CREST Practitioner Security Analyst (CPSA) Practice (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

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 act is known as the Federal Information Security Management Act?**

   A. FISMA

   B. FERPA

   C. GDPR

   D. GLBA

2. **Which protocol is associated with port 190?**

   A. Internet Key Exchange

   B. Gateway Access Control Protocol

   C. Novell Netware over IP

   D. Apple QuickTime

3. **What does the SOA record indicate in a DNS zone?**

   A. The primary domain name

   B. The authoritative name server

   C. The information on email exchange

   D. The IP associated with the zone

4. **What method is utilized in passive OS fingerprinting?**

   A. Sending crafted packets

   B. Observing network behavior and packets

   C. Scanning open ports

   D. Accessing user credentials

5. **Which port is used by the rexec protocol?**

   A. Port 23

   B. Port 21

   C. Port 512

   D. Port 80

6. **What does HTTP status code 302 indicate?**

   A. Not Found

   B. Moved Permanently

   C. Temporarily Moved

   D. Server Error

7. Which database management system uses port 1521?

A. PostgreSQL

B. Oracle

C. MySQL

D. MongoDB

8. Which type of message is known as unicast?

A. A message sent to a group of hosts

B. A message sent from one sender to multiple recipients

C. A message sent from a single sender to a single recipient

D. A message sent to all nodes in a network

9. Which of the following HTTP methods is used to request data from a specified resource?

A. POST

B. GET

C. DELETE

D. PATCH

10. What does the acronym NetBIOS stand for?

A. Network Basic Input/Output System

B. Network Basic Operating System

C. Network Binary Input/Output System

D. Network Binary Operating System

Answers

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

Explanations

1. Which act is known as the Federal Information Security Management Act?

A. FISMA

B. FERPA

C. GDPR

D. GLBA

The Federal Information Security Management Act is commonly referred to by its acronym, FISMA. This legislation was enacted to provide a comprehensive framework for protecting government information, operations, and assets against natural or man-made threats. FISMA requires federal agencies to develop, document, and implement an information security program, ensuring that they follow prescribed security standards and procedures to safeguard sensitive data effectively. FISMA emphasizes the need for regular assessments and the continuous monitoring of information systems, which is crucial for maintaining the integrity, confidentiality, and availability of government information. Its importance in the realm of cybersecurity within federal agencies is underscored by its requirement for compliance with established security frameworks. The other acts listed serve different purposes; for instance, FERPA is concerned with the privacy of student education records, GDPR pertains to data protection and privacy in the European Union, and GLBA deals with the financial privacy of consumers. Understanding the specific focus of each act is essential for recognizing why FISMA is correctly identified as the Federal Information Security Management Act.

2. Which protocol is associated with port 190?

A. Internet Key Exchange

B. Gateway Access Control Protocol

C. Novell Netware over IP

D. Apple QuickTime

The correct association of port 190 is with the Gateway Access Control Protocol (GACP). This protocol plays a role in managing the access control for multimedia gateways, particularly in VoIP (Voice over Internet Protocol) environments. GACP is significant because it helps in establishing, managing, and terminating sessions for voice communications. By operating on port 190, GACP can effectively communicate with other network entities, ensuring that appropriate access controls are in place as voice traffic traverses through a network. In contrast, other protocols listed are associated with different ports. For example, the Internet Key Exchange is associated with port 500, used primarily for securing IPsec connections. Novell Netware over IP has its respective ports for handling file and print services, and Apple QuickTime uses different ports related to streaming multimedia content. Each of these protocols serves distinct functions and operates on specific ports outside of the Gateway Access Control Protocol's designation at port 190.

3. What does the SOA record indicate in a DNS zone?

A. The primary domain name

B. The authoritative name server

C. The information on email exchange

D. The IP associated with the zone

The SOA (Start of Authority) record plays a crucial role in DNS (Domain Name System) zone management. It indicates the authoritative name server for the DNS zone, meaning it specifies which server is the primary source of information for that zone.   This record includes important details such as the primary name server's hostname, the email address of the person responsible for the DNS zone, the zone's serial number (used for tracking changes), and timing parameters. This allows secondary name servers to know where to pull the information from and also helps maintain synchronization between the servers. While primary domain name, email exchange information, and IP addresses are important components of a DNS setup, they are not defined by the SOA record specifically. The SOA serves as the essential reference point for the whole zone, making it vital for efficient domain name resolution and management.

4. What method is utilized in passive OS fingerprinting?

A. Sending crafted packets

B. Observing network behavior and packets

C. Scanning open ports

D. Accessing user credentials

Passive OS fingerprinting involves analyzing network traffic without actively probing the target system, thereby minimizing the risk of detection and potential disruption. This method relies on observing the characteristics of the packets that are already being sent to and from the network, such as the timing, sizes, and flags set within the packets. By gathering this data, security analysts can infer the operating system and its version based on known signatures and behaviors associated with various OS implementations. This technique is particularly useful in environments where stealth is necessary, as it does not introduce any additional traffic that would alert the target system. Therefore, passive OS fingerprinting is a non-intrusive approach that allows analysts to collect valuable information while remaining under the radar.

