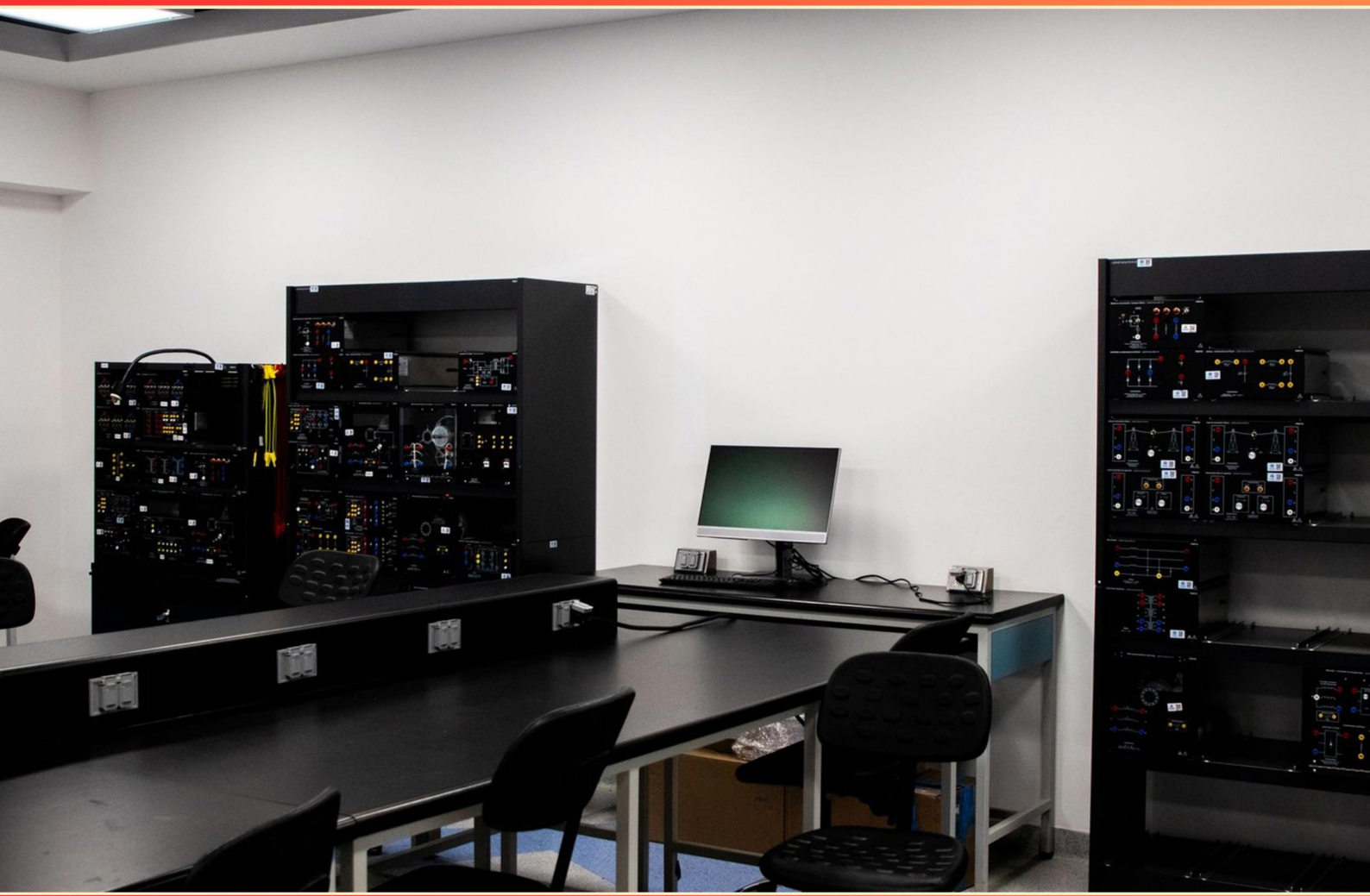
SANS GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL (GICSP) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://sansgicsp.examzify.com

Table of Contents

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.

