U-3

1. **Services provided by Pretty Good Privacy (PGP):**
    - Encryption and decryption of emails and files
    - Digital signatures for data integrity and authentication
    - Key management, including key generation and key revocation
2. **Need and significance of X.509 authentication service:**
    - Need: To establish and verify the identity of entities (such as users or devices) in a network.
    - Significance: X.509 provides a standardized framework for digital certificates, ensuring secure communication by verifying the authenticity of entities involved.
3. **Security options PGP allows when sending an email message:**
    - Encryption of the message content
    - Digital signatures for authentication
    - Compression to reduce the size of the message
4. **Components of ISAKMP General Header:**
    - Initiator's cookie
    - Responder's cookie
    - Next payload
    - Major version
    - Minor version
    - Exchange type
    - Flags
    - Message ID
    - Length
5. **SA (Security Association) of IPSec and its purpose:**
    - Purpose: To define the attributes and parameters of a secure communication channel between two devices.
    - Components: Security parameters such as encryption algorithms, integrity algorithms, and keying information.
6. **How IPSec offers authentication and confidentiality services:**
    - Authentication: Through the use of digital signatures or authentication headers.
    - Confidentiality: Through encryption of the data payload.

7. **Comparison of MIME and S/MIME:**
    - MIME (Multipurpose Internet Mail Extensions) is a standard for extending the format of email messages.
    - S/MIME (Secure/Multipurpose Internet Mail Extensions) is an extension of MIME that adds cryptographic security services.
8. **Role of Ticket Granting Server in inter-realm operations of Kerberos:**
    - The Ticket Granting Server (TGS) issues service tickets for services in other realms, enabling cross-realm authentication.
9. **Scenario where Kerberos scheme is preferred:**
    - In environments where a centralized authentication system is needed for secure and efficient user authentication.
10. **When certificate revocation happens in X.509 authentication service:**
    - Certificate revocation occurs when a certificate needs to be invalidated before its expiration date, often due to compromise or other security reasons.
11. **Why PGP allows segmentation of a message:**
    - Segmentation allows PGP to encrypt and sign large messages in smaller chunks, improving efficiency and overcoming size limitations.
12. **Cryptographic security services provided by S/MIME:**
    - Authentication
    - Message integrity
    - Confidentiality (encryption)
13. **Comparison of signed data content type and enveloped data content type in S/MIME:**
    - Signed Data: Authenticates the origin and integrity of the message.
    - Enveloped Data: Encrypts the content for confidentiality.
14. **Simple authentication dialogue used in Kerberos:**
    - Authentication Server (AS) and Ticket Granting Server (TGS) interaction involving the exchange of tickets for user authentication.
15. **Difference between Certificate Revocation and Delta Revocation in X.509 authentication service:**
    - Certificate Revocation: Invalidates the entire certificate.
    - Delta Revocation: Invalidates only the changes or updates made since the last full certificate revocation.
16. **Comparison of certification of X.509 and PGP:**
    - X.509 uses a hierarchical certificate authority (CA) structure.

- PGP uses a web of trust model, allowing users to sign each other's keys.

U-4

1. **Define worm:**
    - A worm is a self-replicating malware that spreads independently across computer networks. Unlike viruses, worms don't need to attach themselves to host programs and can propagate through various means, often exploiting vulnerabilities in network services.
2. **Three parts of a computer virus:**
    - **Infection Mechanism:** How the virus spreads and infects files or systems.
    - **Triggering Mechanism:** The event or condition that activates the virus.
    - **Payload:** Malicious actions executed by the virus, such as data corruption or system disruption.
3. **Attacks on packet filters:**
    - **IP Spoofing:** Attackers forge the source address of packets to deceive the packet filter.
    - **Tiny Fragment Attacks:** Sending tiny fragments to evade detection by packet filters.
    - **Session Hijacking:** Taking over an existing session to gain unauthorized access.
4. **Different classes of intruders:**
    - **Masquerader or Impersonator:** Pretends to be an authorized user.
    - **Misfeasor:** Authorized user performing unauthorized activities.
    - **Clandestine User:** Unauthorized user trying to gain access.
5. **Define DDoS attack:**
    - DDoS (Distributed Denial of Service) is an attack where multiple compromised computers are used to flood a target system with traffic, overwhelming its resources and causing a denial of service for legitimate users.
6. **Difference between polymorphic and metamorphic viruses; Classification of viruses:**
    - **Polymorphic Virus:** Changes its code to avoid detection while maintaining the same basic functions.
    - **Metamorphic Virus:** Completely rewrites its code to create a new instance with different algorithms.
    - **Classification of Viruses:** Viruses are often classified based on their behavior and the types of systems they infect, such as boot sector viruses, file infector viruses, and macro viruses.
7. **Rule-based anomaly detection:**

- Rule-based anomaly detection involves defining rules that specify normal behavior. Deviations from these rules are flagged as anomalies, indicating potential security threats.

