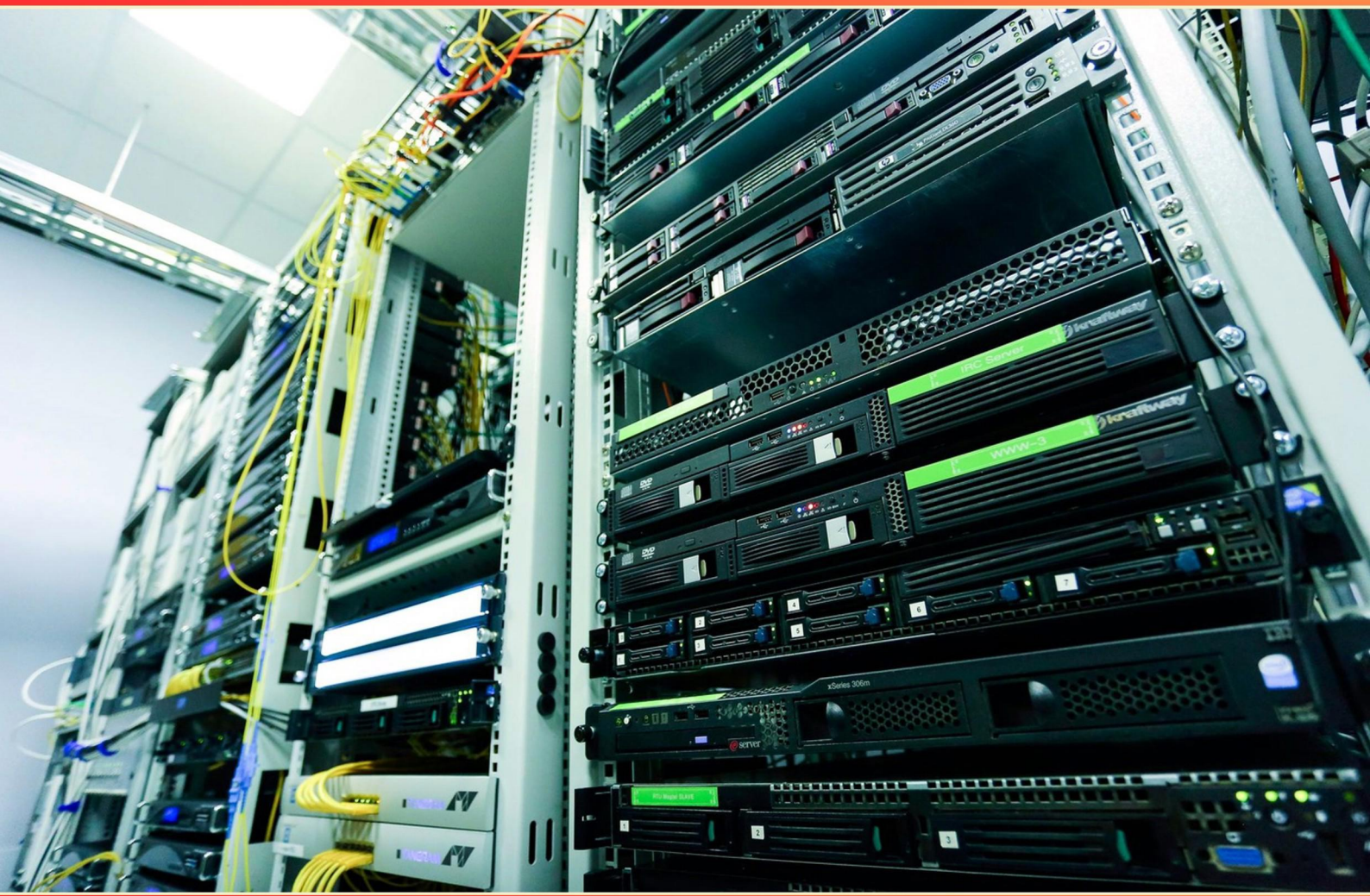
PRCC NETWORK SECURITY PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://prccnetsecurity.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 is the primary goal of Digital Rights Management (DRM)?

