(ISC)2 CERTIFIED IN CYBERSECURITY PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

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. **Which RAID level is characterized by disk mirroring?**

   A. RAID 0

   B. RAID 1

   C. RAID 4

   D. RAID 5

2. **Which of the following methods is effective at preventing replay attacks?**

   A. Man-in-the-middle

   B. Full disk encryption

   C. Session tokens

   D. Mobile device management

3. **What term describes events that result in harmful consequences, such as system crashes or unauthorized access?**

   A. Security Incidents

   B. Adverse Events

   C. Risks

   D. Threats

4. **Do Split Tunnel VPNs allow only traffic destined for the corporate network to be sent through a VPN tunnel, while other traffic is routed directly over the internet?**

   A. True

   B. False

5. **Which device is best suited to separate a network into multiple distinct security zones?**

   A. IPS

   B. Router

   C. Switch

   D. Firewall

6. **What is a common lock type requiring continuous code entry for access?**

   A. Proximity card

   B. Biometric

   C. Magnetic stripe

   D. Cipher

7. Which process involves producing a fixed-size numeric value from data?

A. Hashing
B. Encryption
C. Decryption
D. Encoding

8. What is the typical range for a Bluetooth network?

A. 30 FT / 10 meters
B. 25 FT / 8 meters
C. 10 FT / 2 meters
D. Unlimited

9. IPSec (Internet Protocol Security) operates at what layer of the OSI model?

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 6

10. What is defined as an observable occurrence in a network or system?

A. Event
B. Incident
C. Exploit
D. Sensor

Answers

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

Explanations

1. Which RAID level is characterized by disk mirroring?

A. RAID 0

B. RAID 1

C. RAID 4

D. RAID 5

RAID 1 is characterized by disk mirroring, which means that data is copied identically onto two or more disks. This configuration provides a level of redundancy, ensuring that if one disk fails, the information remains accessible from the other mirrored disk. The primary benefit of RAID 1 is its ability to provide high availability and increased fault tolerance, which is crucial for systems that require constant uptime and data integrity. In RAID 1, the performance for read operations can improve since data can be read simultaneously from multiple disks. However, the write performance may be slightly slower compared to other RAID levels due to the need to write the same data to multiple disks. In contrast, RAID 0 focuses on striping data across multiple disks for improved performance and does not offer redundancy, making it unsuitable for environments where data loss is a concern. RAID 4 and RAID 5 use a different structure by implementing striping along with parity data to provide fault tolerance; however, they do not utilize mirroring like RAID 1 does. Thus, RAID 1 is the only configuration among the options that specifically implements disk mirroring as a method of ensuring data redundancy.

2. Which of the following methods is effective at preventing replay attacks?

A. Man-in-the-middle

B. Full disk encryption

C. Session tokens

D. Mobile device management

Session tokens are an effective method for preventing replay attacks because they serve as unique identifiers for active communication sessions between the client and server. When a session token is issued for a specific session, it becomes valid only for that session duration and often includes a timestamp or a nonce (a number used once) to ensure uniqueness. In the context of a replay attack, an adversary could capture valid data and then retransmit it in an attempt to impersonate a legitimate user. Session tokens can mitigate this risk by requiring each session to have a distinct token, which means that even if a token were to be captured, it would only be valid for that instance and cannot be reused in another session. Additionally, the inclusion of time-sensitive elements (like expiration times) in session tokens makes it difficult for attackers to successfully replay old tokens. To understand this better, let's consider why the other options are less effective against replay attacks. Man-in-the-middle attacks involve intercepting and possibly altering communications between two parties, but they do not specifically defend against the reuse of captured data. Full disk encryption secures data at rest but does not directly address the threats posed by replay attacks in real-time communications. Mobile device management (MDM) helps in managing devices and enforcing security

3. What term describes events that result in harmful consequences, such as system crashes or unauthorized access?

A. Security Incidents

B. Adverse Events

C. Risks

D. Threats

The term that best describes events leading to harmful consequences, such as system crashes or unauthorized access, is typically referred to as adverse events. These events represent occurrences that negatively impact systems, processes, or services, resulting in detrimental outcomes. In cybersecurity, understanding adverse events is crucial because they highlight the consequences that can arise from vulnerabilities or ineffective security measures. Security incidents generally refer to specific occurrences that actually result in a breach or damage, such as a confirmed hacking attempt, whereas adverse events encompass a broader range of harmful outcomes, including those that may not yet qualify as confirmed incidents but signify a potential setback or compromise. Risks relate to the potential for harm or loss but do not inherently describe an event. Instead, risks are assessed against the likelihood of adverse events occurring and their potential impact. Threats are the potential dangers that could exploit vulnerabilities to cause adverse events; while they are closely related, they do not encompass the actual harmful consequences. Therefore, adverse events more accurately capture the essence of harmful outcomes resulting from such incidents or threats in cybersecurity contexts.

4. Do Split Tunnel VPNs allow only traffic destined for the corporate network to be sent through a VPN tunnel, while other traffic is routed directly over the internet?

A. True

B. False

Split Tunnel VPNs are designed to optimize network performance and security by allowing users to access both the corporate network and the public internet simultaneously. In this setup, only traffic that is specifically destined for the corporate network is routed through the VPN tunnel, while all other traffic—such as general web browsing or accessing online services—is directed straight to the internet without going through the VPN. This approach helps in reducing the load on the VPN connection, improves speed for non-corporate traffic, and maintains a level of security for sensitive corporate data being transmitted. The ability to customize which traffic goes through the VPN while allowing other internet activities to bypass it is a defining feature of split tunneling. This configuration can be beneficial in scenarios where bandwidth is limited or where there is a need to access public resources without the latency that can sometimes accompany VPN connections.

