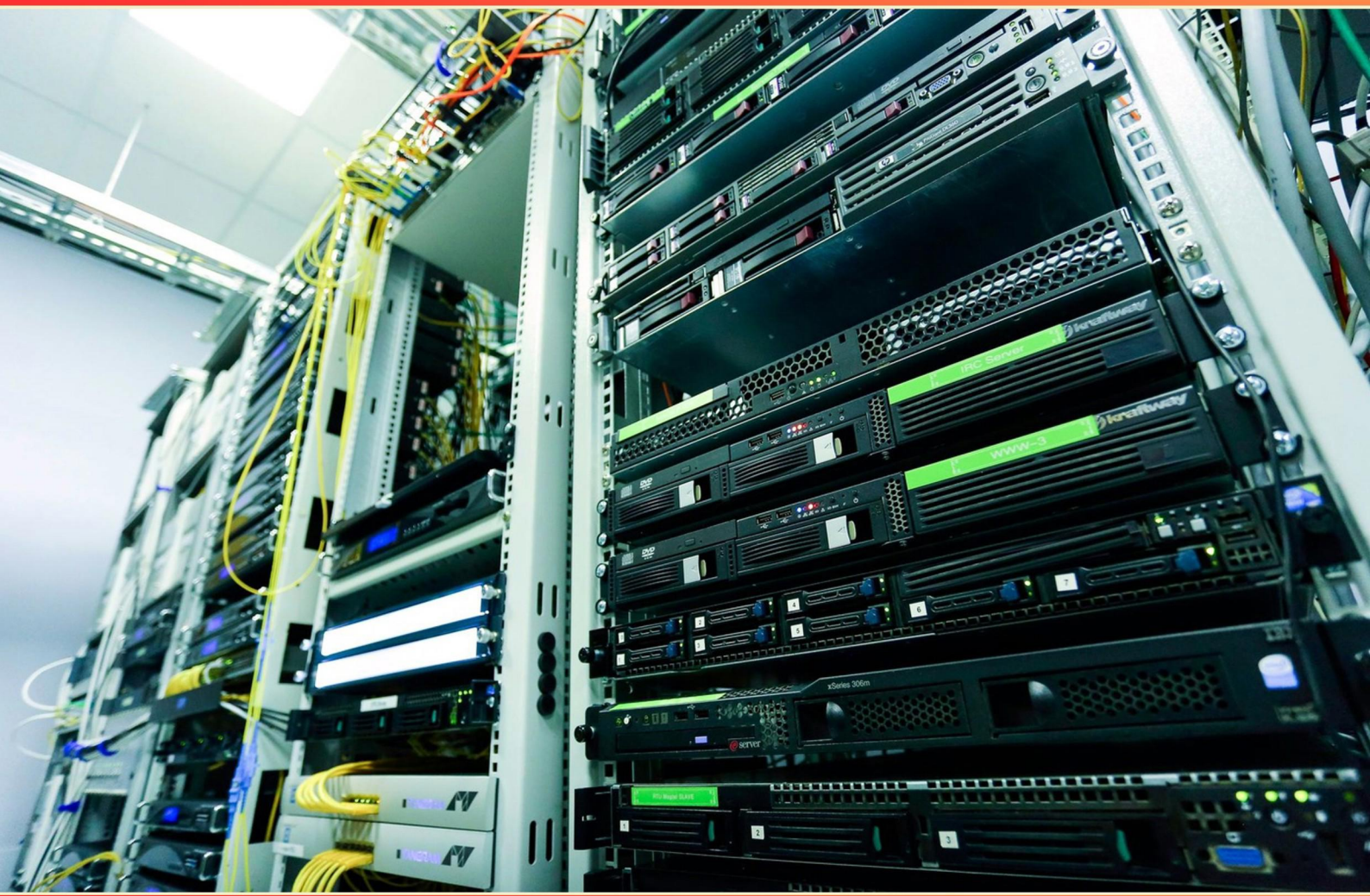
TSA CYBERSECURITY PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://tsacybersecurity.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 15

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 purpose of cybersecurity training for employees?

A. To promote personal growth and development

B. To ensure employees are aware of security policies and practices

C. To encourage teamwork within departments

D. To prepare employees for promotions

2. Which of the following best describes the Web?

A. A vast collection of networking devices

B. The digital content delivered over the Internet

C. A programming language used for sites

D. An Internet access provider

3. What role does threat intelligence play in cybersecurity?

A. It is used for internal audits.

B. It helps in budget allocation for security.

C. It aids in understanding and mitigating threats.

D. It ensures compliance with regulations.

4. What is the term for software that is exclusively controlled by a company and cannot be used or modified without permission?

