CompTIA CySA+ 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 does threat modeling involve?

A. Identifying potential threats and response strategies

B. Developing incident response plans

C. Conducting vulnerability assessments

D. Implementing security controls

2. What is the primary objective of the Cybersecurity Analyst (CySA+) certification?

A. To validate the knowledge and skills necessary to detect and respond to cybersecurity threats

B. To prepare individuals for the CompTIA Security+ exam

C. To teach programming languages for cybersecurity professionals

D. To focus on physical security measures only

3. Which tool would you use to analyze network packets?

A. Firewall

B. Packet sniffer

C. Proxy server

D. Intrusion detection system

4. Which of the following is considered a proactive security measure?

A. Incident response planning

B. Running antivirus scans

C. Vulnerability scanning and remediation

D. Monitoring user activity

5. During a security assessment, what does the SIFT toolkit specialize in?

A. Incident detection with real-time alerts

B. Open-source incident response and forensic analysis

C. Automated vulnerability scanning

D. Data encryption techniques

6. What is the purpose of access controls in an organization?

A. To enable collaboration between all staff

B. To restrict access to sensitive information and systems

C. To improve system performance and speed

D. To collect performance metrics for employees

7. Which cipher suite should NOT be used with OpenSSL?

A. DES

B. AES

C. RSA

D. ECC

8. Which scenario would most likely trigger an incident involving a Cross-site Request Forgery (CSRF) attack?

A. A user clicks on a malicious link while logged into an account

B. Legitimate user credentials are stolen through phishing

C. A web application is exploited due to unpatched flaws

D. A server receives overwhelming traffic from botnets

9. To prevent sensitive information from being disclosed by your web server, which configuration should you change?

A. Set "VerifyNormalization" to 1

B. Set "RemoveServerHeader" to 1

C. Set "EnableLogging" to 1

D. Set "PerProcessLogging" to 1

10. Which regulatory standard focuses on protecting patient health information?

A. GDPR (General Data Protection Regulation)

B. PCI DSS (Payment Card Industry Data Security Standard)

C. HIPAA (Health Insurance Portability and Accountability Act)

D. SOX (Sarbanes-Oxley Act)

Answers

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

Explanations

1. What does threat modeling involve?

A. Identifying potential threats and response strategies

B. Developing incident response plans

C. Conducting vulnerability assessments

D. Implementing security controls

Threat modeling is a proactive approach that focuses on identifying potential threats to a system, application, or organization, and analyzing those threats to develop effective response strategies. This process involves understanding the assets that need protection, the potential adversaries, their possible attack vectors, and the impacts of different types of attacks. By identifying and categorizing these threats, organizations can prioritize their security efforts and allocate resources more effectively to mitigate risks. This approach serves as a foundational practice for enhancing overall security posture, as it allows teams to anticipate potential security issues and implement strategies accordingly. The outcome of threat modeling not only helps in recognizing what needs protection but also guides the development of security controls and response plans in the future. This distinguishes it from the other options, which focus on specific activities that, while important, are not central to the concept of threat modeling itself.

2. What is the primary objective of the Cybersecurity Analyst (CySA+) certification?

A. To validate the knowledge and skills necessary to detect and respond to cybersecurity threats

B. To prepare individuals for the CompTIA Security+ exam

C. To teach programming languages for cybersecurity professionals

D. To focus on physical security measures only

The primary objective of the Cybersecurity Analyst (CySA+) certification is to validate the knowledge and skills necessary to detect and respond to cybersecurity threats. This certification emphasizes a proactive approach to identifying vulnerabilities, mitigating risks, and understanding the intricacies of behavioral analytics, allowing cybersecurity analysts to effectively monitor and respond to security incidents. By covering a range of topics, including threat detection techniques and incident response strategies, CySA+ ensures that certified professionals can actively contribute to their organizations' cybersecurity posture, making them essential assets in a landscape where cyber threats are increasingly sophisticated. This role is critical in identifying and responding to threats swiftly, gaining insights through continuous monitoring, and employing various security tools and methodologies to protect information assets. The focus of this certification on active threat detection and response is what distinguishes it from foundational courses or those strictly concentrated on physical security or programming aspects in cybersecurity.

