Experiment No. 10: IPsec (ESP and AH) Protocol

AIM AND OBJECTIVE

Aim: To study the IPsec (ESP and AH) protocol by capturing the packets using the Wireshark tool.

Objective (Learning Objective): To understand the IPsec framework and the functions of its two main protocols, AH and ESP.

ORAL/VIVA IMPORTANT TOPICS

- IPsec (IP Security) definition and its purpose (authentication, integrity, confidentiality).
- The two main IPsec protocols: Authentication Header (AH) and Encapsulating Security Protocol (ESP).
- Protocol numbers for AH (51) and ESP (50).
- Key Management Protocol: ISAKMP and its port (UDP 500).
- IPsec Modes: Transport Mode vs. Tunnel Mode (especially the part that is encrypted in each).

IMPORTANT QUESTIONS AND ANSWERS (Q&A)

Q1: What is IPsec and what services does it provide? A: IPsec is a suite of protocols that secures IP communication by providing data authentication, integrity, and confidentiality between two communication points across an IP network.

Q2: What is the main difference between AH and ESP? A:

- AH (Authentication Header): Provides authentication and integrity assurance (ensuring data is not modified and the sender is genuine). It does not provide encryption (confidentiality).
- ESP (Encapsulating Security Protocol): Primarily provides confidentiality (encryption) of the data payload. It can also optionally provide authentication and integrity.

Q3: Which ports/protocol numbers are associated with IPsec? A: IPsec uses:

- Protocol 51 for AH traffic.
- Protocol 50 for ESP traffic.
- UDP Port 500 for ISAKMP (Internet Security Association and Key Management Protocol), which handles secure key exchange.

Q4: What are the two modes of IPsec? A:

1. Transport Mode: The IPsec header (AH or ESP) is inserted *after* the original IP header. Typically used for host-to-host communication. In ESP Transport Mode, only the data payload is encrypted.

2. Tunnel Mode: A *new* IP header is prepended to the original IP packet. This mode is used for network-to-network or host-to-network communication (e.g., VPNs). In ESP Tunnel Mode, the entire original IP packet (including the original IP header) is encrypted.