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

Study Guide

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. Don't worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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 does IDS stand for in network security?

A. Intrusion Detection System

B. Internal Data Security

C. Intruder Defense Strategy

D. Internet Detection Source

2. 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

3. What is the primary effect of Denial-of-Service incidents on network resources?

A. They enhance security measures

B. They prevent authorized users from accessing resources

C. They improve network performance

D. They protect against unauthorized access

4. How is quantitative risk analysis defined?

A. Probability of loss X value of loss

B. Value of loss/ Probability of loss

C. Probability of loss + value of loss

D. Probability of loss - value of loss

5. Which tools can incident handlers use to monitor, collect, detect, and analyze user activities on the network?

A. User Behavior Analytics (UBA)

B. SIEM

C. DLP Technologies

D. All the above

6. Which of the following services falls under the category of Software-as-a-Service (SaaS)?

A. Data storage solutions

B. Operating system management

C. Email services

D. Virtual Private Networks

7. What should be disabled for an employee upon termination regarding access?

A. Access rights

B. Security awareness program

C. Human resources

D. All of these choices are correct

8. What mechanism is often used alongside user behaviors to combat insider threats?

A. Audit trails

B. Virtual private networks

C. Proxy servers

D. Firewalls alone

9. What is a critical factor in the management of an incident handling team?

A. Adherence to existing procedures

B. Creating detailed reports

C. Establishing communication protocols

D. Utilizing regular staff meetings

10. The _____ is a semi-trusted network zone that separates the untrusted internet from the company's trusted internal network.

A. DMZ ("demilitarized zone")

B. Buffer zone

C. CAPTCHA zone

D. Hidden field zone

Answers

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

Explanations

1. What does IDS stand for in network security?

A. Intrusion Detection System

B. Internal Data Security

C. Intruder Defense Strategy

D. Internet Detection Source

The term IDS in network security stands for Intrusion Detection System. An Intrusion Detection System is a crucial component of network security that monitors network traffic for suspicious activity and potential threats. It serves to alert administrators about unauthorized access, policy violations, or other malicious activities within a network. IDS can be deployed in various forms, such as network-based or host-based systems, each serving to detect and analyze different types of intrusion. By providing a real-time monitoring system, it allows organizations to respond proactively to security incidents, ensuring the environment remains secure against potential harms. While the other options presented might sound plausible, they do not accurately reflect the recognized term used in the field of network security. Terms like Internal Data Security and Intruder Defense Strategy, while they may relate to the broader subject of security, do not capture the specific function and aim of an IDS, which is fundamentally about detection and response to threats. Similarly, Internet Detection Source does not have any established meaning within the context of cybersecurity frameworks and practices.

2. 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.

3. What is the primary effect of Denial-of-Service incidents on network resources?

A. They enhance security measures

B. They prevent authorized users from accessing resources

C. They improve network performance

D. They protect against unauthorized access

In the context of Denial-of-Service (DoS) incidents, the primary effect is that they prevent authorized users from accessing resources. DoS attacks typically aim to overwhelm a network, service, or application by flooding it with excessive traffic or exploiting vulnerabilities, leading to a degradation or complete loss of service. This disruption can deny legitimate users the ability to connect and utilize the resources they need, resulting in significant downtime and potential financial loss for organizations. The impact of a DoS attack can be far-reaching, often affecting the availability of services that businesses and users rely on, whether that's website access, email services, or any critical online resources. Thus, option B rightly identifies the main consequence of these incidents as the hindrance of authorized user access, illustrating the nature of the threat posed by DoS attacks.

4. How is quantitative risk analysis defined?

A. Probability of loss X value of loss

B. Value of loss/ Probability of loss

C. Probability of loss + value of loss

D. Probability of loss - value of loss

Quantitative risk analysis is a method that evaluates risk in numerical terms to provide a more empirical basis for decision-making. The formula that defines this analysis is the probability of loss multiplied by the value of loss. This approach allows organizations to understand the potential financial impact of various risks they may face. By using this formula, organizations can prioritize risks based on their potential cost if they were to occur, enabling more effective allocation of resources towards risk management and mitigation strategies. This quantitative assessment is particularly valuable for decision-makers as it translates potential risks into concrete financial terms, making it easier to justify investments in risk management initiatives. The other options do not accurately represent the formula used in quantitative risk analysis. They do not provide a direct relationship between the probability of loss and the value of loss as intended in this analysis framework. Understanding the correct definition is crucial for professionals involved in risk assessment and management, ensuring they can make informed decisions based on solid, quantifiable data.

5. Which tools can incident handlers use to monitor, collect, detect, and analyze user activities on the network?

A. User Behavior Analytics (UBA)

B. SIEM

C. DLP Technologies

D. All the above

Incident handlers can utilize a combination of User Behavior Analytics (UBA), Security Information and Event Management (SIEM), and Data Loss Prevention (DLP) technologies to effectively monitor, collect, detect, and analyze user activities on a network. User Behavior Analytics is designed specifically to track user activities and identify anomalies by establishing a baseline of normal behavior. This allows incident handlers to detect potential security breaches when user activity deviates from established patterns. SIEM tools aggregate and analyze log data from various sources within the IT environment to provide insights into security events and threats. They enable incident handlers to monitor real-time activities, correlate data, and generate alerts for suspicious behaviors. Data Loss Prevention technologies focus on protecting sensitive data from being accessed, misused, or lost, often by monitoring user actions in relation to data handling. They help ensure that user activities comply with established policies and regulations. The combination of these tools provides a comprehensive approach to understanding user behaviors and identifying potential incidents before they escalate, making "all the above" the correct choice. Each tool contributes unique capabilities that strengthen the incident handling process.

