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

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 port is used for JetDirect services?

A. 9100

B. 9200

C. 9001

D. 8000

2. What is the purpose of the host.equiv file in a Unix-like system?

A. To configure user permissions for network access

B. To store host keys for SSH authentication

C. To manage firewall rules for connected devices

D. To log system events for security auditing

3. What does TKIP aim to replace?

A. AES

B. WEP

C. SSL

D. IPSec

4. Which of the following describes the nature of an NTLM hash?

A. It stores user credentials securely

B. It uses symmetric encryption for data privacy

C. It is a single-use hashed value

D. It generates a unique identifier for network routes

5. What improvement does NTLM offer over the original LM hash?

A. Faster processing speed

B. More secure password storage

C. Supports longer passwords

D. Less dependency on network resources

6. Which command retrieves the top row of all tables in MS-SQL?

A. SELECT name FROM sysobjects

B. SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA.TABLES

C. SELECT * FROM INFORMATION_SCHEMA.COLUMNS

D. SELECT name FROM master..sysdatabases

SAMPLE

7. What is the main characteristic of multicast transmission?

A. A message is delivered to all network devices

B. A message is sent to a specific device only

C. A message is delivered to a group of hosts

D. A message is sent to the network's router

8. IPv6 was developed primarily to address which issue?

A. Insufficient security in networking protocols

B. IP address exhaustion

C. Lack of data transfer speed

D. Complicated address management

9. IIS 7 defaults are found in which version of Windows?

A. Windows 7

B. Windows Vista, Server 2008

C. Windows Server 2012

D. Windows 8

10. Which description fits the term "autonomous system" in networking?

A. A network controlled by multiple administrators

B. A network with no external connections

C. A network under a single administrative control

D. A network that only operates with internal devices

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which port is used for JetDirect services?

A. 9100

B. 9200

C. 9001

D. 8000

The correct choice, which is associated with JetDirect services, is 9100. This port is commonly used for printing services via the Internet Printing Protocol (IPP) and for networked printers, particularly those that are connected using HP's JetDirect technology. JetDirect allows printers to connect directly to an IP network, facilitating the process of sending print jobs over the network without requiring a dedicated print server. The use of port 9100 is widely accepted in the industry for these purposes, making it a standard for many printer manufacturers as well. This port enables efficient communication between print clients and printers, allowing for quick and reliable job processing. Other ports mentioned in the options serve different functions or are not commonly associated with JetDirect services. For instance, port 9200 may be used for various applications, while ports 9001 and 8000 are typically designated for different services or protocols, such as web applications or service-specific communications. Thus, the selection of port 9100 highlights its specific role in enabling JetDirect service operations within networked printing environments.

2. What is the purpose of the host.equiv file in a Unix-like system?

A. To configure user permissions for network access

B. To store host keys for SSH authentication

C. To manage firewall rules for connected devices

D. To log system events for security auditing

The host.equiv file in a Unix-like system is primarily used to allow user access to remote systems without the need for a password, effectively authorizing users from specified host machines based on the entries in this file. When the system checks this file, it validates whether a user attempting to connect from a listed host should be granted access, thus facilitating seamless communication and file sharing between trusted hosts. This method enhances user convenience, particularly in environments where frequent connections between certain hosts are necessary. It is important to note, however, that while it simplifies access management, it can also introduce security risks if not properly managed, as any misconfiguration could allow unauthorized access. The other options focus on different aspects of system security and administration. Configuring user permissions for network access relates to more granular access control mechanisms that may not utilize the host.equiv file. Storing host keys for SSH authentication pertains to a different security protocol that relies on public-private key pairs rather than host-based access control. Managing firewall rules is a critical function for controlling network traffic but operates separately from the purpose of the host.equiv file. Similarly, logging system events for security auditing involves tracking system operations and is typically handled through different logging mechanisms rather than through the host.equiv file.