5. Which device is best suited to separate a network into multiple distinct security zones?

A. IPS

B. Router

C. Switch

D. Firewall

A firewall is best suited to separate a network into multiple distinct security zones because it is specifically designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. Firewalls can create different security zones by establishing boundaries between different segments of a network and applying specific policies for each zone. This is vital for protecting sensitive data and systems by ensuring that only authorized traffic is allowed to pass between the zones. When a firewall is implemented, it can segment a network so that traffic between different areas of the network is tightly controlled and monitored. For example, an organization may have a public-facing zone for internet traffic, a zone for its internal operations, and a secure zone for sensitive data. The firewall enforces rules on what traffic can traverse between these zones, effectively compartmentalizing and safeguarding the network. Devices like routers, switches, or intrusion prevention systems (IPS) have distinct roles that do not focus primarily on managing security zones. While routers can segment networks and provide some basic packet filtering capabilities, they lack the extensive security features necessary for effective zone separation that firewalls provide. Switches primarily handle traffic within the same network and do not offer the security features needed to separate zones effectively. IPS devices monitor malicious activity and can take action against certain attacks,

6. What is a common lock type requiring continuous code entry for access?

A. Proximity card

B. Biometric

C. Magnetic stripe

D. Cipher

The correct answer is a cipher lock. Cipher locks are commonly used access control mechanisms that require the entry of a numerical code on a keypad for access. This continuous requirement for code entry means that only individuals who know the correct sequence can gain access to the secured area. The need to input a code for every access attempt enhances security, as unauthorized individuals cannot enter without knowing the specific code. In contrast, options such as proximity cards, biometric systems, and magnetic stripes operate differently; they do not necessitate continuous code entry for access. Proximity cards allow access with a simple swipe or tap, while biometric systems utilize physical characteristics like fingerprints or facial recognition to grant access, and magnetic stripe cards require swiping but do not involve ongoing code entry.

7. Which process involves producing a fixed-size numeric value from data?

A. Hashing

B. Encryption

C. Decryption

D. Encoding

The process that involves producing a fixed-size numeric value from data is known as hashing. Hashing takes an input (or "message") and generates a unique, fixed-size string of characters that is typically a numeric value. This value, referred to as the hash, serves as a digital fingerprint of the input data. One of the key features of hashing is that even a small change in the input will produce a significantly different hash output, making it an important tool for ensuring data integrity. Hashing is commonly used in various applications, such as verifying data integrity, securely storing passwords, and creating digital signatures. Unlike encryption, which is designed to protect the confidentiality of data, hashing is non-reversible, meaning there's no way to retrieve the original data from the hash. Other processes mentioned, such as encryption, decryption, and encoding, serve different purposes. Encryption is intended for securing data by converting it into a format that is unreadable without a key, while decryption involves converting the encrypted data back to its original form. Encoding, on the other hand, transforms data into a different format for transmission or storage but is not inherently focused on security and does not produce a fixed-size numeric value like hashing does.

8. What is the typical range for a Bluetooth network?

A. 30 FT / 10 meters

B. 25 FT / 8 meters

C. 10 FT / 2 meters

D. Unlimited

The typical range for a Bluetooth network is approximately 30 feet, or 10 meters. This range can vary based on environmental factors like obstacles and interference from other wireless devices. Bluetooth technology is designed to provide short-range wireless communication, making it ideal for connecting devices like headphones, speakers, and smartphones over relatively short distances. As devices are designed to operate effectively within this range, most applications do not require connections beyond this distance. Therefore, while other options provide lower distances or suggest an unrealistic range like unlimited, the correct choice reflects the standard range achieved under ideal conditions for Bluetooth communication.

9. IPSec (Internet Protocol Security) operates at what layer of the OSI model?

A. Layer 1

B. Layer 2

C. Layer 3

D. Layer 6

IPSec operates at Layer 3 of the OSI model, which is the Network layer. This is significant because Layer 3 is responsible for the delivery of packets from the source to the destination across multiple networks. IPSec provides a suite of protocols that ensure secure communication over an IP network by implementing various security mechanisms such as encryption and authentication. By functioning at this layer, IPSec can protect any traffic that is carried by the Internet Protocol, making it versatile for securing different types of applications and services that rely on IP. This ability to secure traffic between devices across potentially insecure networks is one of the main benefits of using IPSec.

10. What is defined as an observable occurrence in a network or system?

A. Event

B. Incident

C. Exploit

D. Sensor

The term that refers to an observable occurrence in a network or system is "event." In cybersecurity, an event can include any action or occurrence that can be detected by systems or users, such as user logins, file access, or system alerts. Events are crucial for monitoring because they provide the data necessary for understanding the state of the network or system at any given time. In contrast, an "incident" typically refers to a security event that results in an adverse outcome, such as a breach or a denial-of-service attack. An incident requires a response and further investigation. "Exploit," on the other hand, refers to a means of taking advantage of a vulnerability to compromise a system, and "sensor" refers to devices or software that gather data about events happening in a network or system. Understanding these distinctions helps in the broader context of security monitoring and incident response.

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://isc2certifiedincybersecurity.examzify.com

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