Palestine
An-Najah National University
Faculty of Information Technology
Network and Information Security

دولـــــــــــة
فلســـــــــــطين
جامعة النـجـاح الـوطنـيـة
كليـة تكنولوجيا المعلومات
قسم شبكات و امن المعلومات

Experiment#5
IPSec Basic Configuration

Dyaa Al-dein Ashraf Tummazeh **11924899**

Manar Eyad Harb **11924470**

Yara Mohammad Sholi **11924207**

Supervisor:

Dr. Amjad Hawash

Abstract

In this experiment, we going to practice building a secure connection between two hosts by setting up an IPsec connection using two virtual machines.

Introduction

IPsec is a set of protocols and algorithms that are used together to protect the data that was transmitted over the internet or any public network. IPsec is a secure internet protocol because adds encryption and authentication on routing processing, by adding two headers in the IP packet: Authentication Header (AH), and Encapsulation Security Payload (ESP).And, here is two-mode where IPsec protection is applied: the transport mode and tunnel mode.

IPsec includes some protocols that are used in key exchange and key management.

Authentication Header (AH) also provides data integrity and authentication, it does not provide encryption so it does not protect data confidentiality.

Encapsulation Security Payload (ESP) provides data integrity, authentication and encryption.

Internet Key Exchange (IKE) It`s a built-in IPsec protocol that is used as the default key management protocol under the IPsec domain.

Finally, Key management can be done manually, but when it comes to large networks, this is not scalable, so IKE is used in this case.

Procedure

I. Host-to-Host IPSec Communication:

1. In the first, build a simple peer-to-peer network using two linux machines (virtual or standalone). In this experiment the IP address of the two PCs is 172.16.107.29 and 172.16.107.33.

2. Now, make sure that each host is reachable by other by using ping command.

3. There is some basic requirement to create a host-to-host secure communication are:

a. The IP address for both hosts.

b. A unique name to identify the IPsec connection and distinguish it from other devices or connections (for example, `ipsec0`)

c. A fixed encryption key or one automatically generated by `racoon`.

d. A pre-shared authentication key that is used to initiate the connection and exchange encryption keys during the session.

4. Install the IPSec tool with all its needed dependencies using the command:

```
sudo apt-get install -y ipsec-tools
```

5. Open the IPSec configuration file ipsec.conf. At the end of the file, add the following lines with the IPs you have used in your network:

```
conn host-to-host
authby=secret
auto=route
keyexchange=ike
left=172.16.107.29
right=172.16.107.33
type=transport
esp=aes128gcm16!
```

Make sure that the left and right IP addresses are the same in two devices.
The previous lines means:
conn host-to-host: is the connection here is host to host connection.
authby=secret: means the authentication is secret.
auto=route: on demand the IKE daemon will load connections with atuo=route and install trap policies.
keyexchange=ike: the key management here is the internet key exchange.
left=172.16.107.29: the IP address of the left host (IP of device x).
right=172.16.107.33: the IP address of the right host (IP of device y).
type=transport: mode type is transport mode.
esp=aes128gcm16!: the encryption algorithm is aes128gcm16.

