CERTIFIED ETHICAL HACKER CERTIFICATION (CEHV10) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cehv10.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. **Which of the following is a method attackers may use to collect IVs for breaking WEP encryption?**

   A. Running a full system antivirus scan

   B. Listening to network traffic and injecting packets

   C. Updating the firewall settings

   D. Performing regular software updates

2. **What type of privilege escalation involves acquiring privileges of the same level?**

   A. Vertical privilege escalation

   B. Horizontal privilege escalation

   C. Denial of service attack

   D. Privilege misconfiguration

3. **In the realm of hacking, the decision to pursue a target often relies on what criteria?**

   A. Social influence among peers

   B. Technical skills of the hacker

   C. Accessibility and value of the target

   D. Legal implications of hacking

4. **During which phase do hackers attempt to hide their activities on the system?**

   A. The initial access phase

   B. The exploitation phase

   C. The clearing tracks phase

   D. The escalation of privileges phase

5. **What does passive sniffing allow attackers to do in a network using hubs?**

   A. Manipulate packet headers

   B. Capture all traffic passing through the network

   C. Access secured files remotely

   D. Perform DDoS attacks

SAMPLE

6. What role do network diagrams play in cybersecurity?

A. They help in setting up a new network

B. They provide a visual representation of operational policies

C. They help illustrate network architecture for better vulnerability assessments

D. They are used exclusively for compliance audits

7. Which of the following best differentiates between a security audit and penetration testing?

A. Security audit focuses solely on finding vulnerabilities

B. A security audit tests against specific guidelines

C. Penetration testing only identifies security policies

D. Audit checks the adherence to standards only

8. What is the primary cause of insider threats within an organization?

A. Inexperienced management

B. Malicious external hackers

C. Careless or dissatisfied employees

D. Poor organizational structure

9. What is the purpose of a vulnerability assessment?

A. To enforce stricter security policies

B. To improve employee training

C. To identify potential vulnerabilities

D. To launch an aggressive attack

10. What defines an integrity attack in a wireless network?

A. Sending encrypted data packets

B. Sending forged frames to perform different attacks

C. Blocking legitimate traffic

D. Capturing sensitive credentials

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which of the following is a method attackers may use to collect IVs for breaking WEP encryption?

A. Running a full system antivirus scan

B. Listening to network traffic and injecting packets

C. Updating the firewall settings

D. Performing regular software updates

Listening to network traffic and injecting packets is a common method attackers use to collect Initialization Vectors (IVs) for breaking WEP encryption. In WEP (Wired Equivalent Privacy), security relies on the secrecy of the encryption key, which is derived from these IVs. When the WEP protocol is used, IVs are often sent in plaintext and can be captured by anyone monitoring the network traffic. Attackers can actively engage with the network by injecting specially crafted packets. This action increases the chance of generating more unique IVs as a result of repeated packet transmission. Over time, with enough captured IVs, an attacker can use statistical methods or tools like Aircrack-ng to derive the WEP key, thus breaking the encryption. The other options do not pertain to the process of collecting IVs for WEP encryption cracking. Running a full system antivirus scan, updating firewall settings, and performing regular software updates are all security best practices aimed at protecting a system from malicious activity, but they do not directly contribute to the collection of IVs or the compromise of WEP encryption.

2. What type of privilege escalation involves acquiring privileges of the same level?

A. Vertical privilege escalation

B. Horizontal privilege escalation

C. Denial of service attack

D. Privilege misconfiguration

Horizontal privilege escalation involves acquiring privileges of the same level, which typically means that a user gains access to accounts or resources that they normally shouldn't be able to access, without changing their own privilege level. In this scenario, a user may exploit a vulnerability to access other users' data, files, or functionalities that are meant for other users with the same kind of permissions, rather than gaining higher privileges or access to restricted administrative functions. This concept is important in penetration testing and ethical hacking because it highlights the risks associated with user-level security controls. Effective security measures must ensure that users can only access their own data and that proper constraints are in place to prevent unauthorized access to other users' information. Other options, such as vertical privilege escalation, refer to gaining higher privileges (for example, a standard user gaining administrative rights), and a denial of service attack is focused on making systems unavailable rather than gaining privileges. Privilege misconfiguration often relates to improper settings that inadvertently grant excessive access, but it doesn't describe the action of one user accessing another user's same-level resources.

