SV Cyber Security Certification Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

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

Questions

1. **What is the recommended group to assign permissions for a shared folder?**

    A. Domain users

    B. Security group

    C. Distribution group

    D. Local users

2. **On which OSI layer do TCP and UDP protocols function?**

    A. Layer 2

    B. Layer 3

    C. Layer 4

    D. Layer 5

3. **What port does the LDAP protocol commonly use?**

    A. 3389

    B. 8080

    C. 389

    D. 53

4. **Which layer of the OSI model is responsible for session management?**

    A. Layer 3

    B. Layer 4

    C. Layer 5

    D. Layer 6

5. **If you have multiple web servers that need to interact with a SQL server, where should the SQL server be located?**

    A. In a DMZ

    B. On the internet

    C. On the internal network

    D. In a VLAN

6. At which layer of the OSI model do routers operate?

A. Layer 1

B. Layer 2

C. Layer 3

D. Layer 4

7. Which model is commonly referenced to describe networking technologies?

A. TCP/IP model

B. OSI model

C. Internet Protocol Suite

D. Layered Networking Framework

8. Which type of authentication would you use for a highly sensitive transaction?

A. Password-based authentication

B. Two-factor authentication

C. Single sign-on authentication

D. Token-based authentication

9. What is the primary function of a firewall in network security?

A. To enhance network speed

B. To filter packets that can enter or exit a network

C. To store sensitive data securely

D. To manage user permissions

10. How many firewalls are typically required to set up a sandwich DMZ?

A. 1

B. 2

C. 3

D. 4

Answers

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

Explanations

1. What is the recommended group to assign permissions for a shared folder?

A. Domain users

B. Security group

C. Distribution group

D. Local users

Assigning permissions for a shared folder is best done through a security group, as security groups are specifically designed for managing permissions and access to resources in a network environment. When a security group is assigned to a shared folder, all members of that group inherit the permissions that have been granted. This makes it simple to manage access rights since you can add or remove users from the group as needed without having to individually configure permissions for each user. Security groups also allow for more granular control based on roles, meaning that only users who require access to certain resources, such as specific folders, are granted that access. In contrast, domain users represent a broader category that includes all users within the domain, making it less effective for managing specific permissions. Distribution groups are primarily used for email distribution lists and do not have any security context for permissions; thus they cannot be used for granting access to shared folders. Local users would be restricted to a single machine and would lack the scalability and centralized management that a security group provides, particularly in larger organizations with multiple machines and users. Overall, utilizing a security group for shared folder permissions enhances security, simplifies management, and aligns with best practices in access control within IT environments.

2. On which OSI layer do TCP and UDP protocols function?

A. Layer 2

B. Layer 3

C. Layer 4

D. Layer 5

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) both operate at Layer 4 of the OSI (Open Systems Interconnection) model, which is known as the Transport layer. This layer is responsible for end-to-end communication, ensuring that data is transferred reliably and error-free between devices. The primary role of the Transport layer is to manage how data is sent and received. TCP, being a connection-oriented protocol, establishes a connection before data can be sent, ensuring reliability through error-checking and acknowledgment of data packets. On the other hand, UDP is a connectionless protocol that allows for faster transmissions, suitable for applications where speed is critical, and some loss of data is acceptable. Both protocols handle the segmentation of data from the application layer (Layer 5) into manageable pieces and also facilitate the assembly of received segments back into a complete message at the destination. This layer also provides multiplexing services to allow multiple applications to use the network simultaneously. Understanding that TCP and UDP are specifically designed to operate at this layer is essential for grasping how different protocols manage data transmission and reliability, revealing their impact on network performance and application usability.

3. What port does the LDAP protocol commonly use?

A. 3389

B. 8080

C. 389

D. 53

The LDAP (Lightweight Directory Access Protocol) commonly uses port 389 for standard communications. This port is designated for LDAP operations, which include querying and modifying directory services. It allows clients to connect to directory servers and perform tasks such as user authentication, retrieving user information, and modifying directory entries. Port 389 is the designated well-known port for LDAP upon which most LDAP clients and servers will initiate their communications. The importance of this port lies not only in its standard use but also in its capability to support secure communications through an encrypted connection, which is typically established over port 636 for LDAP over SSL (LDAPS). Understanding the common use of this specific port is crucial for network configuration and security planning, as it plays a vital role in managing directory services within networks.

4. Which layer of the OSI model is responsible for session management?

A. Layer 3

B. Layer 4

C. Layer 5

D. Layer 6

The layer of the OSI model responsible for session management is the fifth layer, known as the Session Layer. This layer is crucial because it establishes, manages, and terminates sessions between communicating systems. A session refers to a persistent connection that can contain multiple messages and exchanges during its time of use. The Session Layer is responsible for the following functions: setting up connections, maintaining them during the communication process, ensuring that data is properly synchronized across sessions, and gracefully closing connections when the communication is complete. It plays an essential role in enabling applications to communicate effectively, particularly in scenarios where multiple communications occur simultaneously. In contrast, other layers of the OSI model serve different functions. The layers below the Session Layer focus more on data transport (Layer 4 - Transport Layer) and routing (Layer 3 - Network Layer), while layers above deal with application-specific processes (Layer 6 - Presentation Layer, and Layer 7 - Application Layer). Understanding the distinct roles of each layer is key in networking and cybersecurity, and it highlights the importance of session management within the overall communication process.