3. Which tool would you use to analyze network packets?

A. Firewall

B. Packet sniffer

C. Proxy server

D. Intrusion detection system

Using a packet sniffer is the most effective approach for analyzing network packets. A packet sniffer, also known as a network analyzer or protocol analyzer, allows the capture and inspection of data packets traveling over a network. This tool provides detailed insights into the contents of each packet, including headers and payload data, which can be critical for troubleshooting network issues, monitoring network performance, and analyzing security threats. Packet sniffers can capture a broad range of network traffic, enabling security professionals to detect anomalies, track data flows, and identify unauthorized access attempts. By visualizing the packet data, analysts gain the ability to perform deep dives into network behaviors and identify any potential vulnerabilities or misuse. While firewalls, proxy servers, and intrusion detection systems play important roles in network security and management, they are not primarily designed for packet analysis. Firewalls control incoming and outgoing network traffic based on predetermined security rules, while proxy servers act as intermediaries for requests from clients seeking resources from other servers. Intrusion detection systems focus on identifying suspicious patterns or activities in network traffic but do not provide the same level of detailed packet analysis as a packet sniffer.

4. Which of the following is considered a proactive security measure?

A. Incident response planning

B. Running antivirus scans

C. Vulnerability scanning and remediation

D. Monitoring user activity

The correct choice recognizes vulnerability scanning and remediation as a proactive security measure. This process involves actively searching for potential vulnerabilities in systems before they can be exploited by attackers. By identifying and addressing these weaknesses, organizations can significantly reduce their risk exposure. This proactive approach ensures that security gaps are closed, updates are applied, and proper configurations are enforced, which helps maintain a stronger security posture. In contrast, incident response planning is more about preparing for security incidents after they occur, making it a reactive measure. Running antivirus scans typically aims to detect existing threats rather than prevent them, placing it in a more reactive context, although it can have some proactive elements. Monitoring user activity is generally about observing what users are doing in real time, which is also a reactive measure since it's often used to detect and respond to suspicious activities after they happen.

5. During a security assessment, what does the SIFT toolkit specialize in?

A. Incident detection with real-time alerts

B. Open-source incident response and forensic analysis

C. Automated vulnerability scanning

D. Data encryption techniques

The SIFT toolkit specializes in open-source incident response and forensic analysis, making it a powerful resource for security professionals dealing with digital forensics and incident response tasks. SIFT, which stands for SANS Investigative Forensic Toolkit, provides a comprehensive suite of tools that allow analysts to gather and analyze digital evidence from various sources, including disk images, memory dumps, and network logs. The toolkit includes numerous utilities designed to help examine filesystem structures, recover deleted files, and perform memory analysis, thus facilitating detailed investigations into potential security breaches. By leveraging open-source tools, SIFT also provides flexibility and adaptability for analysts to customize their workflows and adapt their strategies to fit different scenarios. While incident detection with real-time alerts, automated vulnerability scanning, and data encryption techniques are all vital components of a comprehensive cybersecurity strategy, they are not the specific focus of the SIFT toolkit. Thus, the specialization of SIFT in incident response and forensic analysis underlines its importance in examining incidents after they occur, helping organizations understand the nature and extent of security events.

6. What is the purpose of access controls in an organization?

A. To enable collaboration between all staff

B. To restrict access to sensitive information and systems

C. To improve system performance and speed

D. To collect performance metrics for employees

Access controls are fundamental mechanisms in an organization aimed at safeguarding sensitive information and critical systems. Their primary purpose is to ensure that only authorized personnel can access specific data, applications, and resources. This is particularly important in protecting sensitive information from unauthorized use, leakage, or alterations, which could lead to data breaches or compliance violations. By implementing access controls, organizations can enforce policies that clearly define who may view or use specific resources, thereby maintaining the confidentiality, integrity, and availability of their information assets. While collaboration and improved performance are valuable aspects of workplace functionality, they are not the primary focus of access controls. Access controls prioritize security and data governance, which are critical in maintaining trust and operational resilience within an organization. Collecting performance metrics is also unrelated to the core purpose of access controls, which is inherently centered on security rather than productivity or performance monitoring.

