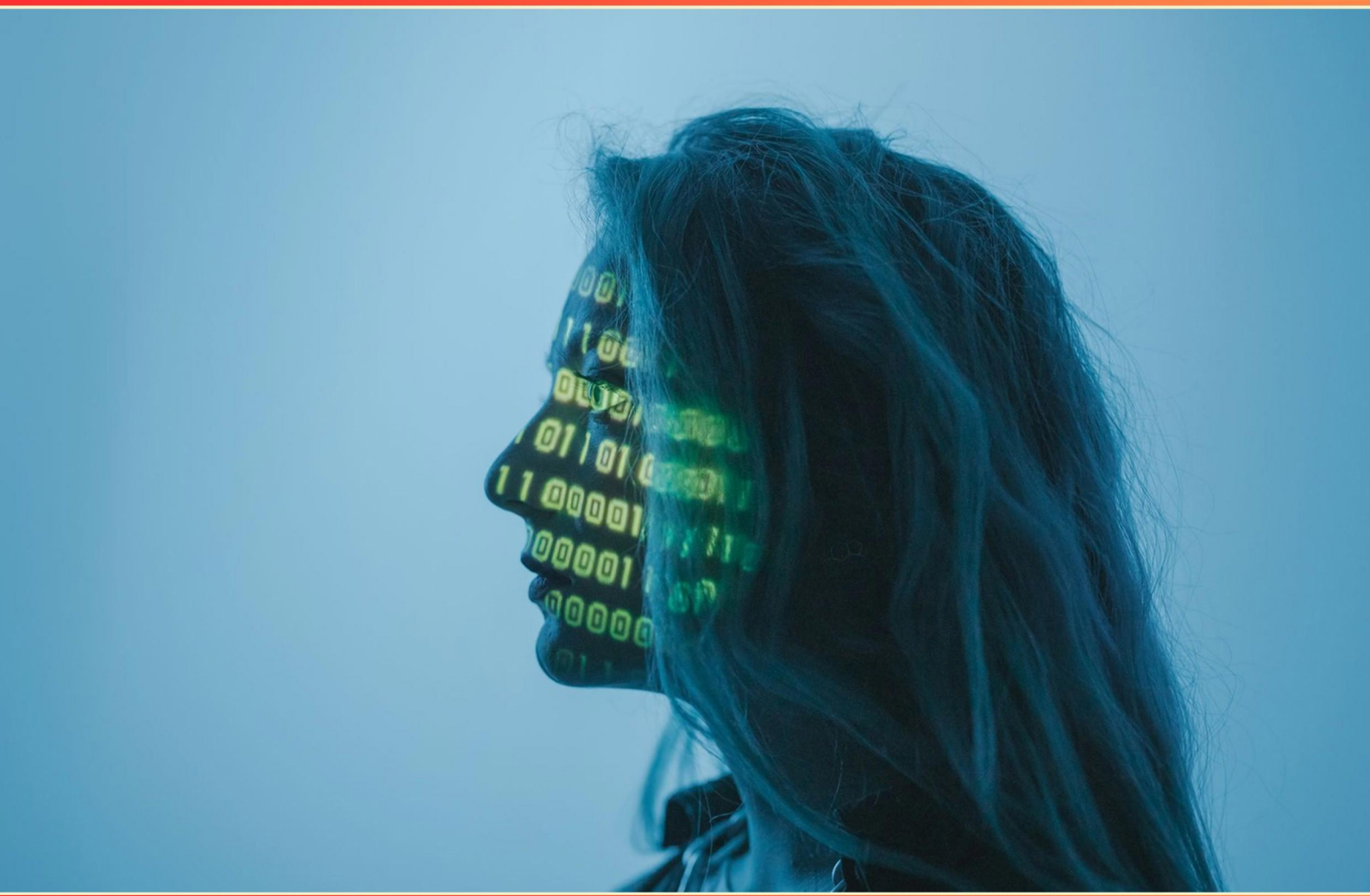
UNIVERSITY OF CENTRAL FLORIDA (UCF) CIS3360 SECURITY IN COMPUTING FINAL PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

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

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 is the purpose of a strong password policy?

