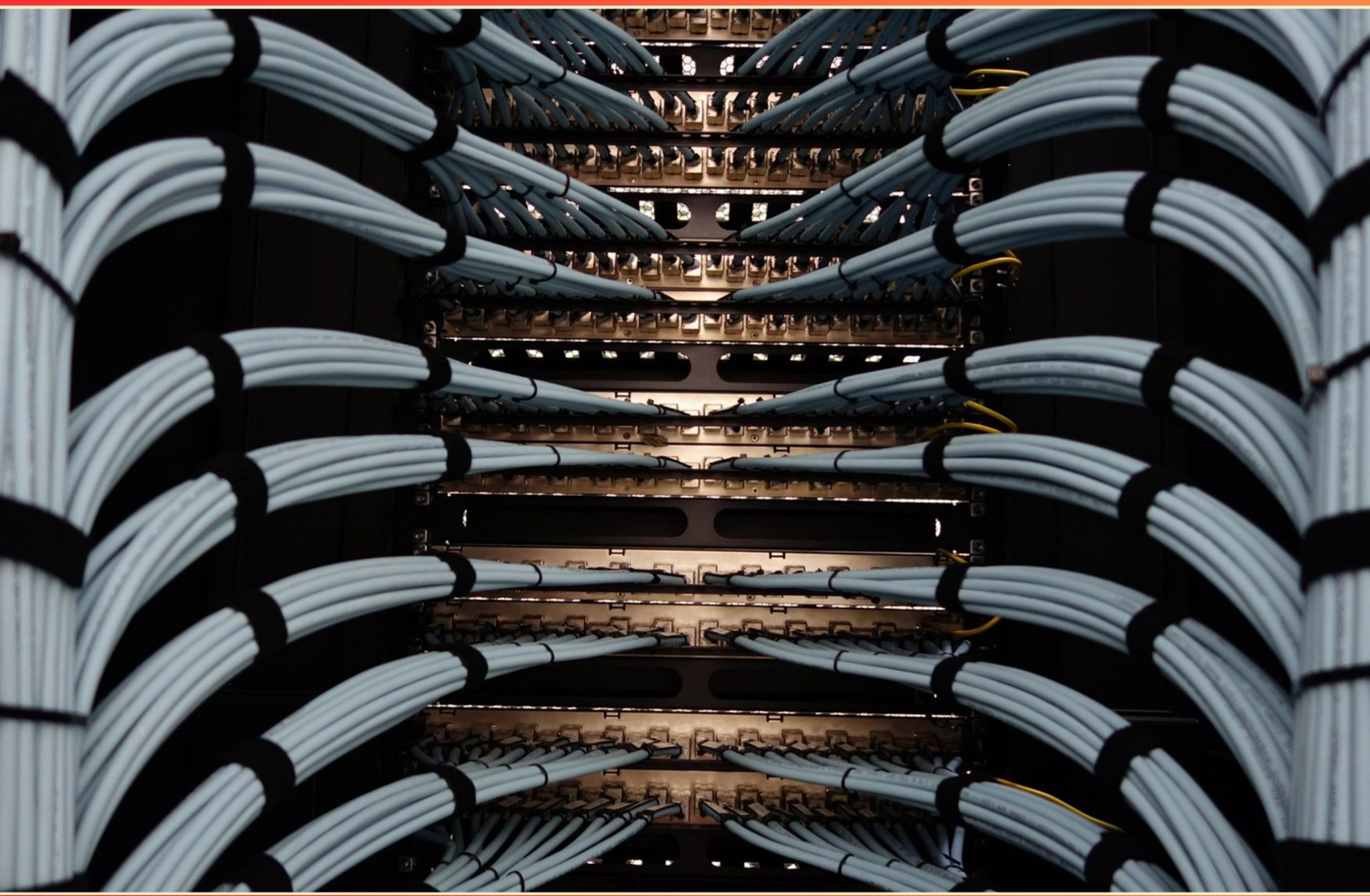
GIAC INFORMATION SECURITY FUNDAMENTALS (GISF) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://giacgisf.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 significance of classifying alerts as true positive, false positive, true negative, and false negative?**

   A. To measure the performance of a security system

   B. To identify the types of threats in the system

   C. To categorize user accesses

   D. To determine the server load

2. **What is typically the action denied to a non-privileged user account?**

   A. Reading files

   B. Modifying system settings

   C. Accessing own files

   D. Executing programs

3. **Which term describes a network of compromised devices that can be controlled by an attacker?**

   A. Trojan horse

   B. Botnet

   C. Malware

   D. Spyware

4. **Can Bluetooth signals be intercepted beyond their typical operational range?**

