Certified Information Systems Security Professional (CISSP) Practice Exam (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. **Which type of network architecture features a DMZ to enhance security?**
   - A. Screened subnet architecture
   - B. Mesh architecture
   - C. Non-screened architecture
   - D. Single firewall architecture

2. **What is the purpose of an Account Lockout feature?**
   - A. To prevent unauthorized users from creating accounts
   - B. To disable an account after a set number of failed logins
   - C. To ensure all accounts are actively monitored
   - D. To allow users to reset their own passwords

3. **How does TACACS function in relation to remote users?**
   - A. It provides central access control mainly for remote users
   - B. It restricts access entirely for remote users
   - C. It guarantees unlimited access for remote users
   - D. It allows users to bypass authentication when off-site

4. **What is the concept of split horizon in networking?**
   - A. A method to maximize bandwidth
   - B. A way to reduce routing loops
   - C. A strategy for data encryption
   - D. A technique to prioritize network traffic

5. **What is the definition of a vulnerability in cybersecurity?**
   - A. The presence of extensive security measures against attacks
   - B. The absence or weakness of a safeguard that could be exploited
   - C. Any flaw in a code that can be addressed by updates
   - D. An instance of unauthorized access to a system

6. **What is a Back Door in terms of cybersecurity?**
   - A. An authorized point of access to a system
   - B. An undocumented method for accessing a system
   - C. A way to bypass normal security protocols
   - D. An automatic system recovery feature

7. Which of the following protocols combines PPTP and L2F?

A. PPP

B. L2TP

C. CHAP

D. LEAP

8. What does separation of duties help to minimize in an organization?

A. Data redundancy

B. Operational inefficiency

C. Risk of fraud and errors

D. Employee turnover

9. What type of network typically encompasses only a very small area?

A. Wide Area Network (WAN)

B. Metropolitan Area Network (MAN)

C. Local Area Network (LAN)

D. Personal Area Network (PAN)

10. What is the purpose of the Internet Control Message Protocol (ICMP)?

A. Data compression for faster transmission

B. Control and manage network traffic

C. Send error messages and operational information

D. Encrypt network data

Answers

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

Explanations

1. Which type of network architecture features a DMZ to enhance security?

A. Screened subnet architecture

B. Mesh architecture

C. Non-screened architecture

D. Single firewall architecture

The screened subnet architecture incorporates a DMZ (Demilitarized Zone) to enhance security by providing an additional layer between the internal network and external threats. In this setup, the DMZ acts as a buffer zone that hosts externally facing services, such as web servers, email servers, or FTP servers. This arrangement allows external users to access certain resources while keeping the internal network secure. By segmenting the network in this manner, even if an attacker compromises a service in the DMZ, they are still blocked from directly accessing the internal network where sensitive data and critical systems reside. The architecture typically employs multiple firewalls or security devices: one firewall controls incoming traffic from the Internet to the DMZ, and a second firewall manages traffic between the DMZ and the internal network. This dual-layer approach strengthens the security posture of the organization by limiting the pathways available for potential attacks. In contrast, the other network architectures mentioned do not inherently use a DMZ, which underscores why the screened subnet architecture is particularly suited for enhancing security through this specific design.

2. What is the purpose of an Account Lockout feature?

A. To prevent unauthorized users from creating accounts

B. To disable an account after a set number of failed logins

C. To ensure all accounts are actively monitored

D. To allow users to reset their own passwords

The purpose of an Account Lockout feature is to disable an account after a set number of failed login attempts. This mechanism is crucial for enhancing security, as it helps to thwart unauthorized access attempts, often associated with brute-force attacks where an attacker tries to gain access by guessing passwords. By locking the account after a predefined threshold of incorrect entries, it mitigates the risk that an unauthorized user could successfully compromise the account through persistence. This feature not only protects sensitive information and resources but also serves as an alert mechanism for administrators about potential attack patterns, allowing them to respond appropriately. Furthermore, it promotes the use of secure passwords by encouraging users to be more discerning about their credential entry. Other options, while relevant to account management and security, do not align with the primary function of the Account Lockout feature. For instance, preventing unauthorized users from creating accounts pertains more to account provisioning strategies rather than post-login security measures. The monitoring of active accounts falls under user auditing practices rather than direct prevention techniques. Lastly, allowing users to reset their own passwords is essential for user support but does not address the security aspect that the Account Lockout feature is specifically designed to combat.

