CREST Practitioner Security Analyst (CPSA) Practice (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. Which port is associated with the Tor network?

A. 9000

B. 9001

C. 8080

D. 6000

2. FTP operates primarily over which type of protocol layer?

A. Application layer

B. Transport layer

C. Network layer

D. Link layer

3. Which protocol is specifically designed for secure authentication in wireless networks?

A. WPA

B. HTTPS

C. FTP

D. SMTP

4. What is the primary purpose of the Gramm-Leach-Bliley Act?

A. Ensuring the security of financial transactions

B. Protecting customer information

C. Regulating banking mergers

D. Standardizing financial disclosures

5. What function does the Post Office Protocol version 3 (POP3) serve?

A. Sending emails

B. Receiving emails

C. Synchronizing time

D. Executing remote commands

6. Which version of Windows NT corresponds to NT 3.5?

- **A. Windows NT 4.0**
- **B. Windows 2000**
- **C. Windows NT 3.51**
- **D. Windows NT 3.5**

7. What is the main purpose of using TCP?

- **A. Real-time streaming**
- **B. Quick connections**
- **C. Reliable communications**
- **D. Simple file transfers**

8. What is the role of a Name Server (NS) Record?

- **A. To specify the server's hardware configuration**
- **B. To announce authoritative name servers for a zone**
- **C. To store user access permissions**
- **D. To cache results from DNS queries**

9. What port number is associated with HTTP?

- **A. Port 80**
- **B. Port 90**
- **C. Port 8080**
- **D. Port 443**

10. Which of the following routing methods allows for real-time adjustments based on network changes?

- **A. Static Routing**
- **B. Dynamic Routing**
- **C. Hybrid Routing**
- **D. Manual Routing**

Answers

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

Explanations

1. Which port is associated with the Tor network?

A. 9000

B. 9001

C. 8080

D. 6000

The Tor network primarily uses port 9001 for its relay traffic. This port is utilized by the Tor process to establish connections between routers in the network, allowing users to access the internet anonymously. Tor is designed to enhance privacy and security by routing internet traffic through a distributed network of relays, and port 9001 plays a crucial role in facilitating this communication. While other ports mentioned in the options, like 8080 and 6000, are commonly associated with web and X11 traffic respectively, and while port 9000 can sometimes be associated with other applications or services, they are not standard for Tor's functionality. Therefore, recognizing port 9001 as the correct answer is essential for understanding the framework and operation of the Tor network.

2. FTP operates primarily over which type of protocol layer?

A. Application layer

B. Transport layer

C. Network layer

D. Link layer

FTP, or File Transfer Protocol, operates primarily at the application layer of the Internet Protocol Suite. This layer is responsible for providing network services directly to end-user applications. FTP is specifically designed to allow users to transfer files over a network, and it offers a set of commands and responses that facilitate these file transfers. By functioning at the application layer, FTP can leverage lower layers (such as the transport layer, which includes protocols like TCP) to manage the actual communication between hosts, but its core functionalities and commands, such as uploading and downloading files, are defined at the application layer. This distinction is crucial in understanding how different layers of the protocol stack work together to enable various network services.

3. Which protocol is specifically designed for secure authentication in wireless networks?

A. WPA

B. HTTPS

C. FTP

D. SMTP

The response points to WPA, which stands for Wi-Fi Protected Access, as the protocol specifically designed for secure authentication in wireless networks. WPA was created to address various security vulnerabilities found in earlier wireless protocols, such as WEP (Wired Equivalent Privacy). WPA uses strong encryption methods, primarily TKIP (Temporal Key Integrity Protocol) and, in its revised version WPA2, employs AES (Advanced Encryption Standard). Besides encryption, WPA includes mechanisms for secure authentication, protecting the integrity of data being transmitted over the wireless network and ensuring that only authorized devices can connect. In contrast, the other protocols listed serve different purposes. HTTPS is an extension of HTTP that secures the transmission of web data but is not specific to wireless networks. FTP is a protocol for transferring files between systems over a network and lacks built-in security features without additional measures. SMTP is a protocol used for sending emails and does not focus on the authentication of wireless connections. Thus, WPA is the appropriate choice for secure authentication in wireless networks, underscoring its role in protecting data integrity and user authentication in environments where wireless access is utilized.

4. What is the primary purpose of the Gramm-Leach-Bliley Act?

A. Ensuring the security of financial transactions

B. Protecting customer information

C. Regulating banking mergers

D. Standardizing financial disclosures

The primary purpose of the Gramm-Leach-Bliley Act (GLBA) is to protect customer information. Enacted in 1999, the GLBA established specific provisions that require financial institutions to provide privacy notices to their clients, informing them of how their personal information is collected, shared, and protected. This law aimed to enhance consumer privacy and data protection within the financial services sector, thus ensuring that institutions safeguard sensitive customer details. While other aspects mentioned in the choices, such as the security of financial transactions, regulating banking mergers, and standardizing financial disclosures, may be relevant to the broader context of financial regulation, they do not capture the fundamental objective of the GLBA as accurately as the focus on customer information protection. The emphasis on privacy and the obligation to maintain confidentiality underlines the act's significance in fostering trust between consumers and financial entities.

