Cisco Cyber Security Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

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**

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 technology would you use to segment a computer network for better performance and security?

A. Virtual Private Network (VPN)

B. VLAN

C. Network Access Control (NAC)

D. Firewall

2. Which type of software actively warns users upon detection of a virus?

A. Antivirus protection

B. Spyware protection

C. Adware protection

D. Phishing protection

3. Which method is NOT used for identity verification in authentication?

A. Something you are

B. Something you have

C. Something you create

D. Something you know

4. What type of antimalware protection blocks known phishing websites?

A. Adware protection

B. Spyware protection

C. Phishing protection

D. Antivirus protection

5. What system monitors network traffic and analyzes packets for malicious activities?

A. IPS

B. Firewall

C. VPN

D. Switch

6. Which type of controls help uncover new potential threats?

A. Preventive Controls

B. Corrective Controls

C. Detective Controls

D. Operational Controls

7. What type of cybersecurity laws provide protection against an organization that wants to share personal data?

A. Data protection laws

B. Privacy laws

C. Intellectual property laws

D. Cybersecurity laws

8. Which of the following best defines phishing?

A. Verbal deception to extract information

B. Technical exploitation of vulnerabilities

C. Fraudulent attempts to obtain sensitive information

D. Unauthorized access to computer systems

9. What is a primary goal of implementing system-specific policies?

A. Enhance user experience

B. Standardize operational practices

C. Manage all organizational data

D. Minimize costs

10. What protocol is used for securely transferring files between devices?

A. File Transfer Protocol (FTP)

B. Hypertext Transfer Protocol (HTTP)

C. Secure Copy (SCP)

D. Transport Layer Security (TLS)

Answers

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

Explanations

1. What technology would you use to segment a computer network for better performance and security?

A. Virtual Private Network (VPN)

B. VLAN

C. Network Access Control (NAC)

D. Firewall

Using VLAN technology is an effective approach to segment a computer network, enhancing both performance and security. A Virtual Local Area Network (VLAN) allows for the logical segmentation of a network at the data link layer (Layer 2) of the OSI model. By creating VLANs, network administrators can group together devices with similar requirements or functions, regardless of their physical location. This segmentation facilitates improved performance since broadcast traffic is restricted to individual VLANs; therefore, it reduces network congestion and enhances overall efficiency. On the security front, VLANs enable better control over communications between devices. By segmenting different departments or types of traffic (such as separating user data from sensitive information), it becomes more difficult for unauthorized users to access critical resources. While other technologies like Virtual Private Networks (VPNs) help secure remote connections, Network Access Control (NAC) focuses on enforcing security policies for devices trying to access the network, and firewalls serve to protect against external threats. However, they do not inherently provide the same level of network segmentation that VLANs offer for improving performance and enhancing security within the network itself.

2. Which type of software actively warns users upon detection of a virus?

A. Antivirus protection

B. Spyware protection

C. Adware protection

D. Phishing protection

Antivirus protection is designed to detect, prevent, and respond to malware threats, including viruses. The key function of antivirus software is its ability to actively monitor file systems, email attachments, and downloads for any suspicious behavior or known virus signatures. Upon detection of a virus, this software promptly alerts the user, providing immediate information about the potential threat. While other types of software, such as spyware protection, adware protection, and phishing protection, focus on their specific threats, they do not represent comprehensive virus protection. Spyware protection specifically targets programs that gather users' personal information without their consent, while adware protection deals with software that automatically delivers advertisements. Phishing protection aims to prevent the theft of sensitive information through deceptive emails or websites. None of these options includes the functionality to proactively warn users upon the detection of a virus in the way that antivirus software does. Therefore, the choice of antivirus protection is accurate as it fulfills the requirement of actively notifying users when a virus is detected.

