PLTW CYBERSECURITY EOC PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://pltwcybersecurityeoc.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 does the grep command do?

A. Search for strings in a file

B. Display the contents of a file

C. Terminate processes running in the system

D. Show the current user ID

2. What is the primary use of the nslookup tool?

A. To find security vulnerabilities

B. To resolve DNS queries

C. To configure network adapters

D. To monitor bandwidth usage

3. What does social engineering refer to?

A. A manipulation technique used to trick individuals into divulging confidential information

B. A method of programming computers to optimize performance

C. A strategy for building secure software

D. A process for updating security protocols

4. What does cryptography encompass?

A. The study of digital currencies

B. The science and art of secure message delivery

C. The analysis of network systems

D. The process of logging data

5. Which command provides information about running processes that include other user's activities?

A. bg

B. ps -ef

C. kill

D. su

SAMPLE

6. Which form of encryption utilizes two distinct keys?

A. Symmetric key encryption
B. Private key encryption
C. Public key encryption
D. Substitution cyphers

7. What are the three steps of a TCP handshake?

A. SYN, SYN-ACK, ACK
B. REQUEST, RESPONSE, CONFIRMATION
C. CONNECT, VERIFY, ESTABLISH
D. ACK, SYN-ACK, SYN-DELETE

8. What does the keyword SEC specify when searching for files?

A. Finds SEC in any file name in any folder
B. Finds any file type
C. Finds files modified on a specific date
D. Finds files associated with the government

9. What does a digital footprint represent?

A. The internal storage of a device
B. The trail of data left by users on the internet
C. The design of a web application
D. The encryption of data in transit

10. What does risk assessment involve?

A. Updating software regularly
B. Identifying and evaluating potential risks
C. Logging all network activity
D. Implementing new technologies

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What does the grep command do?

A. Search for strings in a file

B. Display the contents of a file

C. Terminate processes running in the system

D. Show the current user ID

The grep command is a powerful and widely used utility in Unix/Linux systems that searches for specific strings or patterns within files. When you run grep, you specify the string you want to search for and the file or files you want to search through. The command then scans the content of those files and prints lines that contain the specified string. This functionality makes grep an essential tool for programmers and system administrators who need to quickly locate text within large amounts of data or log files. Its versatility extends to using regular expressions, which allows for complex search patterns, enhancing the effectiveness of text searching in scripts and command-line operations. Given its primary purpose of searching for strings, this makes it the correct answer to the question regarding the functionality of the grep command.

2. What is the primary use of the nslookup tool?

A. To find security vulnerabilities

B. To resolve DNS queries

C. To configure network adapters

D. To monitor bandwidth usage

The primary use of the nslookup tool is to resolve DNS queries. This command-line utility is employed by network professionals to check the Domain Name System (DNS) to gather information about domain names and their associated IP addresses. When a user queries a domain name, nslookup communicates with DNS servers to translate the human-readable domain into its numerical IP address, which allows for proper routing of internet traffic. Using nslookup can help diagnose DNS-related issues, such as confirming whether a domain is properly registered and resolving, checking the expiration of DNS records, or troubleshooting problems related to website accessibility. By facilitating the lookup of these records, nslookup serves as an essential tool in network management and troubleshooting.

3. What does social engineering refer to?

A. A manipulation technique used to trick individuals into divulging confidential information

B. A method of programming computers to optimize performance

C. A strategy for building secure software

D. A process for updating security protocols

Social engineering refers to a manipulation technique used to trick individuals into divulging confidential information. This practice exploits human psychology rather than relying on technical hacking methods. Through social engineering, attackers create scenarios that entice individuals to provide sensitive data such as passwords, personal identification numbers, or other secure details. Common tactics include impersonating a trusted figure or creating a sense of urgency, making individuals more likely to fall for the deception. The other options describe different areas related to cybersecurity or computer science. For instance, programming computers to optimize performance pertains to software engineering rather than the manipulation of individuals. Building secure software refers to practices in software development aimed at preventing vulnerabilities during the design and coding phases. Updating security protocols involves maintaining and enhancing the security measures in place, which again does not involve the direct manipulation of individuals as seen in social engineering techniques. Therefore, the description that focuses on tricking individuals into revealing confidential information accurately defines social engineering.

SAMPLE

4. What does cryptography encompass?

A. The study of digital currencies

B. The science and art of secure message delivery

C. The analysis of network systems

D. The process of logging data

Cryptography encompasses the science and art of secure message delivery because it involves techniques and methods for protecting information by transforming it into a secure format. This transformation ensures that only authorized parties can access and understand the information, preserving confidentiality, integrity, and authenticity. It includes various practices such as encryption, decryption, and the use of cryptographic keys to safeguard the communication between individuals or systems. This fundamental aspect of cryptography plays a crucial role in information security, ensuring that sensitive data remains protected from unauthorized access and potential breaches. In contrast, the study of digital currencies relates more to specific applications of cryptography rather than its broader principles. The analysis of network systems deals with the overall examination of networks to identify vulnerabilities and optimize performance, which is a different focus from the core principles of cryptography. Similarly, the process of logging data pertains to the collection and storage of information, which does not directly involve the secure transmission and protection of that data.

