CREST Practitioner Security Analyst (CPSA) Practice (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **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

2. **What hexadecimal value corresponds to the decimal number 10?**

   A. A

   B. 10

   C. F

   D. B

3. **Which of the following protocols is used for VLAN Trunking?**

   A. STP

   B. CDP

   C. DTP

   D. VLAN

4. **Which port is associated with the Windows RPC (EPM)?**

   A. Port 88

   B. Port 135

   C. Port 110

   D. Port 123

5. **Port 5060 is primarily used for which protocol?**

   A. HTTP

   B. SIP

   C. FTP

   D. SMTP

6. **Which database management system is associated with port 5432?**

   A. MySQL

   B. MongoDB

   C. Postgres

   D. SQLite

7. **What is the classification for Windows XP 64 bit?**

   A. NT 5.1

   B. NT 5.2

   C. NT 6.0

   D. NT 4.0

8. **For IIS 5.1, which default version of Windows is used?**

   A. Windows XP

   B. Windows 2000

   C. Windows Vista

   D. Windows 7

9. **The Payment Card Industry Data Security Standard is commonly referred to as what?**

   A. PCI DSS

   B. PCI Standards

   C. Payment Security Standards

   D. Data Protection Standards

10. **Which protocol specifically supports Internet security associations?**

    A. HTTP

    B. ISAKMP

    C. SMTP

    D. IMAP

Answers

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

Explanations

1. 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.

2. What hexadecimal value corresponds to the decimal number 10?

A. A

B. 10

C. F

D. B

The hexadecimal system is a base-16 numbering system that uses the digits 0-9 to represent values zero through nine, and the letters A-F to represent values ten through fifteen. In this system, the letter 'A' directly corresponds to the decimal value of 10. Therefore, the correct answer is 'A', as it represents 10 in hexadecimal notation. The values 10, F, and B do not correspond to the decimal number 10; '10' in hexadecimal would represent 16 in decimal, 'F' corresponds to 15, and 'B' corresponds to 11. Thus, the only correct representation of the decimal value 10 in hexadecimal is 'A'.

3. Which of the following protocols is used for VLAN Trunking?

A. STP

B. CDP

C. DTP

D. VLAN

The protocol used for VLAN trunking is Dynamic Trunking Protocol (DTP). DTP is a Cisco proprietary protocol that helps to negotiate and manage trunk links between switches. It is responsible for dynamically enabling trunk links and allowing switches to automatically configure the link type, ensuring that multiple VLANs can travel over a single physical link. This is particularly useful in networks where VLANs are extensively used, allowing management of VLAN information and traffic efficiently. In contrast, the other options play different roles in a network. Spanning Tree Protocol (STP) is primarily used for preventing loops in Ethernet networks. Cisco Discovery Protocol (CDP) is used for discovering information about directly connected Cisco devices, while "VLAN" refers to Virtual Local Area Networks in general rather than a specific protocol. Therefore, DTP is the correct choice as it directly relates to VLAN trunking capabilities.

4. Which port is associated with the Windows RPC (EPM)?

A. Port 88

B. Port 135

C. Port 110

D. Port 123

Port 135 is associated with Windows Remote Procedure Call (RPC) and serves as the End Point Mapper (EPM). This port is crucial for service aggregation and communication between different network services on Windows operating systems. When a client makes a call to a service that uses RPC, it first contacts the EPM service on port 135 to determine the dynamic ports used by the requested RPC service. This design allows for more flexible communication and port management in Windows environments, enabling services to communicate without needing to know the exact port numbers in advance. The other ports mentioned—88, 110, and 123—are typically associated with different protocols. Port 88 is used for Kerberos authentication, port 110 is the default port for the Post Office Protocol version 3 (POP3) for email retrieval, and port 123 is used for the Network Time Protocol (NTP), which synchronizes clocks over a network. These ports serve different purposes and are not involved in the functions of Windows RPC.

5. Port 5060 is primarily used for which protocol?

A. HTTP

B. SIP

C. FTP

D. SMTP

Port 5060 is primarily associated with the Session Initiation Protocol (SIP), which is used for signaling and controlling multimedia communication sessions, such as voice and video calls over Internet Protocol (IP) networks. SIP is essential for establishing, maintaining, and terminating real-time sessions, which can include VoIP (Voice over Internet Protocol) communications. The use of this specific port allows devices and applications to establish connections and manage communication sessions effectively. In the context of the other protocols listed, HTTP (Hypertext Transfer Protocol) typically uses port 80 for web traffic; FTP (File Transfer Protocol) commonly operates on ports 20 and 21 for file transfer activities; and SMTP (Simple Mail Transfer Protocol) predominantly uses port 25 to handle email transmission. Each of these protocols serves distinct roles in network communication, further highlighting the unique purpose of SIP and its dedicated use of port 5060 for signaling purposes.