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!

Questions

1. Which of the following is NOT a commonly recognized subtype of IDS?

A. Host Based IDS (HIDS)

B. Network Based IDS (NIDS)

C. Software Based IDS (SBIDS)

D. Signature Based IDS

2. Which type of firewalls are designed to validate OPC connection request messages?

A. Standard firewalls

B. Application-layer firewalls

C. OPC-aware firewalls

D. Proxy firewalls

3. What is a critical step in software remediation verification?

A. Scan the host with a vulnerability scanner

B. Review user feedback on software

C. Update the software to the latest version

D. Delete outdated files

4. Which account provides temporary access without the need for a permanent login?

A. Service Account

B. User Account

C. Guest Account

D. Default Account

5. What defines a socket in networking?

A. A single port used for data transmission

B. A unique pair of IP and port numbers

C. A digital signal for data transfer

D. A protocol for establishing connections

6. During a wireless network audit, what should be deleted to enhance security?

A. Guest usernames

B. Default admin passwords

C. Common connection protocols

D. User access logs

7. What is the primary difference of end-to-end encryption in comparison to link encryption?

A. It encrypts all layers of the network

B. It does not encrypt the header and trailers

C. It uses only symmetric encryption

D. It requires decryption at each network hop

8. What action does Configuration Control ensure during system implementation?

A. System upgrades are performed immediately

B. Improper modifications are prevented

C. Security policies are created

D. Only network traffic is monitored

9. What is a key characteristic of UDP?

A. Connection-oriented

B. Guaranteed delivery

C. Requires more overhead

D. Connectionless

10. What follows the Eradication step in the incident handling process?

A. Lessons Learned

B. Identification

C. Recovery

D. Containment

Answers

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

Explanations

1. Which of the following is NOT a commonly recognized subtype of IDS?

A. Host Based IDS (HIDS)

B. Network Based IDS (NIDS)

C. Software Based IDS (SBIDS)

D. Signature Based IDS

The concept of Intrusion Detection Systems (IDS) encompasses various subtypes that classify how they operate and monitor for potential threats. Among the recognized types are Host Based IDS (HIDS) and Network Based IDS (NIDS), both of which reflect the specific areas they monitor. HIDS operates on specific devices, monitoring activities and system calls to detect malicious behavior, while NIDS examines the network traffic to identify threats across the entire network. Signature Based IDS is another valid subtype that assesses traffic based on known patterns (or signatures) of malicious activity. This method relies on a database of known attack signatures to identify and alert on intrusions. While there are various ways to categorize IDS, "Software Based IDS (SBIDS)" is not recognized as a standard subtype within the field. The term does not refer to a specific operational model or distinct approach that would be universally acknowledged in the cybersecurity community. It doesn't specify a method related to how an IDS functions, making it lesser-known and less formally categorized compared to the other types. Thus, it fits the context of being NOT a commonly recognized subtype of IDS.

2. Which type of firewalls are designed to validate OPC connection request messages?

A. Standard firewalls

B. Application-layer firewalls

C. OPC-aware firewalls

D. Proxy firewalls

OPC-aware firewalls are specifically designed to understand and manage the nuances of OPC (OLE for Process Control) communication. OPC is a set of standards that enables the interoperability of various devices and software within industrial environments. Because OPC connections use specific messaging protocols and data structures, firewalls that are not designed with this in consideration may not effectively filter or manage these requests. The primary function of OPC-aware firewalls is to validate OPC connection requests, ensuring that they adhere to the correct format and contain the necessary authentication information. By validating these messages, OPC-aware firewalls can prevent unauthorized access and potential cyber threats that could exploit vulnerabilities in OPC communications. Other firewall types, like standard firewalls, primarily work on the basis of IP addresses, ports, and simple packet filtering. Application-layer firewalls do inspect some application-level data but may not specifically recognize the intricacies of OPC protocols. Proxy firewalls act as intermediaries for requests but do not have tailored capabilities for handling OPC messages. Thus, the specificity and tailored functionality of OPC-aware firewalls make them the appropriate choice for validating OPC connection requests.

