Welcome to Cert007 - Your Ultimate IT Certification Partner

- Real Exam Questions
- Free Updates
- Expert Support
- Instant Access
- Money-Back Guarantee

Visit us at **https://www.cert007.com/** for more information

Exam : **100-160**

Title : Cisco Certified Support Technician (CCST) Cybersecurity

Version : DEMO

1.What is a common security threat in which an attacker attempts to overwhelm a targeted system by flooding it with Internet traffic?
A. Ransomware
B. Distributed Denial of Service (DDoS) attack
C. Phishing
D. SQL injection
Answer: B
Explanation:
Option 1: Ransomware is a type of malicious software that encrypts a victim's files and demands a ransom in exchange for the decryption key. While it can cause damage to systems, it is not specifically designed to overwhelm a system with Internet traffic.
Option 2: Correct. A Distributed Denial of Service (DDoS) attack is a common security threat in which an attacker attempts to overwhelm a targeted system by flooding it with Internet traffic. This can result in a loss of service availability for legitimate users.
Option 3: Phishing is a type of social engineering attack in which an attacker masquerades as a trustworthy entity to trick individuals into providing sensitive information. It does not involve overwhelming a system with Internet traffic.
Option 4: SQL injection is a type of web application attack in which an attacker manipulates a SQL query to gain unauthorized access to a database. It does not involve overwhelming a system with Internet traffic.

2.Which of the following statements about multi-factor authentication (MFA) is correct?
A. MFA is a security measure that requires users to provide two or more forms of identification to gain access to a system or application.
B. MFA is a security measure that requires users to provide only one form of identification to gain access to a system or application
C. MFA is a security measure that is no longer recommended due to its complexity and potential for user errors.
D. MFA is a security measure that only applies to physical access control systems.
Answer: A
Explanation:
Option 1: This is the correct statement. MFThis is a security measure that requires users to provide two or more forms of identification to gain access to a system or application. It adds an extra layer of security by combining multiple credentials, such as passwords, one-time passcodes, biometrics, or smart cards, to verify a user's identity.
Option 2: This statement is incorrect. MFA requires users to provide two or more forms of identification, not just one.
Option 3: This statement is incorrect. MFThis is still recommended as an effective security measure and is widely used in many industries.
Option 4: This statement is incorrect. MFA can be used for both physical and logical access control systems.

3.Which of the following services or protocols can be used to ensure the security and compliance of an organization's network?

A. NTP (Network Time Protocol)
B. SNMP (Simple Network Management Protocol)
C. DHCP (Dynamic Host Configuration Protocol)
D. DNS (Domain Name System)
Answer: B
Explanation:
Option 1: NTP is a protocol used to synchronize the clocks of computers in a network. While it is important for maintaining accurate time, it does not directly contribute to network security and compliance. This makes it an incorrect answer.
Option 2: SNMP is a protocol used for managing and monitoring network devices. It allows for centralized monitoring, troubleshooting, and configuration of devices. SNMP can play a crucial role in security and compliance by providing real-time information about network devices and their behaviors. This makes it a correct answer.
Option 3: DHCP is a protocol used to assign IP addresses and network configuration parameters to devices on a network. While DHCP is essential for network connectivity, it does not directly contribute to security and compliance. This makes it an incorrect answer.
Option 4: DNS is a protocol used to translate domain names into IP addresses. While DNS is critical for internet connectivity, it does not directly contribute to security and compliance. This makes it an incorrect answer.

4.Which network security feature helps protect against unauthorized data access and ensures confidentiality of sensitive information?
A. Firewall
B. VPN
C. Intrusion Detection System
D. Antivirus
Answer: B
Explanation:
Option 1: Incorrect. A firewall is responsible for controlling incoming and outgoing network traffic based on predetermined security rules. While it can help protect against unauthorized access, it does not specifically ensure confidentiality of sensitive information.
Option 2: Correct. A VPN (Virtual Private Network) creates a secure, encrypted connection between a user's device and a private network, such as a corporate network, over the internet. This helps protect against unauthorized data access and ensures the confidentiality of sensitive information.
Option 3: Incorrect. An Intrusion Detection System (IDS) monitors network traffic for suspicious activity or known attack patterns.
While it can help detect and alert to potential unauthorized access attempts, it does not specifically ensure confidentiality of sensitive information.
Option 4: Incorrect. An antivirus software is used to detect, prevent, and remove malware infections. While it can help protect against unauthorized access, it does not specifically ensure confidentiality of sensitive information.

5.What is a key principle of securing data in the cloud?
A. Implementing strong physical security measures

B. Encrypting data at rest and in transit
C. Using complex passwords for all cloud users
D. Limiting access to the cloud from specific IP addresses
Answer: B
Explanation:
Option 1: Incorrect. Implementing strong physical security measures is important, but it is not the key principle of securing data in the cloud.
Option 2: Correct. Encrypting data at rest and in transit is a key principle of securing data in the cloud. This ensures that even if the data is compromised, it cannot be accessed without the decryption key.
Option 3: Incorrect. Using complex passwords is a good security practice, but it is not the key principle of securing data in the cloud.
Option 4: Incorrect. Limiting access to the cloud from specific IP addresses is a security measure, but it is not the key principle of securing data in the cloud.