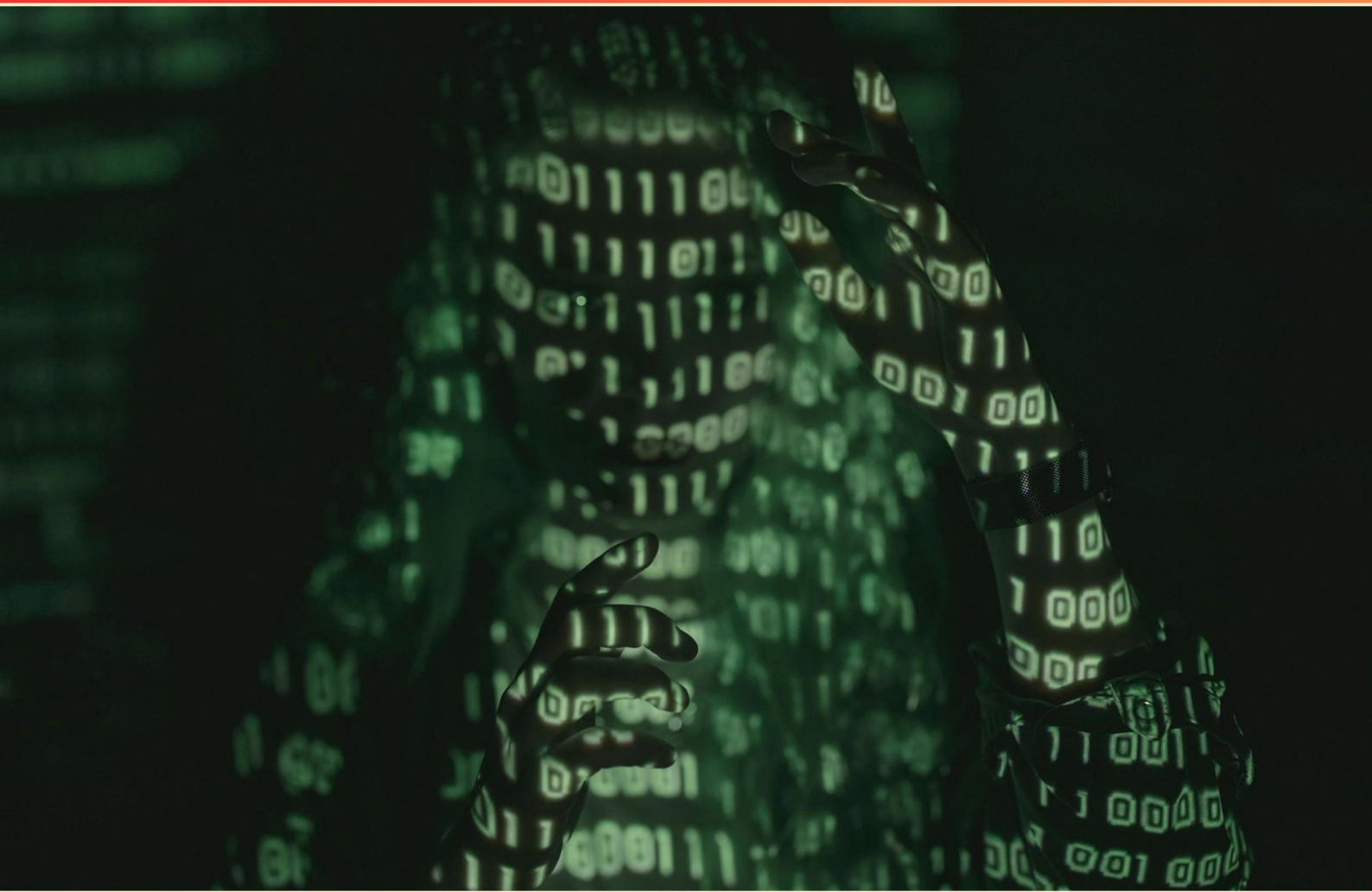


CERTIFIED ETHICAL HACKER 312-50V11 PRACTICE TEST (SAMPLE)

STUDY GUIDE



**SAMPLE STUDY GUIDE
WITH LIMITED QUESTIONS**

**VISIT US ONLINE FOR
THE FULL VERSION STUDY GUIDE**

<https://ceh31250v11.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.

