CompTIA Security+ (SY0-701) Certification Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

This is a sample study guide. To access the full version with hundreds of questions,

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Table of Contents

Copyright 1
Table of Contents 2
Introduction 3
How to Use This Guide 4
Questions 6
Answers 9
Explanations 11
Next Steps 17

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. Don’t worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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. **Which term describes the technique of controlling previously compromised systems to conduct illegal activities?**

   A. Exploited Network

   B. Botnet

   C. Backdoor Access

   D. Malware Infrastructure

2. **Which type of tool is Wireshark considered in network management?**

   A. Network blogging tool

   B. Network analysis tool

   C. Web design software

   D. Database management system

3. **What is the primary function of detective controls in cybersecurity?**

   A. To prevent unauthorized access

   B. To alert and inform about ongoing security incidents

   C. To aid in system recovery

   D. To discourage potential attackers

4. **Which type of authentication is based on something you know?**

   A. Knowledge Factor

   B. Possession Factor

   C. Biometric Factor

   D. Locational Factor

5. **Which factor describes something that a user does?**

   A. Inherence Factor

   B. Location Factor

   C. Possession Factor

   D. Action Factor

6. What type of IDS is installed on a computer or server?

A. Network-based IDS

B. Host-based IDS

C. Hybrid IDS

D. Distributed IDS

7. Which of the following describes a software-based client system that monitors data in use and can stop file transfers?

A. Endpoint DLP Systems

B. Network Security Systems

C. Data Integrity Systems

D. Firewall Systems

8. What is a characteristic feature of network analysis tools like Wireshark?

A. They create network traffic

B. They capture and analyze network traffic

C. They exclusively provide user interface design

D. They reduce server response times

9. What can be a consequence of not effectively managing risk?

A. Reduced employee turnover

B. Increased vulnerability to security breaches

C. Enhanced corporate reputation

D. Lower operational costs

10. What are the three main pillars of security?

A. Confidentiality, Integrity, Availability

B. Identification, Authentication, Authorization

C. Prevention, Detection, Response

D. Safety, Security, Secrecy

Answers

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

Explanations

1. Which term describes the technique of controlling previously compromised systems to conduct illegal activities?

A. Exploited Network

B. Botnet

C. Backdoor Access

D. Malware Infrastructure

The term that describes the technique of controlling previously compromised systems to conduct illegal activities is "botnet." A botnet refers to a network of infected computers, often referred to as "zombies," which are controlled by an attacker without the consent of the owners. The attacker can leverage this network to perform various malicious activities, such as sending spam emails, conducting distributed denial-of-service (DDoS) attacks, or mining cryptocurrency. In this context, "botnet" accurately captures the idea of a collection of compromised systems being directed as a group to achieve malicious objectives. Systems in a botnet are typically infected with malware that allows the attacker to maintain control over them, enabling a wide range of exploitative functions. Other terms, while related to cybersecurity, do not fully encapsulate the organized control and utilization of compromised devices in the same way as a botnet does. Exploited networks, for example, could refer to any network that has been breached but doesn't imply the organized control aspect associated with botnets. Backdoor access refers more to a method of bypassing security controls on a single system rather than controlling a network of systems. Malware infrastructure, while related to the tools and frameworks used for malware deployment, does not specify the network aspect

2. Which type of tool is Wireshark considered in network management?

A. Network blogging tool

B. Network analysis tool

C. Web design software

D. Database management system

Wireshark is recognized as a network analysis tool because it enables users to capture and interactively browse the traffic running on a computer network. This type of software allows for in-depth packet analysis, helping network professionals and security experts to diagnose problems, understand network protocols, and analyze data flows or anomalies. In detail, Wireshark provides the capability to dissect network packets, offering insights into network performance, security vulnerabilities, and traffic management. Its features include filtering options that allow users to see specific traffic flows, as well as the ability to export the captured data for further analysis. This focus on network traffic inspection and analysis is what distinctly categorizes Wireshark as a network analysis tool rather than any of the other options listed. For instance, it is not a blogging tool, as blogging tools facilitate content creation and distribution, which Wireshark does not do. It also does not serve as web design software or a database management system, as those tools are designed for different purposes such as creating websites or managing structured data, respectively.

