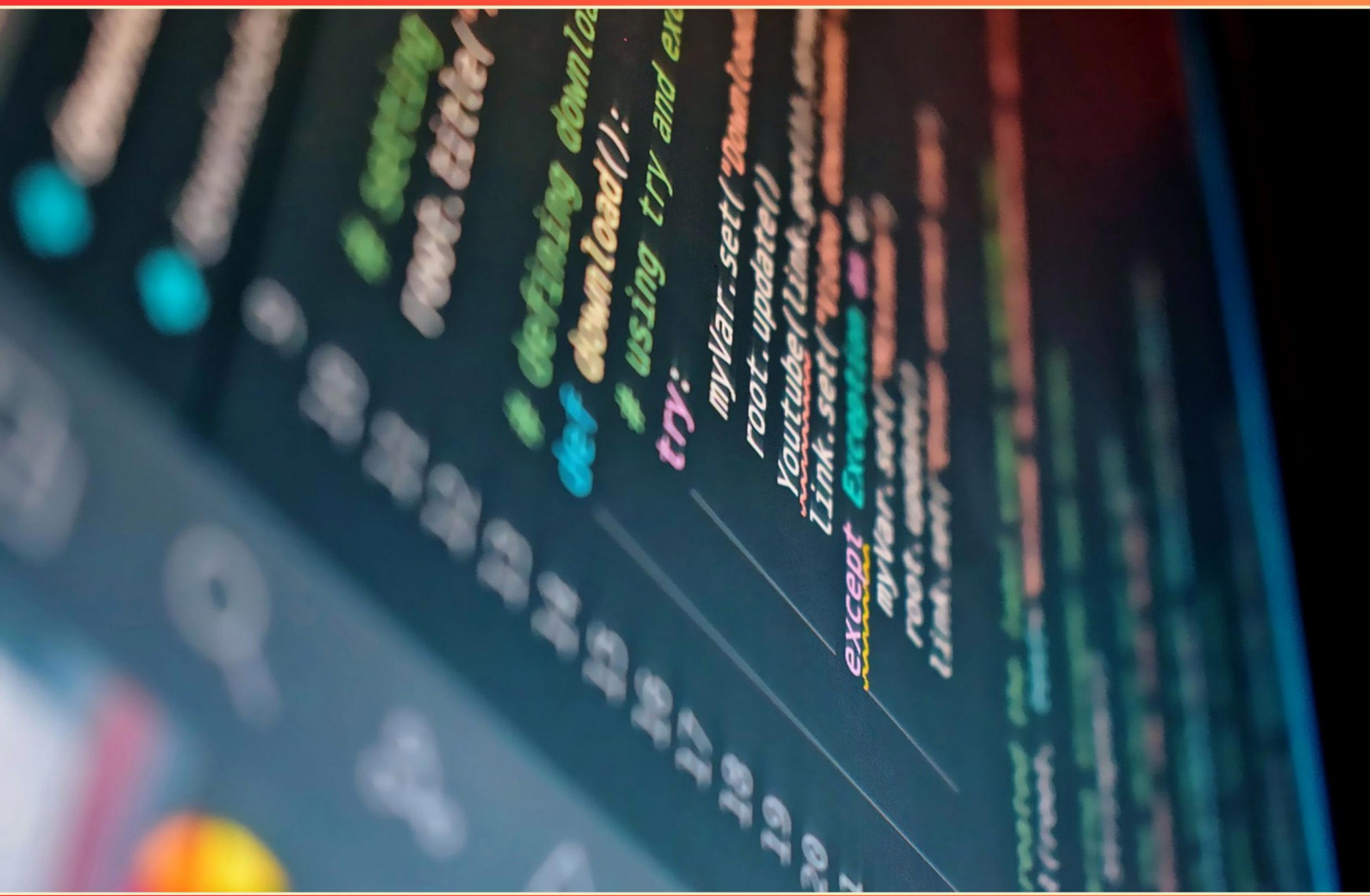
CERTIPORT CYBERSECURITY CERTIFICATION PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://certiportcybersecurity.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. Which of the following is a common reason for successful cyber attacks?

