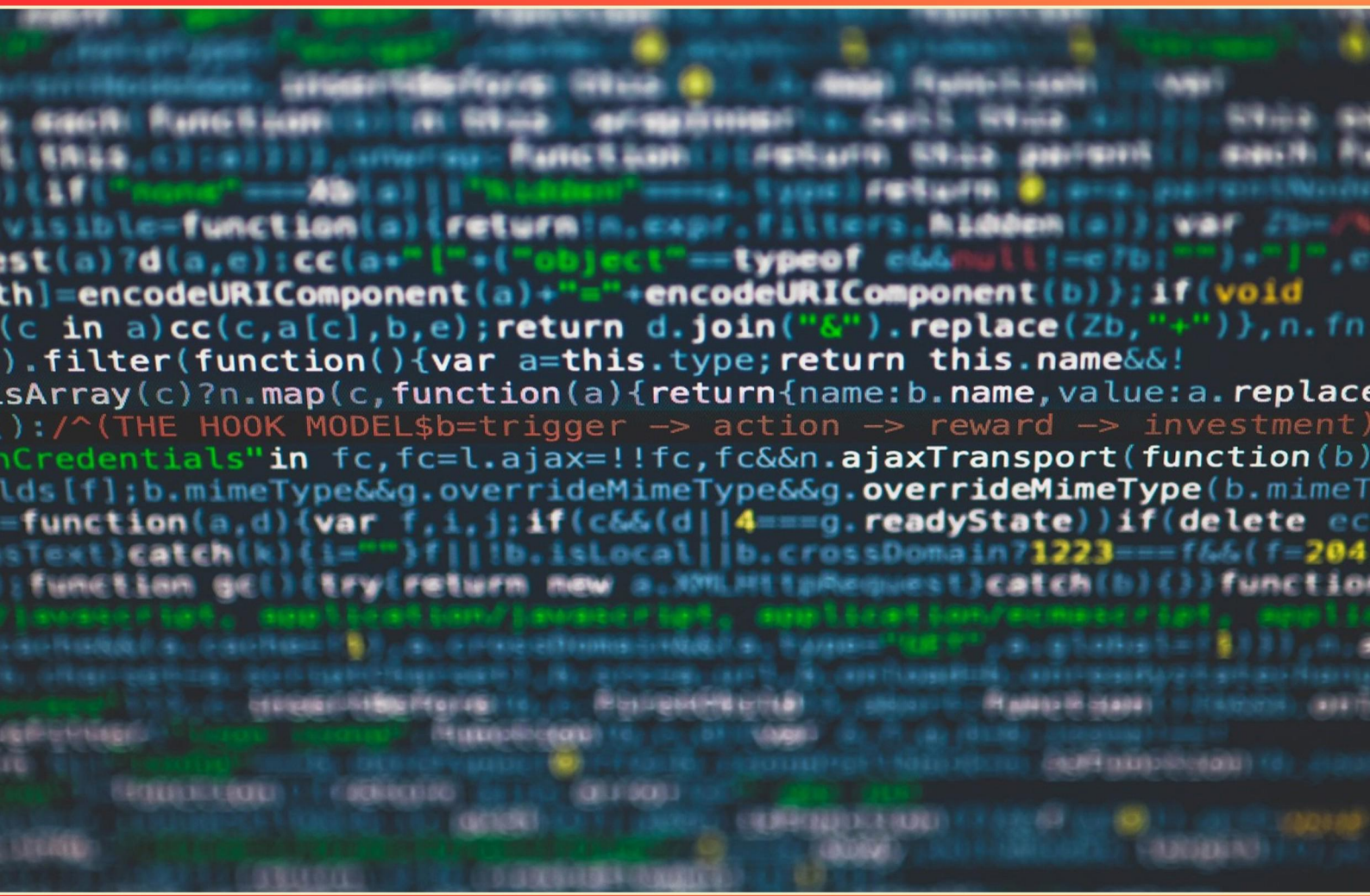
CERTIFIED ETHICAL HACKER CERTIFICATION (CEHV10) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cehv10.examzify.com

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. **Which of the following attacks primarily targets financial transactions using a trojan?**

   A. DNS footprinting

   B. Denial of Service

   C. Man-in-the-Browser

   D. Cross-Site Scripting

2. **Why is network zoning essential for organizations?**

   A. To improve internet connection speeds

   B. To enhance cost management

   C. To enforce appropriate security measures across zones

   D. To provide seamless integration with third-party systems

3. **What activity is NOT part of the target acquisition phase in penetration testing?**

   A. Active probing assaults

   B. Running vulnerability scans

   C. Conducting social engineering attacks

   D. Trusted systems and process assessment

4. **What is the purpose of website footprinting?**

   A. To change website content unnoticed

   B. To collect information about the target website

   C. To improve website visibility in search engines

   D. To create advertisements for the website

5. **What is a primary function of preventive controls in information security?**