3. What is a critical step in software remediation verification?

A. Scan the host with a vulnerability scanner

B. Review user feedback on software

C. Update the software to the latest version

D. Delete outdated files

A critical step in software remediation verification is to scan the host with a vulnerability scanner. This process involves using a specialized tool to identify any remaining vulnerabilities in the software after remediation efforts have been applied. It assesses the effectiveness of the actions taken, such as updates or patches, ensuring that the software is no longer susceptible to known exploits. The use of a vulnerability scanner provides a systematic method to verify that all security measures have been successfully implemented and that there are no additional vulnerabilities present. This step is essential for maintaining the security posture of systems, especially in an industrial context where software vulnerabilities can have significant operational impacts. While reviewing user feedback on software, updating the software to the latest version, or deleting outdated files can be helpful practices, they do not specifically serve as verification steps to confirm that remediation actions were successful. They may contribute to overall software management and security hygiene but do not offer the concrete validation that scanning does. Therefore, scanning with a vulnerability scanner stands out as the necessary step in confirming successful software remediation.

4. Which account provides temporary access without the need for a permanent login?

A. Service Account

B. User Account

C. Guest Account

D. Default Account

The guest account is designed to provide temporary access to a system or network without the need for a permanent login. This type of account allows users to access certain resources without having their own dedicated credentials, making it suitable for situations where a user needs short-term access, such as visitors or contractors who require limited interaction with the system. Guest accounts typically come with restrictions to ensure security, such as limited permissions and access to only specific areas of the system. This helps maintain the integrity and security of the system while still accommodating temporary users. In contrast, service accounts are used for automated processes or services that need continuous access to certain resources, as they require a permanent set of credentials. User accounts are generally assigned to individuals for regular use and often involve permanent access rights. Default accounts typically refer to preconfigured accounts that come with software or hardware, whose access levels can vary but are not specifically meant for temporary users. Therefore, the guest account is specifically intended for those who need short-term access without a permanent login, making it the most appropriate choice among the options provided.

5. What defines a socket in networking?

A. A single port used for data transmission

B. A unique pair of IP and port numbers

C. A digital signal for data transfer

D. A protocol for establishing connections

A socket in networking is indeed defined as a unique pair of IP and port numbers. This pairing allows specific processes to communicate over a network. The IP address identifies a device on the network, while the port number identifies a specific service or application running on that device. When combined, they create a socket that enables sending and receiving data between applications across the network. This concept is fundamental in enabling multiple services to run on a single IP address by differentiating them through their port numbers. Each socket is essentially a communication endpoint that allows for a specific, directed communication channel, ensuring that data sent over the network reaches the correct destination and service. Other choices do not accurately define a socket. A single port alone does not represent the complete context of communication, as it lacks the necessary IP address which is crucial for identifying the specific machine. A digital signal is more about the physical layer of communication rather than the networking concepts of sockets. Similarly, protocols are important for establishing and managing connections, but they are separate from the definition and function of a socket itself.

6. During a wireless network audit, what should be deleted to enhance security?

A. Guest usernames

B. Default admin passwords

C. Common connection protocols

D. User access logs

Deleting default admin passwords is a crucial step in enhancing security during a wireless network audit. Default passwords are often well-known and widely available, making them a prime target for attackers. Many devices and software applications come with preset passwords that are easy to guess or find online. If these are not changed, unauthorized individuals could gain access to the network and its resources, leading to potential breaches, data theft, or other malicious activities. By removing or, more accurately, replacing default admin passwords with strong, unique credentials, the security of the network is significantly improved. It is a foundational practice in cybersecurity to ensure that any networked device has been appropriately secured before being deployed. In the context of other choices, while guest usernames might be managed for security, and user access logs might be important for monitoring and auditing, the immediate threat posed by default admin passwords warrants their deletion to protect against unauthorized access. Common connection protocols may also need assessment, but simply deleting them may not be the best approach; rather, they should be secured or replaced as necessary.

