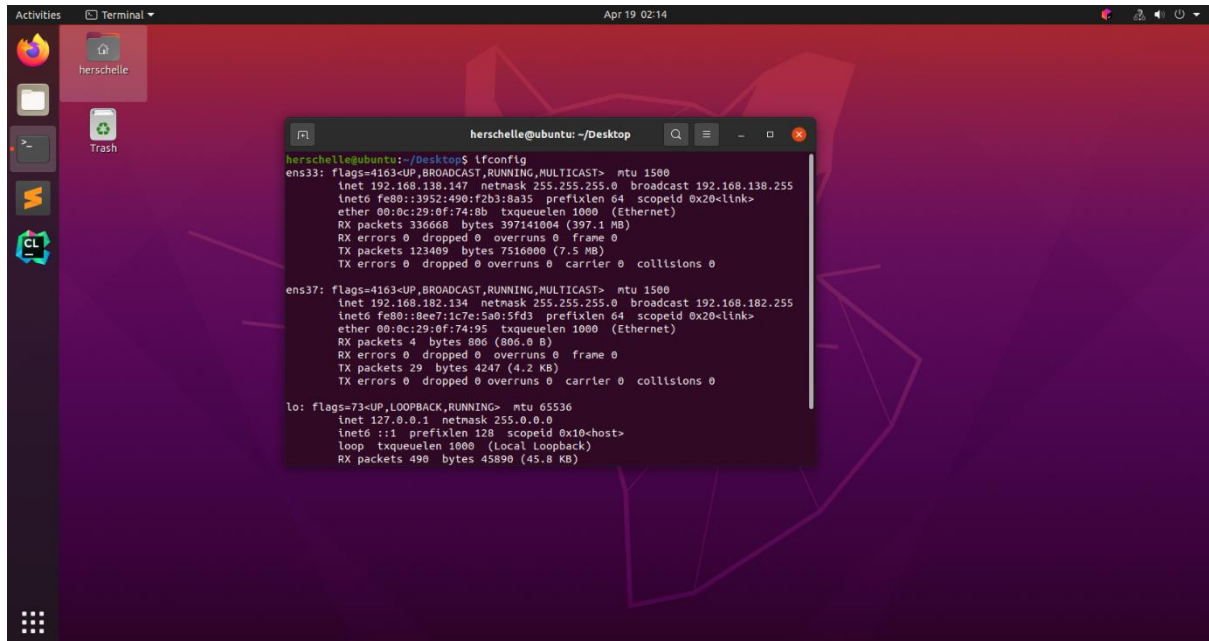


IP of VM2: 192.168.182.134

IP of VM3: 192.168.182.135

VM2:-

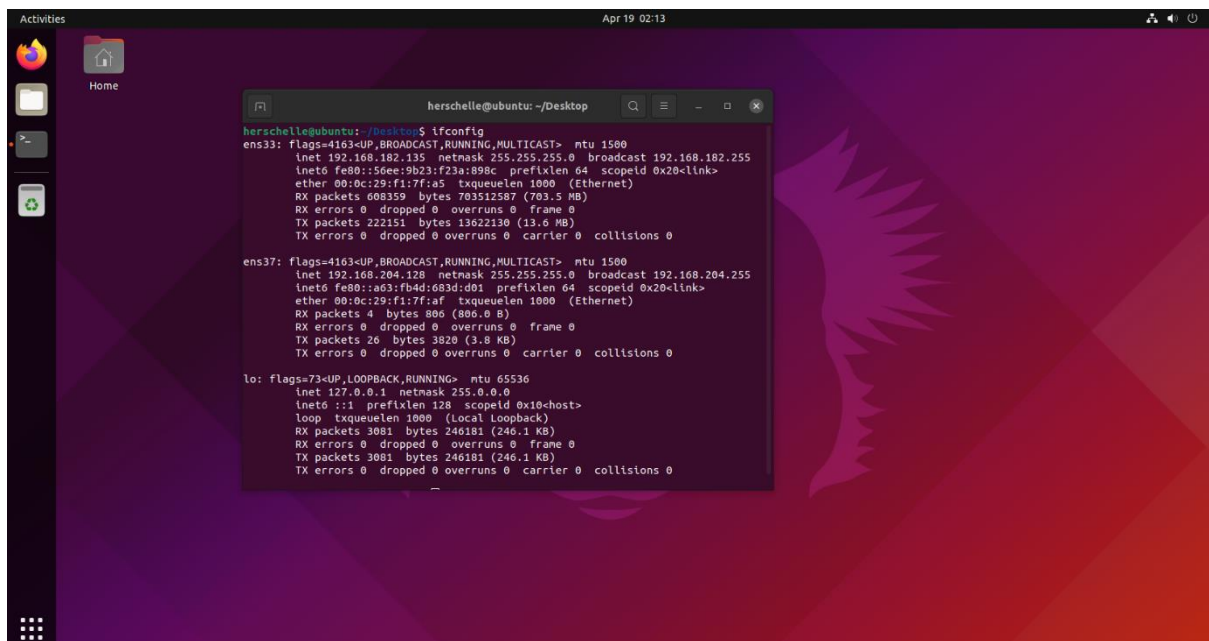


```
herschelle@ubuntu: ~/Desktop
herschelle@ubuntu:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.138.147 netmask 255.255.255.0 broadcast 192.168.138.255
    inet6 fe80::3952:490:f2b3:8a35 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:10:f7:48b txqueuelen 1000 (Ethernet)
    RX packets 336608 bytes 397141004 (397.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 123409 bytes 7516000 (7.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.182.134 netmask 255.255.255.0 broadcast 192.168.182.255
    inet6 fe80::8ee7:1c7e:5a0:5fd3 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:0f:74:95 txqueuelen 1000 (Ethernet)
    RX packets 4 bytes 806 (806.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 29 bytes 4247 (4.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 490 bytes 45890 (45.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

VM3:-



```
herschelle@ubuntu: ~/Desktop
herschelle@ubuntu:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.182.135 netmask 255.255.255.0 broadcast 192.168.182.255
    inet6 fe80::56ee:9b23:f23a:898c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f1:7f:a5 txqueuelen 1000 (Ethernet)
    RX packets 608350 bytes 703512587 (703.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 222151 bytes 13622130 (13.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.204.120 netmask 255.255.255.0 broadcast 192.168.204.255
    inet6 fe80::a63:fb4d:683d:d01 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f1:7f:af txqueuelen 1000 (Ethernet)
    RX packets 4 bytes 806 (806.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26 bytes 3820 (3.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 3081 bytes 246181 (246.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3081 bytes 246181 (246.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

