. This approach was first presented by Diffie and Hellman in their foundational cryptography work. Their presentation showed how a two-key cascade could be attacked by computing and comparing intermediate values, illustrating a fundamental vulnerability in naïve two-stage designs. The other names listed did not originate this technique, so the credit goes to Diffie and Hellman.

2. Which statements about a zone transfer are correct?

A. A zone transfer is accomplished with DNS, passes all zone information that a DNS server maintains, and can be prevented by blocking all inbound TCP port 53 connections.

B. A zone transfer uses UDP only and cannot be blocked by firewalls.

C. Zone transfers share only a portion of zone data and are hard to block.

D. Zone transfers occur without any DNS involvement.

Zone transfers are a DNS mechanism for replicating zone data from one DNS server to another. In a full transfer (AXFR), the transfer includes all resource records for the zone, which is why a zone transfer can reveal the entire zone's information to the receiving server. These transfers happen using the DNS protocol over TCP port 53 to ensure reliable delivery; blocking inbound TCP traffic on port 53 can prevent them, which is a common defense in securing DNS servers. Normal DNS queries use UDP on port 53, but the actual transfer of zone data relies on TCP, so blocking that TCP path stops the transfer. Zone transfers involve DNS, and they can be restricted or blocked with appropriate firewall rules, unlike options that imply UDP-only transfers, no DNS involvement, or partial data transfers.

3. What is the purpose of performing service and OS discovery during vulnerability scanning?

A. To investigate the network topology.

B. To enumerate open ports and identify the operating system on target systems.

C. To patch all known vulnerabilities automatically.

D. To monitor user login activity.

The goal of service and operating system discovery in vulnerability scanning is to identify which ports are open on each host and what OS is running, so the scanner can apply the right checks and tailor the assessment to the actual environment. By fingerprinting active services and their versions, you map the attack surface accurately, reduce false positives, and choose the most relevant vulnerability tests for each target. Knowing the OS and services also helps prioritize findings based on exposure and exploitability for that specific platform. This isn't about mapping the network just for layout, nor about automatically patching everything or monitoring user logins. Discovery informs what exists on the hosts, which is essential before any effective vulnerability assessment and remediation planning.

4. Blocking inbound TCP port 53 connections serves to prevent unauthorized zone transfers.

A. To prevent unauthorized zone transfers.

B. To prevent DNS cache poisoning.

C. To block all DNS queries from external networks.

D. To stop remote code execution on the DNS server.

Zone transfers replicate the DNS zone data from a primary DNS server to its secondary servers and they use TCP on port 53. By blocking inbound TCP connections to port 53, you prevent remote hosts from requesting those transfers, which stops unauthorized disclosure of your zone data. Regular DNS queries, on the other hand, primarily use UDP on port 53, so normal resolution from clients can continue as long as UDP is allowed. If you need to allow legitimate transfers, you should restrict the source IPs and ideally use authentication like TSIG. This measure doesn't directly prevent cache poisoning or remote code execution, which are addressed by different controls and defenses.

5. What is a common characteristic of phishing scams claiming to be from financial institutions?

A. Generic email addresses not belonging to official representatives.

B. Use of official email domain in all emails.

C. Always includes a security badge.

D. Only targets high-net-worth individuals.

Phishing that pretends to be from financial institutions hinges on impersonation to fool the recipient. A key signal is the sender address being generic and not tied to an official representative of the bank. Attackers often use lookalike domains or vague addresses like a generic security or support mailbox to cast a wide net, hoping someone will act on urgency or fear before noticing the mismatch with the bank's real domain. Because legitimate banks normally use verified, official domains for their communications, this mismatch in who the email appears to come from is a strong hint that the message is not truly from the bank. Other options don't fit the pattern. An email that uses the official bank domain would look legitimate, which is why phishers can try to spoof identities but relying on official domains isn't characteristic of scams. Security badges can be faked and aren't a reliable indicator. And phishing isn't limited to high-net-worth individuals; attackers cast a wide net to harvest credentials or data from as many people as possible. Always verify via official channels rather than clicking links or sharing information in response to such messages.

