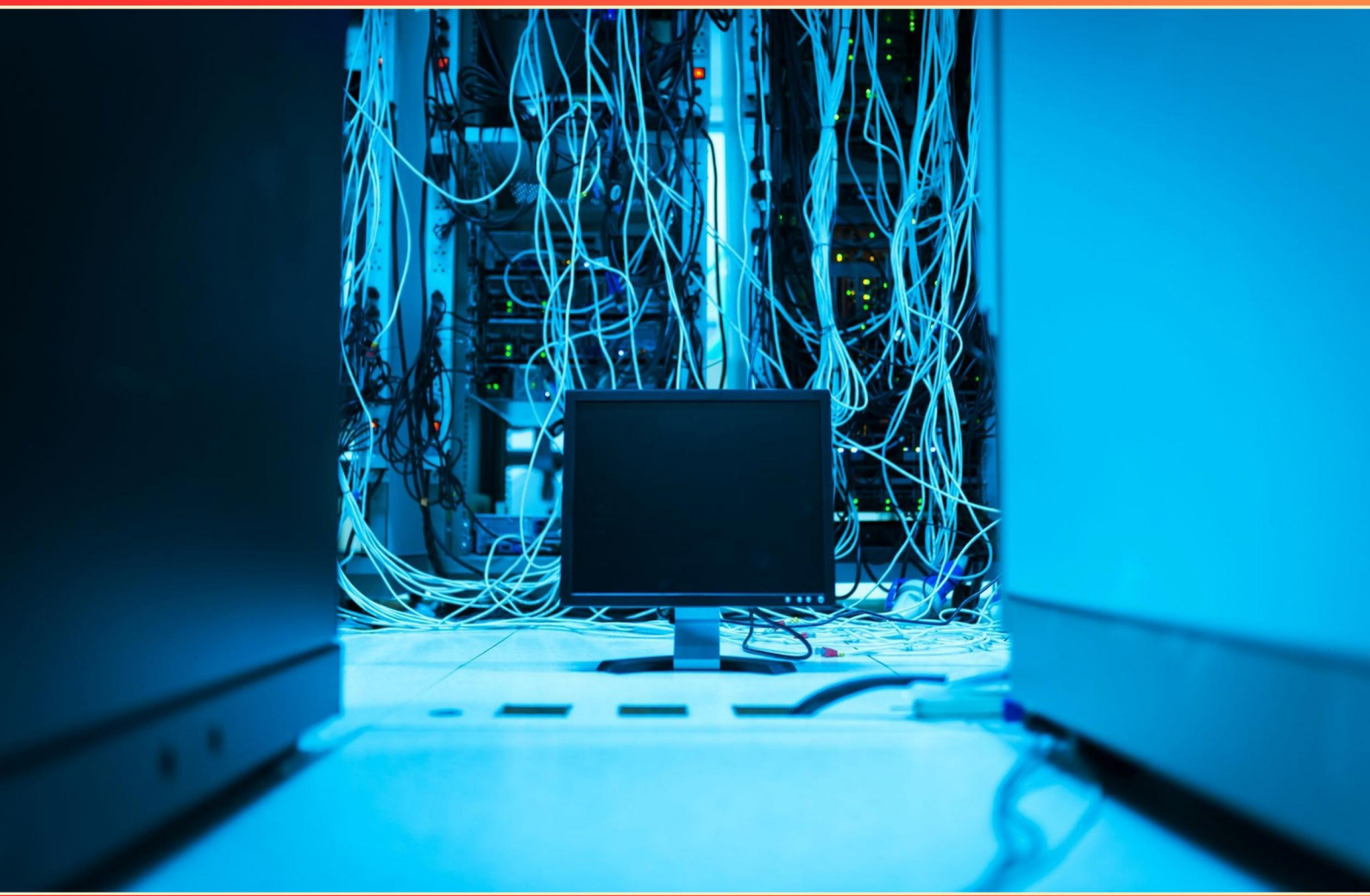
SYSTEMS SECURITY CERTIFIED PRACTITIONER (SSCP) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://syssecuritypractitionersscp.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 are the core concepts of business continuity planning (BCP)?

