CREST Practitioner Security Analyst (CPSA) Practice (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. What is the main purpose of the SIP 'REGISTER' method?

A. Establish a session

B. Register a user with a SIP server

C. Terminate a session

D. Request information

2. What does an A/AAAA Record represent in DNS?

A. A type of security certificate

B. An IP address for domain resolution

C. A record for email routing

D. A method for revoking domain ownership

3. What is the key size of 3DES encryption?

A. 56 bits

B. 168 bits

C. 256 bits

D. 128 bits

4. Which of the following is a characteristic of XSS attacks?

A. They exploit the kernel vulnerabilities

B. They occur only in mobile applications

C. They utilize scripting vulnerabilities in websites

D. They require physical access to the devices

5. What is the main purpose of Dynamic Routing?

A. To manually specify routing table mappings

B. To determine the best route automatically

C. To provide redundancy in routing

D. To enhance network security

6. Which port is associated with the Tor network?

A. 9000

B. 9001

C. 8080

D. 6000

7. In the context of Linux file permissions, what represents the permissions for the group?

A. rwx

B. drwx

C. rwx

D. ---

8. Which algorithm is known for its 128-bit block size and key sizes of up to 256 bits?

A. 3DES

B. RC4

C. AES

D. Blowfish

9. Which protocol is associated with port 110?

A. SMTP

B. IMAP

C. POP3

D. FTP

10. Which of the following is not an advantage of using EAP?

A. Supports multiple authentication methods

B. Utilizes a simple username/password scheme

C. Enables use of hardware-based authentication devices

D. Provides better security in wireless communications

Answers

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

Explanations

1. What is the main purpose of the SIP 'REGISTER' method?

A. Establish a session

B. Register a user with a SIP server

C. Terminate a session

D. Request information

The primary purpose of the SIP 'REGISTER' method is to register a user with a SIP server. When a user agent (such as a SIP phone or soft client) wants to communicate over a SIP network, it needs to inform the SIP server of its address and availability. The 'REGISTER' method accomplishes this by sending information about the user agent's contact details and its current status to the server. This registration allows the SIP server to know where to send incoming calls or messages directed to that user. Once registered, the SIP server can manage routing requests, keeping track of where the user is located and ensuring communication is established effectively. This functionality is essential for SIP networks, as it enables users to be reachable regardless of their current IP address or device.

2. What does an A/AAAA Record represent in DNS?

A. A type of security certificate

B. An IP address for domain resolution

C. A record for email routing

D. A method for revoking domain ownership

The A/AAAA Record in the Domain Name System (DNS) is primarily used to map domain names to IP addresses. When you access a website, your device needs to find the corresponding IP address to connect to it, and that's where the A (Address) and AAAA (IPv6 Address) records come into play. An A record points to a specific IP address that uses the IPv4 format, which is the traditional IP address format consisting of four groups of numbers. Conversely, the AAAA record is used for IPv6 addresses, which are longer and allow for a greater number of unique IP addresses to accommodate the expanding number of devices online. Both records are essential for the domain resolution process, ensuring that users can reach websites by typing in domain names instead of numerical IP addresses. This function is crucial for the seamless operation of the internet, enabling the user-friendly experience we expect when navigating online.

3. What is the key size of 3DES encryption?

A. 56 bits

B. 168 bits

C. 256 bits

D. 128 bits

Three-Fish (3DES), or Triple DES, is a symmetric key block cipher that applies the older Data Encryption Standard (DES) algorithm three times to each data block. The key size for 3DES is 168 bits, which results from utilizing three separate DES keys, each of 56 bits. In 3DES encryption, each of the three keys is used in a sequence of encrypting and decrypting operations. While the theoretical maximum key size can include one of the keys being repeated (which would effectively make it use only 112 bits in certain configurations), the full implementation using three unique keys indeed totals to 168 bits. This enhanced key length significantly strengthens the encryption against brute-force attacks compared to the original DES, which had only a 56-bit key. This is why the key size of 3DES encryption is correctly identified as 168 bits.

4. Which of the following is a characteristic of XSS attacks?

A. They exploit the kernel vulnerabilities

B. They occur only in mobile applications

C. They utilize scripting vulnerabilities in websites

D. They require physical access to the devices

XSS (Cross-Site Scripting) attacks specifically target web applications by exploiting vulnerabilities related to the execution of scripts. The correct answer highlights this core characteristic, as XSS attacks involve injecting malicious scripts into web pages that are viewed by other users. When users load the affected web page, the malicious scripts execute within their browsers, potentially allowing attackers to steal cookies, session tokens, or other sensitive information, and to manipulate webpage content. The other choices do not accurately reflect the nature of XSS attacks. For example, kernel vulnerabilities pertain more to system-level exploits rather than issues within web applications. Additionally, restricting XSS attacks to mobile applications is misleading, since they can occur in any web environment where scripting is permitted. Lastly, XSS does not require physical access because the malicious scripts are executed remotely when users simply access the compromised web pages without the need for direct interaction with the device. Understanding these aspects illustrates how crucial it is to secure web applications against such scripting vulnerabilities.