3. What is the primary function of detective controls in cybersecurity?

A. To prevent unauthorized access

B. To alert and inform about ongoing security incidents

C. To aid in system recovery

D. To discourage potential attackers

Detective controls play a crucial role in cybersecurity by focusing on identifying and alerting organizations about ongoing or potential security incidents. These types of controls are designed to monitor systems and networks for signs of security breaches or anomalies. When a security incident occurs, detective controls ensure that the incident is recognized and reported, enabling a prompt response to mitigate damage. Getting alerts allows security teams to quickly investigate incidents and take necessary actions to protect assets, which is fundamental in minimizing the impact of security breaches. This proactive monitoring contributes significantly to an organization's overall security posture and aids in compliance with various regulatory requirements. In contrast, the other options primarily serve different purposes: preventing unauthorized access involves preventive controls, aiding in system recovery relates to corrective measures, and discouraging potential attackers typically falls under deterrent controls. Each control type plays a unique role in a comprehensive security strategy, but the primary function of detective controls is indeed to detect and report security incidents.

4. Which type of authentication is based on something you know?

A. Knowledge Factor

B. Possession Factor

C. Biometric Factor

D. Locational Factor

The type of authentication that is based on something you know is aptly called the Knowledge Factor. This refers to information that only the user should know, such as passwords, PINs, or answers to security questions. Knowledge-based authentication is fundamental to ensuring that the individual attempting to access a system can confirm their identity by providing this specific piece of information, which should be secret and not easily guessed or discovered by others. In the realm of authentication methods, this contrasts with other factors. The Possession Factor, for example, relies on something the user has, like a security token or a smart card. The Biometric Factor uses unique physical characteristics of the user, such as fingerprints or facial recognition, to verify identity. The Locational Factor would involve the context of the user's location, often evaluated through geolocation services or IP address assessments. Understanding these distinctions helps in implementing robust security measures tailored to various scenarios.

5. Which factor describes something that a user does?

A. Inherence Factor

B. Location Factor

C. Possession Factor

D. Action Factor

The factor that describes something a user does is referred to as the Action Factor. This concept pertains to the observable behaviors or actions performed by a user, which can be used for authentication or establishing a user's identity. In the context of security, understanding user actions, such as keystrokes, gestures, or specific patterns of behavior, can be valuable when implementing behavioral biometrics. This type of measurement provides insights into how a user interacts with a system, adding a layer of security by distinguishing between legitimate users and potential threats based on their activity patterns. The other factors mentioned do not pertain specifically to user actions. The Inherence Factor relates to identity characteristics inherent to the user, like fingerprints or facial recognition. The Location Factor involves the geographic location from which access is attempted, which can help determine trustworthiness based on the origin of the access. The Possession Factor refers to something the user has, such as a smart card or a token, which does not involve user behavior but rather something tangible that can be physically possessed.

6. What type of IDS is installed on a computer or server?

A. Network-based IDS

B. Host-based IDS

C. Hybrid IDS

D. Distributed IDS

A host-based IDS (Intrusion Detection System) is specifically designed to be installed on individual computers or servers, monitoring the activities and events occurring on that specific host. It focuses on detecting suspicious activities by analyzing system logs, file system changes, and process activities. By being localized, it can provide granular insights into the behavior of applications and users on that host. This type of IDS is particularly useful for identifying threats that may not be visible to network-based solutions, as those often monitor traffic flowing across a network rather than the activities taking place on an individual machine. Host-based IDS can alert administrators to unauthorized access attempts, malware infections, or policy violations directly on the system it protects, making it an essential layer in a comprehensive security strategy. Network-based IDS, on the other hand, monitors traffic on the network to identify unusual patterns or known signatures of attacks, while hybrid and distributed IDS refer to systems that combine elements of both host and network-based approaches for broader coverage.

