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

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 kind of information is an employee's bank details classified as?

A. Confidential

B. Personal

C. Classified

D. Public

2. A system compromised via an attacker monitoring Wi-Fi traffic is known as what?

A. A man-in-the-middle attack

B. An evil twin attack

C. A phishing attack

D. A denial of service attack

3. Which of the following protocols employs asymmetric key algorithms?

A. Hypertext Transfer Protocol (HTTP)

B. File Transfer Protocol (FTP)

C. Secure Shell (SSH), Pretty Good Privacy (PGP), Secure Sockets Layer (SSL)

D. Simple Mail Transfer Protocol (SMTP)

4. Can a natural disaster cause a system failure that impacts data availability?

A. Yes

B. No

C. Only if related to power failure

D. It depends on the data center location

5. What cloud-based technology allows users to access application software and databases through their browser?

A. Infrastructure as a Service (IaaS)

B. Software as a Service (SaaS)

C. Platform as a Service (PaaS)

D. Database as a Service (DBaaS)

6. An employee divulging sensitive information to someone impersonating their manager is an example of which type of incident?

A. External

B. Internal

C. Social Engineering

D. Technical Breach

7. What could have caused the modification of customer information in transit, given no equipment failure was noted?

A. Manual error

B. Malicious code

C. Hardware malfunction

D. Network congestion

8. What type of authentication enables a user's account information to be used by third-party services such as Facebook or Google?

A. Kerberos

B. OpenID

C. OAuth

D. LDAP

9. What kind of error occurs when a biometric access system falsely accepts an unauthorized user?

A. Type I

B. Type II

C. Type III

D. Type IV

10. Which type of firewall is designed to protect web applications from various types of attacks?

A. Stateful firewall

B. Next-generation firewall (NGFW)

C. Web application firewall (WAF)

D. Stateless firewall

Answers

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

Explanations

1. What kind of information is an employee's bank details classified as?

A. Confidential

B. Personal

C. Classified

D. Public

An employee's bank details are classified as personal information. Personal information refers to any data that can be used to identify an individual and is specific to them, such as their name, address, contact information, and financial details. In the context of information security and data privacy, personal information is sensitive and needs to be handled with care to protect an individual's privacy. The classification as personal implies that this information is not meant to be shared or accessed by unauthorized individuals. It is protected under various privacy regulations, which stress the importance of safeguarding such information to prevent identity theft, fraud, and other malicious activities. Hence, personal data like bank details falls under strict protection measures. Other classifications, such as confidential, imply a broader category that can include sensitive business information, while classified typically pertains to government or national security information. Public information is readily available and does not carry the same level of sensitivity. Therefore, recognizing bank details specifically as personal reinforces the importance of privacy and security in handling sensitive information about individuals.

2. A system compromised via an attacker monitoring Wi-Fi traffic is known as what?

A. A man-in-the-middle attack

B. An evil twin attack

C. A phishing attack

D. A denial of service attack

In this context, the term that best describes a system compromised through an attacker monitoring Wi-Fi traffic is an evil twin attack. This type of attack occurs when a malicious actor sets up a rogue Wi-Fi access point that mimics a legitimate one, tricking users into connecting to it. Once connected, the attacker can intercept sensitive data and monitor the users' online activities, effectively capturing traffic that would otherwise be protected. The evil twin attack exploits the inherent trust users have in familiar Wi-Fi networks, allowing the attacker to access information such as usernames, passwords, and other sensitive data. This makes it particularly dangerous in public spaces where individuals commonly seek out Wi-Fi connections. While a man-in-the-middle attack is related and involves intercepting communication between two parties, it doesn't specifically denote the scenario where the attacker creates a deceptive Wi-Fi access point. Phishing attacks typically involve tricking users into providing personal information via deceptive emails or fake websites rather than monitoring network traffic on a compromised Wi-Fi network. Denial of service attacks focus on overwhelming a network or service to make it unavailable to its intended users, which is not aligned with monitoring or intercepting Wi-Fi traffic. Thus, the evil twin attack is the most accurate term for the scenario described.

