Computer Hacking Forensic Investigator (CHFI) v11 Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

Table of Contents

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

1. Routers operate at which layer of the OSI model?

- A. 4
- B. 3
- C. 1
- D. 5

2. Which step is essential before presenting evidence in court?

- A. Certification of authenticity
- B. Deleting logs
- C. Modifying evidence
- D. Copying to local drive

3. In a DHCP-enabled network, which logs should you examine to determine which system (MAC address) held a specific IP address at a given time?

- A. On the ARP cache of an individual host
- B. In the Web Server log files
- C. In the DHCP Server log files
- D. There is no way to determine the specific IP address

4. Which organization serves as the certifying body for forensic laboratories?

- A. ASCLD
- B. ISFL
- C. AFLS
- D. AFLCF

5. Which technique involves manually typing different user IDs into logging tools, suggesting tampering?

- A. Parameter tampering
- B. Cross site scripting
- C. SQL injection
- D. Cookie Poisoning

6. **What information can be obtained from DHCP logs?**

   A. **The operating system of the attacker and victim computers**

   B. **IP traffic between the attacker and the victim**

   C. **MAC address of the attacker**

   D. **If any computers on the network are running in promiscuous mode**

7. **What is the first step required when preparing a computer for forensics investigation?**

   A. **Do not turn the computer off or on, run any programs, or attempt to access data on a computer**

   B. **Secure any relevant media**

   C. **Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at Issue**

   D. **Identify the type of data you are seeking, the information you are looking for, and the urgency level of the examination**

8. **Which statement about a Fraggle attack is correct?**

   A. **It uses ICMP**

   B. **It uses TCP**

   C. **It uses UDP**

   D. **It uses HTTP**

9. **In echo data hiding, the secret message is embedded into which element as an echo?**

   A. **Phase spectrum of a digital signal**

   B. **Pseudo-random signal**

   C. **Pseudo-spectrum signal**

   D. **Cover audio signal**

10. **Which action is performed by the fdisk utility on a Linux system?**

   A. **Create partitions**

   B. **Install a filesystem**

   C. **Mount a filesystem**

   D. **Set permissions**

Answers

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

Explanations

1. Routers operate at which layer of the OSI model?

A. 4

B. 3

C. 1

D. 5

Routers forward traffic between different networks by examining the destination IP address and using routing tables to decide the next hop. That ability sits squarely in the Network Layer, Layer 3 of the OSI model. The IP header carries logical addressing that routers use to determine where a packet should go next, enabling inter-network communication. In contrast, Layer 1 covers the physical transmission media, Layer 2 handles local switching with MAC addresses, and Layer 4 concerns transport protocols and ports. Some devices or features may touch other layers (for example, firewalls or NAT affecting higher layers), but the fundamental routing function—deciding the path to a destination using IP addresses—is a Layer 3 activity.

2. Which step is essential before presenting evidence in court?

A. Certification of authenticity

B. Deleting logs

C. Modifying evidence

D. Copying to local drive

Establishing authenticity is essential before evidence is presented in court. This means showing that the digital evidence is exactly what was seized, has not been altered, and is properly accounted for from the moment of collection through to presentation. The certification of authenticity typically involves a documented chain of custody and forensic verification, such as hashing the data to prove integrity and maintaining records of every person who handled the evidence, what was done to it, and when. Courts rely on this certification to trust that the evidence is reliable and admissible. Deleting logs or modifying evidence would destroy integrity and undermine admissibility, so those actions are inappropriate. Copying to a local drive might be part of the handling process, but by itself does not guarantee admissibility without proper authentication and a verified chain of custody.

3. In a DHCP-enabled network, which logs should you examine to determine which system (MAC address) held a specific IP address at a given time?

A. On the ARP cache of an individual host

B. In the Web Server log files

C. In the DHCP Server log files

D. There is no way to determine the specific IP address

DHCP servers keep a lease database that ties each leased IP to a specific device's MAC address, along with the time the lease started and ended. To figure out which system held a particular IP at a given moment, you need to inspect the DHCP server logs because they record the assignment events and the exact MAC-IP mapping with timestamps. The ARP cache on a single host is local and often fleeting, so it doesn't reliably show who had the IP at a past time across the network. Web server logs only show which IPs connected to the server, not the MAC addresses or the historical lease details. Therefore, DHCP server logs provide the authoritative record needed to determine the MAC address associated with an IP at a specific time.