5. Which command provides information about running processes that include other user's activities?

A. bg

B. ps -ef

C. kill

D. su

The command that provides information about running processes, including those initiated by other users, is "ps -ef." This command is a widely used utility in Unix-like operating systems that lists all the currently running processes on the system, along with detailed information such as process IDs, user ownership, CPU usage, and more. When you include the "-e" flag, it tells the system to display processes for all users rather than just the processes owned by the current user. The "-f" flag enhances the output by showing a full-format listing, which includes additional details about the processes, making it easier for users to understand what is happening on the system and identify any processes of interest, including those that may be running under other user accounts. This command is particularly valuable for system administrators and cybersecurity professionals, as it helps monitor system activity and manage processes effectively. Understanding what processes are running and who owns them can be crucial for security assessments and troubleshooting system performance issues.

SAMPLE

6. Which form of encryption utilizes two distinct keys?

A. Symmetric key encryption

B. Private key encryption

C. Public key encryption

D. Substitution cyphers

The chosen answer highlights a crucial concept in cryptography known as public key encryption, also referred to as asymmetric encryption. This encryption method employs two distinct keys: a public key, which can be shared openly to encrypt data, and a private key, which remains confidential and is used to decrypt the received data. The dual-key structure of public key encryption enhances security because even if the public key is known to everyone, the private key remains secret and only accessible to the intended recipient. This asymmetry allows secure communication over insecure channels, ensuring that only the holder of the corresponding private key can access the original information. In contrast, symmetric key encryption uses a single key for both encryption and decryption, meaning that both parties must share the same secret key securely. Private key encryption is essentially synonymous with symmetric key encryption. Substitution ciphers represent a basic form of encryption where each character in the plaintext is substituted for a character in the ciphertext, but they do not inherently utilize the key structure required for the question. Thus, public key encryption stands out as the most appropriate answer due to its use of two distinct keys for enhanced security principles.

7. What are the three steps of a TCP handshake?

A. SYN, SYN-ACK, ACK

B. REQUEST, RESPONSE, CONFIRMATION

C. CONNECT, VERIFY, ESTABLISH

D. ACK, SYN-ACK, SYN-DELETE

*The three steps of a TCP handshake are SYN, SYN-ACK, and ACK. This process is essential for establishing a reliable connection between a client and a server before they begin to exchange data. 1. **SYN**: The client initiates the connection by sending a Synchronize (SYN) packet to the server, indicating that it wants to establish a connection and providing its initial sequence number. 2. **SYN-ACK**: The server responds with a Synchronize-Acknowledge (SYN-ACK) packet. This packet serves a dual purpose: it acknowledges the receipt of the client's SYN packet and also includes the server's own SYN packet, along with its own initial sequence number. 3. **ACK**: Finally, the client sends an Acknowledge (ACK) packet back to the server, confirming that it received the server's SYN-ACK packet. At this point, the TCP connection is fully established, and the two parties can begin to communicate. This three-step process ensures that both the client and server are synchronized and have the proper sequence numbers for tracking the data that will be sent, which is critical in maintaining data integrity during transmission.*

SAMPLE

8. What does the keyword SEC specify when searching for files?

A. Finds SEC in any file name in any folder

B. Finds any file type

C. Finds files modified on a specific date

D. Finds files associated with the government

The keyword SEC, when used in a file search, specifically instructs the search tool to look for "SEC" within file names across all folders. This means that if any file name contains the sequence "SEC," it will be returned in the search results, making it useful for locating files that may be relevant to a particular context, especially if "SEC" is part of a naming convention commonly used by an individual or organization. The other options do not accurately describe the function of the SEC keyword in this context. For instance, while one might assume that a keyword can denote file types or modification dates, this is not the case here. Each of those attributes typically requires different search criteria or parameters distinct from merely searching for text in file names. The specific nature of the keyword SEC reinforces its utility in narrowing down searches efficiently based on naming conventions.

9. What does a digital footprint represent?

A. The internal storage of a device

B. The trail of data left by users on the internet

C. The design of a web application

D. The encryption of data in transit

A digital footprint represents the trail of data left by users on the internet, which encompasses both the information that individuals actively share and the data that is collected about them through their online activities. This includes everything from social media posts and interactions to website visits, search histories, and even data from apps. Understanding digital footprints is crucial because they can have a lasting impact on privacy and personal security. Users need to be aware that their online actions contribute to a persistent record that can be accessed or analyzed by others, including advertisers, employers, and potential cybercriminals. In contrast, the internal storage of a device pertains to the physical hardware used to store files, which does not relate directly to online behavior. The design of a web application involves the user interface and architecture of a website, which are not directly tied to user actions or their resulting data. Finally, the encryption of data in transit refers to securing information as it travels across networks, which is a separate concept from the idea of tracking online behavior through a digital footprint.

SAMPLE

10. What does risk assessment involve?

A. Updating software regularly

B. Identifying and evaluating potential risks

C. Logging all network activity

D. Implementing new technologies

Risk assessment is a crucial process in cybersecurity that focuses on identifying and evaluating potential risks to an organization's information systems and data. This involves systematically analyzing vulnerabilities, threats, and the potential impact of various risks. By doing this, organizations can prioritize their resources and defenses to address the most significant risks effectively. The process typically includes identifying assets that need protection, assessing the threats to those assets, determining the likelihood of those threats materializing, and evaluating the potential consequences. This comprehensive understanding enables organizations to make informed decisions about mitigating risks, which is essential for maintaining the security and integrity of their information systems. While updating software, logging network activity, and implementing new technologies are important components of a robust cybersecurity strategy, these actions are not themselves risk assessment. They may be part of the broader risk management process that follows the assessment phase, but the core focus of risk assessment is specifically on identifying and evaluating risks.

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://pltwcybersecurityeoc.examzify.com

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

SAMPLE