CISCO CYBER SECURITY PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cisco-cybersecurity.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 non-technical method could a cybercriminal use to gather sensitive information from an organization?**

   A. Phishing

   B. Social Engineering

   C. Malware

   D. Hacking

2. **Granting unauthorized access to a corporate headquarters is an example of which type of incident?**

   A. Internal

   B. External

   C. Administrative

   D. Technical

3. **Which protocol governs communication between devices in a remote Linux lab environment accessed from a tablet?**

   A. FTP

   B. HTTP

   C. Secure Shell (SSH)

   D. Telnet

4. **What is a key benefit of disabling internal CD drives and USB ports?**

   A. Enhances system performance

   B. Reduces risk of unauthorized media usage

   C. Improves data speed access

   D. Ensures network stability

5. **What is the primary purpose of a hypervisor in virtualization?**

   A. To manage storage

   B. To monitor network traffic

   C. To create multiple virtual machines

   D. To secure user passwords

SAMPLE

6. To prevent unauthorized access by rogue users, what policy should be implemented?

A. Define strict access control policies, standards, procedures and guidelines

B. Allow open access to all users

C. Use public Wi-Fi only

D. Do not monitor user activities

7. What type of policies should an organization develop to standardize approved applications and operating system configurations?

A. Security policies

B. System-specific policies

C. Access control policies

D. Incident response policies

8. Which device prevents single-packet attacks from reaching their target?

A. VPN

B. IPS

C. IDS

D. Firewall

9. What strategy can be implemented to prevent attacks on SCADA systems?

A. Regular software updates

B. Segregate internal and external networks

C. Use strong passwords

D. Train employees on security

10. Which system passively monitors network traffic without interfering with it?

A. IPS

B. IDS

C. Firewall

D. Proxy server

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What non-technical method could a cybercriminal use to gather sensitive information from an organization?

A. Phishing

B. Social Engineering

C. Malware

D. Hacking

Social engineering is a non-technical method used by cybercriminals to deceive individuals into divulging confidential or sensitive information. This approach relies on manipulating human psychology rather than exploiting technical vulnerabilities. Cybercriminals may employ tactics such as impersonating authority figures, using psychological tricks to create a sense of urgency, or establishing trust to encourage victims to share personal information, passwords, or access credentials. In the context of security, while phishing does involve deceptive tactics to collect sensitive information, it is typically executed through electronic communication, making it a more technical method compared to social engineering. Other terms like malware and hacking refer to technical approaches that involve software and system vulnerabilities, whereas social engineering emphasizes the interpersonal interaction aspect. This distinction is what makes social engineering noteworthy as a non-technical method for information gathering.

2. Granting unauthorized access to a corporate headquarters is an example of which type of incident?

A. Internal

B. External

C. Administrative

D. Technical

The situation of granting unauthorized access to a corporate headquarters is aligned with the concept of external incidents. An external incident typically involves threats that originate from outside the organization and pose a risk to its operations, data, or assets. In this case, if the access was unauthorized, it implies an external actor could have exploited vulnerabilities or gaps in security protocols to gain access to a sensitive area. The nature of external incidents often involves unauthorized attempts to breach physical security or IT systems by individuals or entities that are not part of the organization. This could include cyberattacks, physical break-ins, or any unauthorized intrusion that compromises the security of the organization. In contrast, internal incidents would involve actions or breaches that are perpetrated by individuals within the organization, such as employees or contractors, which is not applicable here since the emphasis is on unauthorized access that appears to be facilitated by external means. Administrative incidents refer to failures in policies or procedures, while technical incidents pertain more to failures in technology or infrastructure. None of these focuses specifically on the notion of access granted inappropriately from an outside source, making external the most fitting classification in this context.