A. Data Integrity

B. Data Sharing

C. Content Protection

D. Performance Monitoring

2. What type of information was compromised in the recent data breach at the online retailer?

A. Financial Data

B. Employee Records

C. Personally Identifiable Information

D. Intellectual Property

3. What is the main purpose of implementing a write blocker during forensic analysis?

A. To enhance the speed of data recovery

B. To prevent alterations of data

C. To encrypt sensitive information

D. To backup data automatically

4. What access control model should a rapidly growing company implement to manage permissions more effectively?

A. MAC

B. RBAC

C. DAC

D. ABAC

5. What is indicated by a user being able to upload third-party apps not found in the App Store?

A. Rooting

B. Jailbreaking

C. Phishing

D. Malware infection

SAMPLE

6. Which security technology is specifically designed to monitor and block unauthorized access to a network?

A. Network Behavior Analysis

B. Intrusion Detection System

C. Firewall

D. Virtual Private Network

7. What is a key setting to consider in a cloud service provider regarding patient data retention?

A. Accessibility

B. Data retention

C. Data transfer speed

D. Data encryption status

8. What method should Annya use for the secure disposal of a failed hard drive?

A. Overwrite data

B. Secure disposal

C. Recycling

D. Data shredding

9. What type of networking device is Suki likely using to analyze traffic among several computers?

A. Router

B. Hub

C. Switch

D. Bridge

10. What type of script format would be helpful for Simone to know in order to create a plug-in for vulnerability scanners?

A. JSON

B. XML

C. NASL

D. HTML

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the primary goal of Digital Rights Management (DRM)?

A. Data Integrity

B. Data Sharing

C. Content Protection

D. Performance Monitoring

The primary goal of Digital Rights Management (DRM) is content protection. This technology encompasses a variety of tools and techniques designed to safeguard digital content from unauthorized use and distribution. DRM systems primarily focus on preventing the illegal copying and redistributing of digital media such as music, movies, eBooks, and software. By implementing DRM, content creators and publishers seek to retain control over their intellectual property, ensuring that users can only access, use, or modify the content according to the terms set by the rights holders. This includes restricting copying, preventing sharing, and controlling how and where the content can be accessed or viewed. While data integrity, data sharing, and performance monitoring are important aspects of data management and security, they do not align with the specific aims of DRM. Data integrity focuses more on ensuring that data remains accurate and unaltered, data sharing deals with the permissions surrounding how data can be distributed or accessed, and performance monitoring refers to tracking system performance and usage. These concepts are relevant in broader contexts but do not specifically capture the protective nature of DRM regarding digital content.

2. What type of information was compromised in the recent data breach at the online retailer?

A. Financial Data

B. Employee Records

C. Personally Identifiable Information

D. Intellectual Property

The compromised information in the recent data breach at the online retailer primarily consisted of Personally Identifiable Information (PII). PII includes data that can be used to uniquely identify an individual, such as names, addresses, phone numbers, email addresses, and sometimes Social Security numbers. The exposure of such information can lead to identity theft and other forms of fraud, making it a significant concern for both consumers and organizations. In the context of the breach, focusing on PII underscores the importance of protecting this type of sensitive data, as it directly impacts individuals' privacy and security. Retailers have vast amounts of customer data, and when that data is not adequately protected, it can lead to widespread consequences, including loss of consumer trust, financial loss, and potential legal ramifications. It is important for organizations to implement robust security measures to safeguard against unauthorized access to PII and to ensure compliance with regulations surrounding data protection.

SAMPLE

3. What is the main purpose of implementing a write blocker during forensic analysis?

A. To enhance the speed of data recovery

B. To prevent alterations of data

C. To encrypt sensitive information

D. To backup data automatically

Implementing a write blocker during forensic analysis serves the crucial purpose of preventing any alterations of data. In the context of forensic investigations, maintaining the integrity of data is paramount. A write blocker is a device or software that allows access to data on a storage medium without the ability to modify or write to that medium. This ensures that the original evidence remains unchanged, preserving its authenticity for analysis and possible court proceedings. When forensic experts handle digital evidence, any writes to the evidence can inadvertently alter key information, such as timestamps or file structures, which could compromise the validity of the investigation. By using a write blocker, analysts can confidently work with the data while ensuring that what they are examining is exactly what was found, thereby adhering to legal and ethical standards. Other choices, while relevant to data management and security, do not address the critical issue of data integrity in forensic analysis. Enhancing speed, encrypting sensitive information, or automatically backing up data do not provide the same level of protection against data alteration, which is the primary concern in a forensic context.

