Security Plus Practice Test (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 type of agreement is more enforceable than a Memorandum of Understanding (MOU)?

A. Contractual Agreement

B. Service Level Agreement (SLA)

C. Partnership Agreement

D. Handshake Agreement

2. Which control is focused on reducing the risk of loss through specific security measures?

A. Operational controls

B. Management controls

C. Technical risk controls

D. Physical security controls

3. What does reporting in IT security management typically include?

A. Incident documentation

B. Alarms, alerts, and trends

C. User access logs

D. Firewall monitoring

4. What are the types of backups that optimize data management during recovery?

A. Mirrored and Shadow Backups

B. Full, Differential, and Incremental Backups

C. Complete and Partial Backups

D. Dynamic and Static Backups

5. How do organizations use big data analysis in the context of cybersecurity?

A. To enhance user training and awareness

B. To correlate attacks and identify patterns

C. To conduct individual user audits

D. To establish data encryption protocols

6. In what order should evidence be collected based on volatility?

A. Hard Drive, CPU Cache, RAM, Remote Logs

B. CPU Cache, RAM, CPU Registers, Swap File

C. Remote Logs, RAM, Swap File, CPU Registers

D. CPU Registers, Hard Drive, Memory, Swap File

7. In what scenario do smurf attacks occur?

A. The attacker impersonates the victim's IP address.

B. Only one computer sends traffic.

C. The victim is a database server.

D. Unique host addresses are targeted.

8. What allows for scalable secure remote access by managing multiple VPN connections?

A. VPN concentrator

B. Firewall

C. Load balancer

D. Proxy server

9. Which site offers the highest level of availability with full equipment and current data?

A. Cold site

B. Warm site

C. Hot site

D. Standard site

10. Which technique involves sifting through garbage to find sensitive information?

A. Dumpster diving

B. Tailgating

C. Watering hole attack

D. Vishing

Answers

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

Explanations

1. What type of agreement is more enforceable than a Memorandum of Understanding (MOU)?

A. Contractual Agreement

B. Service Level Agreement (SLA)

C. Partnership Agreement

D. Handshake Agreement

A Service Level Agreement (SLA) is a type of agreement that's structured to hold parties accountable for their performance in delivering specific services. It typically includes measurable metrics, expectations, and consequences if the terms are not met. Because an SLA is often formalized in writing and includes detailed obligations and standards for service delivery, it is generally more enforceable than a Memorandum of Understanding (MOU), which typically serves as a framework for future agreements without binding commitments. The enforceability of an SLA arises from its clarity and specificity regarding the expectations between the parties, ensuring that they can be held accountable for their commitments. This contrasts with an MOU, which is often considered more of a preliminary or exploratory document that expresses a mutual intention but lacks the binding contractual elements that make SLAs enforceable.

2. Which control is focused on reducing the risk of loss through specific security measures?

A. Operational controls

B. Management controls

C. Technical risk controls

D. Physical security controls

The focus of the question is on controls that specifically aim to reduce the risk of loss through security measures, which aligns perfectly with technical risk controls. Technical controls consist of security mechanisms and safeguards implemented through technological solutions. These include firewalls, intrusion detection systems, encryption, and access control mechanisms. Such controls are designed to protect the integrity, confidentiality, and availability of information by reducing vulnerabilities and threats in technological environments. Operational controls, while important, pertain more to processes and procedures that support day-to-day operations and maintaining security policies rather than directly implementing technical security measures. Management controls involve the governance and oversight aspects of security practices, including risk assessments and policy enforcement, focusing on the broader organizational framework rather than specific technical implementations. Physical security controls address the physical protection of facilities, equipment, and resources, which, while crucial for overall security, do not primarily deal with the technical measures that specifically aim to mitigate risks through technology. Thus, technical risk controls are indeed the most appropriate choice in this context for actively minimizing risk through targeted security implementations.

