University of Central Florida (UCF) CIS3360 Security in Computing Final 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. Don't worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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. Along with IP, which protocol is considered one of the original protocols of the Internet?

A. UDP

B. ICMP

C. TCP

D. HTTP

2. What can TCP distinguish between on the same host?

A. Multiple servers

B. Concurrent applications

C. Data packets

D. Network protocols

3. What is a key characteristic of TCP in terms of connection?

A. It is loss-sensitive.

B. It is stateless.

C. It is connection-oriented.

D. It is bandwidth-reduced.

4. What does patch management refer to in cybersecurity?

A. The process of tracking network traffic and incidents

B. The process of managing and mastering cyber threats

C. The process of managing and installing updates to software

D. The process of monitoring employee usage of company devices

5. What is the "time-based" approach to security?

A. A method of enhancing physical security

B. A strategy focusing on reducing the time of an attacker's opportunity

C. A practice for time management in security systems

D. A technique for improving employee response time

6. Which of the following is NOT part of a strong password policy?

- **A. Use of complex passwords**
- **B. Regular password changes**
- **C. Sharing passwords with coworkers**
- **D. Prohibition of common passwords**

7. Which type of malware spreads without injecting into a host program and usually does not require human interaction?

- **A. Computer virus**
- **B. Ransomware**
- **C. Computer worm**
- **D. Trojan horse**

8. Under which act do copyright holders have the right to reproduce and create derivative works?

- **A. Copyright Act of 1976**
- **B. Copyright Act of 1951**
- **C. Digital Millennium Copyright Act**
- **D. Intellectual Property Act**

9. Which language is typically used for querying databases?

- **A. Data Manipulation Language (DML)**
- **B. Structured Query Language (SQL)**
- **C. Hypertext Markup Language (HTML)**
- **D. JavaScript**

10. What is the purpose of monitoring network traffic?

- **A. To increase data transfer speed**
- **B. To ensure all devices are connected properly**
- **C. To identify and analyze potential security threats**
- **D. To manage user login times**

Answers

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

Explanations

1. Along with IP, which protocol is considered one of the original protocols of the Internet?

A. UDP

B. ICMP

C. TCP

D. HTTP

The correct answer is TCP. TCP, or Transmission Control Protocol, is one of the foundational protocols of the Internet protocol suite, alongside IP (Internet Protocol). Together, they provide a reliable communication mechanism over the internet. TCP is responsible for ensuring that data packets are delivered accurately and in the correct order between devices on a network. It establishes a connection-oriented session between the sender and receiver, enabling features such as error checking, data recovery, and flow control. This reliability is crucial for applications that require certainty that data has been successfully transmitted, such as file transfers and web page loading. While other protocols, such as UDP (User Datagram Protocol) and ICMP (Internet Control Message Protocol), serve specific functions within the network, they do not provide the same level of reliability and connection-oriented service as TCP. UDP is used for applications where speed is more important than reliability, while ICMP is utilized for diagnostic and control purposes in networking. HTTP (Hypertext Transfer Protocol) operates on top of TCP and is used primarily for transferring web pages but is not one of the original protocols of the Internet in the same foundational sense as TCP or IP. This makes TCP a pivotal protocol in the functioning of the Internet, establishing it as one of the original and essential

2. What can TCP distinguish between on the same host?

A. Multiple servers

B. Concurrent applications

C. Data packets

D. Network protocols

TCP (Transmission Control Protocol) uses the combination of IP addresses and port numbers to distinguish between different applications running on the same host. Each application typically listens on a unique port number, and by using this port distinction, TCP can maintain multiple simultaneous connections to different services or applications. When a packet arrives at a host, TCP examines the port number associated with that incoming data to determine which application should receive it. This means that even if there are multiple applications or services running on the same machine, TCP can efficiently direct incoming packets to the correct destination based on the specific port numbers. This ability to manage and separate traffic for concurrent applications is a critical feature that ensures diverse communication channels can operate independently without interference, maximizing the utility of the networked environment.