4. What access control model should a rapidly growing company implement to manage permissions more effectively?

A. MAC

B. RBAC

C. DAC

D. ABAC

A rapidly growing company often faces challenges in managing access permissions as it scales. The Role-Based Access Control (RBAC) model is particularly well-suited for such environments because it simplifies the management of user permissions based on their role within the organization. In RBAC, permissions are assigned to specific roles rather than to individual users. This means that when a new employee joins the organization, they can quickly be assigned to a role that has pre-defined permissions associated with it. As the company evolves, roles can be adjusted or created to reflect changes in responsibilities, making it easy to adapt to organizational growth without having to reconfigure permissions for each individual user. This model enhances security and compliance because it ensures that users only have access to the information necessary for their job functions, thereby reducing the risk of unauthorized access. It streamlines the onboarding process for new employees and minimizes administrative overhead related to managing permissions, which is crucial for a rapidly expanding workforce. By using RBAC, organizations benefit from a structured approach that improves oversight and auditing capabilities over access controls, which are essential in maintaining a secure and efficiently managed environment as the company continues to grow.

SAMPLE

5. What is indicated by a user being able to upload third-party apps not found in the App Store?

A. Rooting

B. Jailbreaking

C. Phishing

D. Malware infection

The ability for a user to upload third-party apps not found in the App Store is indicative of jailbreaking. Jailbreaking is a process that allows users to gain root access to the operating system of their device, primarily on iOS devices. This process modifies the device's restrictions, enabling the installation of applications from sources outside the official App Store, which Apple typically restricts for security reasons. When a device is jailbroken, users can customize their devices further than what is possible with the default settings and can install apps not vetted by Apple, which may not be available in the official repository. While jailbreaking provides greater freedom to the user, it also exposes the device to potential security risks since the installed third-party applications may not always be secure or reliable. Other concepts like rooting may refer to Android devices rather than iOS, and phishing or malware infection relate to different forms of security threats that do not inherently involve the ability to install third-party applications. This distinction highlights why jailbreaking is the most relevant answer concerning the ability to upload and use third-party apps.

6. Which security technology is specifically designed to monitor and block unauthorized access to a network?

A. Network Behavior Analysis

B. Intrusion Detection System

C. Firewall

D. Virtual Private Network

The security technology that is specifically designed to monitor and block unauthorized access to a network is the firewall. A firewall acts as a barrier between a trusted internal network and untrusted external networks, such as the internet. It controls incoming and outgoing traffic based on predetermined security rules, thus preventing unauthorized access while allowing legitimate traffic to pass through. Firewalls can be hardware-based, software-based, or a combination of both. They inspect data packets and determine whether they should be allowed through or blocked, effectively protecting the network from external threats such as intrusions or attacks. In contrast, other choices do not serve the same primary function. For example, an Intrusion Detection System (IDS) monitors network traffic for suspicious activities or policy violations but does not actively block traffic. Instead, it alerts administrators to potential security breaches. A Virtual Private Network (VPN) is designed to create secure connections over the internet, providing privacy and protection for data in transit, but it does not specifically monitor or block unauthorized access to the network itself. Network Behavior Analysis is a technology focused on monitoring and analyzing network traffic patterns to detect anomalies that could indicate a threat or potential breach, but like the IDS, it does not block access. Therefore, the firewall is the most suitable answer

