Q1] What is Encapsulating Security Payload? / Explain the working of Encapsulating Security Payload.

- **ESP** is a protocol within the **IPsec suite** (Internet Protocol Security).
- It provides **confidentiality**, **integrity**, and **authentication** for data transmitted between devices in a network by **encrypting it.**
- ESP encrypts the **payload** of IP packets, ensuring secure transmission of information.
- **Operating Layer**: ESP operates at the **Network layer** and resides within the IP Header.
- **Modes**:
    - **Transport mode**: In this mode, the IP Header is not protected via encryption or authentication. It offers less processing overhead but leaves the header vulnerable.
    - **Tunnel mode**: Mandatory in gateways, tunnel mode creates a new outer IP Header followed by ESP. It provides stronger protection.
- Both communicating systems use a **shared key** for encryption and decryption.
- If you choose both encryption and authentication, ESP first authenticates the packet before decryption.

Q2] Differentiate between / Explain the modes of Encapsulating Security Payload.

1) **Transport Mode:**
    - **Header Position**: The original IP header remains unchanged.
    - **Encryption Scope**: Only the payload (data portion) of the IP packet is encrypted and protected.
    - **ESP Header Location**: The ESP header is placed between the original IP header and the payload.
    - **Use Case**: Typically used for end-to-end communication between hosts or devices.
    - **Example**: Securing traffic between two computers within the same network.
2) **Tunnel Mode:**
    - **Header Position**: The entire original IP packet is encapsulated.
    - **Encryption Scope**: The entire original IP packet, including its header, is encrypted.
    - **New IP Header**: A new IP header is added to the encapsulated packet.
    - **Use Case**: Commonly used between network gateways (e.g., routers, firewalls) or between an end-station and a gateway.
    - **Example**: Establishing a VPN connection between two separate networks over the internet.

Q3] List and explain the components of ESP.

- **Security Parameters Index (32 bits):** Identifies a security association (SA). This is mandatory for managing secure connections. The value of zero is reserved and not transmitted.
- **Sequence Number (32 bits):** A counter that increments with each packet, starting at 1. It helps prevent replay attacks by ensuring packets are received in order.
- **Payload Data (variable size):** The actual data being protected, which could be a transport-level segment or an entire IP packet. It's encrypted for security.
- **Padding (0-255 bytes):** Extra bytes added to align the payload data to the encryption block size, ensuring it fits correctly.
- **Pad Length (8 bits):** Indicates how many padding bytes are present.
- **Next Header (8 bits):** Specifies the type of data in the payload, identifying the first header of the payload content.

- **Authentication Data (variable size):** Optional field that contains integrity information, used if the security association requires it.

Q4] What are the features of IP Sec?

- **Authentication**: Verifies that the data comes from the correct source.Uses digital signatures or shared secrets (pre-shared keys) to confirm the identity of the sender.
- **Confidentiality**: Ensures that data remains private and unreadable to unauthorized parties.(by encrypting)
- **Integrity**: Ensures that data has not been altered during transmission.
- **Key Management**: Manages the cryptographic keys used for encryption and authentication.Includes key exchange (securely sharing keys between parties) and key revocation (replacing old keys with new ones).Internet Key Exchange (IKE) is a protocol that facilitates this process.
- **Tunneling**: IPSec supports tunneling, allowing IP packets to be encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or L2TP (Layer 2 Tunneling Protocol).
- **Flexibility**: IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections
- **Interoperability**: IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments.

Q5] What is IP Security and its uses?

