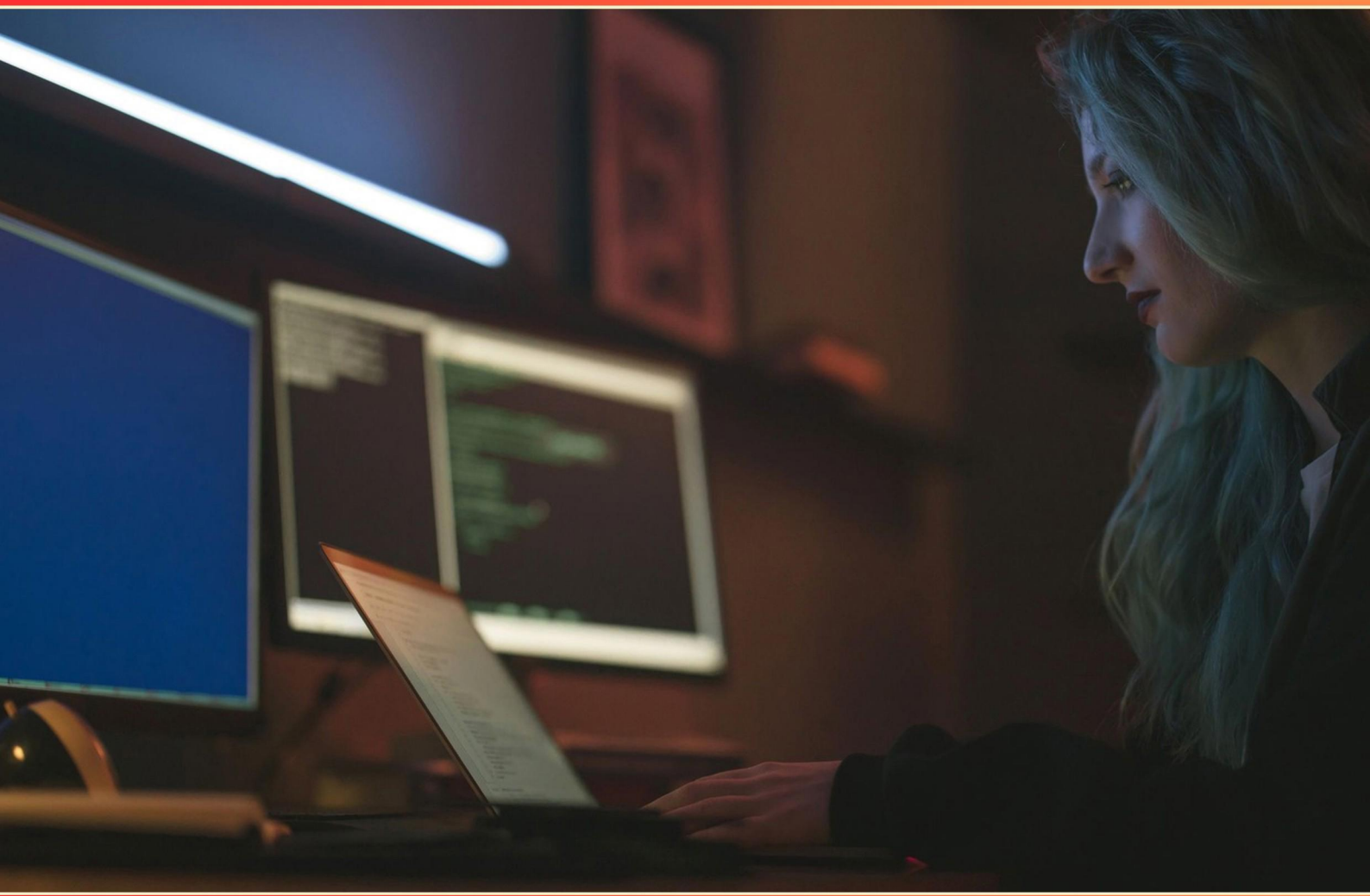
COMPTIA CYSA+ PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://comptia-cysaplus.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

