SECURITY PLUS PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://securityplus.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 15

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. **Which phase in the incident response process is concerned with addressing detected malware threats?**

   A. Preparation

   B. Identification

   C. Containment

   D. Recovery

2. **What type of ranking is considered subjective?**

   A. Qualitative

   B. Quantitative

   C. Absolute

   D. Statistical

3. **Which versions of SNMP are considered insecure?**

   A. SNMPv1 and SNMPv2

   B. SNMPv3 and SNMPv4

   C. SNMP and FTP

   D. SNMPv2 and TLS

4. **What is the primary focus of penetration testing?**

   A. Identifying software bugs

   B. Measuring network performance

   C. Exploiting vulnerabilities in a controlled manner

   D. Implementing security policies

5. **What is the secure version of Telnet?**

   A. Rlogin

   B. SSH

   C. SCP

   D. FTP

SAMPLE

6. What do you need to have in place if your primary plan fails during a data center upgrade?

A. Alternate Strategy

B. Redundant Backup Strategy

C. Backup/Backout Contingency Plan

D. Restoration Plan

7. What is a common drawback of cloud computing concerning data management?

A. Data Encryption Overhead

B. Blended Systems and Data

C. Physical Control Loss

D. Performance Latency

8. What is the outcome of a fuzzer when it encounters an exception?

A. It skips that input

B. It logs the input

C. It crashes the program

D. It ignores the error

9. Which protocol encapsulates EAP in an encrypted TLS tunnel?

A. PEAP (Protected EAP)

B. WPA

C. WEP

D. TLS

10. Which tool detects vulnerabilities by sending random input strings to an application?

A. Vulnerability scanner

B. Fuzzer

C. Port scanner

D. Sniffer

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which phase in the incident response process is concerned with addressing detected malware threats?

A. Preparation

B. Identification

C. Containment

D. Recovery

The phase in the incident response process that focuses on addressing detected malware threats is the identification phase. During this phase, security teams work to determine whether an incident has occurred, what type of malware or threat is present, and gather relevant information regarding the malicious activity. This involves recognizing indicators of compromise, analyzing security alerts, and confirming the nature and scope of the threat. By properly identifying the malware, organizations can understand its impact, formulate an appropriate response, and prevent further damage. This phase is crucial because accurate identification enables a more efficient and effective response in subsequent phases, ensuring that the appropriate containment, eradication, and recovery measures can be implemented accordingly.

2. What type of ranking is considered subjective?

A. Qualitative

B. Quantitative

C. Absolute

D. Statistical

Qualitative ranking is considered subjective because it relies on personal judgments, opinions, and interpretations rather than objective measurements. In qualitative assessments, factors such as feelings, perceptions, and experiences play a significant role in determining the ranking. For instance, when evaluating the effectiveness of a training program, the assessment may depend on participants' feedback and experiences, which can vary widely from one individual to another. In contrast, quantitative rankings are based on numerical data and objective criteria, making them less subjective and more standardized. Absolute rankings refer to a definitive scale or measurement, while statistical rankings involve data analysis methods that can vary but typically focus on objective calculations and metrics. Thus, qualitative rankings stand out as the type that is inherently subjective, featuring interpretations that can differ from person to person.

3. Which versions of SNMP are considered insecure?

A. SNMPv1 and SNMPv2

B. SNMPv3 and SNMPv4

C. SNMP and FTP

D. SNMPv2 and TLS

SNMPv1 and SNMPv2 are considered insecure due to their reliance on community strings for authentication. In these versions, the community strings function like passwords, but they are sent in plaintext over the network. This lack of encryption means that anyone with access to the network can potentially intercept these strings and gain unauthorized access to the SNMP-managed devices. Due to these vulnerabilities, SNMPv3 was developed to address these security shortcomings. It includes features such as authentication, encryption, and access control, significantly enhancing the security of SNMP communications. Therefore, SNMPv1 and SNMPv2 are not suitable for environments that require secure management of network devices, making them inherently less secure compared to SNMPv3. The other options either reference versions of SNMP that are secure (like SNMPv3), or do not pertain to SNMP exclusively, making them less relevant to the question of which versions are deemed insecure.

EXAMPLE

4. What is the primary focus of penetration testing?

A. Identifying software bugs

B. Measuring network performance

C. Exploiting vulnerabilities in a controlled manner

D. Implementing security policies

The primary focus of penetration testing is to exploit vulnerabilities in a controlled manner. This type of testing simulates an attack on a computer system, network, or web application to identify security weaknesses that could be exploited by malicious actors. By conducting a penetration test, organizations can evaluate their security posture and understand how well their defenses stand against actual attack scenarios. Penetration testing is a proactive approach to security, allowing organizations to identify and address vulnerabilities before they can be exploited in real attacks. The controlled nature of this testing means that it is performed by skilled professionals who follow ethical guidelines and legal regulations, ensuring that the testing does not cause unintended damage or disruption. In contrast, identifying software bugs focuses more on coding errors and functionality issues rather than security vulnerabilities. Measuring network performance pertains to the efficiency and speed of network systems, which is unrelated to security assessments. Implementing security policies is about establishing rules and guidelines to protect an organization's information, but it does not involve actively testing for vulnerabilities as penetration testing does.

