EC-COUNCIL CERTIFIED ETHICAL HACKER (CEH) CERTIFICATION PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS



VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://eccouncilceh.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. **Which utility is commonly used to remove files and clear internet browsing history?**

   A. Recycle Bin Cleaner

   B. Disk Cleanup

   C. CCleaner

   D. System Optimizer

2. **In packet crafting for network testing, which program is commonly used to modify packet flags and adjust other packet content?**

   A. Colasoft

   B. Wireshark

   C. Nmap

   D. Metasploit

3. **Which term best describes publicly accessible information about a DNS zone that can be obtained via certain server configurations?**

   A. DNS caching

   B. DNS poisoning

   C. DNS spoofing

   D. DNS zone transfer

4. **What is the primary purpose of deploying a honeypot in a security program?**

   A. Increase throughput

   B. Attract attackers for study

   C. Encrypt traffic

   D. Monitor disk usage

5. **Creating an area of the network where offending traffic is forwarded and dropped is known as _____?**

   A. Port forwarding

   B. Black hole filtering

   C. Traffic shaping

   D. Load balancing

SAMPLE

6. In a smart home, a device that communicates directly with other devices without a central server demonstrates which communication model?

A. Client-server

B. Peer-to-peer

C. Device-to-device

D. Cloud-based

7. Which embedded operating systems are most likely used by a smart car and its drone for control?

A. Windows

B. Integrity RTOS and Snappy

C. Linux

D. VxWorks

8. Which tool is commonly used as an intrusion detection system and can function as an intrusion prevention system?

A. Snort

B. Whois

C. SecurityMetrics Mobile

D. Security vulnerability summary

9. Which of the following describes high-interaction honeypots?

A. They are the simplest form of honeypots with minimal risk

B. They mimic full systems and allow attacker interaction

C. They only log network probes

D. They require no maintenance

10. Which of the following is considered an out-of-band method for distributing a private key?

A. Copying the key to a USB drive

B. Emailing the key

C. Storing the key on a shared network drive

D. Printing the key on paper

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which utility is commonly used to remove files and clear internet browsing history?

A. Recycle Bin Cleaner

B. Disk Cleanup

C. CCleaner

D. System Optimizer

The idea being tested is how cleaning utilities help protect privacy and reclaim space by removing leftover files and traces of online activity. CCleaner is the best fit because it's specifically designed to purge a wide range of unnecessary data, including browser caches, cookies, history, and other traces left by web activity, along with temporary files from the operating system and installed programs. This makes it a popular and effective tool for clearing internet browsing history across multiple browsers in one go. Disk Cleanup is a built-in Windows option that frees space by removing temporary and system files, but it isn't focused on wiping browser histories or traces from multiple browsers. Recycle Bin Cleaner would only empty files from the Recycle Bin, not address browser data or other caches. System Optimizer is a generic term and doesn't point to a specific, widely used cleaning utility. So, CCleaner is the commonly used tool for removing files and clearing internet browsing history.

2. In packet crafting for network testing, which program is commonly used to modify packet flags and adjust other packet content?

A. Colasoft

B. Wireshark

C. Nmap

D. Metasploit

Packet crafting is about building and sending custom packets, changing fields such as TCP flags and various header and payload data to test how devices and security systems respond. The tool that provides a direct, general-purpose way to edit these fields and then transmit the crafted packets is Colasoft's packet-building utility. It's specifically designed for creating packets with precise values in multiple protocol layers, allowing you to toggle flags like SYN, ACK, FIN, and other header bits, as well as adjust payload content. This makes it the best fit for experiments and testing that require manual modification of packet content. Wireshark, by contrast, excels at capturing and analyzing traffic, not at crafting or sending customized packets. Nmap focuses on network discovery and scanning, with some advanced probes, but it isn't a dedicated packet editor for crafting arbitrary packets. Metasploit is an exploitation framework used to deliver payloads and validate vulnerabilities, not a general packet crafting tool.

SAMPLE

3. Which term best describes publicly accessible information about a DNS zone that can be obtained via certain server configurations?

A. DNS caching

B. DNS poisoning

C. DNS spoofing

D. DNS zone transfer

Zone transfers describe the process of copying the contents of a DNS zone from a primary server to secondary servers. When a DNS server is misconfigured to allow transfers to any host, you can request a zone transfer and obtain the entire zone data. That means publicly accessible information about the zone—such as all host names, IP addresses, mail servers, and other records—can be leaked simply by querying the server for a transfer. This is why zone transfer is the term that best fits the scenario. DNS caching stores previously resolved query results on a client or resolver to speed up lookups; it isn't about exposing the full zone data. DNS poisoning and DNS spoofing involve corrupting or forging DNS responses to mislead users or redirect traffic, not about retrieving the complete zone contents via a configured transfer.

4. What is the primary purpose of deploying a honeypot in a security program?

A. Increase throughput

B. Attract attackers for study

C. Encrypt traffic

D. Monitor disk usage

A honeypot is a decoy system placed in a network to lure attackers away from real assets, with the goal of studying their behavior. Its primary purpose is to attract attackers so security teams can observe their methods in a controlled environment. By watching attempted intrusions, malware payloads, command-and-control activity, and exploitation techniques, defenders gain actionable insight into current threats, attacker tools, and typical attack workflows. This information helps improve detection, patch gaps, and incident response, all while keeping production systems safe because the honeypot is isolated and closely monitored. Increasing throughput isn't the goal, since a honeypot isn't meant to handle legitimate traffic efficiently. Encrypting traffic is a protective measure for actual communications, not a tactic for learning attacker behavior. Monitoring disk usage is a general system administration task and not the primary reason for deploying a honeypot.