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

SAMPLE

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

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. **How should a sophisticated breach of the network that has occurred over several months be classified?**

   A. Advanced persistent threat (APT)

   B. Spear phishing

   C. Insider threat

   D. Privilege escalation

2. **What is the primary responsibility of a service consumer in a VPC environment?**

   A. Provision virtual servers

   B. Manage security protocols

   C. Maintain IP address space

   D. Ensure data encryption

3. **What does the acronym GDPR stand for?**

   A. General Data Protection Regulation.

   B. Global Data Processing Rights.

   C. General Digital Privacy Rules.

   D. Global Data Privacy Regulation.

4. **What is a common tactic used in social engineering attacks?**

   A. Phishing emails that impersonate trusted entities

   B. Physical break-ins to secure locations

   C. Denial of service attacks on network servers

   D. Malware installation through software updates

5. **Which category of security controls focuses on policies, procedures, and awareness training?**

   A. Technical controls

   B. Physical controls

   C. Administrative controls

   D. Logical controls

SAMPLE

6. What information does the network intrusion detection system (NIDS) primarily provide?

A. Detection of performance issues

B. Identification of unauthorized access attempts

C. Data backup protocols

D. Comprehensive user analytics

7. Which of the following is a critical function provided by Transport Layer Security (TLS)?

A. Data compression

B. Privacy and data security

C. Network layer control

D. DNS management

8. What does the term "vulnerability assessment" refer to?

A. A process of identifying security weaknesses

B. A method for encrypting data

C. An approach to conduct user training

D. A strategy for securing physical locations

9. What type of analysis is conducted during the threat modeling process?

A. Identifying potential threats and vulnerabilities in a system

B. Developing marketing strategies

C. Assessing user behavior

D. Estimating project costs

10. What is the proper classification of a security breach that employs brute-force methods to compromise a system?

A. Attrition

B. Impersonation

C. Improper Usage

D. Loss or theft of equipment

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. How should a sophisticated breach of the network that has occurred over several months be classified?

A. Advanced persistent threat (APT)

B. Spear phishing

C. Insider threat

D. Privilege escalation

A sophisticated breach of the network that takes place over several months is best classified as an Advanced Persistent Threat (APT). APTs are characterized by their targeted nature, often involving prolonged and covert access to a network. Threat actors behind APTs typically conduct extensive reconnaissance, establish a foothold in the network, and move laterally over time to achieve their objectives, which may include data theft or system compromise. APTs are distinguished by their complexity and persistence, making them different from other threats that may be more opportunistic or require less time and sophistication to carry out. The gradual infiltration and continuous presence within the network support the classification as an APT, as these threats aim to maintain long-term access rather than executing a quick attack. Other options, while relevant to cybersecurity, do not specifically describe a long-term, sophisticated breach. Spear phishing refers to targeted email attacks against specific individuals or organizations but does not inherently imply prolonged engagement. An insider threat involves individuals within the organization misusing their access, which may not necessarily feature the sophisticated techniques common in APTs. Privilege escalation is a technique used during attacks to gain higher access on a network but does not denote the overall nature or strategy behind a long-term breach. Hence, the definition and

2. What is the primary responsibility of a service consumer in a VPC environment?

A. Provision virtual servers

B. Manage security protocols

C. Maintain IP address space

D. Ensure data encryption

The primary responsibility of a service consumer in a Virtual Private Cloud (VPC) environment is to maintain IP address space. This includes managing the allocation and assignment of IP addresses to the resources within their VPC, ensuring that there are no conflicts, and optimizing the use of available addresses. In a VPC setup, users often have the flexibility to define their own private IP address ranges, and managing this space is crucial for proper network functionality and connectivity of resources. Proper management helps in maintaining organized communication between various components within the VPC. Provisioning virtual servers and managing security protocols are typically the responsibilities of the service provider or cloud administrator, who oversees the overall infrastructure and security measures. Ensuring data encryption, while important, falls under data protection measures and can be a shared responsibility between consumers and providers, but primarily relates to the security strategy rather than the core responsibility of managing the virtual environment's address space.

