Certified Ethical Hacker (CEHv13) Module 1 Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. For the full version with hundreds of questions, visit: https://cehv13mod1.examzify.com

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

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 key function of CyberGPT?

   A. Facilitating ethical hacking training

   B. Enhancing determination of bugs

   C. Improving overall security operations

   D. Creating secure AI systems

2. What does availability in information security ensure?

   A. Data can be accessed by anyone at any time

   B. Authorized users can access systems when needed

   C. Data integrity is preserved

   D. Access is restricted to sensitive information

3. What is the role of blue hat hackers?

   A. Permanent employees testing systems

   B. Temporary security professionals testing before product releases

   C. Corporate spies

   D. Extremists promoting causes

4. Which of the following is a method by which a passive attack operates?

   A. Interacting with the target system

   B. Exploiting vulnerabilities through user interaction

   C. Monitoring data transmissions without altering them

   D. Gaining physical access to the system

5. What is the fundamental action of hacking?

   A. Securing a network against attacks

   B. Exploiting vulnerabilities to gain unauthorized access

   C. Monitoring network traffic for threats

   D. Conducting security assessments

6. **What is the consequence of a breach of integrity in information security?**

   - **A. Unauthorized access**
   - **B. Compromised data trustworthiness**
   - **C. Loss of confidentiality**
   - **D. Increased availability issues**

7. **Which component is NOT part of the Cyber Kill Chain Methodology?**

   - **A. Delivery**
   - **B. Weaponization**
   - **C. Monitoring**
   - **D. Exploitation**

8. **The motive behind a hacking attack usually stems from?**

   - **A. A requirement to learn new programming languages**
   - **B. The notion that valuable items are stored in a target system**
   - **C. A desire to improve one’s coding skills**
   - **D. The need to teach others about cybersecurity**

9. **What is the primary goal of the Maintaining Access phase?**

   - **A. To analyze the vulnerabilities**
   - **B. To erase evidence of compromise**
   - **C. To retain control of the compromised system**
   - **D. To exploit vulnerabilities**

10. **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**

Answers

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

Explanations

1. What is the key function of CyberGPT?

- A. Facilitating ethical hacking training
- B. Enhancing determination of bugs
- C. Improving overall security operations
- D. Creating secure AI systems

The key function of CyberGPT revolves around improving overall security operations. This involves utilizing advanced AI capabilities to analyze vast amounts of data related to cybersecurity threats and vulnerabilities. By enhancing security operations, CyberGPT can assist organizations in better identifying, responding to, and mitigating potential threats. The integration of AI in security operations allows for a more proactive approach, enabling quicker detection of anomalies and automating certain security processes, thus improving efficiency. By streamlining security measures and operations, organizations can create a more robust defense against cyber threats. While other options may address important aspects of cybersecurity—like training or bug determination—they do not encapsulate the primary function of CyberGPT, which focuses on the overarching enhancement of security operations through artificial intelligence and data analytics.

2. What does availability in information security ensure?

- A. Data can be accessed by anyone at any time
- B. Authorized users can access systems when needed
- C. Data integrity is preserved
- D. Access is restricted to sensitive information

Availability in information security primarily ensures that authorized users have access to systems and data when they need it. This principle is crucial for maintaining operational efficiency and effective communication within an organization. If systems and data are not available, it can lead to significant disruptions, affecting productivity and ultimately impacting the organization's bottom line. The focus on authorized users means that while availability is important, it recognizes the need for control mechanisms and access restrictions to mitigate risks. This distinction is significant because it does not imply unrestricted access for all, but rather ensures that those who are permitted can retrieve and utilize the necessary information promptly. Availability is one of the core pillars of the CIA triad (Confidentiality, Integrity, and Availability) in information security, and it complements confidentiality and integrity by ensuring that systems remain functional and supportive of the organization's operations.

3. What is the role of blue hat hackers?

A. Permanent employees testing systems

B. Temporary security professionals testing before product releases

C. Corporate spies

D. Extremists promoting causes

Blue hat hackers primarily serve as temporary security professionals who focus on testing systems and applications before product releases. Their role is crucial in ensuring that new software is secure and does not contain vulnerabilities that could be exploited by malicious actors once it is launched. This type of testing is often conducted in a collaborative environment, where blue hats work closely with developers to identify and rectify potential security flaws during the development phase, rather than after a product has already hit the market. By integrating security testing into the development lifecycle, blue hat hackers help organizations ensure a higher standard of security and minimize risks associated with software vulnerabilities. Their contributions are essential for enhancing the overall reliability and safety of technology products, ultimately providing peace of mind for both the developers and the end-users. The focus on testing before product releases distinguishes blue hat hackers from other types of hackers, such as those who may be involved in corporate espionage or other malicious activities, which are not aligned with the objectives of blue hat work.

4. Which of the following is a method by which a passive attack operates?

A. Interacting with the target system

B. Exploiting vulnerabilities through user interaction

C. Monitoring data transmissions without altering them

D. Gaining physical access to the system

A passive attack typically involves the monitoring of data transmissions without making any alterations to the data being sent. The primary goal of such attacks is to gather information without being detected. This contrasts with active attacks, where an attacker tries to manipulate or alter the data. In passive attacks, the attacker may intercept communications, eavesdrop on network traffic, or capture data packets. Since there’s no interaction with the target system or alteration of the data, the attack remains undetected, allowing the attacker to collect valuable information, such as credentials or sensitive data. The other methods listed — interacting with the target system, exploiting vulnerabilities through user interaction, and gaining physical access to the system — all imply some level of active engagement or influence over the target, distinguishing them from the largely non-invasive nature of passive attacks. In active engagements, the attacker modifies the state or behaviour of the target, which is not characteristic of passive strategies.

