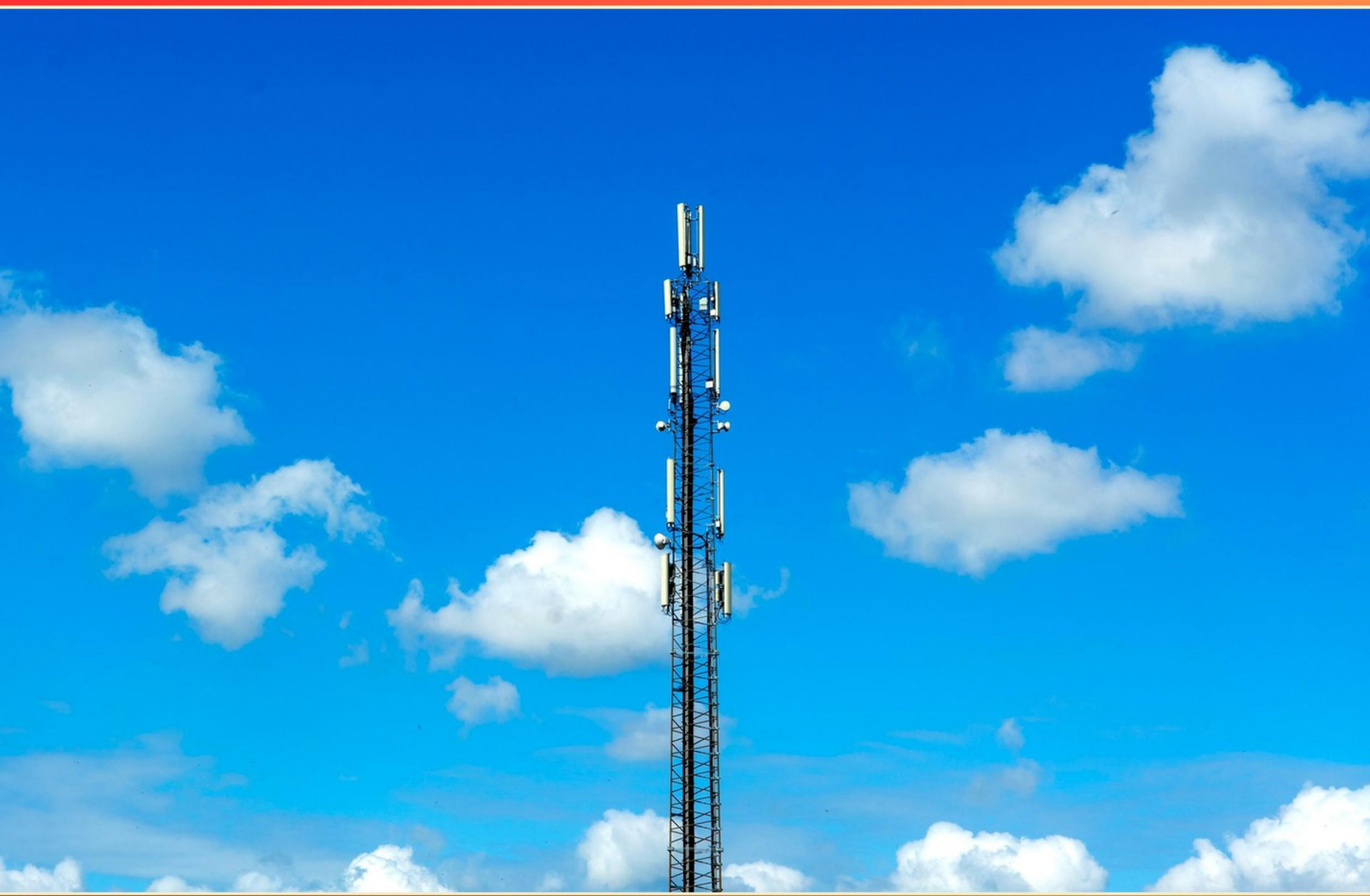
COMPTIA SECURITY+ (SY0-601) CERTIFICATION PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://comptiasecplussy0601.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

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 combination of approaches provides the most secure form of two-factor authentication?**

