Question 1: START
Which of the following defines a subnet mask? (CO1)
Question 1: END
Option_a: Identifies the range of IP addresses in a network
Option_b: Helps in routing IP packets between devices
Option_c: Divides an IP address into network and host portions
Option_d: Determines the MAC address of a device
Correct_option: Divides an IP address into network and host portions.

Question 2: START
What is the primary role of the /etc/hosts file in Linux? (CO1)
Question 2: END
Option_a: Stores information about the local network topology
Option_b: Maps IP addresses to hostnames
Option_c: Configures system-wide security settings
Option_d: Specifies firewall rules
Correct_option: Maps IP addresses to hostnames.

Question 3: START
Which of the following commands is used to start a TCP/IP daemon in Linux? (CO1)
Question 3: END
Option_a: service tcpd start
Option_b: systemctl start tcpd
Option_c: init tcpd
Option_d: start_tcp
Correct_option: systemctl start tcpd.

Question 4: START
Which of the following is a characteristic of a network daemon in Linux systems? (CO1)
Question 4: END
Option_a: They are used for system shutdown processes.
Option_b: They handle specific services such as web or mail servers.
Option_c: They secure network packets and encrypt data.
Option_d: They monitor hardware device drivers.
Correct_option: They handle specific services such as web or mail servers.

Question 5: START
What is a primary security concern when using Telnet for remote connections? (CO1)
Question 5: END
Option_a: Data encryption is used during communication
Option_b: Authentication is performed using public-key cryptography
Option_c: The connection is unencrypted, allowing eavesdropping

Option_d: The connection uses a token-based authentication method
Correct_option: The connection is unencrypted, allowing eavesdropping.

Question 6: START
What is the primary purpose of SSL in network security? (CO1)
Question 6: END
Option_a: To generate encryption keys for FTP connections
Option_b: To secure data transmission over HTTP
Option_c: To perform data hashing for email protection
Option_d: To configure firewalls on a network
Correct_option: To secure data transmission over HTTP.

Question 7: START
Which cryptographic protocol is commonly used to secure FTP connections? (CO1)
Question 7: END
Option_a: TLS (Transport Layer Security)
Option_b: AES (Advanced Encryption Standard)
Option_c: RSA (Rivest-Shamir-Adleman)
Option_d: DES (Data Encryption Standard)
Correct_option: TLS (Transport Layer Security).

Question 8: START
What is a primary concern with using Telnet on a public network? (CO1)
Question 8: END
Option_a: It automatically encrypts the data during transmission
Option_b: It does not support secure authentication methods
Option_c: It uses weak password protection by default
Option_d: It allows remote administrative access without authorization
Correct_option: It does not support secure authentication methods.

Question 9: START
Which of the following is true about the /etc/passwd file in Linux? (CO1)
Question 9: END
Option_a: It contains system-wide user accounts and encrypted passwords
Option_b: It is only used for managing access to network devices
Option_c: It stores IP address mappings to hostnames
Option_d: It contains only information about local network services
Correct_option: It contains system-wide user accounts and encrypted passwords.

Question 10: START
What is the role of DNS in a network? (CO1)
Question 10: END
Option_a: Translates IP addresses to domain names
Option_b: Routes data between devices in the network

Option_c: Provides encryption for secure communication
Option_d: Monitors data traffic for security
Correct_option: Translates IP addresses to domain names.

Question 11: START
What is the primary function of a router in a network? (CO1)
Question 11: END
Option_a: To connect different networks and route data between them
Option_b: To provide wireless access to devices
Option_c: To store and manage data for network devices
Option_d: To encrypt data packets for security
Correct_option: To connect different networks and route data between them.

Question 12: START
Which of the following is true about NAT (Network Address Translation)? (CO1)
Question 12: END
Option_a: It translates public IP addresses to private IP addresses and vice versa
Option_b: It encrypts data transmitted across the network
Option_c: It assigns static IP addresses to network devices
Option_d: It monitors traffic for suspicious activity
Correct_option: It translates public IP addresses to private IP addresses and vice versa.

Question 13: START
Which type of attack involves redirecting traffic to a malicious server? (CO1)
Question 13: END
Option_a: Denial-of-service attack
Option_b: Man-in-the-middle attack
Option_c: Phishing attack
Option_d: DNS spoofing
Correct_option: DNS spoofing.

Question 14: START
Which file is used to configure static IP addresses in a Linux system? (CO1)
Question 14: END
Option_a: /etc/network/interfaces
Option_b: /etc/passwd
Option_c: /etc/hosts
Option_d: /etc/sysctl.conf
Correct_option: /etc/network/interfaces.

Question 15: START
What is the function of an SSL certificate in web security? (CO1)
Question 15: END
Option_a: It provides a unique identity to the website and encrypts communication

Option_b: It authenticates users by validating their passwords
Option_c: It controls access to the website's content
Option_d: It blocks unauthorized IP addresses from accessing the site
Correct_option: It provides a unique identity to the website and encrypts communication.

Question 16: START
What is a key benefit of using HTTPS instead of HTTP? (CO1)
Question 16: END
Option_a: Faster data transmission
Option_b: More reliable connection
Option_c: Encryption of data transmitted between the server and the client
Option_d: Compatibility with older browsers
Correct_option: Encryption of data transmitted between the server and the client.

Question 17: START
Which of the following is used for secure email communication? (CO1)
Question 17: END
Option_a: FTP
Option_b: PGP
Option_c: Telnet
Option_d: SSH
Correct_option: PGP.

Question 18: START
Which of the following is an example of multi-factor authentication? (CO1)
Question 18: END
Option_a: Using a password and an SMS code
Option_b: Using a password
Option_c: Using a PIN
Option_d: Using a fingerprint scan
Correct_option: Using a password and an SMS code.

Question 19: START
What does a firewall do in a network? (CO1)
Question 19: END
Option_a: It filters incoming and outgoing traffic to protect the network
Option_b: It stores sensitive data securely
Option_c: It connects different types of networks
Option_d: It manages wireless access points
Correct_option: It filters incoming and outgoing traffic to protect the network.

Question 20: START
What is the primary function of the DHCP protocol? (CO1)
Question 20: END

Option_a: To assign IP addresses to devices on a network
Option_b: To encrypt data sent over the network
Option_c: To provide secure access to a network
Option_d: To manage DNS settings for devices
Correct_option: To assign IP addresses to devices on a network.

Question 21: START
What does DNS stand for in networking? (CO1)
Question 21: END
Option_a: Dynamic Network Server
Option_b: Domain Name System
Option_c: Data Network Service
Option_d: Digital Network Service
Correct_option: Domain Name System.

Question 22: START
Which of the following is used to prevent unauthorized access to a network by inspecting incoming traffic? (CO1)
Question 22: END
Option_a: Antivirus software
Option_b: Firewall
Option_c: Encryption
Option_d: Proxy server
Correct_option: Firewall.

Question 23: START
What is the primary purpose of a subnet mask in networking? (CO1)
Question 23: END
Option_a: To secure data by encrypting it
Option_b: To divide an IP address into network and host parts
Option_c: To identify the domain name of a server
Option_d: To convert domain names into IP addresses
Correct_option: To divide an IP address into network and host parts.

Question 24: START
Which protocol is commonly used for secure email communication? (CO1)
Question 24: END
Option_a: IMAP
Option_b: SMTP
Option_c: PGP
Option_d: HTTP
Correct_option: PGP.

Question 25: START
What is the main function of the TCP/IP protocol suite? (CO1)
Question 25: END
Option_a: To enable communication between different devices over the internet
Option_b: To provide security for private networks
Option_c: To manage IP addresses within a local network
Option_d: To monitor incoming and outgoing traffic in a network
Correct_option: To enable communication between different devices over the internet.

Question 26: START
What does a MAC address represent in a network? (CO1)
Question 26: END
Option_a: A unique identifier for a device on a network
Option_b: A server address for website hosting
Option_c: A protocol used to secure communication
Option_d: An IP address for internet routing
Correct_option: A unique identifier for a device on a network.

Question 27: START
Which of the following services is responsible for translating domain names to IP addresses? (CO1)
Question 27: END
Option_a: DHCP
Option_b: DNS
Option_c: SMTP
Option_d: FTP
Correct_option: DNS.

Question 28: START
What does the "ping" command do in a network? (CO1)
Question 28: END
Option_a: It sends data packets to test network connectivity
Option_b: It transfers files between network devices
Option_c: It assigns IP addresses to devices
Option_d: It secures data during transmission
Correct_option: It sends data packets to test network connectivity.

Question 29: START
What is the purpose of the "traceroute" command? (CO1)
Question 29: END
Option_a: To encrypt data between two devices
Option_b: To map the route packets take to a destination
Option_c: To assign IP addresses to devices
Option_d: To block unwanted network traffic
Correct_option: To map the route packets take to a destination.

Question 30: START
Which of the following is used to securely connect two remote devices over the internet? (CO1)
Question 30: END
Option_a: Telnet
Option_b: SSH
Option_c: HTTP
Option_d: FTP
Correct_option: SSH.

Question 31: START
Which command is used to display the current IP configuration on a Linux system? (CO1)
Question 31: END
Option_a: ifconfig
Option_b: ipconfig
Option_c: netstat
Option_d: route
Correct_option: ifconfig.

Question 32: START
What is the purpose of using a proxy server in a network? (CO1)
Question 32: END
Option_a: To secure and filter web traffic between clients and servers
Option_b: To assign IP addresses to devices in a network
Option_c: To convert domain names to IP addresses
Option_d: To route data packets between networks
Correct_option: To secure and filter web traffic between clients and servers.

Question 33: START
What does the "netstat" command do in a Linux system? (CO1)
Question 33: END
Option_a: It displays the current network connections and listening ports
Option_b: It configures the network interfaces
Option_c: It assigns IP addresses to devices
Option_d: It monitors firewall activity
Correct_option: It displays the current network connections and listening ports.

Question 34: START
Which type of attack is designed to overwhelm a system by flooding it with excessive traffic? (CO1)
Question 34: END
Option_a: Man-in-the-middle attack
Option_b: Denial-of-service attack
Option_c: Phishing attack
Option_d: DNS spoofing
Correct_option: Denial-of-service attack.

Question 35: START
Which of the following is the most common method for securing data during transmission over the internet? (CO1)
Question 35: END
Option_a: IPsec
Option_b: SSL/TLS
Option_c: VPN
Option_d: FTP
Correct_option: SSL/TLS.

Question 36: START
What does "port forwarding" do in a network? (CO1)
Question 36: END
Option_a: It forwards data to specific ports based on rules defined in a router or firewall
Option_b: It configures static IP addresses for devices
Option_c: It encrypts communication between devices
Option_d: It routes data packets to destination devices based on MAC addresses
Correct_option: It forwards data to specific ports based on rules defined in a router or firewall.

Question 37: START
Which of the following is used to secure remote connections to a server via command line? (CO1)
Question 37: END
Option_a: FTP
Option_b: SSH
Option_c: HTTP
Option_d: SNMP
Correct_option: SSH.

Question 38: START
Which of the following is an example of a session layer protocol? (CO1)
Question 38: END
Option_a: HTTP
Option_b: FTP
Option_c: NetBIOS
Option_d: TCP
Correct_option: NetBIOS.

Question 39: START
What is the purpose of a public key in asymmetric encryption? (CO1)
Question 39: END
Option_a: To encrypt data sent by the sender
Option_b: To decrypt data received by the receiver
Option_c: To authenticate the sender's identity

Option_d: To secure the password during transmission
Correct_option: To encrypt data sent by the sender.

Question 40: START
Which of the following is a disadvantage of using static IP addresses? (CO1)
Question 40: END
Option_a: They are easily assigned by DHCP servers
Option_b: They can be difficult to configure manually on large networks
Option_c: They increase network traffic
Option_d: They are more secure than dynamic IP addresses
Correct_option: They can be difficult to configure manually on large networks.

Question 41: START
Which of the following is used to encrypt web traffic between a client and server? (CO1)
Question 41: END
Option_a: SSL/TLS
Option_b: IPsec
Option_c: SSH
Option_d: FTP
Correct_option: SSL/TLS.

Question 42: START
Which file in a Linux system contains the list of known hosts for SSH connections? (CO1)
Question 42: END
Option_a: /etc/ssh/sshd_config
Option_b: /etc/hosts
Option_c: /etc/known_hosts
Option_d: /etc/ssh/authorized_keys
Correct_option: /etc/known_hosts.

Question 43: START
What does a VPN (Virtual Private Network) provide to users? (CO1)
Question 43: END
Option_a: It secures data by encrypting the communication between two devices over the internet
Option_b: It allows devices to communicate using private IP addresses
Option_c: It manages DNS and routing for devices on a network
Option_d: It provides access to a local network from remote locations
Correct_option: It secures data by encrypting the communication between two devices over the internet.

Question 44: START
Which of the following is an example of an encryption algorithm used to secure data? (CO1)
Question 44: END
Option_a: HTTP

Option_b: DES
Option_c: FTP
Option_d: Telnet
Correct_option: DES.

Question 45: START
Which of the following protocols is primarily used for remote login to a server? (CO1)
Question 45: END
Option_a: SSH
Option_b: FTP
Option_c: Telnet
Option_d: DNS
Correct_option: SSH.

Question 46: START
What is the primary purpose of the /etc/resolv.conf file in Linux? (CO1)
Question 46: END
Option_a: It maps hostnames to IP addresses
Option_b: It configures DNS servers for name resolution
Option_c: It sets firewall rules for the system
Option_d: It lists the installed packages
Correct_option: It configures DNS servers for name resolution.

Question 47: START
Which of the following is a technique used to prevent unauthorized access to a network? (CO1)
Question 47: END
Option_a: Firewall
Option_b: DNS
Option_c: SSL
Option_d: FTP
Correct_option: Firewall.

Question 48: START
Which of the following commands is used to check the status of a network connection in Linux? (CO1)
Question 48: END
Option_a: ifconfig
Option_b: ip link
Option_c: ping
Option_d: netstat
Correct_option: netstat.

Question 49: START
Which protocol provides encryption and secure tunneling for VPN connections? (CO1)

Question 49: END
Option_a: PPTP
Option_b: IPsec
Option_c: FTP
Option_d: Telnet
Correct_option: IPsec.

Question 50: START
What does the "ip route" command display in a Linux system? (CO1)
Question 50: END
Option_a: The routing table for IP packets
Option_b: The current network interface configurations
Option_c: The list of active processes
Option_d: The IP addresses of local devices
Correct_option: The routing table for IP packets.

Question 51: START
Which of the following is an example of a network-layer protocol? (CO1)
Question 51: END
Option_a: IP
Option_b: TCP
Option_c: HTTP
Option_d: FTP
Correct_option: IP.

Question 52: START
What is a primary security concern with using Wi-Fi networks? (CO1)
Question 52: END
Option_a: The network can be accessed without a password
Option_b: Wi-Fi networks transmit data in clear text without encryption
Option_c: Wi-Fi signals are not subject to interference
Option_d: Wi-Fi networks are immune to DoS attacks
Correct_option: Wi-Fi networks transmit data in clear text without encryption.

Question 53: START
What is the function of the "iptables" command in a Linux system? (CO1)
Question 53: END
Option_a: To configure network interfaces
Option_b: To manage firewall rules
Option_c: To view network statistics
Option_d: To start network daemons
Correct_option: To manage firewall rules.

Question 54: START
Which of the following is a method for ensuring data confidentiality in network communication? (CO1)
Question 54: END
Option_a: Encryption
Option_b: Routing
Option_c: Authentication
Option_d: Logging
Correct_option: Encryption.

Question 55: START
Which of the following is true about symmetric encryption algorithms? (CO1)
Question 55: END
Option_a: They use the same key for both encryption and decryption
Option_b: They use different keys for encryption and decryption
Option_c: They are slower than asymmetric algorithms
Option_d: They rely on digital certificates for key exchange
Correct_option: They use the same key for both encryption and decryption.

Question 56: START
Which of the following is the purpose of DNS spoofing? (CO1)
Question 56: END
Option_a: To map domain names to incorrect IP addresses
Option_b: To encrypt DNS queries
Option_c: To secure DNS servers from attacks
Option_d: To authenticate users accessing a domain
Correct_option: To map domain names to incorrect IP addresses.

Question 57: START
What is the main advantage of using IPv6 over IPv4? (CO1)
Question 57: END
Option_a: It supports more devices due to a larger address space
Option_b: It provides better encryption for data transmission
Option_c: It reduces the need for firewalls
Option_d: It is faster than IPv4
Correct_option: It supports more devices due to a larger address space.

Question 58: START
Which of the following is the most secure method of authenticating users for remote access? (CO1)
Question 58: END
Option_a: Username and password
Option_b: Two-factor authentication
Option_c: IP address restriction

Option_d: SSH keys
Correct_option: Two-factor authentication.

Question 59: START
What is the function of an IDS (Intrusion Detection System) in network security? (CO1)
Question 59: END
Option_a: To prevent unauthorized access to the network
Option_b: To monitor network traffic for signs of malicious activity
Option_c: To encrypt data transmitted over the network
Option_d: To block unauthorized IP addresses from accessing the network
Correct_option: To monitor network traffic for signs of malicious activity.

Question 60: START
Which of the following is a risk associated with unsecured Wi-Fi networks? (CO1)
Question 60: END
Option_a: Interception of transmitted data
Option_b: Faster data transmission speeds
Option_c: Reduced signal range
Option_d: Enhanced security for connected devices
Correct_option: Interception of transmitted data.

Question 61: START
Which of the following is used to secure a website's communication over the internet? (CO1)
Question 61: END
Option_a: SSL/TLS
Option_b: FTP
Option_c: HTTP
Option_d: DNS
Correct_option: SSL/TLS.

Question 62: START
Which of the following is true about a "man-in-the-middle" attack? (CO1)
Question 62: END
Option_a: The attacker intercepts and possibly alters the communication between two parties
Option_b: The attacker prevents legitimate users from accessing a service
Option_c: The attacker directly disrupts network traffic by flooding it with requests
Option_d: The attacker gains unauthorized access to a system through a backdoor
Correct_option: The attacker intercepts and possibly alters the communication between two parties.

Question 63: START
What does a router do in a network? (CO1)
Question 63: END
Option_a: It assigns IP addresses to devices

Option_b: It forwards data packets between different networks
Option_c: It secures data through encryption
Option_d: It stores data in memory for quick access
Correct_option: It forwards data packets between different networks.

Question 64: START
What is the purpose of the /etc/passwd file in a Linux system? (CO1)
Question 64: END
Option_a: To store user account information
Option_b: To configure DNS settings
Option_c: To list installed packages
Option_d: To configure network interfaces
Correct_option: To store user account information.