5. If you have multiple web servers that need to interact with a SQL server, where should the SQL server be located?

A. In a DMZ

B. On the internet

C. On the internet network

D. In a VLAN

The SQL server should be located on the internal network because this configuration helps maintain a higher level of security for sensitive data. Web servers typically handle requests from external users, making them more exposed to internet-based threats. By placing the SQL server, which often contains critical data, on the internal network, you create a safeguard against unauthorized access and potential attacks. This internal placement means that access to the SQL server can be tightly controlled through firewalls and access controls. It also allows for safer database management practices since the SQL server does not directly interface with the internet. Additionally, sensitive operations, like database queries, can be executed through the web servers without exposing the SQL server to potential threats from external sources. By contrast, placing the SQL server in a DMZ or on the internet would expose it to higher risks, as both configurations are inherently designed to allow more external communication. A VLAN could potentially provide some segmentation within the internal network, but it does not equate to the robust security features and access controls that come with placing the SQL server directly on the internal network.

6. At which layer of the OSI model do routers operate?

A. Layer 1

B. Layer 2

C. Layer 3

D. Layer 4

Routers operate at Layer 3 of the OSI model, which is known as the Network layer. This layer is responsible for routing packets across different networks and managing logical addressing, typically using IP addresses. Routers analyze the destination IP address of packets, determine the best path for them based on various routing protocols, and forward them accordingly. This functionality is crucial for interconnecting multiple networks, enabling communication between devices on different IP networks. By operating at Layer 3, routers can make decisions about where to send data packets based on network conditions, making them essential components in both local and wide area networks. Other layers, such as Layer 1 (Physical) and Layer 2 (Data Link), deal with the physical transmission of data and the framing of that data, respectively, while Layer 4 (Transport) focuses on the transmission of data segments and ensuring reliable communication. These layers serve different purposes but do not provide the same routing capabilities as the Network layer.

7. Which model is commonly referenced to describe networking technologies?

A. TCP/IP model

B. OSI model

C. Internet Protocol Suite

D. Layered Networking Framework

The OSI (Open Systems Interconnection) model is widely referenced in the context of networking technologies because it provides a comprehensive framework that standardizes the functions of a telecommunication or computing system regardless of its underlying internal structure and technology. The OSI model is divided into seven distinct layers, each representing specific network functions: Physical, Data Link, Network, Transport, Session, Presentation, and Application layers. This stratification allows for clearer conceptualization and troubleshooting of network communication by providing a structured approach to understanding how data is transmitted and received across networks. While other models, such as the TCP/IP model, are also significant in networking, the OSI model is more often used in educational contexts and theoretical discussions because of its clear and methodical layering. This makes it easier for students and professionals to grasp networking concepts and communicate about them effectively. In practical terms, referring to the OSI model also aids in the development of protocols and networking technologies, as it establishes a common language among different products and vendors within the industry.

8. Which type of authentication would you use for a highly sensitive transaction?

A. Password-based authentication

B. Two-factor authentication

C. Single sign-on authentication

D. Token-based authentication

Two-factor authentication is the most robust option for protecting highly sensitive transactions because it requires users to provide two different forms of verification before gaining access. This method combines something the user knows (like a password) with something the user has (like a smartphone or hardware token) or something the user is (biometric data). This layered approach greatly enhances security, as it is not enough for an attacker to know the password; they must also possess the second factor. In highly sensitive scenarios where the stakes are high—such as banking transactions, accessing private files, or entering secure systems—the additional barrier significantly mitigates the risk of unauthorized access. Even if a password is compromised, the presence of a second authentication factor keeps the system secure. This makes two-factor authentication a preferred choice for sensitive operations, aligning with best practices in cybersecurity.

9. What is the primary function of a firewall in network security?

A. To enhance network speed

B. To filter packets that can enter or exit a network

C. To store sensitive data securely

D. To manage user permissions

The primary function of a firewall in network security is to filter packets that can enter or exit a network. Firewalls act as a barrier between a trusted internal network and untrusted external networks, such as the internet. By examining packets of data, firewalls determine whether they should be allowed through based on predetermined security rules. This packet filtering helps to prevent unauthorized access and potential threats from entering the network while also controlling outbound traffic. In addition to filtering traffic, firewalls can also provide logging and monitoring capabilities, alerting administrators to suspicious activities. This essential function is what makes firewalls a critical component of network security, helping to protect systems and data from malicious attacks or unauthorized access. While enhancing network speed, storing sensitive data securely, and managing user permissions are important aspects of overall network and information security, they are not the primary functions of a firewall. These roles are typically handled by other security mechanisms or practices within the broader cybersecurity framework.

10. How many firewalls are typically required to set up a sandwich DMZ?

A. 1

B. 2

C. 3

D. 4

To establish a sandwich DMZ, two firewalls are typically required. The sandwich DMZ architecture leverages a configuration where the DMZ is situated between two firewalls. The primary purpose of this setup is to enhance security by creating multiple layers of defense. The outer firewall acts as the first line of defense, controlling incoming and outgoing traffic to and from the external network (such as the internet). The inner firewall protects the internal network by controlling traffic between the DMZ and the private network. By having two firewalls, the configuration ensures that even if one firewall is compromised, the other can still provide a barrier to protect critical internal resources. This arrangement significantly reduces the risk of unauthorized access and enhances the overall security posture of the network. Using only one firewall would not provide a sandwich configuration and would not achieve the layered security benefits that come with a two-firewall solution. Therefore, two firewalls are essential for setting up a sandwich DMZ effectively.