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

SAMPLE

- 1. In the bank security questions scenario, what is the most likely explanation for the compromise?**
 - A. He provided the password
 - B. His computer had a keylogger
 - C. Password brute forcing
 - D. He provided the answers to security questions

- 2. Which tool is commonly used to identify vulnerabilities on Windows systems during security assessments?**
 - A. Nessus
 - B. Nmap
 - C. Metasploit
 - D. Nikto

- 3. What two conditions must a digital signature meet?**
 - A. Has to be the same number of characters as a physical signature and must be unique
 - B. Has to be unforgeable, and has to be authentic
 - C. Must be unique and have special characters
 - D. Has to be legible and neat

- 4. Which layer 3 protocol would provide end-to-end encryption for FTP traffic?**
 - A. IPsec
 - B. SFTP
 - C. SSL
 - D. FTPS

- 5. During the described APT operation, which lifecycle phase is being executed when spear-phishing and exploiting publicly available servers leads to malware deployment and outbound connectivity?**
 - A. Preparation
 - B. Persistence
 - C. Initial intrusion
 - D. Cleanup

- 6. Which hardware on a computer's motherboard stores encryption keys and releases only a portion of the key to prevent decryption on new hardware?**
- A. CPU
 - B. UEFI
 - C. GPU
 - D. TPM
- 7. Which language feature helps prevent buffer overflow by automatically enforcing array bounds?**
- A. Manual memory management
 - B. Built-in bounds checking
 - C. Pointers arithmetic
 - D. Preprocessor macros
- 8. What type of vulnerability assessment is performed when unusual internal network traffic is observed aimed at cracking the authentication mechanism, prompting a test of weak and outdated security controls?**
- A. Application assessment
 - B. Wireless network assessment
 - C. Host-based assessment
 - D. Distributed assessment
- 9. Abel follows the five-tier container technology architecture and is currently verifying image contents, signing images, and sending them to registries. Which tier is this?**
- A. Tier-1: Developer machines
 - B. Tier-3: Registries
 - C. Tier-4: Orchestrators
 - D. Tier-2: Testing and accreditation systems
- 10. Which biometric characteristic is least likely to be used for a large company's access control?**
- A. Height and Weight
 - B. Iris Patterns
 - C. Fingerprints
 - D. Voice

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. In the bank security questions scenario, what is the most likely explanation for the compromise?

- A. He provided the password
- B. His computer had a keylogger
- C. Password brute forcing
- D. He provided the answers to security questions**

Security questions rely on knowledge the user provides. If an attacker is able to obtain or trick the user into giving the answers to those questions, they can often reset or bypass authentication and gain access to the account without needing the actual password or malware on the device. In many bank breach scenarios, social engineering or phishing targets the answers to security questions, making this the most plausible path to compromise. The other options are less likely in this context: a password being given would be a direct credential theft, but the scenario emphasizes exploiting the knowledge-based questions; a keylogger would require malware on the user's machine to capture keystrokes, which is a different vector; brute-forcing the password is typically mitigated by rate limits, account locks, and other protections, making it a less common path for this type of breach.