7. What is the primary difference of end-to-end encryption in comparison to link encryption?

A. It encrypts all layers of the network

B. It does not encrypt the header and trailers

C. It uses only symmetric encryption

D. It requires decryption at each network hop

The primary difference of end-to-end encryption compared to link encryption lies in the way data is protected throughout its journey across the network. End-to-end encryption focuses on securing the actual payload of the data being transmitted, ensuring that only the intended recipients can read the content, regardless of the intermediate nodes the data passes through. This means that while the headers and trailers necessary for the routing and delivery of the message remain unencrypted, the actual data remains private and secure. In contrast, link encryption encrypts data at each individual link in the network. This method means that the data is decrypted at each hop along the network route, exposing the content to potential unauthorized access at those points. Thus, with end-to-end encryption, the data maintains confidentiality from the sender to the receiver, and only those two parties can decrypt and access the content, while the intermediate nodes do not see the information in its encrypted form. By understanding this, it becomes clear why the statement that end-to-end encryption does not encrypt the header and trailers is a defining characteristic of its approach to securing data transmission.

8. What action does Configuration Control ensure during system implementation?

A. System upgrades are performed immediately

B. Improper modifications are prevented

C. Security policies are created

D. Only network traffic is monitored

Configuration Control is a crucial aspect of system implementation because it focuses on managing and maintaining the integrity of system configurations throughout the development and operational phases. By ensuring that only authorized changes are made to the system, Configuration Control effectively prevents improper modifications. This includes monitoring changes to software, hardware, and associated documentation to protect the system from unapproved alterations that could lead to vulnerabilities, operational disruptions, or non-compliance with industry standards. Maintaining control over configurations helps organizations reduce the risk associated with unvalidated or unauthorized changes that can compromise system security or operational effectiveness. This systematic approach ensures that any modifications are in line with predefined standards and that potential impacts are thoroughly assessed before implementation. On the other hand, the other options focus on different aspects or imply actions that do not align with the primary purpose of Configuration Control. For instance, performing system upgrades immediately does not reflect careful consideration and planning which Configuration Control advocates. Creating security policies is a foundational task but does not pertain directly to the controlled management of current system configurations. Monitoring only network traffic does not encompass the broader scope of tracking and managing system configurations, which is the core function of Configuration Control.

9. What is a key characteristic of UDP?

A. Connection-oriented

B. Guaranteed delivery

C. Requires more overhead

D. Connectionless

A key characteristic of UDP, or User Datagram Protocol, is that it is connectionless. This means that UDP does not establish a connection before sending data and does not maintain a connection during communication. Each data packet, known as a datagram, is sent independently, and the protocol does not ensure that packets arrive in order or that they arrive at all. This characteristic makes UDP faster than connection-oriented protocols like TCP (Transmission Control Protocol), which establish a connection and guarantee delivery of packets. The lack of a connection setup also means that UDP has less overhead, making it suitable for applications where speed is more critical than reliability, such as video streaming or online gaming. The other characteristics associated with UDP – such as not guaranteeing delivery or ordering – further emphasize its connectionless nature, contrasting significantly with protocols that require a connection for communication.

10. What follows the Eradication step in the incident handling process?

A. Lessons Learned

B. Identification

C. Recovery

D. Containment

Following the Eradication step in the incident handling process, the Recovery step is crucial as it focuses on restoring affected systems and services to normal operation after an incident has been dealt with. This involves not only bringing systems back online but also ensuring they are clean and secured against the vulnerabilities that were exploited during the incident. The goal during Recovery is to validate that all malicious activity has been removed and that the systems are functioning correctly and securely. This step is essential to minimize downtime and restore functionality, allowing organizations to return to business as usual while maintaining security vigilance and ensuring such incidents do not occur in the future. It emphasizes the importance of thorough testing and monitoring as part of the recovery efforts to ensure that systems are fully operational and secure.

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://sansgicsp.examzify.com

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