8. **Methods to protect password files from intruders:**
    - **Hashing and Salting:** Storing hashed passwords with unique salts to enhance security.
    - **Encryption:** Encrypting password files to protect sensitive information.
    - **Regular Auditing:** Monitoring and analyzing password file changes for suspicious activities.
9. **Need for honeypots:**
    - Honeypots are used to attract and detect attackers. They help security professionals study attack methods, understand vulnerabilities, and improve overall system security.
10. **Limitations of firewalls:**
    - **Limited Application Layer Filtering:** Firewalls may struggle with filtering at the application layer.
    - **Inability to Detect Malicious Content:** Encrypted traffic can bypass firewall inspection.
    - **False Positives and Negatives:** Firewalls may generate false alarms or miss actual threats.
11. **Role of bastion host:**
    - A bastion host is a highly secured computer system located on the perimeter of a network. It provides a controlled entry point for external users and usually runs only essential services to minimize the attack surface.
12. **Intruder Behavior Patterns with examples:**
    - **Scanning:** An intruder systematically scans the network for vulnerabilities.
    - **Password Attacks:** Repeated login attempts to guess passwords.
    - **Denial of Service:** Overloading a system or network to disrupt services.
13. **Difference between native audit and detection-specific audit records in intrusion detection:**
    - **Native Audit:** Records generated by standard system logging mechanisms.
    - **Detection-Specific Audit Records:** Generated specifically for intrusion detection purposes, capturing information relevant to potential security incidents.
14. **Methods a worm uses to propagate:**
    - **Email Attachment:** Sending infected files via email.
    - **Network Shares:** Exploiting vulnerabilities to spread through shared resources.

- **Drive-By Downloads:** Exploiting browser or software vulnerabilities to infect systems.

15. **Difference between a packet-filtering router and a stateful inspection firewall:**
    - **Packet-Filtering Router:** Filters packets based on predefined rules, examining source and destination addresses and ports.
    - **Stateful Inspection Firewall:** Examines the state of active connections, making decisions based on the context of the traffic and the state of the connection.

U-5

1. **Processing logic of SHA-512:**
    - SHA-512 (Secure Hash Algorithm 512-bit) processes data in 1024-bit blocks and has a message digest of 512 bits. The processing logic involves several steps, including message padding, breaking the message into blocks, and applying a series of mathematical functions (such as bitwise operations, modular addition, and logical functions) in multiple rounds to generate the final hash value.
2. **Implementation steps of MD5:**
    - **Step 1: Initialization:** Initialize four 32-bit variables (A, B, C, D) with specific constant values.
    - **Step 2: Message Padding:** Append padding bits to the message to make its length congruent to 448 modulo 512.
    - **Step 3: Append Length:** Append the original message length in bits as a 64-bit representation.
    - **Step 4: Process Blocks:** Divide the padded message into 512-bit blocks and process each block using a series of logical functions.
3. **Advantages of MD5:**
    - **Fast Computation:** MD5 is relatively fast and computationally efficient.
    - **Widely Used:** It has been widely used for checksums and data integrity verification.
    - **Fixed Output Size:** Always produces a 128-bit hash, making it suitable for various applications.
4. **Initialization procedure of MD5 word buffer:**
    - The MD5 algorithm initializes a 128-bit buffer to specific constant values. These values are the 32-bit representation of the square root of prime numbers.
5. **Features of SHA-512:**
    - **Block Size:** Processes data in 1024-bit blocks.
    - **Word Size:** Operates on 64-bit words.
    - **Number of Rounds:** 80 rounds of processing.
    - **Message Digest Size:** Produces a 512-bit hash value.

- **Complexity:** More complex than SHA-256.

6. **Comparison of different versions of SHA:**
    - SHA-1: 160-bit hash value, considered deprecated due to vulnerabilities.
    - SHA-224: Variant of SHA-256 with a 224-bit hash value.
    - SHA-256: 256-bit hash value.
    - SHA-384: Variant of SHA-512 with a 384-bit hash value.
    - SHA-512: 512-bit hash value.
7. **Compression function of MD5:**
    - The MD5 compression function involves bitwise operations (AND, OR, XOR), modular addition, and logical functions (F, G, H, I) applied to the input data in multiple rounds.
8. **Round function of SHA-512:**
    - The SHA-512 round function involves a series of bitwise operations, modular additions, and logical functions applied to the input data in multiple rounds.
9. **Difference between SHA and MD5:**
    - **Output Size:** SHA has different versions with varying output sizes (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512), while MD5 always produces a 128-bit hash.
    - **Security:** MD5 is considered cryptographically broken and unsuitable for further use due to vulnerabilities, while certain versions of SHA are still considered secure.
10. **History of MD5:**
    - MD5 was designed by Ronald Rivest in 1991 as an improvement over earlier hash functions. It gained popularity for its speed and simplicity. However, vulnerabilities were discovered, leading to its deprecation for cryptographic security purposes.
11. **Process of hashing in MD5:**
    - **Initialization:** Set the initial values of the word buffer.
    - **Message Padding:** Append padding bits and the original message length.
    - **Processing Blocks:** Divide the padded message into blocks and process each block using the MD5 compression function.
    - **Output:** The final output is a 128-bit hash value.