Question 65: START
Which of the following commands is used to display the IP address configuration in Linux? (CO1)
Question 65: END
Option_a: ifconfig
Option_b: netstat
Option_c: route
Option_d: traceroute
Correct_option: ifconfig.

Question 66: START
What does a "brute force" attack involve? (CO1)
Question 66: END
Option_a: Attempting every possible combination of a password until the correct one is found
Option_b: Injecting malicious code into a network
Option_c: Flooding a server with too many requests to crash it
Option_d: Hacking into a system via an unsecured Wi-Fi connection
Correct_option: Attempting every possible combination of a password until the correct one is found.

Question 67: START
Which protocol is used for sending emails over the internet? (CO1)
Question 67: END
Option_a: SMTP
Option_b: FTP
Option_c: HTTP
Option_d: SSH
Correct_option: SMTP.

Question 68: START
Which of the following tools is used to encrypt and secure email messages? (CO1)

Question 68: END
Option_a: PGP
Option_b: SSL
Option_c: IPsec
Option_d: Telnet
Correct_option: PGP.

Question 69: START
Which layer of the OSI model is responsible for routing data packets between different networks? (CO1)
Question 69: END
Option_a: Application layer
Option_b: Transport layer
Option_c: Network layer
Option_d: Data link layer
Correct_option: Network layer.

Question 70: START
What is the purpose of a "firewall" in a network? (CO1)
Question 70: END
Option_a: To encrypt data during transmission
Option_b: To block unauthorized access to a network
Option_c: To route traffic between different networks
Option_d: To provide secure access for remote users
Correct_option: To block unauthorized access to a network.

Question 71: START
Which of the following is a commonly used encryption standard for securing web traffic? (CO1)
Question 71: END
Option_a: AES
Option_b: DES
Option_c: RSA
Option_d: SSL
Correct_option: SSL.

Question 72: START
What is the purpose of the DHCP protocol? (CO1)
Question 72: END
Option_a: To automatically assign IP addresses to devices in a network
Option_b: To provide encryption for secure communication
Option_c: To send and receive emails securely
Option_d: To map domain names to IP addresses
Correct_option: To automatically assign IP addresses to devices in a network.

Question 73: START
Which of the following is a key principle of network security? (CO1)
Question 73: END
Option_a: Confidentiality
Option_b: Redundancy
Option_c: Transparency
Option_d: Accessibility
Correct_option: Confidentiality.

Question 74: START
What is the primary purpose of a system daemon? (CO1)
Question 74: END
Option_a: To manage system services and processes in the background
Option_b: To provide a user interface for system administration
Option_c: To encrypt user data
Option_d: To assign IP addresses to network devices
Correct_option: To manage system services and processes in the background.

Question 75: START
What does the term "spoofing" refer to in the context of network security? (CO1)
Question 75: END
Option_a: Masquerading as another user or device to gain unauthorized access
Option_b: Encrypting data before transmitting it over the network
Option_c: Flooding a system with too much traffic
Option_d: Using a secure tunnel for communication
Correct_option: Masquerading as another user or device to gain unauthorized access.

Question 76: START
Which of the following is used to securely connect two different networks over the internet? (CO1)
Question 76: END
Option_a: VPN
Option_b: SSH
Option_c: DNS
Option_d: SSL
Correct_option: VPN.

Question 77: START
What does the term "sniffing" refer to in network security? (CO1)
Question 77: END
Option_a: Intercepting and analyzing network traffic
Option_b: Spoofing the source of network traffic
Option_c: Blocking unauthorized network traffic
Option_d: Encrypting network traffic for security
Correct_option: Intercepting and analyzing network traffic.

Question 78: START
What does the term "phishing" refer to in network security? (CO1)
Question 78: END
Option_a: Attempting to trick users into revealing sensitive information
Option_b: Flooding a system with excessive traffic
Option_c: Encrypting email messages for confidentiality
Option_d: Spoofing a network device's identity
Correct_option: Attempting to trick users into revealing sensitive information.

Question 79: START
Which of the following is the main purpose of using a "public key" in asymmetric encryption? (CO1)
Question 79: END
Option_a: To encrypt data to be sent to the receiver
Option_b: To decrypt data received from the sender
Option_c: To authenticate the identity of the sender
Option_d: To generate digital certificates
Correct_option: To encrypt data to be sent to the receiver.

Question 80: START
What does the term "Denial-of-Service" (DoS) attack refer to? (CO1)
Question 80: END
Option_a: Disrupting the availability of a service by overwhelming it with excessive requests
Option_b: Intercepting communication between two parties
Option_c: Gaining unauthorized access to a system by guessing passwords
Option_d: Masquerading as a trusted user to gain access to a system
Correct_option: Disrupting the availability of a service by overwhelming it with excessive requests.

Question 81: START
What is the primary function of a proxy server in a network? (CO1)
Question 81: END
Option_a: To filter and forward requests between clients and servers
Option_b: To encrypt data transmitted between two devices
Option_c: To assign IP addresses to devices on the network
Option_d: To store cached data for faster access
Correct_option: To filter and forward requests between clients and servers.

Question 82: START
Which of the following tools is used to test network connectivity in a Linux system? (CO1)
Question 82: END
Option_a: traceroute
Option_b: curl
Option_c: netstat
Option_d: ping
Correct_option: ping.

Question 83: START
Which of the following protocols is responsible for converting domain names to IP addresses? (CO1)
Question 83: END
Option_a: DHCP
Option_b: DNS
Option_c: FTP
Option_d: HTTP
Correct_option: DNS.

Question 84: START
Which of the following is true about a network firewall? (CO1)
Question 84: END
Option_a: It helps prevent unauthorized access to a network
Option_b: It stores data for faster access
Option_c: It forwards data packets between networks
Option_d: It provides encryption for secure communication
Correct_option: It helps prevent unauthorized access to a network.

Question 85: START
Which of the following protocols is used to securely transfer files between devices? (CO1)
Question 85: END
Option_a: FTP
Option_b: SCP
Option_c: SMTP
Option_d: HTTP
Correct_option: SCP.

Question 86: START
What is the purpose of the SSL certificate on a website? (CO1)
Question 86: END
Option_a: To encrypt data exchanged between the website and the user's browser
Option_b: To provide authentication of the website's identity
Option_c: To enable secure email communication
Option_d: To validate the integrity of files transferred over the network
Correct_option: To encrypt data exchanged between the website and the user's browser.

Question 87: START
What is the main purpose of the SSH protocol? (CO1)
Question 87: END
Option_a: To securely transfer files between servers
Option_b: To provide remote access to a device securely
Option_c: To block unauthorized network traffic

Option_d: To monitor network traffic for malicious activity
Correct_option: To provide remote access to a device securely.

Question 88: START
Which of the following best describes a "man-in-the-middle" attack? (CO1)
Question 88: END
Option_a: An attacker intercepts and potentially alters communication between two parties
Option_b: An attacker blocks all communication from an IP address
Option_c: An attacker gains control over the authentication server
Option_d: An attacker gains unauthorized access to a device on the network
Correct_option: An attacker intercepts and potentially alters communication between two parties.

Question 89: START
Which of the following is a security risk associated with using weak passwords? (CO1)
Question 89: END
Option_a: They can be easily guessed or cracked by attackers
Option_b: They slow down network performance
Option_c: They cause data corruption in the system
Option_d: They enable unauthorized users to bypass firewalls
Correct_option: They can be easily guessed or cracked by attackers.

Question 90: START
Which layer of the OSI model ensures the reliable delivery of data packets? (CO1)
Question 90: END
Option_a: Application layer
Option_b: Transport layer
Option_c: Network layer
Option_d: Data link layer
Correct_option: Transport layer.

Question 91: START
Which of the following is the most commonly used cryptographic algorithm for securing email messages? (CO2)
Question 91: END
Option_a: RSA
Option_b: AES
Option_c: PGP
Option_d: DES
Correct_option: PGP.

Question 92: START
What does the "telnet" command allow you to do in a network? (CO2)
Question 92: END
Option_a: Establish a remote connection to a server without encryption

Option_b: Securely transfer files between devices
Option_c: Encrypt messages exchanged between devices
Option_d: Monitor network traffic for security breaches
Correct_option: Establish a remote connection to a server without encryption.

Question 93: START
Which of the following is a typical use of SSL/TLS in web security? (CO2)
Question 93: END
Option_a: Encrypting data between a web server and a browser
Option_b: Encrypting DNS queries
Option_c: Protecting email servers from spam
Option_d: Securely transferring files between devices
Correct_option: Encrypting data between a web server and a browser.

Question 94: START
Which of the following encryption algorithms is commonly used for encrypting files and messages? (CO2)
Question 94: END
Option_a: AES
Option_b: PGP
Option_c: RSA
Option_d: DES
Correct_option: AES.

Question 95: START
What is the primary function of a VPN in network security? (CO2)
Question 95: END
Option_a: To encrypt data and provide a secure tunnel for communication over a public network
Option_b: To block malicious IP addresses from accessing the network
Option_c: To monitor network traffic for suspicious activity
Option_d: To configure and assign IP addresses to devices
Correct_option: To encrypt data and provide a secure tunnel for communication over a public network.

Question 96: START
Which of the following tools is used to perform vulnerability assessments in a network? (CO2)
Question 96: END
Option_a: Nmap
Option_b: PGP
Option_c: OpenSSL
Option_d: Wireshark
Correct_option: Nmap.

Question 97: START
Which of the following methods is used to ensure the authenticity of a message in network communication? (CO2)
Question 97: END
Option_a: Encryption
Option_b: Digital signatures
Option_c: Hashing
Option_d: Compression
Correct_option: Digital signatures.

Question 98: START
Which of the following is an example of a security breach in email communication? (CO2)
Question 98: END
Option_a: Intercepting email messages and reading their content
Option_b: Using encryption to secure email traffic
Option_c: Sending an email with a digital signature
Option_d: Using a secure email server
Correct_option: Intercepting email messages and reading their content.

Question 99: START
What is the purpose of "key management" in cryptography? (CO2)
Question 99: END
Option_a: To manage the generation, distribution, and storage of encryption keys
Option_b: To ensure that digital signatures are valid
Option_c: To monitor the integrity of encrypted data
Option_d: To block unauthorized users from accessing the key repository
Correct_option: To manage the generation, distribution, and storage of encryption keys.

Question 100: START
What does "PGP" stand for in the context of cryptography? (CO2)
Question 100: END
Option_a: Pretty Good Privacy
Option_b: Private General Protection
Option_c: Public General Privacy
Option_d: Public Grid Protocol
Correct_option: Pretty Good Privacy.

Question 101: START
What is the main purpose of encryption in network security? (CO2)
Question 101: END
Option_a: To ensure the confidentiality of data
Option_b: To speed up data transmission
Option_c: To monitor network traffic

Option_d: To authenticate users
Correct_option: To ensure the confidentiality of data.

Question 102: START
Which of the following is the best way to protect a system from brute force attacks? (CO2)
Question 102: END
Option_a: Using complex and lengthy passwords
Option_b: Disabling SSL/TLS encryption
Option_c: Disabling the firewall
Option_d: Using a single authentication method
Correct_option: Using complex and lengthy passwords.

Question 103: START
Which of the following is the primary goal of using SSL certificates on websites? (CO2)
Question 103: END
Option_a: To provide encryption and secure communication between a browser and a server
Option_b: To speed up the connection between the client and the server
Option_c: To assign IP addresses to devices on the network
Option_d: To prevent unauthorized access to a server
Correct_option: To provide encryption and secure communication between a browser and a server.

Question 104: START
Which of the following protocols is used to secure the communication between a user and a website? (CO2)
Question 104: END
Option_a: HTTPS
Option_b: HTTP
Option_c: FTP
Option_d: Telnet
Correct_option: HTTPS.

Question 105: START
Which of the following is an example of a public-key encryption algorithm? (CO2)
Question 105: END
Option_a: RSA
Option_b: DES
Option_c: AES
Option_d: Blowfish
Correct_option: RSA.

Question 106: START
Which of the following techniques is used to defend against a denial-of-service attack? (CO2)
Question 106: END
Option_a: Traffic filtering and rate limiting

Option_b: Using unencrypted communication
Option_c: Reducing the bandwidth of the network
Option_d: Disabling firewalls
Correct_option: Traffic filtering and rate limiting.

Question 107: START
What is the purpose of a digital certificate? (CO2)
Question 107: END
Option_a: To verify the identity of a website or user
Option_b: To monitor network traffic
Option_c: To secure email communications
Option_d: To configure network devices
Correct_option: To verify the identity of a website or user.

Question 108: START
What does the term "hashing" refer to in the context of cryptography? (CO2)
Question 108: END
Option_a: Generating a fixed-length value from a variable-length input
Option_b: Encrypting data for confidentiality
Option_c: Digitally signing a message
Option_d: Generating an encryption key
Correct_option: Generating a fixed-length value from a variable-length input.

Question 109: START
Which of the following is an example of a symmetric encryption algorithm? (CO2)
Question 109: END
Option_a: AES
Option_b: RSA
Option_c: PGP
Option_d: Diffie-Hellman
Correct_option: AES.

Question 110: START
What is the primary function of the IPsec protocol? (CO2)
Question 110: END
Option_a: To secure communication by encrypting and authenticating IP packets
Option_b: To assign IP addresses to devices
Option_c: To monitor network traffic for security breaches
Option_d: To manage encryption keys
Correct_option: To secure communication by encrypting and authenticating IP packets.

Question 111: START
Which of the following tools is used to monitor network traffic for malicious activities? (CO2)
Question 111: END

Option_a: Wireshark
Option_b: Nmap
Option_c: OpenSSL
Option_d: ping
Correct_option: Wireshark.

Question 112: START
Which of the following describes a "zero-day" vulnerability? (CO2)
Question 112: END
Option_a: A vulnerability that is exploited before it becomes known to the vendor
Option_b: A vulnerability that is only present in outdated software
Option_c: A vulnerability that can be fixed with a software update
Option_d: A vulnerability that has been publicly disclosed and patched
Correct_option: A vulnerability that is exploited before it becomes known to the vendor.

Question 113: START
What is the role of the Secure Sockets Layer (SSL) in network security? (CO2)
Question 113: END
Option_a: To provide encryption and authentication between a web server and a browser
Option_b: To assign IP addresses to devices on a network
Option_c: To monitor network traffic for suspicious activity
Option_d: To securely transfer email messages
Correct_option: To provide encryption and authentication between a web server and a browser.

Question 114: START
Which of the following is a common method used in network traffic analysis? (CO2)
Question 114: END
Option_a: Packet sniffing
Option_b: Routing
Option_c: Encryption
Option_d: Compression
Correct_option: Packet sniffing.

Question 115: START
What is the primary function of an intrusion detection system (IDS)? (CO2)
Question 115: END
Option_a: To detect and respond to potential security breaches in a network
Option_b: To monitor system performance
Option_c: To encrypt data during transmission
Option_d: To assign IP addresses to devices on the network
Correct_option: To detect and respond to potential security breaches in a network.

Question 116: START
Which of the following is a form of network attack where the attacker floods a target system with

excessive traffic? (CO2)
Question 116: END
Option_a: Denial of Service (DoS)
Option_b: Man-in-the-middle attack
Option_c: Phishing attack
Option_d: Buffer overflow attack
Correct_option: Denial of Service (DoS).

Question 117: START
What does the "Diffie-Hellman" protocol provide in cryptography? (CO2)
Question 117: END
Option_a: Secure key exchange over an unsecured channel
Option_b: Data encryption for secure communication
Option_c: Digital signatures for authentication
Option_d: Public-key infrastructure management
Correct_option: Secure key exchange over an unsecured channel.

Question 118: START
Which of the following is a typical feature of a security protocol used in email communication? (CO2)
Question 118: END
Option_a: Encryption to ensure confidentiality
Option_b: IP address assignment
Option_c: Network routing
Option_d: System optimization
Correct_option: Encryption to ensure confidentiality.

Question 119: START
Which of the following cryptographic techniques is used to ensure the integrity of a message? (CO2)
Question 119: END
Option_a: Hashing
Option_b: Symmetric encryption
Option_c: Digital signatures
Option_d: Asymmetric encryption
Correct_option: Hashing.

Question 120: START
Which of the following is an example of a malicious code injection attack? (CO2)
Question 120: END
Option_a: SQL injection
Option_b: Denial-of-service
Option_c: Man-in-the-middle
Option_d: Phishing
Correct_option: SQL injection.

Question 121: START
Which of the following network security techniques is designed to protect against unauthorized data access while in transit? (CO2)
Question 121: END
Option_a: Encryption
Option_b: Data masking
Option_c: Authentication
Option_d: Auditing
Correct_option: Encryption.

Question 122: START
What is the purpose of a public key infrastructure (PKI)? (CO2)
Question 122: END
Option_a: To manage the keys used in public-key cryptography
Option_b: To store encrypted data securely
Option_c: To monitor network traffic
Option_d: To configure devices on a network
Correct_option: To manage the keys used in public-key cryptography.

Question 123: START
Which of the following is a common feature of a firewall? (CO2)
Question 123: END
Option_a: Blocking unauthorized incoming and outgoing traffic
Option_b: Managing user passwords
Option_c: Assigning IP addresses to devices
Option_d: Routing network packets between different segments
Correct_option: Blocking unauthorized incoming and outgoing traffic.

Question 124: START
Which of the following techniques is commonly used for secure authentication in network systems? (CO2)
Question 124: END
Option_a: Two-factor authentication
Option_b: Network sniffing
Option_c: Packet routing
Option_d: DNS resolution
Correct_option: Two-factor authentication.

Question 125: START
Which of the following protocols is used to ensure the integrity of files during transfer? (CO2)
Question 125: END
Option_a: SHA-1
Option_b: HTTP
Option_c: TCP

Option_d: SMTP
Correct_option: SHA-1.

Question 126: START
What is the primary purpose of using a VPN in a network? (CO2)
Question 126: END
Option_a: To create a secure tunnel for transmitting data over an unsecured network
Option_b: To assign IP addresses to devices on a network
Option_c: To monitor network traffic for malicious activity
Option_d: To store network data for faster access
Correct_option: To create a secure tunnel for transmitting data over an unsecured network.

Question 127: START
Which of the following is a characteristic of a brute force attack? (CO2)
Question 127: END
Option_a: Trying all possible combinations to guess a password
Option_b: Intercepting and altering communication between two parties
Option_c: Using a virus to disrupt network traffic
Option_d: Exploiting a known vulnerability to gain access
Correct_option: Trying all possible combinations to guess a password.

