CERTIFIED ETHICAL HACKER (CEH) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://ceh.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. **How can web spiders be inhibited from crawling a site?**

   A. By using site: commands

   B. By adding "robots.txt" to the root of the website

   C. By minimizing website content

   D. By enhancing site security features

2. **What is the RIR responsible for Asia?**

   A. AFRINIC

   B. LACNIC

   C. APNIC

   D. RIPE NCC

3. **In the context of a replay attack, what method is frequently used by the attacker?**

   A. Encrypting the communication

   B. Repeating a cryptographic exchange

   C. Decryption of data packets

   D. Capturing login credentials directly

4. **In terms of cybersecurity, what does the term "availability" refer to?**

   A. The protection of communications from hackers

   B. The accessibility of data when needed by legitimate users

   C. The resistance of a system to unauthorized changes

   D. The speed at which data is processed

5. **Which encryption protocol is characterized by a handshake process for authentication?**

   A. PPTP

   B. IPsec

   C. TLS

   D. FTP

SAMPLE

6. Which of the following is NOT a service provided by RIRs?

A. Allocating IP addresses
B. Registering domain names
C. Facilitating internet governance
D. Managing WHOIS services

7. What is the primary objective of a penetration test?

A. To showcase the strengths of an IT system
B. To identify security risks and vulnerabilities
C. To train employees on security protocols
D. To sell security solutions

8. What is a characteristic of misconfiguration attacks?

A. They require advanced hacking skills
B. They exploit poorly designed software
C. They target systems not configured for security
D. They rely on social engineering techniques

9. What is the RIR for South America and the Caribbean?

A. RIPE NCC
B. ARIN
C. LACNIC
D. APNIC

10. What do attackers attempt to do during the Covering Tracks phase?

A. Install backdoors for future access
B. Remove or corrupt log files
C. Conduct further reconnaissance
D. Gain access to additional targets

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. How can web spiders be inhibited from crawling a site?

A. By using site: commands

B. By adding "robots.txt" to the root of the website

C. By minimizing website content

D. By enhancing site security features

Web spiders, also known as web crawlers or bots, are automated programs that systematically browse the internet, indexing pages and gathering data. To control how these spiders interact with a website, the "robots.txt" file serves as an essential mechanism. By placing a "robots.txt" file in the root directory of a website, a site owner can provide specific instructions to the web spiders regarding which parts of the site should not be accessed or indexed. This file includes directives that tell crawling bots whether they are allowed or disallowed from certain directories or pages. For example, if a website owner wants to keep certain sensitive areas or duplicate content from being crawled, they can explicitly mention that in the "robots.txt" file, effectively "inhibiting" the crawlers from accessing that content. In contrast, the other options do not effectively prevent web spiders from crawling a site. Using site: commands is a search engine query method that does not inhibit crawling, but rather, allows you to search for specific pages indexed by search engines. Minimizing website content does not prevent crawlers from accessing the site but may reduce the total number of pages crawled. Enhancing site security features, while important for protecting data, does not specifically prevent web spiders from

2. What is the RIR responsible for Asia?

A. AFRINIC

B. LACNIC

C. APNIC

D. RIPE NCC

The correct answer is APNIC, which stands for the Asia-Pacific Network Information Centre. APNIC is the Regional Internet Registry (RIR) responsible for the Asia-Pacific region, which includes countries such as China, Japan, India, and Australia. Its primary role involves the allocation and management of IP address space, providing support and training for network operators, and contributing to the overall development of the internet in the region. APNIC plays a crucial role in the governance of internet resources in Asia by ensuring that addresses are allocated efficiently and that members have the necessary support to manage their networks. This helps maintain stability within the region's internet infrastructure. The organization also promotes best practices and collaborates with stakeholders to foster the growth of the internet community. Other regional internet registries, such as AFRINIC, LACNIC, and RIPE NCC, serve different geographical areas. AFRINIC is responsible for Africa, LACNIC covers Latin America and the Caribbean, and RIPE NCC operates in Europe, the Middle East, and parts of Central Asia. Each RIR has distinct responsibilities based on their respective regions, which is why APNIC is specifically identified as the RIR for Asia.

