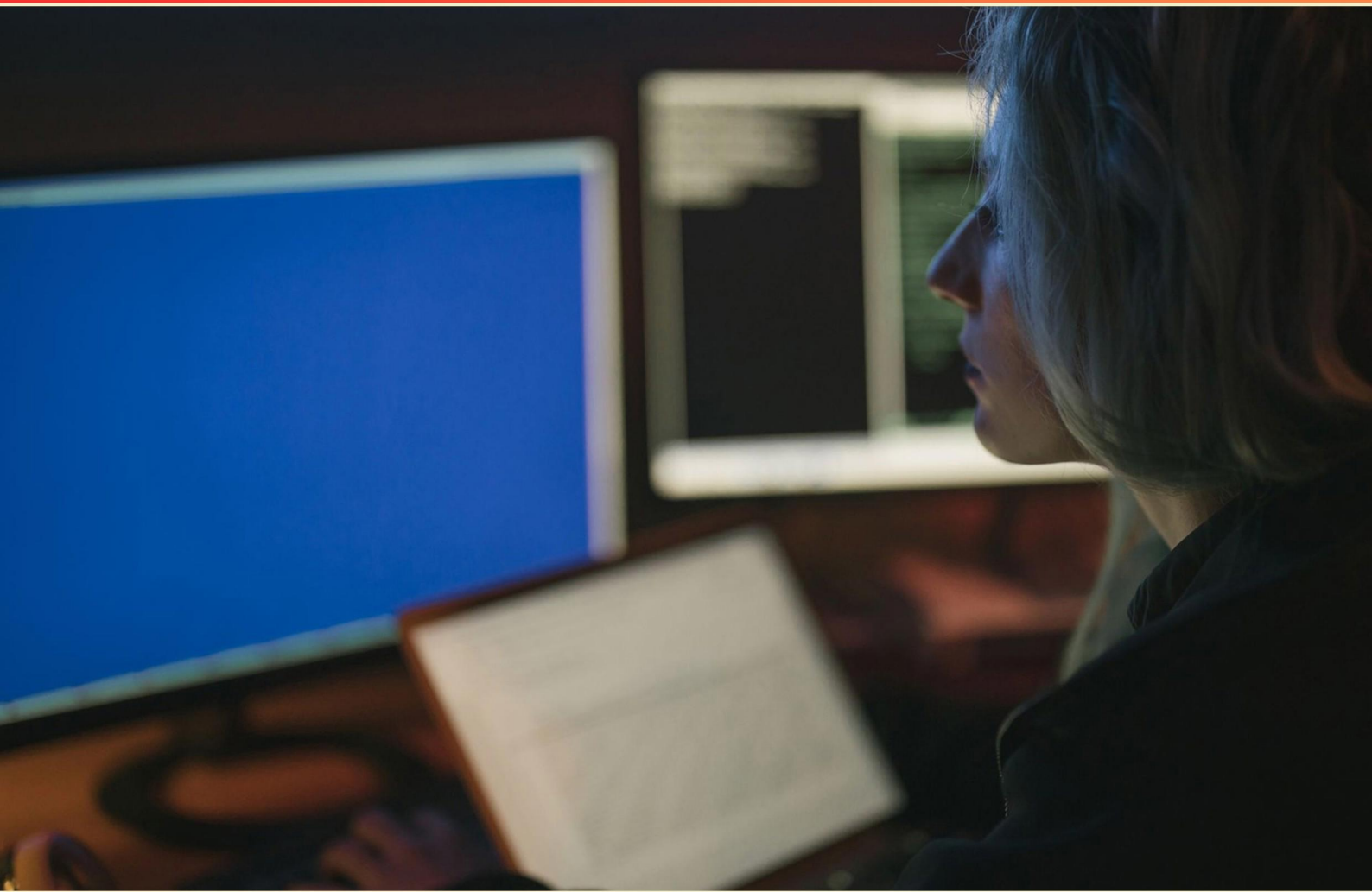


GIAC CERTIFIED INCIDENT HANDLER (GCIH) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



**SAMPLE STUDY GUIDE
WITH LIMITED QUESTIONS**

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

<https://gcihincidenthandler.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	15

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. Second-generation OS fingerprinting uses which characteristics?**
 - A. Initial TTL values
 - B. ICMP codes
 - C. TLS patterns
 - D. Initial TTL, IP ID sequence numbers, and initial TCP window size
- 2. Which of the following is a defense against SQL injection?**
 - A. Limit the permissions of the web app when accessing the database
 - B. Use symmetric encryption for data at rest
 - C. Disable server logging
 - D. Use untrusted external libraries
- 3. Which security tool is cited as capable of mitigating XSS on Apache?**
 - A. Mod_Security for Apache
 - B. Nginx
 - C. IIS URL Rewrite
 - D. Cloudflare WAF
- 4. Password cracking is best described as?**
 - A. Obtain password
 - B. Determining a password when you only have the cipher text representations
 - C. Find valid userID
 - D. Encrypt to see if there is a match
- 5. Which statement about Wellenreiter's development status is true?**
 - A. It is still in development
 - B. It requires a paid license
 - C. No longer in development
 - D. It only runs on Windows
- 6. Which statement about the Warhol/Flash technique is true?**
 - A. It uses a single victim per worm
 - B. Attacker pre-scans the internet for vulnerable machines and preprograms the worm with the first set of victims, and then infected systems continue the worm
 - C. The technique relies on email phishing to spread
 - D. Infected machines are immune after infection

