Vendor: Cisco

Exam Code: 100-160

Exam Name: Cisco Certified Support Technician (CCST) Cybersecurity

Version: DEMO

QUESTION 1

Which of the following is a characteristic of a network-based firewall?

A. Inspects and filters traffic at the application layer
B. Operates at the data link layer
C. Provides protection against external threats only
D. Requires software installed on client devices

Answer: C

Explanation:

Option 1: Incorrect. A network-based firewall inspects and filters traffic at the network layer, not the application layer.
Option 2: Incorrect. A network-based firewall operates at the network layer, not the data link layer.
Option 3: Correct. A network-based firewall provides protection against both external and internal threats.
Option 4: Incorrect. A network-based firewall does not require software installed on client devices.

QUESTION 2

Which of the following is the most secure and recommended method for storing sensitive user data in a database?

A. Storing the data in plain text
B. Using symmetric encryption
C. Using hashing algorithms
D. Using asymmetric encryption

Answer: C

Explanation:

Option 1: Incorrect. Storing sensitive user data in plain text is highly insecure and not recommended. If a database breach occurs, all the data will be exposed without any protection.
Option 2: Incorrect. Using symmetric encryption would require storing the encryption key securely, which can be difficult. Additionally, any access to the data would require the encryption key, adding complexity and potential vulnerabilities.
Option 3: Correct. Using hashing algorithms is the most secure and recommended method for storing sensitive user data in a database. Hashing algorithms convert the data into a fixed-size string, making it difficult to reverse-engineer and obtain the original data. This ensures that even if a breach occurs, the sensitive data remains protected.
Option 4: Incorrect. Using asymmetric encryption would also require storing the encryption keys securely and adds unnecessary complexity for data retrieval, making it less practical for storing sensitive user data in a database.

QUESTION 3

What is the purpose of Security Information and Event Management (SIEM) systems?

A. To analyze network traffic and detect potential security threats.
B. To centrally collect, store, and analyze logs from various systems to detect and respond to security incidents.
C. To encrypt sensitive data to protect it from unauthorized access.
D. To authenticate and authorize users to access network resources.

Answer: B

Explanation:

Option 1: This Option is incorrect. While SIEM systems may perform analysis of network traffic, their primary purpose is not network traffic analysis, but rather log collection and analysis for security incident detection and response.
Option 2: This Option is correct. SIEM systems are designed to centrally collect, store, and analyze logs from various systems to detect and respond to security incidents. They provide real-time monitoring, correlation, and analysis of security events, allowing organizations to identify potential threats and take appropriate actions.
Option 3: This Option is incorrect. Encryption of sensitive data is not the purpose of SIEM systems. While encryption is an important security measure, SIEM systems focus on log management and analysis rather than encryption.
Option 4: This Option is incorrect. User authentication and authorization are not within the scope of SIEM systems. SIEM systems focus on log collection and analysis for security incident detection and response, rather than user access control.

QUESTION 4
Which of the following is a security best practice for securing data in the cloud?

A. Storing sensitive data in clear text
B. Implementing multi-factor authentication
C. Allowing unrestricted access to data
D. Using weak passwords

Answer: B
Explanation:
Option 1: Incorrect. Storing sensitive data in clear text is not a security best practice. It leaves the data vulnerable to unauthorized access and breaches.
Option 2: Correct. Implementing multi-factor authentication is a security best practice for securing data in the cloud. This adds an extra layer of protection by requiring users to provide additional verification beyond just a password.
Option 3: Incorrect. Allowing unrestricted access to data is not a security best practice. Access to data should be properly controlled and limited to authorized individuals or groups.
Option 4: Incorrect. Using weak passwords is not a security best practice. Strong and complex passwords should be used to prevent unauthorized access to data.

QUESTION 5
Which of the following is a principle of data security?

A. Encryption
B. Firewall
C. Intrusion Detection System
D. Data Masking

Answer: A
Explanation:
Option 1: Correct. Encryption is a principle of data security that involves converting data into a form that is unreadable by unauthorized users. This helps protect the confidentiality of data.
Option 2: Incorrect. A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on predetermined security rules. While it plays a role in data security, it is not a principle of data security.
Option 3: Incorrect. An Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports. While it plays a role in data security, it is not a principle of data security.
Option 4: Incorrect. Data masking is a technique that replaces sensitive data with fictitious data to

protect the privacy of data. While it plays a role in data security, it is not a principle of data security.

QUESTION 6
Which of the following features of the Cisco Identity Services Engine (ISE) allows network administrators to define policies for controlling access to network resources based on user identities and user or group attributes?