6. Open the file ipsec.secrets under the etc directory.

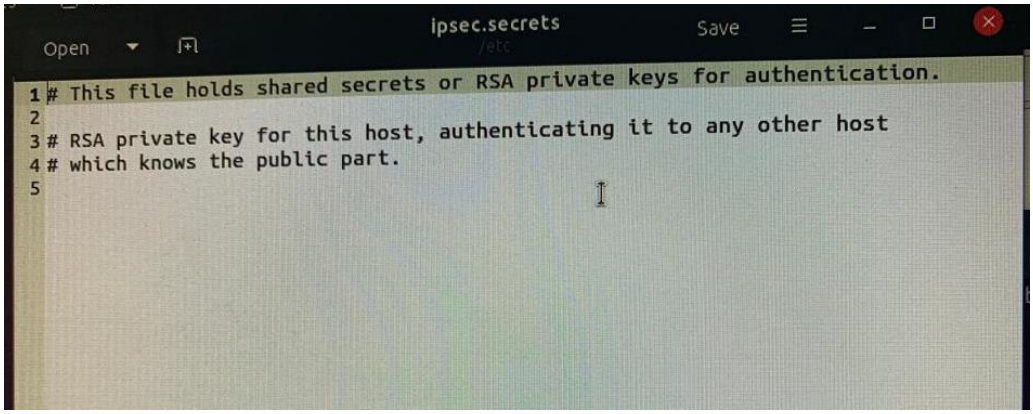


Figure1.1 shows the contains of file ipsec.secrets.

As it shows in figure1.1, file ipsec.secrets contain some comments that show the private key is an RSA key and will use in the authentication part.

Now, add the following line to the file ipsec.secrets. Make sure to include the IPs you have in your network instead of IPX and IPY. In addition, choose a strong password that meets the general security requirements.

IPX IPY : PSK "Your password here!".

In this experiment we write: 172.16.107.29 172.16.107.33 : PSK "Dyaa12345678"

7. Now re-start the IPSec process by using this command:

sudo ipsec restart

We need to re-start IPsec to apply the changes that were done on ipsec.conf, and ipsec.secrets files.

8. Run the command ipsec statusall, to return detailed status information on the connection.

Figure1.2 shows the status of IKE charon daemon.

The last figure shows the IP address of hosts in this connection, the type of the keys that are used, the mode of this connection, and shows the routed connections information.

9. Finally, do the same steps from 4-8 on the other host.

II. Testing the Constructed Tunnel:

1. Issue a ping command from the first host (x) to the second host (y), with packet size equal 4048. That's done by using this command:

ping -s 4048 172.16.107.33

2. Run the command watch ipsec statsuall. This command shows the status of the connection, and depending on the information there is a difference in the security associations between Figure1.2 and Figure1.3 (in the next page).
In Figure1.2 there are no security associations, but in Figure1.3 there are security associations between the two hosts using the IKE protocol.

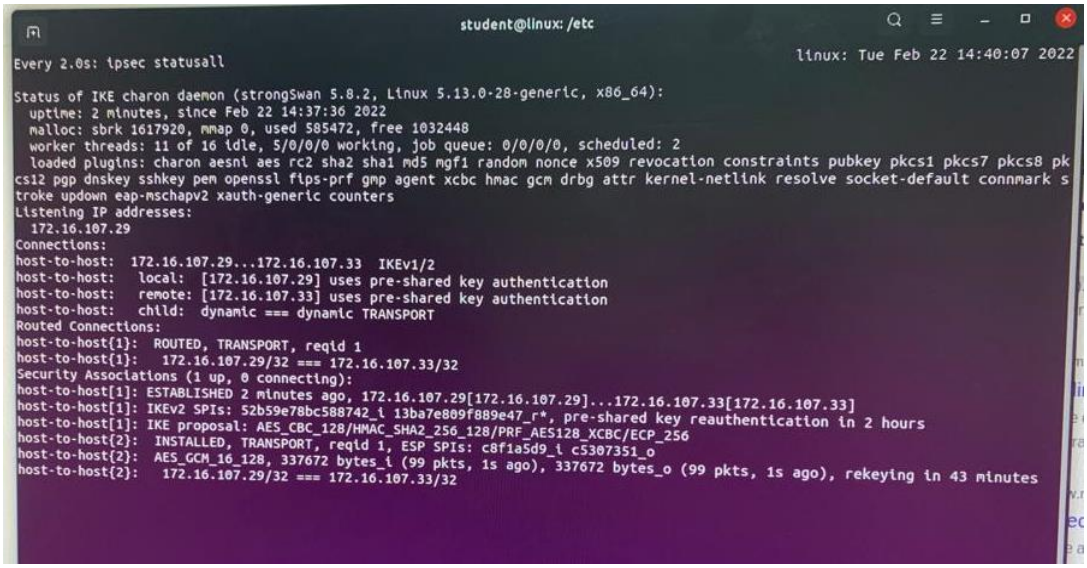
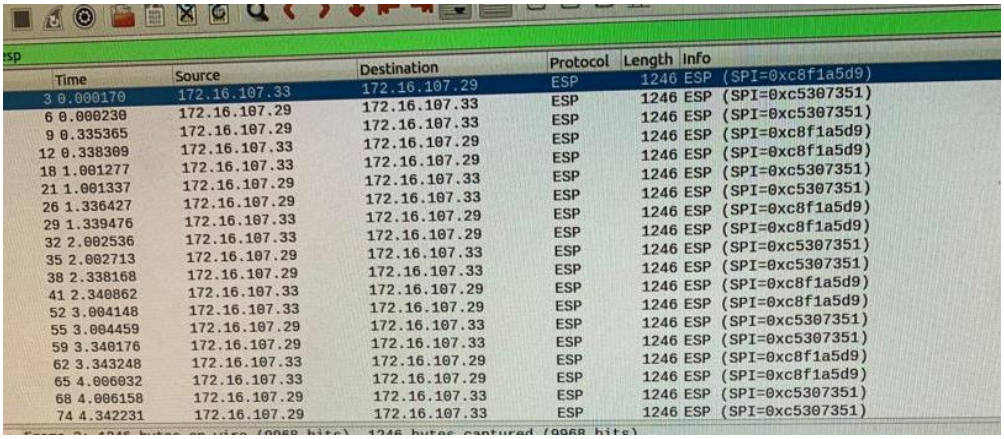