- 7. FlOp analysis is performed on what to identify traffic flow?**
- A. Packet capture file
 - B. Live traffic stream
 - C. DNS logs
 - D. ARP cache
- 8. Which action helps defend against rogue access points in war driving?**
- A. Increase SSID broadcast strength
 - B. Remove renegade access points
 - C. Disable VPN
 - D. Enable WEP encryption
- 9. What does SYSKEY do?**
- A. cannot be used on Windows systems
 - B. adds 128-bit encryption of the SAM database
 - C. logs all password attempts to a central server
 - D. disables SAM database encryption
- 10. During the Preparation phase of Whois reconnaissance defenses, what is a recommended practice?**
- A. Have real contact information with up-to-date records
 - B. Use fake contact information
 - C. Disable WHOIS altogether
 - D. Route WHOIS through anonymizers

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Second-generation OS fingerprinting uses which characteristics?

- A. Initial TTL values
- B. ICMP codes
- C. TLS patterns
- D. Initial TTL, IP ID sequence numbers, and initial TCP window size**

Second-generation OS fingerprinting relies on how a host's TCP/IP stack behaves across several observable fields, not just one. By looking at the initial TTL, the pattern of IP ID sequence numbers, and the initial TCP window size together, you get a multi-faceted fingerprint that more reliably distinguishes operating systems. Each field reflects a different aspect of the stack's implementation, and while network devices can affect a single value, the combination of these three characteristics tends to stay distinctive for a given OS family. TLS patterns or ICMP codes don't provide this kind of multi-field stack fingerprinting: TLS relates to secure handshakes and server configuration, not the host's IP/TCP stack, and ICMP codes alone don't capture the broader stack behavior used in second-generation fingerprinting.

2. Which of the following is a defense against SQL injection?

- A. Limit the permissions of the web app when accessing the database**
- B. Use symmetric encryption for data at rest
- C. Disable server logging
- D. Use untrusted external libraries

Limiting the permissions of the web app's database account is a primary defense against SQL injection because it enforces the principle of least privilege. If an attacker manages to inject malicious SQL, the database user used by the application should only have the minimal rights needed for normal operation, such as reading certain tables or updating specific rows. It should not have rights to drop tables, modify schemas, or execute administrative commands. This containment greatly reduces the potential damage even when an injection succeeds, which is why it's such a strong defensive measure. Other options don't address the injection risk directly. Encrypting data at rest protects data if the storage is accessed, but it doesn't stop or limit what an injected query can do during execution. Disabling server logging removes critical visibility for detecting and responding to attacks. Relying on untrusted external libraries can introduce new vulnerabilities and doesn't fix the injection flaw itself.

3. Which security tool is cited as capable of mitigating XSS on Apache?

- A. Mod_Security for Apache**
- B. Nginx
- C. IIS URL Rewrite
- D. Cloudflare WAF

Mitigating XSS at the server level relies on a Web Application Firewall that can inspect and block malicious input before it reaches the application. Mod_Security for Apache is a WAF module that plugs directly into the Apache HTTP server, allowing you to enforce rule sets that detect and block cross-site scripting attempts in requests and responses. By inspecting parameters, headers, and bodies, it can stop reflected and stored XSS in real time and provide detailed logging for forensics and tuning. While other options serve important roles in web infrastructure, they don't integrate with Apache in the same way: Nginx is a different web server (and would require its own configuration or a separate WAF layer), IIS URL Rewrite is focused on URL manipulation within Windows IIS, and Cloudflare WAF operates at the edge rather than as an Apache module. Therefore, Mod_Security for Apache is the best fit for mitigating XSS directly on an Apache server.

4. Password cracking is best described as?

- A. Obtain password
- B. Determining a password when you only have the cipher text representations**
- C. Find valid userID
- D. Encrypt to see if there is a match

Password cracking is about determining the actual password when you only have the stored, transformed form of it (the cipher text representations such as hashes). The attacker doesn't decrypt something back to plaintext; instead, they generate candidate passwords, apply the same transformation (hashing with the correct algorithm and salt), and check if the result matches the stored value. When a match is found, the plaintext password is recovered. This offline, guess-and-test process—often via brute force or dictionary attacks—is what defines password cracking. That's why this option is the best description: it explicitly captures the idea of deriving the password from its cipher text representations. The other ideas don't match the typical process: obtaining a password directly is not what cracking involves; locating a valid user ID isn't about recovering the password; and simply encrypting to see if there's a match describes a different workflow (encryption-based checking) rather than recovering the plaintext password from its stored form.

