CERTIFIED ETHICAL HACKER (CEHV13) MODULE 1 PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cehv13mod1.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. What does PCI DSS stand for?

A. Payment Confidence Information Data Standards
B. Payment Card Industry Data Security Standard
C. Payment Control Information Data Security
D. Payment Compliance and Integration Data Standards

2. What action is taken during the Clearing Tracks phase?

A. Installing malware
B. Erasing evidence of a breach
C. Gaining administrator privileges
D. Analyzing vulnerabilities

3. What is the role of integrity in information security?

A. To ensure systems are always available
B. To verify that data remains unaltered
C. To keep data confidential
D. To enable easy access to information

4. Which of the following is NOT a category of Information Warfare?

A. Command and Control Warfare
B. Cyberwarfare
C. Social Warfare
D. Electronic Warfare

5. What are 'AI Tools' in the context of ethical hacking used for?

A. To automate and provide insights for ethical hackers
B. To strictly deter cyber threats
C. To monitor networks without user input
D. To solely protect against unauthorized access

6. What does the term "scalability" refer to in the context of AI in hacking?

A. The ability to execute tasks at a faster rate
B. The capability to grow and handle increased loads
C. The efficiency of real-time data transmission
D. The reduction of hardware costs

SAMPLE

7. In the context of cybersecurity, what function does threat detection serve?

A. It identifies potential risks and vulnerabilities
B. It focuses solely on access controls
C. It promotes software development
D. It analyzes market trends

8. Which of the following describes ISO/IEC 27036-3:2023?

A. Guidelines for securing hardware and software
B. Technical guidelines for data encryption
C. Report on internet security trends
D. Standards for corporate financial disclosures

9. What is a key activity involved in the Gaining Access phase?

A. Erasing evidence of a breach
B. Obtaining access to an OS or application
C. Escalating privileges
D. Analyzing existing vulnerabilities

10. PentestGPT assists which group of professionals?

A. Bug bounty hunters
B. Security managers
C. Penetration testers
D. AI developers

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What does PCI DSS stand for?

A. Payment Confidence Information Data Standards

B. Payment Card Industry Data Security Standard

C. Payment Control Information Data Security

D. Payment Compliance and Integration Data Standards

The correct answer is the Payment Card Industry Data Security Standard. PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. It focuses on protecting cardholder data and minimizing payment card fraud. This standard is critical for any entity that handles credit card transactions, as it lays out requirements for security management, policies, and procedures to protect sensitive information from breaches. Compliance with PCI DSS is not only essential for the protection of customer data but also helps businesses avoid potential financial penalties and loss of customer trust. The other options do not accurately reflect the established term or its purpose. They may seem plausible at first glance but fail to describe the recognized standards set by the payment card industry that ensure the protection of cardholder data effectively.

2. What action is taken during the Clearing Tracks phase?

A. Installing malware

B. Erasing evidence of a breach

C. Gaining administrator privileges

D. Analyzing vulnerabilities

During the Clearing Tracks phase, the primary action involves erasing evidence of a breach. This phase is critical for an attacker attempting to cover their tracks after successfully infiltrating a system or network. By erasing evidence, the attacker aims to avoid detection and make it more difficult for security personnel to understand how the breach occurred, who was involved, and what data may have been compromised. This action includes activities such as deleting logs, tampering with timestamps, and covering any changes made during the breach. Successfully clearing tracks allows the attacker to maintain persistence within the network without being discovered, enabling further exploitation or data exfiltration. While installing malware, gaining administrator privileges, or analyzing vulnerabilities are important actions in the broader context of cyber attacks and security assessments, they don't directly pertain to the specific tasks associated with the Clearing Tracks phase. These actions relate more to initial exploitation, privilege escalation, and assessing the security posture of the system, rather than the concealment of an already executed breach.