A. Cutting operational costs during downtime

B. Ensuring mission-critical functions continue during and after a disaster

C. Reversing the effects of a disaster

D. Prioritizing safety over business objectives

2. A password audit checks for what?

A. Minimum password length

B. Password aging

C. All of the items listed

D. Blank passwords

3. Which framework offers guidelines for developing cybersecurity risk management programs?

A. ISO 27001

B. NIST Cybersecurity Framework

C. CIS Controls

D. COBIT

4. Which action is crucial during the digital evidence collection process to maintain a chain of custody?

A. Shutting down the system immediately

B. Documenting the evidence collection process

C. Rebooting the system for clarity

D. Ignoring physical access to the machine

5. What is enforced by Passfilt.dll in terms of password requirements?

A. 8 character minimum password length

B. Each password must include upper case, lower case, numbers, and special characters

C. 90 day password changes

D. 6 character minimum password length

SAMPLE

6. Which of the following is a common outcome of effective vulnerability management?

A. Increased risk of data breaches

B. Reduction of system downtime

C. Increase in the number of vulnerabilities

D. Improved compliance with regulatory requirements

7. Which of the following is NOT a characteristic of RSA?

A. Can produce a digital signature

B. Relies on large prime number factoring

C. Uses third party key distribution centers

D. Is based on a symmetric algorithm

8. Which of the following statements best describes the importance of data backups?

A. They are only necessary for large organizations

B. They help recover from data loss events

C. They replace the need for security measures

D. They should be done once a year

9. What does the term 'attack surface' refer to in cybersecurity?

A. The number of systems on a network

B. The geographical location of servers

C. The sum of all vulnerabilities in a system

D. The total number of user accounts

10. Is it true that only law enforcement personnel are qualified to perform computer forensic investigations?

A. True

B. False

C. Partially true

D. None of the above

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What are the core concepts of business continuity planning (BCP)?

A. Cutting operational costs during downtime

B. Ensuring mission-critical functions continue during and after a disaster

C. Reversing the effects of a disaster

D. Prioritizing safety over business objectives

Business continuity planning (BCP) is fundamentally concerned with ensuring that an organization can maintain and recover its essential functions in the face of a disaster or unexpected disruption. The core concept involves preparing for, responding to, and recovering from incidents that can adversely impact operations. Choosing to focus on ensuring that mission-critical functions continue during and after a disaster is central to the aims of BCP. It involves identifying the critical business processes necessary for maintaining operations and outlining the strategies and resources required to support them during adverse events. This approach ensures that an organization can quickly adapt and sustain essential services, minimize downtime, and mitigate loss. Other options, while related to aspects of risk management and operational considerations, do not encapsulate the fundamental essence of business continuity planning. For instance, focusing on cutting operational costs or reversing the effects of a disaster may divert attention from the primary goal of keeping critical functions active. Even prioritizing safety is important, but in the context of BCP, the primary focus is on continuity and recovery of critical business operations rather than safety as an isolated priority.

2. A password audit checks for what?

A. Minimum password length

B. Password aging

C. All of the items listed

D. Blank passwords

A password audit checks for various critical aspects of password security, aiming to enhance the overall security posture of an organization. By selecting an option that encompasses all items listed, it recognizes the multifaceted nature of password policies. Minimum password length is an important aspect because it ensures that passwords are sufficiently complex to resist brute-force attacks. When passwords are too short, they can be cracked relatively quickly, which undermines the integrity of the authentication process. Password aging is another critical factor, as it dictates how frequently passwords must be changed. Regular updating of passwords helps prevent unauthorized access through compromised credentials that may remain undiscovered for extended periods. Blank passwords represent a significant vulnerability because they allow unauthorized access without any credential checks. Ensuring that all user accounts have assigned passwords is paramount in maintaining security. By choosing an option that encompasses the evaluation of minimum password length, password aging, and the presence of blank passwords, a password audit effectively addresses key vulnerabilities that need to be managed for a robust security policy.