5. What is the main purpose of Dynamic Routing?

A. To manually specify routing table mappings

B. To determine the best route automatically

C. To provide redundancy in routing

D. To enhance network security

The main purpose of dynamic routing is to determine the best route automatically. Dynamic routing protocols allow routers to communicate with each other and share information about network topology changes and the status of network paths. This enables routers to automatically update their routing tables based on the most efficient paths available at any given time. Dynamic routing is particularly beneficial in larger and more complex networks, where manual configuration of static routes would be cumbersome and prone to errors. With dynamic routing, routers can adapt to changes such as network congestion, link failures, or the addition of new network segments, thereby optimizing data transmission by selecting the most efficient routes on-the-fly. While redundancy, enhanced security, and manual routing are important aspects of network management, they do not capture the primary function of dynamic routing, which is the automatic determination of optimal routing paths in response to the network's current state.

6. 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.

7. In the context of Linux file permissions, what represents the permissions for the group?

A. rwx

B. drwx

C. rwx

D. ---

In Linux file permissions, the representation for the permissions assigned to the group typically appears in a specific format. Permissions are shown as a series of characters that denote read (`r`), write (`w`), and execute (`x`) access for the user, group, and others, usually in that order. When you see `rwx`, it designates that the group has read (r), write (w), and execute (x) permissions. This combination indicates that members of the group can perform any action on the file or directory, including viewing its contents, modifying it, and executing it as a program. The presence of `drwx` indicates that it is a directory (the leading `d` signals this) and still includes the same permissions for the group, but it also includes the user's permissions alongside it. In this context, the permissions specifically for the group are shown solely as `rwx`, reflecting that full access is granted to the group members. The option that represents the group's permissions accurately, without additional context from user or others, is indeed `rwx`. The other option, `---`, signifies that the group has no permissions at all, while `drwx` indicates a directory and combines permissions for both the

8. Which algorithm is known for its 128-bit block size and key sizes of up to 256 bits?

A. 3DES

B. RC4

C. AES

D. Blowfish

The algorithm recognized for its 128-bit block size and key sizes ranging up to 256 bits is the Advanced Encryption Standard (AES). AES was established as a symmetric encryption standard by the National Institute of Standards and Technology (NIST) and has become widely adopted due to its strength and efficiency. It operates using block ciphers, which process fixed-size blocks of data—in this case, 128 bits. One of the key features of AES is its flexibility in key sizes, which can be 128, 192, or 256 bits. The option of using a 256-bit key size offers enhanced security and is particularly useful in environments where higher security levels are necessary. While the other algorithms listed also serve as encryption methods, they either do not match the specified block size or key size or are used in different circumstances. For example, 3DES uses a block size of 64 bits, RC4 is a stream cipher and utilizes variable-size keys but does not work with fixed block sizes, and Blowfish has a block size of 64 bits as well. Therefore, AES stands out as the correct choice based on the specific attributes noted in the question.

9. Which protocol is associated with port 110?

A. SMTP

B. IMAP

C. POP3

D. FTP

The protocol associated with port 110 is POP3, which stands for Post Office Protocol version 3. POP3 is used primarily for retrieving emails from a mail server. When a client connects to a mail server using POP3, it requests to download emails stored on the server so that the client can read them offline. The importance of port 110 lies in its designation for this specific protocol, making it essential for email retrieval tasks. Unlike other protocols, POP3 allows users to download emails and usually deletes them from the server after retrieval, although some configurations can leave a copy. This is in contrast to other email retrieval protocols like IMAP, which uses a different port (usually port 143 or 993 for secure connections) and maintains emails on the server, thus enabling users to manage their emails across multiple devices. Understanding these protocols and their corresponding ports is crucial for network configurations, troubleshooting connectivity issues, and ensuring the correct setup for email services.

10. Which of the following is not an advantage of using EAP?

A. Supports multiple authentication methods

B. Utilizes a simple username/password scheme

C. Enables use of hardware-based authentication devices

D. Provides better security in wireless communications

The option regarding the use of a simple username/password scheme is identified correctly as not being an advantage of EAP (Extensible Authentication Protocol). EAP is designed to provide a framework for authentication that supports a variety of methods, including more complex and secure options than just basic username and password. This flexibility allows organizations to implement stronger security measures such as mutual authentication, certificates, and public key infrastructures that go far beyond what a simple username/password system can offer. While username/password schemes are commonly used, they do not leverage the security advantages that EAP can provide with its support for token-based, biometric, or hardware-based methods. This makes EAP a more sophisticated choice for secure environments, particularly in wireless communications, where the risk for interception is higher. Therefore, option B does not align with the core benefits associated with the capabilities that EAP brings to network authentication.