SAMPLE

3. What does TKIP aim to replace?

A. AES

B. WEP

C. SSL

D. IPSec

TKIP, or Temporal Key Integrity Protocol, was introduced as a part of the IEEE 802.11i standard to enhance the security of wireless networks. It specifically aims to replace WEP, which is Wired Equivalent Privacy, a protocol that was widely used but had significant security vulnerabilities. WEP utilized static encryption keys, making it susceptible to various attacks such as key reuse and IV (Initialization Vector) attacks. TKIP addresses these vulnerabilities by implementing a per-packet keying mechanism, which generates a unique encryption key for each data packet. This improvement provides a stronger level of security for wireless communication by ensuring that even if one key is compromised, it does not jeopardize the security of subsequent packets. In contrast, options like AES (Advanced Encryption Standard), SSL (Secure Sockets Layer), and IPSec (Internet Protocol Security) serve different roles and contexts in the security infrastructure. AES is a symmetric encryption standard that can be used independently of TKIP. SSL is a protocol for establishing secure connections over a computer network, often used in web communications, while IPSec is used primarily for securing IP communications by authenticating and encrypting each IP packet. None of these directly relate to the specific improvements TKIP brings to replace WEP's weaknesses.

4. Which of the following describes the nature of an NTLM hash?

A. It stores user credentials securely

B. It uses symmetric encryption for data privacy

C. It is a single-use hashed value

D. It generates a unique identifier for network routes

The nature of an NTLM hash primarily involves its role in storing user credentials securely. NTLM, or NT LAN Manager, is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users and systems across networks. The NTLM hash is a one-way encrypted representation of a user's password, and while it is not impervious to attacks—particularly to hash cracking and rainbow table attacks—it does serve the essential function of protecting the user's password during the authentication process by storing it in a non-reversible format. The use of this hash format means that even if an attacker manages to access the hash values, they cannot easily reconstruct the original passwords, which provides a layer of security. Nonetheless, it is important to note that best practices recommend stronger authentication methods, as NTLM is considered more vulnerable than newer protocols such as Kerberos. The other options do not accurately represent the attributes of NTLM hashes. For instance, NTLM does not use symmetric encryption; instead, it relies on hashing. Additionally, it is not a single-use hashed value, as it can be consistently used until the corresponding password changes. Finally, it does not generate unique identifiers for network routes, which falls outside its functional scope. Thus, the correct choice underscores the

SAMPLE

5. What improvement does NTLM offer over the original LM hash?

A. Faster processing speed

B. More secure password storage

C. Supports longer passwords

D. Less dependency on network resources

The correct answer focuses on the enhancement in security provided by NTLM compared to the original LM hash. NTLM, or NT LAN Manager, improves upon the security of password storage by employing a more robust hashing algorithm. This enhancement addresses several vulnerabilities inherent to the LM hashing method. The LM hash is significantly weaker due to its reliance on a simpler hashing algorithm and its limitations, such as converting the entire password to uppercase and restricting it to a maximum of 14 characters. In contrast, NTLM allows for the use of passwords that are not only longer but also preserve case sensitivity, thus increasing the complexity and strength of the hash. This makes it considerably more difficult for attackers to crack passwords, leading to enhanced protection against brute-force attacks. In summary, NTLM offers better password security by utilizing a more advanced approach to hashing, which fundamentally improves the security posture of systems utilizing NTLM compared to those using LM hashes.

6. Which command retrieves the top row of all tables in MS-SQL?

A. SELECT name FROM sysobjects

B. SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA.TABLES

C. SELECT * FROM INFORMATION_SCHEMA.COLUMNS

D. SELECT name FROM master..sysdatabases

The command that retrieves the top row of all tables in MS-SQL is indeed the second option, as it effectively utilizes the INFORMATION_SCHEMA.TABLES view, which contains metadata about all the tables in the database. The inclusion of the "TOP 1" clause ensures that only one table name is returned, making it clear and concise for retrieving a sample entry from the entirety of the tables present. Gathering metadata from the INFORMATION_SCHEMA views is a standard practice in SQL, as these views provide a standardized way to access database schema information that is compatible across different database systems. By focusing on retrieving the TABLE_NAME, it directly points to the names of tables, which is usually the first step analysts take when needing to explore the database structure or gather insights from it. The other options present different types of queries that do not achieve the goal of retrieving the top row of all tables. Some queries look for specific objects or metadata unrelated to the core requirement of obtaining actual table data, which underscores the accuracy and relevance of the chosen command.

