CERTIPORT NETWORK SECURITY PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://certiportnetsecurity.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. **What term describes the method of analyzing and classifying information based on its sensitivity?**

   A. Infiltration

   B. Information classification

   C. Data destruction

   D. Encryption

2. **Which Windows registry hive contains current settings for the current user?**

   A. HKEY_CLASSES_ROOT

   B. HKEY_CURRENT_USER

   C. HKEY_LOCAL_MACHINE

   D. HKEY_CURRENT_CONFIGURATION

3. **What type of malware is characterized by encrypting files and demanding ransom for decryption?**

   A. Spyware

   B. Worm

   C. Ransomware

   D. Adware

4. **Which tunneling protocol is used to carry packets from unroutable IP addresses across a routable IP network?**

   A. GRE (Generic Routing Encapsulation)

   B. L2TP (Layer 2 Tunneling Protocol)

   C. PPTP (Point-to-Point Tunneling Protocol)

   D. IPsec

5. **What are the three types of attack surfaces?**

   A. Application, Employee, and Network

   B. Hardware, Software, and User

   C. Network, Physical, and Application

   D. User, Network, and Environmental

SAMPLE

6. What does the minimum password age policy enforce in an organization?

A. Forces passwords to be no longer than eight characters

B. Prevents immediate password change after a successful change

C. Requires users to use a password manager

D. Increases password complexity requirements

7. Which Windows registry hive stores settings for the computer as a whole?

A. HKEY_CLASSES_ROOT

B. HKEY_CURRENT_USER

C. HKEY_LOCAL_MACHINE

D. HKEY_CURRENT_CONFIGURATION

8. What first step should you take to share a folder titled "Facebook Photos" while implementing the principle of least privilege?

A. Share the folder with modification permission

B. Share the folder with the read-share permission

C. Grant full control of the folder

D. Set the folder to public access

9. Which of the following would be categorized as a best practice for securing digital certificates?

A. Storing them on a public server

B. Regularly updating and renewing certificates

C. Sharing them widely for compatibility

D. Disabling certificate expiration notifications

10. What is one primary benefit of using a firewall?

A. Increases internet speed

B. Blocks all internet traffic

C. Monitors and controls incoming and outgoing network traffic

D. Replaces antivirus software

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What term describes the method of analyzing and classifying information based on its sensitivity?

A. Infiltration

B. Information classification

C. Data destruction

D. Encryption

The method of analyzing and classifying information based on its sensitivity is known as information classification. This process involves categorizing data to determine how it should be handled and protected. For example, sensitive data might be classified as confidential, while less sensitive information might be labeled as public. Proper information classification is essential in network security as it enables organizations to implement appropriate security measures based on the sensitivity of the data. It helps in compliance with regulations, ensures that sensitive information is only accessible to authorized individuals, and guides the handling and management of data throughout its lifecycle. This practice not only aids in protecting sensitive information but also enhances overall risk management and response strategies in an organization.

2. Which Windows registry hive contains current settings for the current user?

A. HKEY_CLASSES_ROOT

B. HKEY_CURRENT_USER

C. HKEY_LOCAL_MACHINE

D. HKEY_CURRENT_CONFIGURATION

The answer is based on the role of the HKEY_CURRENT_USER registry hive in the Windows operating system. This hive is specifically designed to store configuration settings and preferences that pertain to the currently logged-in user. HKEY_CURRENT_USER contains information such as user profile settings, desktop settings, and application preferences. By accessing this hive, Windows and other applications can retrieve the specific customization and preferences applicable to the user who is currently signed in, making it vital for personalizing the user experience. In contrast, other hives serve different purposes. HKEY_CLASSES_ROOT is primarily used to manage file associations and OLE objects. HKEY_LOCAL_MACHINE contains settings and configurations that apply to the entire computer, regardless of which user is logged in. HKEY_CURRENT_CONFIGURATION, on the other hand, is utilized for storing information related to the current hardware configuration of the system at the time of booting, which is less relevant to individual user settings.