Question 128: START
Which of the following is an example of a cryptographic technique used to maintain data confidentiality? (CO2)
Question 128: END
Option_a: Symmetric encryption
Option_b: Digital signatures
Option_c: Message authentication codes
Option_d: Hashing
Correct_option: Symmetric encryption.

Question 129: START
Which of the following best describes a phishing attack? (CO2)
Question 129: END
Option_a: A fraudulent attempt to obtain sensitive information by pretending to be a trustworthy entity
Option_b: An attempt to overload a system with unnecessary requests
Option_c: An attack that intercepts and alters communication between two parties
Option_d: An attack that exploits a system's software vulnerability
Correct_option: A fraudulent attempt to obtain sensitive information by pretending to be a trustworthy entity.

Question 130: START
What is the function of a digital signature in cryptographic communication? (CO2)

Question 130: END
Option_a: To verify the authenticity of a message or document
Option_b: To encrypt the data in the communication
Option_c: To provide secure email delivery
Option_d: To mask the sender's IP address
Correct_option: To verify the authenticity of a message or document.

Question 131: START
Which of the following is an essential characteristic of symmetric encryption algorithms? (CO2)
Question 131: END
Option_a: The same key is used for both encryption and decryption
Option_b: Different keys are used for encryption and decryption
Option_c: It does not require a key for encryption
Option_d: It uses public-key infrastructure for key management
Correct_option: The same key is used for both encryption and decryption.

Question 132: START
Which of the following types of attacks attempts to impersonate a legitimate user by stealing or mimicking their credentials? (CO2)
Question 132: END
Option_a: Spoofing
Option_b: Phishing
Option_c: Brute force
Option_d: Sniffing
Correct_option: Spoofing.

Question 133: START
Which of the following protocols ensures secure communication for emails? (CO2)
Question 133: END
Option_a: SMTP with SSL/TLS
Option_b: HTTP
Option_c: FTP
Option_d: POP3
Correct_option: SMTP with SSL/TLS.

Question 134: START
Which of the following is the main difference between symmetric and asymmetric encryption? (CO2)
Question 134: END
Option_a: Symmetric encryption uses the same key for both encryption and decryption, while asymmetric encryption uses different keys
Option_b: Asymmetric encryption uses faster algorithms than symmetric encryption
Option_c: Symmetric encryption does not require a key
Option_d: Asymmetric encryption is used only for digital signatures

Correct_option: Symmetric encryption uses the same key for both encryption and decryption, while asymmetric encryption uses different keys.

Question 135: START
Which of the following is the main vulnerability in a man-in-the-middle attack? (CO2)
Question 135: END
Option_a: The attacker can intercept and potentially alter communication between two parties
Option_b: The attacker can access a device's private key
Option_c: The attacker can overload the network with traffic
Option_d: The attacker can block access to legitimate websites
Correct_option: The attacker can intercept and potentially alter communication between two parties.

Question 136: START
What is the function of a Certificate Authority (CA) in PKI? (CO2)
Question 136: END
Option_a: To issue and manage digital certificates
Option_b: To assign IP addresses to devices
Option_c: To monitor network security
Option_d: To store encryption keys
Correct_option: To issue and manage digital certificates.

Question 137: START
What is the role of the public key in asymmetric encryption? (CO2)
Question 137: END
Option_a: To encrypt the message before it is sent to the recipient
Option_b: To decrypt the message after it is received
Option_c: To generate a hash of the message
Option_d: To authenticate the sender's identity
Correct_option: To encrypt the message before it is sent to the recipient.

Question 138: START
Which of the following is a common use of a hash function in cryptography? (CO2)
Question 138: END
Option_a: To ensure data integrity by generating a fixed-length representation of the data
Option_b: To encrypt the data before transmission
Option_c: To authenticate the sender's identity
Option_d: To sign digital certificates
Correct_option: To ensure data integrity by generating a fixed-length representation of the data.

Question 139: START
Which of the following is a disadvantage of symmetric encryption? (CO2)
Question 139: END
Option_a: The key must be securely shared between the sender and the recipient

Option_b: It is slower than asymmetric encryption
Option_c: It does not support digital signatures
Option_d: It cannot be used for large volumes of data
Correct_option: The key must be securely shared between the sender and the recipient.

Question 140: START
Which of the following is an example of a vulnerability scanning tool used in network security? (CO2)
Question 140: END
Option_a: Nessus
Option_b: Netstat
Option_c: Telnet
Option_d: Wireshark
Correct_option: Nessus.

Question 141: START
Which of the following describes the purpose of a VPN tunnel? (CO2)
Question 141: END
Option_a: To secure communication over a public network by encrypting the data
Option_b: To assign a unique IP address to each device on the network
Option_c: To monitor network traffic for malicious activity
Option_d: To optimize data transfer speeds
Correct_option: To secure communication over a public network by encrypting the data.

Question 142: START
Which of the following is an example of an attack that exploits vulnerabilities in a web application? (CO2)
Question 142: END
Option_a: Cross-site scripting (XSS)
Option_b: Denial-of-service
Option_c: Man-in-the-middle
Option_d: Password brute-forcing
Correct_option: Cross-site scripting (XSS).

Question 143: START
Which of the following encryption methods is primarily used in digital certificates? (CO2)
Question 143: END
Option_a: Asymmetric encryption
Option_b: Symmetric encryption
Option_c: Hashing
Option_d: Steganography
Correct_option: Asymmetric encryption.

Question 144: START
What is the purpose of the SSL handshake? (CO2)
Question 144: END
Option_a: To authenticate both parties and establish a secure encryption key for communication
Option_b: To identify the IP addresses of both parties
Option_c: To verify the validity of the digital signature
Option_d: To ensure the confidentiality of passwords
Correct_option: To authenticate both parties and establish a secure encryption key for communication.

Question 145: START
Which of the following methods is used to validate the integrity of a message after it is transmitted? (CO2)
Question 145: END
Option_a: Message authentication code (MAC)
Option_b: Digital signature
Option_c: Public-key encryption
Option_d: Symmetric encryption
Correct_option: Message authentication code (MAC).

Question 146: START
Which of the following is the primary function of an intrusion prevention system (IPS)? (CO2)
Question 146: END
Option_a: To detect and prevent network attacks by analyzing traffic in real-time
Option_b: To provide encryption for data transmission
Option_c: To configure security settings on a network
Option_d: To manage digital certificates
Correct_option: To detect and prevent network attacks by analyzing traffic in real-time.

Question 147: START
Which of the following is used to securely connect a remote user to a corporate network? (CO2)
Question 147: END
Option_a: Virtual Private Network (VPN)
Option_b: Remote Desktop Protocol (RDP)
Option_c: Hypertext Transfer Protocol (HTTP)
Option_d: File Transfer Protocol (FTP)
Correct_option: Virtual Private Network (VPN).

Question 148: START
What is the role of a firewall in network security? (CO2)
Question 148: END
Option_a: To monitor and filter incoming and outgoing network traffic
Option_b: To authenticate users before allowing access
Option_c: To prevent data from being encrypted

Option_d: To provide secure storage for sensitive data
Correct_option: To monitor and filter incoming and outgoing network traffic.

Question 149: START
Which of the following is a key difference between a public key and a private key in asymmetric encryption? (CO2)
Question 149: END
Option_a: The public key is used to encrypt data, and the private key is used to decrypt it
Option_b: The public key is used to authenticate users, and the private key is used to sign data
Option_c: The public key is used to store sensitive information, and the private key is used for verification
Option_d: The public key is used for digital signatures, and the private key is used for encryption
Correct_option: The public key is used to encrypt data, and the private key is used to decrypt it.

Question 150: START
Which of the following is a type of malware that disguises itself as legitimate software? (CO2)
Question 150: END
Option_a: Trojan horse
Option_b: Worm
Option_c: Virus
Option_d: Spyware
Correct_option: Trojan horse.

Question 151: START
What is the main purpose of a honeypot in network security? (CO2)
Question 151: END
Option_a: To attract and deceive attackers in order to detect and analyze their methods
Option_b: To store sensitive data securely
Option_c: To encrypt data transmitted over a network
Option_d: To block unauthorized traffic from reaching a system
Correct_option: To attract and deceive attackers in order to detect and analyze their methods.

Question 152: START
Which of the following is the main goal of an access control list (ACL) in network security? (CO2)
Question 152: END
Option_a: To control and filter network traffic based on predefined rules
Option_b: To authenticate users before granting access to a system
Option_c: To encrypt network communications
Option_d: To manage the allocation of IP addresses
Correct_option: To control and filter network traffic based on predefined rules.

Question 153: START
What is the purpose of a security certificate? (CO2)
Question 153: END

Option_a: To verify the identity of the sender and ensure the integrity of the message
Option_b: To assign a secure IP address to a device
Option_c: To configure firewalls for security
Option_d: To monitor network traffic
Correct_option: To verify the identity of the sender and ensure the integrity of the message.

Question 154: START
Which of the following is the primary function of a VPN gateway? (CO2)
Question 154: END
Option_a: To connect remote users to the corporate network securely
Option_b: To route network traffic between different subnets
Option_c: To assign IP addresses to devices on the network
Option_d: To monitor and filter incoming traffic
Correct_option: To connect remote users to the corporate network securely.

Question 155: START
Which of the following is an example of a hashing algorithm used for ensuring data integrity? (CO2)
Question 155: END
Option_a: SHA-256
Option_b: RSA
Option_c: AES
Option_d: PGP
Correct_option: SHA-256.

Question 156: START
Which of the following is the primary function of a packet filtering firewall? (CO2)
Question 156: END
Option_a: To filter network packets based on predefined rules such as IP addresses and ports
Option_b: To encrypt network data for secure transmission
Option_c: To assign IP addresses to devices on the network
Option_d: To authenticate users before allowing access
Correct_option: To filter network packets based on predefined rules such as IP addresses and ports.

Question 157: START
Which of the following is a technique used in network security to verify the authenticity of a user or device? (CO2)
Question 157: END
Option_a: Authentication
Option_b: Encryption
Option_c: Routing
Option_d: Auditing
Correct_option: Authentication.

Question 158: START
What is the primary role of an email security gateway? (CO2)
Question 158: END
Option_a: To filter out spam and malicious content in email messages
Option_b: To configure email server settings
Option_c: To assign encryption keys for email transmission
Option_d: To manage user email accounts
Correct_option: To filter out spam and malicious content in email messages.

Question 159: START
Which of the following is a type of attack that involves overwhelming a network with excessive traffic to cause a disruption? (CO2)
Question 159: END
Option_a: Denial-of-Service (DoS)
Option_b: Phishing
Option_c: Brute force
Option_d: Man-in-the-middle
Correct_option: Denial-of-Service (DoS).

Question 160: START
Which of the following encryption techniques uses a single key for both encryption and decryption? (CO2)
Question 160: END
Option_a: Symmetric encryption
Option_b: Asymmetric encryption
Option_c: Digital signatures
Option_d: Hashing
Correct_option: Symmetric encryption.

Question 161: START
Which of the following protocols is used to secure web traffic? (CO2)
Question 161: END
Option_a: HTTPS
Option_b: FTP
Option_c: SMTP
Option_d: IMAP
Correct_option: HTTPS.

Question 162: START
What is the purpose of the IPsec protocol in network security? (CO2)
Question 162: END
Option_a: To secure IP communications by encrypting and authenticating traffic
Option_b: To assign IP addresses to devices
Option_c: To configure the firewall settings

Option_d: To monitor network traffic
Correct_option: To secure IP communications by encrypting and authenticating traffic.

Question 163: START
Which of the following best describes a denial-of-service (DoS) attack? (CO2)
Question 163: END
Option_a: An attack that floods a network with traffic to disrupt its operation
Option_b: An attack that intercepts and alters communications between two parties
Option_c: An attack that attempts to obtain sensitive information by impersonating a legitimate user
Option_d: An attack that exploits vulnerabilities in a web application
Correct_option: An attack that floods a network with traffic to disrupt its operation.

Question 164: START
Which of the following is a key characteristic of a public-key cryptosystem? (CO2)
Question 164: END
Option_a: It uses a pair of keys (public and private) for encryption and decryption
Option_b: It uses the same key for both encryption and decryption
Option_c: It uses hashing algorithms to encrypt data
Option_d: It encrypts data without requiring a key
Correct_option: It uses a pair of keys (public and private) for encryption and decryption.

Question 165: START
What does SSL/TLS provide for secure communications over the internet? (CO2)
Question 165: END
Option_a: Encryption, integrity, and authentication
Option_b: Authentication only
Option_c: Encryption only
Option_d: Integrity only
Correct_option: Encryption, integrity, and authentication.

Question 166: START
Which of the following is a tool used to analyze network traffic for security purposes? (CO2)
Question 166: END
Option_a: Wireshark
Option_b: Netstat
Option_c: SSH
Option_d: FTP
Correct_option: Wireshark.

Question 167: START
What is the main purpose of a DMZ (Demilitarized Zone) in network architecture? (CO2)
Question 167: END
Option_a: To provide an additional layer of security between the internal network and the internet

Option_b: To encrypt data transmitted over the network
Option_c: To manage IP address allocation
Option_d: To assign secure IP addresses to devices
Correct_option: To provide an additional layer of security between the internal network and the internet.

Question 168: START
Which of the following encryption algorithms is widely used for encrypting email messages? (CO2)
Question 168: END
Option_a: PGP (Pretty Good Privacy)
Option_b: AES
Option_c: SHA-256
Option_d: RSA
Correct_option: PGP (Pretty Good Privacy).

Question 169: START
Which of the following techniques is used to prevent unauthorized access to a network? (CO2)
Question 169: END
Option_a: Firewalls
Option_b: Encryption
Option_c: Authentication
Option_d: Hashing
Correct_option: Firewalls.

Question 170: START
Which of the following is a type of malware that can replicate itself and spread to other systems? (CO2)
Question 170: END
Option_a: Worm
Option_b: Trojan horse
Option_c: Virus
Option_d: Spyware
Correct_option: Worm.

Question 171: START
Which of the following best describes a vulnerability scan? (CO2)
Question 171: END
Option_a: A tool used to identify potential security weaknesses in a network
Option_b: A tool used to encrypt network traffic
Option_c: A tool used to monitor network traffic for suspicious activity
Option_d: A tool used to block unauthorized traffic
Correct_option: A tool used to identify potential security weaknesses in a network.

Question 172: START
What is the primary function of an intrusion detection system (IDS)? (CO2)
Question 172: END
Option_a: To monitor network traffic for malicious activity and alert administrators
Option_b: To prevent unauthorized access to a network
Option_c: To encrypt network communications
Option_d: To manage security policies
Correct_option: To monitor network traffic for malicious activity and alert administrators.

Question 173: START
Which of the following is used to secure communication in a virtual private network (VPN)? (CO2)
Question 173: END
Option_a: IPsec
Option_b: Telnet
Option_c: SMTP
Option_d: HTTP
Correct_option: IPsec.

Question 174: START
What is the role of the private key in asymmetric encryption? (CO2)
Question 174: END
Option_a: To decrypt data that has been encrypted with the public key
Option_b: To encrypt data for secure transmission
Option_c: To authenticate the sender's identity
Option_d: To generate a hash of the data
Correct_option: To decrypt data that has been encrypted with the public key.

Question 175: START
Which of the following is an advantage of asymmetric encryption? (CO2)
Question 175: END
Option_a: It eliminates the need to securely share a key
Option_b: It is faster than symmetric encryption
Option_c: It does not require a public key
Option_d: It requires only one key for both encryption and decryption
Correct_option: It eliminates the need to securely share a key.

Question 176: START
Which of the following is an example of a brute-force attack? (CO2)
Question 176: END
Option_a: Trying all possible password combinations to gain unauthorized access
Option_b: Intercepting data to steal sensitive information
Option_c: Sending phishing emails to deceive users
Option_d: Using a virus to infect a computer
Correct_option: Trying all possible password combinations to gain unauthorized access.

Question 177: START
Which of the following techniques is used to ensure data privacy when transmitting sensitive information over a network? (CO2)
Question 177: END
Option_a: Encryption
Option_b: Hashing
Option_c: Key management
Option_d: Authentication
Correct_option: Encryption.

Question 178: START
What is the purpose of a digital certificate? (CO2)
Question 178: END
Option_a: To authenticate the identity of the sender and ensure the integrity of the message
Option_b: To encrypt the data in transit
Option_c: To manage the keys used in encryption
Option_d: To assign IP addresses to devices
Correct_option: To authenticate the identity of the sender and ensure the integrity of the message.

Question 179: START
Which of the following describes a man-in-the-middle (MITM) attack? (CO2)
Question 179: END
Option_a: An attacker intercepts and potentially alters the communication between two parties
Option_b: An attacker sends unsolicited messages to deceive users into revealing sensitive information
Option_c: An attacker floods the network with traffic to disrupt its operation
Option_d: An attacker exploits vulnerabilities in a web application to steal data
Correct_option: An attacker intercepts and potentially alters the communication between two parties.

Question 180: START
What is the purpose of a key management system (KMS) in network security? (CO2)
Question 180: END
Option_a: To securely generate, store, and distribute encryption keys
Option_b: To monitor network traffic for malicious activity
Option_c: To filter incoming and outgoing network traffic
Option_d: To authenticate users before allowing access to the network
Correct_option: To securely generate, store, and distribute encryption keys.

Question 181: START
Which of the following is a key feature of an SSL certificate? (CO2)
Question 181: END
Option_a: It verifies the identity of the website and encrypts communication
Option_b: It assigns a unique IP address to the website

Option_c: It manages the server's firewall
Option_d: It prevents denial-of-service attacks
Correct_option: It verifies the identity of the website and encrypts communication.

Question 182: START
Which of the following is an example of two-factor authentication? (CO2)
Question 182: END
Option_a: Using a password and a verification code sent to your mobile device
Option_b: Using a username and password
Option_c: Using a fingerprint for authentication
Option_d: Using a public key and private key pair
Correct_option: Using a password and a verification code sent to your mobile device.

Question 183: START
What does the term 'spoofing' refer to in network security? (CO2)
Question 183: END
Option_a: The act of pretending to be someone else by falsifying data or identities
Option_b: The process of encrypting communication over the network
Option_c: The act of filtering network traffic based on specific rules
Option_d: The method used to generate secure passwords
Correct_option: The act of pretending to be someone else by falsifying data or identities.

Question 184: START
Which of the following is the most secure method for transmitting sensitive information over the internet? (CO2)
Question 184: END
Option_a: Using HTTPS with SSL/TLS encryption
Option_b: Sending it in plain text via email
Option_c: Using FTP with a username and password
Option_d: Using Telnet to transmit data
Correct_option: Using HTTPS with SSL/TLS encryption.