5. What function does the Post Office Protocol version 3 (POP3) serve?

A. Sending emails

B. Receiving emails

C. Synchronizing time

D. Executing remote commands

The Post Office Protocol version 3 (POP3) is primarily designed for receiving emails. It allows email clients to retrieve emails from a mail server. When a user connects to the server using POP3, the protocol facilitates the downloading of messages to the user's device, enabling offline access to their emails. POP3 operates on a client-server model where the client requests emails and the server responds by providing the messages stored. Once emails are downloaded, they can typically be deleted from the server, which is key for users who prefer to store their emails locally rather than on the server. This functionality is distinct from the roles of sending emails (handled by protocols like SMTP), synchronizing time (managed by protocols such as NTP), and executing remote commands (which can be accomplished using protocols like SSH). Thus, POP3's role as a retrieval method aligns precisely with its definition and purpose in email communication.

6. Which version of Windows NT corresponds to NT 3.5?

A. Windows NT 4.0

B. Windows 2000

C. Windows NT 3.51

D. Windows NT 3.5

The version that corresponds to NT 3.5 is indeed Windows NT 3.5 itself. Windows NT 3.5 was a significant release in the Windows NT family, introducing various enhancements over its predecessor, NT 3.1. This version focused on improving support for networking, printing, and added new features like the improved file system. In the context of the other options, Windows NT 4.0 represents a later iteration, released after NT 3.5, and brought a new user interface based on Windows 95 as well as better multimedia capabilities. Windows 2000 is a further evolution in the Windows NT line, succeeding NT 4.0 and incorporating extensive changes to both the user experience and administration features. Windows NT 3.51 is also a subsequent release that improved upon NT 3.5, adding support for new hardware and network protocols but is not directly the version that corresponds to NT 3.5. Thus, the correct connection is made by recognizing that Windows NT 3.5 explicitly refers to that particular version of the operating system.

7. What is the main purpose of using TCP?

A. Real-time streaming

B. Quick connections

C. Reliable communications

D. Simple file transfers

The main purpose of using TCP (Transmission Control Protocol) is to establish reliable communications between devices over a network. TCP is a connection-oriented protocol, meaning it establishes a connection before data can be sent. It ensures that all packets of data are sent, received, and recombined in the correct order, providing mechanisms for error checking and correction. This reliability is essential for applications where data integrity and accuracy are crucial, such as web browsing, email, and file transfers. While other options may present valid features of communication protocols, they do not underscore the primary function of TCP as effectively as reliability. For example, real-time streaming applications typically favor protocols like UDP (User Datagram Protocol) due to their lower latency despite being less reliable. Quick connections could refer more to lightweight protocols that focus on speed rather than reliability. Finally, simple file transfers can utilize timing mechanisms optimized for speed, which TCP handles, but again without emphasizing the inherent reliability that TCP is designed to provide.

8. What is the role of a Name Server (NS) Record?

A. To specify the server's hardware configuration

B. To announce authoritative name servers for a zone

C. To store user access permissions

D. To cache results from DNS queries

The role of a Name Server (NS) Record is to announce authoritative name servers for a zone. This means that the NS record specifies which DNS servers are responsible for that particular domain or zone. When a DNS resolver needs to find information about a domain, it will first look for the NS records to know which servers to contact for further queries. NS records are essential for the functioning of the Domain Name System (DNS) because they help to direct traffic appropriately and ensure that queries for domain names are resolved to the correct IP addresses by identifying the correct authoritative name servers. This supports the distributed nature of DNS, where different zones can be managed by different name servers. The other choices do not accurately describe the function of an NS record. For instance, specifying a server's hardware configuration pertains more closely to server management rather than DNS records. Storing user access permissions is typically associated with access control lists (ACLs) rather than DNS records. Caching results from DNS queries is the role of a DNS resolver or caching server, rather than an NS record. Thus, the function of announcing authoritative name servers is what distinguishes B as the correct answer.

9. What port number is associated with HTTP?

A. Port 80

B. Port 90

C. Port 8080

D. Port 443

The port number associated with HTTP is 80. This is a well-known port typically used for unencrypted web traffic. When a web browser accesses a website using the HTTP protocol, it by default connects to this port unless specified otherwise. This convention helps standardize communications on the internet, allowing servers and clients to recognize where to send and receive data. Ports like 90 and 8080 can also be used for web traffic, but they are not the default. Port 443, on the other hand, is specifically associated with HTTPS, which is the secure version of HTTP, using encryption to protect the data exchanged between the server and client. Understanding the significance of these ports is crucial for anyone working within network or web security, as it aids in configuring firewalls and correctly routing internet traffic.

10. Which of the following routing methods allows for real-time adjustments based on network changes?

A. Static Routing

B. Dynamic Routing

C. Hybrid Routing

D. Manual Routing

Dynamic routing is the correct answer because it utilizes algorithms and protocols to automatically adjust the paths that data packets take across a network in response to changing conditions. Unlike static routing, which requires manual configurations and remains fixed unless updated by an administrator, dynamic routing can detect changes in the network, such as link failures or changes in traffic load, and adapt accordingly. Dynamic routing protocols, like OSPF (Open Shortest Path First) or BGP (Border Gateway Protocol), continuously exchange information about the network's state among routers. This real-time communication allows the routers to make informed decisions about the best paths for data transmission, optimizing performance and improving redundancy. Static routing, on the other hand, does not adapt to network changes, relying solely on preset configurations. Hybrid routing combines elements of both static and dynamic methods but does not inherently provide the same level of real-time adjustment as fully dynamic routing does. Manual routing also involves fixed routes that must be individually managed and adjusted without automatic updates. These methods lack the responsiveness and flexibility that dynamic routing offers.