SAMPLE

3. Which protocol governs communication between devices in a remote Linux lab environment accessed from a tablet?

A. FTP

B. HTTP

C. Secure Shell (SSH)

D. Telnet

Secure Shell (SSH) is the appropriate protocol for governing communication between devices in a remote Linux lab environment, especially when accessing the system from a tablet. SSH is designed specifically for secure remote login and command execution, allowing users to connect to devices over an insecure network while ensuring that both authentication and data transmission are encrypted. This encryption is crucial in a lab environment to protect against eavesdropping and data tampering. Using SSH provides a robust layer of security through strong encryption algorithms and enables secure access to the command line of a remote Linux system. It also supports various authentication methods, including password authentication, public key authentication, and more, enhancing its versatility and security. While other protocols such as FTP and Telnet can facilitate communication with devices, they do not provide the same level of security. FTP, for instance, does not encrypt its traffic, making it vulnerable to interception. Telnet also transmits data in plain text, which is not suitable for secure sessions. HTTP can be used for web traffic but lacks encryption unless paired with HTTPS, which is not specifically intended for command-line access. Thus, SSH stands out as the most secure and suitable choice for remote administration in this context.

4. What is a key benefit of disabling internal CD drives and USB ports?

A. Enhances system performance

B. Reduces risk of unauthorized media usage

C. Improves data speed access

D. Ensures network stability

Disabling internal CD drives and USB ports significantly reduces the risk of unauthorized media usage, which is a critical aspect of organizational security protocols. By restricting access to these ports, you limit the opportunity for employees or attackers to introduce unapproved external devices or media into the system. This action mitigates the likelihood of malware infections, data exfiltration, or the transfer of sensitive information onto potentially compromised devices. In environments where data security is paramount, preventing unauthorized media usage helps ensure that sensitive data does not leave the secure confines of the organization or become vulnerable to external attacks. This proactive approach plays a vital role in protecting data integrity and confidentiality, thereby enhancing overall security posture. While enhancing system performance, improving data speed access, and ensuring network stability may be important considerations in specific contexts, the primary focus when disabling external drives and ports is undeniably centered around mitigating risks associated with unauthorized access and data breaches.

SAMPLE

5. What is the primary purpose of a hypervisor in virtualization?

A. To manage storage

B. To monitor network traffic

C. To create multiple virtual machines

D. To secure user passwords

The primary purpose of a hypervisor in virtualization is to create multiple virtual machines. A hypervisor acts as a layer that sits between the physical hardware and the virtual machines, allowing it to efficiently allocate system resources such as CPU, memory, and storage across these virtual machines. This capability enables the simultaneous running of different operating systems on a single physical machine, facilitating better resource utilization, isolation, and management. While managing storage and monitoring network traffic are important aspects of a virtualized environment, those tasks are typically handled by other components within the infrastructure rather than by the hypervisor itself. For instance, storage management can be performed by storage area networks (SANs) or software-defined storage solutions, and network traffic monitoring may involve specialized tools or software. Additionally, securing user passwords falls outside the scope of a hypervisor's functionality, which is focused on resource management and virtualization rather than security of individual user credentials. Thus, the emphasis on creating multiple virtual machines highlights the core functionality provided by a hypervisor.

6. To prevent unauthorized access by rogue users, what policy should be implemented?

A. Define strict access control policies, standards, procedures and guidelines

B. Allow open access to all users

C. Use public Wi-Fi only

D. Do not monitor user activities

Implementing strict access control policies, standards, procedures, and guidelines is crucial for protecting sensitive resources and preventing unauthorized access by rogue users. These policies define who can access specific resources and under what conditions, thereby establishing clear parameters that help safeguard the organization's information assets. Access control policies typically include methods such as user authentication, authorization processes, and accounting measures that ensure users are properly identified and permitted to access only the necessary information for their role. By clearly outlining security protocols, organizations can mitigate risks associated with unauthorized access, ensuring that even if rogue users attempt to infiltrate the system, they would be blocked by stringent controls in place. Other options, such as allowing open access or relying on public Wi-Fi, drastically undermine security measures and expose the organization to significant risks. Not monitoring user activities also fails to provide visibility into potentially harmful behaviors or access attempts, making it difficult to respond to suspicious actions. Thus, defining and enforcing strict access control policies is essential for maintaining a secure environment against unauthorized access.

SAMPLE

7. What type of policies should an organization develop to standardize approved applications and operating system configurations?