Question 185: START
Which of the following is a method of securing communications in a network through the use of symmetric encryption? (CO2)
Question 185: END
Option_a: AES (Advanced Encryption Standard)
Option_b: RSA (Rivest-Shamir-Adleman)
Option_c: ECC (Elliptic Curve Cryptography)
Option_d: SHA (Secure Hash Algorithm)
Correct_option: AES (Advanced Encryption Standard).

Question 186: START
What is the role of public key infrastructure (PKI) in network security? (CO2)

Question 186: END
Option_a: To manage digital keys for encryption and authentication
Option_b: To monitor network traffic for suspicious activities
Option_c: To assign IP addresses to devices
Option_d: To authenticate devices through physical means
Correct_option: To manage digital keys for encryption and authentication.

Question 187: START
Which of the following best describes the purpose of an email phishing attack? (CO2)
Question 187: END
Option_a: To trick users into revealing sensitive information such as passwords or credit card numbers
Option_b: To infect users' devices with a virus
Option_c: To block network traffic
Option_d: To encrypt users' files
Correct_option: To trick users into revealing sensitive information such as passwords or credit card numbers.

Question 188: START
What does a zero-day exploit refer to in network security? (CO2)
Question 188: END
Option_a: A vulnerability that is exploited by attackers before the vendor has issued a fix
Option_b: A vulnerability that is already known and patched
Option_c: A security breach that occurs at midnight
Option_d: A type of denial-of-service attack
Correct_option: A vulnerability that is exploited by attackers before the vendor has issued a fix.

Question 189: START
What is the purpose of the SSH protocol in network security? (CO2)
Question 189: END
Option_a: To secure remote login and command execution over an unsecured network
Option_b: To manage digital certificates
Option_c: To encrypt emails
Option_d: To filter network traffic
Correct_option: To secure remote login and command execution over an unsecured network.

Question 190: START
Which of the following is a primary function of a web application firewall (WAF)? (CO2)
Question 190: END
Option_a: To filter and monitor HTTP traffic to and from a web application
Option_b: To encrypt traffic between a client and server
Option_c: To manage user access to a website
Option_d: To filter network traffic based on IP address
Correct_option: To filter and monitor HTTP traffic to and from a web application.

Question 191: START
Which of the following is an example of an encryption method used for securing data on a mobile device? (CO2)
Question 191: END
Option_a: Full-disk encryption
Option_b: File compression
Option_c: Data mining
Option_d: Data normalization
Correct_option: Full-disk encryption.

Question 192: START
What is the role of multi-factor authentication (MFA) in network security? (CO2)
Question 192: END
Option_a: To increase the level of security by requiring multiple forms of verification
Option_b: To encrypt communication between devices
Option_c: To configure network firewalls
Option_d: To detect network traffic anomalies
Correct_option: To increase the level of security by requiring multiple forms of verification.

Question 193: START
Which of the following is the main purpose of a data loss prevention (DLP) system? (CO2)
Question 193: END
Option_a: To monitor and prevent the unauthorized transfer of sensitive data
Option_b: To provide encryption for data at rest
Option_c: To prevent denial-of-service attacks
Option_d: To monitor network traffic for malicious activity
Correct_option: To monitor and prevent the unauthorized transfer of sensitive data.

Question 194: START
What does the term "end-to-end encryption" mean? (CO2)
Question 194: END
Option_a: Data is encrypted at the sender's side and decrypted at the receiver's side
Option_b: Data is encrypted on the server and decrypted on the client
Option_c: Data is encrypted on each intermediary device along the path
Option_d: Data is encrypted using symmetric keys
Correct_option: Data is encrypted at the sender's side and decrypted at the receiver's side.

Question 195: START
Which of the following is an example of social engineering? (CO2)
Question 195: END
Option_a: Tricking an individual into revealing personal information by impersonating a legitimate entity
Option_b: Exploiting vulnerabilities in software to gain unauthorized access
Option_c: Encrypting communication to prevent interception

Option_d: Using a virus to disrupt operations
Correct_option: Tricking an individual into revealing personal information by impersonating a legitimate entity.

Question 196: START
Which of the following best describes the function of SSL/TLS certificates in web applications? (CO2)
Question 196: END
Option_a: To secure communication and ensure data integrity between the client and server
Option_b: To authenticate users before allowing access
Option_c: To generate encryption keys for data transfer
Option_d: To monitor network traffic for malicious activity
Correct_option: To secure communication and ensure data integrity between the client and server.

Question 197: START
What is the purpose of a digital signature in public key infrastructure (PKI)? (CO2)
Question 197: END
Option_a: To authenticate the identity of the sender and verify data integrity
Option_b: To encrypt the data being sent
Option_c: To manage encryption keys
Option_d: To assign IP addresses to devices
Correct_option: To authenticate the identity of the sender and verify data integrity.

Question 198: START
Which of the following is the purpose of the DNSSEC protocol? (CO2)
Question 198: END
Option_a: To secure DNS queries and prevent attacks like DNS spoofing
Option_b: To encrypt email communication
Option_c: To configure network firewalls
Option_d: To monitor network traffic
Correct_option: To secure DNS queries and prevent attacks like DNS spoofing.

Question 199: START
Which of the following is a security measure used to protect an organization's physical servers? (CO2)
Question 199: END
Option_a: Access control and monitoring of physical entry
Option_b: Encrypting network traffic
Option_c: Using multi-factor authentication
Option_d: Implementing firewalls
Correct_option: Access control and monitoring of physical entry.

Question 200: START
Which of the following is the primary purpose of a vulnerability management program? (CO2)

Question 200: END
Option_a: To identify, assess, and mitigate security vulnerabilities in the network
Option_b: To encrypt all sensitive data on the network
Option_c: To manage user credentials and access control
Option_d: To configure the firewall settings
Correct_option: To identify, assess, and mitigate security vulnerabilities in the network.

Question201: START
Which component of the Java Runtime Environment (JRE) is responsible for executing Java bytecode? (CO3)
Question201: END
Option_a: Java Compiler
Option_b: Java Virtual Machine (JVM)
Option_c: Java Development Kit (JDK)
Option_d: Java Class Loader
correct_option: Java Virtual Machine (JVM)

Question202: START
Which of the following is used to convert Java source code into bytecode? (CO3)
Question202: END
Option_a: JDK
Option_b: JVM
Option_c: Java Compiler (javac)
Option_d: JRE
correct_option: Java Compiler (javac)

Question203: START
Which security mechanism in Java prevents unauthorized access to system resources? (CO3)
Question203: END
Option_a: Java Security Manager
Option_b: Garbage Collection
Option_c: Java API
Option_d: Class Loader
correct_option: Java Security Manager

Question204: START
What is the primary role of the Java Class Loader? (CO3)
Question204: END

Option_a: Encrypting Java classes
Option_b: Loading Java classes dynamically at runtime
Option_c: Managing memory allocation
Option_d: Handling network communication
correct_option: Loading Java classes dynamically at runtime

Question205: START
Which feature of Java makes it platform-independent? (CO3)
Question205: END
Option_a: Garbage Collection
Option_b: Bytecode Execution in JVM
Option_c: Dynamic Binding
Option_d: Just-In-Time Compilation
correct_option: Bytecode Execution in JVM

Question206: START
Which of the following is NOT a security feature in Java? (CO3)
Question206: END
Option_a: Class Loader
Option_b: Java Security Manager
Option_c: Sandbox Environment
Option_d: SQL Injection Protection
correct_option: SQL Injection Protection

Question207: START
What is the primary function of Java's Just-In-Time (JIT) compiler? (CO3)
Question207: END
Option_a: Convert Java source code to bytecode
Option_b: Compile bytecode to machine code at runtime
Option_c: Manage Java memory efficiently
Option_d: Encrypt Java applications
correct_option: Compile bytecode to machine code at runtime

Question208: START
Which Java API is used for cryptographic operations such as encryption and decryption? (CO3)
Question208: END
Option_a: java.net
Option_b: java.io
Option_c: javax.crypto

Option_d: java.util
correct_option: javax.crypto

Question209: START
Which of the following is a common vulnerability in CGI applications? (CO3)
Question209: END
Option_a: SQL Injection
Option_b: Cross-Site Request Forgery (CSRF)
Option_c: Buffer Overflow
Option_d: All of the above
correct_option: All of the above

Question210: START
How can CGI vulnerabilities be minimized? (CO3)
Question210: END
Option_a: Input validation
Option_b: Using secure HTTP methods
Option_c: Restricting user privileges
Option_d: All of the above
correct_option: All of the above

Question211: START
Which of the following best describes Secure Sockets Layer (SSL) in Java? (CO3)
Question211: END
Option_a: A protocol for encrypting HTTP traffic
Option_b: A Java security package
Option_c: A feature of the Java Virtual Machine
Option_d: A type of database encryption
correct_option: A protocol for encrypting HTTP traffic

Question212: START
Which Java package is used for implementing security policies? (CO3)
Question212: END
Option_a: java.security
Option_b: java.policy
Option_c: javax.crypto
Option_d: java.util
correct_option: java.security

Question213: START
What is the purpose of Java's Security Manager? (CO3)
Question213: END
Option_a: Enforcing access control policies
Option_b: Managing memory allocation
Option_c: Improving performance
Option_d: Handling garbage collection
correct_option: Enforcing access control policies

Question214: START
How does Java ensure memory safety? (CO3)
Question214: END
Option_a: Garbage Collection
Option_b: Explicit Memory Management
Option_c: Manual Deallocation
Option_d: Low-Level Pointers
correct_option: Garbage Collection

Question215: START
What is the primary role of the Java Cryptography Architecture (JCA)? (CO3)
Question215: END
Option_a: Managing Java network security
Option_b: Defining a framework for cryptographic services
Option_c: Handling Java exceptions
Option_d: Implementing the Security Manager
correct_option: Defining a framework for cryptographic services

Question216: START
Which of the following security threats can affect Java web applications? (CO3)
Question216: END
Option_a: Cross-Site Scripting (XSS)
Option_b: SQL Injection
Option_c: Session Hijacking
Option_d: All of the above
correct_option: All of the above

Question217: START
What is the purpose of Java's SecureRandom class? (CO3)
Question217: END
Option_a: Generating random numbers for cryptographic operations
Option_b: Encrypting Java files
Option_c: Managing Java threads
Option_d: Implementing the Java Security Manager
correct_option: Generating random numbers for cryptographic operations

Question218: START
Which method can be used to protect sensitive data in Java? (CO3)
Question218: END
Option_a: Using strong encryption algorithms
Option_b: Storing data in plaintext
Option_c: Disabling security features
Option_d: Using hardcoded credentials
correct_option: Using strong encryption algorithms

Question219: START
Which Java security feature prevents untrusted code from accessing system resources? (CO3)
Question219: END
Option_a: Java Security Manager
Option_b: Java Compiler
Option_c: Garbage Collector
Option_d: JVM Profiler
correct_option: Java Security Manager

Question220: START
What is the primary function of Java's Access Control Mechanism? (CO3)
Question220: END
Option_a: Restricting unauthorized access to system resources
Option_b: Managing database queries
Option_c: Optimizing Java performance
Option_d: Encrypting Java bytecode
correct_option: Restricting unauthorized access to system resources

Question221: START
Which Java feature prevents memory leaks by automatically reclaiming unused memory? (CO3)
Question221: END

Option_a: Garbage Collection
Option_b: Stack Management
Option_c: Manual Memory Allocation
Option_d: Memory Pooling
correct_option: Garbage Collection

Question222: START
Which Java component ensures secure execution of Java programs by verifying bytecode? (CO3)
Question222: END
Option_a: Security Manager
Option_b: Bytecode Verifier
Option_c: Class Loader
Option_d: Just-In-Time Compiler
correct_option: Bytecode Verifier

Question223: START
Which Java framework helps in managing authentication and authorization? (CO3)
Question223: END
Option_a: Spring Security
Option_b: Hibernate
Option_c: JavaFX
Option_d: Java Collections Framework
correct_option: Spring Security

Question224: START
What is the primary function of Java's Policy Tool? (CO3)
Question224: END
Option_a: Encrypting Java applications
Option_b: Managing security policies for Java applications
Option_c: Compiling Java source code
Option_d: Debugging Java programs
correct_option: Managing security policies for Java applications

Question225: START
Which security feature in Java allows restricting file and network access? (CO3)
Question225: END
Option_a: Security Manager
Option_b: Bytecode Verifier
Option_c: Class Loader

Option_d: Garbage Collector
correct_option: Security Manager

Question226: START
How does Java handle access control to sensitive system resources? (CO3)
Question226: END
Option_a: Through Access Control Mechanisms
Option_b: By using Garbage Collection
Option_c: Through Class Loading
Option_d: By disabling security features
correct_option: Through Access Control Mechanisms

Question227: START
Which of the following is a common vulnerability in CGI applications? (CO3)
Question227: END
Option_a: Cross-Site Scripting (XSS)
Option_b: Buffer Overflow
Option_c: SQL Injection
Option_d: All of the above
correct_option: All of the above

Question228: START
What is the best practice for securing CGI scripts? (CO3)
Question228: END
Option_a: Proper input validation
Option_b: Running scripts with minimal privileges
Option_c: Using secure HTTP methods
Option_d: All of the above
correct_option: All of the above

Question229: START
Which of the following is an effective way to minimize SSI vulnerabilities? (CO3)
Question229: END
Option_a: Disabling unnecessary server-side includes
Option_b: Implementing strict access control
Option_c: Using secure scripting languages
Option_d: All of the above
correct_option: All of the above

Question230: START
How can developers protect sensitive data in Java applications? (CO3)
Question230: END
Option_a: Encrypting sensitive data
Option_b: Avoiding storing sensitive data in plaintext
Option_c: Using secure authentication mechanisms
Option_d: All of the above
correct_option: All of the above

Question231: START
What is the role of Java's AccessController class? (CO3)
Question231: END
Option_a: Enforcing security policies
Option_b: Managing Java threads
Option_c: Optimizing Java performance
Option_d: Handling network requests
correct_option: Enforcing security policies

Question232: START
Which of the following helps in preventing SQL Injection attacks? (CO3)
Question232: END
Option_a: Using Prepared Statements
Option_b: Using User Input Directly in Queries
Option_c: Storing Queries in Plaintext Files
Option_d: None of the above
correct_option: Using Prepared Statements

Question233: START
Which Java API helps in managing security certificates? (CO3)
Question233: END
Option_a: java.security.cert
Option_b: javax.crypto
Option_c: java.net
Option_d: java.io
correct_option: java.security.cert

Question234: START
How can Java applications securely store user credentials? (CO3)
Question234: END
Option_a: Using strong hashing algorithms like bcrypt
Option_b: Storing credentials in plaintext

Option_c: Hardcoding passwords in source code
Option_d: Using base64 encoding
correct_option: Using strong hashing algorithms like bcrypt

Question235: START
What is the main advantage of Java's sandbox security model? (CO3)
Question235: END
Option_a: Prevents untrusted code from accessing system resources
Option_b: Improves garbage collection efficiency
Option_c: Helps in debugging Java programs
Option_d: Enhances performance of Java applications
correct_option: Prevents untrusted code from accessing system resources

Question236: START
Which of the following is a security risk when using Java serialization? (CO3)
Question236: END
Option_a: Deserialization of untrusted data
Option_b: Garbage collection failures
Option_c: Memory leaks
Option_d: Slow execution time
correct_option: Deserialization of untrusted data

Question237: START
What is the primary function of Java's ProtectionDomain class? (CO3)
Question237: END
Option_a: Defines security policies for Java classes
Option_b: Handles memory management
Option_c: Manages class loading
Option_d: Manages HTTP requests
correct_option: Defines security policies for Java classes

Question238: START
Which of the following is NOT a common CGI security vulnerability? (CO3)
Question238: END
Option_a: Buffer Overflow
Option_b: Cross-Site Request Forgery (CSRF)
Option_c: SQL Injection
Option_d: Java Garbage Collection
correct_option: Java Garbage Collection

Question239: START
What is the main function of Java's keystore? (CO3)
Question239: END
Option_a: Storing cryptographic keys securely
Option_b: Managing database connections
Option_c: Handling Java threads
Option_d: Performing garbage collection
correct_option: Storing cryptographic keys securely

Question240: START
Which of the following is an effective way to secure Java web applications? (CO3)
Question240: END
Option_a: Using HTTPS for data transmission
Option_b: Validating user input to prevent injection attacks
Option_c: Implementing authentication and authorization mechanisms
Option_d: All of the above
correct_option: All of the above

Question241: START
Which Java security feature prevents unauthorized access to classes and methods? (CO3)
Question241: END
Option_a: Java Access Modifiers
Option_b: Java Compiler
Option_c: Java Security Manager
Option_d: Class Loader
correct_option: Java Access Modifiers

Question242: START
What does the Java KeyStore (JKS) store? (CO3)
Question242: END
Option_a: Private and public keys
Option_b: Java class files
Option_c: JVM configuration settings
Option_d: Garbage collection logs
correct_option: Private and public keys

Question243: START
Which of the following prevents arbitrary code execution in Java? (CO3)
Question243: END
Option_a: Security Manager
Option_b: Garbage Collection

Option_c: Thread Management
Option_d: JIT Compiler
correct_option: Security Manager

Question244: START
What is the purpose of Java's doPrivileged method? (CO3)
Question244: END
Option_a: Executes code with elevated privileges
Option_b: Encrypts Java files
Option_c: Manages memory
Option_d: Handles exceptions
correct_option: Executes code with elevated privileges

Question245: START
How can Java applications securely manage user authentication? (CO3)
Question245: END
Option_a: Implementing multi-factor authentication
Option_b: Storing passwords in plaintext
Option_c: Hardcoding credentials
Option_d: Disabling authentication
correct_option: Implementing multi-factor authentication

Question246: START
Which Java package is used for implementing SSL/TLS security? (CO3)
Question246: END
Option_a: javax.net.ssl
Option_b: java.security
Option_c: javax.crypto
Option_d: java.nio
correct_option: javax.net.ssl

Question247: START
Which attack can be prevented using Java's PreparedStatement? (CO3)
Question247: END
Option_a: SQL Injection
Option_b: Buffer Overflow
Option_c: Cross-Site Scripting (XSS)
Option_d: Denial of Service
correct_option: SQL Injection

Question248: START
What is the purpose of Java's SecureRandom class? (CO3)
Question248: END
Option_a: Generating cryptographically secure random numbers
Option_b: Managing Java threads
Option_c: Handling Java exceptions
Option_d: Encrypting Java files
correct_option: Generating cryptographically secure random numbers

