Certified Ethical Hacker Certification (CEHv10) Practice Test (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 one of the main weaknesses of NetBIOS that hackers exploit?**

   A. It uses complex encryption

   B. It reveals too much system information

   C. It relies solely on passwords

   D. It is heavily regulated

2. **What is the goal of an Information Security Management Program?**

   A. To develop new technologies

   B. To facilitate secure organizational operations

   C. To prevent all cybersecurity attacks

   D. To create public awareness of security

3. **What makes passive sniffing effective in certain network environments?**

   A. It requires intervention from security officers

   B. It does not require sending data packets

   C. It is used for testing security protocols

   D. It manipulates data during transmission

4. **What is one consequence of a confidentiality attack?**

   A. Improved network security measures

   B. Disruption of communication protocols

   C. Unauthorized access to private information

   D. Decreased employee productivity

5. **What are the stages in the five stages of hacking?**

   A. Identification, Authentication, Authorization, Exploitation, Reporting

   B. Reconnaissance, Scanning, Gaining access, Maintaining access, Clearing tracks

   C. Network mapping, Credential harvesting, Privilege escalation, Data exfiltration

   D. Planning, Executing, Testing, Monitoring, Finishing

6. What does ICMP echo scanning accomplish?

A. It analyzes the data packets sent across a network

B. It determines which hosts are active in a target network

C. It sends alerts for unauthorized access attempts

D. It identifies firewall configurations in a network

7. Which type of backup restores the entire data set to its last full form?

A. Incremental backup

B. Differential backup

C. Full backup

D. Snapshot backup

8. What is the objective of a Denial of Service (DoS) attack?

A. To increase server performance

B. To render the target system useless

C. To transmit secure data

D. To authenticate users on the network

9. Which component is NOT part of a hardware keylogger?

A. PC/BIOS Embedded

B. Network-based logger

C. Keylogger keyboard

D. External keylogger

10. What type of attack is characterized by preventing legitimate users from accessing resources?

A. Data breach

B. Denial of Service

C. Session hijacking

D. Phishing

Answers

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

Explanations

1. What is one of the main weaknesses of NetBIOS that hackers exploit?

A. It uses complex encryption

B. It reveals too much system information

C. It relies solely on passwords

D. It is heavily regulated

One of the main weaknesses of NetBIOS that hackers exploit is that it reveals too much system information. NetBIOS, which stands for Network Basic Input/Output System, allows applications on different computers to communicate within a local network. However, it operates in an environment where it can expose critical information about the system, such as the computer name, user accounts, and the resources available on the network. This exposure can give attackers insight into the network's structure and valuable information that could be used to launch attacks, perform reconnaissance, or exploit other vulnerabilities. Since hackers can leverage this information to gain unauthorized access or escalate privileges, it makes NetBIOS a target for exploitation. The other options do not accurately reflect the vulnerabilities inherent to NetBIOS. For instance, it does not employ complex encryption methods; rather, it typically operates without encryption, making it easier for attackers to intercept data. Additionally, while it does use passwords for access control, this reliance alone does not encapsulate a significant weakness as many systems utilize password protection effectively. Lastly, regulations do not directly pertain to the weaknesses of NetBIOS, as the protocol's risks are tied to its design and implementation flaws rather than external regulatory conditions.

2. What is the goal of an Information Security Management Program?

A. To develop new technologies

B. To facilitate secure organizational operations

C. To prevent all cybersecurity attacks

D. To create public awareness of security

The goal of an Information Security Management Program is to facilitate secure organizational operations. This encompasses creating a framework that ensures the confidentiality, integrity, and availability of data within an organization. By doing so, it helps organizations manage security risks by employing a structured and proactive approach to information security. This involves implementing policies, procedures, and controls that safeguard information assets while supporting business needs and objectives. While developing new technologies can be a part of the broader security strategy, it is not the primary goal of an Information Security Management Program. The proactive application of technology is rather a means to achieve the goal of securing operations. Preventing all cybersecurity attacks, although a noble aspiration, is unrealistic; no system can be completely invulnerable. Instead, the focus is on risk management and strengthening defenses to minimize the occurrence and impact of security incidents. As for public awareness of security, while promoting security awareness is important, it is more of a supportive activity rather than the central goal of managing an organization's information security.

