Department of Information Technology

Academic Year: 2022-23 **Semester: V**
Class / Branch: TE IT
Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

EXPERIMENT NO. 9

Aim: To study and implement IPSEC in Linux .

Theory :

IPsec

Internet Protocol Security (IPSec) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. IPSec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.
Internet protocol security (IPsec) is a set of protocols that provides security for Internet Protocol. It can use cryptography to provide security. IPsec can be used for the setting up of virtual private networks (VPNs) in a secure manner.

IPsec involves two security services:

Authentication Header (AH): This authenticates the sender and it discovers any changes in data during transmission.
Encapsulating Security Payload (ESP): This not only performs authentication for the sender but also encrypts the data being sent.

There are two modes of Ipsec:

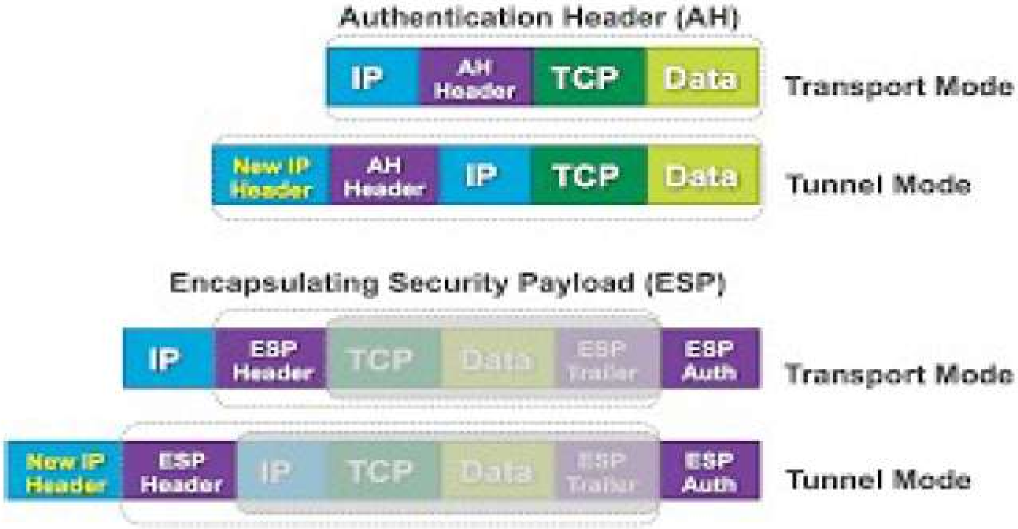
Tunnel Mode: This will take the whole IP packet to form secure communication between two places, or gateways.
Transport Mode: This only encapsulates the IP payload (not the entire IP packet as in tunnel mode) to ensure a secure channel of communication.

Pre-Shared-Key (PSK): A pre-shared-key is an easy to deploy option but it requires strong secrets to be secure. If the PSK is known to many users (which is often the case with IKEv1 XAuth with PSK) any user who knows the secret could impersonate the gateway. Therefore this method is not recommended for large scale deployments.

The IPsec standards define two distinct modes of IPsec operation, transport mode and tunnel mode. The modes do not affect the encoding of packets. The packets are protected by AH, ESP, or both in each mode. The modes differ in policy application when the inner packet is an IP packet, as follows:

In transport mode, the outer header determines the IPsec policy that protects the inner IP packet.

In tunnel mode, the inner IP packet determines the IPsec policy that protects its contents.



Conclusion:

IPsec incorporates all of the most commonly employed security services, including authentication, integrity, confidentiality, encryption and non repudiation. However, the major drawbacks to IPsec are its complexity and the confusing nature of its associated documentation. In spite of these various drawbacks, IPsec is believed by many to be one of the best security systems available.