3. Which method is NOT used for identity verification in authentication?

A. Something you are

B. Something you have

C. Something you create

D. Something you know

In the context of authentication methods, "Something you are," "Something you have," and "Something you know" are all widely recognized categories used to verify a person's identity. "Something you are" refers to biometric methods, such as fingerprints or facial recognition, which rely on unique physical characteristics of an individual. "Something you have" involves possession-based authentication, like security tokens or smart cards, which require the user to possess a physical item to gain access. "Something you know" encompasses knowledge-based authentication, such as passwords or PINs, which depend on the user's ability to recall specific information. On the other hand, "Something you create" is not a standard category of authentication. While users may create certain elements as part of security measures (like security questions or custom passwords), this does not inherently fit the conventional frameworks of identity verification methods. Therefore, it is not classified as a recognized method for identity verification in the authentication process.

4. What type of antimalware protection blocks known phishing websites?

A. Adware protection

B. Spyware protection

C. Phishing protection

D. Antivirus protection

Phishing protection specifically targets and blocks known phishing websites, which are malicious sites designed to trick users into divulging sensitive information such as usernames, passwords, and credit card numbers. This type of protection employs various techniques, including regularly updated blacklists of known phishing URLs, heuristic analysis, and machine learning algorithms to identify and mitigate potential phishing threats in real-time. By actively monitoring web traffic and comparing URLs against these databases, phishing protection can effectively prevent users from engaging with dangerous sites. The other options, while related to cybersecurity, serve different functions. Adware protection focuses on preventing unwanted advertisements that may disrupt user experience or collect data without consent. Spyware protection aims to detect and eliminate software designed to gather user information secretly and transmit it elsewhere, often compromising privacy. Antivirus protection is primarily concerned with detecting and removing malicious software, including viruses and worms, rather than specifically targeting phishing attacks. Therefore, phishing protection is precisely what is needed to contend with threats posed by phishing websites.

5. What system monitors network traffic and analyzes packets for malicious activities?

A. IPS

B. Firewall

C. VPN

D. Switch

The system that monitors network traffic and analyzes packets for malicious activities is an Intrusion Prevention System (IPS). An IPS actively inspects incoming and outgoing traffic and can identify patterns that suggest malicious intent, such as attempts at unauthorized access or the presence of known attack signatures. It not only detects potential threats but also takes action to block or prevent those threats in real time, enhancing network security. In contrast, a firewall primarily acts as a barrier that controls what traffic is allowed to enter or leave a network based on predefined security rules. While it can block certain types of traffic, it does not provide the same level of traffic analysis for the purpose of identifying malicious behavior. A Virtual Private Network (VPN) is primarily designed for creating secure connections over the internet by encrypting data transmissions, focusing on confidentiality and privacy rather than actively monitoring for intrusions. A switch operates at the data link layer to connect devices within a local network, managing data packet forwarding efficiently but is not designed for monitoring or analyzing packets for security threats. Thus, an IPS is specifically tailored for the task of analyzing network traffic for malicious activities, which makes it the correct choice.

6. Which type of controls help uncover new potential threats?

A. Preventive Controls

B. Corrective Controls

C. Detective Controls

D. Operational Controls

Detective controls are designed specifically to identify and uncover potential threats that may not have been previously recognized. These controls continuously monitor systems and activities for unusual patterns, anomalies, or any signs of unauthorized access, thereby facilitating the discovery of emerging threats. Examples include intrusion detection systems, security information and event management (SIEM) systems, and logs that record and analyze user activity. By implementing detective controls, organizations can enhance their security posture by not only responding to incidents but also by proactively identifying new threats before they escalate into significant breaches. This capability is essential for maintaining an updated threat model in an ever-evolving cyber landscape, allowing organizations to adjust their security measures accordingly. Preventive controls, on the other hand, are focused on stopping threats before they occur, while corrective controls aim to rectify issues after they have been detected. Operational controls typically involve the processes and procedures used to manage and maintain security operations but do not specifically address the uncovering of new threats.