SAMPLE

3. What does the acronym GDPR stand for?

A. General Data Protection Regulation.

B. Global Data Processing Rights.

C. General Digital Privacy Rules.

D. Global Data Privacy Regulation.

The acronym GDPR stands for General Data Protection Regulation. This regulation is a comprehensive data protection law that was enacted by the European Union in May 2018. Its primary purpose is to enhance the protection of individuals' data privacy and create a unified approach to data protection across the EU member states. GDPR gives individuals more control over their personal data and mandates strict rules on how organizations collect, process, and store such data. Understanding GDPR is critical for cybersecurity professionals, as compliance with these regulations is essential for any organization that handles the personal data of EU citizens. Organizations must also be aware of the heavy penalties for non-compliance, which serves as a strong incentive to adhere to these regulations. Other options presented do not accurately reflect the established meaning of GDPR, as they either introduce terms that do not exist in the regulatory framework or do not convey the correct emphasis on data protection.

4. What is a common tactic used in social engineering attacks?

A. Phishing emails that impersonate trusted entities

B. Physical break-ins to secure locations

C. Denial of service attacks on network servers

D. Malware installation through software updates

Phishing emails that impersonate trusted entities are a prevalent tactic in social engineering attacks because they exploit human psychology and trust. In these attacks, the attacker often sends an email that appears to be from a legitimate source, such as a bank, company, or a colleague, prompting the recipient to take action, such as clicking a link, providing sensitive information, or downloading an attachment. The goal is to manipulate the target into revealing confidential information, such as passwords or personally identifiable information. This tactic is particularly effective because individuals are often conditioned to trust emails from known or recognizable senders, making them less vigilant about the possibility of deceit. The success of phishing relies heavily on the attackers' ability to craft convincing narratives and the use of social cues that encourage targets to act quickly without questioning the legitimacy of the request. This reflects a fundamental aspect of social engineering: utilizing influence and manipulation rather than technical exploits to achieve malicious objectives. In contrast, the other methods listed involve more technical aspects or require a different approach. For example, physical break-ins typically rely on stealth or force rather than psychological manipulation, while denial of service attacks and malware installations are focused on exploiting system vulnerabilities rather than targeting human behavior directly.

SAMPLE

5. Which category of security controls focuses on policies, procedures, and awareness training?

A. Technical controls

B. Physical controls

C. Administrative controls

D. Logical controls

Administrative controls are crucial in establishing a framework for an organization's security posture. They encompass the development and implementation of policies, procedures, and guidelines that govern security practices within an organization. This category focuses on the human element of security, as it aims to ensure that employees are aware of their roles and responsibilities regarding protecting organizational assets. For instance, administrative controls often include security policies that outline acceptable use, incident response protocols, and data protection measures. Training and awareness programs fall under this category as well, as they help employees understand and adhere to security practices, fostering a culture of security within the organization. The effectiveness of technical and physical controls—those focused on hardware and software protections, as well as physical security measures—hinges on the adherence to the administrative controls put in place. Thus, without strong administrative controls, the implementation of technical and physical security measures could be undermined, leading to potential vulnerabilities.

6. What information does the network intrusion detection system (NIDS) primarily provide?

A. Detection of performance issues

B. Identification of unauthorized access attempts

C. Data backup protocols

D. Comprehensive user analytics

The primary function of a network intrusion detection system (NIDS) is to monitor network traffic for suspicious activities and potential threats, specifically focusing on identifying unauthorized access attempts. NIDS works by analyzing incoming and outgoing traffic in real-time, using signatures and heuristics to detect patterns that indicate possible intrusions, such as abnormal access behavior or known malicious activity. This capability is crucial for maintaining network security, as it allows organizations to respond quickly to potential breaches and safeguard sensitive information. While other systems may be involved in performance monitoring, data management, or user analytics, these functions do not fall within the core scope of NIDS operations, which is strictly related to identifying potential threats and unauthorized accesses within a network environment.

