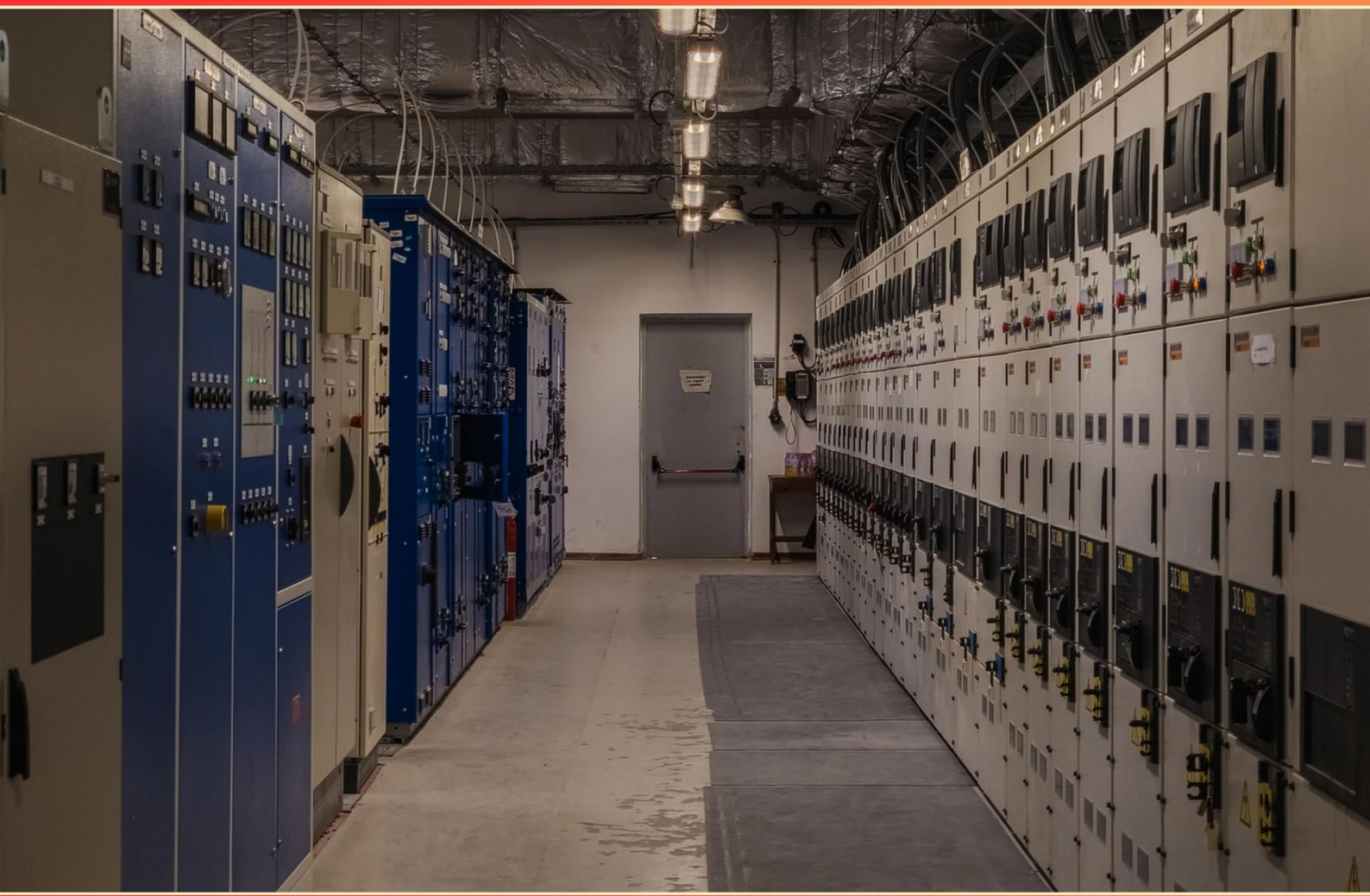
SECURITY+ MASTER DECK PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://secplusmasterdeck.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 term best describes malicious software that warns of deleting files when a specific event occurs, such as an employee's termination?