5. Which port is used by the rexec protocol?

A. Port 23

B. Port 21

C. Port 512

D. Port 80

The rexec protocol, which stands for Remote Execution, uses port 512. This protocol is part of the suite of services that allow users to execute commands on remote computers over the network securely. The use of port 512 is standardized for rexec, ensuring that any software utilizing this protocol will communicate through this specific endpoint. The other port options provided are associated with different protocols and services. For example, port 23 is typically used for Telnet, which is a protocol for text-based communication over the network but does not provide the same level of security as rexec. Port 21 is designated for FTP (File Transfer Protocol), used for transferring files, while port 80 is associated with HTTP (Hypertext Transfer Protocol), which is the foundation of data communication on the web. Therefore, understanding that rexec specifically operates on port 512 is crucial for recognizing its function and ensuring proper configuration of services related to remote command execution.

6. What does HTTP status code 302 indicate?

A. Not Found

B. Moved Permanently

C. Temporarily Moved

D. Server Error

The HTTP status code 302 indicates that a resource has been temporarily moved to a different URI (Uniform Resource Identifier). When a server returns a 302 status code in response to a client request, it informs the client that the requested resource can be found at a different location for the time being. This means that the client should continue to use the original URI for future requests, as the redirection is only temporary. For example, if a user requests a page that has been temporarily relocated to a new URL, a 302 response will guide the client to the new location while indicating that it should not assume the change is permanent. This is important in web development and application behavior, enabling seamless user navigation while maintaining the original resource's accessibility. When interpreting the HTTP status codes, understanding the distinction between temporary and permanent redirection is crucial. In contrast, different status codes, such as those indicating a resource that is not found, permanently moved, or server errors, serve distinct purposes and convey different messages about the state of resources on the server.

7. Which database management system uses port 1521?

A. PostgreSQL

B. Oracle

C. MySQL

D. MongoDB

Port 1521 is the default port used by Oracle Database Management System for its SQL*Net service. This service facilitates communication between the database and applications that connect to it. The use of this specific port enables Oracle to handle client requests and manage connections effectively, ensuring data can be accessed and manipulated securely. While other database management systems like PostgreSQL, MySQL, and MongoDB have their own designated default ports—PostgreSQL uses port 5432, MySQL uses port 3306, and MongoDB uses port 27017—Oracle consistently utilizes port 1521 across various versions. This port association is crucial for systems administrators and security analysts to know, as it plays an integral role in network configuration and security protocols related to Oracle database environments.

8. Which type of message is known as unicast?

A. A message sent to a group of hosts

B. A message sent from one sender to multiple recipients

C. A message sent from a single sender to a single recipient

D. A message sent to all nodes in a network

Unicast refers to a communication method in networking where a message is sent from a single sender to a single recipient. This type of message is directed specifically and solely at one target host, ensuring that only that particular recipient receives the transmission, distinct from other forms of communication like multicast or broadcast. In the context of networking, unicast is often utilized for direct communication sessions, such as web browsing, where a user's request for a webpage is sent to the server, and the corresponding response is sent back uniquely to that user. The characteristic of unicast communication highlights its precision and the efficiency it provides in scenarios where targeted messaging is essential. Understanding this concept is crucial when considering the different communication methodologies in network design and security, as it helps determine appropriate approaches for managing data flow and analyzing potential vulnerabilities associated with distinct communication types.

9. Which of the following HTTP methods is used to request data from a specified resource?

A. POST

B. GET

C. DELETE

D. PATCH

The method used to request data from a specified resource is GET. This method is fundamental to the Hypertext Transfer Protocol (HTTP) and is primarily utilized when a client wants to retrieve data from a server.   GET requests are designed to fetch data without causing any side effects on the server, which means that making a GET request should not result in any changes to the server's state or resources. This idempotent nature allows clients to safely repeat these requests without the risk of unintended consequences. In contrast, POST is used to send data to the server to create or update a resource, which involves modifying the server's state. DELETE is specifically meant for removing a resource, while PATCH is employed to apply partial modifications to an existing resource. Each of these methods serves different purposes within the framework of HTTP, but for the task of retrieving data, GET is the appropriate choice.

10. What does the acronym NetBIOS stand for?

A. Network Basic Input/Output System

B. Network Basic Operating System

C. Network Binary Input/Output System

D. Network Binary Operating System

The acronym NetBIOS stands for Network Basic Input/Output System. This term refers to a networking industry standard that allows applications on separate computers to communicate over a local area network (LAN). Initially developed for IBM PC Networking, NetBIOS provides services related to the session layer of the OSI model, enabling communication between devices by providing a set of networking protocols that allow programs to communicate within a local network. This option accurately captures the primary function and original design intent of NetBIOS, focusing on enabling input and output operations over a network, which was critical when networked computing was developing. Understanding this concept is fundamental for security analysts, as NetBIOS can be a vector for various network security vulnerabilities and attacks.

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!