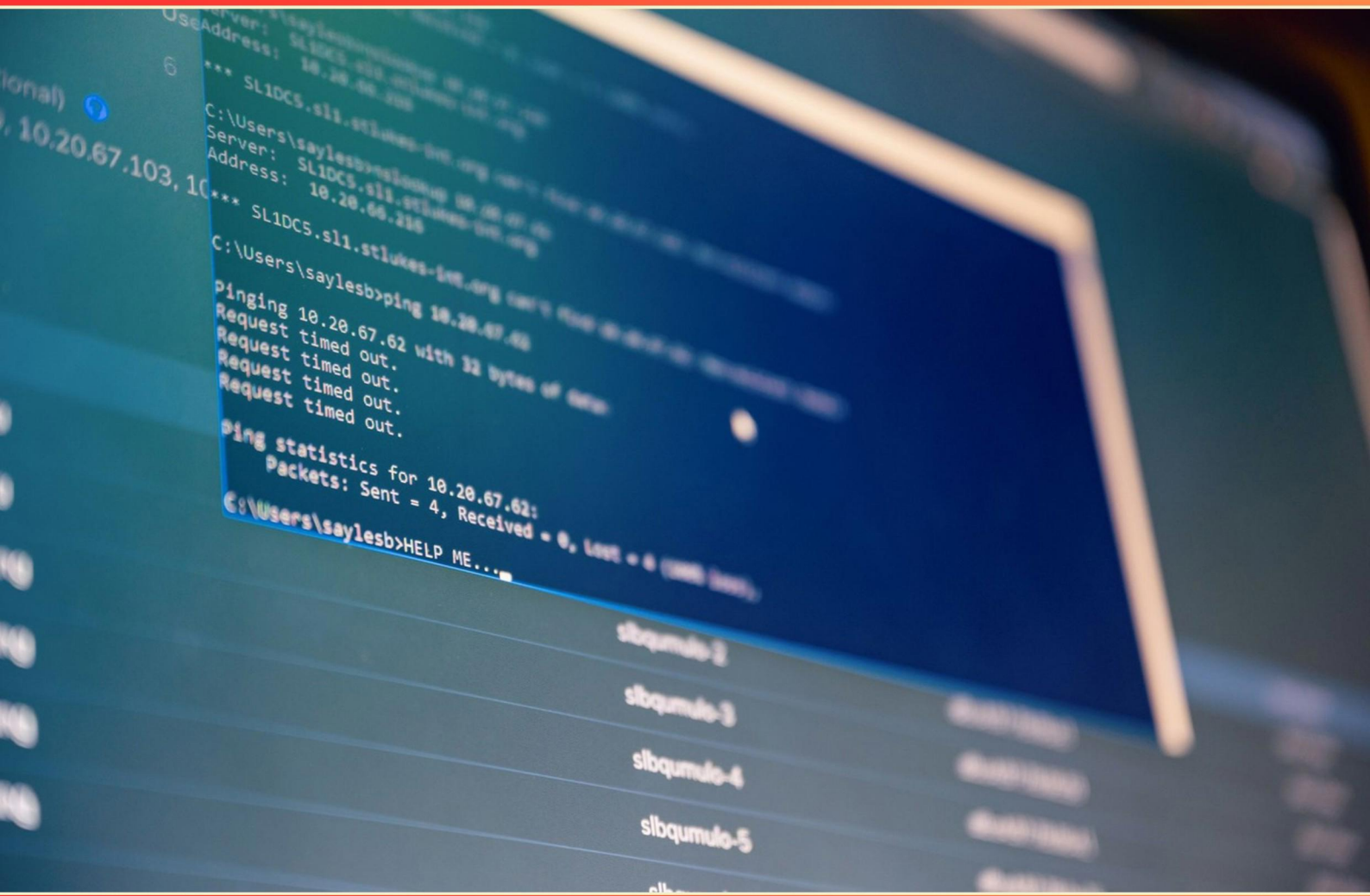
COMPTIA SECURITY+ PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://comptiasecurityplus.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. **What occurs when a switch is flooded with random MAC addresses, causing a MAC address overflow?**