7. What type of cybersecurity laws provide protection against an organization that wants to share personal data?

A. Data protection laws

B. Privacy laws

C. Intellectual property laws

D. Cybersecurity laws

The correct choice is privacy laws, which specifically address the handling and sharing of personal data by organizations. These laws are designed to safeguard individuals' personal information and provide individuals with rights regarding their data—such as the right to know how their data is used, the ability to access that data, and the right to request its deletion. Privacy laws mandate that organizations must obtain consent from individuals before sharing their personal information with third parties. This ensures that personal data is not distributed without the clear and informed consent of the person to whom the data pertains, thus fostering trust between consumers and organizations. Moreover, compliance with privacy laws often necessitates transparency regarding data handling practices, reinforcing the protection of individuals' rights related to their personal information. While data protection laws also focus on how personal data is processed and protected, privacy laws are more directly concerned with the consent and rights of individuals regarding their personal information. Intellectual property laws focus on protecting creations of the mind like inventions and artistic works, and cybersecurity laws deal more with securing information systems and mitigating cyber threats rather than the specific sharing of personal data.

8. Which of the following best defines phishing?

A. Verbal deception to extract information

B. Technical exploitation of vulnerabilities

C. Fraudulent attempts to obtain sensitive information

D. Unauthorized access to computer systems

Phishing is best defined as fraudulent attempts to obtain sensitive information. This method typically involves deception, where attackers masquerade as trustworthy entities in electronic communications, most commonly through emails, but it can also occur in text messages or social media. The objective is to trick individuals into revealing personal information, such as passwords, credit card details, or social security numbers. The key characteristic of phishing is its reliance on manipulation and impersonation rather than on exploiting technical vulnerabilities or security flaws. It often exploits social engineering principles, playing on the targets' emotions—such as fear or urgency—to prompt them to act quickly without careful consideration. In contrast, other definitions involve different types of security threats: verbal deception refers to social engineering but lacks the electronic component that defines phishing; technical exploitation targets system vulnerabilities rather than manipulating individuals for their data; and unauthorized access to computer systems refers to hacking rather than the specific act of deceit involved in phishing attacks. Each of these options emphasizes different methods or targets within the realm of cybersecurity, but only phishing aligns specifically with the fraudulent acquisition of sensitive information through electronic deception.

9. What is a primary goal of implementing system-specific policies?

A. Enhance user experience

B. Standardize operational practices

C. Manage all organizational data

D. Minimize costs

The primary goal of implementing system-specific policies is to standardize operational practices. These policies establish clear guidelines and protocols tailored to specific systems within an organization. By standardizing practices, organizations can ensure consistency in how different systems are used and managed, leading to better efficiency and compliance with regulatory requirements. This also helps in training users, as they will have a clear understanding of how to interact with particular systems based on established policies. Additionally, standardized practices reduce variability, which can lead to errors and security vulnerabilities, thereby enhancing the overall security posture of the organization. While enhancing user experience, managing organizational data, and minimizing costs are important considerations for businesses, they are more secondary benefits that can arise from the establishment of standardized policies rather than the primary goal. The focus on operational consistency is essential for effective system governance and risk management.

10. What protocol is used for securely transferring files between devices?

A. File Transfer Protocol (FTP)

B. Hypertext Transfer Protocol (HTTP)

C. Secure Copy (SCP)

D. Transport Layer Security (TLS)

Secure Copy (SCP) is a network protocol that specifically allows for the secure transfer of files between devices over a network. It utilizes the SSH (Secure Shell) protocol to provide authentication and encryption, ensuring that the data being transferred remains confidential and secure from potential eavesdropping or interception. What sets SCP apart from other protocols is its inherent focus on security. While File Transfer Protocol (FTP) does allow for file transfers, it does so without encryption, exposing data to vulnerabilities during transit. Hypertext Transfer Protocol (HTTP) is designed for transferring web pages and is not secure by default, although it has a secure version (HTTPS) that uses TLS. Transport Layer Security (TLS) itself is a cryptographic protocol aimed at securing communications over a computer network but does not directly transfer files. The combination of using SSH for secure authentication and encryption makes SCP the preferred choice for securely transferring files, affirming its role as the correct answer in the context of secure file transfer protocols.

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!