5. What is the fundamental action of hacking?

A. Securing a network against attacks

B. Exploiting vulnerabilities to gain unauthorized access

C. Monitoring network traffic for threats

D. Conducting security assessments

The fundamental action of hacking revolves around the concept of exploiting vulnerabilities to gain unauthorized access to systems, networks, or data. This core activity is at the heart of what defines hacking in both ethical and unethical contexts. Ethical hackers, or penetration testers, engage in this practice to identify and assess vulnerabilities in a system with the intent of improving security measures. While securing a network, monitoring traffic, and conducting security assessments are all critical activities within the broader field of cybersecurity, they serve different purposes and are not the defining action that characterizes hacking itself. Securing a network focuses on proactive measures to prevent unauthorized access, monitoring traffic is about detecting potential threats, and conducting security assessments aims at evaluating the overall security posture of a system. In contrast, the act of exploiting vulnerabilities emphasizes the use of knowledge and techniques to bypass security mechanisms, which is a fundamental skill that underpins both attacking and defending in the realm of cybersecurity. Understanding this primary action helps differentiate the roles of hackers and highlights the ongoing need for vigilance in securing information systems against such exploits.

6. What is the consequence of a breach of integrity in information security?

A. Unauthorized access

B. Compromised data trustworthiness

C. Loss of confidentiality

D. Increased availability issues

A breach of integrity in information security primarily results in compromised data trustworthiness. Integrity ensures that data remains accurate, reliable, and unaltered by unauthorized individuals. When integrity is breached, it indicates that the information may have been modified or tampered with, leading to discrepancies that can misinform decisions and damage the credibility of the data. This undermines the overall trust in the system and the information it holds. While unauthorized access can be a factor in integrity breaches, it more directly pertains to confidentiality rather than integrity itself. Similarly, while issues of availability may arise due to other factors, they are not directly indicative of a breach of integrity. Loss of confidentiality refers to unauthorized access to sensitive information, unrelated to the integrity of that information. Conversely, when data integrity is lost, the trustworthiness of the data is fundamentally compromised, making it the most relevant consequence.

7. Which component is NOT part of the Cyber Kill Chain Methodology?

A. Delivery

B. Weaponization

C. Monitoring

D. Exploitation

The Cyber Kill Chain Methodology, developed by Lockheed Martin, outlines the stages of a cyber attack from the initial reconnaissance to the final objective of the attack. Each stage is designed to provide security professionals with a framework to identify and disrupt malicious activities at various points in the attack cycle. The stages defined in the Cyber Kill Chain include: 1. **Reconnaissance: The attacker gathers information about the target. 2. **Weaponization**: The attacker creates a deliverable payload, like a virus, coupled with an exploit. 3. **Delivery**: The attacker transmits the weapon to the target. 4. **Exploitation**: The attacker exploits the vulnerability to execute malicious code on the target's system. 5. **Installation**: The attacker installs malware on the target system. 6. **Command and Control (C2)**: The attacker establishes a communication channel with the compromised system. 7. **Actions on Objectives**: The attacker performs their intended action, such as data theft or system disruption. Monitoring, while it is a crucial component of a security strategy and aids in detecting and responding to threats, is not one of the defined stages within the Cyber Kill Chain. It is more of a continuous activity that supports overall security**

8. The motive behind a hacking attack usually stems from?

A. A requirement to learn new programming languages

B. The notion that valuable items are stored in a target system

C. A desire to improve one's coding skills

D. The need to teach others about cybersecurity

The motive behind a hacking attack often arises from the belief that valuable items are stored within the target system. This could include sensitive data, financial information, intellectual property, or various forms of digital assets that hold monetary or strategic value. Attackers typically choose targets based on the potential rewards that can be gained, such as stealing personal information for identity theft, accessing proprietary data for competitive advantage, or even disrupting systems for ransom. Understanding this motive is crucial for cybersecurity professionals as it informs their strategies for protecting information and systems against such threats. The other options, while they may reflect personal interests or goals in a different context, do not directly address the common motivations that drive individuals to engage in hacking activities.

9. What is the primary goal of the Maintaining Access phase?

A. To analyze the vulnerabilities

B. To erase evidence of compromise

C. To retain control of the compromised system

D. To exploit vulnerabilities

The primary goal of the Maintaining Access phase is to retain control of the compromised system. After successfully exploiting a system and gaining access, an ethical hacker or security professional aims to ensure that they can continue to exploit that access in the future. This might involve installing backdoors, creating user accounts, or implementing other methods that allow them to return to the system without needing to go through the initial exploitation process again. Maintaining access is critical for both ethical hackers, who need to ensure they can provide ongoing support or recommendations for security improvements, as well as for malicious actors who seek to exploit systems for nefarious purposes. The focus here is on ensuring ongoing control, which contrasts with other phases such as analysis or cleanup, which do not prioritize retention of access.

10. 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.

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!