4. Which organization serves as the certifying body for forensic laboratories?

A. ASCLD

B. ISFL

C. AFLS

D. AFLCF

In forensic science, a lab earns formal recognition through a dedicated accrediting body that audits and validates the lab's quality systems and technical competence. ASCLD, the American Society of Crime Laboratory Directors, oversees the accreditation program (historically known as ASCLD/LAB) that evaluates whether a forensic laboratory meets established standards for management, personnel qualifications, method validation, QA/QC, proficiency testing, and proper record-keeping. This makes ASCLD the recognized certifying body for forensic laboratories, signaling that the lab operates to consistent, credible standards. The other organizations listed do not serve as the primary certifying authority for forensic labs in this context.

5. Which technique involves manually typing different user IDs into logging tools, suggesting tampering?

A. Parameter tampering

B. Cross site scripting

C. SQL injection

D. Cookie Poisoning

Manipulating the identifiers that the application uses to control access. When a web app relies on a parameter like a user ID in requests to fetch data, an attacker can manually change that value to try to access someone else's information. This direct alteration of input parameters to influence server behavior is known as parameter tampering. It's distinct from injecting scripts (XSS), injecting SQL commands (SQL injection), or corrupting cookies (cookie poisoning), because those techniques involve code execution, database commands, or manipulating stored session data, not simply changing a request's parameter values to spoof identity. The core idea is that trust is placed in data sent by the client, so server-side validation and proper authorization checks are essential to defend against this.

6. What information can be obtained from DHCP logs?

A. The operating system of the attacker and victim computers

B. IP traffic between the attacker and the victim

C. MAC address of the attacker

D. If any computers on the network are running in promiscuous mode

DHCP logs focus on the DHCP transaction and tie it to the client's hardware address. When a device joins the network, it sends a DHCP Discover that includes its MAC address, and the DHCP server records that MAC along with the IP it offers, the IP it eventually leases, lease duration, and timestamps. Because the MAC is part of each log entry, you can identify which device requested a lease and link activity to that specific device on the network. OS details, actual IP traffic between devices, and NIC states like promiscuous mode aren't provided by DHCP logs; those require other sources such as OS fingerprints, packet captures, or monitoring tools.

7. What is the first step required when preparing a computer for forensics investigation?

A. Do not turn the computer off or on, run any programs, or attempt to access data on a computer

B. Secure any relevant media

C. Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at Issue

D. Identify the type of data you are seeking, the information you are looking for, and the urgency level of the examination

Preserving evidence in its original state is the priority. The moment you start interacting with the device—turning it on or off, running programs, or accessing data—you risk altering data, changing timestamps, overwriting memory, or otherwise contaminating the evidence. Keeping the computer untouched ensures the integrity of the data and supports a reliable chain of custody, making it possible to create an admissible forensic image later. After establishing this baseline, you would proceed with proper steps like securing the relevant media and documenting the scene, but those actions should follow the decision to avoid any modification of the system.

8. Which statement about a Fraggle attack is correct?

A. It uses ICMP

B. It uses TCP

C. It uses UDP

D. It uses HTTP

Fraggle is the UDP-based amplification attack. Like Smurf, it uses spoofed source addresses to trigger responses from a broadcast network, but it does so with UDP services rather than ICMP. An attacker sends a flood of UDP datagrams to a broadcast address targeting services such as UDP echo or chargen. Each host on the broadcast network replies to the spoofed source (the victim), producing a large volume of UDP responses directed at the victim. Because UDP is connectionless and lacks a handshake, spoofing the sender’s address is straightforward and the responses multiply, leading to the flood. This is why the statement that Fraggle uses UDP is the correct one. It’s not about ICMP, TCP, or HTTP—the mechanism relies on UDP-based reflection and amplification.

9. In echo data hiding, the secret message is embedded into which element as an echo?

A. Phase spectrum of a digital signal

B. Pseudo-random signal

C. Pseudo-spectrum signal

D. Cover audio signal

In echo data hiding, the secret message is carried by modifying the original audio itself. You create a delayed, attenuated copy of the cover audio and add it back to the original signal. This superimposed echo contains the encoded bits, so the hidden data resides in the cover audio signal. The other options refer to spectral components or separate signals, but the technique uses the actual audio waveform as the carrier, with the echo serving as the data-carrying feature. Detecting the message involves analyzing the echo pattern—its delay and amplitude—within the cover audio.

10. Which action is performed by the fdisk utility on a Linux system?

A. Create partitions

B. Install a filesystem

C. Mount a filesystem

D. Set permissions

fdisk is a partition editor. It directly edits the partition table on a disk, letting you create new partitions, delete them, change their type, or toggle boot flags. Creating partitions is the action fdisk is designed to perform, which is why it’s the correct choice. Note that installing or setting up a filesystem is a separate step done with a tool like mkfs, mounting a filesystem is done with mount (and fstab), and setting permissions affects files inside a mounted filesystem, not the partition table itself.

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://chfiv11.examzify.com

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