CREST PRACTITIONER SECURITY ANALYST (CPSA) PRACTICE (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://crest-cpsa.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 primary function of the SNMP 'Trap' response?

A. To set a value

B. To asynchronously inform the manager of an event

C. To retrieve a single value

D. To change a value

2. Which port is associated with the Border Gateway Protocol (BGP)?

A. 179

B. 389

C. 443

D. 80

3. Which object identifier pertains to the software name according to the standard format?

A. 1.3.6.1.2.1.25.4.2.1.4

B. 1.3.6.1.2.1.25.1.6.0

C. 1.3.6.1.2.1.25.6.3.1.2

D. 1.3.6.1.2.1.77.1.2.25

4. What is the role of IANA in networking?

A. Managing domain names

B. Assigning public IP addresses

C. Overseeing internet standards

D. Distributing software updates

5. What is the full form of CDMA in telecommunications?

A. Common Division Multiple Access

B. Code Division Multiple Access

C. Carrier Division Multiple Access

D. Code Data Multiple Access

6. What is the main purpose of DHCP in networking?

A. Allocates IP addresses to devices on a network

B. Connects networks and routes traffic

C. Secures wireless communications

D. Manages VLAN information

SAMPLE

7. Which of the following protocols helps in the secure identity verification of nodes over a non-secure network?

A. Network Time Protocol

B. Post Office Protocol version 3

C. Kerberos

D. Remote Procedure Call

8. Which wireless protocol is associated with Bluetooth technology?

A. 802.11b

B. 802.15

C. 802.11n

D. 802.11g

9. What does NFS stand for?

A. Network File System

B. Network Function System

C. Network File Storage

D. Network Function Storage

10. What are VLANs primarily used for in networking?

A. Switching protocols

B. Logical segmentation of a network

C. Routing between networks

D. Utilizing analog signals

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the primary function of the SNMP 'Trap' response?

A. To set a value

B. To asynchronously inform the manager of an event

C. To retrieve a single value

D. To change a value

The primary function of the SNMP (Simple Network Management Protocol) 'Trap' response is to asynchronously inform the manager of an event. In the context of SNMP, a trap is a type of message that is sent from an SNMP agent to an SNMP manager without being explicitly requested. This mechanism allows the agent to alert the manager about significant events or changes in device status, such as faults, changes in configurations, or breaches of predefined thresholds. By using traps, the SNMP manager doesn't have to continuously poll devices for their status; instead, it can receive real-time notifications about important issues as they occur. This is particularly useful for maintaining network security and performance, as it allows for quicker responses to incidents and abnormalities. The other answer choices do not align with the function of traps. Setting or changing values pertains to SNMP set commands, which are used to modify the configuration of a device. Retrieving a single value relates to SNMP get commands, which are designed to request specific data from managed devices. Therefore, the unique capability of traps to notify the manager automatically and without polling makes option B the correct choice.

2. Which port is associated with the Border Gateway Protocol (BGP)?

A. 179

B. 389

C. 443

D. 80

The port associated with the Border Gateway Protocol (BGP) is 179. BGP is a standardized exterior gateway protocol used to exchange routing information between different autonomous systems on the Internet. The choice of port 179 for BGP is well-established and is specified in the Internet Assigned Numbers Authority (IANA) service name and port number registry. In the context of networking, port numbers are crucial for establishing communication between different services and applications. The specific allocation of port numbers helps ensure that data sent over the internet reaches its intended destination without interference from other services. For BGP, using port 179 allows routers and networking equipment to listen for BGP messages and properly manage the exchange of routing information across diverse networks. Other ports listed, such as 389, 443, and 80, are used for different networking protocols and services (LDAP, HTTPS, and HTTP respectively) and are not related to BGP. Each of these protocols has its designated port to facilitate specific types of communication, further emphasizing the importance of using the correct port for the intended protocol.

SAMPLE

3. Which object identifier pertains to the software name according to the standard format?

A. 1.3.6.1.2.1.25.4.2.1.4

B. 1.3.6.1.2.1.25.1.6.0

C. 1.3.6.1.2.1.25.6.3.1.2

D. 1.3.6.1.2.1.77.1.2.25

In the context of object identifiers (OIDs) used in network management, the correct choice reflects the standard defined structure for retrieving software names. The OID pertaining to software names is specifically designed within the management information base (MIB) to allow for consistent identification and enumeration of installed software on systems. The chosen identifier, which is associated with software name, delineates software components effectively and enables network management systems to query and represent this information in a standardized manner. This is pivotal for functions such as inventory management, compliance tracking, and audit trails concerning the software present on devices. The other identifiers relate to different aspects of network management: some may pertain to system uptime, performance metrics, or different types of data that do not directly correspond to the software name. This distinction is crucial for identifying the correct OID that provides software identification data specifically, which directly aligns with the requirements stated in the question.

4. What is the role of IANA in networking?

A. Managing domain names

B. Assigning public IP addresses

C. Overseeing internet standards

D. Distributing software updates

The role of the Internet Assigned Numbers Authority (IANA) in networking primarily involves assigning public IP addresses. IANA is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources. This organization manages the allocation of IP address space for various entities, ensuring that each device connected to the Internet has a unique address through the assignment of public IP addresses. This function is crucial for maintaining the integrity of the Internet and preventing address conflicts, which can lead to connectivity issues. IANA also plays a part in the coordination of autonomous system numbers (ASNs) and other registry-related duties necessary for effective internetworking. While managing domain names, overseeing internet standards, and distributing software updates are essential for the broader functioning of the Internet, these responsibilities fall under the purview of other organizations or entities, such as the Internet Corporation for Assigned Names and Numbers (ICANN) for domain names and various standard-setting organizations for internet protocols.