3. What type of malware is characterized by encrypting files and demanding ransom for decryption?

A. Spyware

B. Worm

C. Ransomware

D. Adware

Ransomware is a type of malware specifically designed to encrypt files on a victim's system, making them inaccessible. The attackers then demand a ransom payment from the victim in exchange for the decryption key needed to restore access to those files. This form of cyberattack has become increasingly prevalent, targeting individuals, companies, and institutions alike. In contrast to other types of malware, such as spyware, which is focused on stealthily gathering information without the user's knowledge, or worms, which propagate across networks without requiring user intervention, ransomware's primary goal is financial gain through extortion. Adware, on the other hand, primarily focuses on displaying unwanted advertisements, often leading to a diminished user experience rather than outright file encryption. Thus, the defining characteristic of ransomware is its ability to lock users out of their own data and leverage that situation for financial profit.

SAMPLE

4. Which tunneling protocol is used to carry packets from unroutable IP addresses across a routable IP network?

A. GRE (Generic Routing Encapsulation)

B. L2TP (Layer 2 Tunneling Protocol)

C. PPTP (Point-to-Point Tunneling Protocol)

D. IPsec

The correct answer is based on the function and design of GRE (Generic Routing Encapsulation). GRE is a tunneling protocol that encapsulates a wide variety of network layer protocols, allowing data transmission of packets across an IP network. This capability is particularly beneficial for treating unroutable IP addresses, which typically cannot traverse the conventional internet routing structure. By encapsulating these packets, GRE enables communication between networks that may be separated by non-compatible IP networks. GRE is versatile because it can encapsulate multiple protocols, making it suitable for connecting disparate network architectures. The use of GRE is often seen in virtual private networks (VPNs) and in situations where point-to-point connections are required over a shared infrastructure, allowing for substantial flexibility in network design and implementation. When considering other protocols listed, while L2TP and PPTP are also tunneling protocols, they primarily focus on the establishment of VPNs and the encapsulation of Layer 2 packets, rather than handling unroutable IP addresses specifically. IPsec, on the other hand, is a security protocol suite that provides confidentiality, authentication, and integrity for IP packets but does not serve the primary role of encapsulating unroutable addresses. In summary, GRE is the optimal choice for this specific requirement of carrying

5. What are the three types of attack surfaces?

A. Application, Employee, and Network

B. Hardware, Software, and User

C. Network, Physical, and Application

D. User, Network, and Environmental

The correct answer includes the three types of attack surfaces: Application, Employee, and Network. Each of these elements represents a different domain where a security vulnerability can be exploited. The Application attack surface focuses on vulnerabilities within software applications. This includes issues such as coding errors, misconfigurations, or unsecured APIs, which attackers can exploit to gain unauthorized access or perform malicious activities. The Employee attack surface pertains to human factors in security. Employees can inadvertently create security holes through actions such as falling for phishing scams or mishandling sensitive data. This aspect emphasizes the need for training and awareness to mitigate risks associated with human behavior. The Network attack surface involves vulnerabilities found within the network infrastructure itself. This can include unsecured networks, weak firewall configurations, and exposed services that could be targeted by attackers to gain unauthorized access to systems and data. Overall, these three areas are critical to understanding and managing security risks, as each presents unique challenges in safeguarding an organization's digital assets. The other options focus a bit on different categorizations, but they do not encapsulate the comprehensive range of attack surfaces as effectively as this answer.

SAMPLE

6. What does the minimum password age policy enforce in an organization?

A. Forces passwords to be no longer than eight characters

B. Prevents immediate password change after a successful change

C. Requires users to use a password manager

D. Increases password complexity requirements

The minimum password age policy primarily enforces a restriction on how frequently users can change their passwords. Specifically, it prevents users from immediately changing their password after a successful change. This policy is designed to enhance security by reducing the likelihood of users altering their passwords back to a previous one shortly after changing them, which can undermine the purpose of requiring stronger or new passwords. By implementing a minimum password age, organizations encourage users to maintain their passwords for a specific duration before they can opt for a change, thus promoting better password hygiene and adherence to security protocols. This mitigates the risks associated with quickly cycling through passwords, providing a stronger defense against potential threats that exploit weak password management practices.