5. Creating an area of the network where offending traffic is forwarded and dropped is known as _____?

A. Port forwarding

B. Black hole filtering

C. Traffic shaping

D. Load balancing

This question tests the idea of diverting unwanted traffic into a dedicated network area where it is discarded, a sinkhole approach often called black hole filtering. By routing offending traffic to a black hole (or null route), the traffic is effectively forwarded into a disposal point and then dropped, preventing it from consuming resources or reaching targets. This is a quick, blunt defense that protects the rest of the network without trying to inspect or alter the traffic. Port forwarding maps external connections to internal hosts, not about filtering hostile traffic. Traffic shaping controls bandwidth usage and QoS, not discarding traffic. Load balancing spreads traffic across multiple servers, which also isn't about dropping harmful traffic.

SAMPLE

6. In a smart home, a device that communicates directly with other devices without a central server demonstrates which communication model?

A. Client-server

B. Peer-to-peer

C. Device-to-device

D. Cloud-based

Direct interaction between devices without a central server is best described as device-to-device communication. In a smart home, this means devices talk to each other locally—over short-range protocols like Bluetooth, Zigbee, or Matter—without routing commands through a hub or cloud. This setup reduces latency and dependence on a remote server, which is why it's categorized as device-to-device. While peer-to-peer can also describe direct device interactions, the emphasis here is on the established device-to-device model where each device communicates with others itself rather than relying on an intermediary that mediates all traffic. The other options imply routes through a central destination: client-server relies on a central server, and cloud-based depends on cloud infrastructure to relay data.

7. Which embedded operating systems are most likely used by a smart car and its drone for control?

A. Windows

B. Integrity RTOS and Snappy

C. Linux

D. VxWorks

Real-time, deterministic behavior is essential for control tasks in a smart car and its drone. Embedded operating systems used for these roles must guarantee predictable timing, fast and reliable interrupt handling, and strong isolation between critical control tasks and other processes. Integrity RTOS and Snappy are designed for this kind of safety-critical, resource-constrained environment. They provide memory protection, process isolation, and tight, certifiable safety features that help ensure the control loops in both automotive and aerial platforms operate reliably under all conditions. Windows is a general-purpose OS and is not built for hard real-time control. Linux can run embedded systems, but hard real-time guarantees are not inherent without special patches and configurations. VxWorks is a capable RTOS and is used in many industries, but the pairing of Integrity RTOS and Snappy reflects the typical choice for high-assurance control in automotive and drone applications.

SAMPLE

8. Which tool is commonly used as an intrusion detection system and can function as an intrusion prevention system?

A. Snort

B. Whois

C. SecurityMetrics Mobile

D. Security vulnerability summary

The concept being tested is how intrusion detection and prevention tools operate and the way one tool can switch from monitoring to actively blocking traffic. Snort is a classic example: it's a signature-based system that analyzes network traffic against a set of rules to identify known attack patterns. When used as an IDS, Snort monitors traffic and generates alerts, logs, or notifications based on those rules. But it can also be deployed inline in the network path so it's able to take action in real time—dropping, replaying, or modifying packets that match its rules—effectively functioning as an intrusion prevention system. This dual capability is what makes Snort widely used for both detection and prevention. The other options don't fit this role. Whois is a domain registration lookup service and has nothing to do with monitoring or blocking traffic. SecurityMetrics Mobile is a security assessment/product, not a network IDS/IPS tool. A security vulnerability summary is a report, not an active monitoring or protection tool.

9. Which of the following describes high-interaction honeypots?

A. They are the simplest form of honeypots with minimal risk

B. They mimic full systems and allow attacker interaction

C. They only log network probes

D. They require no maintenance

High-interaction honeypots are built to resemble real systems, running actual services, applications, and operating systems so an attacker can interact with them like they would with a live environment. This realism lets defenders observe deep, complex attacker techniques, tools, and workflows in action, capturing rich data about how intruders probe, exploit, and move through a network. Because the setup is essentially a full, live system, it yields insights into real-world behaviors that simpler decoys cannot provide, such as malware payloads, command sequences, and pivot methods. However, this level of interaction also means higher risk and more ongoing work to keep the honeypot isolated from production assets, monitored, and maintained to prevent abuse or escape. The description described here emphasizes the full-system, interactive nature that distinguishes high-interaction honeypots from simpler, low-interaction ones, which are easier to manage and provide less detailed attacker information, and from setups that merely log probes or require no maintenance.

SAMPLE

10. Which of the following is considered an out-of-band method for distributing a private key?

A. Copying the key to a USB drive

B. Emailing the key

C. Storing the key on a shared network drive

D. Printing the key on paper

Out-of-band distribution means moving the private key through a channel that is separate from the normal electronic data path, reducing the chance of interception. Physical transfer methods—such as handing over a USB drive or printing the key on paper and delivering it in person—are classic out-of-band options because they don't travel over the same network or email channels that can be compromised. In contrast, sending the key via email travels through an electronic channel that is widely exposed to risks like interception or unauthorized access, so it's not considered out-of-band. Storing the key on a shared network drive also relies on the same network path and permissions, making it in-band as well. The key idea is to minimize exposure by using a separate, ideally offline, medium for distribution. Therefore, to practice true out-of-band distribution, you would use physical media or printed paper delivery rather than email.

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://eccouncilceh.examzify.com

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

SAMPLE