SAMPLE

5. What is the full form of CDMA in telecommunications?

A. Common Division Multiple Access

B. Code Division Multiple Access

C. Carrier Division Multiple Access

D. Code Data Multiple Access

The term CDMA in telecommunications stands for Code Division Multiple Access. This technology is a channel access method used by various radio communication technologies. It allows multiple signals to occupy a single transmission channel, optimizing the use of available bandwidth. In CDMA, each user is assigned a unique code that modulates their signal. This enables multiple users to share the same frequency band without interfering with each other's transmissions. The code used for each user ensures that their communication can be separated and decoded at the receiver's end, even when all users transmit simultaneously. This efficient use of spectrum and ability to handle many simultaneous calls makes CDMA a popular choice in wireless communication systems, particularly in mobile networks. Understanding the principles of CDMA is crucial for grasping how modern digital cellular systems operate, as well as for recognizing its significance in the evolution of telecommunication technologies.

6. What is the main purpose of DHCP in networking?

A. Allocates IP addresses to devices on a network

B. Connects networks and routes traffic

C. Secures wireless communications

D. Manages VLAN information

The primary purpose of DHCP, or Dynamic Host Configuration Protocol, in networking is to allocate IP addresses to devices on a network dynamically. When a device connects to a network, it requires an IP address to communicate with other devices. DHCP facilitates this by automating the process. It allows the network administrator to configure a range of IP addresses that can be assigned to devices, thereby ensuring that IP addresses are distributed without manual intervention. This process not only simplifies network management but also helps prevent IP address conflicts, as DHCP keeps track of which addresses are in use and which are available. Additionally, DHCP can provide other information such as the subnet mask, default gateway, and DNS server addresses, which are essential for proper network configuration and communication. In contrast, connecting networks and routing traffic pertains to the function of routers and switches. Securing wireless communications involves different protocols and technologies that focus on encryption and authentication. Managing VLAN information relates to how network segmentation is implemented to improve performance and security but is not a core function of DHCP.

SAMPLE

7. Which of the following protocols helps in the secure identity verification of nodes over a non-secure network?

A. Network Time Protocol

B. Post Office Protocol version 3

C. Kerberos

D. Remote Procedure Call

The correct choice for secure identity verification of nodes over a non-secure network is Kerberos. This protocol is specifically designed to provide secure authentication and ensure that both users and services can verify each other's identities before establishing a connection. Kerberos operates on the principle of tickets that are issued by a trusted third-party authentication server. When a client wants to access a service, it first requests a ticket from this server, which it uses to prove its identity to the service it wishes to access. This process protects credentials by ensuring they are never sent over the network in plaintext, thus providing strong protection against eavesdropping and replay attacks. In general, other options do not serve the same purpose. For instance, the Network Time Protocol is primarily used for clock synchronization rather than identity verification. The Post Office Protocol version 3 is designed for retrieving emails from a server and also lacks mechanisms for secure node identification. Finally, Remote Procedure Call focuses on allowing programs to execute code on a remote server rather than providing identity verification. This delineation underscores why Kerberos is the appropriate protocol for secure identity verification in this context.

8. Which wireless protocol is associated with Bluetooth technology?

A. 802.11b

B. 802.15

C. 802.11n

D. 802.11g

The choice associated with Bluetooth technology is indeed linked to the 802.15 specification. This standard outlines the protocols for short-range wireless connectivity and is designed for personal area networks (PAN). Bluetooth operates within this standard, allowing various devices to communicate wirelessly over short distances, typically within a range of about 10 meters. In contrast, the other options pertain to wireless local area networks (WLAN) and are part of the 802.11 family of protocols. These are primarily used for networking and internet access over broader distances, focusing on higher data rates and connectivity capabilities compared to the short-range approach of Bluetooth. Specifically, 802.11b, 802.11g, and 802.11n address different generations and improvements in wireless LAN technology, but none are suitable for Bluetooth functionality.

9. What does NFS stand for?

A. Network File System

B. Network Function System

C. Network File Storage

D. Network Function Storage

NFS stands for Network File System, which is a distributed file system protocol commonly used in UNIX and Linux environments to allow a user on a client computer to access files over a network in the same way they access local storage. NFS enables sharing of directories and files and allows for easy data management across multiple systems. It operates on the client-server model, facilitating the sharing of files between devices connected over a network, without requiring users to understand the complexities of the underlying network protocols. The other options do not accurately describe NFS. "Network Function System" suggests a different context that is not related to file sharing, while "Network File Storage" and "Network Function Storage" imply storage solutions that lack the specific functionality and architecture detailed in the original NFS.

SAMPLE

10. What are VLANs primarily used for in networking?

A. Switching protocols

B. Logical segmentation of a network

C. Routing between networks

D. Utilizing analog signals

VLANs, or Virtual Local Area Networks, are primarily used for the logical segmentation of a network. This segmentation allows network administrators to create separate networks within the same physical infrastructure, which can improve performance and enhance security. By grouping devices into distinct VLANs, traffic can be isolated, meaning that a broadcast from one VLAN does not affect devices in another VLAN. This isolation also helps in managing network policies, optimizing bandwidth usage, and establishing different sets of security measures for different user groups or departments without requiring changes to the physical layout of the network. The other options do not accurately reflect the primary function of VLANs. For example, switching protocols pertain more to the methods by which data is forwarded in a network and are not specific to VLANs. Routing between networks refers to the process of directing packets between different networks, which involves Layer 3 processes rather than the Layer 2 functionalities that VLANs participate in. Utilizing analog signals is not relevant in the context of VLANs, as they deal with digital data and the logical organization of networks, not analog signal transmission.

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://crest-cpsa.examzify.com

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

SAMPLE