7. Which Windows registry hive stores settings for the computer as a whole?

A. HKEY_CLASSES_ROOT

B. HKEY_CURRENT_USER

C. HKEY_LOCAL_MACHINE

D. HKEY_CURRENT_CONFIGURATION

The Windows registry hive that stores settings for the computer as a whole is HKEY_LOCAL_MACHINE. This hive contains configuration information for the hardware, operating system, and software settings that are applicable to the entire computer, rather than to individual user profiles. The HKEY_LOCAL_MACHINE hive is key for system-wide settings and is essential for the operating system's performance and security. It includes data like system drivers, hardware settings, and many application configurations that need to be consistent across all users on the machine. In contrast, other hives like HKEY_CURRENT_USER hold settings that are specific to the current logged-in user, ensuring personalized experiences and preferences. HKEY_CLASSES_ROOT is primarily used for file association settings and COM information, while HKEY_CURRENT_CONFIGURATION deals with information relevant to the current hardware profile in use, typically only reflecting changes during system boot rather than comprehensive system-wide settings.

8. What first step should you take to share a folder titled "Facebook Photos" while implementing the principle of least privilege?

A. Share the folder with modification permission

B. Share the folder with the read-share permission

C. Grant full control of the folder

D. Set the folder to public access

Sharing the folder titled "Facebook Photos" with read-share permission aligns perfectly with the principle of least privilege. This principle states that users should have the minimum levels of access – or permissions – they need to perform their job functions. By providing read-share permission, you ensure that users can view and access the photos without being able to modify, delete, or alter any of the contents within the folder. This reduces the risk of accidental changes or malicious actions by limiting the interaction that users have with the folder's contents. Using modification permission would not adhere to the principle of least privilege, as it allows users the capability to change the folder's contents, which is unnecessary for merely viewing photos. Granting full control would exceed what is needed and poses a greater risk, as it lets users alter folder settings and delete files. Setting the folder to public access opens it to anyone, which circumvents the principle of least privilege altogether by greatly expanding access beyond intended recipients.

SAMPLE

9. Which of the following would be categorized as a best practice for securing digital certificates?

A. Storing them on a public server

B. Regularly updating and renewing certificates

C. Sharing them widely for compatibility

D. Disabling certificate expiration notifications

Regularly updating and renewing certificates is a vital best practice for securing digital certificates. Digital certificates have a defined validity period, after which they expire. If a certificate is allowed to expire, it can lead to disruptions in service, expose systems to risks, and hinder secure communication. By routinely updating and renewing certificates, organizations maintain a secure environment and ensure that the cryptographic keys remain valid and trustworthy. Furthermore, consistent renewal helps keep pace with evolving security standards and encryption methods. Keeping certificates updated minimizes vulnerabilities that could be exploited by malicious actors, ensuring that only the latest, most secure versions of certificates are in operation. Adopting this practice allows an organization to uphold its reputation for security and trustworthiness when facilitating secure transactions and communications.

10. What is one primary benefit of using a firewall?

A. Increases internet speed

B. Blocks all internet traffic

C. Monitors and controls incoming and outgoing network traffic

D. Replaces antivirus software

A primary benefit of using a firewall is that it monitors and controls incoming and outgoing network traffic. Firewalls act as a barrier between a trusted internal network and untrusted external networks, such as the internet. They analyze packets of data based on predefined security rules, allowing administrators to define what traffic should be permitted and what should be blocked. This capability is essential for preventing unauthorized access to sensitive information and protecting against various cyber threats, such as malware and hacking attempts. By effectively managing network traffic, firewalls help maintain the integrity and security of the network environment, which is crucial for organizations relying on digital communications and data exchange. Increasing internet speed is not a function of firewalls, as their primary role involves traffic management and security rather than performance enhancement. While firewalls can prevent unwanted traffic that may degrade performance, they do not directly increase the speed of internet access. Similarly, firewalls do not block all internet traffic; rather, they selectively allow or deny traffic based on the established rules. Lastly, while firewalls contribute to overall network security, they do not replace antivirus software, which serves a different purpose in detecting and neutralizing malware on devices. Firewalls and antivirus programs work together to create a comprehensive security strategy.

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://certiportnetsecurity.examzify.com

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

SAMPLE