SAMPLE

3. In the context of a replay attack, what method is frequently used by the attacker?

A. Encrypting the communication

B. Repeating a cryptographic exchange

C. Decryption of data packets

D. Capturing login credentials directly

In the context of a replay attack, the primary method used by the attacker involves repeating or retransmitting a previous cryptographic exchange. This attack typically occurs when an attacker captures a data transmission (which could include authentication information or other sensitive data) and then replays it to gain unauthorized access or to impersonate a user. Replay attacks exploit the fact that some systems do not adequately differentiate between legitimate requests and repeated requests. By capturing the legitimate data transmission and resending it, the attacker can trick the system into believing that they are a valid user or entity. This is particularly concerning in situations where time-sensitive tokens or session identifiers are not utilized to distinguish new requests from old ones. Though encrypting communication, decrypting data packets, and capturing login credentials can be associated with different forms of attacks, they do not specifically describe the mechanics of a replay attack. The essence of a replay attack lies in the act of taking an existing valid transmission and playing it back, rather than manipulating the data or credentials directly.

4. In terms of cybersecurity, what does the term "availability" refer to?

A. The protection of communications from hackers

B. The accessibility of data when needed by legitimate users

C. The resistance of a system to unauthorized changes

D. The speed at which data is processed

The term "availability" in cybersecurity pertains specifically to the accessibility of data and systems when required by legitimate users. This principle is one of the core components of the CIA triad, which stands for Confidentiality, Integrity, and Availability. When discussing availability, it is essential to ensure that systems are up and running efficiently, allowing authorized users to access the information they need without undue delay or obstacles. This involves implementing measures such as redundancy, failover systems, and regular maintenance to protect against downtime or system failures. The focus on legitimate users highlights the importance of ensuring that authorized personnel can access the data they need without being hindered by outages or restrictions. The other options, while relevant to various aspects of cybersecurity, do not accurately capture the essence of availability. The protection of communications from hackers relates more closely to confidentiality, while resistance to unauthorized changes pertains to integrity. Lastly, the speed of data processing concerns performance rather than the availability of access to data.

SAMPLE

5. Which encryption protocol is characterized by a handshake process for authentication?

A. PPTP

B. IPsec

C. TLS

D. FTP

The correct answer involves the TLS (Transport Layer Security) protocol, which is specifically designed to provide secure communication over a computer network. TLS employs a handshake process that establishes a secure session between a client and server. This process includes the exchange of cryptographic keys and authentication information to ensure that both parties are legitimate and that the communication is encrypted. During the handshake, both parties negotiate the encryption algorithms and keys they will use for the session, thus facilitating a secure connection before any data is transmitted. In contrast, while protocols such as PPTP (Point-to-Point Tunneling Protocol) and IPsec (Internet Protocol Security) are used for secure data transmission, they do not incorporate a handshake process in the same structured manner as TLS for authentication purposes. PPTP primarily relies on a different set of security measures that do not involve a detailed authentication handshake process, and IPsec utilizes a more complex approach focusing on securing the IP layer of a network rather than the handshake method that TLS is known for. FTP (File Transfer Protocol), on the other hand, does not provide encryption inherently and does not incorporate an authentication handshake process like TLS. Instead, it transfers data in plaintext, making it less secure for transferring sensitive information. Understanding the unique handshake process used

6. Which of the following is NOT a service provided by RIRs?

A. Allocating IP addresses

B. Registering domain names

C. Facilitating internet governance

D. Managing WHOIS services

RIRs, or Regional Internet Registries, are organizations responsible for the allocation and management of IP address resources within specific regions. Their primary role includes allocating IP addresses to Internet Service Providers (ISPs) and other large organizations, as well as managing WHOIS services that provide information about the registration of IP addresses. Facilitating internet governance is also part of their responsibilities, often involving coordination with global and regional entities to ensure that policies related to IP address management are upheld. However, registering domain names is not a service provided by RIRs. Domain name registration falls under the purview of domain registrars, which operate under the auspices of organizations like ICANN (the Internet Corporation for Assigned Names and Numbers) that manage the domain name system (DNS) globally. This distinction is important, as it highlights the different roles that these organizations play in the internet infrastructure; RIRs focus on IP addresses while registrars deal with domain names.