Figure1.3 shows the status of the connection.

3. Use tcpdump to capture ESP packets. Write those packets to a file named ESP.cap. Then using Wireshark open ESP.cap file and captured all ESP packets.



	Time	Source	Destination	Protocol	Length	Info
3	0.000170	172.16.107.33	172.16.107.29	ESP	1246	ESP (SPI=0xc8f1a5d9)
6	0.000230	172.16.107.29	172.16.107.33	ESP	1246	ESP (SPI=0xc5307351)
9	0.335365	172.16.107.29	172.16.107.33	ESP	1246	ESP (SPI=0xc5307351)
12	0.338309	172.16.107.33	172.16.107.29	ESP	1246	ESP (SPI=0xc8f1a5d9)
18	1.001277	172.16.107.33	172.16.107.29	ESP	1246	ESP (SPI=0xc8f1a5d9)
21	1.001337	172.16.107.29	172.16.107.33	ESP	1246	ESP (SPI=0xc5307351)
26	1.336427	172.16.107.29	172.16.107.33	ESP	1246	ESP (SPI=0xc5307351)
29	1.339476	172.16.107.33	172.16.107.29	ESP	1246	ESP (SPI=0xc8f1a5d9)
32	2.002536	172.16.107.33	172.16.107.29	ESP	1246	ESP (SPI=0xc8f1a5d9)
35	2.002713	172.16.107.29	172.16.107.33	ESP	1246	ESP (SPI=0xc5307351)
38	2.338168	172.16.107.29	172.16.107.33	ESP	1246	ESP (SPI=0xc5307351)
41	2.340862	172.16.107.33	172.16.107.29	ESP	1246	ESP (SPI=0xc8f1a5d9)
52	3.004148	172.16.107.33	172.16.107.29	ESP	1246	ESP (SPI=0xc8f1a5d9)
55	3.004459	172.16.107.29	172.16.107.33	ESP	1246	ESP (SPI=0xc5307351)
59	3.340176	172.16.107.29	172.16.107.33	ESP	1246	ESP (SPI=0xc5307351)
62	3.343248	172.16.107.33	172.16.107.29	ESP	1246	ESP (SPI=0xc8f1a5d9)
65	4.006032	172.16.107.33	172.16.107.29	ESP	1246	ESP (SPI=0xc8f1a5d9)
68	4.006158	172.16.107.29	172.16.107.33	ESP	1246	ESP (SPI=0xc5307351)
74	4.342231	172.16.107.29	172.16.107.33	ESP	1246	ESP (SPI=0xc5307351)

Figure1.4 shows some ESP caputred packets with there SPI vlaue.