SAMPLE

3. What is the role of integrity in information security?

A. To ensure systems are always available

B. To verify that data remains unaltered

C. To keep data confidential

D. To enable easy access to information

Integrity in information security refers to the assurance that data remains accurate, consistent, and unaltered throughout its lifecycle. This is essential to prevent unauthorized modifications that could compromise the reliability of information. When data integrity is upheld, users can trust that the information they are analyzing or relying upon has not been tampered with or corrupted, whether intentionally or unintentionally. In an environment where data is constantly being created, transmitted, and stored, mechanisms like checksums, hashes, and digital signatures are implemented to ensure that any changes to data are detectable. Maintaining data integrity protects against threats such as data breaches, malware attacks, or human error, thus ensuring that organizations can operate based on trustworthy information. The other choices reflect important elements of information security but do not pertain specifically to the role of integrity. System availability relates more to the resilience and uptime of systems, confidentiality focuses on limiting access to data, and ease of access pertains to usability and user experience. All of these aspects are vital to information security overall, but integrity specifically zeroes in on the correctness and trustworthiness of data.

4. Which of the following is NOT a category of Information Warfare?

A. Command and Control Warfare

B. Cyberwarfare

C. Social Warfare

D. Electronic Warfare

The answer is rooted in the established categories of information warfare, which include Command and Control Warfare, Cyberwarfare, and Electronic Warfare. These categories encompass various techniques and strategies used in military and strategic contexts to gain advantages over opponents through information manipulation, cyber operations, and control of electronic assets. Command and Control Warfare focuses on disrupting the enemy's command and control capabilities, impairing their decision-making processes. Cyberwarfare refers to the strategic use of digital attacks against an adversary to damage, disrupt, or disable their networks and systems. Electronic Warfare involves the use of electromagnetic energy to control the electromagnetic spectrum, attacking or defending against enemy electronic systems. While "Social Warfare" may pertain to the manipulation of social dynamics and public opinion, it is not formally recognized as a distinct category of information warfare in the same structured way that the others are. This distinction emphasizes the established and recognized categories in the context of military doctrine and strategic operations, making it clear why it is considered the outlier in this list.

SAMPLE

5. What are 'AI Tools' in the context of ethical hacking used for?

A. To automate and provide insights for ethical hackers

B. To strictly deter cyber threats

C. To monitor networks without user input

D. To solely protect against unauthorized access

The context of 'AI Tools' in ethical hacking primarily focuses on their ability to automate processes and provide critical insights for ethical hackers. These tools leverage artificial intelligence to analyze vast amounts of data, identify patterns, and predict potential vulnerabilities that may not be evident through manual analysis alone. By automating repetitive tasks, AI tools allow ethical hackers to concentrate on more complex and strategic elements of their assessments, enhancing efficiency and effectiveness in identifying and addressing security risks. While options discussing deterrence, monitoring, or protection may appear relevant to cybersecurity, they do not encapsulate the comprehensive utility of AI tools within ethical hacking. AI tools are not solely designed to deter threats or provide passive monitoring; instead, their core function is to assist in proactive identification and mitigation of vulnerabilities, thus empowering ethical hackers to bolster defenses effectively.

6. What does the term "scalability" refer to in the context of AI in hacking?

A. The ability to execute tasks at a faster rate

B. The capability to grow and handle increased loads

C. The efficiency of real-time data transmission

D. The reduction of hardware costs

In the context of AI in hacking, "scalability" refers to the system's capability to grow and manage increased loads effectively. This means that as the demand for processing power, data handling, or the complexity of tasks increases, the AI system can accommodate this growth without a significant drop in performance. Scalability encompasses not only the ability to increase capacity by adding resources but also the way a system can adapt to handle more data, users, or more complex operations efficiently. This is particularly important in cybersecurity and ethical hacking, as threats can evolve and require more resources to analyze and mitigate. A scalable AI system can adjust to handle these changes seamlessly, ensuring that security measures are maintained even as the volume of data and the complexity of tasks increase.