6. Which of the following services falls under the category of Software-as-a-Service (SaaS)?

A. Data storage solutions

B. Operating system management

C. Email services

D. Virtual Private Networks

The correct answer highlights that email services exemplify the Software-as-a-Service (SaaS) model. SaaS refers to software distribution models where applications are hosted in the cloud and made available to users over the internet, typically through a subscription model. Email services like Gmail, Outlook, or Yahoo Mail are perfect representations of this model since they provide users with access to their email accounts and all associated functionalities without requiring any downloads or local installations. Users can access these services from any device with internet connectivity, illustrating the key benefit of SaaS: ease of access and management without the need for physical infrastructure. On the other hand, data storage solutions, while they can overlap with the SaaS model, often refer to Infrastructure-as-a-Service (IaaS), which typically emphasizes backend storage capabilities rather than front-end software applications. Operating system management is more aligned with Platform-as-a-Service (PaaS) or IaaS, as it involves managing the platform or infrastructure rather than providing software for end-user interaction. Virtual Private Networks (VPNs) are also not aligned with SaaS. Instead, they mainly focus on establishing secure access to a network and serve more as a network security solution than as a software application delivered over the cloud. This distinction reinforces

7. What should be disabled for an employee upon termination regarding access?

A. Access rights

B. Security awareness program

C. Human resources

D. All of these choices are correct

Disabling access rights for an employee upon termination is crucial for maintaining the security of an organization. When an employee leaves the company, whether voluntarily or involuntarily, it is essential to revoke their access to systems, networks, and sensitive data immediately. This helps prevent unauthorized access and protects the organization from potential data breaches or insider threats. By ensuring that former employees no longer have access rights, the organization can maintain a secure environment and safeguard confidential information. The other options do not directly relate to immediate security measures upon employee termination. While security awareness programs and human resources play important roles in employee management and organizational security practices, they do not specifically address the immediate need to disable access rights. Therefore, the focus on access rights as an essential action underscores its importance in upholding a secure operational state after an employee's departure.

8. What mechanism is often used alongside user behaviors to combat insider threats?

A. Audit trails

B. Virtual private networks

C. Proxy servers

D. Firewalls alone

Audit trails are a critical mechanism used to monitor user behaviors and activities within an organization, particularly when addressing the challenge of insider threats. By maintaining detailed logs of user actions, audit trails enable organizations to track and analyze behaviors that could indicate malicious intent or policy violations. The implementation of audit trails helps in identifying unusual or unauthorized actions taken by users. For example, if a user accesses sensitive data that is outside of their typical behavior pattern or is not aligned with their job responsibilities, the audit logs can provide clear evidence of this anomaly. This kind of monitoring is essential for timely intervention and can aid in the investigation process if an insider threat is detected. In contrast, while virtual private networks, proxy servers, and firewalls play important roles in overall network security, they are primarily focused on securing data transmissions, managing network traffic, and creating barriers against external threats. These tools do not specifically address the behavioral monitoring aspect that audit trails provide, making them less effective in identifying and mitigating insider threats.

9. What is a critical factor in the management of an incident handling team?

A. Adherence to existing procedures

B. Creating detailed reports

C. Establishing communication protocols

D. Utilizing regular staff meetings

Establishing communication protocols is a critical factor in the management of an incident handling team because effective communication ensures that all team members are informed and coordinated during an incident response. Communication protocols facilitate the timely exchange of information, which is vital for rapid decision-making and execution of response measures. They help in defining how information is shared among team members, the tools to be used for communication, and the frequency of updates, especially during high-stress situations like an ongoing cyber incident. When communication protocols are clear and robust, they enable the team to respond more efficiently and effectively, reducing the risk of misunderstandings or information gaps that could hinder response efforts. Without solid communication, even the best plans and processes can falter due to a lack of alignment among team members. While adherence to existing procedures, creating detailed reports, and utilizing regular staff meetings are also important aspects of incident management, they do not have the same direct impact on the immediate, real-time coordination required during an incident. Communication serves as the backbone through which these other elements can be executed successfully.

10. The _____ is a semi-trusted network zone that separates the untrusted internet from the company's trusted internal network.

A. DMZ ("demilitarized zone")

B. Buffer zone

C. CAPTCHA zone

D. Hidden field zone

The term "DMZ" or "demilitarized zone" refers to a network architecture designed to enhance security by creating a separate area that acts as a buffer between an untrusted external network, such as the internet, and a trusted internal network. The DMZ typically hosts public-facing services, such as web servers or email servers, allowing external users to access these services while providing a protective barrier for the internal network. This design minimizes the risk of unauthorized access to sensitive internal resources, as any potential attack or breach occurs within the DMZ rather than the core internal systems. In contrast, the other options do not represent a widely recognized network security architectural concept. A buffer zone, while it might sound relevant, is not a standard term used in the context of network segmentation in cybersecurity. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a security measure used to verify user authenticity rather than a network structure. Similarly, a hidden field zone does not have any established significance in network security or segmentation. Thus, the DMZ stands out as the correct choice due to its specific role in network security management.

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!