3. What is a key characteristic of TCP in terms of connection?

A. It is loss-sensitive.

B. It is stateless.

C. It is connection-oriented.

D. It is bandwidth-reduced.

A key characteristic of TCP (Transmission Control Protocol) is that it is connection-oriented. This means that a connection must be established between the two communicating devices before data can be transmitted. TCP uses a three-way handshake process to set up a connection, where initial synchronization between the sender and receiver takes place, ensuring that both parties are ready to communicate, and that they can agree on parameters for the session. Being connection-oriented provides several benefits, including reliable communication through the use of acknowledgment packets that confirm receipt of data, as well as the ability to manage flow control and congestion control. This ensures that the data is delivered in the order it was sent and without loss, providing a more reliable transmission compared to connectionless protocols like UDP (User Datagram Protocol), which sends data without establishing a connection first.

4. What does patch management refer to in cybersecurity?

A. The process of tracking network traffic and incidents

B. The process of managing and mastering cyber threats

C. The process of managing and installing updates to software

D. The process of monitoring employee usage of company devices

Patch management in cybersecurity pertains to the process of managing and installing updates to software. This includes the identification, acquisition, installation, and verification of software patches that address vulnerabilities or bugs in applications and operating systems. By applying patches, organizations can protect themselves against security exploits and ensure that their systems function properly. Regular patch management is vital to maintaining a secure computing environment, as unpatched software can be exploited by attackers to gain unauthorized access or cause harm to the system. The importance of patch management is underscored during incidents where vulnerabilities are discovered, often leading to recommendations from software vendors or security advisories to apply patches promptly. This proactive approach not only mitigates security risks but also enhances system performance and longevity. Other options mentioned do not accurately capture the essence of patch management. Tracking network traffic and incidents focuses on monitoring and analyzing data flows within a network, while managing cyber threats encompasses broader strategies such as risk assessment and incident response. Monitoring employee usage of company devices relates to behavioral analysis and policy enforcement, which is distinct from the technical aspect of keeping software updated.

5. What is the "time-based" approach to security?

A. A method of enhancing physical security

B. A strategy focusing on reducing the time of an attacker's opportunity

C. A practice for time management in security systems

D. A technique for improving employee response time

The "time-based" approach to security primarily focuses on reducing the time frame during which an attacker can exploit vulnerabilities or access sensitive information. This strategy emphasizes the importance of minimizing the time from the moment an attack begins until it is detected and mitigated, thereby reducing the potential damage that can occur during that window. The core idea is that by significantly shortening the time period an attacker has to act, organizations can improve their overall security posture. This could involve implementing faster detection mechanisms, incident response procedures, and employing strategies like proactive monitoring and threat intelligence to anticipate and thwart attacks before they can escalate. This approach can lead to the formulation of various security policies and technologies that enhance an organization's resilience against attacks by ensuring that appropriate measures are swiftly put in place in response to identified threats. By controlling the time an attacker has access to a system, the severity and impact of security breaches can be significantly decreased, which encourages a more robust security framework.

6. Which of the following is NOT part of a strong password policy?

A. Use of complex passwords

B. Regular password changes

C. Sharing passwords with coworkers

D. Prohibition of common passwords

A strong password policy is essential for maintaining security and protecting sensitive information. The option that suggests sharing passwords with coworkers directly contradicts the fundamental principles of a strong password policy. Sharing passwords poses significant risks, as it undermines the individual accountability and control over access that a strong password policy aims to establish. When multiple people use the same password, it becomes difficult to trace the source of any security breach, and the overall security of the system is compromised. Additionally, if a shared password falls into the wrong hands, the consequences can be far-reaching, potentially affecting the integrity of sensitive data. The other options—using complex passwords, requiring regular password changes, and prohibiting common passwords—are all integral components of a strong password policy. Complex passwords ensure enhanced security by making it harder for unauthorized users to guess them. Regularly changing passwords minimizes the risk of long-term exposure from leaked or compromised passwords. Prohibiting common passwords helps to protect against attacks that use popular or easily guessed passwords, which are frequently exploited by attackers. Thus, the focus of a strong password policy should always prioritize individual password secrecy and the methods to secure access properly, making the sharing of passwords completely inappropriate in such a framework.

