

Lab Assignment 8

AP21110010302

Krish Srivastava

CSE – E

Network Security – CSE 315L

nat-t-ipsec-vpn.pcapng

The image shows a Wireshark packet capture of a NAT-T IPsec VPN. The packet list on the left shows several packets, with packet 17 selected. The packet details pane on the right shows the structure of the selected packet, which is an Internet Protocol Version 4 packet. The packet is an ICMP Echo (ping) request from 192.168.3.2 to 192.168.3.2. The packet is encapsulated in an ESP (Encapsulating Security Payload) packet, which is further encapsulated in an IP packet. The packet is marked as 'Unverified' for the checksum and status fields.

ikev2_cbc_hmac.pcapng

The image shows a Wireshark packet capture of an IKEv2 CBC HMAC. The packet list on the left shows several packets, with packet 1 selected. The packet details pane on the right shows the structure of the selected packet, which is an Internet Protocol Version 4 packet. The packet is an ICMP Echo (ping) request from 192.168.3.2 to 192.168.3.2. The packet is encapsulated in an ESP (Encapsulating Security Payload) packet, which is further encapsulated in an IP packet. The packet is marked as 'Unverified' for the checksum and status fields.

esp4-ctr-hmac.pcapng

The image shows a Wireshark capture of a network packet. The packet list on the left shows a single packet (No. 1) at time 0.000000, source 201.25.64.2, destination 201.25.64.1, protocol ESP, length 158. The packet details pane shows the following structure:

- Ethernet II, Src: Fa0/20:19:05:85:49 (fa:19:05:85:49), Dst: ee:48:19:05:85:49 (ee:48:19:05:85:49)
- Internet Protocol Version 4, Src: 201.25.64.2, Dst: 201.25.64.1
- ICMP Echo (ping) request
- Checksum: 0x70f5 (correct)
- Identifier (ID): 1033 (0x03ff)
- Sequence Number (Seq): 1033 (0x03ff)
- Source Address: 201.25.64.2
- Destination Address: 201.25.64.1
- Encapsulating Security Payload (ESP)

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, ICMP header, and the ESP payload.

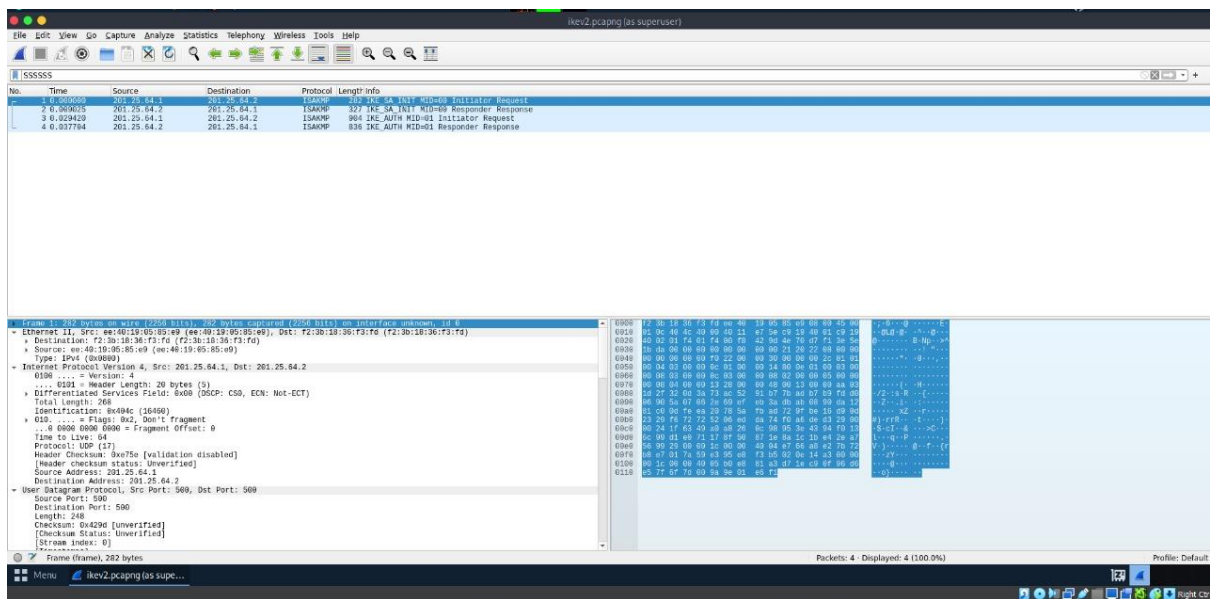
esp-transport-esn.pcapng

The image shows a Wireshark capture of a network packet. The packet list on the left shows a single packet (No. 2) at time 0.000162, source 201.25.64.1, destination 201.25.64.2, protocol ESP, length 134. The packet details pane shows the following structure:

- Ethernet II, Src: Fa0/20:19:05:85:49 (fa:19:05:85:49), Dst: ee:48:19:05:85:49 (ee:48:19:05:85:49)
- Internet Protocol Version 4, Src: 201.25.64.1, Dst: 201.25.64.2
- Encapsulating Security Payload (ESP)

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and the ESP payload.

ikev2.pcapng



ipv6_tcp.pcapng

