Certiport 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. **Application-level firewalls are generally more or less resource-intensive than traditional firewalls?**

   A. More resource-intensive

   B. Less resource-intensive

   C. Equally resource-intensive

   D. Not applicable

2. **Which backup method saves all changed files since the last full backup?**

   A. Full backup

   B. Incremental backup

   C. Differential backup

   D. Complete backup

3. **Which of the following is considered a technical control in cybersecurity?**

   A. IDs

   B. Training manual

   C. Policy review

   D. Awareness programs

4. **Which type of DNS record is used to lookup an associated host or domain name by its IP address?**

   A. A Record

   B. MX Record

   C. PTR Record

   D. SOA Record

5. **What is one effective way to protect your computer from hackers and malicious software?**

   A. Using a virtual private network

   B. Installing a web browser extension

   C. Using Windows firewall

   D. Disabling all updates

6. What type of VPN often requires users to connect through a web browser?

A. IPSec VPN

B. Site-to-site VPN

C. SSL VPN

D. Remote access VPN

7. What is a key feature of two-factor authentication?

A. It requires two passwords

B. It combines something you know and something you have

C. It is only applicable to online banking

D. It cannot be bypassed

8. Which of the following best describes the function of a firewall?

A. Encrypts data

B. Blocks unauthorized access

C. Enhances internet speed

D. Restores deleted files

9. What does the term spoofing refer to in the context of security?

A. Fake identity creation

B. Sending large amounts of unrequested emails

C. Intercepting secure messages

D. Accessing unauthorized data

10. What is the name of the segments into which a router can divide a physical network?

A. Subnets

B. VLANs

C. Domains

D. Clusters

Answers

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

Explanations

1. Application-level firewalls are generally more or less resource-intensive than traditional firewalls?

A. More resource-intensive

B. Less resource-intensive

C. Equally resource-intensive

D. Not applicable

Application-level firewalls operate at a higher level in the OSI model compared to traditional firewalls, which primarily filter traffic based on IP addresses and ports. They inspect the actual content of the traffic, analyzing applications-specific protocols and enforcing security policies based on the application behavior. This intricate processing demands more computational resources, including CPU and memory, making application-level firewalls more resource-intensive compared to traditional firewalls. They engage in deep packet inspection and maintain stateful information about sessions, which increases their workloads significantly. In contrast, traditional firewalls often focus on simpler tasks such as allowing or blocking traffic based solely on predefined rules concerning protocols and IP addresses, which typically consume fewer resources. So, when comparing the two, it's evident that application-level firewalls require more resources to perform their advanced tasks effectively.

2. Which backup method saves all changed files since the last full backup?

A. Full backup

B. Incremental backup

C. Differential backup

D. Complete backup

The method that saves all changed files since the last full backup is the differential backup. This approach captures not only new or modified files but also keeps track of all changes made since the last full backup was completed. This means that you only need to have the last full backup and the most recent differential backup to restore the system to its latest state. In contrast, a full backup captures all files every time it is performed, resulting in a larger amount of data being stored but providing a complete snapshot of all the data at a specific point in time. An incremental backup, on the other hand, saves only the changes made since the last backup of any kind (either full or incremental), meaning that to restore to the latest state, one would need the last full backup and all subsequent incremental backups. Finally, the term "complete backup" is often used interchangeably with a full backup, further emphasizing that it captures everything without reference to incremental changes.

3. Which of the following is considered a technical control in cybersecurity?

A. IDs

B. Training manual

C. Policy review

D. Awareness programs

Technical controls in cybersecurity refer to the mechanisms that are implemented through technology to mitigate risks and enhance security. These controls are often automated and can include hardware and software solutions that protect systems and data from threats. In this case, identifiers, such as IDs, fall under the category of technical controls. They are used to authenticate users, grant access to resources, and track user activity within a system. The implementation of identification mechanisms is crucial to enforce security policies and ensure that only authorized users have access to sensitive information or systems. On the other hand, the training manual, policy review, and awareness programs are classified as administrative or physical controls rather than technical ones. While they are important for establishing a secure environment and ensuring that staff understand procedures and policies, they do not involve the technological measures necessary to block or mitigate threats directly. Thus, the emphasis on IDs highlights their role as a direct technological measure to strengthen cybersecurity defenses.

4. Which type of DNS record is used to lookup an associated host or domain name by its IP address?

A. A Record

B. MX Record

C. PTR Record

D. SOA Record

The correct choice is the PTR Record, as it is specifically designed for reverse DNS lookups. This means that it allows for the resolution of an IP address back to its associated domain name or host. When a DNS resolver performs a reverse lookup, it queries the PTR record of the IP address, which then provides the name of the host that corresponds to that IP. This is particularly useful for various applications, including email systems where verifying the domain associated with an IP address can be critical for authenticating the source of the message. In contrast, other record types serve different purposes. An A Record is used for mapping a domain name to an IPv4 address, while an MX Record is utilized for specifying mail exchange servers for a domain, essential in email routing. The SOA Record contains administrative information about the domain, including the primary name server and the domain's serial number, but does not facilitate reverse lookups. Thus, the PTR Record is the only choice that serves the specific function of mapping an IP address back to a host or domain name.

