EC-Council Certified Incident Handler (ECIH) Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

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. **What function does a UBA (User Behavior Analytics) tool typically provide?**

   A. Monitoring user behavior for anomalies

   B. Data encryption for sensitive data

   C. Network traffic analysis

   D. System performance optimization

2. **What is the name of the email service platform by Novell NetWare that stores messages in proprietary databases?**

   A. GroupWise

   B. NovelWise

   C. GroupSmart

   D. Yesware

3. **What's a common indicator of a potential insider threat?**

   A. Exploiting external network vulnerabilities

   B. Unauthorized access to sensitive files

   C. Increased network traffic from unknown sources

   D. Frequent system downtime

4. **What security strategy is characterized by multilayered protection to minimize attacks on organizational assets?**

   A. Three-way handshake

   B. Likelihood analysis

   C. Covert channel

   D. Defense-in-depth

5. **Which step is NOT part of securing computer networks against insider threats?**

   A. Configuring firewalls

   B. Allowing open file sharing

   C. Monitoring outbound HTTP and HTTPS traffic

   D. Reducing transfers to authorized users

6. Hexagon received many malformed TCP/IP packets, causing their main server to crash. Which type of attack did the adversary use?

A. DoS attack

B. Session Hijacking

C. Man-in-the-Middle

D. Cross-Site-Scripting

7. Which type of security misconfiguration vulnerability supports weak algorithms and uses expired or invalid certificates, exposing users' data to untrusted third parties?

A. Parameter / form tampering

B. Improper error handling

C. Unvalidated inputs

D. Insufficient transport layer protection

8. What is a disadvantage of using Platform-as-a-Service (PaaS)?

A. All of these choices are correct.

B. Scalability

C. Prebuilt business functionality

D. Data privacy

9. Which of the following is an indication of unauthorized use of a standard user account?

A. Use of a secret account

B. Alert of network and host IDS

C. Misplaced hardware parts

D. Increase in the usage of resources

10. Temporary shutdown and restoration of the infected system are common techniques in which stage of incident response?

A. Preparation

B. Containment

C. Recovery

D. Identification

Answers

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

Explanations

1. What function does a UBA (User Behavior Analytics) tool typically provide?

A. Monitoring user behavior for anomalies

B. Data encryption for sensitive data

C. Network traffic analysis

D. System performance optimization

User Behavior Analytics (UBA) tools are specifically designed to monitor and analyze user behavior within a network. The primary function of these tools is to identify patterns of normal activity based on historical data and then flag any anomalies that deviate from this established baseline. This capability is crucial for detecting potential security threats, including insider threats, compromised accounts, and other malicious activities that may not be caught by traditional security measures. By focusing on user behavior, UBA tools can provide organizations with valuable insights into interactions with data and applications, further enhancing the ability to respond to suspicious activities swiftly. This proactive monitoring approach is essential for maintaining security in today's dynamic digital environments, where user actions can indicate a significant risk to organizational assets.

2. What is the name of the email service platform by Novell NetWare that stores messages in proprietary databases?

A. GroupWise

B. NovelWise

C. GroupSmart

D. Yesware

The email service platform by Novell NetWare that stores messages in proprietary databases is called GroupWise. This solution was developed to provide email, calendaring, task management, and other collaborative features in a unified interface, specifically targeting enterprise environments. GroupWise uses a unique database structure to store messages, which enhances its organization and retrieval capabilities compared to more traditional mail systems. This proprietary data management approach allows for advanced features such as email threading and enhanced security. The other options do not accurately represent Novell's email service. NovelWise and GroupSmart do not exist as recognized email platforms, while Yesware is a tool designed primarily for sales professionals that helps with email tracking and productivity but is not affiliated with Novell NetWare or its messaging services. Thus, GroupWise stands out as the correct answer given its established role in Novell's suite of enterprise communication solutions.