   A. Password and security question

   B. Password and fingerprint

   C. Password and smart card

   D. Password and one-time token

2. **In which scenario would steganography most likely be employed?**

   A. Obfuscation

   B. Integrity

   C. Non-repudiation

   D. Blockchain

3. **Which type of certificate would be best for a company that wants to secure multiple subdomains?**

   A. SAN

   B. Wildcard

   C. Extended validation

   D. Self-signed

4. **What is the primary goal of a disaster recovery plan?**

   A. To enhance system performance

   B. To ensure compliance with regulations

   C. To restore critical functions after a disaster

   D. To manage risks effectively

5. **What is the purpose of including a CVSS score in a vulnerability assessment report?**

   A. To validate the vulnerability exists through penetration testing

   B. To research appropriate mitigation techniques

   C. To find required software patches

   D. To prioritize remediation based on possible impact

SAMPLE

6. Which access control scheme allows an object's access policy to be determined by its owner?

A. Role-based access control

B. Discretionary access control

C. Mandatory access control

D. Attribute-based access control

7. Which RAID level should a cybersecurity administrator select to achieve two-drive redundancy for fault tolerance?

A. 0

B. 1

C. 5

D. 6

8. Which incident response step involves actions to protect critical systems while maintaining business operations?

A. Investigation

B. Containment

C. Recovery

D. Lessons learned

9. Which training activity would be most suitable for enhancing the skill levels of a company's developers?

A. A capture-the-flag competition

B. A phishing simulation

C. Physical security training

D. Basic awareness training

10. Which solution allows guests at a corporate headquarters to access the Internet while requiring acceptance of an acceptable use policy?

A. Implement open PSK on the APs

B. Deploy a WAF

C. Configure WIPS on the APs

D. Install a captive portal

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What combination of approaches provides the most secure form of two-factor authentication?

A. Password and security question

B. Password and fingerprint

C. Password and smart card

D. Password and one-time token

The most secure form of two-factor authentication combines something you know (like a password) with something you have (such as a smart card). This approach effectively mitigates the risks associated with single-factor authentication which relies solely on a password. A smart card serves as a physical device that must be possessed by the user, adding an additional layer of security. Even if an attacker manages to obtain the user's password through methods like phishing or social engineering, they would still need the physical smart card to gain access, making it significantly harder for unauthorized users to compromise an account. Other combinations like a password and a fingerprint (biometric) or a one-time token also provide strong security. However, they may be more vulnerable to specific attacks. For instance, biometric systems can be subject to spoofing, and one-time tokens can sometimes be intercepted or used incorrectly. In contrast, the use of a smart card implies a tangible item that must be physically present, enhancing security against remote attacks. Thus, the combination of password and smart card represents a robust form of two-factor authentication due to its dual-layer defense, combining knowledge with possession.

2. In which scenario would steganography most likely be employed?

A. Obfuscation

B. Integrity

C. Non-repudiation

D. Blockchain

Steganography is primarily used for the purpose of concealing information within other non-suspicious data, such as embedding messages within images or audio files. This technique allows individuals to communicate covertly without drawing attention to the existence of the hidden information. In the context of the choices provided, obfuscation aligns perfectly with the goal of steganography, which is to obscure the message's presence rather than its content. Obfuscation involves making information unclear or unintelligible, and steganography achieves this by hiding information in plain sight. Consequently, it serves as a method of obfuscating data communications, ensuring that unauthorized observers cannot easily discern the presence of sensitive content. The other scenarios, such as integrity, non-repudiation, and blockchain, do not directly apply to the primary functions and aims of steganography. Integrity pertains to ensuring the accuracy and trustworthiness of data, non-repudiation deals with preventing users from denying their actions, and blockchain focuses on secure, decentralized record-keeping without inherently involving hidden information. Thus, steganography's role in obfuscation makes it the most appropriate context among the provided options.

