Certified Ethical Hacker Version 11 (CEHv11) Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Sample study guide. For the full version with hundreds of questions, visit: https://cehv11.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

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 type of keylogger operates within a malware hypervisor on the host operating system?**

   A. Hypervisor-Based Keylogger

   B. Form-Grabbing-Based Keylogger

   C. Memory-Injection-Based Keylogger

   D. JavaScript-Based Keylogger

2. **Which term describes a gateway technology used to connect and integrate multiple web applications?**

   A. Api

   B. Web Shell

   C. Weevely

   D. Web Shell Detector

3. **Which vulnerability occurs when input from a client is not validated before being processed by web applications and backend servers?**

   A. Unvalidated Inputs

   B. Parameter/Form Tampering

   C. Improper Error Handling

   D. Web Service Attack

4. **Which term describes the practice of sending spam through instant messaging that leads to credential theft?**

   A. Instant Chat Messenger

   B. Spimming

   C. Whaling attack

   D. Spamming

5. **The attacker analyzes the embedded algorithm used to detect distinguishing statistical changes along with the length of the embedded data.**

   A. Chi-square Attack

   B. Distinguishing Statistical attack

   C. Blind Classifier attack

   D. zsteg

SAMPLE

6. Which container vulnerability scanning tool is listed among the following?

A. Trivy

B. Clair

C. Dadga

D. Nessus

7. Intercepts IP addresses, MAC addresses, and VLANs connected to the switch in a network?

A. Arpspoof

B. Data Interception

C. Rogue DHCP Server Attack

D. Address Resolution Protocol (ARP)

8. Which software is described as PC-user activity-monitoring software running secretly in the background?

A. Zemana AntiLogger

B. Power Spy

C. Anti-keyloggers

D. SUPERAnti Spyware

9. Which service would you query to determine if a user's IP is on known blacklists?

A. Bug bounty program

B. Acunetix WVS

C. Apility.io

D. RASP

10. What term describes attackers exploiting pre-installed tools on Windows to install and run malicious code?

A. Native applications

B. Legitimate applications

C. Fileless malware

D. PowerShell abuse

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which type of keylogger operates within a malware hypervisor on the host operating system?

A. Hypervisor-Based Keylogger

B. Form-Grabbing-Based Keylogger

C. Memory-Injection-Based Keylogger

D. JavaScript-Based Keylogger

Understanding where keystroke data can be captured helps distinguish keylogger types. A hypervisor-based keylogger operates inside a malware hypervisor on the host operating system, sitting beneath the guest OS and intercepting input before it reaches the OS. This virtualization layer position lets it monitor keystrokes stealthily across the system, often evading ordinary security tools that run within the OS. In contrast, form-grabbing-based keyloggers focus on data entered into web forms, memory-injection-based keyloggers inject into running processes to capture data in memory, and JavaScript-based keyloggers operate inside a web page to log keystrokes in the browser. So, the scenario described matches the hypervisor-based keylogger.

2. Which term describes a gateway technology used to connect and integrate multiple web applications?

A. Api

B. Web Shell

C. Weevely

D. Web Shell Detector

APIs provide the standard way for software components to talk to each other and work together. They define how to request services, what data formats to use (such as JSON or XML), and what actions are available. Because APIs expose well-defined interfaces, multiple web applications can connect to each other through these gateways, enabling data exchange, authentication, and service orchestration across systems. This gateway role—bridging different apps so they can operate together—is why this term is the best fit for describing a mechanism that connects and integrates multiple web applications. The other terms refer to different concepts: a web shell is a remote command interface left on a compromised server, Weevely is a PHP backdoor for remote access, and a web shell detector is a defensive tool to identify such backdoors. None of these describe a standard means of integrating multiple web applications.

SAMPLE

3. Which vulnerability occurs when input from a client is not validated before being processed by web applications and backend servers?

A. Unvalidated Inputs

B. Parameter/Form Tampering

C. Improper Error Handling

D. Web Service Attack

Unvalidated input means the application accepts data from a user without checking that it's safe, well-formed, or within expected boundaries before it's processed by the web app or backend services. When input isn't validated, crafted data can influence queries, commands, or file paths, leading to injections, logic errors, or data exposure. Validating and sanitizing input—using strict allow-lists, enforcing types and length checks, and parameterizing downstream calls—helps prevent these issues. This description matches unvalidated inputs precisely: client data is accepted and processed without proper validation. The other issues describe different problems—tampering is about altering request data to gain advantage, improper error handling concerns leaking or mismanaging errors, and web service attacks cover broader service-targeted exploits.

4. Which term describes the practice of sending spam through instant messaging that leads to credential theft?

A. Instant Chat Messenger

B. Spimming

C. Whaling attack

D. Spamming

The main idea here is deceptive messaging through instant messaging used to steal credentials. Spimming combines spam with instant messaging to spread quickly in channels people trust, like chat apps. Attackers often pose as a friend or coworker and push a fake login prompt or a link to a spoofed site, aiming to harvest usernames, passwords, or tokens. This makes it a form of phishing that is specifically carried out over IM platforms, taking advantage of real-time delivery and the perceived legitimacy of a familiar contact. It's different from generic email spam and from whaling, which targets top executives; spimming is the IM-focused phishing tactic designed for credential theft. To defend, verify unexpected messages, avoid clicking suspicious links, enable multi-factor authentication, and educate users to spot impersonations and spoofed profiles.

SAMPLE

5. The attacker analyzes the embedded algorithm used to detect distinguishing statistical changes along with the length of the embedded data.

