Group C- Assignment No. 17

Title:

To study the IPsec (ESP and AH) protocol by capturing the packets using Wiresharktool.

Outcomes:

Retrieve IPsec (ESP and AH) protocol by capturing the packets using Wireshark tool.

.

Theory:

The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols
between 2 communica ts. The
and confiden
protocols needed for secure key exchange and key management are defined in it.

What Ports Does IPSEC Operate On?

UDP port 500 should be opened as should IP protocols 50 and 51. UDP port 500 should be opened
to allow for ISAKMP to be forwarded through the firewall while protocols 50 and 51 allow ESP and
AH traffic to be forwarded resp

What is ISAKMP?

ISAKMP stands for Internet Security
Associa
components of an IPSEC VPN that must be in place in order for it to func
the public traffic that is being forwarded between the client and VPN server or VPN server to VPN
server.

What are ESP and AH?

No, ESP is not Extra-Sensory
Percep
stands for Authen

Encapsula

ESP gives prot area indica wherea protected
data packet has been signed for integrity, and an Encrypted area
which
indicates the informa
tunneled, ESP protects only the IP data payload (hence the name), and not the IP
header.

ESP may be used to ensure confiden -replay service (a form of p
integrity, some degree of traffic level
confiden
sequence integrity which guards against the use of commands or
creden
captured through password sniffing or similar a

Authen

Authen
protocol suite, which authen of IP packets (datagrams) and guarantees
integrity of the data. The AH confirms the origina the
contents (both the header and payload) have not been changed since transmission. If
security
associa een established, AH can
a be
dow technique.4

How Do They All Work Together?

When properly configured, an IPSEC VPN provides
mu
security mode and integrity of the data that is

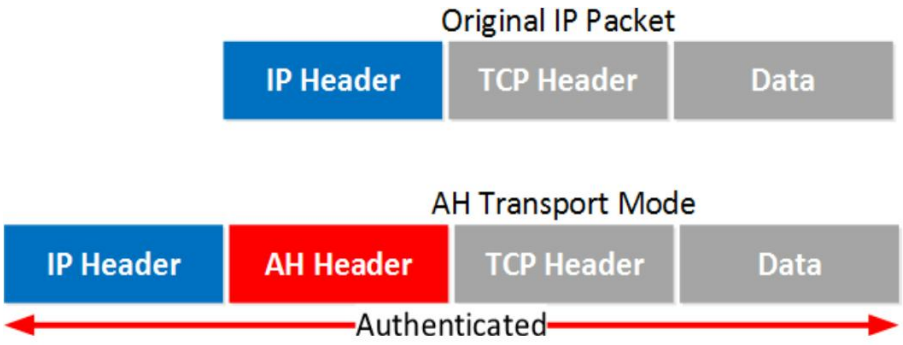
being tran
the data has not been intercepted and altered in transit and that they can rely on what they are
seeing.

IPsec Protocols

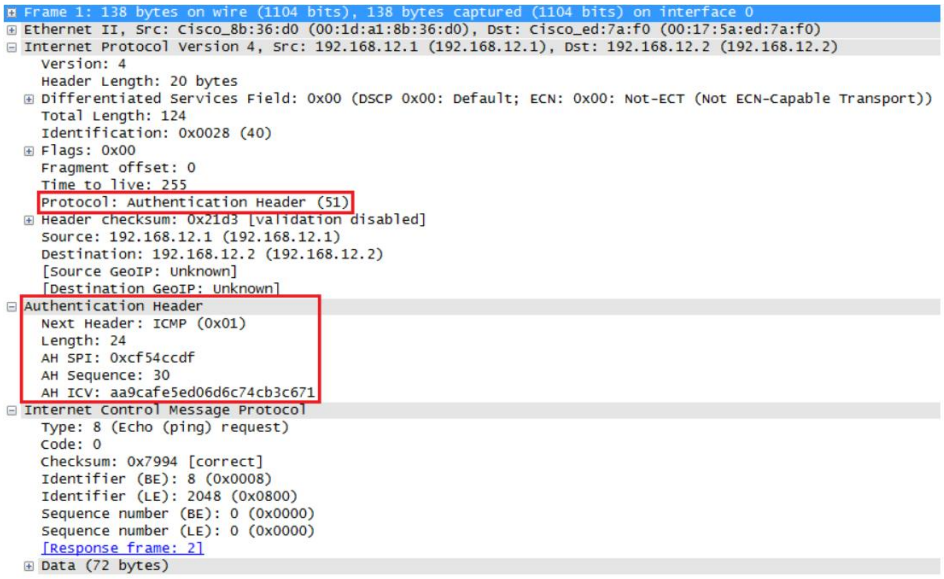
AH and/or ESP are the two protocols that we use to actually protect user data. Both of them can be
used in transport or tunnel mode, let's walk through all the possible
Authen Protocol