SAMPLE

3. Which framework offers guidelines for developing cybersecurity risk management programs?

A. ISO 27001

B. NIST Cybersecurity Framework

C. CIS Controls

D. COBIT

The NIST Cybersecurity Framework is specifically designed to provide organizations with a structured approach to developing and managing cybersecurity risk management programs. It emphasizes identifying, protecting, detecting, responding to, and recovering from cybersecurity incidents. This framework is flexible and can be adapted to different types and sizes of organizations, making it an invaluable resource for establishing risk management practices. The NIST Cybersecurity Framework encourages organizations to assess their current cybersecurity practices against a set of standards and guidelines, helping them identify gaps and areas for improvement. This approach enables organizations to effectively prioritize their resources based on the risks they face, thus enhancing their overall security posture. In contrast, other frameworks like ISO 27001, while they pertain to information security management, focus more specifically on establishing an Information Security Management System (ISMS) rather than directly offering guidelines for developing a comprehensive cybersecurity risk management program. CIS Controls provide a set of best practices for securing systems and data but are not as broad or structured in terms of risk management processes as the NIST Cybersecurity Framework. COBIT is mainly geared towards IT governance and management and, while it addresses risk, it is not solely focused on cybersecurity risk management as the NIST framework is.

4. Which action is crucial during the digital evidence collection process to maintain a chain of custody?

A. Shutting down the system immediately

B. Documenting the evidence collection process

C. Rebooting the system for clarity

D. Ignoring physical access to the machine

Documenting the evidence collection process is crucial during the digital evidence collection phase to maintain a chain of custody because it provides a detailed account of every action taken with respect to the evidence. This includes recording who collected the evidence, the time and date of collection, the location, and the condition of the evidence at each stage of handling. Maintaining clear and meticulous documentation ensures that the integrity of the evidence is preserved, which is vital for legal proceedings. A well-documented chain of custody allows for the evidence to be traced back to its source, verifies that it has not been altered, and establishes its authenticity, which is critical for establishing its validity in a court of law. The other choices do not support the integrity of the evidence collection process. Shutting down the system immediately may lead to loss of volatile data, while rebooting the system can alter evidence, compromising its integrity. Ignoring physical access to the machine disregards potential tampering that could affect the evidence's admissibility. Thus, documentation is not only a best practice but an essential part of legal and forensic protocols to ensure that the collected evidence can withstand scrutiny.

SAMPLE

5. What is enforced by Passfilt.dll in terms of password requirements?

A. 8 character minimum password length

B. Each password must include upper case, lower case, numbers, and special characters

C. 90 day password changes

D. 6 character minimum password length

Passfilt.dll is a functionality in Windows systems that is responsible for enforcing password complexity requirements. This means that it checks the passwords being created or changed to ensure they meet certain criteria. When a password requirement includes stipulations such as the necessity for upper case letters, lower case letters, numbers, and special characters, it enhances the security of user accounts by making passwords harder to guess or crack. This complexity is a vital aspect of password policies because it ensures that passwords are not simple or easily predictable, thus significantly reducing the potential for unauthorized access. When users create a password that adheres to these rules, they help to bolster the overall security posture of the system. This choice correctly aligns with the functionality of Passfilt.dll, which is designed to impose stricter passwords, thereby addressing the growing concerns over security vulnerabilities that can arise from weak password practices. Other options mentioned pertain to specific character lengths or password expiration durations, which are managed through different settings and policies within the operating system, but do not directly reflect the specific enforcement role of Passfilt.dll regarding password complexity requirements.

6. Which of the following is a common outcome of effective vulnerability management?

A. Increased risk of data breaches

B. Reduction of system downtime

C. Increase in the number of vulnerabilities

D. Improved compliance with regulatory requirements

Effective vulnerability management plays a critical role in strengthening an organization's security posture. One of the primary benefits is the reduction of system downtime. By actively identifying, assessing, and mitigating vulnerabilities, an organization can proactively address issues before they lead to security incidents. This proactive approach minimizes the likelihood of successful attacks, which can result in significant disruptions to services and operations. When vulnerabilities are managed properly, systems can remain operational without the interruptions that often come from responding to and recovering from security breaches or incidents. Additionally, regular updates and patches can improve system performance, further contributing to maintenance of uptime. The other outcomes are either negative or do not directly result from effective vulnerability management. For instance, increased risks or number of vulnerabilities would indicate ineffective management, while improved compliance, while beneficial, is usually a secondary effect rather than a direct outcome of managing vulnerabilities effectively.