A. Chi-square Attack

B. Distinguishing Statistical attack

C. Blind Classifier attack

D. zsteg

Distinguishing statistical attack focuses on detecting hidden data by looking for statistical changes introduced by embedding and, in some cases, estimating how much data was embedded. The idea is that hiding data alters the normal statistical properties of the media (such as pixel value distributions or correlations), and by examining these changes you can tell that something was embedded and even gauge the payload length. That's exactly what the described scenario is about: analyzing the embedded process to spot distinguishing statistical changes and infer how long the embedded data is. A chi-square attack is a concrete statistical method that looks at histogram deviations to spot LSB modifications, but it's one specific technique within the broader category of statistical attacks. A blind classifier attack relies on machine learning to distinguish stego from cover using features, not necessarily focusing on the embedded algorithm's statistical changes or payload length. zsteg is a practical tool for detecting steganography in images, often targeting LSB steganography in color channels, rather than describing this particular attack approach.

6. Which container vulnerability scanning tool is listed among the following?

A. Trivy

B. Clair

C. Dadga

D. Nessus

Container vulnerability scanning focuses on inspecting a container image to identify known CVEs and insecure packages within its layers before deployment. A tool that specializes in this task will analyze the image's installed OS packages and libraries, map them to vulnerability databases, and report severities, affected components, and remediation guidance. Dagda is a dedicated container image vulnerability scanner. It targets Docker images directly, pulling together vulnerability data from multiple sources and analyzing the image's layers to surface known issues. That focused purpose makes it a natural fit for questions about container-specific scanning tools. Trivy and Clair are also container-focused scanners: they examine images for OS-package and library vulnerabilities and integrate with registries or CI pipelines. Nessus, by contrast, is a broad vulnerability scanner for hosts, networks, and applications; while it can touch containers, it's not specialized for container image analysis in the same way. So, among the listed options, Dagda is a container image vulnerability scanner, which is why it's a valid pick in this context, with Trivy and Clair as other widely used container scanners and Nessus serving a broader vulnerability-scanning role.

SAMPLE

7. Intercepts IP addresses, MAC addresses, and VLANs connected to the switch in a network?

A. Arpspoof

B. Data Interception

C. Rogue DHCP Server Attack

D. Address Resolution Protocol (ARP)

Data interception is the act of eavesdropping on network traffic to observe the addresses and segmentation details that devices reveal. When traffic is captured in a network that uses switches, you're able to see IP addresses and MAC addresses as packets move, and you can also learn the VLAN identifiers carried in the frames. This matches the idea of intercepting the information connected to the switch, including who is on the network and how traffic is segmented. ARPspoof is a technique that can enable interception by placing the attacker in the traffic path, but it's a method used to achieve data interception, not the broad concept itself. A rogue DHCP server attack focuses on altering IP address assignment and network configuration rather than passively observing traffic. ARP is the protocol that maps IP addresses to MAC addresses, not the act of intercepting data.

8. Which software is described as PC-user activity-monitoring software running secretly in the background?

A. Zemana AntiLogger

B. Power Spy

C. Anti-keyloggers

D. SUPERAnti Spyware

Covert PC-user activity monitoring software is designed to run invisibly in the background to collect what a user does on a computer. Among the options, the one marketed as a surveillance tool that can stay hidden in the background fits this description best. Power Spy is described as a PC-user activity-monitoring program that runs secretly in the background, capable of logging actions like keystrokes, websites visited, apps used, and possibly taking screenshots for remote viewing. The other tools serve different purposes: Zemana AntiLogger and Anti-keyloggers are defensive tools meant to detect or block keyloggers to protect user data, not to secretly monitor the user's activity themselves. SUPERAnti Spyware is an anti-malware/anti-spyware scanner designed to detect and remove threats, not to monitor user activity covertly. So Power Spy matches the description of secretly monitoring a user's activity in the background.

SAMPLE

9. Which service would you query to determine if a user's IP is on known blacklists?

A. Bug bounty program

B. Acunetix WVS

C. Apility.io

D. RASP

IP reputation checks are used to see if a particular address appears on known blacklists. To determine this, you query a service that aggregates multiple blacklist feeds and can report whether the given IP is listed, along with reasons and timing. Apility.io fits this need because it's a dedicated IP reputation/blacklist lookup service with an API that checks an IP across many feeds (spam and abuse lists) and returns listing status. This lets you decide whether to allow, challenge, or block traffic based on the IP's reputation. The other options serve different purposes: a bug bounty program is for reporting vulnerabilities in exchange for rewards, a vulnerability scanner like Acunetix WVS scans apps for weaknesses, and RASP provides runtime protection within an application. They don't provide a direct lookup of an IP's blacklist status.

10. What term describes attackers exploiting pre-installed tools on Windows to install and run malicious code?

A. Native applications

B. Legitimate applications

C. Fileless malware

D. PowerShell abuse

Leveraging built-in Windows tools to install and run malicious code centers on native applications—the software that already ships with the operating system. Attackers reuse these pre-installed utilities to execute payloads, download additional components, or run commands, which helps them blend in with normal activity and often avoids triggering alarms set for unfamiliar software. Because the focus is on using what is already present on the system rather than introducing new tools, the broad term that fits best is native applications. While PowerShell abuse is a real example of this tactic, it describes a specific tool being misused rather than the general idea of exploiting pre-installed tools. Fileless malware relates to staying in memory or using living-off-the-land techniques, which can involve native tools but is not the exact term for the concept described. Legitimate applications don't imply misuse, so they don't capture the malicious exploitation described.

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://cehv11.examzify.com

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

SAMPLE