A. Network Access Profiles
B. Identity Firewall
C. Profiling
D. TrustSec

Answer: C
Explanation:
Option 1: Network Access Profiles: Network Access Profiles in Cisco ISE define the behavior of network devices when they are accessed by authenticated users. They are a set of policies that determine how network resources are allocated to users or user groups, and what level of access they have.
Option 2: Identity Firewall: Cisco ISE's Identity Firewall feature enables network administrators to apply firewall policies based on user identities. It allows for granular control over network access and can enforce allow, deny, or redirect actions based on user attributes.
Option 3: Profiling: This is the correct answer. Cisco ISE's Profiling feature is used to dynamically classify endpoints connecting to the network based on their characteristics, such as their MAC addresses, IP addresses, and DHCP options. This information is then used to enforce access policies.
Option 4: TrustSe TrustSec is a Cisco security solution that provides secure access control across the network infrastructure. While TrustSec is related to identity and access management, it is not a feature of Cisco ISE specifically.

QUESTION 7
What is the purpose of multi-factor authentication?

A. To provide multiple layers of security by requiring users to provide more than one form of identification
B. To simplify the login process by only requiring one form of identification
C. To restrict access to certain users by requiring additional authorization
D. To prevent unauthorized access by encrypting user credentials

Answer: A
Explanation:
Option 1: Correct. Multi-factor authentication adds an extra layer of security by requiring users to provide more than one form of identification, such as a password and a fingerprint or a security token.
Option 2: Incorrect. Multi-factor authentication does not simplify the login process, but rather adds an additional step to verify the user's identity.
Option 3: Incorrect. While multi-factor authentication can help restrict access to certain users, its main purpose is to provide an extra layer of security rather than additional authorization.
Option 4: Incorrect. While encryption is an important security measure, multi-factor authentication is specifically designed to provide multiple layers of security by requiring multiple forms of identification.

QUESTION 8
What is a common vulnerability in cloud-based systems?

A. Inadequate access controls
B. Outdated antivirus software
C. Weak passwords
D. Lack of network segmentation

Answer: A
Explanation:
Option 1: Correct: Inadequate access controls can leave cloud-based systems vulnerable to unauthorized access and data breaches.
Option 2: Incorrect: Outdated antivirus software is a concern for individual devices but not specific to cloud-based systems.
Option 3: Incorrect: Weak passwords can be a vulnerability but not a common one in cloud-based systems, which usually have password policies in place.
Option 4: Incorrect: Lack of network segmentation can be a vulnerability, but it is not as common as inadequate access controls.

QUESTION 9
Which of the following is a best practice for managing security policies and procedures?

A. Implementing a regular review process for security policies
B. Relying solely on default security settings
C. Allowing users to create and manage their own security policies
D. Not documenting the security policies and procedures

Answer: A
Explanation:
Option 1: Correct: Implementing a regular review process for security policies ensures that they are up- to-date and aligned with the organization's current security needs.
Option 2: Incorrect: Relying solely on default security settings is not a best practice as default settings may not provide adequate protection and may not be appropriate for the organization's specific needs.
Option 3: Incorrect: Allowing users to create and manage their own security policies can lead to inconsistencies, lack of control, and potential security vulnerabilities.
Option 4: Incorrect: Not documenting the security policies and procedures makes it difficult to enforce and communicate these policies to employees.

QUESTION 10
Which of the following is a best practice for implementing strong password policies within an organization?

A. Allowing users to choose their own passwords, regardless of complexity
B. Requiring users to change their password every 90 days
C. Storing passwords in clear text in a central database
D. Allowing users to reuse their previous passwords

Answer: B
Explanation:
Option 1: Incorrect. Allowing users to choose their own passwords, regardless of complexity, can lead to weak passwords that are easily guessed or cracked.

Option 2: Correct. Requiring users to change their password every 90 days helps to ensure that passwords are regularly updated and less likely to be compromised.
Option 3: Incorrect. Storing passwords in clear text in a central database is a security risk as it exposes the passwords to potential unauthorized access.
Option 4: Incorrect. Allowing users to reuse their previous passwords increases the risk of unauthorized access as attackers may already be aware of the user's previous passwords.

QUESTION 11
What is the primary reason for implementing multi-factor authentication in a cloud environment?

A. To provide an additional layer of security
B. To simplify the authentication process
C. To reduce costs
D. To improve performance

Answer: A
Explanation:
Option 1: Correct. Implementing multi-factor authentication provides an additional layer of security by requiring users to provide multiple forms of authentication to access cloud resources.
Option 2: Incorrect. The primary reason for implementing multi-factor authentication is to provide an additional layer of security, not to simplify the authentication process.
Option 3: Incorrect. The primary reason for implementing multi-factor authentication is to provide an additional layer of security, not to reduce costs.
Option 4: Incorrect. The primary reason for implementing multi-factor authentication is to provide an additional layer of security, not to improve performance.

QUESTION 12
Which security feature provides network segmentation by creating virtual networks?

