SANS SECURITY'S FOUNDATION PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://sanssecurityfoundation.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 technique is used to ensure data integrity in transit?

A. Encryption

B. Hashing

C. Tokenization

D. Decryption

2. What is the Risk Strategy that involves stopping risky business practices?

A. Risk Reduction

B. Risk Transfer

C. Risk Mitigation

D. Risk Avoidance

3. What type of data does TLS primarily protect?

A. Data at rest

B. Data in transit

C. Data in storage

D. Data left on devices

4. Which approach is primarily used to prevent unauthorized access to sensitive information?

A. Risk assessment

B. Encryption

C. Public Key Infrastructure

D. Firewalls

5. What is the primary role of antivirus software?

A. To create secure passwords for users

B. To protect systems from malware by detecting and removing it

C. To manage user accounts

D. To analyze network traffic

6. What is the purpose of incident response planning?

A. To monitor network traffic continuously

B. To respond effectively to security incidents

C. To design new software systems

D. To conduct employee evaluations

SAMPLE

7. The aim of patch management is to?

A. Identify employee needs

B. Acquire and install software updates for security improvements

C. Enhance physical security measures

D. Reduce the number of software applications

8. What does risk acceptance imply in a business context?

A. Eliminating all potential risks faced

B. Allowing certain risks to exist after mitigation strategies

C. Implementing extensive control measures

D. Documenting every possible risk scenario

9. Which statement best describes the operational model of "malware as a service"?

A. It focuses on creating security features for users

B. It provides tools and malware for criminal activities

C. It offers free trials of malware detection software

D. It licenses users to develop their own malware

10. What does the acronym SIEM stand for?

A. System Information and Event Management

B. Security Information and Event Management

C. Security Intelligence and Event Management

D. Security Information and Encryption Management

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What technique is used to ensure data integrity in transit?

A. Encryption

B. Hashing

C. Tokenization

D. Decryption

Hashing is a technique used to ensure data integrity in transit by creating a fixed-size string of characters from input data, regardless of its size. This string, often referred to as a hash value or checksum, is generated through a specific algorithm that produces a unique value for different sets of input data. When data is sent over a network, the sender can compute the hash of the original data and send both the data and the hash value to the receiver. Upon receipt, the receiver will compute the hash of the received data and compare it to the hash value sent by the sender. If both hash values match, it indicates that the data has not been altered during transit, thereby ensuring its integrity. This process does not obscure the data but confirms its authenticity and completeness. Other techniques serve different purposes; for example, encryption primarily protects confidentiality by transforming data into an unreadable format for unauthorized users, while tokenization replaces sensitive data with non-sensitive equivalents to minimize exposure to risk. Decryption is the reverse of encryption, aiming to restore the readable form of encrypted data, but it does not verify data integrity.

2. What is the Risk Strategy that involves stopping risky business practices?

A. Risk Reduction

B. Risk Transfer

C. Risk Mitigation

D. Risk Avoidance

The strategy of stopping risky business practices is best described by risk avoidance. This approach involves eliminating any activities or conditions that could lead to potential risks. When an organization adopts risk avoidance, it makes deliberate decisions to steer clear of specific actions or processes that may expose it to danger or loss. For example, if a company identifies that entering a new market poses significant risks of financial loss or reputational damage, it might choose not to enter that market at all. By making this choice, the organization effectively avoids any risks that could arise from that market entry. In contrast, risk reduction focuses on minimizing the impact or likelihood of risks rather than eliminating them completely. Risk transfer involves shifting the responsibility of a risk to another party, such as through insurance. Risk mitigation includes implementing measures to reduce the severity of potential negative outcomes but still allows for the possibility of the risk occurring. These distinctions clarify why stopping risky business practices aligns closely with the concept of risk avoidance.

