Shubham Chemate
Roll No. 31118

PICT, PUNE

Assignment 13.

Title: Study of IPsec.

Problem Statement: To study IPsec (ESP & AH) protocol by capturing the packet using wireshark tool.

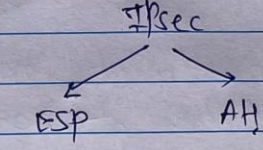
Prerequisite: Knowledge of protocols & wireshark.

Learning Objective:
Learn about use & importance of IPsec.

Theory:

IPsec:

1) It stands for IP security.
2) It is an Internet Engineering Task force standard suit of protocols between 2 communication points across the IP network that provide data authentication, integrity, confidentiality.
3) It also defines the encrypted, decrypted & authenticated packets.
4) The IPsec protocols are needed for secure key exchange & key management.
5) UDP port 500 should be opened as should IP protocols 50 & 51.



PICT, PUNE

Encapsulating Security Protocol:

a) It gives protection to upper layer new protocols, with a signed area where a protected data packet has been signed for integrity & encrypted area which indicates the information that protected with confidentiality.

b) Unless a data packet is being tunneled, ESP protects only the IP data payload and not the IP header.

Authentication Header:

a) Authentication header is a new protocol & part of the internet protocol Security (IPsec) protocol suit, which authenticates the origin of IP packet & guarantees the integrity of data.

b) The AH confirms the originating source of a packet & ensures that it's contents have been chaged since transmission.

Conclusion:

In this study assignment, I have studied about IPsec & ESP, AH protocols.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.12.1	192.168.12.2	ISAKMP	210	Identity Protection (Main Mode)
2	0.042929	192.168.12.2	192.168.12.1	ISAKMP	150	Identity Protection (Main Mode)
3	0.085175	192.168.12.1	192.168.12.2	ISAKMP	326	Identity Protection (Main Mode)
4	0.138292	192.168.12.2	192.168.12.1	ISAKMP	346	Identity Protection (Main Mode)
5	0.191233	192.168.12.1	192.168.12.2	ISAKMP	150	Identity Protection (Main Mode)
6	0.196275	192.168.12.2	192.168.12.1	ISAKMP	118	Identity Protection (Main Mode)
7	0.202103	192.168.12.1	192.168.12.2	ISAKMP	262	Quick Mode
8	0.208529	192.168.12.2	192.168.12.1	ISAKMP	262	Quick Mode
9	0.213251	192.168.12.1	192.168.12.2	ISAKMP	102	Quick Mode

- Frame 1: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits)
- Ethernet II, Src: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0), Dst: Cisco_ed:7a:f0 (00:17:5a:ed:7a:f0)
- Internet Protocol Version 4, Src: 192.168.12.1, Dst: 192.168.12.2
- User Datagram Protocol, Src Port: 500, Dst Port: 500
- Internet Security Association and Key Management Protocol

```
0000  00 17 5a ed 7a f0 00 1d  a1 8b 36 d0 08 00 45 c0   ..Z.z.....6...E.
0010  00 c4 02 89 00 00 ff 11  1e 8c c0 a8 0c 01 c0 a8   ................
0020  0c 02 01 f4 01 f4 00 b0  29 24 e4 7a 59 1f d0 57   ........)$.zY..W
0030  58 7f 00 00 00 00 00 00  00 00 01 10 02 00 00 00   X...............
0040  00 00 00 00 00 a8 0d 00  00 3c 00 00 00 01 00 00   .........<......
0050  00 01 00 00 00 30 01 01  00 01 00 00 00 28 01 01   .....0.......(..
0060  00 00 80 01 00 07 80 0e  00 80 80 02 00 02 80 04   ................
0070  00 02 80 03 00 01 80 0b  00 01 00 0c 00 04 00 01   ................
0080  51 80 0d 00 00 14 4a 13  1c 81 07 03 58 45 5c 57   Q.....J.....XE\W
0090  28 f2 0e 95 45 2f 0d 00  00 14 43 9b 59 f8 ba 67   (...E/....C.Y..g
00a0  6c 4c 77 37 ae 22 ea b8  f5 82 0d 00 00 14 7d 94   lLw7."........}.
00b0  19 a6 53 10 ca 6f 2c 17  9d 92 15 52 9d 56 00 00   ..S..o,....R.V..
00c0  00 14 90 cb 80 91 3e bb  69 6e 08 63 81 b5 ec 42   ......>.in.c...B
00d0  7b 1f                                             {.
```