   A. No, they cannot be intercepted at all

   B. Yes, but only in controlled environments

   C. Yes, with specialized equipment like BlueSniper rifles

   D. Only Bluetooth Class 1 signals can be intercepted

5. **What does a MAC address do?**

   A. Identifies online services

   B. Uniquely identifies each node on a network

   C. Routes packets across the internet

   D. Resolves hostnames to IP addresses

SAMPLE

6. Which of the following is NOT one of the five phases of an attack?

A. Reconnaissance

B. Negotiation

C. Covering tracks

D. Gaining access

7. What is the purpose of likelihood and impact estimates in the risk management process?

A. To evaluate asset value

B. To identify threats

C. To assess the potential damage and frequency of threats

D. To determine response strategies

8. In Windows, what is the purpose of NTFS?

A. To provide a framework for application performance

B. To control and enforce file access permissions

C. To enable multi-user access on a network

D. To backup system files securely

9. Which term describes a condition that allows a threat to potentially exploit a system?

A. Risk

B. Vulnerability

C. Exposure

D. Incident

10. What phase of an attack involves identifying assets that could be targeted for exploitation?

A. Gaining access

B. Scanning

C. Reconnaissance

D. Maintaining access

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the significance of classifying alerts as true positive, false positive, true negative, and false negative?

A. To measure the performance of a security system

B. To identify the types of threats in the system

C. To categorize user accesses

D. To determine the server load

Classifying alerts as true positive, false positive, true negative, and false negative is significant because it allows organizations to measure the performance of their security systems effectively. By categorizing alert outcomes this way, security teams can assess how well their detection mechanisms are functioning. True positives indicate successful detection of actual threats, while false positives reveal alerts generated for non-threats, which can lead to wasted resources and alert fatigue. True negatives confirm that the system correctly identified safe conditions, and false negatives represent missed detections of real threats. Analyzing these classifications helps in refining detection algorithms, improving system responses, and ultimately enhancing the security posture. This classification system allows for critical insights into the efficiency and effectiveness of security systems and informs strategies for ongoing improvements in threat detection and incident response protocols.

2. What is typically the action denied to a non-privileged user account?

A. Reading files

B. Modifying system settings

C. Accessing own files

D. Executing programs

The action that is typically denied to a non-privileged user account is modifying system settings. Non-privileged users are designed to have limited access to the system's core functions and configurations to maintain security and system stability. Allowing unrestricted access to system settings could lead to unintentional or malicious changes that can compromise the integrity and security of the system. Non-privileged users can generally read files, access their own files, and execute programs, provided they have the necessary permissions for those specific tasks. This controlled access is essential for ensuring that users can perform their roles without risking the configuration and security of the overall system. Restricting the ability to modify system settings helps protect against potential misuse or accidents that could disrupt the operation of the network or systems.

3. Which term describes a network of compromised devices that can be controlled by an attacker?

A. Trojan horse

B. Botnet

C. Malware

D. Spyware

A botnet refers to a network of compromised devices that are controlled by an attacker to perform coordinated tasks, often without the knowledge of the device owners. These devices, also known as "bots" or "zombies," can include anything from personal computers to IoT devices that have been infected with malware. Once they are part of the botnet, the attacker can use them for various malicious activities such as launching Distributed Denial of Service (DDoS) attacks, sending out spam emails, or mining cryptocurrencies, all while remaining largely undetected. The significance of the term "botnet" lies in the collective power it provides to an attacker; by harnessing multiple compromised devices, they can achieve far greater impact compared to using a single device. Botnets exemplify one of the major threats in cybersecurity, as they can exploit vulnerabilities on a massive scale, making them a substantial topic of concern in information security.

SAMPLE

4. Can Bluetooth signals be intercepted beyond their typical operational range?

A. No, they cannot be intercepted at all

B. Yes, but only in controlled environments

C. Yes, with specialized equipment like BlueSniper rifles

D. Only Bluetooth Class 1 signals can be intercepted

The correct answer indicates that Bluetooth signals can indeed be intercepted beyond their typical operational range using specialized equipment, such as BlueSniper rifles. Bluetooth technology typically operates within a range of approximately 10 to 100 meters depending on the class of the device and environmental factors. However, with equipment designed for long-range interception, individuals can capture Bluetooth communications from a much greater distance than what is generally accepted as the operational range. BlueSniper rifles, for example, are capable of detecting and intercepting signals from Bluetooth devices by using high-gain antennas and amplifiers. This capability highlights a critical aspect of security concerning wireless technologies: even well-established protocols can have vulnerabilities that could be exploited by knowledgeable attackers with the right tools. Understanding this helps illustrate the larger security concerns associated with wireless communication, emphasizing the need for proper security measures to safeguard data and communications transmitted over Bluetooth. This acknowledgment of potential exploitation is crucial for practitioners in the field of information security.

5. What does a MAC address do?

A. Identifies online services

B. Uniquely identifies each node on a network

C. Routes packets across the internet

D. Resolves hostnames to IP addresses

A MAC (Media Access Control) address plays a crucial role in networking by uniquely identifying each node on a local network. It is a hardware address that is embedded into the network interface card (NIC) of a device, such as a computer or a router. Unlike IP addresses that can change depending on the network configuration, MAC addresses remain constant and serve as a permanent identifier for devices on the same local area network (LAN). The uniqueness of the MAC address is what allows network devices to communicate with one another properly. When data packets are transmitted over the network, the MAC address is used to ensure that the information reaches the correct device. This ability to uniquely identify devices is essential for managing network traffic and maintaining efficient communication between devices. In contrast, the other options provided are functionalities that are not associated with MAC addresses: - Identifying online services pertains to service discovery on the internet and is not related to MAC addresses. - Routing packets across the internet is performed by routers using IP addresses, not MAC addresses. - Resolving hostnames to IP addresses is the function of DNS (Domain Name System), separating it further from the role of a MAC address. Overall, a MAC address is fundamental for networking, acting as a unique identifier for devices, enabling successful