A. To enforce regular software updates

B. To enhance security against unauthorized access

C. To streamline user access management

D. To provide easy recovery options

2. What do databases produce based on queries from users?

A. Documents

B. Reports

C. Graphs

D. Charts

3. What is the typical duration of a patent?

A. 10 years

B. 15 years

C. 20 years

D. 25 years

4. What is the first step to spoof an SSID?

A. Set Up a VPN

B. Use a Firewall

C. Place a Rogue AP in a Public Location

D. Install Antivirus Software

5. Session hijacking can be easily facilitated by which of the following?

A. Strong Encryption

B. Public Key Infrastructure

C. Impersonating an Access Point

D. Multi-Factor Authentication

6. What is a potential outcome of effective penetration testing?

A. Increased network speed

B. Identification of security gaps before exploitation

C. Reduction of employee turnover

D. Improved software redundancy

7. What type of packet does the server send in response to a client's connection request?

A. ACK packet

B. SYN/ACK packet

C. Connection packet

D. Data packet

8. What is paid to a patent holder for lost profits due to infringement?

A. Compensation funds

B. Legal compensation

C. License fees

D. Royalty payments

9. What is a firewall, and how does it function?

A. A device that protects against malware

B. A network security device that monitors and controls traffic

C. A tool for backing up data securely

D. A system for tracking user behavior

10. What role does a firewall play in network security?

A. It encrypts all data sent over the network

B. It monitors traffic and blocks unauthorized access

C. It stores backup copies of network data

D. It manages user access and permissions on a network

Answers

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

Explanations

1. What is the purpose of a strong password policy?

A. To enforce regular software updates

B. To enhance security against unauthorized access

C. To streamline user access management

D. To provide easy recovery options

A strong password policy is primarily designed to enhance security against unauthorized access. This is crucial because passwords serve as the first line of defense protecting sensitive information and systems. By establishing guidelines that dictate the complexity, length, and overall strength of passwords, organizations can significantly reduce the risk of unauthorized individuals gaining access to their systems. The implementation of such a policy encourages users to create unique and difficult-to-guess passwords, which are less susceptible to common attacks, such as brute force or dictionary attacks. Moreover, it often includes recommendations for regular password changes and the use of multifactor authentication, which further strengthen security. While other options may touch on related security measures or administrative benefits, the core purpose of a strong password policy is directly linked to the protection it provides against unauthorized access, making it a crucial element of a comprehensive security strategy.

2. What do databases produce based on queries from users?

A. Documents

B. Reports

C. Graphs

D. Charts

Databases primarily produce reports based on user queries because reports are formatted outputs that summarize and organize data in a way that is useful for decision-making and analysis. When users query a database, they are often looking to extract specific data points or a collection of related data that provides insights or information. Reports can be tailored to include various types of data representations such as tables, lists, and specific sections of detailed information that allow users to draw conclusions or understand trends. This makes reports a common and crucial output of database systems, as they facilitate communication of the underlying data. While documents, graphs, and charts can be generated from database queries, they are generally considered additional forms of representation rather than the primary product of direct database query output. Charts and graphs are often used within reports to visualize the data, but the foundational output that summarizes the queried data is the report itself.

3. What is the typical duration of a patent?

A. 10 years

B. 15 years

C. 20 years

D. 25 years

The typical duration of a patent is generally 20 years from the date of filing. This timeframe is established to provide inventors with a significant period during which they can exclusively exploit their inventions, allowing them to recover the costs of development and potentially earn a profit. After this period, the patent expires, and the protected invention enters the public domain, making it available for others to use or develop further without infringement concerns. This structure is designed to balance the interests of inventors and the public, encouraging innovation while eventually allowing society to benefit from new inventions. In specific scenarios, such as design patents or plants, the duration can vary slightly, but the standard for utility patents is indeed 20 years.

4. What is the first step to spoof an SSID?

A. Set Up a VPN

B. Use a Firewall

C. Place a Rogue AP in a Public Location

D. Install Antivirus Software

The first step to spoof an SSID involves placing a rogue access point (AP) in a public location. This strategy enables an attacker to create a fake wireless network that mimics a legitimate one, enticing users to connect to it under the assumption that they are accessing a trusted network. By doing this, the attacker can capture sensitive information, such as authentication credentials or other data transmitted over the network. The other options do not directly contribute to spoofing an SSID. Setting up a VPN, for instance, is primarily a security measure to protect data in transit, but it does not involve creating or manipulating wireless networks. Using a firewall helps to monitor and control incoming and outgoing network traffic based on predetermined security rules, but it does not facilitate SSID spoofing. Similarly, installing antivirus software focuses on protecting a device from malware but does not relate to the direct process of spoofing an SSID. Thus, placing a rogue AP is the most relevant action for achieving the goal of SSID spoofing.

5. Session hijacking can be easily facilitated by which of the following?

A. Strong Encryption

B. Public Key Infrastructure

C. Impersonating an Access Point

D. Multi-Factor Authentication

Session hijacking typically involves an attacker gaining unauthorized access to a user's active session by exploiting vulnerabilities in the network or the user's device. One common method for facilitating session hijacking is through the impersonation of an access point. When an attacker sets up a rogue access point that appears to be a legitimate network, unsuspecting users may connect to it, believing they are accessing a trusted network. This rogue access point can be used to intercept traffic, including session cookies and other sensitive information. By capturing this data, an attacker can effectively take over an existing session that a user is engaged in, thus gaining unauthorized access to the user's account and sensitive data. In contrast, strong encryption, public key infrastructure, and multi-factor authentication are all security measures designed to protect data and user sessions. Strong encryption secures data in transit, making it difficult for attackers to read intercepted messages. Public key infrastructure involves encrypting data in a way that requires keys to access, thereby adding a layer of protection against unauthorized access. Multi-factor authentication increases the security of the authentication process by requiring multiple forms of verification, making it significantly harder for an attacker to successfully hijack a session even if they have partial information. Each of these other options contributes to enhancing security, rather than facilitating