7. Which of the following describes a software-based client system that monitors data in use and can stop file transfers?

A. Endpoint DLP Systems

B. Network Security Systems

C. Data Integrity Systems

D. Firewall Systems

The correct choice is a software-based client system known as Endpoint DLP (Data Loss Prevention) Systems. These systems are designed to monitor and protect sensitive data in use by tracking activities involving data access, modifications, and transfers. By employing various techniques, these systems can recognize when a user attempts to transfer files that meet certain criteria (for example, those containing sensitive information) and can intervene by blocking or stopping those transfers to prevent data leakage. Endpoint DLP systems operate at the endpoint level, meaning they function directly on the devices used by employees, such as computers or mobile devices. This allows them to enforce policies regarding how data is handled and shared, whether it is through email, cloud services, or removable storage devices. Understanding the role of Endpoint DLP systems is critical in a security framework, particularly in environments that handle sensitive data, as this technology helps organizations comply with regulations and protects proprietary information from unauthorized access or transmission.

8. What is a characteristic feature of network analysis tools like Wireshark?

A. They create network traffic

B. They capture and analyze network traffic

C. They exclusively provide user interface design

D. They reduce server response times

Network analysis tools like Wireshark are designed primarily to capture and analyze network traffic. This capability allows users to monitor the data packets that traverse a network in real-time, which is crucial for troubleshooting issues, understanding network flows, and identifying potential security threats. By examining the details of these packets, such as their source and destination addresses, protocols used, and payload data, users can gain insights into network performance and detect anomalies. The function of capturing network traffic is essential for network administrators and security professionals who need to assess the health of a network and ensure it operates as intended. Analyzing the captured traffic enables them to diagnose problems, optimize configurations, and enhance security measures. Creating network traffic, providing user interface design, or reducing server response times do not accurately describe the primary functions of a network analysis tool like Wireshark, which is focused on observation and examination rather than generation or solely design-related tasks.

9. What can be a consequence of not effectively managing risk?

A. Reduced employee turnover

B. Increased vulnerability to security breaches

C. Enhanced corporate reputation

D. Lower operational costs

Not effectively managing risk can lead to increased vulnerability to security breaches. When an organization fails to identify, assess, and mitigate risks, it leaves itself exposed to a variety of threats that can compromise sensitive data, disrupt operations, and damage relationships with clients and stakeholders. Effective risk management involves continuously monitoring for vulnerabilities and implementing appropriate controls to protect against potential breaches. If these measures are lacking, an organization is more likely to experience attacks or incidents that can lead to significant financial loss, legal repercussions, and a tarnished reputation. Therefore, businesses must prioritize risk management to safeguard their assets, ensure compliance with regulations, and maintain the trust of their customers.

10. What are the three main pillars of security?

A. Confidentiality, Integrity, Availability

B. Identification, Authentication, Authorization

C. Prevention, Detection, Response

D. Safety, Security, Secrecy

The three main pillars of security are Confidentiality, Integrity, and Availability, often referred to as the CIA triad. Confidentiality ensures that information is accessible only to those authorized to have access. It aims to protect sensitive information from unauthorized disclosure, employing various measures such as encryption and access controls. Integrity refers to the accuracy and reliability of data, ensuring that it is not altered in an unauthorized way. This pillar maintains the trustworthiness of information, using checksums, hashing, and validation techniques to detect unauthorized changes. Availability ensures that information and resources are accessible to authorized users when needed. This aspect of security involves implementing measures to prevent downtime and ensure systems are operational, including redundancy, failover systems, and regular updates. By focusing on these three pillars, organizations can create a robust security framework that protects their information assets effectively.

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://comptiasecplussy0701.examzify.com

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