A. Security policies

B. System-specific policies

C. Access control policies

D. Incident response policies

Developing system-specific policies is essential for standardizing approved applications and operating system configurations within an organization. These policies serve as formal guidelines that dictate how systems should be configured and what software should be allowed, thereby ensuring consistency and security across the network. System-specific policies provide clear criteria for evaluating and approving applications and configurations, helping to prevent unauthorized or vulnerable software from being used. By establishing these guidelines, organizations can enforce compliance, mitigate risks, and enhance overall security posture. These policies often detail the requirements for software installation, baseline configurations, patch management, and monitoring practices, making them a foundational element of a robust cybersecurity framework. In contrast, security policies generally cover a broader range of security issues without diving into specific systems or applications. Access control policies focus on managing user permissions rather than the configurations of systems themselves, and incident response policies are designed to outline the procedures to follow when a security incident occurs. Therefore, while all these types of policies play vital roles in an organization's cybersecurity strategy, system-specific policies are the most relevant for standardizing approved applications and OS configurations.

8. Which device prevents single-packet attacks from reaching their target?

A. VPN

B. IPS

C. IDS

D. Firewall

The device that prevents single-packet attacks from reaching their target is an Intrusion Prevention System (IPS). An IPS actively monitors network traffic and can take predefined actions to block, drop, or alert on suspicious packets, thus providing a proactive defense against various attacks, including single-packet attacks that may exploit vulnerabilities in a system or application. An IPS is designed to analyze traffic in real-time, detecting and responding to threats immediately. By inspecting individual packets and their behavior, it can identify and mitigate attacks that may seek to manipulate or disrupt a service, such as those that utilize a series of deceptive or malformed packets aimed at causing a failure or exploitation. In contrast, a firewall primarily focuses on permitting or denying traffic based on predetermined security rules but may not analyze packet-level details to the same extent as an IPS. While a Virtual Private Network (VPN) secures and directs traffic and an Intrusion Detection System (IDS) monitors for malicious activity without actively blocking it, they do not provide the same level of protection against single-packet or other types of active attacks as an IPS does.

SAMPLE

9. What strategy can be implemented to prevent attacks on SCADA systems?

A. Regular software updates

B. Segregate internal and external networks

C. Use strong passwords

D. Train employees on security

Segregating internal and external networks is a highly effective strategy to prevent attacks on SCADA (Supervisory Control and Data Acquisition) systems. This approach operates on the principle of isolating critical infrastructure from potential threats originating from the internet or unsecured networks. By implementing network segmentation, you can create zones of trust within the network, ensuring that sensitive components of the SCADA system are not directly accessible from external environments. This isolation minimizes the risk of unauthorized access and potential exploits, as even if an attacker gains access to the external network or less secure internal segments, they face additional barriers when attempting to reach the SCADA systems. Firewalls, intrusion detection systems, and secure gateways can control and monitor traffic between these segregated networks, providing an added layer of security. In contrast, while regular software updates, strong passwords, and employee training are all important facets of a holistic cybersecurity strategy, they do not specifically address the risk exposure of SCADA systems in the same direct manner as network segregation. Software updates reduce vulnerabilities, strong passwords enhance access control, and training raises awareness, but without proper network segregation, these measures alone might not sufficiently protect SCADA systems from determined or sophisticated attacks. Therefore, network segregation stands out as a fundamental preventive measure to shield

10. Which system passively monitors network traffic without interfering with it?

A. IPS

B. IDS

C. Firewall

D. Proxy server

An Intrusion Detection System (IDS) is designed to passively monitor network traffic for the purpose of identifying suspicious activities or policy violations. Unlike an Intrusion Prevention System (IPS), which actively blocks or prevents identified threats in real-time, an IDS simply observes and analyzes the data flowing through the network. It generates alerts or notifications when potential threats are detected, allowing network administrators to take action based on that data without impacting the current traffic flow. The primary function of an IDS centers on surveillance and logging, providing insights into network activities without directly influencing them. This characteristic is crucial for environments where data integrity and continuity are vital, as it ensures that normal operations are not disrupted by automated countermeasures. In contrast, systems like firewalls and proxy servers are designed to actively manage and control network traffic, either by allowing or blocking such traffic based on predetermined security policies, which means they do not fit the criterion of passive monitoring. The approach of an IDS offers a layer of security through visibility and awareness, which is fundamental in cybersecurity practices.

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://cisco-cybersecurity.examzify.com

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

SAMPLE