2. Which tool is commonly used to identify vulnerabilities on Windows systems during security assessments?

- A. Nessus**
- B. Nmap
- C. Metasploit
- D. Nikto

Identifying vulnerabilities on Windows systems during security assessments is best done with a dedicated vulnerability scanner. Nessus performs this role by continuously checking Windows hosts against a large, up-to-date database of known vulnerabilities, missing patches, misconfigurations, and exposure gaps. It can run both authenticated scans (where it logs into the target to verify patch levels and config settings) and unauthenticated scans, producing prioritized results with CVE IDs and actionable remediation steps. This combination of broad coverage, depth of checks for Windows-specific issues, and clear reporting makes it the most effective choice for identifying vulnerabilities across Windows environments. Tools like Nmap are great for discovering hosts and services and can use scripts to hint at issues, but they're not primarily built to catalog and rate vulnerabilities across an entire Windows network. Metasploit focuses on exploiting discovered weaknesses to validate them, which is valuable for proof-of-exploit testing but not for wide-ranging vulnerability identification. Nikto targets web servers for common web-related problems, not general Windows system vulnerabilities.

3. What two conditions must a digital signature meet?

- A. Has to be the same number of characters as a physical signature and must be unique
- B. Has to be unforgeable, and has to be authentic**
- C. Must be unique and have special characters
- D. Has to be legible and neat

Digital signatures rely on public key cryptography to provide trust. The two conditions are that a signature is authentic and unforgeable. Authenticity means the signature proves it was created by the holder of the corresponding private key, tying it to the signer. Unforgeable means no one else can create a valid signature on that message without access to the private key. Together, they ensure the signer's identity can be verified and that the signature cannot be forged, which also guards against tampering since changing the message would cause the signature verification to fail. The other options mix up properties like length, legibility, or "uniqueness," which do not guarantee authenticity or unforgeability in the digital realm.

4. Which layer 3 protocol would provide end-to-end encryption for FTP traffic?

- A. IPsec**
- B. SFTP
- C. SSL
- D. FTPS

IPsec is a network-layer security protocol that protects IP packets as they travel between hosts. By using the Encapsulating Security Payload (ESP), it provides confidentiality, integrity, and authentication for all traffic moving across the network, so FTP traffic (which rides on IP/TCP) is encrypted end-to-end regardless of the application layer specifics. This is why IPsec is the layer 3 choice for securing FTP traffic. SFTP is an application-layer file transfer protocol (SSH-based), so it isn't a layer 3 protocol. SSL/TLS and FTPS secure the transport or application layer connections for particular sessions rather than encrypting the entire IP payload at the network layer, so they don't fulfill the layer 3 end-to-end encryption requirement.

5. During the described APT operation, which lifecycle phase is being executed when spear-phishing and exploiting publicly available servers leads to malware deployment and outbound connectivity?

- A. Preparation
- B. Persistence
- C. Initial intrusion**
- D. Cleanup

Gaining the first foothold in the target environment is being described here. Spear-phishing aims to get a user to reveal credentials or execute malware, giving an entry point, and exploiting publicly available servers to deploy malware and establish outbound connectivity creates the initial connection back to the attacker's infrastructure. Together, these actions define the moment the attacker first enters the network and establishes a foothold, which is the initial intrusion phase. After this, attackers might seek persistence or escalate access, but the scenario centers on gaining that initial entry. Preparation and cleanup describe pre-attack planning or post-operation removal of traces, and persistence refers to maintaining access after entry, not the initial entry itself.

6. Which hardware on a computer's motherboard stores encryption keys and releases only a portion of the key to prevent decryption on new hardware?

- A. CPU
- B. UEFI
- C. GPU
- D. TPM**

The concept here is hardware-based key storage and platform-bound release, realized by the Trusted Platform Module. The TPM is a dedicated chip on the motherboard that securely generates, stores, and uses cryptographic keys. For disk encryption, the actual key material can be held inside the TPM and only released to the operating system under strict conditions that prove the system's integrity. Because the keys are tied to the TPM and to the measured state of the hardware, moving the drive to a different motherboard or altering firmware prevents the TPM from releasing the key, so decryption on new hardware doesn't occur. The idea of releasing only a portion of the key reflects that the key never leaves the TPM in usable form; cryptographic operations happen inside the TPM and only valid, condition-checked results are provided to the OS. Other components like the CPU, GPU, or UEFI don't provide this secure, hardware-bound key storage and verification capability, which is why this hardware is the correct answer.