3. How does TACACS function in relation to remote users?

A. It provides central access control mainly for remote users

B. It restricts access entirely for remote users

C. It guarantees unlimited access for remote users

D. It allows users to bypass authentication when off-site

TACACS, which stands for Terminal Access Controller Access-Control System, functions as an authentication protocol that provides centralized access control, particularly for remote users. It is designed to manage access to network resources by allowing organizations to authenticate, authorize, and account for users attempting to connect from remote locations. This centralized approach means that instead of user credentials being managed locally on each device or server, they are stored and maintained in a central database or server. This enhances security and management efficiency by ensuring that all users, including remote ones, must authenticate against the same set of credentials. In this context, remote users can access network services, provided they authenticate successfully according to the policies established by the organization using TACACS. Such functionality is critical for organizations that need to enforce security policies and ensure that only authorized individuals can access sensitive systems or data from outside the corporate network. The other options present scenarios that misrepresent TACACS's functionality. TACACS does not restrict remote users entirely, nor does it guarantee unlimited access — that would contradict the purpose of access control. Additionally, TACACS requires authentication, so allowing users to bypass it when off-site would undermine the security model it provides. Thus, the central access control that TACACS offers is crucial for managing the security

4. What is the concept of split horizon in networking?

A. A method to maximize bandwidth

B. A way to reduce routing loops

C. A strategy for data encryption

D. A technique to prioritize network traffic

The concept of split horizon is primarily related to routing in network communications, especially within distance-vector routing protocols. It is designed to prevent routing loops, which can occur when routers continuously update each other with routes that have not been validated. By using the split horizon technique, a router does not advertise paths back out of the interface from which they were learned. This means that if a router learns about a route from a neighbor on a specific interface, it will not send updates about that route back to that same neighbor. This approach effectively reduces the possibility of incorrect routing information being propagated and creating loops, which can lead to significant delays and costly inefficiencies in data transmission. In environments utilizing protocols like RIP (Routing Information Protocol), split horizon is crucial in maintaining stable network operations, improving the overall reliability of network communication. The other options address different networking concepts that do not correlate with the intention of split horizon. Maximizing bandwidth, strategies for data encryption, and traffic prioritization involve entirely different methodologies and principles in the realm of networking.

5. What is the definition of a vulnerability in cybersecurity?

A. The presence of extensive security measures against attacks

B. The absence or weakness of a safeguard that could be exploited

C. Any flaw in a code that can be addressed by updates

D. An instance of unauthorized access to a system

A vulnerability in cybersecurity refers to a specific weakness or absence of a safeguard that could be exploited by attackers to gain unauthorized access to or perform unauthorized actions on a system. This definition highlights the essential nature of vulnerabilities as points of risk where an attacker can potentially exploit flaws or deficiencies in security mechanisms, leading to various forms of cyber threats. While the other options mention aspects related to security, they do not accurately capture what constitutes a vulnerability. For instance, having extensive security measures does not create vulnerabilities; rather, it typically aims to mitigate them. Flaws in code can be a type of vulnerability but are not exhaustive enough to define all vulnerabilities, as they can also exist in processes, configurations, or physical security. Unauthorized access is a consequence of a vulnerability being exploited rather than a definition of the vulnerability itself. Thus, the correct answer encapsulates the specific concept of a vulnerability accurately within the context of cybersecurity.

6. What is a Back Door in terms of cybersecurity?

A. An authorized point of access to a system

B. An undocumented method for accessing a system

C. A way to bypass normal security protocols

D. An automatic system recovery feature

In the context of cybersecurity, a backdoor refers to an undocumented method for accessing a system. This means that it is a way for someone, typically a developer or an attacker, to gain unauthorized access without going through the standard authentication processes or security measures that are typically in place. Backdoors can be intentionally created by developers for legitimate purposes, such as troubleshooting or system administration, but they pose a significant security risk if they are discovered and exploited by malicious actors. The presence of a backdoor undermines the integrity of a system since it allows access without proper oversight or controls. The other options do not accurately capture the essence of what a backdoor is. An authorized point of access would imply that it is well-documented and intended for legitimate use, contradicting the very nature of a backdoor. Bypassing normal security protocols might happen through a backdoor, but stating that a backdoor is merely a means to bypass these protocols does not encompass the full definition or the risk associated with it. Lastly, an automatic system recovery feature is unrelated to unauthorized access; rather, it pertains to system resilience and recovery processes.

