PRCC Network Security Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

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.

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!

Questions

1. **What set of software tools ensures company security policies extend to data stored in the cloud?**

   A. Virtual Private Network

   B. Cloud Access Security Broker

   C. Intrusion Detection System

   D. Firewalls

2. **Which tool would Marco use to discover other resources within an organization's network after exploiting a perimeter firewall vulnerability?**

   A. Nslookup

   B. Netcat

   C. Wireshark

   D. Nmap

3. **Masa is targeted by someone impersonating IT personnel. What type of attack is he experiencing?**

   A. Phishing

   B. Impersonation

   C. Spear Phishing

   D. Social Engineering

4. **What type of access control is indicated by the error message that specifies different access levels for a user trying to access a resource?**

   A. MAC

   B. DAC

   C. RBAC

   D. ABAC

5. **What is a recommended method to prevent brute force attacks during a login process?**

   A. Implement CAPTCHA during login attempts

   B. Analyze the frequency of attempted logins

   C. Increase the password complexity requirements

   D. Limit user access to single login at a time

6. Which tool might a threat actor use to examine the source code of a program they detected during a scan?

A. Debugger

B. Decompiler

C. Disassembler

D. Sniffer

7. Which network device creates virtual connections and segments traffic within different departments of an organization?

A. Router

B. Switch

C. Access Point

D. Firewall

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

A. MAC

B. RBAC

C. DAC

D. ABAC

9. What type of attack involves intercepting communications between two parties?

A. Denial of service

B. MITM attack

C. Brute force attack

D. SQL injection

10. The service model that provides complete management of hardware and networking while allowing users to focus on applications is known as?

A. IaaS

B. PaaS

C. SaaS

D. FaaS

Answers

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

Explanations

1. What set of software tools ensures company security policies extend to data stored in the cloud?

A. Virtual Private Network

B. Cloud Access Security Broker

C. Intrusion Detection System

D. Firewalls

The Cloud Access Security Broker (CASB) is the correct choice because it acts as an intermediary between an organization's on-premises infrastructure and cloud services. Its primary role is to enforce security policies that the organization has established, ensuring that data access and storage in the cloud align with those policies. CASBs provide visibility into cloud application usage and data security. They help mitigate risks associated with data exposure, unauthorized access, and data leakage. By utilizing a CASB, organizations can implement consistent security measures across various cloud services, ensuring compliance with regulations and protecting sensitive information stored in the cloud even when it is outside of traditional physical boundaries. While a Virtual Private Network (VPN) creates a secure connection between a user and a network, it does not specifically manage cloud application security policies. An Intrusion Detection System (IDS) monitors network traffic for suspicious activity, but it does not directly enforce data policies within cloud environments. Firewalls are critical for protecting networks from unauthorized access and threats but are primarily used to control traffic rather than to enforce security policies related to cloud applications. Thus, the CASB stands out as the tool specifically designed to extend and manage company security policies for data stored in the cloud.

2. Which tool would Marco use to discover other resources within an organization's network after exploiting a perimeter firewall vulnerability?

A. Nslookup

B. Netcat

C. Wireshark

D. Nmap

The most appropriate tool for discovering other resources within an organization's network after exploiting a perimeter firewall vulnerability is Nmap. This tool specializes in network scanning and enumeration, allowing a user to discover hosts and services on a computer network. It can provide information such as open ports, running services, and operating system details, which is invaluable for understanding the network's layout and any additional vulnerabilities that may be present. Nslookup is primarily used for querying DNS to obtain domain name or IP address mapping information. While useful for gathering some information about network resources, it does not facilitate the broader scanning and enumeration of hosts that Nmap does. Netcat is a versatile networking utility that can read and write data across network connections. It can be used for banner grabbing or as a backdoor, but it is not designed specifically for network discovery and does not provide comprehensive scanning capabilities. Wireshark is a packet analysis tool that captures network traffic. While it can be instrumental in inspecting data as it travels over the network, it does not perform the active scanning and mapping functions needed to uncover a wide range of resources on a network effectively. Thus, Nmap is the most suitable choice for the task at hand since it offers robust scanning capabilities to identify resources on a network after gaining