Question249: START
How can Java applications protect against session hijacking? (CO3)
Question249: END
Option_a: Using HTTPS
Option_b: Implementing session timeouts
Option_c: Regenerating session IDs after login
Option_d: All of the above
correct_option: All of the above

Question250: START
Which Java API provides functionality for digital signatures? (CO3)
Question250: END
Option_a: java.security.Signature
Option_b: java.nio.file
Option_c: java.util.Date
Option_d: java.net.HttpURLConnection
correct_option: java.security.Signature

Question251: START
Which of the following helps in preventing Cross-Site Scripting (XSS) attacks in Java applications? (CO3)
Question251: END
Option_a: Input validation
Option_b: Encoding user input
Option_c: Using Content Security Policy (CSP)
Option_d: All of the above
correct_option: All of the above

Question252: START
What is the role of Java's AccessController class? (CO3)
Question252: END
Option_a: Enforces access control policies

Option_b: Manages Java threads
Option_c: Handles garbage collection
Option_d: Encrypts Java files
correct_option: Enforces access control policies

Question253: START
Which Java security feature ensures bytecode integrity? (CO3)
Question253: END
Option_a: Bytecode Verifier
Option_b: Just-In-Time Compiler
Option_c: Garbage Collector
Option_d: Thread Scheduler
correct_option: Bytecode Verifier

Question254: START
Which Java class is used for message authentication codes (MAC)? (CO3)
Question254: END
Option_a: javax.crypto.Mac
Option_b: java.security.MessageDigest
Option_c: java.util.HashMap
Option_d: java.io.File
correct_option: javax.crypto.Mac

Question255: START
Which Java API provides encryption and decryption functionality? (CO3)
Question255: END
Option_a: javax.crypto
Option_b: java.sql
Option_c: java.nio.file
Option_d: java.net
correct_option: javax.crypto

Question256: START
How can Java applications prevent clickjacking attacks? (CO3)
Question256: END
Option_a: Using X-Frame-Options header
Option_b: Implementing Content Security Policy (CSP)
Option_c: Using frame-busting scripts
Option_d: All of the above
correct_option: All of the above

Question257: START
Which of the following is a best practice for handling sensitive data in Java applications? (CO3)
Question257: END
Option_a: Encrypting sensitive data
Option_b: Avoiding hardcoded credentials
Option_c: Using secure key management
Option_d: All of the above
correct_option: All of the above

Question258: START
What is the primary purpose of Java's SecurityManager class? (CO3)
Question258: END
Option_a: Enforcing security policies
Option_b: Managing Java threads
Option_c: Handling garbage collection
Option_d: Encrypting Java files
correct_option: Enforcing security policies

Question259: START
Which Java security mechanism prevents unauthorized access to system resources? (CO3)
Question259: END
Option_a: Security Manager
Option_b: Garbage Collection
Option_c: Just-In-Time Compilation
Option_d: Java Compiler
correct_option: Security Manager

Question260: START
Which Java security tool is used for managing keystores? (CO3)
Question260: END
Option_a: keytool
Option_b: jconsole
Option_c: jstack
Option_d: jstat
correct_option: keytool

Question261: START
Which of the following is the best method to protect sensitive data from unauthorized access? (CO3)
Question261: END
Option_a: Encrypting data at rest and in transit
Option_b: Storing passwords in plaintext
Option_c: Using weak hashing algorithms
Option_d: Allowing unrestricted access to data
correct_option: Encrypting data at rest and in transit

Question262: START
Which of the following helps minimize vulnerabilities in Server-Side Includes (SSI)? (CO3)
Question262: END
Option_a: Disabling SSI when not needed
Option_b: Allowing unrestricted file execution
Option_c: Running SSI scripts with administrative privileges
Option_d: Avoiding input validation
correct_option: Disabling SSI when not needed

Question263: START
What is the primary risk of enabling Server-Side Includes (SSI) on a web server? (CO3)
Question263: END
Option_a: Unauthorized file access and execution
Option_b: Slow website performance
Option_c: Increased database load
Option_d: Poor user experience
correct_option: Unauthorized file access and execution

Question264: START
Which method is the most effective for securely storing passwords? (CO3)
Question264: END
Option_a: Storing in plaintext
Option_b: Using SHA-1 hashing
Option_c: Hashing with bcrypt or Argon2
Option_d: Encrypting passwords with a reversible algorithm
correct_option: Hashing with bcrypt or Argon2

Question265: START
Which practice helps protect sensitive data in transit? (CO3)
Question265: END
Option_a: Using HTTPS/TLS encryption

Option_b: Sending data over HTTP
Option_c: Storing sensitive data in session cookies
Option_d: Using weak encryption algorithms
correct_option: Using HTTPS/TLS encryption

Question266: START
How can developers prevent injection attacks in SSI-enabled applications? (CO3)
Question266: END
Option_a: Validating and sanitizing user input
Option_b: Allowing all input without checks
Option_c: Running SSI scripts with high privileges
Option_d: Disabling all security headers
correct_option: Validating and sanitizing user input

Question267: START
What is the primary purpose of Data Loss Prevention (DLP) solutions? (CO3)
Question267: END
Option_a: Detecting and preventing unauthorized data transfers
Option_b: Increasing system performance
Option_c: Encrypting all stored data
Option_d: Managing network traffic
correct_option: Detecting and preventing unauthorized data transfers

Question268: START
Which of the following is an effective way to secure API keys? (CO3)
Question268: END
Option_a: Storing them in environment variables
Option_b: Hardcoding them in source code
Option_c: Sharing them publicly
Option_d: Using weak encryption
correct_option: Storing them in environment variables

Question269: START
How can organizations protect sensitive files from unauthorized access? (CO3)
Question269: END
Option_a: Implementing file encryption
Option_b: Using open file permissions
Option_c: Storing sensitive data in public directories
Option_d: Sharing files over unsecured email
correct_option: Implementing file encryption

Question270: START
What is the best way to prevent directory traversal attacks in SSI? (CO3)
Question270: END
Option_a: Restricting file access to necessary directories
Option_b: Allowing direct file execution
Option_c: Running all scripts with administrator rights
Option_d: Disabling all security configurations
correct_option: Restricting file access to necessary directories

Question271: START
Which security measure helps protect sensitive database records? (CO3)
Question271: END
Option_a: Implementing encryption for stored data
Option_b: Allowing unrestricted database queries
Option_c: Disabling authentication for database access
Option_d: Storing data in plaintext
correct_option: Implementing encryption for stored data

Question272: START
What is a common method for minimizing SSI vulnerabilities? (CO3)
Question272: END
Option_a: Using whitelisting for allowed commands
Option_b: Allowing all commands to execute
Option_c: Disabling security patches
Option_d: Running SSI scripts with root privileges
correct_option: Using whitelisting for allowed commands

Question273: START
Which tool can help detect and prevent unauthorized data access? (CO3)
Question273: END
Option_a: Data Loss Prevention (DLP)
Option_b: Web browser
Option_c: Media Player
Option_d: Task Manager
correct_option: Data Loss Prevention (DLP)

Question274: START
What is a recommended practice for securing sensitive data in backups? (CO3)
Question274: END
Option_a: Encrypting backup files
Option_b: Storing backups in public folders
Option_c: Keeping backups unprotected
Option_d: Using weak passwords
correct_option: Encrypting backup files

Question275: START
How can organizations reduce the risk of exposing sensitive information in logs? (CO3)
Question275: END
Option_a: Masking or encrypting sensitive data
Option_b: Storing full credit card numbers in logs
Option_c: Logging all user passwords
Option_d: Making logs publicly accessible
correct_option: Masking or encrypting sensitive data

Question276: START
What is the best method to prevent unauthorized file modifications? (CO3)
Question276: END
Option_a: Implementing file integrity monitoring
Option_b: Allowing all users to modify files
Option_c: Using weak authentication methods
Option_d: Keeping file permissions open
correct_option: Implementing file integrity monitoring

Question277: START
Which of the following is a secure way to store API secrets? (CO3)
Question277: END
Option_a: Using a secrets management tool
Option_b: Hardcoding them in source code
Option_c: Storing them in publicly accessible locations
Option_d: Embedding them in URLs
correct_option: Using a secrets management tool

Question278: START
How can organizations protect sensitive data in the cloud? (CO3)
Question278: END
Option_a: Encrypting data before uploading
Option_b: Using weak authentication methods

Option_c: Disabling security features
Option_d: Storing all files in public folders
correct_option: Encrypting data before uploading

Question279: START
What is the best way to prevent unauthorized access to a web application? (CO3)
Question279: END
Option_a: Implementing multi-factor authentication (MFA)
Option_b: Allowing weak passwords
Option_c: Disabling encryption
Option_d: Sharing login credentials
correct_option: Implementing multi-factor authentication (MFA)

Question280: START
Which security measure can help protect sensitive data in transit? (CO3)
Question280: END
Option_a: Using TLS encryption
Option_b: Sending data over HTTP
Option_c: Storing credentials in URLs
Option_d: Disabling encryption
correct_option: Using TLS encryption

Question281: START
Which of the following best helps prevent privilege escalation attacks? (CO3)
Question281: END
Option_a: Implementing the principle of least privilege (PoLP)
Option_b: Assigning administrative rights to all users
Option_c: Disabling access controls
Option_d: Running all applications as root
correct_option: Implementing the principle of least privilege (PoLP)

Question282: START
What is an effective way to secure sensitive configuration files? (CO3)
Question282: END
Option_a: Restricting file access permissions
Option_b: Storing files in publicly accessible locations
Option_c: Embedding secrets in source code
Option_d: Allowing all users to modify configurations
correct_option: Restricting file access permissions

Question283: START
Which technique can help secure session data? (CO3)
Question283: END
Option_a: Using secure, HttpOnly cookies
Option_b: Storing session data in local storage
Option_c: Allowing session IDs in URLs
Option_d: Using plaintext session tokens
correct_option: Using secure, HttpOnly cookies

Question284: START
How can developers prevent cross-site scripting (XSS) attacks? (CO3)
Question284: END
Option_a: Encoding user input
Option_b: Allowing script execution in input fields
Option_c: Disabling security features
Option_d: Storing user input without validation
correct_option: Encoding user input

Question285: START
Which of the following helps in securing database queries? (CO3)
Question285: END
Option_a: Using parameterized queries
Option_b: Allowing direct user input in SQL queries
Option_c: Storing SQL queries in client-side scripts
Option_d: Hardcoding credentials in queries
correct_option: Using parameterized queries

Question286: START
What is an effective method to prevent unauthorized data access in cloud environments? (CO3)
Question286: END
Option_a: Using strong access controls
Option_b: Storing sensitive data in public cloud storage
Option_c: Allowing default credentials
Option_d: Disabling encryption
correct_option: Using strong access controls

Question287: START
How can organizations prevent unauthorized physical access to sensitive data? (CO3)

Question287: END
Option_a: Implementing biometric authentication
Option_b: Leaving data storage devices unlocked
Option_c: Storing sensitive documents in open areas
Option_d: Using shared login credentials
correct_option: Implementing biometric authentication

Question288: START
What is the primary purpose of encryption for sensitive data? (CO3)
Question288: END
Option_a: Protecting data confidentiality
Option_b: Improving data processing speed
Option_c: Reducing storage space
Option_d: Making data accessible to all users
correct_option: Protecting data confidentiality

Question289: START
Which of the following is an example of a secure hashing algorithm? (CO3)
Question289: END
Option_a: SHA-256
Option_b: MD5
Option_c: Base64
Option_d: ROT13
correct_option: SHA-256

Question290: START
How can developers securely store API authentication credentials? (CO3)
Question290: END
Option_a: Using a vault or secrets management system
Option_b: Hardcoding credentials in source code
Option_c: Storing API keys in public repositories
Option_d: Embedding secrets in URLs
correct_option: Using a vault or secrets management system

Question291: START
Which security measure helps protect against man-in-the-middle (MITM) attacks? (CO3)
Question291: END
Option_a: Enforcing TLS encryption
Option_b: Using HTTP for all connections

Option_c: Disabling authentication mechanisms
Option_d: Allowing self-signed certificates
correct_option: Enforcing TLS encryption

Question292: START
How can organizations prevent unauthorized API access? (CO3)
Question292: END
Option_a: Using API keys and OAuth
Option_b: Allowing unrestricted API calls
Option_c: Disabling authentication
Option_d: Embedding API credentials in client-side scripts
correct_option: Using API keys and OAuth

Question293: START
Which of the following is a best practice for managing encryption keys? (CO3)
Question293: END
Option_a: Storing them in a secure key management system
Option_b: Hardcoding keys in application code
Option_c: Using weak encryption algorithms
Option_d: Sharing encryption keys publicly
correct_option: Storing them in a secure key management system

Question294: START
What is the best way to ensure file integrity? (CO3)
Question294: END
Option_a: Using file hashing and digital signatures
Option_b: Allowing unrestricted file modifications
Option_c: Storing files in publicly accessible directories
Option_d: Using weak access control mechanisms
correct_option: Using file hashing and digital signatures

Question295: START
Which of the following security practices helps prevent data breaches? (CO3)
Question295: END
Option_a: Implementing strong access control policies
Option_b: Storing sensitive data in plaintext
Option_c: Using weak passwords
Option_d: Allowing public access to confidential information
correct_option: Implementing strong access control policies

Question296: START
What is the recommended method to secure sensitive user input? (CO3)
Question296: END
Option_a: Validating and sanitizing input
Option_b: Accepting all user input without checks
Option_c: Storing user input directly in logs
Option_d: Disabling security features
correct_option: Validating and sanitizing input

Question297: START
Which of the following is a secure method for handling user authentication? (CO3)
Question297: END
Option_a: Using multi-factor authentication (MFA)
Option_b: Hardcoding user passwords
Option_c: Using weak password policies
Option_d: Storing passwords in plaintext
correct_option: Using multi-factor authentication (MFA)

Question298: START
Which of the following helps in preventing unauthorized data modifications? (CO3)
Question298: END
Option_a: Implementing access control lists (ACLs)
Option_b: Allowing unrestricted file changes
Option_c: Disabling logging mechanisms
Option_d: Using default security configurations
correct_option: Implementing access control lists (ACLs)

Question299: START
What is the primary function of audit logs in security? (CO3)
Question299: END
Option_a: Tracking and monitoring security events
Option_b: Deleting user data automatically
Option_c: Increasing system performance
Option_d: Storing user passwords
correct_option: Tracking and monitoring security events

Question300: START
How can organizations ensure secure remote access to sensitive data? (CO3)
Question300: END
Option_a: Using VPN and multi-factor authentication
Option_b: Allowing open remote access

Option_c: Disabling encryption for remote users
Option_d: Sharing login credentials via email
correct_option: Using VPN and multi-factor authentication

Question301: START
Which cryptographic technique ensures both message authentication and integrity? (CO4)
Question301: END
Option_a: Hash Function
Option_b: Digital Signature
Option_c: Message Authentication Code (MAC)
Option_d: Symmetric Encryption
correct_option: Message Authentication Code (MAC)

Question302: START
What is the primary purpose of a Message Authentication Code (MAC)? (CO4)
Question302: END
Option_a: Encrypt messages
Option_b: Verify the authenticity and integrity of a message
Option_c: Generate random numbers
Option_d: Store passwords securely
correct_option: Verify the authenticity and integrity of a message

Question303: START
Which of the following is a cryptographic hash function? (CO4)
Question303: END
Option_a: RSA
Option_b: AES
Option_c: SHA-256
Option_d: Diffie-Hellman
correct_option: SHA-256

Question304: START
Which characteristic is essential for a secure hash function? (CO4)
Question304: END
Option_a: It should be easily reversible
Option_b: It should generate the same output for different inputs
Option_c: It should be collision-resistant
Option_d: It should require a secret key
correct_option: It should be collision-resistant

Question305: START
What is the main security concern with weak hash functions like MD5 and SHA-1? (CO4)
Question305: END
Option_a: They are too slow
Option_b: They are vulnerable to collision attacks
Option_c: They require too much storage
Option_d: They cannot generate digests
correct_option: They are vulnerable to collision attacks

Question306: START
Which hashing algorithm is considered more secure for cryptographic applications? (CO4)
Question306: END
Option_a: MD5
Option_b: SHA-1
Option_c: SHA-256
Option_d: CRC32
correct_option: SHA-256

Question307: START
Which algorithm is used in Digital Signature Standard (DSS)? (CO4)
Question307: END
Option_a: RSA
Option_b: DSA
Option_c: AES
Option_d: Blowfish
correct_option: DSA

Question308: START
Which of the following properties does a digital signature provide? (CO4)
Question308: END
Option_a: Confidentiality and integrity
Option_b: Authentication and non-repudiation
Option_c: Encryption and decryption
Option_d: Compression and encoding
correct_option: Authentication and non-repudiation

Question309: START
What is the role of the private key in digital signatures? (CO4)
Question309: END
Option_a: Encrypt the message
Option_b: Generate the digital signature
Option_c: Verify the digital signature
Option_d: Convert the message to ciphertext
correct_option: Generate the digital signature

Question310: START
Which component verifies a digital signature? (CO4)
Question310: END
Option_a: Private key
Option_b: Public key
Option_c: Hash function
Option_d: Encryption algorithm
correct_option: Public key

Question311: START
What is the main advantage of using a digital signature over a simple MAC? (CO4)
Question311: END
Option_a: It provides non-repudiation
Option_b: It is faster
Option_c: It does not require a private key
Option_d: It uses symmetric encryption
correct_option: It provides non-repudiation

Question312: START
Which of the following best describes a cryptographic hash function? (CO4)
Question312: END
Option_a: A function that encrypts data using a key
Option_b: A function that generates a fixed-length digest from input data
Option_c: A function that compresses files for transmission
Option_d: A function that converts data into a different encoding format
correct_option: A function that generates a fixed-length digest from input data

Question313: START
Which of the following ensures the security of a hash function? (CO4)
Question313: END

Option_a: Pre-image resistance
Option_b: Key length
Option_c: High computational cost
Option_d: Short hash output
correct_option: Pre-image resistance

Question314: START
What is the purpose of HMAC (Hashed Message Authentication Code)? (CO4)
Question314: END
Option_a: To encrypt messages
Option_b: To authenticate and verify message integrity
Option_c: To generate keys for encryption
Option_d: To compress data
correct_option: To authenticate and verify message integrity

Question315: START
Which of the following is NOT a cryptographic hash function? (CO4)
Question315: END
Option_a: MD5
Option_b: SHA-256
Option_c: RSA
Option_d: SHA-512
correct_option: RSA