3. What makes passive sniffing effective in certain network environments?

A. It requires intervention from security officers

B. It does not require sending data packets

C. It is used for testing security protocols

D. It manipulates data during transmission

Passive sniffing is effective in certain network environments primarily because it does not require sending data packets. This means that a passive sniffer can monitor and capture data packets that are already being transmitted over the network without altering or interacting with the network traffic. In environments like switched networks where data is segregated, passive sniffing allows an attacker or security professional to analyze traffic without detection, as they are simply observing the data flows rather than injecting their own packets or commands into the network. In contrast, the other options don't accurately describe the nature or effectiveness of passive sniffing. For instance, requiring intervention from security officers would imply an active scenario wherein alerts could be triggered, potentially compromising the stealth aspect of passive sniffing. Similarly, using it for testing security protocols or manipulating data during transmission indicates an active engagement with the data flow, which contradicts the fundamental principle of passive sniffing that revolves around observation without interference.

4. What is one consequence of a confidentiality attack?

A. Improved network security measures

B. Disruption of communication protocols

C. Unauthorized access to private information

D. Decreased employee productivity

One consequence of a confidentiality attack is unauthorized access to private information. Such an attack typically targets sensitive data, where an attacker seeks to bypass security measures to gain information that is meant to be kept confidential, such as personal identification numbers, financial records, or proprietary business data. Once attackers successfully infiltrate a system, they can compromise privacy, leading to not only the exposure of sensitive data but also potential misuse of that information, resulting in identity theft, financial loss, or reputational damage to individuals or organizations. Although the other options mention possible effects related to security or productivity, they do not directly address the primary aim of a confidentiality attack, which is to access restricted data without permission.

5. What are the stages in the five stages of hacking?

A. Identification, Authentication, Authorization, Exploitation, Reporting

B. Reconnaissance, Scanning, Gaining access, Maintaining access, Clearing tracks

C. Network mapping, Credential harvesting, Privilege escalation, Data exfiltration

D. Planning, Executing, Testing, Monitoring, Finishing

The correct answer identifies a structured approach to ethical hacking that encompasses the various stages hackers typically follow during an attack. The stages of reconnaissance, scanning, gaining access, maintaining access, and clearing tracks represent a comprehensive methodology for understanding the attack process. Starting with reconnaissance, this initial phase involves gathering as much information as possible about the target system or network. This allows the ethical hacker to identify potential vulnerabilities that can be exploited later. The scanning phase follows, where the hacker actively probes the target to gather detailed data about the systems and services that are running. This can include discovering live hosts, open ports, and identifying available services that could be targeted. Next is the gaining access stage, where the ethical hacker uses the information collected to exploit identified vulnerabilities, gaining entry into the target system or network. This is the critical phase where the actual attack occurs. Once access is gained, maintaining access becomes important. In this stage, the hacker implements various methods to keep their presence in the system, which allows for ongoing access in the future if needed. Finally, clearing tracks involves removing any evidence of the attack, which is crucial for a real hacker to avoid detection. In ethical hacking practice, this is often about understanding how to protect against such actions, ensuring that the vulnerabilities

6. What does ICMP echo scanning accomplish?

A. It analyzes the data packets sent across a network

B. It determines which hosts are active in a target network

C. It sends alerts for unauthorized access attempts

D. It identifies firewall configurations in a network

ICMP echo scanning is a technique primarily used to ascertain the status of hosts within a target network. When an ICMP echo request (commonly known as a "ping") is sent to a host, if that host is active and configured to respond, it will send back an ICMP echo reply. This exchange enables the scanning tool or individual to discern which devices are currently online and responsive within the specified range of IP addresses. The value of this method lies in its simplicity and efficiency for checking the operational status of network devices without the need for complex configurations or invasive techniques. It essentially helps create an inventory of live hosts that can be further probed for additional services or vulnerabilities in subsequent steps of a security assessment. Other options do not accurately reflect the primary purpose of ICMP echo scanning. While analyzing data packets, alerting for unauthorized access, and identifying firewall configurations are important aspects of network security and management, they do not specifically relate to the core functionality of conducting ICMP echo requests.