   A. To monitor network traffic in real-time

   B. To enforce access control mechanisms and prevent security violations

   C. To track user activity on the network

   D. To address security incidents after they occur

6. Which of the following is NOT considered a common network threat?

A. Denial of Service attacks

B. Cloud Computing Threats

C. Network segmentation

D. Man in the middle attack

7. What does the last character of a NetBIOS name represent?

A. Service or name record type

B. Username for authentication

C. Network protocol type

D. Host domain classification

8. Open System Authentication (OSA) is utilized in the context of which type of network access?

A. WPA wireless networks

B. VPN connections

C. WEP protocol Wi-Fi networks

D. Ethernet wired networks

9. What is the function of TKIP in WPA?

A. To manage user authentication

B. To provide encryption using a single key

C. To ensure packet integrity with unique keys

D. To enforce network bandwidth limits

10. 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

Answers

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

Explanations

1. Which of the following attacks primarily targets financial transactions using a trojan?

A. DNS footprinting

B. Denial of Service

C. Man-in-the-Browser

D. Cross-Site Scripting

The attack that primarily targets financial transactions using a trojan is the Man-in-the-Browser. This type of attack involves malware infecting a user's web browser, inserting itself into the communication between the user and the web application without the user's knowledge. When the trojan is installed, it can intercept information being sent to and from the browser, including sensitive financial transaction data. For instance, it can manipulate the transaction details, such as altering the recipient's account information during a funds transfer, allowing the attacker to redirect funds without the victim's awareness. This makes it particularly dangerous for online banking and e-commerce, as the user believes they are engaging in legitimate transactions when, in fact, they are being manipulated. In contrast, other attack methods such as DNS footprinting, Denial of Service, and Cross-Site Scripting, do not specifically target financial transactions in the same manner. DNS footprinting is primarily used for reconnaissance rather than direct financial manipulation, Denial of Service aims to make a service unavailable rather than to steal or alter financial data, and Cross-Site Scripting typically exploits a vulnerability in web pages to inject malicious scripts but does not necessarily involve financial transaction interception directly in the same way as a Man-in-the-Browser attack does

2. Why is network zoning essential for organizations?

A. To improve internet connection speeds

B. To enhance cost management

C. To enforce appropriate security measures across zones

D. To provide seamless integration with third-party systems

Network zoning is essential for organizations primarily because it allows for the enforcement of appropriate security measures across different zones. By segmenting the network into distinct zones, each with its own security controls, organizations can better protect sensitive data and critical resources. This approach helps mitigate risks by limiting access to sensitive areas of the network based on predefined security policies. For example, a security zone containing sensitive financial data can have stricter access controls compared to a zone intended for public-facing applications. This segmentation ensures that even if one zone is compromised, the attacker would still face barriers in accessing other zones, thereby containing potential breaches. This practice also facilitates compliance with regulatory requirements, as organizations may need to implement specific security measures for data privacy and protection. By having designated zones, it becomes easier to apply and audit these measures, enhancing overall security posture. Other potential benefits, such as improving internet connection speeds or providing seamless integration with third-party systems, are secondary to the primary goal of securing network resources. Similarly, while cost management can be a side effect of efficient zoning, it is not the primary focus of this practice. The emphasis on security measures is what makes zoning a fundamental aspect of network design and management.

3. What activity is NOT part of the target acquisition phase in penetration testing?

A. Active probing assaults

B. Running vulnerability scans

C. Conducting social engineering attacks

D. Trusted systems and process assessment

The target acquisition phase in penetration testing involves gathering information about the target system or organization to understand its structure, technologies, and vulnerabilities. This phase is crucial as it establishes the groundwork for further penetration testing activities. Conducting social engineering attacks stands out as not fitting within this phase. Social engineering typically involves manipulating individuals to gain confidential information, rather than focusing on technical aspects of the target's systems or networks. During the target acquisition phase, the emphasis is primarily on collecting data through methods like active probing, running vulnerability scans, and assessing trusted systems or processes. These techniques are aimed at understanding the technical vulnerabilities and configurations, rather than addressing the human element as social engineering does. Thus, while social engineering can be a component of a broader penetration testing strategy, it is not aligned with the specific goals or activities of the target acquisition phase, which is fundamentally about framework and environment assessment rather than exploiting human factors.

4. What is the purpose of website footprinting?

A. To change website content unnoticed

B. To collect information about the target website

C. To improve website visibility in search engines

D. To create advertisements for the website

The primary purpose of website footprinting is to collect information about the target website. This process involves gathering data related to the website's structure, technology stack, associated domains, server information, and other relevant attributes that can help an ethical hacker understand the target better for security assessments. By establishing a detailed profile of the website, ethical hackers can identify potential vulnerabilities, weaknesses, and exploitable areas that may be susceptible to attacks. Footprinting is essential for planning a penetration test or security audit because it provides insights that help in mapping out the attack vectors and preparing the tools and techniques that might be employed during the security assessment. This proactive approach is critical in identifying potential security issues before malicious actors can exploit them.

