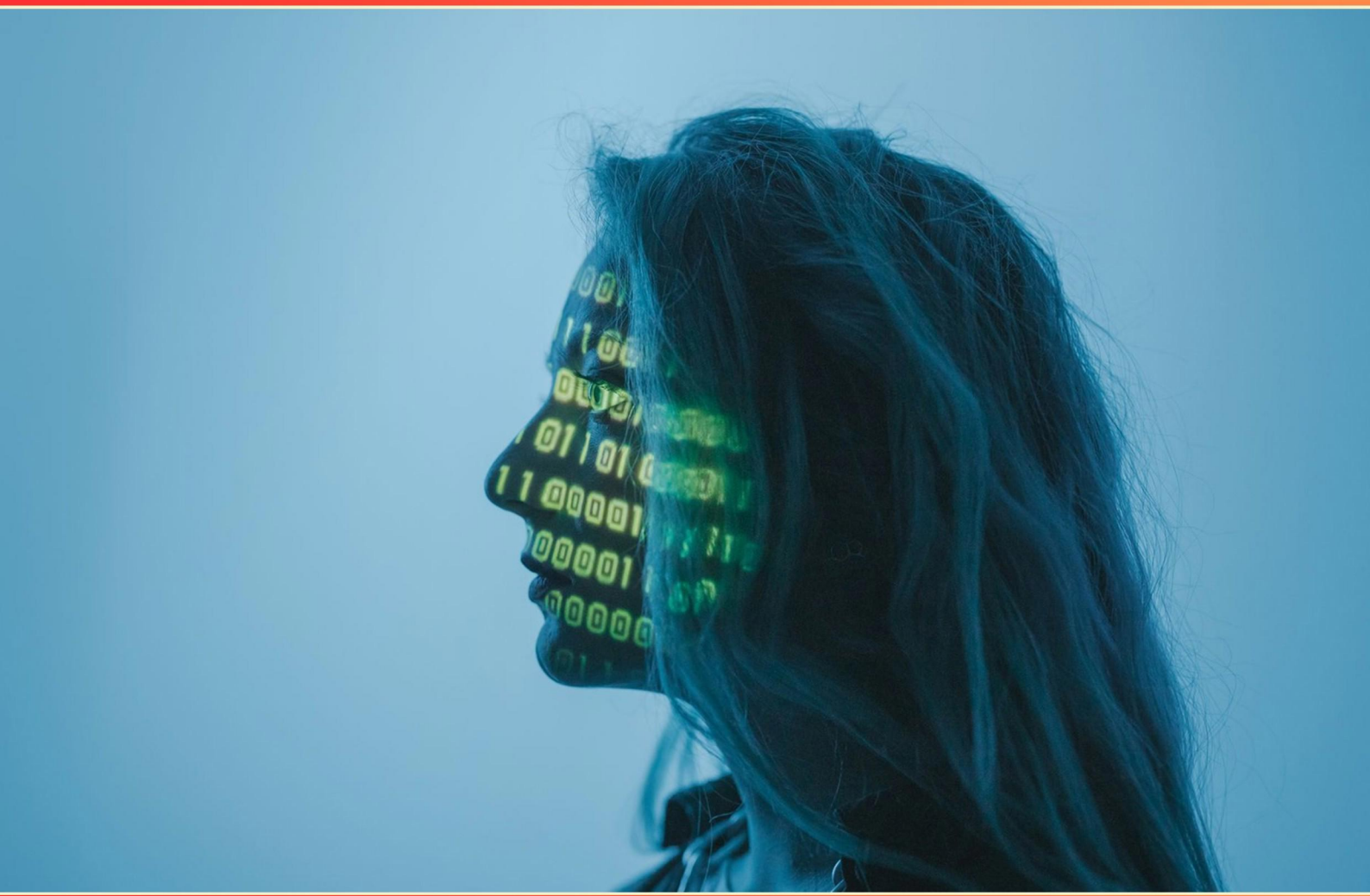
UNIVERSITY OF CENTRAL FLORIDA (UCF) CIS3360 SECURITY IN COMPUTING FINAL PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

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

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

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

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. What is the primary goal of a cyber attacker?