3. Which of the following protocols employs asymmetric key algorithms?

A. Hypertext Transfer Protocol (HTTP)

B. File Transfer Protocol (FTP)

C. Secure Shell (SSH), Pretty Good Privacy (PGP), Secure Sockets Layer (SSL)

D. Simple Mail Transfer Protocol (SMTP)

The reason this answer is correct lies in the nature of the protocols listed in this option, which employ asymmetric key algorithms as part of their security mechanisms. Secure Shell (SSH) uses asymmetric encryption primarily for authenticating clients and servers, allowing secure remote logins over unsecured networks. Pretty Good Privacy (PGP) is a data encryption and decryption program that provides cryptographic privacy and authentication for data communication, utilizing asymmetric key algorithms for securely sharing keys. Secure Sockets Layer (SSL) also incorporates asymmetric encryption to establish a secure connection between clients and servers, initially exchanging a session key that will be used for symmetric encryption during the actual data transfer. The other protocols listed do not utilize asymmetric key algorithms in the same way. Hypertext Transfer Protocol (HTTP) is a foundational web protocol that does not incorporate any security features inherently; it transmits data in plaintext. File Transfer Protocol (FTP) is another protocol used for transferring files but does not provide encryption or authentication through asymmetric keys inherently, although secure variants like FTPS exist. Simple Mail Transfer Protocol (SMTP) is primarily designed for sending emails and, similar to HTTP, does not implement asymmetric encryption as part of its standard operations. Thus, option C is validated as the correct answer as it

4. Can a natural disaster cause a system failure that impacts data availability?

A. Yes

B. No

C. Only if related to power failure

D. It depends on the data center location

A natural disaster can indeed cause a system failure that impacts data availability. Natural disasters such as floods, earthquakes, hurricanes, and wildfires can damage physical infrastructure, including data centers, servers, and network equipment. When such an event occurs, it may disrupt operations and lead to loss of access to critical data, thereby affecting the availability of services reliant on that data. While the response may vary depending on factors such as the resilience of the infrastructure and the geographic location of the data center, the fundamental risk posed by natural disasters is significant. They can have widespread and unpredictable effects, leading to extended outages and potential data loss if proper disaster recovery and business continuity planning are not in place. Hence, affirming that a natural disaster can cause system failures impacting data availability is accurate and underscores the importance of implementing appropriate risk management strategies in cybersecurity.

5. What cloud-based technology allows users to access application software and databases through their browser?

A. Infrastructure as a Service (IaaS)

B. Software as a Service (SaaS)

C. Platform as a Service (PaaS)

D. Database as a Service (DBaaS)

The correct choice is Software as a Service (SaaS) because it specifically refers to a cloud computing model that delivers software applications over the internet. Users can access these applications through a web browser without needing to install software on their local devices, which provides convenience and flexibility. SaaS examples include applications like Google Workspace, Salesforce, and Microsoft 365, where the software is hosted in the cloud and available to users seamlessly via their browsers. This model eliminates the need for managing hardware or software installations for end-users, centralizes management, and often provides automatic updates and scalability. While Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) provide essential cloud resources and frameworks for building and deploying applications, they do not directly deliver application software to users in the manner SaaS does. Likewise, Database as a Service (DBaaS) focuses specifically on delivering database management services over the cloud, rather than comprehensive software applications. Thus, SaaS stands out as the correct answer for providing browser-based access to application software and databases.

6. An employee divulging sensitive information to someone impersonating their manager is an example of which type of incident?

A. External

B. Internal

C. Social Engineering

D. Technical Breach

When an employee reveals sensitive information to someone impersonating their manager, it exemplifies a social engineering incident. Social engineering refers to the manipulative tactics used by attackers to deceive individuals into divulging confidential information or performing actions that compromise security. In this scenario, the impersonator has exploited trust and authority, one of the key principles in social engineering, to trick the employee into revealing information. This incident is characterized by the human element of security rather than a breach resulting from technical vulnerabilities or external attacks, clearly indicating that it falls under the category of social engineering. The other classifications, such as external, internal, and technical breach, describe different scenarios that do not fit this particular incident. External incidents typically involve outside attackers trying to breach a system, internal incidents refer to breaches that originate from within the organization, and technical breaches involve hacking or exploiting vulnerabilities in systems or software. In this case, the element of deception and manipulation points specifically towards social engineering as the defining feature of the incident.

