EC-Council Certified Ethical Hacker (CEH) v13 (312-50v13) 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. **What is the role of anti-virus software in maintaining a Vulnerability Management Program?**

   A. To regularly update and protect systems from known vulnerabilities.

   B. To monitor network performance.

   C. To enforce password policies.

   D. To log all user activity.

2. **Host-based application firewalls are commonly used together with what security mechanism?**

   A. IDS alone

   B. Packet filter

   C. VPN gateway

   D. Antivirus signature only

3. **In cybersecurity, enumeration refers to which activity?**

   A. Scanning network ranges for open ports.

   B. The process of extracting information about a target system or network.

   C. Encrypting communications for secure transmission.

   D. Performing vulnerability scanning.

4. **How does the probability of an event occurring relate to the Annual Rate of Occurrence (ARO)?**

   A. ARO represents the likelihood of an event happening within a year.

   B. ARO is the annual cost of risk.

   C. ARO indicates the severity of the asset loss.

   D. ARO measures asset value.

5. **What is the role of transport layer port numbers in firewall checks?**

   A. They help determine which packets are allowed or denied access to the network

   B. They encrypt data

   C. They define user permissions

   D. They identify IP addresses.

6. What does a vulnerability scan help identify in a system?

A. Potential security weaknesses that could be exploited.

B. Data encryption keys

C. Real-time traffic anomalies

D. User authentication failures

7. What is the known plaintext attack against DES that suggests using two keys is no more secure than one?

A. Meet-in-the-middle attack.

B. Brute-force attack.

C. Differential cryptanalysis.

D. Side-channel attack.

8. What is the purpose of filtering ports 137 and 139?

A. To prevent unauthorized null sessions on the network

B. To allow SMB to function unimpeded

C. To block web traffic

D. To enable remote desktop

9. What is the main purpose of a vulnerability scanner?

A. To maintain hardware inventory

B. To identify security weaknesses in a system or network

C. To monitor user activity

D. To log network traffic

10. What is the risk of using higher timing values (-T) in Nmap scans?

A. Higher -T values increase speed but sacrifice stealth.

B. Higher -T values decrease speed but improve stealth.

C. They block the scan entirely.

D. They make scans completely stealthy.

Answers

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

Explanations

1. What is the role of anti-virus software in maintaining a Vulnerability Management Program?

A. To regularly update and protect systems from known vulnerabilities.

B. To monitor network performance.

C. To enforce password policies.

D. To log all user activity.

The main idea here is that antivirus software helps reduce risk from known vulnerabilities by staying current with threat definitions and blocking malware that tries to exploit those weaknesses. When antivirus definitions are regularly updated, the program can recognize and stop already-known malware strains that target weaknesses in the system or applications. This keeps systems safer while patches and other mitigations are being applied, because it prevents the malware from succeeding even if a vulnerability exists. In practice, antivirus acts as a protective layer that prevents exploitation of vulnerabilities by malicious code, complements patch management, and provides quarantine and remediation of infected files. It's not primarily about monitoring network performance, enforcing password policies, or logging all user activity, which are handled by other controls and tools.

2. Host-based application firewalls are commonly used together with what security mechanism?

A. IDS alone

B. Packet filter

C. VPN gateway

D. Antivirus signature only

Host-based application firewalls focus on controlling how individual applications on a host communicate over the network, enforcing rules at the application level. They are most effective when paired with a packet-filtering mechanism that operates at the network/transport layer, which blocks unwanted traffic before it even reaches the host. This combination provides defense in depth: the network filter catches broad, preemptive blocks, while the host-based firewall enforces stricter, application-specific policies on that machine, reducing the risk from traffic that slips past the network filter or targets particular apps. Other options don't fit as well because an IDS is for detection rather than blocking traffic on the host, a VPN gateway handles remote access, and antivirus signatures protect against malware rather than govern network traffic at the application level.

3. In cybersecurity, enumeration refers to which activity?

A. Scanning network ranges for open ports.

B. The process of extracting information about a target system or network.

C. Encrypting communications for secure transmission.

D. Performing vulnerability scanning.

The asked concept is about extracting information from a target. Enumeration is the phase where you gather detailed data from a system or network after initial discovery. It goes beyond simply seeing that something exists; it digs into what the system is, what it runs, and who can access it. In practice, enumeration pulls out specifics like user accounts and group memberships, computer names, network shares, service versions, OS details, and authentication methods. For example, you might query a Windows system to enumerate users, groups, and available shares, or query directory services and SNMP to learn about devices, accounts, and configurations. This focused information gathering helps map the target's potential attack surface and plan follow-on steps. This is distinct from port scanning, which only identifies open ports; vulnerability scanning, which looks for known weaknesses; and encryption, which protects data in transit. Enumeration's purpose is to reveal actionable details about the target's structure and resources.

