Tarun kumar yadav
2014110
NS lab Assignment 3

Question 1

PC1 IP address : 192.168.32.109
PC2 IP address : 192.168.32.110

Part 1

PC 1
sudo modprobe dummy
sudo ip link set name eth10 dev dummy0
sudo ip addr add 10.10.10.1/24 brd + dev eth10 label eth10:0
sudo sysctl -w net.ipv4.ip_forward=1
sudo route add -net 20.20.20.0 netmask 255.255.255.0 gw 192.168.32.110 dev eno1

PC 2
sudo modprobe dummy
sudo ip link set name eth10 dev dummy0
sudo ip addr add 20.20.20.1/24 brd + dev eth10 label eth10:0
sudo sysctl -w net.ipv4.ip_forward=1
sudo route add -net 10.10.10.0 netmask 255.255.255.0 gw 192.168.32.109 dev eno1

After this run ping 20.20.20.1 from PC1 and ping 10.10.10.1 from PC2

Part 2

As I am worked on ubuntu 16.04 i.e I used strongswan for setting up vpn tunnel
Install strongswan on both hosts i.e A and B

Sudo apt-get install ipsec-tools strongswan-starter

PC1

Sudo gedit edit /etc/ipsec.conf

And copy below text in it.

```
conn red-to-blue
    authby=secret
    auto=route
    keyexchange=ike
    left=192.168.32.109
    right=192.168.32.110
    type=tunnel
    esp=aes128gcm16!
```

sudo gedit /etc/ipsec.secrets
And copy below code in it.
192.168.32.109 192.168.32.110 : PSK "pass”

Sudo ipsec restart

PC2

Sudo gedit /etc/ipsec.conf
And copy below text in it.

```
conn blue-to-red
    authby=secret
    auto=route
    keyexchange=ike
    left=192.168.32.110
    right=192.168.32.109
    type=tunnel
    esp=aes128gcm16!
```

sudo gedit /etc/ipsec.secrets
And copy below code in it.
192.168.32.110 192.168.32.109 : PSK "pass”

Sudo ipsec restart

Testing our Tunnel

From PC2
Ping 10.10.10.1 OR ping 192.168.32.109

From PC1
sudo tcpdump esp OR sudo Wireshark (and capture esp packets)

I have attached the screenshot of the output and the pcap file.

Question 2

PC 1
Step 1 => gpg2 --full-gen-key
// generating public and private key

Step 2 => gpg2 --export --armor tarun14110@iiitd.ac.in > tarun-pubkey.asc
// making copy of public key

Step 3 => gpg2 --export-secret-keys --armor tarun14110@iiitd.ac.in > tarun-privkey.asc
// making copy of private key

Step 6 => gpg --decrypt FCS_Assignment4.pdf.gpg > secret.pdf

PC 2
Step 4 => gpg --import tarun-pubkey.asc
// importing public key for encryption

Step 5 => gpg --encrypt --recipient NSLab FCS_Assignment4.pdf
// encrypting the file

Note: private and public key along with encrypted file is attached