A. Strongly configured firewalls

B. Widespread vulnerabilities

C. Regular software updates

D. High employee awareness

2. What is one significant advantage of cloud computing regarding maintenance?

A. Users must manage all updates

B. The cloud provider updates the hardware

C. The cloud operates without any physical security

D. Local computing resources are prioritized

3. What type of information is primarily found in system logs within the event viewer?

A. Information about user preferences

B. Details regarding incidents related to the operating system

C. Lists of installed software

D. Network traffic statistics

4. What is the primary purpose of establishing a chain of custody in forensics?

A. To prove the evidence was never altered

B. To ensure that evidence is handled by authorized personnel only

C. To facilitate easy access to evidence by investigators

D. To document the collection method of evidence

5. What does BYOD stand for in a cybersecurity context?

A. Bring Your Own Device

B. Buy Your Online Data

C. Better Your Online Defense

D. Backup Your Online Documents

SAMPLE

6. Which Act regulates the privacy of consumer financial information?

A. GDPR

B. FERPA

C. GLBA

D. HIPAA

7. What is a key characteristic of spear phishing attacks?

A. They target large groups indiscriminately

B. They focus on specific individuals or groups

C. They use social media exclusively for contact

D. They rely solely on email communication

8. What is the main goal of limiting user access rights according to the Principle of Least Privilege?

A. To improve network speed

B. To enhance user convenience

C. To prevent unauthorized access and maintain security

D. To allow for easier tracking of user activity

9. In legal cases, what consequence could result from a broken chain of custody?

A. The evidence may be deemed inadmissible in court

B. The case may be dismissed completely

C. The accused may receive a lighter sentence

D. The investigation may be reopened

10. What is the definition of malware?

A. Software intended to assist computer functions

B. Software intended to damage or disable computers and systems

C. Software that protects against threats

D. Legitimate software used for productivity

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which of the following is a common reason for successful cyber attacks?

A. Strongly configured firewalls

B. Widespread vulnerabilities

C. Regular software updates

D. High employee awareness

Widespread vulnerabilities are a common reason for successful cyber attacks because they create opportunities for attackers to exploit weaknesses in systems, applications, or networks. When software and hardware have known vulnerabilities that have not been addressed, attackers can take advantage of these flaws to gain unauthorized access, steal data, or disrupt services. This can occur in various forms, such as unpatched software, outdated systems, or misconfigured settings that leave entry points open to malicious actors. In the context of cybersecurity, it is essential for organizations to identify and mitigate vulnerabilities regularly. This includes conducting vulnerability assessments, implementing security patches, and ensuring that configurations adhere to best practices. By addressing widespread vulnerabilities, organizations significantly reduce the risk of successful cyber attacks. In contrast, factors such as strongly configured firewalls, regular software updates, and high employee awareness are proactive measures that defend against cyber threats. Strong firewalls block unauthorized access, regular updates close security gaps, and knowledgeable employees are less likely to fall for phishing attacks or other social engineering tactics. These factors contribute to a robust security posture, which helps prevent cyber attacks rather than being a reason for their success.

2. What is one significant advantage of cloud computing regarding maintenance?

A. Users must manage all updates

B. The cloud provider updates the hardware

C. The cloud operates without any physical security

D. Local computing resources are prioritized

One significant advantage of cloud computing regarding maintenance is that the cloud provider takes responsibility for updating the hardware. This means that users do not have to worry about the time, cost, and resources associated with maintaining physical hardware, such as servers, storage devices, and networking components. The cloud provider ensures that the infrastructure is kept up to date with the latest technology and security measures, which allows users to focus on their core business processes rather than IT maintenance tasks. This approach diminishes the need for in-house IT teams to dedicate time and effort to hardware updates, leading to increased efficiency and reduced operational costs for users. In contrast, the other options present responsibilities or aspects of maintenance that do not align with the benefits of cloud computing. Users managing all updates would imply a burden, while the inaccurate notion of the cloud operating without any physical security could pose significant risks. Prioritizing local computing resources does not highlight the advantage of cloud maintenance, as it suggests a different focus entirely.