6. What is a potential outcome of effective penetration testing?

A. Increased network speed

B. Identification of security gaps before exploitation

C. Reduction of employee turnover

D. Improved software redundancy

Effective penetration testing serves as a proactive security measure designed to identify vulnerabilities and security gaps within a system or network before they can be exploited by malicious actors. By simulating attacks, penetration testers can uncover weaknesses related to security configurations, outdated software, and potential entry points for attackers. This process allows organizations to address and remediate these vulnerabilities, thereby strengthening their overall security posture and preventing breaches that could lead to data loss or financial damage. While increased network speed, reduction of employee turnover, and improved software redundancy might be beneficial aspects of an organization's operation, they are not direct outcomes derived from the effective implementation of penetration testing. The primary purpose of this testing is to enhance security by identifying and addressing gaps, making the identification of security gaps before exploitation the most relevant and significant outcome in this context.

7. What type of packet does the server send in response to a client's connection request?

A. ACK packet

B. SYN/ACK packet

C. Connection packet

D. Data packet

When a client initiates a connection request to a server in the context of the Transmission Control Protocol (TCP), the server's response is a SYN/ACK packet. This is part of the three-way handshake process that establishes a TCP connection. Initially, the client sends a SYN packet to indicate a desire to establish a connection. Upon receiving this SYN packet, the server responds not only to acknowledge the receipt of the SYN but also to indicate that it is ready to establish a connection. Therefore, it sends a SYN/ACK packet, combining both the synchronization (SYN) to request a connection and acknowledgment (ACK) to confirm the receipt of the client's request. The SYN/ACK packet signifies that the server is actively participating in the connection establishment process and is prepared to communicate further. Following this, the client will send an ACK packet back to the server to complete the handshake, resulting in a fully established connection. The other types of packets listed are not relevant in this context: an ACK packet is simply an acknowledgment of received data but does not initiate a connection; a connection packet is not a formally defined packet type in the TCP/IP suite; and a data packet pertains to the actual data transfer after the connection has been established, not the initial handshake process

8. What is paid to a patent holder for lost profits due to infringement?

A. Compensation funds

B. Legal compensation

C. License fees

D. Royalty payments

The compensation paid to a patent holder for lost profits due to infringement is known as legal compensation. This refers specifically to the financial restitution that a patent holder seeks in a legal context when they can demonstrate that their profits have been adversely affected by another party's unauthorized use of their patented invention. Such legal compensation can include not only the lost profits that the patent holder would have made had the infringement not occurred but also any additional damages that the court deems appropriate. This concept is important in intellectual property law, as it provides a means for patent holders to seek justice and recovery for economic harm caused by infringement. While license fees and royalty payments may involve compensation for use of a patent, these terms are generally associated with authorized agreements where the patent holder is willingly allowing use of their invention in exchange for payment. Legal compensation, in this instance, specifically addresses the harm and losses that arise from infringement actions without permission.

9. What is a firewall, and how does it function?

A. A device that protects against malware

B. A network security device that monitors and controls traffic

C. A tool for backing up data securely

D. A system for tracking user behavior

A firewall is fundamentally a network security device designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. It serves as a barrier between a trusted internal network and untrusted external networks, such as the Internet. By analyzing the data packets that attempt to enter or leave the network, it can allow or block traffic based on established security protocols. The primary function of a firewall is to prevent unauthorized access while allowing legitimate communication. It can configure various rules to specify what type of traffic to permit or deny. This helps protect against threats such as unauthorized access attempts, intrusion attempts, and other malicious activities that could compromise network security. The other options do not accurately capture the core function of a firewall. While malware protection (mentioned in the first option) is important, it is not the primary role of a firewall but rather falls under the function of antivirus software. The choice regarding data backup refers to a different aspect of data security entirely and does not pertain to the monitoring of network traffic. Lastly, tracking user behavior is typically handled by different tools focused on analytics or monitoring rather than core network security devices.

10. What role does a firewall play in network security?

A. It encrypts all data sent over the network

B. It monitors traffic and blocks unauthorized access

C. It stores backup copies of network data

D. It manages user access and permissions on a network

A firewall is a crucial component of network security that functions primarily to monitor and control incoming and outgoing network traffic based on predetermined security rules. By inspecting the data packets that are transmitted across a network, a firewall has the capability to block unauthorized access attempts, ensuring that malicious traffic does not infiltrate a system while allowing legitimate traffic to pass through. This monitoring and blocking mechanism can be applied at various levels, including the network layer or application layer, depending on the type of firewall being used. Firewalls can be hardware-based, software-based, or a combination of both, and they are essential in creating a barrier between a trusted internal network and untrusted external networks, such as the internet. The other options describe functions that are generally not associated with firewalls. For example, encrypting data, storing backups, or managing user access and permissions involve different specific security measures and tools within an overall cybersecurity strategy. Each of these functions is important, but they do not align with the fundamental role of a firewall in protecting network integrity and preventing unauthorized access.

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!