3. What's a common indicator of a potential insider threat?

A. Exploiting external network vulnerabilities

B. Unauthorized access to sensitive files

C. Increased network traffic from unknown sources

D. Frequent system downtime

Unauthorized access to sensitive files is a common indicator of a potential insider threat because it often indicates that an employee or someone with legitimate access is misusing their credentials for malicious purposes, such as data theft or leakage. Insiders may have the ability to access sensitive information legitimately but may choose to exploit that access for personal gain, to harm the organization, or to facilitate data breaches. This behavior can be particularly insidious, as it can occur without triggering the same alarms that would accompany external attacks. In contrast, while exploiting external network vulnerabilities focuses on threats from outside the organization, increased network traffic from unknown sources may point more toward external intrusions. Frequent system downtime is often associated with technical issues or operational inefficiencies rather than deliberate malicious intent. Therefore, unauthorized access to sensitive files stands out as a clear warning sign of potential insider misconduct.

4. What security strategy is characterized by multilayered protection to minimize attacks on organizational assets?

A. Three-way handshake

B. Likelihood analysis

C. Covert channel

D. Defense-in-depth

The security strategy characterized by multilayered protection to minimize attacks on organizational assets is known as defense-in-depth. This approach involves deploying multiple layers of security measures throughout an organization's infrastructure, ensuring that if one layer is breached, others remain intact to mitigate the risk of an attack. Layers can include physical security, network security, application security, and endpoint security, among others. By using defense-in-depth, organizations create a more robust security posture. This means that attackers face multiple barriers, making it significantly more challenging to successfully compromise the system. Additionally, this strategy not only focuses on preventing attacks but also emphasizes detection and response capabilities, enabling organizations to react effectively to incidents should they occur. The other options do not embody the concept of multilayered protection like defense-in-depth does. For instance, a three-way handshake is a process used in TCP/IP networks for establishing a connection and ensuring reliable communication but does not relate to an overall security strategy. Likelihood analysis pertains to assessing the probability of certain risks occurring, while covert channels involve unauthorized communication paths within a network, neither of which encapsulate a comprehensive defensive strategy.

5. Which step is NOT part of securing computer networks against insider threats?

A. Configuring firewalls

B. Allowing open file sharing

C. Monitoring outbound HTTP and HTTPS traffic

D. Reducing transfers to authorized users

Allowing open file sharing is not a step in securing computer networks against insider threats because it creates an environment where unauthorized access to sensitive data is easily facilitated. Open file sharing can lead to excessive exposure of files and data to all users within the network, increasing the risk of an insider misusing the available information. By not restricting or controlling file sharing, organizations make it difficult to monitor who accesses what, thus negating efforts to mitigate insider threats. In contrast, configuring firewalls, monitoring outbound HTTP and HTTPS traffic, and reducing transfers to authorized users all represent proactive measures aimed at protecting the network from potential misuse. Firewalls act as barriers to unauthorized access, monitoring traffic helps in detecting anomalies that may indicate malicious behavior, and limited file transfers ensure that sensitive information is only accessible to those who have a legitimate need, significantly reducing the risk posed by insider threats.

6. Hexagon received many malformed TCP/IP packets, causing their main server to crash. Which type of attack did the adversary use?

A. DoS attack

B. Session Hijacking

C. Man-in-the-Middle

D. Cross-Site-Scripting

The scenario describes a situation where malformed TCP/IP packets are used to cause a main server to crash. This type of activity aligns with a Denial of Service (DoS) attack. A DoS attack typically involves overwhelming a server or network resource by flooding it with excessive traffic or exploiting vulnerabilities, which leads to service disruption. In this case, the use of malformed packets indicates an intention to exploit the server's handling of network traffic, resulting in an inability to process legitimate requests, thereby rendering the service unavailable to users. Other options represent different forms of attacks. Session Hijacking involves taking control of a user's session after authentication, which is unrelated to packet manipulation or server crashing. A Man-in-the-Middle attack intercepts communication between two parties to eavesdrop or impersonate one of them, rather than directly causing server failures. Cross-Site Scripting (XSS) focuses on injecting malicious scripts into web pages viewed by users, which is also distinct from the actions described in the question. Therefore, the classification of this scenario as a DoS attack is clearly appropriate, reflecting the method of exploiting network protocols to achieve disruption.

7. Which type of security misconfiguration vulnerability supports weak algorithms and uses expired or invalid certificates, exposing users' data to untrusted third parties?