SAMPLE

3. What type of data does TLS primarily protect?

A. Data at rest

B. Data in transit

C. Data in storage

D. Data left on devices

TLS (Transport Layer Security) primarily protects data in transit. This security protocol is designed to ensure privacy and data integrity when transmitting data over a network. It encrypts the data being sent between the sender and receiver, making it challenging for unauthorized parties to intercept and understand the information during transmission. This encryption safeguards against eavesdropping and tampering, which are significant threats in the context of data moving across potentially insecure networks such as the internet. The other choices refer to different states of data. Data at rest pertains to inactive data stored physically in any digital form (like databases or files on a disk). Data in storage is somewhat synonymous with data at rest. Meanwhile, data left on devices refers to information that may be temporarily cached or saved on devices but is not actively being transmitted over a network. These states do not align with the specific function of TLS, which focuses solely on protecting data while it is being transmitted.

4. Which approach is primarily used to prevent unauthorized access to sensitive information?

A. Risk assessment

B. Encryption

C. Public Key Infrastructure

D. Firewalls

Encryption is a critical method for protecting sensitive information by converting data into a format that cannot be easily understood by unauthorized individuals. This process ensures that even if data is intercepted or accessed without permission, it remains unintelligible without the appropriate decryption key. By rendering the information unreadable to anyone who does not have the requisite credentials, encryption acts as a robust barrier against unauthorized access. In addition, while risk assessment, public key infrastructure, and firewalls contribute to overall security, they serve different functions. Risk assessments identify vulnerabilities and potential threats, enabling organizations to make informed decisions about security measures. Public Key Infrastructure (PKI) is a framework used to manage digital certificates and encryption keys, but it is not a preventive technology in itself; rather, it supports encryption and secure communications. Firewalls help control network traffic and establish a barrier between a trusted internal network and untrusted external networks, but they do not directly encrypt sensitive information. Each of these plays a significant role in a security architecture, but encryption specifically focuses on encoding data to prevent unauthorized access.

SAMPLE

5. What is the primary role of antivirus software?

A. To create secure passwords for users

B. To protect systems from malware by detecting and removing it

C. To manage user accounts

D. To analyze network traffic

The primary role of antivirus software is to protect systems from malware by detecting and removing it. This includes a range of malicious software threats, such as viruses, worms, Trojan horses, ransomware, and spyware. Antivirus software works by scanning files, monitoring system behavior, and utilizing signature-based detection methods to identify known malware signatures. It also adapts to recognize new threats through heuristics and other techniques aimed at identifying suspicious activity. This protective function is essential in maintaining the integrity and security of computer systems, preventing data breaches, and ensuring safe usage of technology. By regularly updating its database of malware signatures and employing advanced detection methods, antivirus software serves as a crucial line of defense against various cyber threats, helping to safeguard user data and overall system performance.

6. What is the purpose of incident response planning?

A. To monitor network traffic continuously

B. To respond effectively to security incidents

C. To design new software systems

D. To conduct employee evaluations

The purpose of incident response planning is to respond effectively to security incidents. This planning involves developing a structured process that organizations can follow when a security event occurs, ensuring that incidents are managed promptly and efficiently. A well-crafted incident response plan helps minimize the impact of security breaches, reduce recovery time, and protect valuable assets and data. It outlines the roles and responsibilities of the incident response team, establishes communication protocols during an incident, and provides strategies to contain, eradicate, and recover from security threats. This focused approach is critical because the speed and effectiveness of the response can significantly affect the overall outcome of the incident, including potential damage to the organization's reputation and finances. Other options, while related to aspects of security and organizational management, do not align with the primary purpose of incident response planning, which is not about monitoring, software design, or employee evaluations. Instead, it emphasizes preparedness and effectiveness in dealing with incidents as they arise.