A. To increase internet speed for users
B. To gather intelligence on network performance
C. To steal information or disrupt services
D. To enhance the security of a network

2. 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

3. What does the term "data breach" refer to?

A. A successful cyber attack on personal devices
B. An incident where unauthorized access to data occurs
C. A loss of data due to hardware failure
D. A type of malware that steals information

4. UDP is classified as what type of protocol?

A. Transport layer protocol
B. Application layer protocol
C. Network layer protocol
D. Session layer protocol

5. The main purpose of TTL in networking is to:

A. Ensure delivery of packets
B. Establish connection parameters
C. Limit the number of routing hops
D. Enhance packet security

6. Which method can best protect against an insider threat?

A. Regular external audits
B. Comprehensive employee monitoring
C. Strong access controls and user permissions
D. Daily security updates

SAMPLE

7. Both source and destination processes in TCP are identified by what?

A. Ports

B. Protocols

C. Addressing schemes

D. Connection types

8. What does the Copyright Act of 1976 primarily address?

A. Patent duration

B. Copyright protection and rights

C. Trademark regulations

D. Trade secret laws

9. 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

10. What kind of packets does NAT manage in the network?

A. Only TCP packets

B. Only UDP packets

C. Both TCP and UDP packets

D. None of the above

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the primary goal of a cyber attacker?

A. To increase internet speed for users

B. To gather intelligence on network performance

C. To steal information or disrupt services

D. To enhance the security of a network

The primary goal of a cyber attacker is to steal information or disrupt services. This encompasses a range of malicious activities that aim to exploit vulnerabilities within systems, networks, or applications. By stealing sensitive data—such as personal information, financial records, or intellectual property—attackers can either use it for personal gain or sell it on the dark web. Disrupting services, on the other hand, can lead to significant operational downtime, affecting businesses and individuals alike. This can manifest in various forms, including denial-of-service attacks or ransomware, which not only jeopardize data integrity but also can have long-lasting financial repercussions for organizations. In contrast, enhancing security, increasing internet speed, or gathering intelligence on network performance do not align with the motives typical of cyber attackers, who operate with the intent of harming individuals or organizations for profit, notoriety, or other malicious outcomes. Understanding these motivations is critical in developing robust cybersecurity strategies and improving defenses against such threats.

2. 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.

SAMPLE

3. What does the term "data breach" refer to?

A. A successful cyber attack on personal devices

B. An incident where unauthorized access to data occurs

C. A loss of data due to hardware failure

D. A type of malware that steals information

The term "data breach" specifically refers to an incident where unauthorized access to data occurs. This can happen when sensitive, protected, or confidential information is accessed or disclosed without proper authorization, which may involve hackers exploiting security vulnerabilities or employees accessing data they are not permitted to view. Understanding this definition is crucial, as data breaches can have significant implications for individuals and organizations, often leading to identity theft, financial loss, and damage to reputation. This delineation also emphasizes the difference between unauthorized access and other events such as hardware failure or malware infections, which involve different contexts and consequences. Consequently, the focus on unauthorized access within the definition of a data breach is what distinguishes it from the other options provided, highlighting its core aspect of unauthorized interaction with sensitive data.

4. UDP is classified as what type of protocol?

A. Transport layer protocol

B. Application layer protocol

C. Network layer protocol

D. Session layer protocol

UDP, or User Datagram Protocol, is classified as a transport layer protocol. It operates at the transport layer of the OSI model, which is responsible for end-to-end communication and data transfer between hosts. UDP is primarily used for applications that require fast, efficient transmission of data, where the overhead of establishing a connection (as required by TCP) is not necessary. As a transport layer protocol, UDP provides a means for applications to send messages without the complexities of connection setup and management, enabling low-latency communication. It allows data to be sent in discrete chunks called datagrams and does not guarantee delivery, order, or error correction, making it suitable for applications like video streaming, online gaming, and voice over IP, where speed is prioritized over reliability. Other options refer to different layers of the OSI model: the application layer deals with end-user interactions and services, the network layer is focused on routing packets between networks, and the session layer manages sessions of communication between applications. Therefore, they do not apply to the characteristics and functions of UDP.

5. The main purpose of TTL in networking is to:

A. Ensure delivery of packets

B. Establish connection parameters

C. Limit the number of routing hops

D. Enhance packet security

The main purpose of Time to Live (TTL) in networking is to limit the number of routing hops that a packet can take within a network. Each time a packet is forwarded by a router, its TTL value is decreased by one. When the TTL reaches zero, the packet is discarded and not forwarded any further. This mechanism helps prevent packets from circulating indefinitely in the network due to routing errors or loops, thus managing network traffic and resources efficiently. By enforcing a limit on how long a packet can exist in the network, TTL plays a critical role in maintaining network stability and performance. The other choices refer to different aspects of networking; for example, ensuring delivery of packets is more a function of the transport layer protocols like TCP. Establishing connection parameters pertains to how connections are set up, often handled by the transport layer as well. Enhancing packet security involves encryption and authentication processes rather than TTL, which is purely a routing efficiency mechanism.