A. Parameter / form tampering

B. Improper error handling

C. Unvalidated inputs

D. Insufficient transport layer protection

The correct answer is insufficient transport layer protection. This type of vulnerability occurs when the protocols used to transmit data are not secure, which can be exacerbated by weak algorithms or the use of expired or invalid certificates. When proper encryption standards are not enforced, data can be intercepted by untrusted third parties during transmission. For example, if a website uses outdated encryption methods or has not updated its security certificates, users' sensitive data can be easily compromised. In this context, the vulnerability relates to the lack of adequate security measures in the transport layer, which is responsible for ensuring secure communication over a network. Without robust mechanisms in place, such as TLS (Transport Layer Security), data integrity and confidentiality cannot be guaranteed, leaving the data exposed. Other options like parameter/form tampering, improper error handling, and unvalidated inputs pertain to different types of vulnerabilities that primarily affect the application layer or data integrity, rather than the transport layer's ability to secure data in transit.

8. What is a disadvantage of using Platform-as-a-Service (PaaS)?

A. All of these choices are correct.

B. Scalability

C. Prebuilt business functionality

D. Data privacy

Choosing data privacy as a disadvantage of using Platform-as-a-Service (PaaS) highlights a significant concern associated with cloud services. When organizations leverage PaaS, they are essentially outsourcing the management of their application development environment to a third-party provider. This often means that sensitive data, including user information and application data, is stored off-site in the provider's data centers. Because the data is not under the organization's direct control, there may be concerns regarding how it is protected and who has access to it. This raises potential issues related to compliance with data protection regulations such as GDPR or HIPAA, where the organization remains liable for data breaches even if the data is managed by a third party. Additionally, the security practices of the PaaS provider may not always align with the organization's own security standards and policies, leading to vulnerabilities. While scalability and prebuilt business functionality are generally regarded as advantages of PaaS, they do not inherently present disadvantages in the same way that data privacy does. Scalability allows organizations to handle increased demand without major infrastructure changes, and prebuilt functionalities can expedite the development process. However, these benefits must be evaluated against the potential risks to data privacy and security when deciding to use PaaS. Therefore, data privacy

9. Which of the following is an indication of unauthorized use of a standard user account?

A. Use of a secret account

B. Alert of network and host IDS

C. Misplaced hardware parts

D. Increase in the usage of resources

The indication of unauthorized use of a standard user account is best represented by the use of a secret account. Secret accounts, often referred to as "backdoor" accounts, are not disclosed to system administrators and may be used by unauthorized individuals to gain access to systems without normal authentication processes. If a secret account is utilized within an environment where standard user accounts are expected to be in use, it raises significant security concerns regarding unauthorized access and potential breaches. While alerts from network and host Intrusion Detection Systems (IDS) may signify suspicious activity, they are more general indicators of potential threats and can be triggered by various legitimate activities. Misplaced hardware parts may suggest physical security issues, but do not directly point to unauthorized account usage. An increase in resource usage is also not definitive, as it could stem from legitimate user activities or system processes, rather than an indication of unauthorized access through accounts. Thus, the presence of a secret account stands out as a clear sign of potential unauthorized use.

10. Temporary shutdown and restoration of the infected system are common techniques in which stage of incident response?

A. Preparation

B. Containment

C. Recovery

D. Identification

The stage of incident response where temporary shutdown and restoration of the infected system are applied is containment. Containment aims to limit the impact of the incident, preventing it from spreading to other systems or networks. By temporarily shutting down the affected systems, responders can isolate the threat and prevent further damage. This action is crucial during containment as it helps protect the organization's assets while the incident is being analyzed. Restoration is also a part of containment, as once the threat is isolated and addressed, the ultimate goal is to restore the system to normal operations. This may involve cleaning the infected system and restoring data from backups to ensure that it is functioning securely. In other stages, such as preparation, the focus is on having the necessary plans and tools in place before any incident occurs. During the recovery phase, the emphasis shifts to restoring and validating system functionality after the incident has been dealt with, rather than immediate containment. In the identification stage, the process centers on recognizing the incident and determining its nature and extent, rather than taking actions to mitigate it.

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://eccouncilecih.examzify.com

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