SAMPLE

7. Which of the following is NOT a characteristic of RSA?

A. Can produce a digital signature

B. Relies on large prime number factoring

C. Uses third party key distribution centers

D. Is based on a symmetric algorithm

The choice that states RSA is based on a symmetric algorithm is correct to identify as not a characteristic of RSA. RSA, which stands for Rivest-Shamir-Adleman, is fundamentally an asymmetric encryption algorithm. Asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption. This contrasts with symmetric algorithms, which rely on a single key for both encryption and decryption. RSA's security is based on the mathematical difficulty of factoring large prime numbers. This is a crucial aspect of RSA and underlies its functionality and strength in securing communications. Additionally, RSA is indeed capable of producing digital signatures, enhancing its utility in verifying authenticity and securing messages. Furthermore, while RSA can utilize third-party key distribution centers in certain systems for facilitating secure communication, this is not a defining characteristic of RSA itself. Overall, the distinction of RSA as an asymmetric algorithm is fundamental to its operation and application in cryptography.

8. Which of the following statements best describes the importance of data backups?

A. They are only necessary for large organizations

B. They help recover from data loss events

C. They replace the need for security measures

D. They should be done once a year

The importance of data backups primarily revolves around their role in facilitating the recovery from data loss events. Data loss can occur due to various reasons, including hardware failure, accidental deletion, ransomware attacks, or natural disasters. In such scenarios, having an effective backup strategy in place ensures that an organization can restore its data to a pre-loss state, minimizing the impact on operations and maintaining business continuity. Regular backups can also provide recovery points, allowing users to retrieve the most current information before the data loss incident occurred. In addition to recovery, backups are a critical part of an organization's overall risk management and disaster recovery plan. They fulfill a preventive function, reducing the likelihood of irreversible damage to important information that is otherwise essential for functioning operations. This underscores why having a solid backup strategy is vital for organizations of all sizes, not just large ones. Other choices fall short of capturing the comprehensive role of backups in data protection. For instance, backups should be considered a supplement to security measures rather than a replacement, and they need to be performed more frequently than just once a year to ensure data resilience.

9. What does the term 'attack surface' refer to in cybersecurity?

A. The number of systems on a network

B. The geographical location of servers

C. The sum of all vulnerabilities in a system

D. The total number of user accounts

The term 'attack surface' in cybersecurity refers to the sum of all vulnerabilities in a system. This concept encompasses all the different points where an unauthorized user (an attacker) could enter or extract data from a system. A larger attack surface indicates that there are more potential vulnerabilities to exploit, making it crucial for security professionals to understand and mitigate these risks. The attack surface can include various elements such as software applications, network services, user accounts, protocols in use, and even physical components like network hardware. By identifying and analyzing the attack surface, organizations can better prioritize their security efforts, ensuring that the most vulnerable areas are addressed first.

SAMPLE

10. Is it true that only law enforcement personnel are qualified to perform computer forensic investigations?

A. True

B. False

C. Partially true

D. None of the above

The assertion that only law enforcement personnel are qualified to perform computer forensic investigations is false. While it is true that law enforcement agencies have specialized training and tools to conduct forensics for legal cases, they are not the only entities capable of performing these investigations. Computer forensic investigations can also be carried out by private firms, corporate security teams, and independent professionals who have the necessary expertise. In various situations, organizations may conduct their own forensic investigations to handle internal incidents, protect proprietary information, and comply with regulatory requirements. Moreover, educational institutions offer programs and certifications that train individuals in forensic methodologies, allowing a broader range of professionals to obtain skills in this field. The option suggesting that this statement is partially true might imply that there are certain circumstances where only law enforcement can conduct specific types of investigations, but the general capability for conducting these investigations is not restricted solely to law enforcement personnel. Therefore, stating that it is false better captures the broader reality of the field of computer forensics.

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://syssecuritypractitionersscp.examzify.com

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

SAMPLE