3. What does reporting in IT security management typically include?

A. Incident documentation

B. Alarms, alerts, and trends

C. User access logs

D. Firewall monitoring

In IT security management, reporting encompasses a variety of elements, one of which includes alarms, alerts, and trends. This is crucial because these components help in monitoring and analyzing security events within an organization. Alarms are triggered by certain predefined security criteria and alert security personnel of potential incidents or breaches, while alerts provide immediate notifications of identified threats or anomalies. Additionally, trends help organizations understand patterns of security incidents over time, which can be invaluable for proactive management and prevention strategies. This reporting is essential for effective incident management, ensuring that security teams can respond promptly and efficiently to potential threats, while also aiding in long-term security planning and adjustments based on observed data. By focusing on alarms, alerts, and trends, organizations can assess the effectiveness of current measures and refine their strategies to enhance overall security posture.

4. What are the types of backups that optimize data management during recovery?

A. Mirrored and Shadow Backups

B. Full, Differential, and Incremental Backups

C. Complete and Partial Backups

D. Dynamic and Static Backups

The types of backups that optimize data management during recovery are Full, Differential, and Incremental Backups. Each of these methods offers a specific way to safeguard data while enhancing recovery efficiency. Full backups involve copying all data within a designated set, providing a comprehensive snapshot that ensures all files are backed up at once. While this method can take longer and require more storage space, its strength lies in the simplicity of recovery—restoring from a single set of data. Differential backups, on the other hand, back up only the data that has changed since the last full backup. This method significantly reduces the backup time compared to full backups and facilitates quicker recovery than relying on multiple incremental backups, as you would only need the last full backup and the most recent differential backup to restore the data. Incremental backups capture only the data that has changed since the last backup (whether it's a full or incremental backup). This approach minimizes storage use and shortens backup time, but recovery can take longer since each incremental backup must be applied in succession following the last full backup. By using a combination of these methods, organizations can effectively manage large volumes of data and ensure quick recovery from various types of data loss scenarios. This optimization makes full, differential, and incremental backups the

5. How do organizations use big data analysis in the context of cybersecurity?

A. To enhance user training and awareness

B. To correlate attacks and identify patterns

C. To conduct individual user audits

D. To establish data encryption protocols

Organizations leverage big data analysis in cybersecurity primarily to correlate attacks and identify patterns. This approach enables them to analyze vast amounts of data from various sources, such as network logs, security alerts, and user behavior data. By identifying patterns and correlations, organizations can detect anomalies indicative of security threats, such as emerging attack vectors or previously unknown vulnerabilities. Through this analytical capability, security teams can respond more effectively to incidents by understanding the context and scale of threats. For example, recognizing patterns in phishing attacks over time can enhance the organization's ability to predict and prevent future incidents. Moreover, big data tools can facilitate real-time monitoring of network activities, enhancing the organization's situational awareness and improving the overall security posture. The other options, while relevant in some contexts, do not utilize big data analysis in the same impactful way. User training and awareness initiatives, individual user audits, and encryption protocols are crucial components of an overall security strategy but do not primarily hinge upon the capabilities offered by big data analysis in the realm of correlating attacks and identifying patterns.

6. In what order should evidence be collected based on volatility?

A. Hard Drive, CPU Cache, RAM, Remote Logs

B. CPU Cache, RAM, CPU Registers, Swap File

C. Remote Logs, RAM, Swap File, CPU Registers

D. CPU Registers, Hard Drive, Memory, Swap File

The correct answer emphasizes the order of evidence collection based on volatility, which is crucial in digital forensics. Evidence should generally be collected starting with the most volatile data and ending with the least volatile. When collecting evidence, CPU cache is the most volatile because it contains recently used data that will be lost if power is removed. Next in the hierarchy of volatility is RAM, which stores active processes and data currently in use. After RAM, CPU registers hold immediate data needed for processing but are less critical in forensic investigations. Finally, a swap file, which is a portion of the hard drive used as virtual memory, is the least volatile since it is persistent storage and will survive power loss. Understanding the concept of volatility helps in preserving evidence effectively, adhering to the principle of collecting data that may change or be lost quickly. Collecting evidence in the correct order ensures that the most transient and critical information is secured before it gets overwritten or lost.