   A. Network Congestion

   B. MAC Flood

   C. Address Saturation

   D. Port Malfunction

2. **What does Privileged Access Management (PAM) primarily focus on?**

   A. Regular user access management.

   B. Management of admin roles and access.

   C. Creating typical user accounts.

   D. Public access control policies.

3. **What term describes the amount of a resource being utilized by a system or service?**

   A. Saturation

   B. Utilization

   C. Capacity

   D. Consumption

4. **Which process allows security personnel to verify if there has been a change to the system's baseline?**

   A. Authentication

   B. Access Control

   C. Attestation

   D. Identity Verification

5. **What is the main goal of ensuring data Availability?**

   A. To prevent unauthorized access to data

   B. To ensure data is accessible when and where needed

   C. To archive data for future reference

   D. To backup information regularly

SAMPLE

6. What open-source solution offers SSO capabilities utilizing SAML?

A. Protected EAP (PEAP)

B. Shibboleth

C. OpenID

D. Cross-Certification

7. Which access control model allows an administrator to implement security policies across all users?

A. Discretionary Access Control (DAC)

B. Rule-Based Access Control

C. Role-Based Access Control

D. Mandatory Access Control (MAC)

8. Which term describes a method that does not explicitly define sensitive content types for data protection?

A. Audit Log

B. Imprecise Method

C. File Integrity Monitoring

D. Precise Method

9. What issue arises from vendor lock-in?

A. Increased competition among vendors

B. Dependency on a single vendor's products

C. Limited availability of products

D. Improved service level agreements

10. What term is used for a process that ensures applications meet acceptable levels of security for their intended functions?

A. Cybersecurity Assessment

B. Software Assurance

C. Quality Assurance

D. Risk Management

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What occurs when a switch is flooded with random MAC addresses, causing a MAC address overflow?

A. Network Congestion

B. MAC Flood

C. Address Saturation

D. Port Malfunction

When a switch is flooded with random MAC addresses, it leads to a phenomenon known as a MAC flood. This occurs when the switch's MAC address table, which is designed to store MAC addresses to forward frames appropriately, becomes overwhelmed with unwanted or extraneous entries. As the table fills up, the switch can no longer effectively learn valid MAC addresses, causing it to default into a mode where it forwards frames to all ports rather than to a specific destination. This disruption of the normal operation results in increased network traffic and can dramatically reduce overall network performance, as the switch behaves more like a hub, sending out broadcasts to all devices instead of unicast transmissions to specific devices. The confusion often arises with terms like network congestion and address saturation; while these are related concepts, they do not specifically describe the process of overwhelming the switch's MAC address table directly. A port malfunction implies a hardware failure, which is not what happens in the case of a MAC flood. Hence, identifying the phenomenon as a MAC flood accurately captures the specific action that disrupts network functionality in this scenario.

2. What does Privileged Access Management (PAM) primarily focus on?

A. Regular user access management.

B. Management of admin roles and access.

C. Creating typical user accounts.

D. Public access control policies.

Privileged Access Management (PAM) primarily focuses on the management of administrative roles and access. PAM is designed to ensure that only authorized personnel have access to critical systems and sensitive data by enforcing strict policies and controls surrounding privileged accounts. These privileged accounts, such as those belonging to system administrators or root users, have heightened abilities to modify system configurations and access sensitive information, making them prime targets for malicious actors. By controlling and monitoring how these accounts are used, PAM helps to minimize risks associated with data breaches and prevents unauthorized actions that could compromise security. PAM solutions often include features such as session recording, access controls, and automated password management for privileged accounts, further enhancing the security posture of an organization by tightly regulating who can perform sensitive operations. This focus on managing admin roles and access is crucial in maintaining an organization's security and integrity, particularly in complex environments where the potential for abuse or misconfiguration is significant.