5. What is the secure version of Telnet?

A. Rlogin

B. SSH

C. SCP

D. FTP

The secure version of Telnet is SSH, which stands for Secure Shell. SSH provides a secure channel over an unsecured network by using encryption to protect the data being transmitted. This is crucial because Telnet transmits data, including login credentials, in plaintext, making it vulnerable to interception by attackers. SSH not only encrypts the session but also offers enhanced authentication methods, such as public key authentication, which adds an extra layer of security compared to Telnet. This makes SSH the preferred choice for remote administration and secure file transfers, effectively replacing Telnet in most applications that require secure remote access. In contrast, the other options do not fulfill the role of a secure Telnet alternative. Rlogin is a remote access protocol that lacks the encryption capabilities provided by SSH. SCP, or Secure Copy Protocol, is used for securely transferring files but does not offer the command-line interface and session management capabilities that SSH provides. FTP, or File Transfer Protocol, likewise does not include security features and transmits data in plaintext, making it unsuitable for secure communication.

SAMPLE

6. What do you need to have in place if your primary plan fails during a data center upgrade?

A. Alternate Strategy

B. Redundant Backup Strategy

C. Backup/Backout Contingency Plan

D. Restoration Plan

Having a backup/backout contingency plan is crucial during a data center upgrade because it outlines the specific steps to take if the primary upgrade plan encounters unforeseen issues or fails. This contingency plan is designed to ensure that you can return to a known good state, minimizing downtime and disruption to services. A backup/backout contingency plan includes predefined procedures for reverting changes, restoring data, and securing the infrastructure. By preparing this plan ahead of time, organizations can ensure that they are equipped to handle emergencies effectively, thereby maintaining business continuity. While an alternate strategy might be useful in some scenarios, it generally focuses on alternative approaches rather than specifically addressing the need to revert or restore after a failed implementation. Similarly, a redundant backup strategy is aimed at ensuring data preservation and availability rather than the immediate recovery actions needed after an upgrade failure. A restoration plan primarily deals with bringing systems back online, which while important, doesn't account for the specific context of backtracking changes made during the upgrade process.

7. What is a common drawback of cloud computing concerning data management?

A. Data Encryption Overhead

B. Blended Systems and Data

C. Physical Control Loss

D. Performance Latency

One significant drawback of cloud computing regarding data management is the loss of physical control. When organizations utilize cloud services, they often store their data in remote servers managed by third-party providers. This means they do not have direct access to the physical hardware where their data resides, which can raise concerns about data security and compliance. Organizations may struggle with ensuring that their data is stored securely and is accessed only by authorized personnel, as the physical controls are out of their hands. This shift can complicate audits and regulatory compliance obligations, as the data is subject to the policies and protections of the cloud provider. Additionally, in instances of data breach or loss, the affected organization may have limited recourse because they lack direct oversight of the environment housing their information. This factor is crucial for businesses that handle sensitive information and must maintain strict data governance standards.

SAMPLE

8. What is the outcome of a fuzzer when it encounters an exception?

A. It skips that input

B. It logs the input

C. It crashes the program

D. It ignores the error

When a fuzzer encounters an exception, the expected outcome is that it may crash the program. Fuzzers are tools designed to test software for security vulnerabilities by inputting a wide range of unexpected or random data. When the software being tested fails to handle one of these inputs properly, it often results in an exception, which can lead to a crash. This behavior is crucial for identifying flaws in the program's error handling and stability under unusual conditions. Crashing the program can reveal serious vulnerabilities that could be exploited by an attacker, such as buffer overflows or other types of memory corruption. Identifying these weaknesses is essential for developers to patch and improve the robustness of their applications, ultimately enhancing their security posture. Therefore, the successful identification of a crash as a result of an exception indicates that the fuzzer is doing its job effectively by exposing potential security risks.

9. Which protocol encapsulates EAP in an encrypted TLS tunnel?

A. PEAP (Protected EAP)

B. WPA

C. WEP

D. TLS

Protected Extensible Authentication Protocol (PEAP) encapsulates EAP within a secure, encrypted Transport Layer Security (TLS) tunnel. This design enhances security by preventing interception and tampering of authentication messages during the authentication process. PEAP typically requires a server-side certificate, allowing clients to authenticate the server before establishing a secure connection, thus adding an additional layer of trust and security. By using PEAP, organizations can implement a more secure method for authenticating users within networks, particularly in scenarios requiring secure wireless connections. The encapsulation in the TLS tunnel ensures that sensitive information, such as user credentials, is not sent in plaintext, protecting it from eavesdroppers. This makes PEAP a favored choice in environments requiring enhanced security for network access authentication.

10. Which tool detects vulnerabilities by sending random input strings to an application?

A. Vulnerability scanner

B. Fuzzer

C. Port scanner

D. Sniffer

The choice of a fuzzer is accurate because a fuzzer is specifically designed to test applications by sending a wide range of random, unexpected, or malformed input strings to identify vulnerabilities. This technique can uncover security weaknesses such as buffer overflows, memory leaks, and other issues that could be exploited by attackers. Fuzzing helps to reveal how the application behaves under unexpected conditions, allowing developers to address these vulnerabilities before they can be exploited in a real-world attack. Its proactive approach to security testing is essential for ensuring robust software that can handle a variety of input scenarios gracefully. In contrast, vulnerability scanners systematically analyze code or systems for known vulnerabilities, but they do not employ the same tactic of using random inputs. Port scanners focus on identifying open ports and services running on a network, while sniffers capture network traffic but do not test applications for vulnerabilities through input manipulation. Each serves a different purpose in the security landscape, but the fuzzer is uniquely positioned to discover vulnerabilities that are not easily detected by other methods.

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://securityplus.examzify.com

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

SAMPLE