5. What is one effective way to protect your computer from hackers and malicious software?

A. Using a virtual private network

B. Installing a web browser extension

C. Using Windows firewall

D. Disabling all updates

Using a firewall, like the one that comes with Windows, is a critical line of defense against unauthorized access and malicious software. A firewall monitors and controls incoming and outgoing network traffic based on predetermined security rules. By setting up these rules, the firewall can block potentially harmful connections and filter traffic based on various criteria, such as IP addresses and ports. This proactive measure helps in identifying and preventing unwanted access attempts, ultimately protecting sensitive data and the overall integrity of the system. While other choices have their merits, they do not provide the comprehensive protection that a firewall offers. For example, a virtual private network (VPN) can help secure your internet connection, but it primarily focuses on privacy and anonymity rather than actively defending against threats. Similarly, installing a web browser extension might enhance specific features or block ads, but it won't offer robust security against broader threats. Disabling all updates is counterproductive, as updates frequently contain crucial security patches that protect against newly discovered vulnerabilities. Therefore, a firewall is an effective and essential component of a comprehensive cybersecurity strategy.

6. What type of VPN often requires users to connect through a web browser?

A. IPSec VPN

B. Site-to-site VPN

C. SSL VPN

D. Remote access VPN

The choice of an SSL VPN is accurate because it specifically allows users to connect to a secure network via a standard web browser. This technology uses the SSL (Secure Sockets Layer) protocol to encrypt the data transmitted between the client and server, which is particularly useful for remote users who may not have dedicated VPN client software installed. SSL VPNs are designed to provide more flexible access to applications and data without the need for extensive configuration or installation. Users can typically access their network resources by simply navigating to a designated URL in their browser, which simplifies the connection process and often enhances compatibility across different devices and operating systems. In contrast, other types of VPNs, such as IPSec and site-to-site VPNs, generally require specific client software or configuration on the user's device, making them less accessible through a simple web browser interface. While remote access VPNs can also facilitate user connections, they may not specifically rely on web browsers like SSL VPNs do.

7. What is a key feature of two-factor authentication?

A. It requires two passwords

B. It combines something you know and something you have

C. It is only applicable to online banking

D. It cannot be bypassed

The key feature of two-factor authentication is that it combines something you know (like a password or PIN) with something you have (such as a hardware token, a smartphone app, or a text message code). This layered approach to security adds an extra level of protection, making it much more difficult for unauthorized users to gain access to an account, even if they have compromised the password. By requiring both elements, two-factor authentication enhances security and significantly reduces the likelihood of unauthorized access. The other options do not accurately represent the nature of two-factor authentication. Requiring two passwords does not align with the fundamental concept of using different types of verification factors. Additionally, two-factor authentication is not limited to online banking; it is widely used across various applications and services, from social media to corporate networks. Finally, while two-factor authentication greatly improves security, it cannot be completely bypassed; there may still be methods through which it can be circumvented, such as social engineering or phishing attacks.

8. Which of the following best describes the function of a firewall?

A. Encrypts data

B. Blocks unauthorized access

C. Enhances internet speed

D. Restores deleted files

A firewall functions primarily to block unauthorized access to or from a private network. It acts as a barrier between a trusted internal network and untrusted external networks, such as the Internet. By monitoring and controlling incoming and outgoing network traffic based on predetermined security rules, firewalls help to protect against threats such as intrusions, attacks, and unauthorized data access. This protective role is crucial in maintaining the security and integrity of the system it safeguards. The other options describe different functions that are not related to the core purpose of a firewall. For example, encryption is about securing data by converting it into a form that cannot be easily understood by unauthorized users, which is not what a firewall does. Enhancing internet speed is not a function of firewalls; rather, they can occasionally introduce latency due to the processing of network traffic. Finally, restoring deleted files is related to data recovery or backup solutions, and is outside the scope and capability of a firewall's protective function.

9. What does the term spoofing refer to in the context of security?

A. Fake identity creation

B. Sending large amounts of unrequested emails

C. Intercepting secure messages

D. Accessing unauthorized data

Spoofing in the context of security primarily refers to the act of creating a fake identity or impersonating another entity to deceive a victim. This can involve various tactics, such as falsifying email headers to make it appear as if a message is coming from a legitimate source, or masquerading as a trusted website to capture sensitive information like passwords. The essence of spoofing lies in the misleading representation of identity, aimed at tricking individuals or systems to execute actions that they normally would not. The other options focus on different security threats or types of malicious activities. Sending large amounts of unrequested emails describes the practice of spamming, which primarily floods users with unwanted messages but does not necessarily involve impersonation. Intercepting secure messages pertains more to eavesdropping or man-in-the-middle attacks, where communication is being monitored or altered without the knowledge of the participating parties. Accessing unauthorized data relates to data breaches or hacking attempts where individuals gain access to information they should not have, but again, this doesn't inherently involve the deception associated with spoofing. Thus, the focus on fake identity creation distinctly captures the essence of spoofing, making it the correct choice in understanding this specific security concept.

10. What is the name of the segments into which a router can divide a physical network?

A. Subnets

B. VLANs

C. Domains

D. Clusters

The correct choice, subnets, refers to the logical divisions of a larger network created by a router to improve performance and manageability. Subnetting allows the segmentation of a network into smaller, more efficient parts, making it easier to manage traffic, isolate network segments for security purposes, and optimize network performance. Each subnet operates as a distinct network segment, enhancing the overall structure and functionality of the broader physical network. VLANs, or Virtual Local Area Networks, are related in that they also segment networks, but they do so at the data link layer, allowing multiple networks to coexist on the same physical infrastructure. Domains typically refer to administrative boundaries in network or security contexts, while clusters are more relevant in computing for grouping network resources. Therefore, the term that best represents the segments created by a router in a physical network is indeed subnets.

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!