6. Which database management system is associated with port 5432?

A. MySQL

B. MongoDB

C. Postgres

D. SQLite

Port 5432 is the default network port for PostgreSQL, which is an object-relational database management system. This association is crucial for database administrators and analysts when configuring firewall settings, connecting applications, or troubleshooting network issues related to database access. Understanding specific ports tied to certain database systems helps in securing the environment and ensuring that only the right traffic can access the database, which is essential in maintaining data integrity and confidentiality. For the other options, MySQL primarily uses port 3306, MongoDB uses port 27017, and SQLite is a file-based database that does not operate over a network port. This distinction highlights why the choice of PostgreSQL is the correct answer.

7. What is the classification for Windows XP 64 bit?

A. NT 5.1

B. NT 5.2

C. NT 6.0

D. NT 4.0

The classification for Windows XP 64 bit is NT 5.2. Windows XP itself is built on the Windows NT architecture, and the specific versioning of Windows XP recognizes different variations based on the architecture it supports. The standard 32-bit version of Windows XP is classified as NT 5.1, while Windows XP Professional x64 Edition specifically aligns with NT 5.2 due to its ability to support 64-bit processing. This distinction is essential for understanding the technical capabilities and system requirements associated with different versions of Windows. The other classifications mentioned do not correspond to the 64-bit version of Windows XP. NT 6.0 pertains to Windows Vista, and NT 4.0 reflects an earlier generation of Windows operating systems. Understanding these classifications is crucial for identifying compatibility and features when working with various versions of Windows operating systems.

8. For IIS 5.1, which default version of Windows is used?

A. Windows XP

B. Windows 2000

C. Windows Vista

D. Windows 7

The correct answer is that IIS 5.1 is associated with the default version of Windows XP. This version of Internet Information Services (IIS) was specifically designed to work with Windows XP Professional, offering features suitable for web development and hosting on that platform. IIS 5.1 provided a platform for hosting web applications and was part of Microsoft's effort to integrate web services into their operating system packages. Windows XP, released in 2001, was aimed at providing users with a more robust and user-friendly interface, including support for web functionalities through IIS 5.1. In contrast, the other operating systems mentioned, such as Windows 2000, Windows Vista, and Windows 7, are either earlier or later versions that do not align with IIS 5.1. Windows 2000 indeed supported IIS 5.0, while Windows Vista introduced IIS 7.0, further enhancing the features and security of web hosting capabilities. Windows 7 also included newer versions of IIS, reflecting the progression in web server technology. Therefore, the specific pairing of IIS 5.1 with Windows XP makes it the appropriate choice.

9. The Payment Card Industry Data Security Standard is commonly referred to as what?

A. PCI DSS

B. PCI Standards

C. Payment Security Standards

D. Data Protection Standards

The widely recognized term for the Payment Card Industry Data Security Standard is indeed PCI DSS. This acronym stands for Payment Card Industry Data Security Standard, which outlines a collection of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. PCI DSS is critical for safeguarding sensitive payment card data against theft and fraud, providing guidelines that help organizations protect cardholder information. The use of PCI DSS as the standard terminology is vital for clear communication within the payment card industry, as it encompasses specific requirements and practices that entities must follow to comply with this standard. Understanding this term is crucial for professionals in security and compliance roles, as it is a key aspect of data security related to payment processing.

10. Which protocol specifically supports Internet security associations?

A. HTTP

B. ISAKMP

C. SMTP

D. IMAP

The protocol that specifically supports Internet security associations is ISAKMP (Internet Security Association and Key Management Protocol). ISAKMP is integral to establishing, negotiating, managing, and transferring keys and security associations used in various security protocols, most notably in conjunction with IPsec. It functions as a framework for a key management protocol rather than defining actual encryption or authentication algorithms. By enabling secure communication and negotiating security parameters, ISAKMP plays a vital role in establishing secure channels over the Internet. On the other hand, HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), and IMAP (Internet Message Access Protocol) are designed for data transmission and email communication but do not focus on security associations. They may employ security measures like TLS for secure transport, but they do not inherently provide a framework for managing security associations like ISAKMP does. Thus, ISAKMP is the clear choice for supporting Internet security associations.