3. Masa is targeted by someone impersonating IT personnel. What type of attack is he experiencing?

A. Phishing

B. Impersonation

C. Spear Phishing

D. Social Engineering

Masa is experiencing an impersonation attack, where the attacker pretends to be someone he trusts—specifically, IT personnel. This type of attack relies on deception to gain the target's trust and then extract sensitive information or gain unauthorized access to systems. Impersonation attacks can take place through various channels, including email, phone calls, or in person, and they often exploit the victim's belief in the authority of the impersonator. In this context, the impersonator is leveraging the trust associated with IT personnel to deceive Masa into providing information or taking actions that compromise security. While options such as phishing, spear phishing, and social engineering all involve deceptive tactics, they represent different nuances of attack strategies. Phishing generally involves deceptive emails that try to trick users into revealing personal information, while spear phishing is a more targeted variation of phishing aimed at specific individuals. Social engineering is a broader term that encompasses various tactics, including impersonation, but does not specifically highlight the act of pretending to be someone else. Thus, the directness of "impersonation" as it relates to the scenario is what makes this answer the most appropriate.

4. What type of access control is indicated by the error message that specifies different access levels for a user trying to access a resource?

A. MAC

B. DAC

C. RBAC

D. ABAC

The correct answer is that the described scenario is indicative of Role-Based Access Control (RBAC). In situations where different access levels are specified for users accessing a resource, it suggests that permissions are assigned based on the roles assigned to various users within the system. In RBAC, permissions are not assigned to individual users; rather, they are associated with roles, allowing users to take on different roles and associate with varying levels of access based on their job functions or responsibilities. As a result, the access control mechanism ensures that users can only perform actions that are appropriate for their designated role, creating a more manageable and organized security framework. This contrasts with Mandatory Access Control (MAC), which typically relies on system-enforced access levels that cannot be easily altered, and Discretionary Access Control (DAC), where the owner of the resource has the flexibility to determine access rights. Attribute-Based Access Control (ABAC) employs policies based on attributes and conditions, adding complexity by evaluating various properties of users, resources, and environmental factors to enforce access decisions. The situation described, focusing on static access levels tied to user roles, is best aligned with RBAC principles, which streamline access control management while enhancing security and compliance within systems.

5. What is a recommended method to prevent brute force attacks during a login process?

A. Implement CAPTCHA during login attempts

B. Analyze the frequency of attempted logins

C. Increase the password complexity requirements

D. Limit user access to single login at a time

A recommended method to prevent brute force attacks during a login process is to implement CAPTCHA during login attempts. CAPTCHA works by adding an additional challenge that requires human interaction, such as identifying distorted letters or selecting images that meet certain criteria. This mechanism significantly boosts security by thwarting automated scripts that are typically employed in brute force attacks since bots cannot easily solve these challenges. The other methods, while they may contribute to overall security, do not directly prevent brute force attacks as effectively. For instance, analyzing the frequency of attempted logins could help identify and alert administrators to suspicious activity, but it doesn't actively stop the automated attempts. Increasing password complexity requirements makes it more difficult for attackers to guess passwords, but it does not by itself deter a determined brute force attack that can still try a wide variety of combinations. Limiting user access to a single login at a time may help mitigate some risks but could also be inconvenient to legitimate users, potentially leading to a poor user experience. By incorporating CAPTCHA into the login process, organizations can significantly reduce the risk of automated login attempts from brute force attacks, enhancing the overall security of their authentication mechanisms.