SAMPLE

3. What term describes the amount of a resource being utilized by a system or service?

A. Saturation

B. Utilization

C. Capacity

D. Consumption

The term that accurately describes the amount of a resource being utilized by a system or service is utilization. Utilization refers to the proportion of capacity that is actually used at any given time. It is a critical concept in resource management, as it helps administrators understand how much of their available resources—such as CPU, memory, or bandwidth—are being actively deployed to support workloads. In the context of monitoring systems and performance, utilization is essential for identifying potential bottlenecks, assessing the efficiency of resource allocation, and making informed decisions regarding scaling or optimizing services. By analyzing utilization metrics, organizations can ensure that resources are used effectively without oversubscribing or exceeding thresholds that could lead to degradation of performance.

4. Which process allows security personnel to verify if there has been a change to the system's baseline?

A. Authentication

B. Access Control

C. Attestation

D. Identity Verification

The process that allows security personnel to verify if there has been a change to the system's baseline is attestation. This process involves a formal declaration or confirmation of the integrity, state, or quality of the system in question. When attestation is performed, it assesses whether current configurations and states match an established baseline. By comparing the current system state to the baseline, personnel can identify unauthorized changes or deviations that may indicate a security incident or compromise. Attestation is particularly important in maintaining security compliance and assurance, as it emphasizes the need for systems to maintain their intended configurations and prevents unauthorized modifications. This process is often part of a broader security governance strategy that ensures systems remain in a known and trusted state. The other processes, while important in their own rights, do not specifically focus on verifying changes to a system's baseline in the same way. For example, authentication is primarily about verifying the identity of users or devices, access control involves managing permissions to resources, and identity verification is focused on the confirmation of a person's or entity's identity. Each of these plays a role in security, but attestation specifically addresses the integrity and state of the system, making it the correct choice for this context.

SAMPLE

5. What is the main goal of ensuring data Availability?

A. To prevent unauthorized access to data

B. To ensure data is accessible when and where needed

C. To archive data for future reference

D. To backup information regularly

The primary goal of ensuring data availability is to make certain that data is accessible when and where it is needed. This concept is crucial in information security and IT infrastructure management, as it focuses on providing continuous access to data and services for authorized users. Maintaining high availability involves implementing the necessary technologies and processes, such as redundancy, failover mechanisms, and network reliability, to minimize downtime and interruptions. While preventing unauthorized access, archiving, and regular backups are important components of data management and security, they do not specifically address the concept of availability. Preventing unauthorized access is more related to confidentiality, archiving pertains to long-term data storage, and regular backups are critical for data recovery but do not guarantee that data will be available at all times. Therefore, the emphasis on ensuring data is accessible when and where needed directly aligns with the overarching goal of data availability.

6. What open-source solution offers SSO capabilities utilizing SAML?

A. Protected EAP (PEAP)

B. Shibboleth

C. OpenID

D. Cross-Certification

Shibboleth is an open-source solution that provides single sign-on (SSO) capabilities through the implementation of the Security Assertion Markup Language (SAML). SAML is an open standard that allows organizations to exchange authentication and authorization data between identity providers and service providers. Shibboleth leverages this protocol to enable secure, seamless access to multiple applications and web resources using a single set of credentials. With its robust support for federated identity management, Shibboleth facilitates user authentication across various domains without requiring users to log in separately to each service. This streamlines the user experience, enhances security by minimizing the number of credentials that need to be managed, and helps organizations maintain control over user access. The other options, while they serve functionalities related to authentication and security, do not specifically provide SSO capabilities utilizing SAML in the same way that Shibboleth does. For example, Protected EAP is a protocol for securing wireless connections, OpenID is a decentralized authentication standard that does not rely on SAML, and Cross-Certification refers to the practice of allowing different public key infrastructure (PKI) systems to interact, rather than an SSO solution.