6. In risk management, which concept represents the monetary loss expected from a single incident?

A. Annual Rate of Occurrence

B. Security Loss Expectancy

C. Single Loss Expectancy

D. Single Loss Event

Single Loss Expectancy measures the monetary loss that would result from one incident affecting an asset. It captures the impact of a single event, not how often it happens or the yearly total. The value is found by multiplying the asset's value by the exposure factor (the portion of the asset lost in that incident). For example, an asset valued at $100,000 with a 40% exposure factor would have an SLE of $40,000. This is distinct from frequency-based metrics like the annualized rate of occurrence, which tells you how often incidents occur in a year, or from terms used to describe yearly losses (often referred to as Security Loss Expectancy or ALE). A Single Loss Event is simply describing an incident, not its monetary impact quantified as a single-event loss.

7. What is the significance of the SOA record version in DNS?

A. It indicates the TTL value of zone records.

B. It specifies the mail exchange server.

C. It lists the authoritative servers.

D. It indicates the version of the zone file and helps in managing DNS records.

The key idea is that the SOA record includes a serial number that acts as a version stamp for the zone. Every time you change the zone data, you increment this serial. Secondary (slave) DNS servers compare their copy's serial with the master's serial; if the master's serial is newer, they fetch an updated zone transfer (IXFR/AXFR) to bring their data up to date. This serial/version mechanism coordinates updates across all DNS servers and ensures consistency of the zone information. It's different from TTL, which governs how long individual records are cached. The primary master and administrative contact are indicated by other fields in the SOA, while the full list of authoritative servers is defined by NS records and not the version number. The mail routing is handled by MX records, not the SOA serial. So, the SOA version is about signaling the zone's version and driving synchronization via zone transfers.

8. If '/bin/sh' is found in the ASCII output of a network IDS entry, what does this imply?

A. The traffic shows a benign shell command.

B. The attacker is attempting to launch a command-line shell.

C. The IDS signature is misconfigured.

D. The data indicates a file transfer over SSH.

Seeing the exact string /bin/sh in ASCII within a network IDS alert typically signals an attempt to invoke the command-line shell on the target. In Unix-like systems, /bin/sh is the standard shell binary, and many exploits or payloads try to spawn a shell to run commands, gain interactive access, or set up remote control. If the IDS payload contains that path, it suggests the attacker is trying to execute shell commands rather than simply transferring data or signaling a benign operation. This is a strong indicator of a command execution or shell-launch attempt. The other options don't fit because a benign shell command, misconfiguration, or an SSH file transfer would not usually manifest as the literal shell path in IDS output.

9. Tripwire is primarily used to detect unauthorized changes to what?

A. Network traffic

B. System files and web content

C. User accounts

D. DNS records

The main idea here is file integrity monitoring. Tripwire is a host-based integrity checker that creates a baseline snapshot of critical files and directories—such as system binaries, configuration files, and web content stored on a server. It records cryptographic hashes, permissions, and other attributes. On subsequent scans, Tripwire compares the current state to the baseline; any unauthorized modification triggers an alert, helping you detect tampering, malware, or unintended changes. Because of that focus, Tripwire is best suited to guarding system files and web content, not network traffic, user accounts, or DNS records, which are typically monitored by other security tools like network intrusion detectors, authentication logs, or DNS-change monitors.

10. What is the role of the application server in the recommended architecture?

A. To operate on the internal network and process application logic

B. To face the Internet and handle incoming web requests

C. To store and manage data

D. To route traffic between networks

In a typical multi-tier setup, the application server is the layer that runs the business logic on the internal network. It takes input from the web front end (or API gateway), processes that input according to the application's rules, coordinates workflows, and talks to the database and other services to produce the needed results. It stays behind the firewall and isn't exposed directly to the Internet; external requests are handled by the web server or gateway first, which then passes them to the application server. This role differs from the tasks of other components: the web server (or gateway) faces the Internet and handles incoming web requests, the database server stores and manages data, and routers/firewalls route or control traffic between networks. Therefore, the application server's primary function is to operate on the internal network and execute the application's logic.

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://eccouncil31250v13.examzify.com

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