7. In what scenario do smurf attacks occur?

A. The attacker impersonates the victim's IP address.

B. Only one computer sends traffic.

C. The victim is a database server.

D. Unique host addresses are targeted.

Smurf attacks are a type of denial-of-service (DoS) attack that exploits the Internet Control Message Protocol (ICMP). In this scenario, the attacker takes advantage of the broadcast addressing feature of IP networks by sending ICMP echo request (ping) packets to the broadcast address of a network while spoofing the victim's IP address. This means that all devices on the network respond to the ping request, causing a flood of traffic directed towards the victim's address. The consequence of this influx of responses can overwhelm the victim's network resources, making services unavailable. This method effectively amplifies the attack, as multiple devices respond to a single request, significantly increasing the amount of traffic directed at the victim. The key aspect of this attack is the IP address impersonation, which misleads the responding devices into sending their replies to the victim instead of the attacker, thus leading to the denial of service.

8. What allows for scalable secure remote access by managing multiple VPN connections?

A. VPN concentrator

B. Firewall

C. Load balancer

D. Proxy server

The VPN concentrator is specifically designed to manage multiple VPN connections efficiently, making it the best choice for scalable secure remote access. It facilitates the establishment of numerous VPN tunnels, which enables organizations to connect a large number of remote users or branch offices to a secure network. The concentrator handles the encryption and decryption of the data being sent over the VPN, ensuring that the traffic remains secure, and it can also manage user authentication and authorization. The ability of a VPN concentrator to scale is a critical feature, particularly for enterprises that need to support various users simultaneously without compromising performance or security. This scalable architecture allows organizations to adapt to growing demands for remote access, making it a vital component in secure networking solutions. In contrast, other options like firewalls primarily focus on controlling access to the network rather than managing VPN connections specifically. Load balancers distribute traffic across multiple servers but do not inherently provide VPN capabilities. Proxy servers act as intermediaries for requests from clients seeking resources from other servers, but they do not facilitate the establishment of secure VPN connections in the same manner. Therefore, the VPN concentrator stands out as the appropriate choice for the scenario described.

9. Which site offers the highest level of availability with full equipment and current data?

A. Cold site

B. Warm site

C. Hot site

D. Standard site

A hot site is designed to provide the highest level of availability and minimal downtime for critical systems. This type of site is equipped with hardware, software, and the infrastructure needed to immediately take over operations in the event of a disaster. It is maintained in a constant state of readiness, often mirroring the primary site's environment with real-time or near-real-time backups of data. This ensures that, in the event of a failure, services can be restored quickly with little to no data loss since the data is up-to-date. In contrast, a cold site would have no live systems or data, requiring significant time and resources to bring up to operational status. A warm site holds some equipment and may offer partial availability, but it does not have the most recent data readily available, as it typically requires manual updates or synchronization. A standard site does not denote a specific recovery strategy and would not guarantee the same level of preparedness or immediacy in the event of an incident. Therefore, the hot site is the most effective choice for organizations that prioritize minimizing downtime and maintaining continuous access to their critical operations.

10. Which technique involves sifting through garbage to find sensitive information?

A. Dumpster diving

B. Tailgating

C. Watering hole attack

D. Vishing

The technique that involves sifting through garbage to find sensitive information is known as dumpster diving. This practice is often employed by attackers to gather confidential data, such as discarded documents with personal information, account details, or company data, which can provide insight into a target's vulnerabilities. They seek out anything that may have been improperly discarded, including physical documents or discarded electronic devices that could still contain data. By recovering this information, attackers can potentially use it to launch further attacks, conduct identity theft, or gain unauthorized access to secure areas or systems. This emphasizes the importance of proper data disposal and secure document shredding to protect sensitive information.

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://securityplus.examzify.com

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