7. In the context of cybersecurity, what function does threat detection serve?

A. It identifies potential risks and vulnerabilities

B. It focuses solely on access controls

C. It promotes software development

D. It analyzes market trends

Threat detection plays a crucial role in cybersecurity by identifying potential risks and vulnerabilities within a system or network. This process involves monitoring systems for signs of malicious activity or weaknesses that could be exploited by attackers. By detecting threats, organizations can take proactive measures to mitigate risks, enhance their overall security posture, and protect sensitive data from breaches. The key aspect of threat detection is its ability to recognize not only existing vulnerabilities but also emerging threats that may not yet have been addressed by conventional security measures. This aspect allows cybersecurity professionals to respond effectively, ensuring that systems are resilient against evolving cyber threats. The other options, while they touch on important areas related to cybersecurity and technology, do not pertain directly to the specific function of threat detection. Access controls are critical but focus mainly on preventing unauthorized access, rather than detecting threats. Similarly, promoting software development and analyzing market trends, while valuable in their own rights, do not directly contribute to identifying or managing threats within the cybersecurity landscape.

SAMPLE

8. Which of the following describes ISO/IEC 27036-3:2023?

A. Guidelines for securing hardware and software

B. Technical guidelines for data encryption

C. Report on internet security trends

D. Standards for corporate financial disclosures

The correct description of ISO/IEC 27036-3:2023 is that it provides guidelines for securing hardware and software within the realm of information security. This standard is part of the larger ISO/IEC 27036 series, which focuses on information security for supplier relationships. Specifically, part 3 addresses "Information security in supplier relationships," offering guidelines on how organizations should manage security risks associated with third-party providers, including the protection of hardware and software systems. The emphasis is on establishing a framework to mitigate risks to information security that may arise in supplier relationships. Options that discuss data encryption, internet security trends, or corporate financial disclosures do not align with the primary focus of ISO/IEC 27036-3:2023, as this standard is not directly concerned with those topics. Thus, the emphasis on securing hardware and software in the context of supplier relationships distinctly highlights why this understanding is critical in adhering to effective information security practices.

9. What is a key activity involved in the Gaining Access phase?

A. Erasing evidence of a breach

B. Obtaining access to an OS or application

C. Escalating privileges

D. Analyzing existing vulnerabilities

The Gaining Access phase is crucial in the ethical hacking process, as it directly involves successfully breaching a target's defenses to gain control over a system, application, or network. This phase marks the transition from preparation and planning to active exploitation, where the attacker uses various methods, such as exploiting vulnerabilities, leveraging social engineering techniques, or employing password attacks, to obtain access to operating systems or applications. Once access is obtained, further actions can be taken, such as gathering information or moving laterally within the network. Therefore, obtaining access to an operating system or application is considered a foundational step in this phase. This is essential not only for ethical hackers who are performing penetration tests but also for malicious actors during a cyber attack. The other choices, while part of the overall ethical hacking process, do not align with the primary focus of the Gaining Access phase. Erasing evidence of a breach falls under actions taken after gaining access, while escalating privileges refers to actions that can happen after access has already been obtained. Analyzing existing vulnerabilities is a preparatory step that occurs prior to gaining access, focusing on identifying weaknesses without having yet attempted to exploit them.

SAMPLE

10. PentestGPT assists which group of professionals?

A. Bug bounty hunters

B. Security managers

C. Penetration testers

D. AI developers

PentestGPT is specifically designed to assist penetration testers, who are professionals engaged in testing the security of systems, networks, and applications. These testers mimic the actions of malicious hackers but do so in a legal and ethical manner to uncover vulnerabilities that could be exploited. By employing tools like PentestGPT, penetration testers can streamline and enhance their processes, making it easier to identify and address security weaknesses. While bug bounty hunters, security managers, and AI developers relate to cybersecurity and technology, they have different core responsibilities that do not align with the primary function of PentestGPT. Bug bounty hunters focus on finding vulnerabilities in systems and are often rewarded for their discoveries, but they operate outside of a formal engagement with organizations. Security managers oversee security protocols and policies within an organization, directing rather than executing technical testing. AI developers focus on creating and improving AI systems, which is outside the realm of penetration testing. Therefore, the primary audience for PentestGPT's capabilities is indeed penetration testers.

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://cehv13mod1.examzify.com

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

SAMPLE