7. Which of the following protocols combines PPTP and L2F?

A. PPP

B. L2TP

C. CHAP

D. LEAP

The correct answer is L2TP, which stands for Layer 2 Tunneling Protocol. L2TP is a tunneling protocol used to support virtual private networks (VPNs) and is notable for combining the features of two earlier protocols: Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Forwarding (L2F). PPTP provides a way to encapsulate Point-to-Point Protocol (PPP) packets, allowing for the secure transmission of data over the Internet. L2F, on the other hand, was developed by Cisco as a way to provide similar capabilities for PPP connections but with an emphasis on layer 2 tunneling for various protocols. By combining these elements, L2TP inherits the ability to tunnel multiple protocols and enhances the security and delivery of PPP packets. The other options do not fulfill this requirement. PPP is a data link layer protocol used for point-to-point connections, but it does not involve tunneling by itself. CHAP (Challenge Handshake Authentication Protocol) is an authentication scheme used within the PPP framework, not a tunneling protocol. LEAP (Lightweight EAP) is an authentication protocol used in wireless local area networks, which is unrelated to tunneling

8. What does separation of duties help to minimize in an organization?

A. Data redundancy

B. Operational inefficiency

C. Risk of fraud and errors

D. Employee turnover

Separation of duties is a fundamental principle in security and internal controls that helps to minimize the risk of fraud and errors within an organization. By dividing responsibilities among different individuals or teams, the organization ensures that no single person has complete control over any critical process or transaction. This structure not only serves as a deterrent against fraudulent activities, as it requires collusion between multiple parties to carry out illicit actions, but it also reduces the chance of unintentional errors that can occur when one person is responsible for all aspects of a task. Implementing separation of duties requires a careful analysis of workflows and processes to identify areas where responsibilities can be split effectively – for instance, in financial transactions where one employee initiates a transaction, another approves it, and a third handles the reconciliation. This layered control creates checks and balances that enhance overall security and accountability within the organization, thereby minimizing the propensity for both fraud and mistakes. The other options, while relevant to organizational management, do not directly relate to the protective mechanisms established by separation of duties. Data redundancy deals with the unnecessary duplication of data, operational inefficiency pertains to wasted resources or time in processes, and employee turnover revolves around staff retention rather than security controls.

9. What type of network typically encompasses only a very small area?

A. Wide Area Network (WAN)

B. Metropolitan Area Network (MAN)

C. Local Area Network (LAN)

D. Personal Area Network (PAN)

The type of network that typically encompasses only a very small area is known as a Personal Area Network (PAN). A PAN is designed for personal use and usually connects devices that are in close proximity to an individual, typically within a range of about 10 meters. This could include connections between devices like smartphones, tablets, laptops, and other electronics using technologies such as Bluetooth or Wi-Fi. In contrast, a Local Area Network (LAN) covers a larger area, typically within a single building or campus, allowing multiple devices to connect and communicate over a limited geographical space. A Metropolitan Area Network (MAN) serves a larger geographic area than a LAN but is still smaller than a Wide Area Network (WAN), which can span across cities, countries, or even continents, connecting multiple LANs over great distances. Given these distinctions, the PAN is specifically designed for personal device connectivity in a confined space, making it the correct choice for the question regarding networks limited to a very small area.

10. What is the purpose of the Internet Control Message Protocol (ICMP)?

A. Data compression for faster transmission

B. Control and manage network traffic

C. Send error messages and operational information

D. Encrypt network data

The Internet Control Message Protocol (ICMP) serves a crucial role in network communications by primarily providing a mechanism to send error messages and operational information regarding network issues. When devices on a network encounter problems, such as an unreachable host or a lack of resources to forward packets, ICMP facilitates the delivery of these important notifications. This allows network administrators and devices to diagnose and respond to network conditions effectively, enhancing overall network reliability and troubleshooting. While other options may suggest functions relevant to network management or performance, they do not accurately represent the core purpose of ICMP. For instance, data compression is not a function of ICMP; it focuses on transmission efficiency rather than error handling. Similarly, while ICMP can be involved in managing network traffic indirectly through error reporting, its primary function remains centered on communication about errors and operational status rather than direct traffic control. Lastly, ICMP does not provide data encryption, as it is not designed for securing data but rather for conveying messages about the status of communications on the network.

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://cissp.examzify.com

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