Computer Hacking Forensic Investigator (CHFI) Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

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

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

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

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. **What is an important characteristic of forensic evidence?**
   - **A. It must be collected without regard to legality**
   - **B. It should remain unchanged from its original state**
   - **C. It can be publicly shared without restrictions**
   - **D. It is only relevant in criminal cases**

2. **Which type of passwords are transmitted in clear text over networks?**
   - **A. Clear text passwords**
   - **B. Obfuscated passwords**
   - **C. Hashed passwords**
   - **D. Hex passwords**

3. **What is the definition of cyber-crime?**
   - **A. Any illegal act involving technology**
   - **B. Any illegal act involving a gun**
   - **C. Web-based illegal acts**
   - **D. Acts committed by organized crime groups**

4. **What is NOT correct when documenting an electronic crime scene?**
   - **A. Document the physical scene**
   - **B. Document related electronic components**
   - **C. Record the power status of the computer**
   - **D. Write down the color of the suspect's clothing**

5. **What does the acronym IMEI stand for?**
   - **A. International Mobile Equipment Identity**
   - **B. Internal Mobile Equipment Identity**
   - **C. International Multiple Equipment Identity**
   - **D. International Media Equipment Identification**

6. Which method of Wi-Fi mapping involves creating symbols in public places to identify open Wi-Fi networks?

- **A. WarWalking**
- **B. WarFlying**
- **C. WarChalking**
- **D. WarDriving**

7. What type of network attack involves overwhelming a mailbox with excessive emails?

- **A. Email spamming**
- **B. Mail bombing**
- **C. Phishing**
- **D. Email spoofing**

8. What does 'social engineering' in the context of cybersecurity mean?

- **A. Taking advantage of social networks**
- **B. Manipulating people to gain sensitive information**
- **C. Creating social media campaigns for awareness**
- **D. Using social skills for team collaboration**

9. What is a primary function of tasklist in a Windows operating system?

- **A. To map network drives**
- **B. To list currently running processes**
- **C. To display network statistics**
- **D. To configure user accounts**

10. Which of the following represents a common form of data encryption?

- **A. MD5 hashing**
- **B. AES encryption**
- **C. Base64 encoding**
- **D. Hexadecimal conversion**

Answers

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

Explanations

1. What is an important characteristic of forensic evidence?

A. It must be collected without regard to legality

B. It should remain unchanged from its original state

C. It can be publicly shared without restrictions

D. It is only relevant in criminal cases

An important characteristic of forensic evidence is that it should remain unchanged from its original state. This integrity is crucial for ensuring that the evidence is credible and can stand up in court. If the evidence is altered or tampered with, it may be deemed inadmissible or unreliable in judicial proceedings. The preservation of the authenticity of forensic evidence allows forensic investigators to accurately represent the findings, maintain the chain of custody, and support the legal process effectively. Collecting evidence in a way that disregards legality compromises its integrity and can lead to legal challenges. Similarly, while certain types of forensic evidence may eventually be shared, there are often strict regulations regarding confidentiality and the handling of sensitive information that protect the rights of individuals involved. Lastly, forensic evidence is relevant in various contexts and not limited strictly to criminal cases; for instance, it can also play a role in civil litigation and corporate investigations.

2. Which type of passwords are transmitted in clear text over networks?

A. Clear text passwords

B. Obfuscated passwords

C. Hashed passwords

D. Hex passwords

Clear text passwords are indeed transmitted in clear text over networks, meaning they are sent without any encryption or transformation that would obscure their content. This makes them vulnerable to interception by anyone monitoring the network traffic. When passwords are transmitted in this manner, any user with access to the communication channel can easily read and capture them, which poses a significant security risk. In contrast, obfuscated passwords typically involve some form of encoding or masking that makes them less readable, though not necessarily secure. Hashed passwords undergo a transformation to create a fixed-size string that obscures the original password, but they are not suitable for transmission as-is since they cannot be easily reversed unless additional information is provided. Hex passwords, while potentially part of a representation format, do not imply that the passwords are secure in transit and can also be vulnerable. Thus, the characteristic of clear text passwords being sent without any protective measures is what makes them the correct identification in this context.

3. What is the definition of cyber-crime?

A. Any illegal act involving technology

B. Any illegal act involving a gun

C. Web-based illegal acts

D. Acts committed by organized crime groups

The definition of cyber-crime encompasses a broad range of illegal activities that involve technology. This includes crimes such as hacking, identity theft, online fraud, and distribution of malicious software. The essence of cyber-crime lies in the use of computers or the internet to engage in activities that violate laws or regulations. While options like web-based illegal acts or acts committed by organized crime groups could be aspects of cyber-crime, they do not capture the complete scope of the term. Cyber-crime is not limited to online activities or specific groups; it includes any illegal act that occurs within the realm of technology, making the first choice the most comprehensive and accurate definition.

4. What is NOT correct when documenting an electronic crime scene?

A. Document the physical scene

B. Document related electronic components

C. Record the power status of the computer

D. Write down the color of the suspect's clothing

When documenting an electronic crime scene, the focus is primarily on gathering information that is relevant to the technology involved and the crime being investigated. Documenting the physical scene, related electronic components, and the power status of the computer are all crucial steps to ensure a thorough record of the environment in which the cybercrime occurred. Recording the power status of the computer helps forensic investigators understand whether the device was actively in use, shut down, or potentially being tampered with at the time the crime was committed. Additionally, documenting electronic components provides critical context for the investigation, such as identifying devices that may contain evidence or further elucidate the methods used by the perpetrator. In contrast, writing down the color of the suspect's clothing does not pertain directly to the electronic evidence and, therefore, is not a necessary component of documenting the electronic crime scene. While such details may be relevant in a broader criminal investigation, they fall outside the scope of best practices for documentation focused on electronic components and digital evidence, which is the primary objective in this context.

