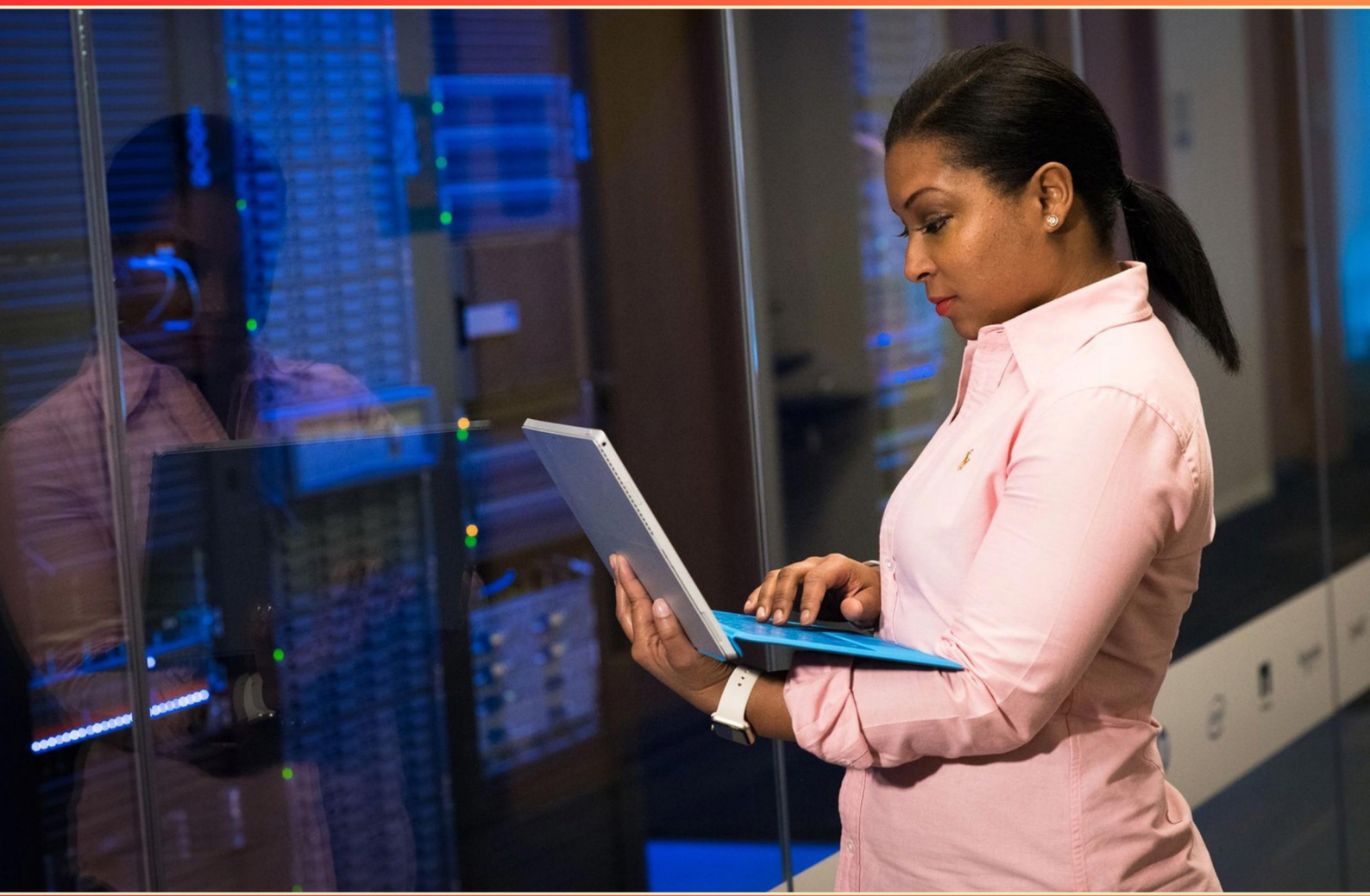
EC-COUNCIL CERTIFIED INCIDENT HANDLER (ECIH) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://eccouncilecih.examzify.com

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. **Which of the following is defined as the existence of a weakness in the design or implementation error that can lead to an unexpected, undesirable event compromising the security of the system?**

   A. Vulnerability

   B. Patch

   C. Attack

   D. Incident

2. **What type of DNS attack involves conducting phishing scams by registering a similar domain name to a cloud service provider?**