7. Which type of malware spreads without injecting into a host program and usually does not require human interaction?

A. Computer virus

B. Ransomware

C. Computer worm

D. Trojan horse

The correct answer is that the computer worm is a type of malware that spreads independently and typically does not require human interaction to propagate. Unlike other forms of malware such as viruses, which need to attach themselves to a host file in order to spread, worms are standalone programs that exploit vulnerabilities in networks or systems to replicate themselves. This ability allows them to move across networks without direct user engagement, relying on flaws or security holes in operating systems or applications to proliferate. In contrast, a computer virus requires a host file to attach itself to and cannot spread on its own. Ransomware typically demands action from users, such as payment, to unlock files, and it often utilizes other methods to spread rather than self-replicating. Trojan horses disguise themselves as legitimate software but cannot self-replicate like worms; they require users to unknowingly execute them to initiate their malicious activity. Therefore, the characteristic nature of worms distinguishes them as the type of malware that spreads without needing a host program and usually operates without human involvement.

8. Under which act do copyright holders have the right to reproduce and create derivative works?

A. Copyright Act of 1976

B. Copyright Act of 1951

C. Digital Millennium Copyright Act

D. Intellectual Property Act

The correct choice is the Copyright Act of 1976. This act significantly expanded the rights of copyright holders and established the legal framework for copyright in the United States. Under this act, copyright holders are granted exclusive rights to reproduce their works and to create derivative works based on their original creations. This means they can control how their works are used, adapted, or altered, thereby ensuring that they receive recognition and financial benefits from their intellectual property. The Copyright Act of 1976 established that copyright protection covers both published and unpublished works and provides a lengthy term of protection, ensuring that creators have a substantial period during which they can monetize their work. Other acts, such as the Copyright Act of 1951, primarily established foundational copyright principles but did not offer the exhaustive rights introduced in 1976. The Digital Millennium Copyright Act focuses on issues surrounding digital infringement and online content, while the Intellectual Property Act is a broader term that does not specifically pertain to copyright law in the same way as the 1976 act.

9. Which language is typically used for querying databases?

A. Data Manipulation Language (DML)

B. Structured Query Language (SQL)

C. Hypertext Markup Language (HTML)

D. JavaScript

Structured Query Language (SQL) is the standard programming language specifically designed for managing and manipulating relational databases. It allows users to perform various operations such as querying data, updating records, inserting new data, and deleting existing records. SQL provides a set of commands that facilitate these tasks in a structured manner, making it easier to interact with the database and retrieve the information required for various applications. While Data Manipulation Language (DML) is a subset of SQL that focuses on data manipulation, it does not encompass the full range of features and functionalities that SQL offers. Hypertext Markup Language (HTML) is primarily used for creating and structuring content on the web, not for querying databases. JavaScript, although frequently used for enhancing interactivity on web pages, is not specifically tailored for database queries. Hence, SQL is recognized as the appropriate and dedicated language for querying databases, making it the correct choice for this question.

10. What is the purpose of monitoring network traffic?

A. To increase data transfer speed

B. To ensure all devices are connected properly

C. To identify and analyze potential security threats

D. To manage user login times

Monitoring network traffic serves a critical function in identifying and analyzing potential security threats, making it essential for maintaining the integrity and security of a computing environment. By examining the data packets that traverse the network, security professionals can detect unusual patterns or activities that may indicate malicious behavior, such as unauthorized access attempts, data exfiltration, or the presence of malware. This proactive approach enables organizations to respond promptly to threats, implement necessary countermeasures, and strengthen their overall cybersecurity posture. In contrast, while increasing data transfer speed, ensuring proper device connections, or managing user login times may improve network performance, efficiency, or user experience, they do not directly relate to the primary purpose of monitoring network traffic for security purposes. Monitoring is fundamentally about safeguarding the network from potential risks rather than simply enhancing operational metrics.

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://ucf-cis3360-final.examzify.com

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