5. What is a primary function of preventive controls in information security?

A. To monitor network traffic in real-time

B. To enforce access control mechanisms and prevent security violations

C. To track user activity on the network

D. To address security incidents after they occur

Preventive controls in information security are designed primarily to enforce measures that stop security violations before they can happen. By implementing access control mechanisms, organizations can restrict unauthorized access to sensitive data and systems, effectively safeguarding against potential threats. This aspect of preventive controls is integral to forming a proactive security posture. When access controls are properly enforced, they limit who can view or interact with specific information assets, thereby reducing the risk of data breaches or security incidents related to unauthorized access. This solution aims to mitigate potential vulnerabilities and create a secure environment for data and operations. On the other hand, monitoring network traffic serves more as a detective function rather than a preventative measure, as it only alerts the organization to potential issues after they emerge. Tracking user activity also fits into a detective or analytical role, providing insights into behavior rather than preventing threats. Addressing security incidents post-occurrence falls under reactive controls, which focus on damage containment and recovery rather than prevention. Thus, option B accurately reflects the primary purpose of preventive controls in information security.

6. Which of the following is NOT considered a common network threat?

A. Denial of Service attacks

B. Cloud Computing Threats

C. Network segmentation

D. Man in the middle attack

Network segmentation is a strategy used to improve security and performance within a network by dividing it into smaller, manageable parts. It helps limit access to sensitive information and reduces the attack surface by isolating segments of the network from each other. This practice enhances prevention against various threats rather than being a threat itself. In contrast, denial of service attacks, cloud computing threats, and man in the middle attacks are all significant types of network threats. Denial of service attacks aim to disrupt services by overwhelming resources, cloud computing threats involve vulnerabilities inherent in cloud environments, and man-in-the-middle attacks involve intercepting communications between two parties without their knowledge. All these scenarios pose risks and challenges that security professionals must mitigate. Thus, network segmentation stands apart as a protective measure, solidifying its position as not being a common network threat.

7. What does the last character of a NetBIOS name represent?

A. Service or name record type

B. Username for authentication

C. Network protocol type

D. Host domain classification

The last character of a NetBIOS name plays a crucial role in identifying the type of service or name record associated with that particular name. In the NetBIOS naming convention, names can represent various services, and this last character acts as a single character code that indicates what kind of service the name is registered for. For instance, specific characters designate whether the name is for a workstation, server, or other types of resources within the network. This mechanism allows systems to distinguish between different types of services and facilitates proper communication and resource allocation in a network environment. Therefore, understanding this aspect of NetBIOS naming is essential for network administrators and security professionals when managing resources and ensuring the efficient functioning of network services.

8. Open System Authentication (OSA) is utilized in the context of which type of network access?

A. WPA wireless networks

B. VPN connections

C. WEP protocol Wi-Fi networks

D. Ethernet wired networks

Open System Authentication (OSA) is a method used primarily in WEP (Wired Equivalent Privacy) protocol Wi-Fi networks to manage how devices gain access to the wireless network. In the context of OSA, the authentication process is relatively simple—any device that sends an authentication request will be granted access without any requirement for credentials or pre-shared keys, making it easy for devices to connect to the network. WEP networks implement OSA for their authentication processes, allowing clients to connect without the need for complex encryption or key management. This contrasts with more secure protocols, such as WPA (Wi-Fi Protected Access), which use more advanced forms of authentication that require mutual authentication between client and the access point, ensuring higher levels of security. On the other hand, VPN connections and Ethernet wired networks typically have their own specific authentication methods that are more secure and require user credentials or pre-established keys. Thus, they do not utilize OSA in their authentication processes.

9. What is the function of TKIP in WPA?

A. To manage user authentication

B. To provide encryption using a single key

C. To ensure packet integrity with unique keys

D. To enforce network bandwidth limits

The correct answer is rooted in the key functions that TKIP (Temporal Key Integrity Protocol) serves within the framework of WPA (Wi-Fi Protected Access). TKIP was designed as an enhancement over the older WEP (Wired Equivalent Privacy) for wireless network security. TKIP's primary function is to ensure packet integrity by using a unique key for each packet. This is a critical development compared to WEP, where the same key was used for all packets during a session, leading to vulnerabilities in data integrity. With TKIP, a unique key is generated for each packet, utilizing a per-packet key mixing function that combines the base key with a sequence counter. This approach enhances security by ensuring that even if an attacker could intercept multiple packets, they would find it exceedingly difficult to decipher them without knowing the specific key involved, thereby protecting against replay attacks and providing strong data integrity checks. Other considerations about the other options include user authentication, which is not a primary function of TKIP but rather a responsibility allocated to other protocols within WPA. While TKIP does provide encryption, it does not use a single key for this purpose, as the use of unique keys is fundamental to its function. Finally, enforcing network bandwidth limits is unrelated to the role that TK

10. 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.

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!