5. Which statement about Wellenreiter's development status is true?

- A. It is still in development
- B. It requires a paid license
- C. No longer in development**
- D. It only runs on Windows

Understanding a software project's status helps you interpret what its future looks like. When a project is no longer in development, active work has stopped: no new features, no regular bug fixes, and often no new releases. It may be labeled as archived or end-of-life, and you shouldn't expect ongoing support. This is why saying Wellenreiter is no longer in development is the best answer—the statement aligns with the project being effectively inactive or discontinued. You can usually verify this by looking for signs like no recent commits or releases, an official end-of-life note from the maintainers, or documentation stating it's in maintenance or archived mode. The other possibilities—ongoing development, requiring a paid license, or running only on Windows—would typically come with indicators such as recent development activity, licensing requirements stated in the terms, or platform-specific documentation, which aren't implied by the given status.

6. Which statement about the Warhol/Flash technique is true?

- A. It uses a single victim per worm
- B. Attacker pre-scans the internet for vulnerable machines and preprograms the worm with the first set of victims, and then infected systems continue the worm
- C. The technique relies on email phishing to spread**
- D. Infected machines are immune after infection

Warhol/Flash spreads primarily through social engineering via email, you can think of it as relying on users to click a malicious link or open a harmful attachment in a phishing message. Once a user is tricked into executing the payload, the malware can install and then use the infected machine to propagate further—often by sending itself to contacts found in the victim's address book or by leveraging the user's email capabilities. This phishing-based approach explains why the technique is described as a spread method rooted in tricking people rather than relying on automated network scanning or a fixed list of pre-seeded victims. The idea that infected machines become immune after infection isn't accurate, and the other options describe propagation methods (like pre-scanned victims or a single victim per worm) that don't match the phishing-driven pattern.

7. FlOp analysis is performed on what to identify traffic flow?

- A. Packet capture file**
- B. Live traffic stream
- C. DNS logs
- D. ARP cache

FlOp analysis for identifying traffic flow relies on the actual captured network traffic data. A packet capture file (pcap) contains the raw frames with precise timestamps, source and destination IPs and ports, protocols, and even payloads. This detailed record lets you reconstruct conversations, measure flow characteristics (such as duration, bytes transferred, and inter-arrival times), and spot patterns like unusual bursts or beaconing. While analyzing a live traffic stream can also reveal flows in real time, a saved packet capture provides a reproducible, analyzable dataset that is standard for this kind of flow analysis. DNS logs show domain queries, not the full traffic relationships between hosts, and ARP cache only maps IPs to MAC addresses without describing ongoing traffic flows. Thus, the packet capture file is the appropriate data source for identifying traffic flow.

8. Which action helps defend against rogue access points in war driving?

- A. Increase SSID broadcast strength
- B. Remove renegade access points**
- C. Disable VPN
- D. Enable WEP encryption

Rogue access points are unauthorized wireless devices that show up in a network area, often discovered during war driving. The defense is to detect and remove these renegade APs so they can't be used to intercept traffic or impersonate the legitimate network. Removing renegade access points directly eliminates the threat source and strengthens control over wireless access. Other options don't address the problem effectively. Increasing the SSID broadcast strength merely makes networks more visible and doesn't remove the rogue device. Disabling VPN doesn't tackle rogue APs and shifts the focus away from wireless control. Enabling WEP encryption is outdated and insecure; it doesn't prevent rogue APs and can give a false sense of security.

9. What does SYSKEY do?

- A. cannot be used on Windows systems
- B. adds 128-bit encryption of the SAM database**
- C. logs all password attempts to a central server
- D. disables SAM database encryption

SYSKEY is designed to protect the SAM database by encrypting it with a 128-bit key. The SAM stores password hashes, and applying strong encryption to that database adds a protective layer so that, if the SAM file is obtained, the hashes aren't easily readable without decrypting the data. This is what the option describing 128-bit encryption of the SAM database is conveying. The other statements don't match SYSKEY's function: it isn't about logging password attempts, it isn't something that prevents Windows from running, and it doesn't disable SAM encryption.

10. During the Preparation phase of Whois reconnaissance defenses, what is a recommended practice?

- A. Have real contact information with up-to-date records**
- B. Use fake contact information
- C. Disable WHOIS altogether
- D. Route WHOIS through anonymizers

Keeping WHOIS records accurate and up to date is essential when preparing defenses against Whois reconnaissance. Real, current contact information ensures there is a reliable channel to receive abuse reports, verify domain ownership, and coordinate with the registrar or law enforcement if necessary. This makes it possible to quickly respond to potential abuse or social engineering attempts that rely on public registration data, and it supports proper accountability and governance around the domain. Using fake contact information undermines incident response and ownership verification—the legitimate contacts may never be reached, delaying takedowns, disputes, or notifications to the right people. Disabling WHOIS or routing it through anonymizers reduces transparency and makes it harder to manage abuse, enforce policies, and comply with registrar requirements, which is counterproductive for defense.

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://gcihincidenthandler.examzify.com>

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

SAMPLE