Question316: START
What is the main security concern with hash collisions? (CO4)
Question316: END
Option_a: Different inputs produce the same hash value
Option_b: Hash functions are too slow
Option_c: Hash values take up too much storage
Option_d: Hash functions can be reversed easily
correct_option: Different inputs produce the same hash value

Question317: START
Which function of a cryptographic hash is used to verify message integrity? (CO4)
Question317: END
Option_a: Hashing

Option_b: Encryption
Option_c: Decryption
Option_d: Key exchange
correct_option: Hashing

Question318: START
Which algorithm is widely used for digital signatures? (CO4)
Question318: END
Option_a: AES
Option_b: DES
Option_c: RSA
Option_d: Blowfish
correct_option: RSA

Question319: START
How does a digital signature ensure message authentication? (CO4)
Question319: END
Option_a: By encrypting the entire message
Option_b: By generating a unique hash of the message and signing it with a private key
Option_c: By using symmetric key encryption
Option_d: By hashing the message with MD5
correct_option: By generating a unique hash of the message and signing it with a private key

Question320: START
Which type of attack tries to find two different inputs that produce the same hash value? (CO4)
Question320: END
Option_a: Brute-force attack
Option_b: Collision attack
Option_c: Man-in-the-middle attack
Option_d: Side-channel attack
correct_option: Collision attack

Question321: START
Which security property does HMAC provide over standard hashing? (CO4)
Question321: END
Option_a: Confidentiality
Option_b: Authentication and integrity

Option_c: Key exchange
Option_d: Non-repudiation
correct_option: Authentication and integrity

Question322: START
What is the primary weakness of MD5 as a cryptographic hash function? (CO4)
Question322: END
Option_a: It is too slow for modern applications
Option_b: It produces long hash values
Option_c: It is vulnerable to collision attacks
Option_d: It requires a secret key
correct_option: It is vulnerable to collision attacks

Question323: START
Which of the following is a property of a secure hash function? (CO4)
Question323: END
Option_a: It should be deterministic
Option_b: It should produce variable-length output
Option_c: It should be reversible
Option_d: It should be computationally cheap
correct_option: It should be deterministic

Question324: START
Which of the following is NOT a feature of a digital signature? (CO4)
Question324: END
Option_a: Non-repudiation
Option_b: Confidentiality
Option_c: Integrity
Option_d: Authentication
correct_option: Confidentiality

Question325: START
Which algorithm is primarily used in DSS (Digital Signature Standard)? (CO4)
Question325: END
Option_a: RSA
Option_b: DSA
Option_c: AES

Option_d: SHA-256
correct_option: DSA

Question326: START
Which part of a digital signature process requires the sender's private key? (CO4)
Question326: END
Option_a: Signature generation
Option_b: Signature verification
Option_c: Hash computation
Option_d: Key exchange
correct_option: Signature generation

Question327: START
Which method is used to verify a digital signature? (CO4)
Question327: END
Option_a: Encrypting the signature with the sender's public key
Option_b: Hashing the message again and comparing it to the decrypted signature
Option_c: Re-encrypting the message
Option_d: Generating a new digital signature
correct_option: Hashing the message again and comparing it to the decrypted signature

Question328: START
What is the primary purpose of SHA (Secure Hash Algorithm)? (CO4)
Question328: END
Option_a: Encrypting sensitive data
Option_b: Generating unique hash values for data integrity verification
Option_c: Secure key exchange
Option_d: Performing symmetric encryption
correct_option: Generating unique hash values for data integrity verification

Question329: START
Which of the following provides stronger security? (CO4)
Question329: END
Option_a: SHA-1
Option_b: SHA-256
Option_c: MD5
Option_d: CRC32
correct_option: SHA-256

Question330: START
Which cryptographic function is used in digital certificates to ensure authenticity? (CO4)

Question330: END
Option_a: Hash functions
Option_b: Symmetric encryption
Option_c: Digital signatures
Option_d: Message Authentication Code (MAC)
correct_option: Digital signatures

Question331: START
What is the purpose of the Keyed-Hash Message Authentication Code (HMAC)? (CO4)
Question331: END
Option_a: Encrypting messages
Option_b: Authenticating messages and verifying integrity
Option_c: Generating digital signatures
Option_d: Managing key exchanges
correct_option: Authenticating messages and verifying integrity

Question332: START
Which of the following makes hash functions useful for authentication? (CO4)
Question332: END
Option_a: One-way property
Option_b: Reversibility
Option_c: Large computational overhead
Option_d: Use of symmetric keys
correct_option: One-way property

Question333: START
Which factor determines the strength of a cryptographic hash function? (CO4)
Question333: END
Option_a: Hash length and collision resistance
Option_b: Key exchange speed
Option_c: Encryption key size
Option_d: Use of secret keys
correct_option: Hash length and collision resistance

Question334: START
Which of the following is NOT an authentication protocol? (CO4)
Question334: END
Option_a: Kerberos
Option_b: OAuth

Option_c: SHA-256
Option_d: RADIUS
correct_option: SHA-256

Question335: START
How does a digital signature ensure data integrity? (CO4)
Question335: END
Option_a: By encrypting the entire message
Option_b: By hashing the message and signing the hash
Option_c: By using symmetric encryption
Option_d: By hashing the message twice
correct_option: By hashing the message and signing the hash

Question336: START
Which of the following best describes a one-way function? (CO4)
Question336: END
Option_a: A function that can be easily reversed
Option_b: A function that is computationally difficult to invert
Option_c: A function that encrypts data
Option_d: A function that performs key exchange
correct_option: A function that is computationally difficult to invert

Question337: START
What is the main reason SHA-1 is considered insecure? (CO4)
Question337: END
Option_a: It is too slow
Option_b: It is vulnerable to collision attacks
Option_c: It requires large storage
Option_d: It does not generate hash values
correct_option: It is vulnerable to collision attacks

Question338: START
What is the output length of SHA-256? (CO4)
Question338: END
Option_a: 128 bits
Option_b: 160 bits
Option_c: 256 bits

Option_d: 512 bits
correct_option: 256 bits

Question339: START
What is the primary security advantage of a cryptographic hash function? (CO4)
Question339: END
Option_a: It ensures data confidentiality
Option_b: It provides message authentication and integrity
Option_c: It encrypts the message
Option_d: It speeds up network transmission
correct_option: It provides message authentication and integrity

Question340: START
Which of the following is the primary use case of a digital signature? (CO4)
Question340: END
Option_a: Confidentiality
Option_b: Authentication and non-repudiation
Option_c: Data compression
Option_d: Speed optimization
correct_option: Authentication and non-repudiation

Question341: START
Which of the following is a characteristic of biometrics in entity authentication? (CO4)
Question341: END
Option_a: Requires physical tokens
Option_b: Based on unique physiological traits
Option_c: Involves memorized secrets
Option_d: Uses encryption keys
correct_option: Based on unique physiological traits

Question342: START
What is the primary function of a password in authentication? (CO4)
Question342: END
Option_a: To provide a cryptographic key for encryption
Option_b: To act as a secret shared between the user and the system
Option_c: To generate a secure session identifier
Option_d: To store user identity in a secure database
correct_option: To act as a secret shared between the user and the system

Question343: START
Which of the following describes a challenge-response authentication protocol? (CO4)

Question343: END
Option_a: Both parties share a long-term password
Option_b: One party sends a random challenge, and the other responds with a correct answer
Option_c: Both parties use the same biometric input for authentication
Option_d: A password is encrypted and transmitted over a secure channel
correct_option: One party sends a random challenge, and the other responds with a correct answer

Question344: START
What is the main advantage of biometric authentication over passwords? (CO4)
Question344: END
Option_a: It is faster to use than passwords
Option_b: It is more resistant to theft or forgery
Option_c: It is easier to remember
Option_d: It requires no additional hardware
correct_option: It is more resistant to theft or forgery

Question345: START
Which of the following is an example of a biometric factor used in authentication? (CO4)
Question345: END
Option_a: Password
Option_b: Fingerprint
Option_c: Security token
Option_d: PIN code
correct_option: Fingerprint

Question346: START
What is the primary purpose of Kerberos in authentication systems? (CO4)
Question346: END
Option_a: To secure data with end-to-end encryption
Option_b: To authenticate users in a client-server network
Option_c: To manage network traffic efficiently
Option_d: To perform one-time password generation
correct_option: To authenticate users in a client-server network

Question347: START
Which protocol is used in Kerberos to securely authenticate users in a network? (CO4)
Question347: END

Option_a: Public Key Infrastructure
Option_b: Ticket Granting Ticket (TGT)
Option_c: Secure Sockets Layer (SSL)
Option_d: Secure Hash Algorithm (SHA)
correct_option: Ticket Granting Ticket (TGT)

Question348: START
In the context of X.509 certificates, what is typically included in a certificate? (CO4)
Question348: END
Option_a: The user's password
Option_b: The user's biometric data
Option_c: The public key and associated information
Option_d: The private key for the user
correct_option: The public key and associated information

Question349: START
Which of the following is a key component of the challenge-response authentication protocol? (CO4)
Question349: END
Option_a: A shared secret between the client and server
Option_b: A random challenge issued by the server
Option_c: An encrypted password transmission
Option_d: A biometric scan
correct_option: A random challenge issued by the server

Question350: START
Which of the following is NOT a common biometric characteristic used for authentication? (CO4)
Question350: END
Option_a: Iris scan
Option_b: Fingerprint
Option_c: Voice recognition
Option_d: Personal identification number (PIN)
correct_option: Personal identification number (PIN)

Question351: START
What is the main risk associated with password-based authentication? (CO4)
Question351: END
Option_a: Passwords are hard to remember

Option_b: Passwords can be easily guessed or stolen
Option_c: Passwords require additional hardware
Option_d: Passwords require network connectivity
correct_option: Passwords can be easily guessed or stolen

Question352: START
In Kerberos, what does the Key Distribution Center (KDC) do? (CO4)
Question352: END
Option_a: It generates random passwords for users
Option_b: It issues ticket-granting tickets and service tickets
Option_c: It verifies biometric data
Option_d: It encrypts communication between clients and servers
correct_option: It issues ticket-granting tickets and service tickets

Question353: START
Which of the following is a main advantage of using challenge-response protocols for authentication? (CO4)
Question353: END
Option_a: The user's password is never transmitted over the network
Option_b: It requires a physical token to function
Option_c: It eliminates the need for cryptographic keys
Option_d: It works without any user involvement
correct_option: The user's password is never transmitted over the network

Question354: START
What does X.509 primarily deal with in the context of authentication? (CO4)
Question354: END
Option_a: Password management
Option_b: Public key infrastructure (PKI) and digital certificates
Option_c: Biometric authentication standards
Option_d: Secure network protocols
correct_option: Public key infrastructure (PKI) and digital certificates

Question355: START
Which biometric factor is typically used in fingerprint recognition systems? (CO4)
Question355: END
Option_a: Voice pitch
Option_b: Iris patterns
Option_c: Finger ridge patterns
Option_d: Hand shape
correct_option: Finger ridge patterns

Question356: START
In a challenge-response authentication system, how does the server validate the user's identity? (CO4)
Question356: END
Option_a: By comparing the response to a pre-stored password
Option_b: By matching the response with the user's biometric data
Option_c: By verifying a digital signature associated with the response
Option_d: By verifying the user's answer to a random challenge
correct_option: By verifying the user's answer to a random challenge

Question357: START
Which cryptographic method does Kerberos rely on for authentication? (CO4)
Question357: END
Option_a: Public key cryptography
Option_b: Symmetric key cryptography
Option_c: Asymmetric key cryptography
Option_d: Diffie-Hellman exchange
correct_option: Symmetric key cryptography

Question358: START
In the context of X.509 certificates, what is the role of a certificate authority (CA)? (CO4)
Question358: END
Option_a: To generate a user's public and private keys
Option_b: To issue and validate digital certificates
Option_c: To store user credentials
Option_d: To encrypt communication channels
correct_option: To issue and validate digital certificates

Question359: START
Which of the following is a major challenge when implementing biometric authentication? (CO4)
Question359: END
Option_a: Difficulty in obtaining accurate biometric samples
Option_b: Biometric data is easy to steal and forge
Option_c: Biometric authentication is too slow for practical use
Option_d: Biometric devices are too expensive
correct_option: Difficulty in obtaining accurate biometric samples

Question360: START
What is the primary benefit of using multi-factor authentication (MFA)? (CO4)
Question360: END
Option_a: It simplifies user authentication
Option_b: It provides additional layers of security beyond a single method
Option_c: It allows users to bypass password entry
Option_d: It eliminates the need for biometric data
correct_option: It provides additional layers of security beyond a single method

Question361: START
Which of the following is a disadvantage of using passwords for authentication? (CO4)
Question361: END
Option_a: Passwords are difficult to implement
Option_b: Passwords can be shared or stolen
Option_c: Passwords require expensive hardware
Option_d: Passwords are inherently faster than biometric authentication
correct_option: Passwords can be shared or stolen

Question362: START
In challenge-response authentication, which of the following is used to generate the response? (CO4)
Question362: END
Option_a: A pre-shared secret key
Option_b: A one-time password
Option_c: A cryptographic hash of the challenge
Option_d: A biometric scan
correct_option: A cryptographic hash of the challenge

Question363: START
What type of cryptography does X.509 use to secure digital certificates? (CO4)
Question363: END
Option_a: Asymmetric cryptography
Option_b: Symmetric cryptography
Option_c: Hash functions
Option_d: Quantum cryptography
correct_option: Asymmetric cryptography

Question364: START
Which authentication method is most likely to be vulnerable to brute force attacks? (CO4)

Question364: END
Option_a: Biometrics
Option_b: Passwords
Option_c: Challenge-response
Option_d: Digital certificates
correct_option: Passwords

Question365: START
What is the primary purpose of the Ticket Granting Ticket (TGT) in Kerberos? (CO4)
Question365: END
Option_a: To authenticate the client to the server
Option_b: To authenticate the server to the client
Option_c: To grant access to encrypted communication
Option_d: To request a service ticket from the KDC
correct_option: To request a service ticket from the KDC

Question366: START
In biometric systems, which of the following is typically required to ensure accuracy in matching biometric data? (CO4)
Question366: END
Option_a: High-quality sensors and training data
Option_b: A pre-shared password
Option_c: Encrypted storage for biometric data
Option_d: A secure communication protocol
correct_option: High-quality sensors and training data

Question367: START
Which of the following would most likely be used as a factor in multi-factor authentication? (CO4)
Question367: END
Option_a: A fingerprint scan
Option_b: A username and password combination
Option_c: A security question
Option_d: A challenge-response pair
correct_option: A fingerprint scan

Question368: START
What is a primary feature of the X.509 certificate in the context of public key infrastructure (PKI)? (CO4)

Question368: END
Option_a: It encrypts user passwords
Option_b: It provides a user's public key and certificate details
Option_c: It generates challenge-response tokens
Option_d: It stores biometric data
correct_option: It provides a user's public key and certificate details

Question369: START
What role does the Key Distribution Center (KDC) serve in the Kerberos protocol? (CO4)
Question369: END
Option_a: It encrypts the communication between clients
Option_b: It issues service tickets for clients
Option_c: It generates passwords for users
Option_d: It stores user credentials
correct_option: It issues service tickets for clients

Question370: START
Which is the most secure biometric authentication technique? (CO4)
Question370: END
Option_a: Fingerprint recognition
Option_b: Voice recognition
Option_c: Iris recognition
Option_d: Face recognition
correct_option: Iris recognition

Question371: START
In Kerberos, how does the client obtain a service ticket? (CO4)
Question371: END
Option_a: By providing a password to the KDC
Option_b: By sending a request to the KDC with the TGT
Option_c: By authenticating directly to the server
Option_d: By entering a one-time password
correct_option: By sending a request to the KDC with the TGT

Question372: START
Which of the following can be a risk of using biometric data for authentication? (CO4)
Question372: END
Option_a: Biometric data can be stolen and misused
Option_b: Biometric authentication is not accurate enough
Option_c: Biometric systems are always slow

Option_d: Biometric data can be easily shared between users
correct_option: Biometric data can be stolen and misused

Question373: START
Which type of attack is prevented by challenge-response authentication systems? (CO4)
Question373: END
Option_a: Brute-force attacks
Option_b: Man-in-the-middle attacks
Option_c: Phishing attacks
Option_d: Denial-of-service attacks
correct_option: Man-in-the-middle attacks

Question374: START
Which of the following is a key feature of a password policy designed to improve security? (CO4)
Question374: END
Option_a: Allowing easy-to-remember passwords
Option_b: Enforcing periodic password changes
Option_c: Using only numeric passwords
Option_d: Enabling biometric authentication instead of passwords
correct_option: Enforcing periodic password changes

Question375: START
Which of the following is NOT a challenge of using Kerberos in an enterprise network? (CO4)
Question375: END
Option_a: Time synchronization between client and server
Option_b: Managing multiple user credentials
Option_c: Single point of failure in the KDC
Option_d: The need for a trusted third party
correct_option: Managing multiple user credentials

Question376: START
What does an X.509 certificate typically contain? (CO4)
Question376: END
Option_a: The user's encrypted password
Option_b: The user's public key and certificate authority's signature
Option_c: The user's personal identification number

Option_d: The user's biometric data
correct_option: The user's public key and certificate authority's signature

Question377: START
Which type of authentication is considered the most convenient for users? (CO4)
Question377: END
Option_a: Biometric authentication
Option_b: Password-based authentication
Option_c: Multi-factor authentication
Option_d: Challenge-response authentication
correct_option: Biometric authentication

Question378: START
In the context of challenge-response authentication, what is the role of the "challenge"? (CO4)
Question378: END
Option_a: To authenticate the user based on biometrics
Option_b: To generate a random question for the user
Option_c: To provide a time-sensitive challenge for the user to prove identity
Option_d: To store a secret password for later verification
correct_option: To provide a time-sensitive challenge for the user to prove identity

Question379: START
Which of the following is true about the X.509 certificate structure? (CO4)
Question379: END
Option_a: It contains only the private key of the user
Option_b: It is signed by a trusted certificate authority (CA)
Option_c: It stores encrypted passwords
Option_d: It is issued by the client
correct_option: It is signed by a trusted certificate authority (CA)

Question380: START
What is the main purpose of the Key Distribution Center (KDC) in Kerberos authentication? (CO4)
Question380: END
Option_a: To issue time-stamped authentication tokens
Option_b: To maintain a record of user passwords
Option_c: To issue service tickets and manage authentication processes
Option_d: To encrypt communication channels
correct_option: To issue service tickets and manage authentication processes