5. What does the acronym IMEI stand for?

A. International Mobile Equipment Identity

B. Internal Mobile Equipment Identity

C. International Multiple Equipment Identity

D. International Media Equipment Identification

The acronym IMEI stands for International Mobile Equipment Identity. This unique number is assigned to mobile devices and serves as a way to identify them on a mobile network. Each IMEI number is specific to a single device, which helps carrier networks to ensure that only legitimate devices can connect to their services. The IMEI can be used for various purposes, such as tracking stolen devices or identifying a mobile phone when reporting it lost. Understanding what IMEI represents is crucial, especially in the context of cybersecurity and mobile device management, where ensuring device authenticity and tracking is vital for preventing unauthorized access and misuse. The other options, while containing aspects of the correct definition, do not accurately represent the established and widely accepted meaning of the IMEI.

6. Which method of Wi-Fi mapping involves creating symbols in public places to identify open Wi-Fi networks?

A. WarWalking

B. WarFlying

C. WarChalking

D. WarDriving

The method of Wi-Fi mapping that involves creating symbols in public places to identify open Wi-Fi networks is known as WarChalking. This practice includes marking specific symbols on sidewalks or walls to indicate the presence and status of wireless networks. These symbols are often used to communicate whether a network is secure, unsecured, or requires specific access credentials. WarChalking emerged as a way to document and share information about accessible Wi-Fi networks, making it easier for users to find connections in urban areas. The other methods listed, while related to the exploration and mapping of Wi-Fi networks, do not involve the act of symbolically marking locations. WarDriving, for instance, refers to driving around in a vehicle while collecting data on Wi-Fi networks, often visualized using GPS technology. WarFlying involves using drones to discover wireless networks from the air, and WarWalking is similar to WarDriving but typically done on foot without the mobility of a vehicle. Thus, WarChalking specifically stands out for its unique aspect of using physical symbols to communicate information about Wi-Fi networks in public spaces.

7. What type of network attack involves overwhelming a mailbox with excessive emails?

A. Email spamming

B. Mail bombing

C. Phishing

D. Email spoofing

Mail bombing refers to a specific type of network attack where an individual's email account is inundated with an excessive number of emails in a very short period, causing potential disruption and preventing the user from accessing their legitimate emails. This tactic can overload the recipient's mailbox, leading to service denial or making email management impossible. While email spamming does involve sending bulk unsolicited emails, it does not necessarily focus on overwhelming a specific mailbox to the extent that mail bombing does. Phishing involves tricking individuals into providing sensitive information, and email spoofing is a tactic used to forge the sender's address to make emails appear legitimate. These concepts, although related to email security, do not specifically describe the act of flooding a mailbox as mail bombing does.

8. What does 'social engineering' in the context of cybersecurity mean?

A. Taking advantage of social networks

B. Manipulating people to gain sensitive information

C. Creating social media campaigns for awareness

D. Using social skills for team collaboration

Social engineering, in the context of cybersecurity, refers to the psychological manipulation of individuals to gain confidential or sensitive information, such as login credentials or personal data. This technique exploits human psychology rather than technical hacking strategies, making it particularly challenging to defend against since it often relies on trust, fear, or other emotional triggers. While taking advantage of social networks can be a component of social engineering tactics, it does not encompass the full breadth of what social engineering entails, which is primarily the manipulation of individuals themselves to extract information. Similarly, creating social media campaigns for awareness is focused on promoting safety rather than exploiting vulnerabilities, and using social skills for team collaboration is more about effective communication in a professional environment rather than gaining unauthorized access to information. The essence of social engineering lies in its ability to deceive individuals into revealing information they otherwise might not share, making the manipulation of people to gain sensitive information the most accurate definition.

9. What is a primary function of tasklist in a Windows operating system?

A. To map network drives

B. To list currently running processes

C. To display network statistics

D. To configure user accounts

The primary function of tasklist in a Windows operating system is to list currently running processes. This command provides a snapshot of all active processes, including their Process ID (PID), session number, and memory usage, which is critical for system monitoring, troubleshooting, and management. Being able to see which processes are currently running on a system helps users and administrators identify resource-hogging applications, potential malware, or any unexpected applications that may be consuming system resources. The tasklist command offers a command-line interface alternative to the graphical Task Manager, making it useful for remote management and automation through scripts. Other options such as mapping network drives, displaying network statistics, and configuring user accounts serve entirely different purposes and do not relate to process management or monitoring on a Windows system.

10. Which of the following represents a common form of data encryption?

A. MD5 hashing

B. AES encryption

C. Base64 encoding

D. Hexadecimal conversion

The correct choice represents a widely recognized and robust form of encryption. AES (Advanced Encryption Standard) is a symmetric encryption algorithm that encrypts data in fixed block sizes (typically 128 bits) using key sizes of 128, 192, or 256 bits. It uses the same key for both encryption and decryption, making it efficient for securing sensitive information. AES is widely adopted across various industries due to its security strength and performance, and it is often the encryption standard used for data protection in government, financial, and personal applications. While MD5 hashing is often mentioned in discussions about data security, it is actually a hashing algorithm rather than an encryption method, and it is not suitable for data encryption because it is a one-way function. Base64 encoding is primarily used for encoding binary data into ASCII text format and does not provide encryption; it merely allows for data representation. Hexadecimal conversion entails representing binary data in a human-readable format, which does not provide security or confidentiality. Thus, AES encryption stands out as an appropriate choice for data encryption, ensuring the confidentiality and integrity of data.

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://chfi.examzify.com

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