AH offers authen encryp
by calcula
that can be changed

in transit (TTL and header checksum). Let's start with transport mode… Transport mode is simple, it
just adds an AH header after the IP header. Her e's anexample of an IP packet that carries some
TCP traffic:



And here's what that looks like in Wireshark:



Above you can see the AH header in between the IP header and ICMP header. This is acapture I took of a ping between two routers. You can see that AH uses 5 fields:

Next Header: this iden

Length: this is the length of the AH header.

SPI (Security Parameters Index): this is an 32-bit iden packet belongs.

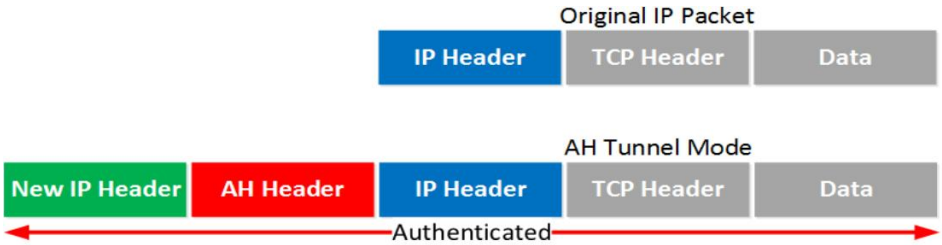
Sequence: this is the sequence number that helps against replay a

ICV (Integrity Check Value): this is the calculated hash for the en calculates a hash, when it's not the same you know something is wrong.

Let’s c

could be useful when you are using private IP addresses and you need to tunnel your traffic over

the Internet. It’s possible with AH but it doesn’t offer encryp on:



The en

```
Frame 1: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface 0
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 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
    Version: 4
    Header Length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 144
    Identification: 0x0215 (533)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: Authentication Header (51)
    Header checksum: 0x1fd2 [validation disabled]
    Source: 192.168.12.1 (192.168.12.1)
    Destination: 192.168.12.2 (192.168.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Authentication Header
    Next Header: IPIP (0x04)
    Length: 24
    AH SPI: 0x646adc80
    AH Sequence: 5
    AH ICV: 606d214066853c0390cfe577
Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
    Version: 4
    Header Length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 100
    Identification: 0x003c (60)
    Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x2209 [validation disabled]
    Source: 192.168.12.1 (192.168.12.1)
    Destination: 192.168.12.2 (192.168.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Internet Control Message Protocol
```

Above you can see the new IP header, then the AH header and finally the original IPpacket that
carries some ICMP traffic.

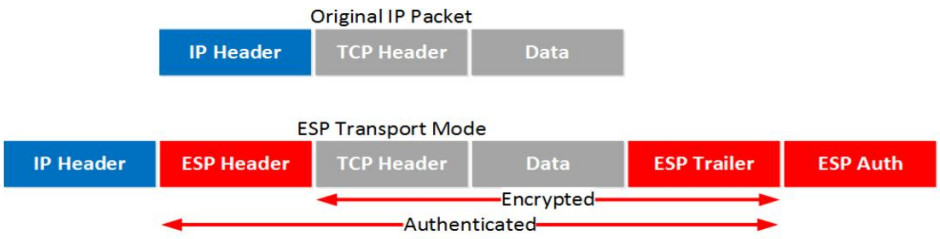
One problem with AH is that it doesn't play well with NAT / PAT. Fields in the IP header like TTL and
the checksum are excluded by AH because it knows these will change. The IP addresses and port
numbers however are included. If you change these with NAT, the ICV of AH fails.

Let's c

ESP
(Encapsula
ESP is the more popular choice of the two since it allows you to encrypt IP traffic. Wecan use it in
transport or tunnel mode, let's look at both.