7. What is the main characteristic of multicast transmission?

A. A message is delivered to all network devices

B. A message is sent to a specific device only

C. A message is delivered to a group of hosts

D. A message is sent to the network's router

Multicast transmission is specifically designed to send a single message to a group of hosts that are interested in receiving that message, rather than broadcasting it widely to all devices on the network or directing it to just one specific device. This is particularly efficient for applications where a message, such as a video stream or a software update, needs to reach multiple recipients without the need for replication of the transmission for each individual recipient. The essence of multicast is the ability to efficiently utilize bandwidth by allowing a sender to transmit a message just once to a designated group. This optimizes network resources and reduces unnecessary traffic. Thus, the main characteristic of multicast transmission is that it effectively delivers messages to a select group of hosts that have expressed interest in receiving them, facilitating resource sharing and better management of network traffic.

SAMPLE

8. IPv6 was developed primarily to address which issue?

A. Insufficient security in networking protocols

B. IP address exhaustion

C. Lack of data transfer speed

D. Complicated address management

The primary motivation behind the development of IPv6 was to address IP address exhaustion. With the proliferation of devices connected to the internet, the original protocol, IPv4, became inadequate due to its limited address space, which could accommodate approximately 4.3 billion unique addresses. As the number of internet-connected devices surged, it became evident that a new solution was necessary to provide a vastly larger pool of addresses. IPv6 significantly expands the address space, allowing for approximately 340 undecillion (3.4 x 10^38) unique IP addresses. This expansion not only accommodates the growing number of devices but also enables the potential for innovations in networking and the development of new applications that require unique addressing. While other issues, such as security or data transfer speed, are important considerations in network design and protocols, they were not the primary driver for the creation of IPv6. Instead, the focus was on ensuring that every device in the world could have a unique address without concerns of running out of available addresses. Thus, the enhancement of IP address capacity was key to the transition to IPv6.

9. IIS 7 defaults are found in which version of Windows?

A. Windows 7

B. Windows Vista, Server 2008

C. Windows Server 2012

D. Windows 8

The correct answer highlights that Internet Information Services (IIS) 7 defaults are found in Windows Vista and Windows Server 2008. IIS 7 was first introduced with Windows Server 2008 and was also included in Windows Vista as a feature that could be enabled. This integration was significant because it provided a more robust web server environment with improved features compared to previous versions. In Windows Vista, IIS 7 served developers and users with enhanced management features and a modular architecture that allowed components to be separated, thus making it easier to manage and extend. Similarly, Windows Server 2008 benefited from these advancements, offering enterprise-level features suitable for larger applications and services. While other options represent newer versions of Windows and IIS (like Windows Server 2012 and Windows 8), they do not pertain to the initial defaults of IIS 7. Windows 7, for example, does have IIS capabilities, but the defaults associated with IIS 7 were primarily tied to the earlier operating systems mentioned.

SAMPLE

10. Which description fits the term "autonomous system" in networking?

A. A network controlled by multiple administrators

B. A network with no external connections

C. A network under a single administrative control

D. A network that only operates with internal devices

The term "autonomous system" in networking refers specifically to a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the internet. This means that it operates as a distinct unit, managing its own routing decisions independently of other networks. This definition aligns with the concept of a network under a single administrative control, which highlights the essential characteristic of an autonomous system: that it is governed and managed by one entity, enabling consistent policy implementation and route management across all connected devices within that system. In the context of internet routing, autonomous systems communicate using specific protocols, such as BGP (Border Gateway Protocol), to exchange routing information with other networks while maintaining their own internal routing policies. This centralized control allows for better coordination, management, and security measures tailored to the organization's needs. In contrast, the other options do not capture the essence of what defines an autonomous system in networking. For instance, a network controlled by multiple administrators does not ensure a unified routing policy, while a network with no external connections would not qualify as an autonomous system since its primary characteristic is its relation to other systems in terms of routing. Similarly, a network that only operates with internal devices lacks the key element of external communication that defines an autonomous

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