SAMPLE

3. What type of information is primarily found in system logs within the event viewer?

A. Information about user preferences

B. Details regarding incidents related to the operating system

C. Lists of installed software

D. Network traffic statistics

System logs within the event viewer primarily contain details regarding incidents related to the operating system. These logs are a critical resource for system administrators and security professionals, as they track events such as system errors, warnings, and informational messages that occur at the operating system level. This includes boot processes, application crashes, system updates, security violations, and other essential operations that help in diagnosing issues or monitoring system health. By analyzing the data in these logs, individuals can identify patterns, catch anomalies, and respond to potential threats or malfunctions promptly. The focus on incidents related to the operating system is crucial for maintaining system integrity and security, allowing administrators to take actionable measures based on the recorded events. While user preferences, lists of installed software, and network traffic statistics are all important aspects of system management and security, they are categorized separately and do not typically reside within the system logs of the event viewer.

4. What is the primary purpose of establishing a chain of custody in forensics?

A. To prove the evidence was never altered

B. To ensure that evidence is handled by authorized personnel only

C. To facilitate easy access to evidence by investigators

D. To document the collection method of evidence

The primary purpose of establishing a chain of custody in forensics is to ensure that evidence is handled by authorized personnel only. This process is critical for maintaining the integrity of the evidence throughout the entire investigation. By documenting each instance that evidence is accessed, transferred, or analyzed, the chain of custody helps to prevent tampering, contamination, or loss of evidence. It establishes a clear record of who has handled the evidence and under what circumstances, which serves to validate its authenticity in court. This careful oversight is essential because any break or lapse in this chain can jeopardize the admissibility of the evidence, undermining the entire investigative process. The other options, while addressing aspects related to evidence management, do not encompass the broad protective scope of the chain of custody. For instance, proving that evidence was never altered is a consequence of maintaining a proper chain rather than its primary purpose. Similarly, providing easy access is not typically an objective of the chain of custody; rather, the focus is on maintaining security and authenticity. Finally, while documenting the collection method is important, it is just one component of the overall chain of custody process, which is more concerned with tracking the evidence's handling over time.

SAMPLE

5. What does BYOD stand for in a cybersecurity context?

A. Bring Your Own Device

B. Buy Your Online Data

C. Better Your Online Defense

D. Backup Your Online Documents

In a cybersecurity context, BYOD stands for "Bring Your Own Device." This concept refers to the practice of allowing employees or users to utilize their personal devices—such as smartphones, tablets, and laptops—for work-related tasks and to access corporate data and applications. The significance of BYOD lies in its ability to enhance flexibility and productivity among employees, as it enables them to work from various devices that they are already comfortable using. However, this practice also raises important security considerations. Organizations must implement robust security policies and controls to protect sensitive data and ensure that personal devices do not introduce vulnerabilities into the corporate network. This includes measures such as data encryption, secure access protocols, and regular security training for users. Overall, BYOD presents both opportunities and challenges within the cybersecurity landscape, making it a crucial topic for organizations to address.

6. Which Act regulates the privacy of consumer financial information?

A. GDPR

B. FERPA

C. GLBA

D. HIPAA

The Gramm-Leach-Bliley Act (GLBA) primarily focuses on the protection of consumer financial information by requiring financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. This act establishes the importance of privacy in the financial sector, mandating that institutions take measures to ensure the confidentiality and security of consumer data. By requiring the creation of privacy notices and allowing consumers to opt-out of certain information-sharing practices, GLBA aims to provide consumers with greater control over their personal financial information. This makes it the appropriate regulation regarding the privacy of consumer financial data, distinguishing it from acts that pertain to education or health information.