A. Open-Source Software

B. Freeware

C. Proprietary Software

D. Shareware

5. You can access some websites from a public library network but not others. What is the likely reason?

A. Poor Internet connection

B. A proxy server is filtering access

C. Outdated browser version

D. Firewall restrictions

SAMPLE

6. Which type of attack is aimed at overwhelming a system with traffic?

A. Phishing attack

B. Denial-of-Service (DoS) attack

C. Man-in-the-middle (MitM) attack

D. Data breach attack

7. What does remote access security focus on?

A. Enhancing physical security at remote sites

B. Securing network connections from remote locations

C. Managing user passwords remotely

D. Developing mobile applications

8. Assigning a unique letter (such as N:) to a shared drive is called ____ the drive.

A. Mapping

B. Connecting

C. Sharing

D. Linking

9. Cyber hygiene refers to what?

A. Specific coding practices in programming

B. Maintenance steps for system health

C. The physical cleaning of computer hardware

D. The use of anti-virus software only

10. What role does monitoring employee activities play in cybersecurity?

A. It ensures all employees are happy

B. It helps identify potential insider threats

C. It is used solely for performance reviews

D. It discourages team collaboration

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the primary purpose of cybersecurity training for employees?

A. To promote personal growth and development

B. To ensure employees are aware of security policies and practices

C. To encourage teamwork within departments

D. To prepare employees for promotions

The primary purpose of cybersecurity training for employees is to ensure they are aware of security policies and practices. This training equips employees with the knowledge and skills necessary to identify potential threats, understand their role in maintaining security protocols, and apply best practices in their daily activities. By being informed about the organization's cyber policies, employees can help safeguard sensitive information, mitigate risks, and contribute to a culture of security within the organization. While personal growth and development, teamwork, and promotional preparation can be beneficial outcomes of various training programs, they do not specifically address the critical need for employees to understand and adhere to cybersecurity measures. The focus of cybersecurity training is predominantly on fostering an informed workforce capable of recognizing and responding to cyber threats effectively.

2. Which of the following best describes the Web?

A. A vast collection of networking devices

B. The digital content delivered over the Internet

C. A programming language used for sites

D. An Internet access provider

The best description of the Web is that it refers to the digital content delivered over the Internet. This content includes websites, web applications, and various online resources that are accessed using web browsers. The Web operates on protocols such as HTTP and HTTPS, allowing users to retrieve and interact with information hosted on servers around the world. While the other options contain elements that relate to the broader infrastructure of networking and the Internet, they do not specifically define what the Web itself encompasses. For example, networking devices are integral to Internet connectivity but do not describe the content or the user experience that the Web provides. Similarly, programming languages are tools used to create websites and applications but do not define the Web as a whole. An Internet access provider refers to a service that connects users to the Internet, bypassing the central aspect of what the Web actually delivers to those users.

3. What role does threat intelligence play in cybersecurity?

A. It is used for internal audits.

B. It helps in budget allocation for security.

C. It aids in understanding and mitigating threats.

D. It ensures compliance with regulations.

Threat intelligence plays a crucial role in cybersecurity by aiding organizations in understanding and mitigating threats. This involves gathering, analyzing, and applying information about potential or existing threats to enhance an organization's defensive capabilities. By leveraging threat intelligence, organizations can identify patterns and trends in malicious activity, recognize indicators of compromise, and prioritize their responses to protect their assets effectively. The insights gained from threat intelligence enable security teams to be proactive rather than reactive, allowing them to implement necessary measures to address vulnerabilities before they can be exploited by attackers. This also facilitates informed decision-making regarding security strategies and resource allocation, thus enhancing the overall security posture of the organization. Effective use of threat intelligence contributes to timely incident response, improved risk management, and an informed understanding of the evolving threat landscape.

SAMPLE

4. What is the term for software that is exclusively controlled by a company and cannot be used or modified without permission?

A. Open-Source Software

B. Freeware

C. Proprietary Software

D. Shareware

Proprietary software refers to programs that are owned by an individual or a company, granting that entity full control over its use, distribution, and modification. This means that users need permission to access the source code, make alterations, or redistribute the software. Proprietary software typically comes with a license that outlines how it can be used, which often requires payment or subscription to maintain legal access. In contrast, open-source software allows users to view, modify, and distribute the source code, fostering collaboration and innovation. Freeware is software that is available for use at no monetary cost but may still have restrictions regarding modification or redistribution. Shareware is a type of software that is distributed on a trial basis and often requires payment for continued use, but may allow users to explore functionalities before purchasing. Understanding these distinctions is crucial for navigating software licensing and development, especially in environments that prioritize security and compliance.

5. You can access some websites from a public library network but not others. What is the likely reason?

A. Poor Internet connection

B. A proxy server is filtering access

C. Outdated browser version

D. Firewall restrictions

Accessing some websites from a public library network while being unable to reach others is most likely due to a proxy server filtering access. In many public networks, such as those in libraries, proxy servers are implemented to manage internet traffic and enforce specific access policies. These servers can restrict access to certain sites deemed inappropriate or non-educational based on established guidelines. Typically, libraries use this approach to ensure that their resources are used for educational and informational purposes, thereby fostering a safe and productive environment for all users. By filtering content, they can block harmful or non-compliant websites, while still allowing access to those that fit within their accepted use policies. This filtering mechanism is an important aspect of cybersecurity in public networks, helping to protect users from accessing potentially harmful content while guiding them toward useful resources. The other reasons do not specifically relate to controlled access policies in the same way that a proxy server does, which makes this answer the most relevant in the context of the question.