SAMPLE

7. What is the primary objective of a penetration test?

A. To showcase the strengths of an IT system

B. To identify security risks and vulnerabilities

C. To train employees on security protocols

D. To sell security solutions

The primary objective of a penetration test is to identify security risks and vulnerabilities within an IT system. Conducted by ethical hackers, penetration testing involves simulating real-world attacks to assess the security posture of the system. This process allows organizations to understand potential weaknesses before they can be exploited by malicious actors, enabling them to bolster their defenses. Through this proactive approach, a detailed analysis of how an attacker might breach the system is achieved, helping to pinpoint specific areas that require improvement. The ultimate goal is not only to discover vulnerabilities but also to provide actionable recommendations for remediation, thereby enhancing overall security and protecting sensitive data. While showcasing strengths, training employees, or selling solutions may be auxiliary benefits, they do not encapsulate the fundamental purpose of penetration testing. The focus remains predominantly on risk identification and vulnerability assessment, which is critical for safeguarding organizational assets.

8. What is a characteristic of misconfiguration attacks?

A. They require advanced hacking skills

B. They exploit poorly designed software

C. They target systems not configured for security

D. They rely on social engineering techniques

The characteristic that identifies misconfiguration attacks revolves around the idea that these attacks specifically focus on systems that have not been configured to adhere to security best practices. Misconfiguration can occur during the initial setup of a system, software, or network equipment when security settings are overlooked or improperly set, creating vulnerabilities that can be exploited by attackers. By targeting these inadequately secured systems, attackers can gain unauthorized access or perform malicious actions without needing sophisticated hacking skills. This makes it a prevalent tactic among cybercriminals, as many organizations may unintentionally leave these security gaps. The focus on poorly configured systems underscores the importance of following security protocols and conducting regular audits to ensure that all security measures are properly implemented. In contrast, options that mention advanced hacking skills, poorly designed software, or reliance on social engineering techniques pertain to different attack vectors that do not specifically align with the nature of misconfiguration attacks. Misconfiguration is primarily about the improper setup of security configurations, rather than the design flaws of the software itself, advanced tactics, or manipulating individuals for access.

SAMPLE

9. What is the RIR for South America and the Caribbean?

A. RIPE NCC

B. ARIN

C. LACNIC

D. APNIC

The correct answer is C, LACNIC (Latin America and Caribbean Network Information Centre), which is the Regional Internet Registry responsible for managing IP address allocation in South America and the Caribbean. LACNIC was established to ensure the efficient and fair distribution of internet resources in this region, and it works closely with organizations and governments to promote internet development and address related challenges. Understanding LACNIC's role is crucial for recognizing how IP addresses and other resources are distributed globally. Each Regional Internet Registry serves specific geographic areas, and LACNIC's responsibilities include allocating IP addresses and Autonomous System Numbers (ASNs) to local internet service providers and organizations within its jurisdiction. The other options represent different regions: RIPE NCC manages Europe, the Middle East, and parts of Central Asia. ARIN operates in the United States, Canada, and some parts of the Caribbean. APNIC oversees the Asia-Pacific region. This geographic distribution underscores the importance of LACNIC in facilitating internet growth and connectivity specifically in South America and the Caribbean, distinguishing it as the correct answer.

10. What do attackers attempt to do during the Covering Tracks phase?

A. Install backdoors for future access

B. Remove or corrupt log files

C. Conduct further reconnaissance

D. Gain access to additional targets

During the Covering Tracks phase, attackers aim to erase or alter evidence of their presence within a system, which significantly includes the removal or corruption of log files. Log files are crucial for documenting the activities that take place on a system, including successful intrusions, executed commands, and unauthorized access. By manipulating or deleting these logs, attackers can obscure their actions, making it challenging for security teams to trace their movements and identify the intrusion. This phase is critical for maintaining stealth and prolonging their access to the compromised environment without detection. While other activities such as installing backdoors or conducting further reconnaissance may be part of an attacker's broader strategy, the specific focus during the Covering Tracks phase is primarily on removing or tampering with logs to hide their activities.

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://ceh.examzify.com

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

SAMPLE