SAMPLE

6. Which method can best protect against an insider threat?

A. Regular external audits

B. Comprehensive employee monitoring

C. Strong access controls and user permissions

D. Daily security updates

Strong access controls and user permissions are essential for protecting against insider threats because they limit the ability of employees to access sensitive data that is not necessary for their roles. By implementing a principle of least privilege, organizations ensure that each employee has only the minimum level of access required to perform their job functions. This helps mitigate the risk that an insider, whether malicious or simply negligent, can exploit their access to sensitive information. Furthermore, strong access controls can include measures such as authentication requirements, regular reviews of permissions, and segregation of duties. These practices deter potential insider threats by making unauthorized access more difficult and less tempting. Additionally, maintaining an audit trail of access requests and actions taken can help in detecting and responding to any suspicious behavior by insiders. This layered approach strengthens the overall security posture of the organization against risks that stem from within.

7. Both source and destination processes in TCP are identified by what?

A. Ports

B. Protocols

C. Addressing schemes

D. Connection types

The correct answer is that both source and destination processes in TCP are identified by ports. In the context of the Transmission Control Protocol (TCP), a port number is used to distinguish different processes or services running on the same device. Each application that communicates over the network does so using a unique combination of an IP address and a port number, often referred to as a socket. When a TCP connection is established, the source process (the application sending the data) specifies a source port, and the destination process (the application receiving the data) specifies a destination port. This architecture allows multiple applications to run on the same server without interfering with each other, and it facilitates proper routing of data packets to the correct application. The other options do not accurately describe how TCP identifies processes. Protocols refer to the set of rules governing the transmission of data, addressing schemes pertain to how devices are uniquely identified on the network (such as IP addresses), and connection types generally refer to the state of a connection rather than specifying the processes involved. Thus, ports are the specific identifiers that enable the differentiation of processes in the TCP communication model.

SAMPLE

8. What does the Copyright Act of 1976 primarily address?

A. Patent duration

B. Copyright protection and rights

C. Trademark regulations

D. Trade secret laws

The Copyright Act of 1976 is primarily focused on establishing the legal framework for copyright protection and rights in the United States. This Act aims to promote the progress of science and useful arts by granting authors and creators exclusive rights to their works for a limited time. It covers a wide range of creative expressions, including literary, musical, and artistic works, and defines the scope of copyright protection, the rights that copyright holders possess, and the limitations on these rights, such as fair use. By setting these guidelines, the act helps to balance the interests of creators in controlling their work and the public's interest in accessing and using creative content. This makes it crucial for anyone involved in the creation, distribution, or consumption of artistic and intellectual works to understand the implications of copyright law as outlined in the 1976 Act. The other options address different areas of intellectual property law: patent duration pertains to inventions, trademark regulations deal with brand identifiers, and trade secret laws focus on protecting confidential business information. Thus, they are not relevant contenders for the primary focus of the Copyright Act of 1976.

9. 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.

SAMPLE

10. What kind of packets does NAT manage in the network?

A. Only TCP packets

B. Only UDP packets

C. Both TCP and UDP packets

D. None of the above

NAT, or Network Address Translation, is a method used in networking that allows multiple devices on a private network to share a single public-facing IP address. It operates at the network layer and is capable of managing both TCP and UDP packets, which are the primary protocols used for data transmission over the Internet. TCP (Transmission Control Protocol) is a connection-oriented protocol that ensures reliable data transmission, while UDP (User Datagram Protocol) is a connectionless protocol that is faster but does not guarantee delivery. NAT must be able to handle both types of packets because it translates the private IP addresses of devices within a local network to a public IP address and vice versa, regardless of whether the traffic is using TCP or UDP. This ability allows devices in a private network to connect to external networks and ensures seamless communication regardless of the protocol being used. Since NAT functions at a level that encompasses both of these transport layer protocols, it efficiently manages the packets from each, thereby enabling the necessary connectivity and communication for applications that use either TCP or UDP.

SAMPLE

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!

SAMPLE