SAMPLE

6. Which type of attack is aimed at overwhelming a system with traffic?

A. Phishing attack

B. Denial-of-Service (DoS) attack

C. Man-in-the-middle (MitM) attack

D. Data breach attack

A Denial-of-Service (DoS) attack is designed to overwhelm a system with an excessive amount of traffic. The primary goal of this type of attack is to make the targeted service or network unavailable to its intended users. By flooding the target with a high volume of requests, the attacker consumes the system's resources, leading to slower response times or a complete crash, thus denying legitimate users access to the service. In contrast, phishing attacks focus on tricking individuals into revealing sensitive information, while man-in-the-middle (MitM) attacks intercept and alter communications between two parties. A data breach attack typically involves accessing sensitive data unlawfully, rather than overwhelming a system with traffic. Understanding these distinctions helps in recognizing the intent and method behind different cybersecurity threats.

7. What does remote access security focus on?

A. Enhancing physical security at remote sites

B. Securing network connections from remote locations

C. Managing user passwords remotely

D. Developing mobile applications

Remote access security primarily focuses on securing network connections from remote locations. This area of cybersecurity is crucial as more users access networks from various off-site locations, such as their homes or public spaces. The goal is to ensure that these remote connections are protected from unauthorized access and other cybersecurity threats. To achieve this, remote access security employs various methods and technologies, including VPNs (Virtual Private Networks), secure sockets layer (SSL) encryption, and two-factor authentication. These measures help safeguard the data transmitted over the network and ensure that users can securely connect to organizational resources while maintaining confidentiality and integrity. Other options do not adequately capture the essence of remote access security. While enhancing physical security at remote sites is important for overall security, it does not specifically pertain to the security of network connections. Managing user passwords remotely, though relevant to cybersecurity, is a narrower focus and doesn't encompass the broader picture of securing the network as a whole. Developing mobile applications is also outside the primary concern of remote access security, which is focused on protecting the connectivity and traffic between users and the organizational infrastructure.

SAMPLE

8. Assigning a unique letter (such as N:) to a shared drive is called ____ the drive.

A. Mapping

B. Connecting

C. Sharing

D. Linking

Assigning a unique letter to a shared drive is referred to as mapping the drive. Mapping simplifies the process of accessing network drives, allowing users to assign a designated letter that represents a specific shared folder or disk on the network. This action creates a shortcut that users can easily recognize and use, making it more convenient to navigate to shared resources without needing to remember the full network path. Mapping is particularly useful in environments where multiple users need consistent access to shared resources. By associating a shared drive with a unique letter, users can quickly find and access files without dealing with potentially complex directory structures. This process improves productivity and collaboration in environments that rely on shared data. The other terms, while related to networking and data access, do not accurately describe the act of assigning a letter to a drive. Connecting might refer to establishing a connection to the network or a device, sharing typically involves allowing others to access files or resources, and linking can imply creating a reference or pathway but does not specifically denote the assignment of a drive letter. Thus, mapping stands out as the correct terminology in this context.

9. Cyber hygiene refers to what?

A. Specific coding practices in programming

B. Maintenance steps for system health

C. The physical cleaning of computer hardware

D. The use of anti-virus software only

Cyber hygiene encompasses the set of practices and maintenance steps that individuals and organizations take to ensure the security, efficiency, and health of their systems. This approach focuses on regular updates, patch management, monitoring system performance, and ensuring that security measures are in place, which contributes to reducing vulnerabilities and the risk of cyberattacks. Maintaining system health involves routine activities such as updating software, managing user permissions, and backing up data, which can ultimately improve an organization's cybersecurity posture. Hence, identifying and implementing good cyber hygiene practices can help prevent common threats and enhance overall cybersecurity resilience.

10. What role does monitoring employee activities play in cybersecurity?

A. It ensures all employees are happy

B. It helps identify potential insider threats

C. It is used solely for performance reviews

D. It discourages team collaboration

Monitoring employee activities plays a crucial role in cybersecurity by helping organizations identify potential insider threats. By observing patterns of behavior and access to sensitive information, monitoring can reveal unusual activities that may indicate a breach or malicious intent. For instance, if an employee accesses data outside of their typical job responsibilities or during odd hours, this could trigger an alert for further investigation. Additionally, by maintaining vigilance over employee actions, organizations can foster a more secure environment by proactively addressing risks before they culminate in significant security incidents. This process not only helps safeguard sensitive data but also serves to deter unauthorized actions by creating awareness that activities are being monitored. While it's true that performance reviews and promoting teamwork are important aspects of a productive work environment, they are not the primary focus of monitoring in the context of cybersecurity.

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://tsacybersecurity.examzify.com

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

SAMPLE