SAMPLE

7. What is a key setting to consider in a cloud service provider regarding patient data retention?

A. Accessibility

B. Data retention

C. Data transfer speed

D. Data encryption status

When considering a cloud service provider for storing patient data, data retention is a pivotal setting to address. Healthcare organizations are governed by strict regulations, such as HIPAA in the United States, which dictate how long patient data must be retained. This can include not only the duration of retention but also the specific protocols for data archival, deletion, and retrieval. By focusing on data retention, organizations can ensure compliance with legal requirements, ethical standards, and internal policies governing patient records. Effective data retention policies help safeguard against unintentional data loss and ensure that historical patient information is accessible when necessary, such as for audits or ongoing patient care. In contrast, while accessibility is important for operational efficiency and data transfer speed can impact the usability of the cloud service, these factors do not address the legal and compliance obligations associated with patient data. Data encryption is crucial for protecting data in transit and at rest but does not directly relate to how long the data is kept or how it is managed over time, which is the core concern addressed by data retention policies.

8. What method should Annya use for the secure disposal of a failed hard drive?

A. Overwrite data

B. Secure disposal

C. Recycling

D. Data shredding

Using secure disposal for a failed hard drive involves physically destroying or rendering the drive unusable so that data cannot be recovered. Secure disposal methods include techniques such as shredding, crushing, or incinerating the hard drive, which effectively eliminates the risk of data breaches resulting from the recovery of data from the drive. While overwriting data, data shredding, and recycling are all methods associated with managing data, they do not provide the level of security necessary for a failed hard drive. Overwriting may not be effective if the drive is malfunctioning or if data remnants are still recoverable. Data shredding, while secure, is a specific technique that falls under the broader category of secure disposal. Recycling, on the other hand, does not guarantee that the data will be securely destroyed, and it may inadvertently allow access to sensitive information. Therefore, emphasizing secure disposal as the preferred method highlights its effectiveness in ensuring that all data on the failed hard drive is irretrievable and thus protects against potential security risks.

SAMPLE

9. What type of networking device is Suki likely using to analyze traffic among several computers?

A. Router

B. Hub

C. Switch

D. Bridge

The correct answer is a switch, which is designed to analyze and manage network traffic between multiple computers on a local area network (LAN). A switch operates at the data link layer of the OSI model, intelligently directing data packets specifically to the devices that need them rather than broadcasting packets to all connected devices. This ability allows for more efficient use of network bandwidth and helps minimize collisions, making it easier to analyze traffic patterns, monitor network performance, and troubleshoot issues more effectively. Switches maintain a MAC address table, which helps them learn which devices are connected to which ports, enhancing the speed and accuracy of traffic management. In a scenario where Suki is analyzing traffic among several computers, the switch's capacity to handle multiple simultaneous data streams while keeping traffic contained and organized is essential. While routers, hubs, and bridges are also network devices, they serve different functions that are less suited for in-depth traffic analysis among several computers. A router connects different networks and directs data between them, whereas a hub simply broadcasts data to all connected devices without filtering or directing it. A bridge, on the other hand, connects two segments of a network and operates similarly to a switch but is generally less efficient in managing traffic. Therefore, a switch is the ideal device for the

10. What type of script format would be helpful for Simone to know in order to create a plug-in for vulnerability scanners?

A. JSON

B. XML

C. NASL

D. HTML

C is the correct choice because NASL, or Nessus Attack Scripting Language, is specifically designed for writing scripts or plug-ins that work with vulnerability scanning tools like Nessus. It provides a standardized way to check for vulnerabilities, automate scans, and report findings, making it essential knowledge for anyone looking to develop or contribute to such tools. Understanding NASL allows developers to create custom scripts that can accurately perform vulnerability checks and to integrate new checks into existing scanning frameworks. This scripting language is tailored to the operational needs of security assessments, making it the most relevant format for someone interested in vulnerability scanning. Other formats such as JSON, XML, and HTML serve different purposes—JSON is primarily used for data interchange, XML is used for storing and transporting data, and HTML is oriented towards web page structure and content presentation. Therefore, while these formats have their own significance in various contexts, they do not specifically cater to the needs of creating vulnerability scanner plug-ins in the same way that NASL does.

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://prccnetsecurity.examzify.com

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

SAMPLE