4. How does the probability of an event occurring relate to the Annual Rate of Occurrence (ARO)?

A. ARO represents the likelihood of an event happening within a year.

B. ARO is the annual cost of risk.

C. ARO indicates the severity of the asset loss.

D. ARO measures asset value.

Understanding how often a risk event is expected to occur in a year is the key idea here. The Annual Rate of Occurrence (ARO) is the expected number of times a specific incident happens within one year. It's a measure of frequency or probability per year, not a dollar amount or a measure of loss severity. In risk calculations, you combine ARO with the loss you incur per incident (the single loss expectancy, SLE) to get the annual loss expectancy (ALE). So, knowing the ARO tells you how often to expect the event within a year, which is why it's the best fit for describing probability/frequency in this context. It isn't the annual cost (that's ALE), the severity of a loss per incident (that's SLE), or asset value. For example, if you expect 0.5 incidents per year and each incident costs $100,000, the ALE would be 0.5 × 100,000 = $50,000 per year.

5. What is the role of transport layer port numbers in firewall checks?

A. They help determine which packets are allowed or denied access to the network

B. They encrypt data

C. They define user permissions

D. They identify IP addresses.

Port numbers at the transport layer identify which service or application a packet is intended for on the destination host. Firewalls use these numbers to decide whether to allow or block traffic based on the service being accessed. For example, traffic targeting well-known ports like 80 (HTTP) or 443 (HTTPS) is commonly permitted, while access to other ports may be denied. This role is distinct from encryption (which is about protecting data in transit) and from user permissions (which are about who is allowed to do what). IP addresses locate the endpoints, while port numbers point to the specific service on those endpoints. In practice, many firewalls also track connection state, using the combination of IPs and ports to manage and validate ongoing communications.

6. What does a vulnerability scan help identify in a system?

A. Potential security weaknesses that could be exploited.

B. Data encryption keys

C. Real-time traffic anomalies

D. User authentication failures

Vulnerability scanning targets the weaknesses in a system that could be exploited by attackers. It checks assets for known security gaps, missing patches, misconfigurations, default or weak credentials, and insecure services, producing a report that helps you prioritize remediation based on risk. It isn't about locating encryption keys, which are sensitive data, nor about spotting real-time traffic anomalies (that's the realm of anomaly detection or IDS), nor about pinpointing specific authentication failures. The focus is on identifying weaknesses that, if left unaddressed, could be exploited to breach the system.

7. What is the known plaintext attack against DES that suggests using two keys is no more secure than one?

A. Meet-in-the-middle attack.

B. Brute-force attack.

C. Differential cryptanalysis.

D. Side-channel attack.

This question tests the idea that simply applying DES twice with two keys doesn't necessarily give you double the security. In a known-plaintext meet-in-the-middle attack on double DES, you start with a known plaintext P and its ciphertext C = E_K2(E_K1(P)). You compute and store all values of E_K1(P) for every possible K1. Then you walk through all possible K2 by computing D_K2(C) and look for matches with the stored E_K1(P) values. A match reveals a candidate pair of keys (K1, K2). The work factor ends up around 2^57, not 2^112, showing that two-key DES doesn't provide the expected security boost over single DES. That's why this option is the best answer: it's a specific known-plaintext attack that demonstrates the limited security gain from using two DES keys. The other choices describe different attack categories that don't capture the phenomenon in question—brute-force is a generic exhaustive search, differential cryptanalysis is a cryptanalytic technique, and a side-channel attack exploits physical leakage.

8. What is the purpose of filtering ports 137 and 139?

A. To prevent unauthorized null sessions on the network

B. To allow SMB to function unimpeded

C. To block web traffic

D. To enable remote desktop

NetBIOS over TCP/IP uses ports 137 and 139 to support Windows network file sharing and name resolution. If these ports are open, an attacker can establish null sessions—anonymous connections to a Windows host that allow enumeration of usernames, shares, and other information. Filtering these ports blocks those unauthenticated connections, reducing the risk of information disclosure and reconnaissance. This is why the best answer is to prevent unauthorized null sessions on the network. Web traffic and remote desktop use different ports (like 80/443 for web and 3389 for RDP), so blocking 137 and 139 specifically targets the SMB/NetBIOS exposure.

9. What is the main purpose of a vulnerability scanner?

A. To maintain hardware inventory

B. To identify security weaknesses in a system or network

C. To monitor user activity

D. To log network traffic

A vulnerability scanner's main purpose is to automatically identify security weaknesses in a system or network by scanning hosts, services, and applications against databases of known vulnerabilities, misconfigurations, and missing patches. This produces a report that helps prioritize remediation based on severity, so you can reduce risk before attackers exploit flaws. It isn't about maintaining hardware inventory (asset management), monitoring user activity (user behavior auditing), or logging network traffic (traffic capture or IDS/IPS functions).

10. What is the risk of using higher timing values (-T) in Nmap scans?

A. Higher -T values increase speed but sacrifice stealth.

B. Higher -T values decrease speed but improve stealth.

C. They block the scan entirely.

D. They make scans completely stealthy.

Raising the timing value in Nmap speeds up the probe rate. Higher timing templates push probes out faster, reduce the idle wait between steps, and increase parallelism. That speed comes at a cost: the scan becomes louder on the network, making it more likely to be noticed by IDS/IPS, firewalls, or admins, and it can trigger rate limiting or blocking. So you gain speed but sacrifice stealth. The other options aren't correct because higher timing doesn't block scans entirely, nor does it make scans completely stealthy; it actually reduces stealth by increasing detectability.

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!