A. Logic bomb

B. Rootkit

C. Trojan horse

D. Worm

2. Which type of device is often used to monitor access and enforce security policies in an organization?

A. IoT sensors

B. Network switches

C. Access control systems

D. Routers

3. When connecting to an unsecure wired network, which threat is least likely to be a concern?

A. Man-in-the-middle attacks

B. Evil twins

C. Packet sniffing

D. Data encryption

4. Which method is NOT effective in preventing server-side request forgery (SSRF) attacks?

A. Implementing strict input validation

B. Removing all SQL code from submitted HTTP queries

C. Restricting outbound connections

D. Logging and monitoring requests

5. Which of these threats is least likely to be a common email threat vector?

A. Phishing

B. Malware

C. Cross-site scripting

D. Ransomware

SAMPLE

6. Which of the following is not a common firmware defense mechanism for protecting against exploits?

A. Encrypting firmware

B. Regular updates to the firmware

C. Hardware authentication

D. Using open-source firmware

7. What type of cyber attack is characterized by a link in an email that appears legitimate but is designed to deceive users?

A. Spear phishing

B. Whaling

C. Phishing

D. Smishing

8. Which of the following is not considered a best practice to defend against business email compromise (BEC) attacks?

A. Implementing multi-factor authentication

B. Insisting on confirmation through multiple communication channels

C. Delete all attachments from emails

D. Training employees on phishing awareness

9. What is a common motivation for nation-state threat actors?

A. Financial gain

B. Espionage

C. Cyber vandalism

D. Data theft for sale

10. What type of effort do postings from foreign agents during a political campaign represent?

A. Propaganda

B. Disinformation

C. Censorship

D. Cyber espionage

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What term best describes malicious software that warns of deleting files when a specific event occurs, such as an employee's termination?

A. Logic bomb

B. Rootkit

C. Trojan horse

D. Worm

The term that best describes malicious software designed to trigger a harmful action, such as deleting files when a specific event occurs (like an employee's termination), is a logic bomb. A logic bomb is a piece of malicious code that is programmed to execute a specified action when certain conditions are met. In this case, the condition is the termination of an employee, which serves as the trigger for the logic bomb to execute its destructive function. Logic bombs can be particularly insidious because they may remain dormant until the triggering event occurs, making them hard to detect during normal operations. Rootkits typically provide unauthorized access to a computer while hiding their presence. They do not specifically relate to triggering actions based on events like employee terminations. Trojan horses disguise themselves as legitimate software but often perform harmful actions without the user's knowledge, while worms are self-replicating programs that spread across networks. None of these options fit the specific scenario given in the question, emphasizing why the logic bomb is the most appropriate answer.

2. Which type of device is often used to monitor access and enforce security policies in an organization?

A. IoT sensors

B. Network switches

C. Access control systems

D. Routers

Access control systems are specifically designed to monitor and manage access to physical or digital resources within an organization, enforcing security policies effectively. These systems can include mechanisms such as card readers, biometric scanners, keypads, and software that logs access attempts, providing a detailed audit trail. By using these devices, organizations can determine who has access to specific areas or information and can enforce rules regarding that access, such as time restrictions or user permission levels. In contrast, IoT sensors are primarily used for data gathering and monitoring environmental conditions but do not inherently enforce security policies related to access. Network switches manage and direct traffic within a network but lack the access control capabilities of dedicated access control systems. Routers, on the other hand, facilitate network connectivity and can provide some level of security through firewalls or access control lists, but they are not tailored to monitor or enforce access policies in the same comprehensive manner as access control systems do.