SAMPLE

7. Which access control model allows an administrator to implement security policies across all users?

A. Discretionary Access Control (DAC)

B. Rule-Based Access Control

C. Role-Based Access Control

D. Mandatory Access Control (MAC)

The correct choice emphasizes the capability of Role-Based Access Control (RBAC) to implement security policies efficiently across all users within an organization. RBAC is centered around the roles that users hold within the organization. Each role is associated with the permissions required to perform particular tasks, allowing administrators to define what actions a user can perform based solely on their assigned role rather than on individual user permissions. This model facilitates a streamlined management process because when a user's role changes, only their role needs to be updated to reflect the new permissions, rather than changing permissions for every single user individually. This scalability and ease of management make RBAC particularly effective for organizations where user access needs to be controlled dynamically and ensures that policies remain consistent across all users in similar roles. By using RBAC, organizations can enforce security policies uniformly, reducing the risk of human error and ensuring that users have access only to the information necessary for their roles. This model supports various compliance requirements and enhances overall security posture by promoting the principle of least privilege.

8. Which term describes a method that does not explicitly define sensitive content types for data protection?

A. Audit Log

B. Imprecise Method

C. File Integrity Monitoring

D. Precise Method

The term that describes a method not explicitly defining sensitive content types for data protection is "imprecise method." This refers to a general data protection approach that does not narrow down or specify particular categories of sensitive information. Instead of having well-defined rules or categories for what constitutes sensitive data, an imprecise method might employ broader policies that apply to data in a more overall manner. For instance, an imprecise method might enforce blanket encryption across all data without discriminating based on whether it's personally identifiable information (PII), health data, or financial records. While this approach can provide a level of protection, it may not be as effective in targeting and addressing specific vulnerabilities that sensitive data types present. In contrast, a precise method would explicitly identify and categorize sensitive content, leading to tailored security measures focused on protecting those specific data types based on their unique risks and regulatory requirements. An audit log is a record-keeping tool used to track access and changes to data but does not describe a protection methodology per se. File integrity monitoring is a specific technique used to detect unauthorized changes to files and does not inherently relate to content type definitions.

SAMPLE

9. What issue arises from vendor lock-in?

A. Increased competition among vendors

B. Dependency on a single vendor's products

C. Limited availability of products

D. Improved service level agreements

Vendor lock-in occurs when a customer becomes dependent on a single vendor's products or services and finds it challenging to switch to a different vendor without incurring significant costs or disruptions. This dependency can lead to several drawbacks, including reduced flexibility and leverage over the vendor in terms of pricing, support, and features. Once a company invests heavily in a particular vendor's technology or solutions, migrating to a different system often requires substantial effort, new training, and additional expenses associated with switching, which can create a hurdle for future business decisions and innovations. In contrast, increased competition among vendors typically leads to better pricing and more options, which doesn't align with the concept of vendor lock-in. Limited availability of products and improved service level agreements are also not direct issues resulting from vendor lock-in; rather, these might be influenced by other factors in the market or specific vendor strategies. Thus, the dependency on a single vendor is the core issue that defines vendor lock-in.

10. What term is used for a process that ensures applications meet acceptable levels of security for their intended functions?

A. Cybersecurity Assessment

B. Software Assurance

C. Quality Assurance

D. Risk Management

The term used for a process that ensures applications meet acceptable levels of security for their intended functions is Software Assurance. This concept encompasses a set of practices and processes designed to ensure that software is developed and maintained with security in mind, addressing potential vulnerabilities and ensuring that security controls are implemented effectively throughout the software development lifecycle. Software Assurance involves validation and verification techniques, including testing, evaluation, and analysis, to confirm that the software behaves as expected and adheres to security standards. This is crucial in the development of applications, as it helps to mitigate risks and protect sensitive data from threats and vulnerabilities, providing confidence to stakeholders that the software is secure and reliable in its operations. The other terms mentioned have distinct focuses: Cybersecurity Assessment typically refers to a review of existing security measures and identifying weaknesses in an organization's cybersecurity posture. Quality Assurance pertains to ensuring that a product meets certain quality standards, but it does not specifically address security. Risk Management involves a broader approach to identifying, assessing, and prioritizing risks in various contexts, including but not limited to software security, without solely focusing on the integrity of software applications themselves.

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://comptiasecurityplus.examzify.com

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

SAMPLE