7. Which cipher suite should NOT be used with OpenSSL?

A. DES

B. AES

C. RSA

D. ECC

The recommendation against using DES (Data Encryption Standard) with OpenSSL stems from its known vulnerabilities and inadequate key length. DES utilizes a fixed key size of 56 bits, which has been deemed insufficient to withstand modern computational power and cryptanalysis techniques. The security landscape has evolved, and DES is now considered obsolete, with significant weaknesses that make it susceptible to brute-force attacks. In contrast, AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman), along with ECC (Elliptic Curve Cryptography), are strong and widely accepted algorithms in cryptographic practices. AES uses variable key lengths (128, 192, or 256 bits), providing robust security. RSA is a widely used public-key cryptographic method, and ECC offers the same level of security as RSA but with shorter key lengths, making it more efficient. Since the contemporary standards prioritize security and efficiency, the use of DES is discouraged in modern cryptographic implementations, especially when alternatives like AES, RSA, and ECC provide much more robust protection.

8. Which scenario would most likely trigger an incident involving a Cross-site Request Forgery (CSRF) attack?

A. A user clicks on a malicious link while logged into an account

B. Legitimate user credentials are stolen through phishing

C. A web application is exploited due to unpatched flaws

D. A server receives overwhelming traffic from botnets

An incident involving a Cross-site Request Forgery (CSRF) attack is most likely triggered when a user clicks on a malicious link while logged into an account. CSRF attacks exploit the trust that a web application has in the user's browser. When the user is already authenticated, clicking on a malicious link can cause the browser to send a request to the web application on behalf of the user, potentially executing unwanted actions without their consent. This type of attack relies on the fact that the authenticated session is still active, allowing malicious requests to be processed as if they came from the legitimate user. In this scenario, the attacker's link takes advantage of the logged-in state to perform actions like changing account settings or making transactions, all without the user's awareness. The other scenarios do not specifically pertain to CSRF. For instance, stealing legitimate user credentials through phishing is typically related to credential theft and would more likely lead to unauthorized access rather than a CSRF attack. Exploiting vulnerabilities in a web application due to unpatched flaws pertains to different types of attacks such as SQL injection or cross-site scripting (XSS). Lastly, overwhelming server traffic from botnets is more indicative of a denial-of-service (DoS) attack and does not involve the user's

9. To prevent sensitive information from being disclosed by your web server, which configuration should you change?

A. Set "VerifyNormalization" to 1

B. Set "RemoveServerHeader" to 1

C. Set "EnableLogging" to 1

D. Set "PerProcessLogging" to 1

Configuring the web server to set "RemoveServerHeader" to 1 is an essential step in enhancing security by preventing the disclosure of sensitive information. The server header typically contains details about the web server software and version in use, which can provide attackers with valuable information for exploiting vulnerabilities specific to that software. By removing this header, you limit the information available to potential attackers, thus reducing the risk of targeted attacks against your web server. Enhancing your server's security by hiding such details is a proactive measure, as it helps to obscure the server's identity and reduces the potential attack surface. While the other configurations can be relevant in a broader security context, such as logging capabilities, they do not directly prevent sensitive information disclosure in the same way that removing the server header does.

10. Which regulatory standard focuses on protecting patient health information?

A. GDPR (General Data Protection Regulation)

B. PCI DSS (Payment Card Industry Data Security Standard)

C. HIPAA (Health Insurance Portability and Accountability Act)

D. SOX (Sarbanes-Oxley Act)

The Health Insurance Portability and Accountability Act (HIPAA) is the regulatory standard that specifically focuses on protecting patient health information. Enacted in the United States in 1996, HIPAA establishes national standards for the protection of health information, ensuring that patients' medical records and personal health information are properly secured and kept confidential. The regulations apply to healthcare providers, health plans, and healthcare clearinghouses that handle protected health information (PHI). HIPAA's Privacy Rule gives patients rights over their health information, including the right to access their records and request corrections. The Security Rule complements the Privacy Rule by setting national standards for the protection of electronic PHI (ePHI) through administrative, physical, and technical safeguards. In the context of the other regulations mentioned: GDPR focuses on data protection and privacy for individuals within the European Union, PCI DSS addresses security standards for payment card transactions, and SOX pertains to corporate governance and financial practices in publicly traded companies. None of these directly targets the protection of patient health information, highlighting why HIPAA is the appropriate choice for this question.

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://comptia-cysaplus.examzify.com

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