SAMPLE

3. When connecting to an unsecure wired network, which threat is least likely to be a concern?

A. Man-in-the-middle attacks

B. Evil twins

C. Packet sniffing

D. Data encryption

In the context of connecting to an unsecured wired network, data encryption is least likely to be a concern because encryption typically relates to the protection of data in transit or at rest. In unsecured environments, such as public or poorly secured wired networks, the primary threats involve direct interception and manipulation of data by malicious individuals. Man-in-the-middle attacks, evil twins, and packet sniffing represent active or passive threats that exploit the vulnerabilities of an unsecure network. For instance, a man-in-the-middle attack can occur when an attacker intercepts communications between two parties. Evil twin threats, while more commonly associated with wireless networks, might also apply if a rogue device mimics legitimate network services. Packet sniffing refers to the ability to capture and analyze network traffic, allowing attackers to glean sensitive information. In contrast, data encryption is a defensive measure intended to protect information, and while it is essential for safeguarding data during transmission or storage, its absence is what heightens concern in this type of network. If encryption is not employed, data traveling over the network is inherently vulnerable, but in this context, the existence of encryption is what defines a potential concern rather than a direct threat like those listed.

4. Which method is NOT effective in preventing server-side request forgery (SSRF) attacks?

A. Implementing strict input validation

B. Removing all SQL code from submitted HTTP queries

C. Restricting outbound connections

D. Logging and monitoring requests

Server-Side Request Forgery (SSRF) attacks exploit the vulnerabilities of a server by allowing an attacker to send crafted requests to unintended destinations. When evaluating the methods to mitigate these attacks, it is clear that removing SQL code from submitted HTTP queries does not directly address the root of SSRF vulnerabilities. While SQL injection is a different type of attack that manipulates database queries, SSRF primarily concerns itself with how the server processes outbound connections based on input it receives. Therefore, simply removing SQL code does not prevent SSRF because the attack does not inherently rely on SQL injection techniques. Instead, SSRF focuses on how requests are crafted and sent from the server, often targeting internal resources or services. In contrast, implementing strict input validation ensures that only expected and legitimate requests are processed. Restricting outbound connections limits the server's capacity to initiate requests to external or internal systems, thereby reducing the attack surface for potential SSRF exploits. Finally, logging and monitoring requests help in identifying and responding to anomalous behavior that might suggest an ongoing SSRF attack or other vulnerabilities being exploited. Thus, the method that does not effectively prevent SSRF attacks is the removal of SQL code from submitted HTTP queries, as it does not address the mechanics of how these

SAMPLE

5. Which of these threats is least likely to be a common email threat vector?

A. Phishing

B. Malware

C. Cross-site scripting

D. Ransomware

Cross-site scripting (XSS) is least likely to be a common email threat vector because it primarily exploits vulnerabilities in web applications and is executed in the context of a user's browser rather than through an email client. XSS attacks generally involve injecting malicious scripts into web pages that are then viewed by users. This means the attacker typically needs to lure victims to a compromised website where the scripts can run, rather than sending emails. On the other hand, phishing directly targets users through email by tricking them into providing sensitive information, such as usernames and passwords. Malware can also be widely distributed via email attachments or links, making it a prominent email threat. Ransomware can be spread through malicious email attachments or links that, when activated, encrypt user files and demand a ransom. Therefore, these threats are more directly associated with email than cross-site scripting, which operates in a different context.

6. Which of the following is not a common firmware defense mechanism for protecting against exploits?

A. Encrypting firmware

B. Regular updates to the firmware

C. Hardware authentication

D. Using open-source firmware

Using open-source firmware is not traditionally considered a common defense mechanism for protecting against firmware exploits. While open-source firmware has its own merits, such as transparency and community-driven development, it does not inherently include specific security features designed to protect against exploits. Security mechanisms are more focused on methods like encrypting firmware, implementing regular updates, and utilizing hardware authentication to safeguard firmware from unauthorized modifications and attacks. Encrypting firmware helps in preventing tampering and ensures that only authenticated code can be executed. Regular updates enable the deployment of security patches and improvements that can address newly discovered vulnerabilities. Hardware authentication is a crucial mechanism to verify the integrity of firmware and ensure that only trusted firmware can run on the hardware, thereby thwarting potential exploits. In contrast, using open-source firmware doesn't automatically provide these specific protections, which is why it stands out as an option that does not align with common firmware defense strategies.