4. Show the Security Associations (SAs) that have been implemented on the first host (x) , by using ipsec_spi command or from ipsec statusall command.

5. Now do ping from the second host (y) to the first host (x). Capture an ESP packet on the first host and check its SPI.

6. Change the pre-shared key value in one of the hosts, restart the IPSec process, and do ping again. Is there any captured packet?

There are no captured packets because there are no packets sent between two hosts; because this type of connection required have a pre-shared key between the hosts, so when changing the password there is no pre-shared key between two hosts.

III. SSH With the Constructed Tunnel:

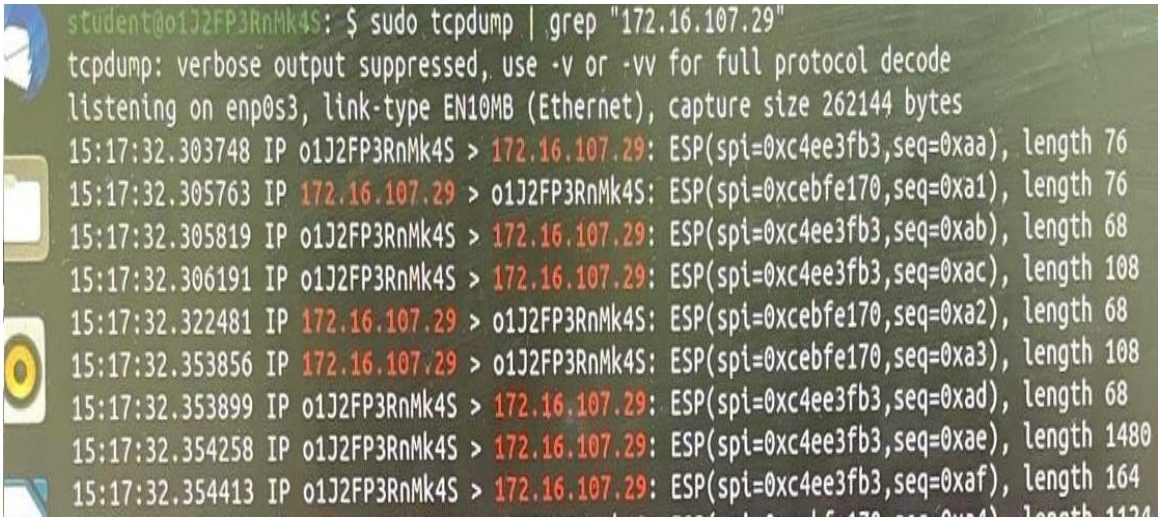
1. Install an SSH client on both machines. Make sure that it is installed using the command ssh.

2. Install an SSH server on both machines. If it is not installed, then you have to use the following command:
sudo apt-get install openssh-server ii.

3. Run the tcpdump on one machine and try to capture ESP packets.

4. Connect SSH from one machine to another. You can use the command ssh username@host-ip-address with the password of the host you are connecting to

5. Capture ESP packets.



tcpdump command was used to listen on the traffic of the network card, incoming and outgoing, we were looking for an ESP packet.
For the first ESP packet in the picture, it shows that tcpdump gives us the time this packet was sent, source and destination IP address,

the SPI value for the ESP packet since IPsec is applied, And the length of the packet.

Conclusion

In the end, in this experiment, we learned about how to make an IPsec connection between hosts, what is the main acquirement to build the connection, and how to open an SSH connection with the constructed tunnel.

References

TechTarget (IPsec).
Cloudflare.
ZoomAdmin.
https://wiki.strongswan.org/projects/strongswan/wiki/ipseccommand
http://manpages.ubuntu.com/manpages/bionic/man4/ipsec.4freebsd.html
https://seedsecuritylabs.org/
https://wiki.strongswan.org/projects/strongswan/wiki/