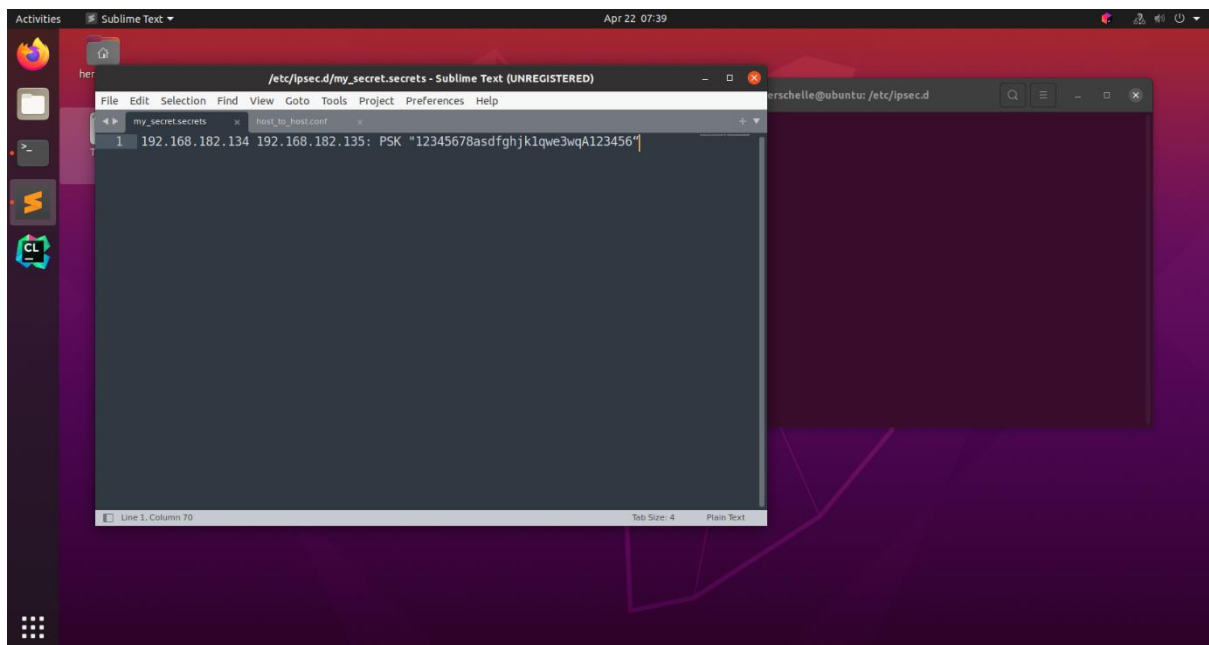
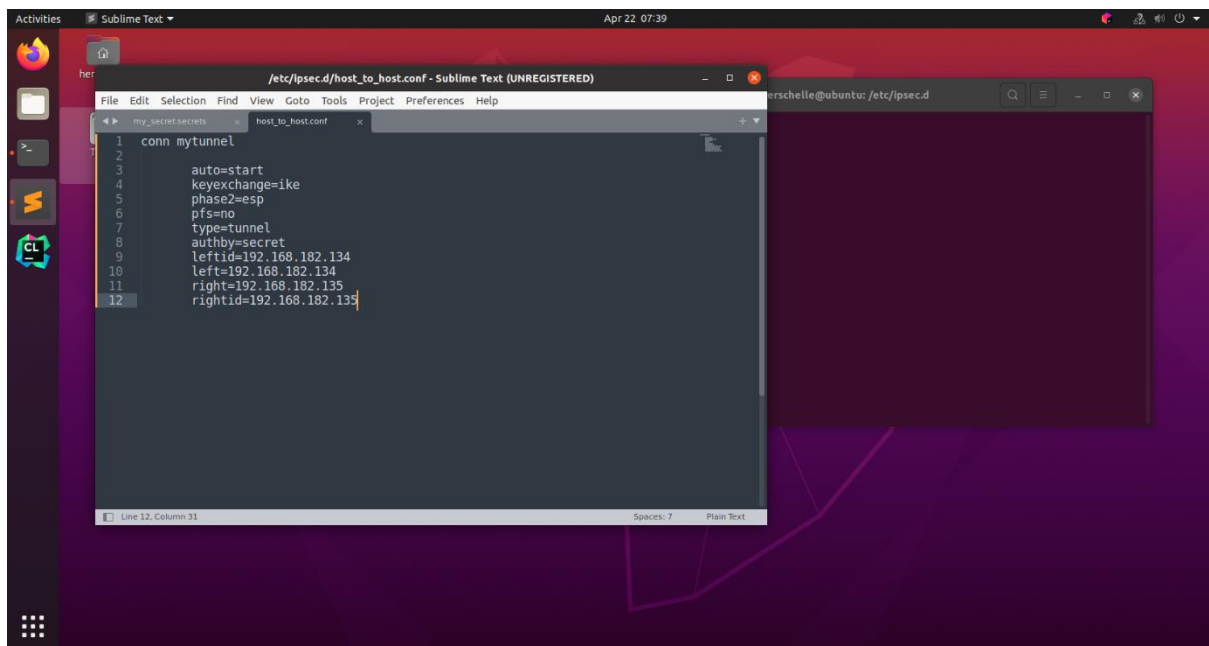
On VM2 and VM3 do the following:

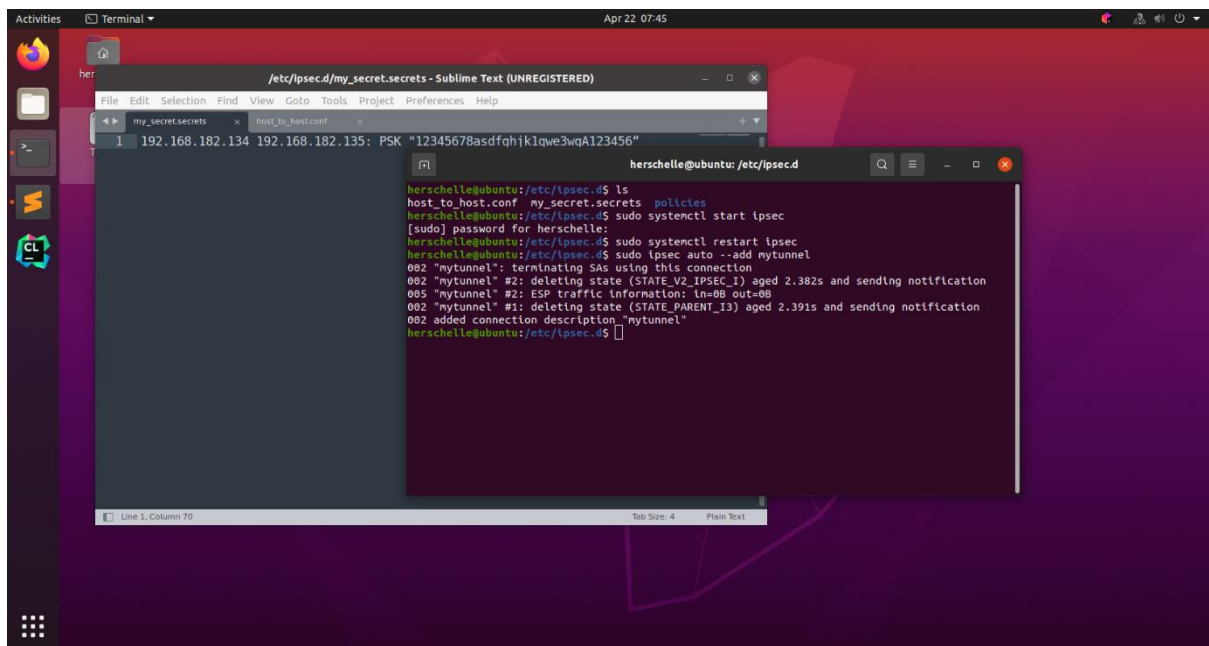
apt-get install libreswan

systemctl enable ipsec

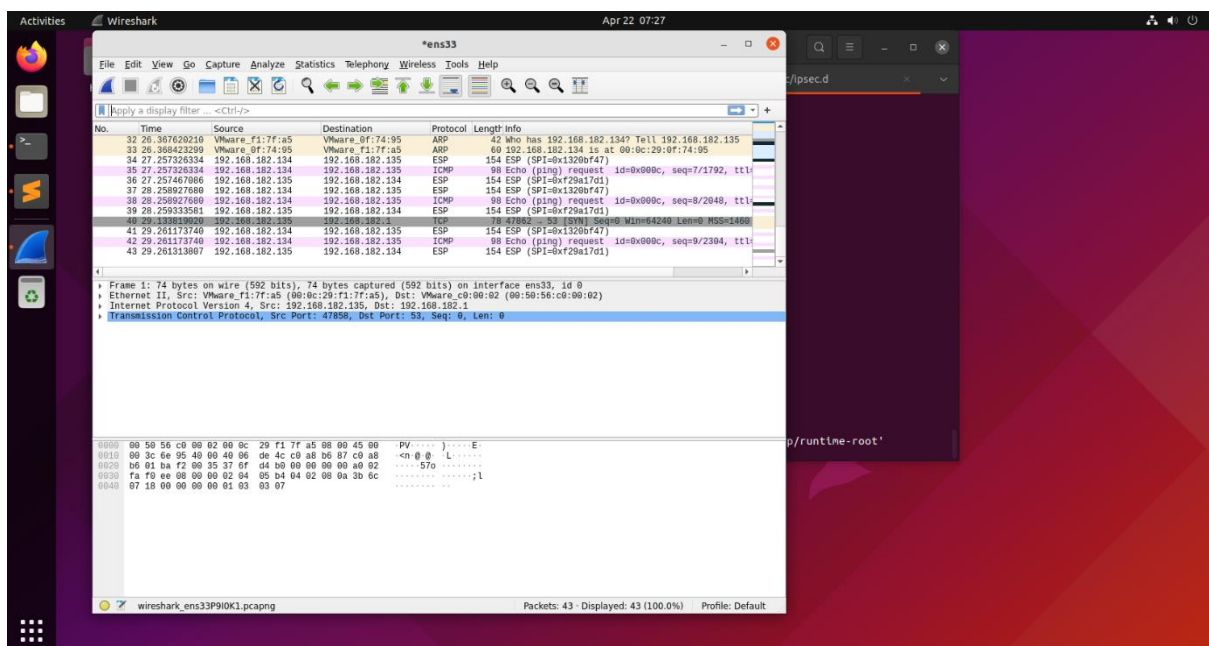
ipsec initnss

In /etc/ipsec.d/ directory add the following files with following data





Ping from VM2 and fire up wireshark on VM3 and we can see esp packets.



Wireshark/Tcpdump acts weirdly with IPsec, it decrypts the incoming packet which can see in the screenshot above. The same is written at the end of the below link.

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sec-host-to-host_vpn_using_libreswan

To verify that packets are being sent via the VPN tunnel, issue a command as `root` in the following format:

```
~]# tcpdump -n -i interface esp or udp port 500 or udp port 4500
00:32:32.632165 IP 192.1.2.45 > 192.1.2.23: ESP(spi=0x63ad7e17,seq=0x1a), length 132
00:32:32.632592 IP 192.1.2.23 > 192.1.2.45: ESP(spi=0x4841b647,seq=0x1a), length 132
00:32:32.632592 IP 192.0.2.254 > 192.0.1.254: ICMP echo reply, id 2489, seq 7, length 64
00:32:33.632221 IP 192.1.2.45 > 192.1.2.23: ESP(spi=0x63ad7e17,seq=0x1b), length 132