SAMPLE

7. Which of the following is a critical function provided by Transport Layer Security (TLS)?

A. Data compression

B. Privacy and data security

C. Network layer control

D. DNS management

The critical function provided by Transport Layer Security (TLS) is privacy and data security. TLS is designed to secure communications over a computer network by providing a secure channel between users and servers. It achieves this through encryption, which ensures that data transmitted over the network is protected from eavesdroppers and unauthorized access. In addition to encryption, TLS also provides authentication, ensuring that the parties in a communication are who they claim to be, as well as integrity, which verifies that the data has not been altered in transit. These features collectively support confidentiality and trustworthiness in online transactions and data exchange, making privacy and data security the core purpose of TLS. Other functions like data compression, while it may be utilized in some contexts with TLS, are not fundamental to its role in securing data. Network layer control and DNS management fall outside the scope of TLS's responsibilities, as they pertain more to different layers of the networking stack and different protocols that govern internet traffic.

8. What does the term "vulnerability assessment" refer to?

A. A process of identifying security weaknesses

B. A method for encrypting data

C. An approach to conduct user training

D. A strategy for securing physical locations

The term "vulnerability assessment" specifically refers to a systematic process of identifying security weaknesses in an organization's information systems, applications, or network infrastructure. This process involves the discovery, evaluation, and prioritization of potential vulnerabilities that could be exploited by attackers, enabling organizations to take appropriate measures to mitigate risks. A vulnerability assessment typically includes techniques such as automated scanning tools, manual testing, and reviews of system configurations to uncover weaknesses that could compromise security. By identifying these vulnerabilities, organizations can implement patches, changes, or additional security controls to enhance their overall security posture. The other options represent different activities that, while related to cybersecurity, do not define a vulnerability assessment. Encrypting data is focused on protecting information from unauthorized access during transit or storage. Conducting user training aims to educate employees on security best practices and awareness. Securing physical locations relates to physical security measures rather than the assessment of technical vulnerabilities within systems.

SAMPLE

9. What type of analysis is conducted during the threat modeling process?

A. Identifying potential threats and vulnerabilities in a system

B. Developing marketing strategies

C. Assessing user behavior

D. Estimating project costs

The type of analysis conducted during the threat modeling process primarily involves identifying potential threats and vulnerabilities in a system. This process is essential for understanding the security posture of an application or infrastructure by systematically examining where it is susceptible to attacks or exploitation. During threat modeling, professionals typically assess various components of the system, such as data flows, entry and exit points, and assets that need protection. This strategic approach enables organizations to prioritize security measures, effectively allocate resources, and implement preventive actions before threats can be realized. Identifying potential threats allows for a proactive stance on security, rather than a reactive one, enhancing the resilience of the system against various attack vectors.

10. What is the proper classification of a security breach that employs brute-force methods to compromise a system?

A. Attrition

B. Impersonation

C. Improper Usage

D. Loss or theft of equipment

The classification of a security breach that employs brute-force methods to compromise a system is classified as attrition. This type of attack typically involves an attacker attempting numerous combinations of credentials in order to gain unauthorized access to a system. Attrition, in a cybersecurity context, refers to the gradual weakening or erosion of defenses over time, often achieved through repeated attempts to breach security, like those seen in brute-force attacks. The other classifications do not accurately describe this scenario. Impersonation involves an attacker taking on the identity of a legitimate user to gain access or perform malicious actions; this is not applicable when describing brute-force attacks. Improper usage refers to legitimate users abusing their access rights, which does not apply to an external attacker using brute-force tactics. Loss or theft of equipment pertains to physical security incidents where devices are stolen or lost, which is unrelated to the method of compromise described in the question. Thus, attrition is the most fitting classification for a brute-force security breach.

SAMPLE

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://comptia-cysaplus.examzify.com

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

SAMPLE