Question381: START
What is a key advantage of using challenge-response authentication over password-based systems? (CO4)
Question381: END
Option_a: It requires no cryptographic operations
Option_b: The password is never transmitted over the network
Option_c: It eliminates the need for encryption
Option_d: It simplifies the user experience
correct_option: The password is never transmitted over the network

Question382: START
In X.509 certificates, what is used to ensure the integrity of the certificate's content? (CO4)
Question382: END
Option_a: A digital signature by the certificate authority (CA)
Option_b: The use of a one-time password
Option_c: A shared secret between the client and the server
Option_d: The certificate owner's biometric data
correct_option: A digital signature by the certificate authority (CA)

Question383: START
Which of the following can be an advantage of using biometric authentication systems? (CO4)
Question383: END
Option_a: Biometric systems are inexpensive to implement
Option_b: Biometric data cannot be forgotten or lost
Option_c: Biometric systems do not require user consent
Option_d: Biometric systems work without any sensors
correct_option: Biometric data cannot be forgotten or lost

Question384: START
What is the main advantage of using multi-factor authentication (MFA)? (CO4)
Question384: END
Option_a: It only requires one authentication factor
Option_b: It offers a higher level of security by combining multiple authentication methods
Option_c: It allows the use of weak passwords
Option_d: It simplifies the authentication process for users
correct_option: It offers a higher level of security by combining multiple authentication methods

Question385: START
Which of the following is a key vulnerability of biometric authentication? (CO4)
Question385: END
Option_a: Biometric data can be easily changed
Option_b: Biometric data can be easily hacked or stolen
Option_c: Biometric systems cannot be automated
Option_d: Biometric systems are often not compatible with passwords
correct_option: Biometric data can be easily hacked or stolen

Question386: START
In Kerberos authentication, what is the function of the service ticket? (CO4)
Question386: END
Option_a: It stores the user's password
Option_b: It grants access to a specific service after the user is authenticated
Option_c: It encrypts communication between the client and server
Option_d: It provides a shared secret for secure authentication
correct_option: It grants access to a specific service after the user is authenticated

Question387: START
What does the X.509 standard primarily define? (CO4)
Question387: END
Option_a: Password policies for network security
Option_b: Digital certificates and public key infrastructure
Option_c: Challenge-response authentication protocols
Option_d: Biometric authentication standards
correct_option: Digital certificates and public key infrastructure

Question388: START
Which of the following is a disadvantage of using passwords for authentication? (CO4)
Question388: END
Option_a: Passwords require biometric scans
Option_b: Passwords can be easily forgotten or stolen
Option_c: Passwords are always encrypted
Option_d: Passwords cannot be used for authentication on multiple devices
correct_option: Passwords can be easily forgotten or stolen

Question389: START
Which of the following is NOT a factor in multi-factor authentication? (CO4)
Question389: END
Option_a: Something you know (e.g., password)
Option_b: Something you have (e.g., token)
Option_c: Something you are (e.g., fingerprint)
Option_d: Something you think (e.g., security question)
correct_option: Something you think (e.g., security question)

Question390: START
In the context of Kerberos, what is the purpose of the Authentication Service (AS)? (CO4)
Question390: END
Option_a: To issue the client's service tickets
Option_b: To encrypt the communication between client and server
Option_c: To verify the client's identity and provide a TGT
Option_d: To manage network traffic
correct_option: To verify the client's identity and provide a TGT

Question391: START
Which of the following is the main function of public key certificates in X.509? (CO4)
Question391: END
Option_a: To encrypt passwords securely
Option_b: To authenticate the identity of users or services
Option_c: To store biometric data
Option_d: To create random challenges for authentication
correct_option: To authenticate the identity of users or services

Question392: START
Which is a potential limitation of using biometrics for authentication? (CO4)
Question392: END
Option_a: Biometric systems are inexpensive
Option_b: Biometric data cannot be revoked once compromised
Option_c: Biometric systems are not scalable
Option_d: Biometric systems do not require any hardware
correct_option: Biometric data cannot be revoked once compromised

Question393: START
What is the purpose of encryption in Kerberos authentication? (CO4)
Question393: END
Option_a: To store user credentials in a secure manner
Option_b: To ensure that service tickets cannot be intercepted or modified

Option_c: To verify the integrity of user passwords
Option_d: To prevent unauthorized access to the KDC
correct_option: To ensure that service tickets cannot be intercepted or modified

Question394: START
What type of cryptography is used in the public key infrastructure (PKI) for X.509 certificates? (CO4)
Question394: END
Option_a: Symmetric cryptography
Option_b: Asymmetric cryptography
Option_c: Hash-based cryptography
Option_d: Quantum cryptography
correct_option: Asymmetric cryptography

Question395: START
Which of the following is true about biometric authentication? (CO4)
Question395: END
Option_a: It always requires a password to function
Option_b: It is based on unique physical or behavioral characteristics
Option_c: It is less secure than password-based authentication
Option_d: It works without any user interaction
correct_option: It is based on unique physical or behavioral characteristics

Question396: START
Which of the following is an example of something "you have" in multi-factor authentication? (CO4)
Question396: END
Option_a: A password
Option_b: A fingerprint scan
Option_c: A security token or smartcard
Option_d: A PIN code
correct_option: A security token or smartcard

Question397: START
What does the term "replay attack" refer to in the context of authentication? (CO4)
Question397: END
Option_a: An attacker intercepts and reuses valid authentication data
Option_b: An attacker attempts to guess a user’s password
Option_c: An attacker forges a digital signature
Option_d: An attacker decrypts a service ticket
correct_option: An attacker intercepts and reuses valid authentication data

Question398: START
Which of the following protocols uses a "ticket" to authenticate users? (CO4)
Question398: END
Option_a: SSL/TLS
Option_b: OAuth
Option_c: Kerberos
Option_d: LDAP
correct_option: Kerberos

Question399: START
Which of the following is a common challenge in using biometric authentication systems? (CO4)
Question399: END
Option_a: High accuracy rate
Option_b: Privacy concerns and potential misuse of data
Option_c: Ease of implementation
Option_d: Reliability of password systems
correct_option: Privacy concerns and potential misuse of data

Question400: START
Which authentication method combines something you know, something you have, and something you are? (CO4)
Question400: END
Option_a: Two-factor authentication
Option_b: Multi-factor authentication
Option_c: Challenge-response authentication
Option_d: Password-based authentication
correct_option: Multi-factor authentication

Question401: START
Which key management technique is used in PGP to handle encryption keys securely? (CO5)
Question401: END

Option_a: Centralized Key Distribution
Option_b: Web of Trust Model
Option_c: Diffie-Hellman Key Exchange
Option_d: Key Escrow System
correct_option: Web of Trust Model

Question402: START
In S/MIME, which cryptographic mechanism is primarily responsible for ensuring non-repudiation of an email message? (CO5)
Question402: END

Option_a: Symmetric Encryption
Option_b: Digital Signature
Option_c: Message Digest
Option_d: Public Key Infrastructure (PKI)
correct_option: Digital Signature

Question403: START
Which type of attack is specifically designed to exploit vulnerabilities in email security mechanisms like PGP and S/MIME? (CO5)
Question403: END

Option_a: Replay Attack
Option_b: EFAIL Attack
Option_c: Padding Oracle Attack
Option_d: Birthday Attack
correct_option: EFAIL Attack

Question404: START
Which email security protocol uses asymmetric encryption for key exchange but symmetric encryption for message confidentiality? (CO5)
Question404: END

Option_a: S/MIME
Option_b: STARTTLS
Option_c: PGP
Option_d: DKIM
correct_option: PGP

Question405: START
What is a major limitation of S/MIME when compared to PGP in terms of email security implementation? (CO5)
Question405: END

Option_a: S/MIME requires a centralized certificate authority
Option_b: S/MIME does not support message integrity
Option_c: S/MIME only encrypts subject lines, not email bodies

Option_d: S/MIME does not allow multiple encryption keys
correct_option: S/MIME requires a centralized certificate authority

Question406: START
Which of the following email security techniques is primarily used to verify the legitimacy of an email sender's domain? (CO5)
Question406: END

Option_a: SPF (Sender Policy Framework)
Option_b: TLS (Transport Layer Security)
Option_c: SSL (Secure Sockets Layer)
Option_d: AES (Advanced Encryption Standard)
correct_option: SPF (Sender Policy Framework)

Question407: START
What is the primary role of DKIM (DomainKeys Identified Mail) in email security? (CO5)
Question407: END

Option_a: Encrypting email content for confidentiality
Option_b: Authenticating the sender by verifying a digital signature
Option_c: Blocking spam emails using AI
Option_d: Automatically deleting phishing emails
correct_option: Authenticating the sender by verifying a digital signature

Question408: START
Which protocol is used by email clients to retrieve encrypted emails securely from a mail server? (CO5)
Question408: END

Option_a: IMAP over SSL/TLS
Option_b: SMTP
Option_c: DKIM
Option_d: SPF
correct_option: IMAP over SSL/TLS

Question409: START
Which attack manipulates an email’s sender address to make it appear as if it was sent from a trusted source? (CO5)
Question409: END

Option_a: Phishing
Option_b: Email Spoofing

Option_c: MITM (Man-in-the-Middle) Attack
Option_d: Zero-Day Attack
correct_option: Email Spoofing

Question410: START
What is the main security risk when using STARTTLS for securing email transmissions? (CO5)
Question410: END

Option_a: It does not support backward compatibility
Option_b: It is vulnerable to downgrade attacks like STRIPTLS
Option_c: It encrypts only metadata and not the message body
Option_d: It requires all recipients to use the same encryption key
correct_option: It is vulnerable to downgrade attacks like STRIPTLS

Question411: START
What encryption algorithm does PGP primarily use for symmetric key encryption? (CO5)
Question411: END
Option_a: AES
Option_b: RSA
Option_c: Blowfish
Option_d: DES
correct_option: AES

Question412: START
Which key is used to encrypt the message in PGP? (CO5)
Question412: END
Option_a: Sender's public key
Option_b: Receiver's private key
Option_c: Receiver's public key
Option_d: Sender's private key
correct_option: Receiver's public key

Question413: START
What is the primary purpose of a PGP digital signature? (CO5)
Question413: END
Option_a: Encrypt the message content
Option_b: Ensure message authenticity and integrity
Option_c: Compress the message for faster transmission

Option_d: Generate a one-time key for encryption
correct_option: Ensure message authenticity and integrity

Question414: START
Which cryptographic principle does PGP use to ensure both confidentiality and authentication? (CO5)
Question414: END
Option_a: Symmetric encryption only
Option_b: Asymmetric encryption only
Option_c: Hybrid encryption (both symmetric and asymmetric)
Option_d: Hashing only
correct_option: Hybrid encryption (both symmetric and asymmetric)

Question415: START
What is the function of the Web of Trust in PGP? (CO5)
Question415: END
Option_a: A centralized key verification system
Option_b: A method to verify the authenticity of public keys
Option_c: A technique for encrypting emails automatically
Option_d: A database for storing encrypted messages
correct_option: A method to verify the authenticity of public keys

Question416: START
Which hash function is commonly used in PGP for digital signatures? (CO5)
Question416: END
Option_a: SHA-256
Option_b: MD5
Option_c: SHA-1
Option_d: CRC32
correct_option: SHA-256

Question417: START
In PGP, what is the role of a session key? (CO5)
Question417: END
Option_a: It acts as a temporary key to encrypt the actual message
Option_b: It is used for signing the message
Option_c: It replaces the recipient's public key
Option_d: It is shared between the sender and receiver for authentication only
correct_option: It acts as a temporary key to encrypt the actual message

Question418: START
How does PGP protect against key compromise? (CO5)
Question418: END
Option_a: By using key revocation and expiration mechanisms
Option_b: By allowing only symmetric encryption
Option_c: By encrypting the private key with a random key
Option_d: By ensuring keys are never shared publicly
correct_option: By using key revocation and expiration mechanisms

Question419: START
What does PGP use to ensure a recipient can decrypt a message securely? (CO5)
Question419: END
Option_a: The sender's private key
Option_b: A pre-shared symmetric key
Option_c: The recipient's public key and a session key
Option_d: A one-time pad encryption method
correct_option: The recipient's public key and a session key

Question420: START
What is one limitation of PGP in large-scale communication networks? (CO5)
Question420: END
Option_a: PGP keys must be stored on physical devices
Option_b: The Web of Trust model can be difficult to manage
Option_c: PGP does not support end-to-end encryption
Option_d: PGP only works on UNIX-based systems
correct_option: The Web of Trust model can be difficult to manage

Question421: START
What is the primary purpose of S/MIME in email communication? (CO5)
Question421: END
Option_a: To provide end-to-end encryption and digital signatures for emails
Option_b: To compress email attachments for faster transmission
Option_c: To filter spam emails before they reach the inbox
Option_d: To manage email storage on the server
correct_option: To provide end-to-end encryption and digital signatures for emails

Question422: START
Which encryption algorithm is commonly used by S/MIME for securing email content? (CO5)
Question422: END
Option_a: RSA
Option_b: AES
Option_c: Blowfish
Option_d: SHA-256
correct_option: AES

Question423: START
How does S/MIME ensure the authenticity of an email sender? (CO5)
Question423: END
Option_a: By using a digital signature based on the sender's private key
Option_b: By encrypting the email subject line
Option_c: By requiring the sender to enter a password before sending an email
Option_d: By validating the sender's IP address
correct_option: By using a digital signature based on the sender's private key

Question424: START
What type of cryptography does S/MIME use for encrypting emails? (CO5)
Question424: END
Option_a: Symmetric encryption only
Option_b: Asymmetric encryption only
Option_c: A combination of symmetric and asymmetric encryption
Option_d: Hash-based encryption
correct_option: A combination of symmetric and asymmetric encryption

Question425: START
Which organization defines the S/MIME standard? (CO5)
Question425: END
Option_a: IETF (Internet Engineering Task Force)
Option_b: IEEE (Institute of Electrical and Electronics Engineers)
Option_c: W3C (World Wide Web Consortium)
Option_d: ISO (International Organization for Standardization)
correct_option: IETF (Internet Engineering Task Force)

Question426: START
What is required for a user to sign and encrypt emails using S/MIME? (CO5)
Question426: END
Option_a: A digital certificate issued by a Certificate Authority (CA)
Option_b: A static password shared between sender and receiver
Option_c: A special email client that supports S/MIME only
Option_d: A dedicated email server for S/MIME encryption
correct_option: A digital certificate issued by a Certificate Authority (CA)

Question427: START
Which of the following is a limitation of S/MIME? (CO5)
Question427: END
Option_a: It does not support encryption of email attachments
Option_b: It requires a centralized Certificate Authority (CA) for key management
Option_c: It can only be used on web-based email services
Option_d: It does not support digital signatures
correct_option: It requires a centralized Certificate Authority (CA) for key management

Question428: START
What is the role of a Certificate Authority (CA) in S/MIME? (CO5)
Question428: END
Option_a: To issue and verify digital certificates for users
Option_b: To encrypt emails between sender and receiver
Option_c: To store all encrypted emails in a secure database
Option_d: To act as an intermediary in email transmission
correct_option: To issue and verify digital certificates for users

Question429: START
How does S/MIME differ from PGP in key management? (CO5)
Question429: END
Option_a: S/MIME uses a centralized Certificate Authority, while PGP relies on a Web of Trust
Option_b: S/MIME uses only symmetric encryption, while PGP uses asymmetric encryption
Option_c: S/MIME does not require any key management, whereas PGP does
Option_d: S/MIME generates new encryption keys for every email
correct_option: S/MIME uses a centralized Certificate Authority, while PGP relies on a Web of Trust

Question430: START
Which email clients commonly support S/MIME? (CO5)
Question430: END
Option_a: Microsoft Outlook, Apple Mail, and Mozilla Thunderbird
Option_b: Gmail and Yahoo Mail (without plugins)
Option_c: WhatsApp and Signal
Option_d: Facebook Messenger and Telegram
correct_option: Microsoft Outlook, Apple Mail, and Mozilla Thunderbird

Question431: START
What is the primary purpose of IP Security (IPSec)? (CO5)
Question431: END
Option_a: To provide encryption and authentication for IP packets
Option_b: To increase the speed of data transmission over the internet
Option_c: To manage domain name resolutions efficiently
Option_d: To allocate IP addresses dynamically
correct_option: To provide encryption and authentication for IP packets

Question432: START
Which two main protocols are used in IPSec? (CO5)
Question432: END
Option_a: HTTP and HTTPS
Option_b: AH (Authentication Header) and ESP (Encapsulating Security Payload)
Option_c: TCP and UDP
Option_d: ICMP and ARP
correct_option: AH (Authentication Header) and ESP (Encapsulating Security Payload)

Question433: START
Which IPSec protocol provides encryption for data confidentiality? (CO5)
Question433: END
Option_a: AH (Authentication Header)
Option_b: ESP (Encapsulating Security Payload)
Option_c: TCP (Transmission Control Protocol)
Option_d: ICMP (Internet Control Message Protocol)
correct_option: ESP (Encapsulating Security Payload)

Question434: START
What is the function of the Authentication Header (AH) in IPSec? (CO5)
Question434: END
Option_a: To provide confidentiality by encrypting IP packets
Option_b: To authenticate the sender and ensure data integrity
Option_c: To compress data for faster transmission
Option_d: To assign dynamic IP addresses
correct_option: To authenticate the sender and ensure data integrity

Question435: START
Which of the following IPSec modes encrypts only the payload and not the IP header? (CO5)
Question435: END
Option_a: Tunnel mode
Option_b: Transport mode
Option_c: Passive mode
Option_d: Gateway mode
correct_option: Transport mode

Question436: START
Which key management protocol is used in IPSec for secure key exchange? (CO5)
Question436: END
Option_a: HTTPS
Option_b: IKE (Internet Key Exchange)
Option_c: SSL/TLS
Option_d: DNSSEC
correct_option: IKE (Internet Key Exchange)

Question437: START
What is the default port used by IKE for IPSec key exchange? (CO5)
Question437: END
Option_a: 443
Option_b: 500
Option_c: 22
Option_d: 3389
correct_option: 500

Question438: START
In IPSec, what does Perfect Forward Secrecy (PFS) ensure? (CO5)

Question438: END
Option_a: That a compromised session key cannot be used to decrypt past communications
Option_b: That the same encryption key is reused for all sessions
Option_c: That IPSec tunnels remain active indefinitely
Option_d: That data is compressed before encryption
correct_option: That a compromised session key cannot be used to decrypt past communications

Question439: START
Which encryption algorithm is commonly used in IPSec for data confidentiality? (CO5)
Question439: END
Option_a: RSA
Option_b: AES
Option_c: SHA-256
Option_d: MD5
correct_option: AES