   A. Domain Snipping

   B. Domain Hijacking

   C. DNS Poisoning

   D. Cybersquatting

3. **What characteristic is typical for a Denial of Service (DoS) attack?**

   A. It impersonates users to gain unauthorized access

   B. It overwhelms a system with traffic to make it unavailable

   C. It hijacks browsing sessions

   D. It targets specific databases for information theft

4. **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

5. **Which aspect does not relate to Denial-of-Service Incidents?**

   A. Overloading resources

   B. Preventing access to legitimate users

   C. Stealing sensitive information

   D. Disrupting network services

6. What does DLP stand for in the context of cybersecurity tools?

A. Data Loss Prevention

B. Data Leak Protocol

C. Data Logging Process

D. Distributed Layer Protocol

7. Which security element prevents unauthorized changes to data or resources?

A. Integrity

B. Authenticity

C. Non-repudiation

D. Availability

8. Which factor is crucial in determining the effectiveness of an incident response plan?

A. The complexity of the network

B. The level of employee training

C. Regular updates and testing of the plan

D. The size of the organization

9. What term refers to an organization's readiness to utilize digital evidence efficiently?

A. Expert testimony

B. Forensic readiness

C. Data acquisition

D. First response

10. What software can Dhru use to perform network traffic analysis and detect malicious connections?

A. Microsoft Baseline Security Analyzer (MBSA)

B. Wireshark

C. MagicTree

D. KeepNote

Answers

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

Explanations

1. Which of the following is defined as the existence of a weakness in the design or implementation error that can lead to an unexpected, undesirable event compromising the security of the system?

A. Vulnerability

B. Patch

C. Attack

D. Incident

The term that best describes a weakness in the design or implementation of a system, which can result in an unexpected and undesirable event that compromises security, is "vulnerability." A vulnerability serves as a potential entry point for attackers, allowing them to exploit the weakness to perform unauthorized actions or access sensitive information. Understanding vulnerabilities is crucial in the field of incident handling as they help identify areas in a system that require protective measures or remediation efforts. By recognizing and addressing these weaknesses, organizations can enhance their security posture and prevent future incidents. The other terms, while relevant to cybersecurity, refer to different concepts. A patch is a software update designed to correct vulnerabilities or bugs, an attack refers to an action taken by an adversary to exploit a vulnerability, and an incident is an event that represents a security breach or attempted breach. Each of these plays a significant role in the broader context of cybersecurity, but "vulnerability" specifically highlights the underlying weaknesses that can lead to security issues.

2. What type of DNS attack involves conducting phishing scams by registering a similar domain name to a cloud service provider?

A. Domain Snipping

B. Domain Hijacking

C. DNS Poisoning

D. Cybersquatting

The correct choice is associated with the concept of registering a domain name that closely resembles that of a legitimate cloud service provider in order to deceive users into thinking they are visiting the official site. This method is commonly referred to as cybersquatting. Cybersquatters typically exploit user confusion by creating domains that are not only similar in name but often involve minor variations such as altering a character or using a different top-level domain. When users mistakenly enter the URL of the fraudulent domain, they can be directed to phishing sites designed to harvest personal information, such as login credentials or payment details. This practice is particularly effective due to the human tendency to not closely scrutinize web addresses. As users are lured into the trap of entering sensitive information on these fraudulent sites, the attackers can execute their phishing scams successfully. While other terms like domain hijacking or DNS poisoning involve different types of domain and DNS-related attacks, they do not specifically center around the registration of similar domain names to impersonate legitimate entities.

3. What characteristic is typical for a Denial of Service (DoS) attack?

A. It impersonates users to gain unauthorized access

B. It overwhelms a system with traffic to make it unavailable

C. It hijacks browsing sessions

D. It targets specific databases for information theft

A characteristic that is typical for a Denial of Service (DoS) attack is that it overwhelms a system with traffic to make it unavailable. This type of attack aims to disrupt the normal functioning of a targeted server, service, or network by flooding it with an excessive amount of requests or data. The result is that legitimate users are unable to access the services, which is the primary objective of a DoS attack. Understanding DoS attacks is crucial, as they can result in substantial downtime, financial loss, and damage to a company's reputation. A DoS attack typically does not concern itself with stealing data, impersonating users, or hijacking sessions, which distinguishes it from other types of cyber threats. Instead, the focus is purely on causing disruption and denial of service to legitimate users.

4. 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.

5. Which aspect does not relate to Denial-of-Service Incidents?

A. Overloading resources

B. Preventing access to legitimate users

C. Stealing sensitive information

D. Disrupting network services

In the context of Denial-of-Service (DoS) incidents, the primary aim is to disrupt the availability of services or resources, making them unusable for legitimate users. The correct answer highlights that stealing sensitive information is not a characteristic associated with DoS attacks. Denial-of-Service attacks typically focus on overloading resources, such as servers or bandwidth, which leads to slowing down or completely blocking access to services. This aligns with the goals of preventing access to legitimate users and disrupting network services, both of which are fundamental tactics employed during a DoS incident. However, the act of stealing information is typically associated with other forms of cyber attacks, such as data breaches or theft incidents, rather than Denial-of-Service attacks. In essence, while DoS attacks seek to deny service, they do not have the objective of facilitating information theft, which is why this aspect does not relate to Denial-of-Service incidents.