SAMPLE

7. The aim of patch management is to?

A. Identify employee needs

B. Acquire and install software updates for security improvements

C. Enhance physical security measures

D. Reduce the number of software applications

The aim of patch management is fundamentally about acquiring and installing software updates to improve security. This process helps ensure that all software applications are updated to their latest versions, which typically include fixes for vulnerabilities that could be exploited by attackers. By keeping software up to date, organizations can protect their systems from known security flaws, thereby reducing the risk of breaches and ensuring the integrity of their data and systems. Regularly applying patches and updates also helps maintain compliance with industry regulations and standards that require organizations to protect sensitive information. The proactive management of patches is an essential component of a comprehensive cybersecurity strategy, as it addresses vulnerabilities that could otherwise be exploited by malicious actors. The other options, while important in their own contexts, do not directly relate to the primary goal of patch management. Identifying employee needs pertains to human resources and organizational support, enhancing physical security measures focuses on protecting the physical assets of an organization, and reducing the number of software applications does not specifically address the necessity of updating existing applications for security reasons.

8. What does risk acceptance imply in a business context?

A. Eliminating all potential risks faced

B. Allowing certain risks to exist after mitigation strategies

C. Implementing extensive control measures

D. Documenting every possible risk scenario

Risk acceptance in a business context signifies that an organization acknowledges the presence of certain risks and decides to allow them to persist after having implemented suitable mitigation strategies. This approach implies a calculated decision where the potential impact and likelihood of the risks are weighed against the costs and feasibility of further mitigation efforts. Accepting risk does not mean ignoring it; rather, it involves a thorough assessment of risks and a thoughtful decision-making process regarding which risks to manage actively and which can be tolerated. The rationale behind this strategy can vary – it might be due to the costs of additional control measures being higher than the potential impact of the risk, or perhaps the organization believes that existing controls adequately minimize the threat. In contrast, eliminating all potential risks is often impractical or unrealistic, as risk is inherent to any business operation. Implementing extensive control measures can lead to over-engineering, where the costs outweigh the benefits. Documenting every possible risk scenario can also become unmanageable and detracts from focusing on those risks that are most critical to the organization's objectives and operational integrity. Thus, risk acceptance is a strategic approach that recognizes the balance between risk and reward in the context of business operations.

SAMPLE

9. Which statement best describes the operational model of "malware as a service"?

A. It focuses on creating security features for users

B. It provides tools and malware for criminal activities

C. It offers free trials of malware detection software

D. It licenses users to develop their own malware

The statement that describes the operational model of "malware as a service" best indicates that it provides tools and malware for criminal activities. This model enables criminals to access a variety of malicious software and tools without needing to have advanced technical skills or knowledge. Essentially, it operates similarly to legitimate software-as-a-service models, allowing users to rent or purchase malware components that can be utilized for various cybercriminal activities, such as launching attacks, stealing data, or deploying ransomware. In this context, the availability of malware as a service democratizes cybercrime, making it easier for individuals to engage in illicit activities by lowering the barrier to entry. This model often includes not only the malware itself but also support services, guides, and infrastructure needed for successful exploitation. The other options do not accurately reflect the operational model related to malware as a service. For instance, focusing on creating security features for users pertains more to cybersecurity solutions rather than malware distribution. Offering free trials of malware detection software is related to defensive measures and does not fit the description of a service aimed at facilitating criminal activity. Licensing users to develop their own malware could imply a creative or legitimate aspect of software development, which contradicts the intent behind malware as a service, where ready-to-use products are offered instead

10. What does the acronym SIEM stand for?

A. System Information and Event Management

B. Security Information and Event Management

C. Security Intelligence and Event Management

D. Security Information and Encryption Management

The acronym SIEM stands for Security Information and Event Management. This term describes a comprehensive solution that combines security information management (SIM) and security event management (SEM) into one product. SIEM systems collect and analyze security event data from across an organization's IT infrastructure, providing real-time analysis of security alerts generated by applications, network hardware, and other security technologies. This allows organizations to detect and respond to security threats more effectively, maintaining a robust security posture. Understanding SIEM is crucial for organizations aiming to improve their security operations, as it helps in identifying potential incidents by correlating data from diverse sources. This capability enhances an organization's ability to proactively mitigate threats and respond to incidents efficiently.

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://sanssecurityfoundation.examzify.com

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

SAMPLE