SAMPLE

3. Which type of certificate would be best for a company that wants to secure multiple subdomains?

A. SAN

B. Wildcard

C. Extended validation

D. Self-signed

*A Wildcard certificate would be the best choice for a company that wants to secure multiple subdomains because it simplifies the management of SSL/TLS certificates for various subdomains under a single main domain. For example, if the main domain is example.com, a Wildcard certificate can be used to secure *.example.com, which allows it to cover subdomains such as blog.example.com, shop.example.com, and mail.example.com without needing separate certificates for each one. This approach not only saves time and effort in obtaining and renewing multiple certificates but also reduces costs, as there is only one certificate to manage. Wildcard certificates are widely supported and recognized, making them a suitable solution for companies dealing with multiple subdomains. In contrast, SAN (Subject Alternative Name) certificates can also secure multiple domains but are typically used for different primary domains rather than subdomains of a single domain. Extended validation certificates are focused on providing a higher level of assurance and require a rigorous validation process, primarily intended for businesses wanting to demonstrate increased legitimacy rather than for managing multiple subdomains. Self-signed certificates, while useful for internal testing or development environments, do not offer the same level of trust and recognition as those issued by a Certificate Authority, making them less suitable for securing public-facing*

4. What is the primary goal of a disaster recovery plan?

A. To enhance system performance

B. To ensure compliance with regulations

C. To restore critical functions after a disaster

D. To manage risks effectively

The primary goal of a disaster recovery plan is to restore critical functions after a disaster. This involves creating strategies and procedures that will enable an organization to recover and continue operations following a disruptive event such as a natural disaster, cyber-attack, or equipment failure. The disaster recovery plan outlines how to quickly restore IT infrastructure and business operations to minimize downtime and impact on the organization. This is essential for ensuring business continuity, protecting data integrity, and maintaining service levels to customers and stakeholders. While aspects like enhancing system performance, ensuring compliance with regulations, and managing risks are important components of an overall business continuity strategy, they do not capture the main objective of disaster recovery, which specifically focuses on the immediate response and recovery actions post-disaster.

SAMPLE

5. What is the purpose of including a CVSS score in a vulnerability assessment report?

A. To validate the vulnerability exists through penetration testing

B. To research appropriate mitigation techniques

C. To find required software patches

D. To prioritize remediation based on possible impact

Including a CVSS (Common Vulnerability Scoring System) score in a vulnerability assessment report serves primarily to aid in prioritizing remediation efforts based on the potential impact of the identified vulnerabilities. The CVSS score provides a standardized metric that quantifies the severity of a vulnerability, taking into account factors such as exploitability, impact on confidentiality, integrity, and availability, and the potential for widespread harm. By categorizing vulnerabilities according to their risk level, organizations can effectively allocate resources and focus on addressing the most critical vulnerabilities first, which helps to mitigate the overall risk to their systems. For example, a vulnerability with a high CVSS score represents a more significant threat, warranting immediate attention, while those with lower scores may be scheduled for future consideration. Other options do not directly relate to the primary purpose of the CVSS score. Validating vulnerabilities through penetration testing, researching mitigation techniques, and finding software patches are important activities in vulnerability management, but they do not reflect the scoring system's main function, which is focused on risk assessment and prioritization.

6. Which access control scheme allows an object's access policy to be determined by its owner?

A. Role-based access control

B. Discretionary access control

C. Mandatory access control

D. Attribute-based access control

Discretionary access control (DAC) is an access control scheme where the owner of an object (such as a file or resource) has the authority to determine who can access it and what permissions those users have. This means that individual users can make decisions about who can read, write, or execute their objects. In a DAC system, the owner can grant or revoke access rights based on their preferences, which provides flexibility and facilitates the management of access permissions on a more personal basis. This model is commonly used in file systems and certain applications, allowing users to decide how their data is shared or restricted. Other access control schemes operate under different principles. For example, role-based access control (RBAC) assigns permissions based on the roles assigned to users within an organization rather than ownership. Mandatory access control (MAC) enforces restrictions based on regulations or policies determined by a central authority, rather than user discretion. Attribute-based access control (ABAC) utilizes attributes (such as user characteristics or resource types) to determine access rights, rather than relying on the owner's judgment.