A. VLANs
B. VLANs
C. Intrusion Prevention System (IPS)
D. Virtual Private Network (VPN)

Answer: A
Explanation:
Option 1: Correct, VLANs (Virtual Local Area Networks) provide network segmentation by creating virtual networks, allowing different groups of devices to be logically separated on the same physical network.
Option 2: Incorrect, Firewalls are designed to monitor and filter network traffic based on predetermined security rules, but they do not provide network segmentation by creating virtual networks.
Option 3: Incorrect, An Intrusion Prevention System (IPS) is a security appliance or software that monitors network traffic for suspicious activity and takes action to prevent potential threats, but it does not provide network segmentation by creating virtual networks.
Option 4: Incorrect, A Virtual Private Network (VPN) is a secure tunnel between two or more devices, typically used to connect remote sites or allow remote users to access the private network. It does not provide network segmentation by creating virtual networks.

QUESTION 13
Which of the following is a network security device that operates at the session layer of the OSI model?

A. Firewall
B. Intrusion Detection System (IDS)
C. Intrusion Prevention System (IPS)
D. SSL/TLS

Answer: B
Explanation:
Option 1: Incorrect. A firewall operates at the network layer (layer of the OSI model, not the session layer (layer 5).
Option 2: Correct. An Intrusion Prevention System (IPS) operates at the session layer (layer 5) of the OSI model. It monitors network traffic in real-time and can block or prevent malicious activities.
Option 3: Incorrect. An Intrusion Detection System (IDS) operates at the network layer (layer of the OSI model, not the session layer (layer 5).
Option 4: Incorrect. SSL/TLS is a cryptographic protocol that operates at the transport layer (layer of the OSI model, not the session layer (layer 5).

QUESTION 14
Which of the following is a feature of cloud computing?

A. On-premises hosting
B. Hardware provisioning
C. Data encryption
D. Physical server maintenance

Answer: C
Explanation:
Option 1: Incorrect. On-premises hosting refers to hosting applications and data on local servers within an organization's physical infrastructure. It is not a feature of cloud computing.
Option 2: Incorrect. Hardware provisioning is the process of setting up and configuring the physical infrastructure required to run applications and store data. While this is an important aspect of cloud computing, it is not a specific feature of cloud computing.
Option 3: Correct. Data encryption is a feature of cloud computing that ensures the security and confidentiality of data stored and transmitted within the cloud. It protects sensitive information from unauthorized access.
Option 4: Incorrect. Physical server maintenance involves activities such as hardware repairs, upgrades, and maintenance tasks associated with physical servers. While these tasks are necessary for managing an on-premises infrastructure, they are not specific features of cloud computing.

QUESTION 15
Which security technology uses an agent-based approach to protect endpoints and is designed to detect and prevent malicious activities?

A. Firewall
B. Intrusion Prevention System (IPS)
C. Data Loss Prevention (DLP)
D. Advanced Malware Protection (AMP)

Answer: D
Explanation:

Option 1: Incorrect. A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on predetermined security rules.
Option 2: Incorrect. An Intrusion Prevention System (IPS) is a network security device that monitors network traffic and is designed to detect and prevent unauthorized access and malicious activities.
Option 3: Incorrect. Data Loss Prevention (DLP) is a security technology that prevents sensitive data from being lost, stolen, or inadvertently leaked.
Option 4: Correct. Advanced Malware Protection (AMP) uses an agent-based approach to protect endpoints and detect and prevent known and unknown malicious activities. It includes features such as file reputation analysis, sandboxing, and behavior-based malware detection.

QUESTION 16
Which of the following is true regarding secure web gateways (SWG)?

A. SWGs provide protection against malware and advanced threats
B. SWGs are primarily used to secure internal web applications.
C. SWGs are no longer necessary with the advent of cloud-based applications.
D. SWGs can only be deployed on-premises

Answer: A
Explanation:
Option 1: Correct. Secure web gateways (SWG) provide protection against malware and advanced threats. They act as an intermediary between users and the internet, inspecting web traffic to detect and block malicious content and prevent data loss.
Option 2: Incorrect. While secure web gateways (SWG) can be used to secure internal web applications, their primary function is to provide protection against malware and advanced threats.
Option 3: Incorrect. Secure web gateways (SWG) are still necessary, even with the advent of cloud- based applications. They provide additional security controls and visibility for web traffic, regardless of whether the applications are on-premises or in the cloud.
Option 4: Incorrect. Secure web gateways (SWG) can be deployed both on-premises and in the cloud, depending on the organization's needs and preferences.

QUESTION 17
Which feature allows endpoints to communicate directly with each other, bypassing the network?

A. Firewall
B. IPS
C. VPN
D. Peer-to-Peer

Answer: D
Explanation:
Option 1: Incorrect. A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on predetermined security rules.
Option 2: Incorrect. An IPS (Intrusion Prevention System) is a network security device that monitors network traffic for malicious activity and takes immediate action to prevent attacks.
Option 3: Incorrect. A VPN (Virtual Private Network) is a secure connection between two or more endpoints over a public network, providing encryption and privacy for data communication.
Option 4: Correct. Peer-to-peer (P2P) is a decentralized communication model where endpoints can directly communicate with each other without the need for a central server or network infrastructure.