7. Which language feature helps prevent buffer overflow by automatically enforcing array bounds?

- A. Manual memory management
- B. Built-in bounds checking**
- C. Pointers arithmetic
- D. Preprocessor macros

Automatic bounds checking is the feature that prevents buffer overflow by ensuring array accesses stay within valid indices. Each time you index an array, the language verifies that the index is between 0 and the array length minus one; if it isn't, it raises an error or exception instead of writing past the end of the buffer. This runtime guard stops many overflow scenarios that would otherwise corrupt adjacent memory. Manual memory management and pointer arithmetic don't provide automatic protection; they let you compute addresses and write data without built-in checks, increasing the risk of overruns. Preprocessor macros aren't runtime safeguards either—they're text substitutions that happen before compilation and won't prevent out-of-bounds writes during execution. In languages that enforce bounds automatically, the safety comes from the language's runtime or type system enforcing those checks, reducing the chance of a buffer overflow from ordinary array usage.

8. What type of vulnerability assessment is performed when unusual internal network traffic is observed aimed at cracking the authentication mechanism, prompting a test of weak and outdated security controls?

- A. Application assessment
- B. Wireless network assessment**
- C. Host-based assessment
- D. Distributed assessment

This question is about the security of wireless network authentication controls. When you observe unusual internal traffic aimed at cracking the authentication mechanism, you're looking at weaknesses in how the wireless network authenticates devices and grants access. A wireless network assessment specifically targets these areas—testing for weak or outdated encryption (like older WPA/WEP configurations), weak passphrases, misconfigured authentication settings, WPS issues, and the presence of rogue access points—to determine if the wireless entry point can be compromised. This aligns with a wireless network assessment because it focuses on the protections that govern who can connect to the network and how securely those connections are established. It's not centered on testing application software for bugs, nor on evaluating a single host's security in isolation, and "distributed assessment" isn't the standard term used for targeting wireless authentication controls.

9. Abel follows the five-tier container technology architecture and is currently verifying image contents, signing images, and sending them to registries. Which tier is this?

- A. Tier-1: Developer machines
- B. Tier-3: Registries
- C. Tier-4: Orchestrators
- D. Tier-2: Testing and accreditation systems**

In this scenario, the focus is on validating and certifying container images before they enter the publication stage. Verifying image contents ensures the image has the expected components and hasn't been tampered with, while signing provides a cryptographic guarantee of provenance and integrity. These steps establish trust and policy compliance before an image is allowed into a registry, which is then used for distribution and deployment. This aligns with the testing and accreditation tier, the gatekeeping phase that vets images for quality and security before they're published. Developer machines are where images are created, registries are the storage/publish points, and orchestrators deploy from registries. So performing verification and signing prior to sending to registries sits squarely in the testing and accreditation layer.

10. Which biometric characteristic is least likely to be used for a large company's access control?

A. Height and Weight

B. Iris Patterns

C. Fingerprints

D. Voice

Biometric access control relies on traits that are distinctive and stable over time so a system can reliably identify who someone is. Height and weight don't fit well here because they aren't unique to individuals—many people share similar heights or body sizes—and they can change over time with weight fluctuations, posture, clothing, or health. That makes them unreliable as a primary identifier for access control, leading to higher error rates. In contrast, iris patterns and fingerprints are highly unique to each person and remain stable for long periods, which is why they're common choices for secure entry systems. Voice can also be used in some environments, though it's more sensitive to ambient conditions and certain spoofing risks. So, height and weight are the least suitable biometric characteristics for a large company's access control due to their lack of distinctiveness and stability.

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://ceh31250v11.examzify.com>

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

SAMPLE