Question440: START
What is the purpose of the Security Association (SA) in IPSec? (CO5)
Question440: END
Option_a: To establish and manage secure connections between two devices
Option_b: To dynamically assign IP addresses to devices
Option_c: To filter out malicious traffic from the network
Option_d: To configure firewall rules for secure connections
correct_option: To establish and manage secure connections between two devices

Question441: START
Which component of IPSec is responsible for negotiating security parameters? (CO5)
Question441: END
Option_a: ESP
Option_b: AH
Option_c: IKE
Option_d: GRE
correct_option: IKE

Question442: START
In IPSec, which mode is typically used for VPN connections? (CO5)

Question442: END
Option_a: Transport mode
Option_b: Tunnel mode
Option_c: Gateway mode
Option_d: Hybrid mode
correct_option: Tunnel mode

Question443: START
Which of the following is NOT an advantage of using IPSec? (CO5)
Question443: END
Option_a: Provides strong encryption and authentication
Option_b: Requires no additional configuration on network devices
Option_c: Supports VPNs for secure remote access
Option_d: Ensures data integrity and protection against tampering
correct_option: Requires no additional configuration on network devices

Question444: START
How does IPSec protect against replay attacks? (CO5)
Question444: END
Option_a: By using sequence numbers and anti-replay windows
Option_b: By encrypting all IP headers
Option_c: By using only symmetric encryption
Option_d: By rejecting packets from unknown IP addresses
correct_option: By using sequence numbers and anti-replay windows

Question445: START
Which hashing algorithm is commonly used for data integrity in IPSec? (CO5)
Question445: END
Option_a: AES
Option_b: SHA-256
Option_c: RSA
Option_d: ECC
correct_option: SHA-256

Question446: START
Which type of VPN commonly uses IPSec for secure communication? (CO5)
Question446: END
Option_a: SSL VPN
Option_b: Site-to-Site VPN

Option_c: PPTP VPN
Option_d: L2TP VPN without encryption
correct_option: Site-to-Site VPN

Question447: START
What does ESP in IPSec provide that AH does not? (CO5)
Question447: END
Option_a: Integrity and authentication
Option_b: Encryption for confidentiality
Option_c: Secure DNS resolution
Option_d: Dynamic routing
correct_option: Encryption for confidentiality

Question448: START
Which transport protocol does IPSec commonly use? (CO5)
Question448: END
Option_a: UDP
Option_b: TCP
Option_c: ICMP
Option_d: FTP
correct_option: UDP

Question449: START
What is the main difference between Tunnel Mode and Transport Mode in IPSec? (CO5)
Question449: END
Option_a: Tunnel mode encrypts the entire IP packet, while Transport mode encrypts only the payload
Option_b: Transport mode encrypts the entire IP packet, while Tunnel mode encrypts only the payload
Option_c: Tunnel mode does not provide encryption
Option_d: Transport mode is only used for wireless networks
correct_option: Tunnel mode encrypts the entire IP packet, while Transport mode encrypts only the payload

Question450: START
Which of the following best describes IPSec's role in securing network traffic? (CO5)
Question450: END
Option_a: It provides encryption and authentication for IP packets to ensure secure communication

Option_b: It replaces traditional firewalls by blocking unauthorized traffic
Option_c: It only encrypts passwords transmitted over the network
Option_d: It is used solely for securing email communication
correct_option: It provides encryption and authentication for IP packets to ensure secure communication

Question451: START
What is the primary goal of web security? (CO5)
Question451: END
Option_a: To improve website loading speed
Option_b: To protect web applications from cyber threats and vulnerabilities
Option_c: To increase search engine rankings
Option_d: To ensure websites comply with HTML standards
correct_option: To protect web applications from cyber threats and vulnerabilities

Question452: START
Which type of attack involves injecting malicious SQL queries into a web application? (CO5)
Question452: END
Option_a: Cross-Site Scripting (XSS)
Option_b: SQL Injection (SQLi)
Option_c: Distributed Denial of Service (DDoS)
Option_d: Phishing
correct_option: SQL Injection (SQLi)

Question453: START
What security measure helps prevent Cross-Site Scripting (XSS) attacks? (CO5)
Question453: END
Option_a: Using strong passwords
Option_b: Escaping or sanitizing user input
Option_c: Disabling cookies
Option_d: Enabling pop-up blockers
correct_option: Escaping or sanitizing user input

Question454: START
Which web security vulnerability allows attackers to execute scripts in a victim's browser? (CO5)
Question454: END
Option_a: Cross-Site Request Forgery (CSRF)
Option_b: Clickjacking
Option_c: Cross-Site Scripting (XSS)

Option_d: Man-in-the-Middle (MITM) Attack
correct_option: Cross-Site Scripting (XSS)

Question455: START
Which protocol is recommended for encrypting web traffic? (CO5)
Question455: END
Option_a: HTTP
Option_b: HTTPS
Option_c: FTP
Option_d: Telnet
correct_option: HTTPS

Question456: START
What is the primary function of a Web Application Firewall (WAF)? (CO5)
Question456: END
Option_a: To encrypt all website data
Option_b: To block malicious traffic and prevent attacks on web applications
Option_c: To store backup copies of a website
Option_d: To optimize website speed
correct_option: To block malicious traffic and prevent attacks on web applications

Question457: START
Which of the following attacks exploits a vulnerability in session management? (CO5)
Question457: END
Option_a: Session Hijacking
Option_b: Buffer Overflow
Option_c: Denial of Service (DoS)
Option_d: Social Engineering
correct_option: Session Hijacking

Question458: START
What is Clickjacking? (CO5)
Question458: END
Option_a: A technique where an attacker tricks a user into clicking on something different from what they perceive
Option_b: A form of phishing attack that sends fake login pages
Option_c: An attack that injects JavaScript into a web page
Option_d: A method used to encrypt website traffic

correct_option: A technique where an attacker tricks a user into clicking on something different from what they perceive

Question459: START
How can websites protect against Cross-Site Request Forgery (CSRF) attacks? (CO5)
Question459: END
Option_a: By using CAPTCHA and CSRF tokens
Option_b: By enabling HTTP instead of HTTPS
Option_c: By allowing all scripts to run on the browser
Option_d: By disabling JavaScript
correct_option: By using CAPTCHA and CSRF tokens

Question460: START
Which security header helps prevent browsers from loading a website in an iframe to mitigate Clickjacking attacks? (CO5)
Question460: END
Option_a: X-Frame-Options
Option_b: Content-Security-Policy (CSP)
Option_c: Referrer-Policy
Option_d: Strict-Transport-Security (HSTS)
correct_option: X-Frame-Options

Question461: START
Who are intruders in the context of system security? (CO5)
Question461: END
Option_a: Legitimate users accessing their own data
Option_b: Unauthorized users attempting to gain access to a system
Option_c: Software developers writing secure code
Option_d: IT administrators managing firewalls
correct_option: Unauthorized users attempting to gain access to a system

Question462: START
Which of the following is an example of malicious software (malware)? (CO5)
Question462: END
Option_a: Antivirus software
Option_b: Firewall
Option_c: Trojan horse
Option_d: Secure Socket Layer (SSL)
correct_option: Trojan horse

Question463: START
What is the primary purpose of a firewall? (CO5)
Question463: END
Option_a: To detect and remove viruses from a computer
Option_b: To block unauthorized access while allowing legitimate traffic
Option_c: To scan emails for phishing attempts
Option_d: To increase the processing speed of a system
correct_option: To block unauthorized access while allowing legitimate traffic

Question464: START
Which type of malware replicates itself and spreads to other computers? (CO5)
Question464: END
Option_a: Worm
Option_b: Trojan horse
Option_c: Spyware
Option_d: Ransomware
correct_option: Worm

Question465: START
Which of the following best describes a Trojan horse? (CO5)
Question465: END
Option_a: A program that disguises itself as legitimate software but performs malicious activities
Option_b: A type of malware that encrypts files and demands ransom
Option_c: A self-replicating program that spreads without user intervention
Option_d: A tool used to remove viruses from infected systems
correct_option: A program that disguises itself as legitimate software but performs malicious activities

Question466: START
Which method can help prevent malware infections? (CO5)
Question466: END
Option_a: Avoiding software updates
Option_b: Downloading files from untrusted sources
Option_c: Using strong passwords and security patches
Option_d: Disabling firewalls and antivirus software
correct_option: Using strong passwords and security patches

Question467: START
Which of the following is NOT a type of malware? (CO5)
Question467: END
Option_a: Adware
Option_b: Spyware
Option_c: Firewall
Option_d: Ransomware
correct_option: Firewall

Question468: START
What is a key characteristic of ransomware? (CO5)
Question468: END
Option_a: It slows down internet speed
Option_b: It encrypts files and demands payment for decryption
Option_c: It monitors user activity for targeted ads
Option_d: It automatically updates security patches
correct_option: It encrypts files and demands payment for decryption

Question469: START
Which type of malware records a user's keystrokes to steal sensitive information? (CO5)
Question469: END
Option_a: Adware
Option_b: Keylogger
Option_c: Rootkit
Option_d: Worm
correct_option: Keylogger

Question470: START
What is the primary purpose of an Intrusion Detection System (IDS)? (CO5)
Question470: END
Option_a: To prevent unauthorized access to a network
Option_b: To monitor and detect suspicious activities within a system
Option_c: To scan a system for viruses and remove them
Option_d: To encrypt sensitive data for secure transmission
correct_option: To monitor and detect suspicious activities within a system

Question471: START
Which of the following is NOT a function of a firewall? (CO5)
Question471: END
Option_a: Blocking unauthorized access
Option_b: Filtering network traffic
Option_c: Detecting and removing malware
Option_d: Allowing legitimate traffic through
correct_option: Detecting and removing malware

Question472: START
Which type of virus attaches itself to executable files and spreads when the file is executed? (CO5)
Question472: END
Option_a: Boot sector virus
Option_b: Macro virus
Option_c: File infector virus
Option_d: Polymorphic virus
correct_option: File infector virus

Question473: START
What does a rootkit do? (CO5)
Question473: END
Option_a: Encrypts user files and demands ransom
Option_b: Provides hackers with remote access to a system while hiding its presence
Option_c: Displays unwanted advertisements on a system
Option_d: Monitors and records user activity for targeted marketing
correct_option: Provides hackers with remote access to a system while hiding its presence

Question474: START
Which of the following best describes phishing? (CO5)
Question474: END
Option_a: A technique where attackers trick users into providing sensitive information by posing as legitimate entities
Option_b: A form of malware that replicates itself and spreads
Option_c: A security tool used to block malicious websites
Option_d: A technique to speed up internet browsing
correct_option: A technique where attackers trick users into providing sensitive information by posing as legitimate entities

Question475: START
Which of the following security measures can help prevent phishing attacks? (CO5)
Question475: END
Option_a: Using a VPN for all online activities
Option_b: Never clicking on suspicious email links
Option_c: Avoiding the use of antivirus software
Option_d: Disabling firewalls on all devices
correct_option: Never clicking on suspicious email links

Question476: START
What is the difference between an IDS and an IPS? (CO5)
Question476: END
Option_a: IDS detects threats but does not take action, while IPS detects and prevents threats
Option_b: IDS blocks malicious traffic, while IPS only detects it
Option_c: IDS is used for malware removal, while IPS is used for authentication
Option_d: IDS is hardware-based, while IPS is software-based
correct_option: IDS detects threats but does not take action, while IPS detects and prevents threats

Question477: START
Which malware type locks a user's system and demands payment to unlock it? (CO5)
Question477: END
Option_a: Spyware
Option_b: Ransomware
Option_c: Worm
Option_d: Trojan horse
correct_option: Ransomware

Question478: START
Which type of firewall filters traffic at the network layer based on IP addresses and port numbers? (CO5)
Question478: END
Option_a: Application-layer firewall
Option_b: Packet-filtering firewall
Option_c: Stateful firewall
Option_d: Host-based firewall
correct_option: Packet-filtering firewall

Question479: START
Which of the following is a common way malware spreads? (CO5)
Question479: END
Option_a: Opening email attachments from unknown senders
Option_b: Using strong passwords
Option_c: Keeping operating systems up to date
Option_d: Using secure browsing habits
correct_option: Opening email attachments from unknown senders

Question480: START
Which firewall technology tracks the state of active connections and allows only legitimate responses? (CO5)
Question480: END
Option_a: Packet-filtering firewall
Option_b: Application-layer firewall
Option_c: Stateful firewall
Option_d: Proxy firewall
correct_option: Stateful firewall

Question481: START
Which technique is used to disguise a virus to avoid detection? (CO5)
Question481: END
Option_a: Keylogging
Option_b: Polymorphism
Option_c: Phishing
Option_d: Denial of Service (DoS)
correct_option: Polymorphism

Question482: START
Which security practice helps prevent brute-force attacks? (CO5)
Question482: END
Option_a: Using CAPTCHA and account lockout policies
Option_b: Keeping firewall settings disabled
Option_c: Running unknown executable files
Option_d: Downloading software from untrusted sources
correct_option: Using CAPTCHA and account lockout policies

Question483: START
What does spyware do? (CO5)
Question483: END
Option_a: Encrypts files and demands ransom

Option_b: Monitors user activities and sends data to third parties
Option_c: Creates fake security alerts to scare users
Option_d: Blocks internet access completely
correct_option: Monitors user activities and sends data to third parties

Question484: START
Which type of attack overloads a system with excessive traffic to disrupt service? (CO5)
Question484: END
Option_a: Phishing
Option_b: Denial of Service (DoS)
Option_c: Spoofing
Option_d: Social Engineering
correct_option: Denial of Service (DoS)

Question485: START
What does a firewall use to determine which traffic to allow or block? (CO5)
Question485: END
Option_a: A predefined set of security rules
Option_b: The number of active users on the network
Option_c: The current system performance level
Option_d: The geographic location of users
correct_option: A predefined set of security rules

Question486: START
Which of the following is an example of a hardware firewall? (CO5)
Question486: END
Option_a: Windows Defender Firewall
Option_b: A dedicated network security appliance
Option_c: An antivirus program
Option_d: A browser extension
correct_option: A dedicated network security appliance

Question487: START
What is the function of a proxy firewall? (CO5)
Question487: END
Option_a: It acts as an intermediary between users and the internet to filter traffic
Option_b: It encrypts files for secure storage
Option_c: It scans for viruses in downloaded files
Option_d: It speeds up internet browsing
correct_option: It acts as an intermediary between users and the internet to filter traffic

Question488: START
What is the purpose of an antivirus program? (CO5)
Question488: END
Option_a: To create strong passwords for users
Option_b: To detect and remove malicious software
Option_c: To optimize a computer's speed
Option_d: To filter spam emails
correct_option: To detect and remove malicious software

Question489: START
Which of the following is a primary method for preventing unauthorized access to a system? (CO5)
Question489: END
Option_a: Using multi-factor authentication (MFA)
Option_b: Allowing all incoming connections
Option_c: Disabling firewall settings
Option_d: Clicking on unknown email links
correct_option: Using multi-factor authentication (MFA)

Question490: START
Which type of virus infects the master boot record (MBR) of a system? (CO5)
Question490: END
Option_a: Polymorphic virus
Option_b: Boot sector virus
Option_c: Macro virus
Option_d: File infector virus
correct_option: Boot sector virus

Question491: START
What is the primary purpose of two-factor authentication (2FA)? (CO5)
Question491: END
Option_a: To reduce the need for strong passwords
Option_b: To provide an additional layer of security by requiring a second form of verification
Option_c: To encrypt all user data automatically
Option_d: To speed up the login process

correct_option: To provide an additional layer of security by requiring a second form of verification

Question492: START
Which of the following is an example of social engineering? (CO5)
Question492: END
Option_a: Exploiting a software vulnerability to gain access
Option_b: Tricking users into revealing passwords through deceptive messages
Option_c: Using brute-force attacks to crack a password
Option_d: Installing a keylogger on a victim's computer
correct_option: Tricking users into revealing passwords through deceptive messages

Question493: START
Which attack exploits the trust between a user and a website to perform unauthorized actions? (CO5)
Question493: END
Option_a: SQL Injection (SQLi)
Option_b: Cross-Site Request Forgery (CSRF)
Option_c: Man-in-the-Middle (MITM) Attack
Option_d: Phishing
correct_option: Cross-Site Request Forgery (CSRF)

Question494: START
What does a botnet typically consist of? (CO5)
Question494: END
Option_a: A group of networked printers
Option_b: A collection of compromised computers controlled by an attacker
Option_c: A secure cloud-based backup system
Option_d: A firewall system that filters internet traffic
correct_option: A collection of compromised computers controlled by an attacker

Question495: START
Which security measure helps prevent brute-force attacks on a login page? (CO5)
Question495: END
Option_a: Implementing account lockout policies after multiple failed attempts
Option_b: Allowing unlimited login attempts
Option_c: Using only short passwords
Option_d: Disabling password encryption
correct_option: Implementing account lockout policies after multiple failed attempts

Question496: START
What is the main function of an Intrusion Prevention System (IPS)? (CO5)
Question496: END
Option_a: To detect and block potential threats in real time
Option_b: To remove all malware from a system
Option_c: To encrypt files for secure transmission
Option_d: To allow unrestricted access to the network
correct_option: To detect and block potential threats in real time

Question497: START
Which of the following is a common indicator of a phishing email? (CO5)
Question497: END
Option_a: A request for sensitive information, such as passwords or bank details
Option_b: A personalized message from a trusted source
Option_c: A subject line related to recent account activity
Option_d: An email with no links or attachments
correct_option: A request for sensitive information, such as passwords or bank details

Question498: START
What is the role of a honeypot in cybersecurity? (CO5)
Question498: END
Option_a: To serve as bait for attackers and analyze their activities
Option_b: To store backup copies of sensitive data
Option_c: To encrypt all internet traffic
Option_d: To provide free internet access to users
correct_option: To serve as bait for attackers and analyze their activities

Question499: START
Which of the following security measures protects against eavesdropping on a network? (CO5)
Question499: END
Option_a: Using HTTPS instead of HTTP
Option_b: Disabling firewalls
Option_c: Using weak passwords
Option_d: Allowing open Wi-Fi access
correct_option: Using HTTPS instead of HTTP

Question500: START
Which of the following best describes the Zero Trust security model? (CO5)

Question500: END
Option_a: Trusting all users inside the network by default
Option_b: Assuming all network traffic, both inside and outside, is untrusted and verifying every request
Option_c: Allowing all traffic to pass through without authentication
Option_d: Only monitoring external threats while ignoring internal threats
correct_option: Assuming all network traffic, both inside and outside, is untrusted and verifying every request