7. What is a key characteristic of spear phishing attacks?

A. They target large groups indiscriminately

B. They focus on specific individuals or groups

C. They use social media exclusively for contact

D. They rely solely on email communication

Spear phishing attacks are characterized by their targeted approach, focusing on specific individuals or groups rather than casting a wide net like traditional phishing attempts. This personalized strategy often involves gathering detailed information about the target, such as their role within an organization, interests, or connections, allowing attackers to craft convincing messages that increase the likelihood of success. The specificity in the attacks is what differentiates spear phishing from more general phishing scams, which typically aim at a broad audience without a personalized strategy. By honing in on particular victims, attackers can exploit trust and familiarity, making their fraudulent requests appear more legitimate. This tailored approach is what makes spear phishing particularly dangerous and effective.

SAMPLE

8. What is the main goal of limiting user access rights according to the Principle of Least Privilege?

A. To improve network speed

B. To enhance user convenience

C. To prevent unauthorized access and maintain security

D. To allow for easier tracking of user activity

The main goal of limiting user access rights according to the Principle of Least Privilege is to prevent unauthorized access and maintain security. This principle dictates that users should only have the minimum level of access necessary to perform their job functions. By restricting access rights, organizations can significantly reduce the risk of accidental or malicious misuse of sensitive data and resources. When users are granted only the privileges they absolutely need, it limits the potential attack surface, helping to protect critical systems and information from threats, both internal and external. This approach is fundamentally rooted in cybersecurity best practices and is a key strategy in mitigating risks associated with users who may inadvertently expose systems to vulnerabilities or those who may have malevolent intentions. Thus, applying the Principle of Least Privilege is crucial for strengthening an organization's overall security posture.

9. In legal cases, what consequence could result from a broken chain of custody?

A. The evidence may be deemed inadmissible in court

B. The case may be dismissed completely

C. The accused may receive a lighter sentence

D. The investigation may be reopened

A broken chain of custody is critical in legal proceedings, particularly when it involves evidence. The chain of custody refers to the process of maintaining and documenting the handling of evidence from the time it is collected until it is presented in court. If there is a break in this chain, it raises questions about the integrity and reliability of the evidence. As a result, if the evidence cannot be proven to have been handled properly and securely, it may be considered tainted or manipulated, and consequently, a judge may rule that the evidence is inadmissible in court. This ruling can significantly weaken the prosecution's case, as they may lose key pieces of evidence that could have supported their arguments or claims. In contrast, while a dismissed case, lighter sentences, or reopening investigations may occur in some contexts, these are not direct consequences of a broken chain of custody but rather dependent on various factors specific to the individual circumstances of each case. The integrity of evidence is paramount, and thus, the inadmissibility of evidence is the most immediate and clear consequence of a broken chain of custody.

SAMPLE

10. What is the definition of malware?

A. Software intended to assist computer functions

B. Software intended to damage or disable computers and systems

C. Software that protects against threats

D. Legitimate software used for productivity

Malware, short for malicious software, is specifically designed to damage, disrupt, or gain unauthorized access to computer systems and networks. The emphasis is on the harmful intent behind malware, which includes a variety of forms such as viruses, worms, Trojans, ransomware, and spyware. Malware can lead to data theft, system failures, and even the exploitation of computer resources for malicious purposes. In contrast, software that assists computer functions, protects against threats, or is used legitimately for productivity serves beneficial roles in computing. Such software includes system utilities, antivirus programs, and office productivity applications. These definitions highlight the polar opposite of malware's intent, reinforcing that the principal characteristic of malware is its goal to harm rather than help. This context underscores why the definition of malware, focused on its intent to damage or disable systems, is the most accurate and relevant.

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://certiportcybersecurity.examzify.com

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

SAMPLE