7. What could have caused the modification of customer information in transit, given no equipment failure was noted?

A. Manual error

B. Malicious code

C. Hardware malfunction

D. Network congestion

The modification of customer information in transit, without any noted equipment failure, can be attributed to the presence of malicious code. This could be a form of software that is intentionally designed to alter data as it is being transmitted over the network. Malicious code may come from various sources such as a compromised endpoint within the network, phishing attacks that result in malware installation, or even from vulnerabilities in the software used for data transmission. In this context, malicious code can manipulate data packets or intercept and modify the information being transferred, leading to unauthorized changes in customer data. This reinforces the importance of comprehensive security measures and monitoring systems to detect and prevent such malicious activities, ensuring the integrity and confidentiality of sensitive information in transit. Although manual errors can also lead to modification, they typically pertain to human actions rather than external threats, and equipment failure is ruled out in this scenario as a method of data alteration. Hardware malfunctions typically result in loss or corruption of data rather than deliberate modification, and network congestion does not typically allow for changes in data content; it might cause delays or packet loss without altering the actual information being transmitted.

8. What type of authentication enables a user's account information to be used by third-party services such as Facebook or Google?

A. Kerberos

B. OpenID

C. OAuth

D. LDAP

OAuth is the correct choice because it is an open standard for access delegation that allows third-party services to use a user's account information without sharing the user's password. When a user opts to log in to a service using their Facebook or Google account, OAuth facilitates this process. It provides a secure token to the third-party service, enabling it to access the user's account information (such as name and email) with permission, while the user maintains control over their credentials. This mechanism helps enhance user experience by allowing users to authenticate with a familiar service rather than creating new accounts for each application. OAuth focuses on authorization, meaning it allows the third party limited access to the user's information as per the terms defined during the authentication process, rather than full access to the user's account. In contrast, other authentication methods like Kerberos are primarily designed for network authentication, requiring both server and client to prove their identity securely within a trusted network. OpenID was an earlier standard for decentralized authentication but has largely been superseded by OAuth, which addresses more extensive use cases and security requirements. LDAP, or Lightweight Directory Access Protocol, is used for directory services and doesn't offer the same type of federated authentication capabilities that OAuth provides.

9. What kind of error occurs when a biometric access system falsely accepts an unauthorized user?

A. Type I

B. Type II

C. Type III

D. Type IV

A biometric access system that falsely accepts an unauthorized user is experiencing a Type II error. In the context of biometric systems, a Type II error, also known as a false acceptance or false positive, occurs when the system incorrectly identifies an unauthorized individual as an authorized user. This type of error undermines the security of the system, as it could allow someone without legitimate access to gain entry to secure areas or information. Biometric systems strive to minimize this risk, as a high false acceptance rate can lead to significant vulnerabilities. Type I errors, in contrast, involve a false rejection of an authorized user, meaning legitimate users are incorrectly denied access. Understanding the distinction between these errors is critical for designing and implementing effective biometric security measures. Recognizing Type II errors is essential for improving system accuracy and enhancing overall security.

10. Which type of firewall is designed to protect web applications from various types of attacks?

A. Stateful firewall

B. Next-generation firewall (NGFW)

C. Web application firewall (WAF)

D. Stateless firewall

A Web Application Firewall (WAF) is specifically designed to protect web applications from a variety of attacks, such as cross-site scripting (XSS), SQL injection, and other vulnerabilities that can be exploited via HTTP/HTTPS traffic. Unlike traditional firewalls that primarily focus on filtering and controlling network traffic based on predetermined rules, a WAF operates at the application layer and can analyze the content of the web traffic to identify and block malicious requests targeted at web applications. WAFs employ various techniques to safeguard web applications, including inspecting incoming requests, enforcing security policies, and being able to differentiate between legitimate user behavior and potentially harmful actions. This makes them an essential component in a comprehensive security strategy for any organization that utilizes web applications, particularly in the face of increasing cyber threats. The other options, while serving important functions in network security, do not specifically address the needs of web applications in the same manner a WAF does. Stateful and stateless firewalls primarily focus on the transport layer and manage traffic flow based on established connections or static rules. Next-generation firewalls (NGFW) offer additional features such as intrusion prevention and application awareness, but they do not provide the specialized layer of protection that a WAF uniquely offers for web applications.

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!