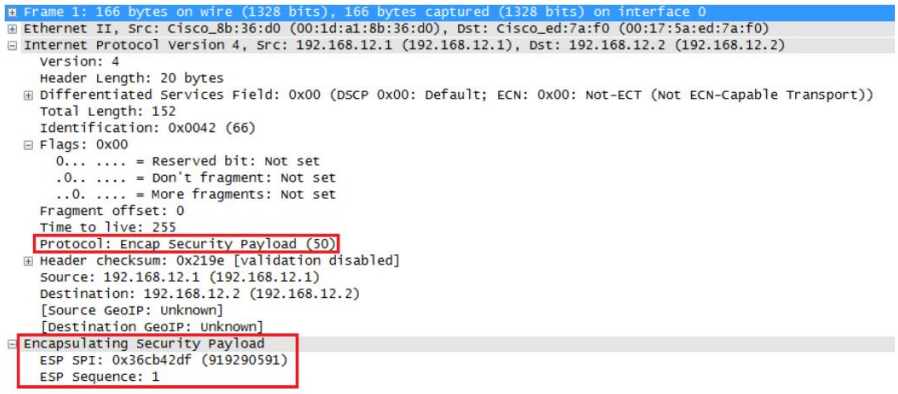
Transport Mode

When we use transport mode, we use the original IP header and insert an ESP header.Here's what
it looks like:



Above you can see that we add an ESP header and trailer. Our transport layer (TCP for example)
and payload will be encrypted. It also offers but unlike AH, it'snot for the en IP authen
packet.

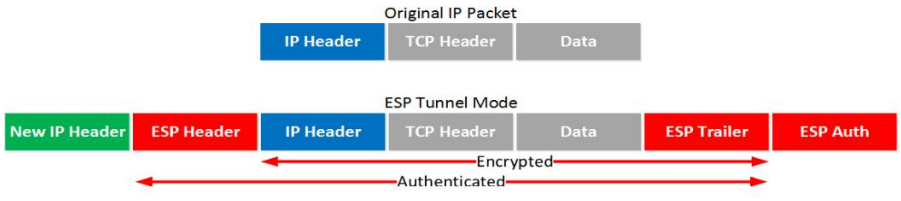
Here's what it looks like in wireshark:



Above you can see the original IP packet and that we are using ESP. The IP header is incleartext but
everything else is encrypted.

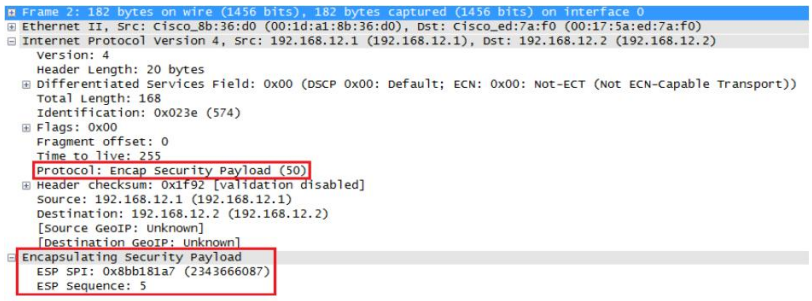
Tunnel Mode

How about ESP in tunnel mode? This is where we use a new IP header which is usefulfor site-to-
site VPNs:



It's similar to transport mode but we add a new header. The original IP header is nowalso
encrypted.

Here's what it looks like in wireshark:



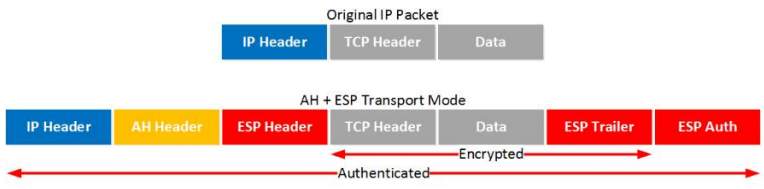
The output of the capture is above is similar to what you have seen in transport mode.The only
difference is that this is a new IP header, you don't get to see the original IPheader.

AH and ESP

This one confuses a lot of people, it's possible to use AH and ESP at the same
out!

Transport Mode

Let's start with transport mode, here's what the IP packet will look like:



With transport mode we will use the original IP header, followedby an AH and ESPheader. The
transport layer, payload and ESP trailer will be encrypted.

Because we also use AH, the IP packet is authen en

Here's what it looks likein wireshark:

Above you can see the original IP packet, the AH header and the ESP header.

Conclusion:

Hence we had studied the IPsec (ESP and AH) protocol by capturing the packets

usingWireshark tool.