7. Which type of backup restores the entire data set to its last full form?

A. Incremental backup

B. Differential backup

C. Full backup

D. Snapshot backup

The type of backup that restores the entire data set to its last full form is a full backup. This process involves creating a complete copy of all data files, configurations, and system information at a specific point in time. When a full backup is executed, it ensures that every aspect of the data is captured and can be restored in its entirety, without the need to reference any other backup sets. In contrast, an incremental backup captures only the data that has changed since the last backup (whether that last backup was a full backup or another incremental one) and requires previous backups to restore the entire dataset. A differential backup, while also focusing on changes, accumulates the changes since the last full backup, meaning it can grow larger over time and also requires the last full backup in the restoration process. A snapshot backup, on the other hand, takes a snapshot of the data at a specific moment but may not provide a complete backup suitable for full restoration depending on the system it supports. Ultimately, to restore an entire data set to its last full state seamlessly, a full backup is the appropriate choice.

8. What is the objective of a Denial of Service (DoS) attack?

A. To increase server performance

B. To render the target system useless

C. To transmit secure data

D. To authenticate users on the network

The objective of a Denial of Service (DoS) attack is to render the target system useless. In a DoS attack, the attacker aims to overwhelm a network, service, or system by flooding it with excessive requests or exploiting vulnerabilities, which ultimately leads to a slowdown or complete shutdown of the system. This disruption prevents legitimate users from accessing the targeted resources, thus achieving the primary goal of the attack. The other options focus on positive outcomes or processes unrelated to the malicious nature of a DoS attack. For instance, increasing server performance or transmitting secure data does not align with the intentions behind initiating a DoS attack, which is to disrupt rather than enhance functionality or security. Similarly, authenticating users relates to validating access rights rather than causing service interruptions. Therefore, the option that emphasizes incapacitating the target directly reflects the fundamental aim of a Denial of Service attack.

9. Which component is NOT part of a hardware keylogger?

A. PC/BIOS Embedded

B. Network-based logger

C. Keylogger keyboard

D. External keylogger

A hardware keylogger is a physical device that captures keystrokes made by a user on a keyboard. The options include various configurations and implementations of keyloggers, and the focus here is on identifying a component that does not fit within the traditional hardware keylogger category. A PC/BIOS embedded keylogger is integrated within a computer's motherboard or BIOS, allowing it to log keystrokes without any software installation. A keylogger keyboard is a specialized keyboard that has keylogging functions built-in, directly capturing the keystrokes as they are typed. An external keylogger is a standalone device that connects between the keyboard and the computer, capturing data from the keyboard's output. In contrast, a network-based logger does not fit the hardware keylogger category, as it operates over a network to capture data rather than directly interfacing with a physical keyboard or being a specific type of device. Network-based loggers typically focus on capturing data transmitted over network connections, like intercepting keystrokes sent across the internet, and do not involve direct physical interaction with user input devices. Thus, identifying "network-based logger" as NOT part of a hardware keylogger accurately highlights the distinction between types of loggers and their operational mechanisms.

10. What type of attack is characterized by preventing legitimate users from accessing resources?

A. Data breach

B. Denial of Service

C. Session hijacking

D. Phishing

Denial of Service (DoS) attacks are specifically designed to disrupt the normal functioning of targeted services, making them unavailable to legitimate users. This type of attack is characterized by overwhelming the target with a flood of traffic or requests that it cannot handle, thus preventing authentic users from accessing the resources they need. In these scenarios, the attacker's goal is to render the service inoperable, which can lead to downtime, loss of productivity, and potentially significant financial losses for an organization. Denial of Service attacks can exploit various vulnerabilities, including network bandwidth limitations or application capacity, effectively locking out legitimate users while the attacker remains outside the system. The other options each define different types of security threats: a data breach involves unauthorized access to sensitive information; session hijacking refers to taking control of a user's active session; and phishing is a technique used to deceive individuals into providing sensitive information by masquerading as a trustworthy entity. None of these options specifically focus on denying access to legitimate users in the same manner that a denial of service attack does.

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!