6. Which tool might a threat actor use to examine the source code of a program they detected during a scan?

A. Debugger

B. Decompiler

C. Disassembler

D. Sniffer

The decompiler is a tool that converts executable programs back into a higher-level programming language code, allowing a threat actor to examine the source code or the logic of the program. This process is crucial for understanding how the program operates, identifying vulnerabilities, analyzing functionality, and possibly manipulating the program for malicious purposes. By using a decompiler, a threat actor gains insights into the original structure and data flow of the software, which can help identify exploits or weaknesses that could be exploited. The ease of understanding the program's logic, control structures, and algorithms is what makes decompilation particularly valuable in a security context. Other tools mentioned, such as debuggers and disassemblers, serve different functions. A debugger is used for examining and testing code execution line-by-line, with the primary goal of identifying and fixing errors rather than fully retrieving high-level source code. A disassembler translates binary code into assembly language, which is low-level and may be difficult for someone looking to understand the program's original source code. A sniffer is a network monitoring tool, used to capture and analyze data packets traveling over a network, and does not pertain to analyzing the code of a single program.

7. Which network device creates virtual connections and segments traffic within different departments of an organization?

A. Router

B. Switch

C. Access Point

D. Firewall

The correct choice, a switch, is fundamental in network architecture as it enables the segmentation of network traffic effectively. Switches operate at the data link layer (Layer 2) and utilize MAC addresses to forward data to the correct destination within a local area network (LAN). By creating virtual connections, switches facilitate communication between devices while efficiently managing data traffic. This segmentation is particularly valuable in organizational settings where different departments might need to communicate without impacting each other's bandwidth or data flows. For instance, a switch can create VLANs (Virtual Local Area Networks), which allow distinct groups within the same physical network to operate separately, enhancing security and reducing collisions. In contrast, routers connect different networks, typically operating at the network layer and helping direct packets between different subnets or to the internet. Access points serve to extend a wired network by adding wireless capabilities, allowing devices to connect over Wi-Fi, but do not create segments within the traffic. Firewalls work primarily as security devices that filter traffic based on predetermined security rules and do not manage the segmentation of traffic within a specific local network. Thus, the functionality of a switch to create virtual connections and segment traffic distinctly positions it as the accurate answer.

8. 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.

9. What type of attack involves intercepting communications between two parties?

A. Denial of service

B. MITM attack

C. Brute force attack

D. SQL injection

The attack type that involves intercepting communications between two parties is a man-in-the-middle (MITM) attack. In a MITM attack, the attacker secretly relays and possibly alters the communication between the parties who believe they are directly communicating with each other. This type of attack can allow the attacker to eavesdrop on the conversation, steal data, or inject malicious content into the communication stream. MITM attacks can occur in various forms, such as session hijacking, where an attacker takes control of a user's session after they have authenticated themselves, or through techniques like packet sniffing, where data packets being transmitted over a network are intercepted. The critical aspect of a MITM attack is the deceitful positioning of the attacker within the communication process, making it appear as if two parties are securely communicating with each other when, in fact, the attacker is in control of that communication. In contrast, other attack types like denial of service focus on overwhelming a system to make it unavailable, brute force attacks involve guessing passwords or encryption keys, and SQL injection targets databases to manipulate or retrieve sensitive data. Each of these attacks employs different techniques and goals, distinct from the interception of real-time communications characteristic of MITM attacks.

10. The service model that provides complete management of hardware and networking while allowing users to focus on applications is known as?

A. IaaS

B. PaaS

C. SaaS

D. FaaS

The service model that allows users to concentrate on their applications while the provider manages all underlying hardware and networking aspects is Platform as a Service (PaaS). This model provides a complete development and deployment environment in the cloud, offering tools and services that streamline the process of building, testing, and deploying applications. PaaS allows developers to focus on writing code without worrying about the complexities of infrastructure management, operating systems, and middleware. In PaaS, the provider manages everything from hardware resources to networking, allowing users to benefit from scalable infrastructure and integrated development frameworks. This includes various services such as database management, application hosting, and development tools, which enhances productivity and accelerates the deployment timeframe. Understanding the distinctions between PaaS and other service models is essential. Infrastructure as a Service (IaaS) provides virtualized hardware resources but requires users to manage everything above that layer, including the operating system and middleware. Software as a Service (SaaS) delivers hosted applications, where users interact with software through the internet without control over the underlying infrastructure. Function as a Service (FaaS), typically related to serverless computing, allows developers to run code in response to events but does not provide the full development environment that PaaS does

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!