6. What does DLP stand for in the context of cybersecurity tools?

A. Data Loss Prevention

B. Data Leak Protocol

C. Data Logging Process

D. Distributed Layer Protocol

In the context of cybersecurity tools, DLP stands for Data Loss Prevention. This refers to a set of strategies, technologies, and processes designed to detect and prevent the unauthorized access, transfer, or destruction of sensitive data. DLP tools are crucial for organizations to safeguard their intellectual property, customer information, and other critical data from potential breaches. They help monitor, detect, and respond to unauthorized data sharing or leaks, ensuring compliance with relevant data protection regulations. Understanding the importance of DLP helps professionals recognize how essential it is to protect organizational data and maintain its confidentiality. By implementing effective DLP solutions, organizations can mitigate risks related to data breaches and avoid the financial and reputational damage that can result from such incidents.

7. Which security element prevents unauthorized changes to data or resources?

A. Integrity

B. Authenticity

C. Non-repudiation

D. Availability

Integrity is the security element that specifically focuses on preventing unauthorized changes to data or resources. It ensures that data remains accurate, consistent, and trustworthy throughout its lifecycle. This means that if data is altered, it can be detected, and the integrity measures can verify whether it has been compromised or modified by unauthorized individuals. To maintain integrity, organizations often implement controls such as hashing, checksums, and digital signatures. These techniques can help in verifying that the data has not been tampered with and is in the same state as when it was originally created or intended to be used. By ensuring integrity, organizations protect the trustworthiness of their data, which is crucial for decision-making processes and compliance requirements. The other options, while important aspects of information security, do not directly address the issue of unauthorized changes. Authenticity verifies the identity of users or systems but does not prevent modifications to data. Non-repudiation ensures that actions cannot be denied after they have occurred, but it does not inherently prevent changes. Availability focuses on ensuring that systems and data are accessible when needed but does not relate to the integrity of the data itself.

8. Which factor is crucial in determining the effectiveness of an incident response plan?

A. The complexity of the network

B. The level of employee training

C. Regular updates and testing of the plan

D. The size of the organization

The effectiveness of an incident response plan is significantly determined by regular updates and testing of the plan. An incident response plan must evolve alongside the organization's operations, threat landscape, and technology advancements. Regular updates ensure that the plan remains relevant and incorporates lessons learned from past incidents, emerging threats, and changes in business processes. Testing the plan through simulations or tabletop exercises allows an organization to evaluate its readiness, identify gaps or weaknesses, and improve the responses in real scenarios. This cycle of updating and testing reinforces the preparedness of the response team and the overall resilience of the organization against incidents. While other factors, such as employee training, network complexity, and organizational size, do play roles in incident response, the continuous refinement and evaluation of the incident response plan is what truly enhances its effectiveness in mitigating risks and handling incidents efficiently.

9. What term refers to an organization's readiness to utilize digital evidence efficiently?

A. Expert testimony

B. Forensic readiness

C. Data acquisition

D. First response

The term that refers to an organization's readiness to utilize digital evidence efficiently is forensic readiness. Forensic readiness implies that an organization has established processes and strategies to gather and preserve digital evidence before a potential computer security incident occurs. This preparation enables the organization to quickly respond to incidents and maximize the value of the digital evidence collected. Forensic readiness is crucial because it helps organizations ensure that evidence is obtained in a manner that is legally admissible and retains its integrity. This includes having appropriate policies, training, and technological resources in place. By having these measures, an organization can effectively handle incidents, which can lead to more effective investigations and responses. Other terms, such as expert testimony, pertain to the presentation aspect of evidence in legal circumstances and do not involve proactive measures related to evidence management. Data acquisition refers more narrowly to the process of collecting data from systems and may not encompass the broader readiness and strategic initiatives. First response typically focuses on the immediate actions taken during an incident but doesn't address the preparatory measures needed for handling digital evidence efficiently.

10. What software can Dhru use to perform network traffic analysis and detect malicious connections?

A. Microsoft Baseline Security Analyzer (MBSA)

B. Wireshark

C. MagicTree

D. KeepNote

Wireshark is a powerful network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network. It is particularly well-suited for network traffic analysis, as it provides detailed insights into the packets transmitted over a network, including their origin, destination, and contents. This level of detail is essential for identifying malicious connections, as it enables the analyst to recognize patterns or anomalies that could indicate security threats. The other options do not fit the criteria for network traffic analysis effectively. Microsoft Baseline Security Analyzer is primarily a tool for assessing the security state of Microsoft systems rather than analyzing network traffic. MagicTree serves more as a mind mapping and note-taking tool, without capabilities for network analysis. KeepNote is a note-taking application designed for recording information rather than capturing or analyzing live network data. Thus, Wireshark stands out as the appropriate choice for detecting and analyzing network traffic for malicious activities.

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!