SAMPLE

3. In the realm of hacking, the decision to pursue a target often relies on what criteria?

A. Social influence among peers

B. Technical skills of the hacker

C. Accessibility and value of the target

D. Legal implications of hacking

The choice focusing on the accessibility and value of the target is essential in the decision-making process for hackers. Hackers often evaluate targets based on how easily they can be accessed, which includes considering the security measures in place, the potential vulnerabilities, and how likely they are to succeed in breaching those defenses. Additionally, the target's value—be it financial, strategic, or sensitive data—is crucial. A high-value target that is also easy to access presents an attractive opportunity, driving the decision to pursue that specific target. While other factors play a role, such as technical skills that could determine the feasibility of an attack or the legal implications that could deter some individuals, the core of this decision often revolves around whether a target is both accessible and holds significant value. This means that, practically speaking, the accessibility and value assessment often take precedence in targeting strategies among hackers.

4. During which phase do hackers attempt to hide their activities on the system?

A. The initial access phase

B. The exploitation phase

C. The clearing tracks phase

D. The escalation of privileges phase

The clearing tracks phase is the point in a hacking process where the intruder actively works to erase any sign of their presence or activities on the compromised system. This is critical for maintaining access to the target environment and evading detection by security teams. Hackers may delete logs, modify timestamps, and utilize various tools to obfuscate their actions, all aimed at reducing the likelihood of detection during and after the attack. In contrast, the initial access phase refers to the methods used by hackers to gain entry into a system, exploiting vulnerabilities or using social engineering techniques. The exploitation phase focuses on leveraging that initial access to execute malicious code or commands. The escalation of privileges phase involves gaining higher access levels to obtain more control over the system, but clearing tracks specifically pertains to the actions taken after having successfully infiltrated the system to cover one's traces.

SAMPLE

5. What does passive sniffing allow attackers to do in a network using hubs?

A. Manipulate packet headers

B. Capture all traffic passing through the network

C. Access secured files remotely

D. Perform DDoS attacks

Passive sniffing is a technique used by attackers to monitor and capture data packets traveling through a network. This method is particularly effective in networks that utilize hubs, as hubs broadcast incoming packets to all connected devices rather than directing traffic to specific endpoints. When an attacker employs passive sniffing in a hub-based network, they can intercept and capture all traffic that passes through the hub. This means that any unencrypted data, including sensitive information such as usernames, passwords, and other plaintext communications, can be collected and analyzed without altering the data or affecting the network's operation. The ability to capture all traffic is what makes passive sniffing a powerful tool for attackers, providing them with valuable insights into network activity without being detected. In contrast, manipulating packet headers or accessing secured files typically requires active involvement or different tactics that go beyond the scope of passive sniffing. Similarly, performing DDoS (Distributed Denial-of-Service) attacks involves overwhelming a target system, which is unrelated to the capabilities of passive sniffing.

6. What role do network diagrams play in cybersecurity?

A. They help in setting up a new network

B. They provide a visual representation of operational policies

C. They help illustrate network architecture for better vulnerability assessments

D. They are used exclusively for compliance audits

Network diagrams are crucial in cybersecurity as they offer a visual representation of the network architecture, which is essential for conducting effective vulnerability assessments. By illustrating how various components of a network connect and interact with each other—such as servers, devices, firewalls, and data paths—security professionals can identify potential weaknesses and vulnerabilities in the design or configuration of the network. This visual tool aids in understanding the flow of data, pinpointing areas of risk, and determining the impact of potential threats. It allows cybersecurity analysts to visualize the layout and communication paths, facilitating a more comprehensive risk analysis. By assessing these diagrams, security teams can prioritize vulnerabilities and develop strategies to mitigate risks effectively, enhancing the overall security posture of the organization. The other choices relate to aspects of network management or compliance, but do not specifically address the primary role of network diagrams in assisting with the identification and analysis of vulnerabilities.