SAMPLE

7. Which RAID level should a cybersecurity administrator select to achieve two-drive redundancy for fault tolerance?

A. 0

B. 1

C. 5

D. 6

Choosing RAID 6 for two-drive redundancy offers significant advantages in ensuring data integrity and availability. RAID 6 uses a technique known as striping with dual parity. This means that data is distributed across multiple disks in a way that allows for the recovery of data even if two drives fail simultaneously. In the event of a failure, RAID 6 can reconstruct the lost data from the remaining drives using the dual parity information, which is spread across the disk array. This construction makes it particularly beneficial in environments where data loss could have severe implications, allowing for high fault tolerance. While RAID levels like 1 and 5 also provide redundancy, they have limitations. RAID 1 offers redundancy via mirroring (one drive mirrors another), which enables only single-drive fault tolerance. RAID 5 provides single-drive redundancy using parity but cannot withstand the failure of more than one drive without data loss. Therefore, RAID 6 stands out as the best choice for scenarios that require strong protection against data loss due to multiple drive failures.

8. Which incident response step involves actions to protect critical systems while maintaining business operations?

A. Investigation

B. Containment

C. Recovery

D. Lessons learned

Containment is the incident response step that directly focuses on protecting critical systems and maintaining business operations. This stage is crucial in preventing further damage during a security incident, ensuring that the impact is minimized, and that essential business processes can continue functioning. By isolating affected systems, security teams can effectively limit the scope of the incident. This often involves implementing temporary solutions, such as shutting down compromised systems, blocking malicious traffic, or applying patches, while allowing unaffected systems and services to remain operational. The goal is to prevent the spread of the incident and to safeguard invaluable resources until a deeper investigation and recovery can take place. This differs from other stages in the incident response process. Investigation is primarily focused on identifying the causes and details of the incident. Recovery involves restoring systems and services to normal operation after they have been fixed and secured. The lessons learned phase is all about reflecting on the incident to improve future responses and security measures. Therefore, containment is specifically tailored to deal with immediate risks and protect critical operations during an incident.

SAMPLE

9. Which training activity would be most suitable for enhancing the skill levels of a company's developers?

A. A capture-the-flag competition

B. A phishing simulation

C. Physical security training

D. Basic awareness training

The selected answer pertains to a phishing simulation, which is effective for enhancing developers' skills in recognizing and addressing social engineering threats that could compromise code integrity or application security. Phishing attacks often target individuals, including software developers, by attempting to deceive them into divulging sensitive information or credentials. By participating in these simulations, developers can learn to identify suspicious emails, links, and messages, ultimately reinforcing their awareness of security practices and encouraging a stronger security culture within the organization. The other training activities, while valuable in their own contexts, do not specifically enhance the technical skillset or the specific threat awareness necessary for developers. For instance, a capture-the-flag competition primarily focuses on general cybersecurity skills and may not directly relate to the programming and development issues that developers face. Physical security training is important for protecting corporate assets but does not address the specific digital threats developers encounter. Basic awareness training typically covers general security principles and may not delve deeply enough into the specific issues that developers deal with on a day-to-day basis. Therefore, the phishing simulation stands out as the most appropriate choice for elevating developers' security skills.

10. Which solution allows guests at a corporate headquarters to access the Internet while requiring acceptance of an acceptable use policy?

A. Implement open PSK on the APs

B. Deploy a WAF

C. Configure WIPS on the APs

D. Install a captive portal

A captive portal is a web page that users must view and interact with before being granted broader access to the Internet. This page often includes an acceptable use policy that must be acknowledged by the user. By utilizing a captive portal, the corporate headquarters can effectively ensure that guests agree to the organization's rules and policies regarding Internet use before accessing the network. The use of open PSK (Pre-Shared Key) on access points does not provide a mechanism for policy acceptance, as it simply allows access without any conditions or acknowledgment from the guest, making it less secure and controlled. A Web Application Firewall (WAF) is designed primarily to protect web applications by filtering and monitoring HTTP traffic, which does not facilitate the guest access process or policy acceptance. A Wireless Intrusion Prevention System (WIPS) focuses on monitoring and protecting wireless networks from intrusions and does not serve to authenticate or inform guests of usage policies. Thus, a captive portal is the most suitable solution for the requirement presented.

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://comptiasecplussy0601.examzify.com

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

SAMPLE