SAMPLE

7. What type of cyber attack is characterized by a link in an email that appears legitimate but is designed to deceive users?

A. Spear phishing

B. Whaling

C. Phishing

D. Smishing

The type of cyber attack characterized by a link in an email that appears legitimate but is designed to deceive users is known as phishing. Phishing attacks typically involve fraudulent emails that mimic reputable organizations, often leading recipients to click on harmful links that may harvest sensitive information or deliver malware. Spear phishing is similar to phishing but is more targeted. It focuses on specific individuals or organizations rather than a broad audience, which is not the case in this scenario. Whaling is a variant of phishing aimed at high-profile targets, such as executives, making it a more sophisticated form of targeted attacks. Smishing, on the other hand, involves malware delivered via SMS messages rather than email, so it does not fit the description provided in the question. Therefore, the correct choice clearly identifies a general form of deceptive cyber attacks aimed at a broad range of potential victims via email.

8. Which of the following is not considered a best practice to defend against business email compromise (BEC) attacks?

A. Implementing multi-factor authentication

B. Insisting on confirmation through multiple communication channels

C. Delete all attachments from emails

D. Training employees on phishing awareness

Deleting all attachments from emails is not considered a best practice for defending against business email compromise (BEC) attacks because it can hinder legitimate business communication and collaboration. Attachments are a common and necessary component of many email communications, such as invoices, reports, and other documents. While it is important to be cautious about attachments due to the risk of malware, completely deleting them overlooks the potential for secure and necessary business interactions. In contrast, implementing multi-factor authentication adds an essential layer of security, making it more difficult for unauthorized users to gain access to email accounts. Insisting on confirmation through multiple communication channels helps to verify the authenticity of emails, thereby preventing potential fraud or deception. Training employees on phishing awareness empowers them to recognize and respond appropriately to suspicious emails, significantly reducing the risk of BEC attacks.

SAMPLE

9. What is a common motivation for nation-state threat actors?

A. Financial gain

B. Espionage

C. Cyber vandalism

D. Data theft for sale

Nation-state threat actors are often motivated primarily by espionage, which involves gathering intelligence to further their national interests. This can include spying on other governments, military operations, or economic strategies, providing valuable insights that can guide policy decisions and strategic planning. The focus on espionage is driven by the desire to gain a competitive advantage over rival nations. Unlike individual hackers or cybercriminal groups who may be primarily seeking financial gain, nation-state actors typically operate under state sponsorship and have access to significant resources and sophisticated tools that aid in these intelligence-gathering missions. Engaging in espionage can involve cyber operations that infiltrate critical infrastructure systems, steal sensitive information, or disrupt military capabilities, all of which aim to protect or enhance a nation's security and power on the global stage. As such, understanding the motivations behind nation-state activities highlights the complexity of cybersecurity threats that go beyond mere financial considerations, emphasizing geopolitical implications in the digital realm.

10. What type of effort do postings from foreign agents during a political campaign represent?

A. Propaganda

B. Disinformation

C. Censorship

D. Cyber espionage

Postings from foreign agents during a political campaign represent disinformation as they often involve the deliberate spread of misleading or false information aimed at influencing public perception and behavior. Disinformation is a tactic used to undermine trust, create confusion, and shift public opinion by promoting narratives that may benefit one political agenda over another. This manipulation is particularly concerning during political campaigns, as it can disrupt democratic processes and influence electoral outcomes by swaying voters based on fabricated or distorted information rather than facts. In the context of foreign involvement, these postings are typically designed to exploit divisions within a target population or to create tensions, further emphasizing the strategic use of disinformation in modern political landscapes.

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://secplusmasterdeck.examzify.com

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

SAMPLE