SAMPLE

7. Which of the following best differentiates between a security audit and penetration testing?

A. Security audit focuses solely on finding vulnerabilities

B. A security audit tests against specific guidelines

C. Penetration testing only identifies security policies

D. Audit checks the adherence to standards only

The correct choice highlights that a security audit is conducted against specific guidelines. This means that during a security audit, an organization systematically evaluates its security policies, procedures, and controls to ensure compliance with established standards, regulations, or best practices. Audits often involve a comprehensive review of documentation, configurations, and security controls to assess whether they meet the defined benchmarks. In contrast, penetration testing is primarily focused on identifying vulnerabilities by simulating attacks on the system to determine how an attacker could exploit weaknesses. While both processes contribute to an organization's security posture, they serve distinct purposes: audits assess compliance and effectiveness of existing security measures, whereas penetration testing aims to discover security flaws through active exploitation. The other options fail to capture the essence of what differentiates these two concepts clearly. For instance, stating that a security audit focuses solely on finding vulnerabilities overlooks the broader compliance and procedural checks involved. Similarly, indicating that penetration testing only identifies security policies is misleading, as it involves testing the effectiveness of those policies through simulated attacks rather than merely identifying their existence. The notion that audits check adherence to standards only simplifies the process too much, as effective audits also evaluate risk management and overall security posture rather than just compliance with standards.

8. What is the primary cause of insider threats within an organization?

A. Inexperienced management

B. Malicious external hackers

C. Careless or dissatisfied employees

D. Poor organizational structure

The primary cause of insider threats within an organization stems from careless or dissatisfied employees. These individuals may inadvertently compromise security due to negligence, such as failing to follow security protocols or mishandling sensitive information. Moreover, employees experiencing dissatisfaction—whether from job dissatisfaction, personal issues, or perceived unfair treatment—might be more likely to engage in malicious behavior, possibly exploiting their access to data and systems for personal gain or to retaliate against the organization. While other options mention factors that can contribute to vulnerabilities in an organization, they do not directly represent the primary cause of insider threats. Inexperienced management may lead to poor security practices, but it is not solely responsible for insider threats. Malicious external hackers are distinctly separate from insider threats, as they are not internal to the organization. A poor organizational structure can create confusion and inefficiencies but doesn't directly contribute to threats posed by insiders. The behavior and attitudes of employees, particularly when they are careless or dissatisfied, are the core reasons behind a significant proportion of insider threats.

SAMPLE

9. What is the purpose of a vulnerability assessment?

A. To enforce stricter security policies

B. To improve employee training

C. To identify potential vulnerabilities

D. To launch an aggressive attack

The purpose of a vulnerability assessment is to identify potential vulnerabilities within a system, network, or application. This process involves systematically evaluating the environment to discover weaknesses that could be exploited by attackers. By identifying these vulnerabilities, organizations can prioritize them according to severity and risk, enabling the implementation of appropriate security measures to mitigate potential threats. A vulnerability assessment typically involves using automated tools and manual techniques to carry out scans, analyze the infrastructure, and produce reports detailing the findings. The ultimate goal is to proactively enhance security posture and protect sensitive data before any exploitation can occur. The other choices, while related to broader security practices, do not directly capture the primary objective of a vulnerability assessment. Enforcing stricter security policies and improving employee training can be outcomes of a vulnerability assessment, but they do not describe the assessment's core function itself. Launching an aggressive attack is contrary to the ethical guidelines that govern vulnerability assessments.

10. What defines an integrity attack in a wireless network?

A. Sending encrypted data packets

B. Sending forged frames to perform different attacks

C. Blocking legitimate traffic

D. Capturing sensitive credentials

An integrity attack in a wireless network typically involves actions that compromise the integrity of data being transmitted. Sending forged frames is a prime example of this type of attack. By manipulating or crafting data packets to appear as if they are originating from a legitimate source, an attacker can disrupt the communication process, inject false information, or manipulate the intended outcome of the communication. This undermines the trustworthiness and accuracy of the data within the network, which is central to an integrity attack. In contrast, other options such as sending encrypted data packets relate more to confidentiality rather than integrity. Blocking legitimate traffic can lead to denial-of-service situations, which disrupts accessibility rather than altering data integrity. Capturing sensitive credentials is focused on confidentiality and data theft, rather than integrity issues—although capturing credentials can lead to other integrity-related attacks, they are not integrity attacks themselves. Thus, sending forged frames directly relates to the concept of altering data integrity, making it the correct choice.

SAMPLE

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://cehv10.examzify.com

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

SAMPLE