SAMPLE

6. Which of the following is NOT one of the five phases of an attack?

A. Reconnaissance

B. Negotiation

C. Covering tracks

D. Gaining access

Negotiation is not recognized as one of the five phases of an attack, which typically include reconnaissance, gaining access, maintaining access, covering tracks, and the final phase of actions on objectives. The reconnaissance phase involves gathering information about the target, which is crucial for the attacker to identify potential vulnerabilities. Gaining access refers to penetrating the security mechanisms to enter the target environment. Covering tracks is essential for attackers to erase or obscure their actions to avoid detection. In contrast, negotiation does not align with these structured phases. It may imply a scenario where attackers discuss or seek terms with victims but does not fit into the primary methodology of attacking systems or networks. Understanding these phases is vital for protecting against attacks, as it allows security professionals to identify and mitigate threats at various stages of the attack lifecycle.

7. What is the purpose of likelihood and impact estimates in the risk management process?

A. To evaluate asset value

B. To identify threats

C. To assess the potential damage and frequency of threats

D. To determine response strategies

The purpose of likelihood and impact estimates in the risk management process is to assess the potential damage and frequency of threats. This assessment provides a framework for understanding how likely certain risks are to occur and the extent of their potential consequences if they do. By estimating likelihood, organizations can gauge how probable it is for specific threats to materialize. This involves analyzing historical data, trends, and contextual factors that could influence future occurrences. Impact estimates complement this by determining the severity of the potential consequences that could arise from these threats. This dual assessment allows organizations to prioritize their risks more effectively, focusing resources and mitigation strategies on the risks that are most likely to occur and that could cause the most significant damage. This comprehensive understanding is crucial in ensuring that organizations allocate their risk management efforts efficiently, thereby enhancing their overall security posture and resilience against threats.

SAMPLE

8. In Windows, what is the purpose of NTFS?

A. To provide a framework for application performance

B. To control and enforce file access permissions

C. To enable multi-user access on a network

D. To backup system files securely

The purpose of NTFS, or New Technology File System, in Windows is primarily to control and enforce file access permissions. NTFS is a file system that supports advanced data management features, including file and directory permissions, encryption, disk quota limits, and rich metadata. This allows system administrators to set specific permissions for users and groups, thus ensuring that sensitive data is only accessible by authorized individuals. By enforcing file access permissions, NTFS plays a crucial role in maintaining data security and integrity within the operating system. This is particularly important in environments where multiple users operate on a shared system or network, as it helps prevent unauthorized access and data breaches. The other responses refer to various functionalities that can be associated with file systems in a more general sense, but do not capture the primary role of NTFS regarding security and access control. While NTFS does contribute to performance, multi-user access, and data backup in broader contexts, its standout feature that distinctly marks its utility in Windows environments is its robust file access control capabilities.

9. Which term describes a condition that allows a threat to potentially exploit a system?

A. Risk

B. Vulnerability

C. Exposure

D. Incident

The term that describes a condition that allows a threat to potentially exploit a system is vulnerability. In the context of information security, a vulnerability refers to a weakness or flaw in a system, whether it's in hardware, software, or policies, that can be targeted by an attacker. When a system has an existing vulnerability, it is essentially an open door that could be exploited by threats, such as malware, unauthorized access, or data breaches. Identifying vulnerabilities is a crucial part of maintaining security because addressing these weaknesses can significantly reduce the risk of successful attacks. In contrast, risk refers to the potential for loss or damage when a threat exploits a vulnerability; exposure is the state of being open to loss or damage, and incident refers to an occurrence of a security breach or failure, which is a consequence of vulnerabilities being exploited. These terms are related but highlight different aspects of information security, making vulnerability the most accurate choice for defining the condition that allows for potential exploitation.

SAMPLE

10. What phase of an attack involves identifying assets that could be targeted for exploitation?

A. Gaining access

B. Scanning

C. Reconnaissance

D. Maintaining access

The phase of an attack that involves identifying assets that could be targeted for exploitation is the reconnaissance phase. During reconnaissance, attackers gather information about the target environment, which may include details about network infrastructure, systems, services, and vulnerabilities. This crucial step helps attackers pinpoint specific assets that could be exploited to gain further access or control. Reconnaissance can involve passive techniques, such as searching for publicly available information, or active techniques, like network scanning or social engineering. By effectively mapping out the target's assets, attackers can strategize their approach and choose the most effective methods for infiltrating the network. In contrast, other phases such as gaining access, scanning, and maintaining access are subsequent steps that build upon the foundation laid during reconnaissance. Gaining access focuses on exploiting identified vulnerabilities, scanning involves probing for open ports and services post-reconnaissance, and maintaining access deals with ensuring continued entry after an initial compromise.

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://giacgisf.examzify.com

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

SAMPLE