- Internet Protocol (IP) is the common standard that controls how data is transmitted across the internet. It Refers to a collection of communication rules or protocols used to establish secure network connections.
- IP Sec (Internet Protocol Security) is a standard suite of protocols between two communication points across the IP network
- It is created by Internet Engineering Task Force (IETF) that provide data authentication, integrity, and confidentiality
- For **example**, it encrypts data at the source and then decrypts it at the destination. It also verifies the source of the data.
- Uses of IPsec:
    - **Encryption:** To encrypt application layer data, IPsec can scramble the content so that only the person you're sending it to can read it. This keeps your messages private.
    - **Security:** IPsec ensures that the instructions they send to each other about where to deliver data are safe from eavesdroppers and tampering
    - **Authentication:** provides authentication without encryption.IPsec can add a special tag to the data to confirm it's from a trusted source, even if the data itself isn't scrambled.
    - **Protection:** protects the network data by setting up circuits using IPsec tunneling in which all data being sent between the two endpoints is encrypted and also this is how a VPN (Virtual Private Network) works

Q6] What are the two main protocols used in the IP security architecture to secure data flow?

The IP security architecture uses two main protocols to secure data flow:

- **ESP (Encapsulation Security Payload)** -

    - provides confidentiality services by encrypting the data.
    - ESP consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication.
    - It can operate in either transport mode, where only the payload is encrypted, or tunnel mode, where the entire IP packet is encrypted.
- **AH (Authentication Header)** -
    - provides authentication and integrity services by verifying the authenticity and integrity of the data.
    - AH provides connectionless integrity, data origin authentication, and an optional anti-replay service.
    - It can also operate in transport or tunnel mode.

Q7]What are the key components of the IP security architecture besides the protocols?

- **Encryption Algorithms:**
    - Defines the cryptographic methods used for encrypting data in the ESP protocol Examples include AES, Blowfish, Triple DES, ChaCha, DES-CBC, etc.
    - Encryption algorithms provide confidentiality services by scrambling the data so it is unreadable to unauthorized parties
- **Authentication Algorithms:**
    - Defines the cryptographic methods used for authenticating and verifying the integrity of data in both ESP and AH protocols Examples include HMAC-SHA, HMAC-MD5, etc.
    - Authentication algorithms provide data origin authentication and ensure the data has not been tampered with in transit

- **Domain of Interpretation (DOI):**
    - Provides documentation support and defines the values needed for the AH and ESP protocols to interoperate Serves as an identifier that allows the communicating parties to understand the security parameters being used

- **Key Management Procedures:**
    - Describes how encryption and authentication keys are securely exchanged between the communicating parties Enables the establishment of Security Associations (SAs) which define the security parameters for the IPsec session Protocols like Internet Key Exchange (IKE) handle the automated negotiation and management of keys
    -

Q8] What is Authentication Header?

The Authentication Header (AH) is an Internet Protocol security (IPsec) component that provides the following key functions:

- Provides connectionless integrity and data origin authentication for IP datagrams
- Offers protection against replay attacks by using a sequence number field
- Ensures that the data has not been modified during transit

Q9] What is replay attack and how can we stay protected from it?

- Replay attacks occur when an attacker intercepts and retransmits valid network communications to gain unauthorized access or disrupt a system.
- To protect against replay attacks:
    - Practice robust session management
    - Employ anti-replay mechanisms
    - Leverage message integrity checks
    - Implement unique identifiers
    - Use encryption to secure data in transit

Q10] What is the difference between Authentication Header and Encapsulation Security payload?

- **Functionality:**
    - AH provides data integrity, data origin authentication, and optional replay protection, but does not provide encryption or confidentiality.
    - ESP provides data confidentiality through encryption, as well as optional data origin authentication, data integrity, and replay protection
- **Packet Coverage:**
    - AH authenticates the entire IP packet, including the outer IP header, except for certain mutable fields.
    - ESP authenticates only the IP datagram portion of the packet, not the outer IP header.
- **Modes of Operation:**
    - Both AH and ESP support transport mode and tunnel mode.
    - In transport mode, AH protects the original IP packet, while ESP encrypts the payload and adds a new IP header.
    - In tunnel mode, AH protects the entire original IP packet, while ESP encapsulates the original packet within a new IP header.
- **Usage Guidance:**
    - AH is rarely used alone, as ESP with null encryption can provide the same authentication and integrity protection.
    - ESP is generally recommended for most VPN tunneling use cases, as it provides both encryption and authentication.