00:32:33.632731 IP 192.1.2.23 > 192.1.2.45: ESP(spi=0x4841b647,seq=0x1b), length 132
00:32:33.632731 IP 192.0.2.254 > 192.0.1.254: ICMP echo reply, id 2489, seq 8, length 64
00:32:34.632183 IP 192.1.2.45 > 192.1.2.23: ESP(spi=0x63ad7e17,seq=0x1c), length 132
00:32:34.632607 IP 192.1.2.23 > 192.1.2.45: ESP(spi=0x4841b647,seq=0x1c), length 132
00:32:34.632607 IP 192.0.2.254 > 192.0.1.254: ICMP echo reply, id 2489, seq 9, length 64
00:32:35.632233 IP 192.1.2.45 > 192.1.2.23: ESP(spi=0x63ad7e17,seq=0x1d), length 132
00:32:35.632685 IP 192.1.2.23 > 192.1.2.45: ESP(spi=0x4841b647,seq=0x1d), length 132
00:32:35.632685 IP 192.0.2.254 > 192.0.1.254: ICMP echo reply, id 2489, seq 10, length 64
```

Where *interface* is the interface known to carry the traffic. To end the capture with `tcpdump`, press `Ctrl` + `C` .



Note

The `tcpdump` commands interacts a little unexpectedly with IPsec . It only sees the outgoing encrypted packet, not the outgoing plaintext packet. It does see the encrypted incoming packet, as well as the decrypted incoming packet. If possible, run `tcpdump` on a router between the two machines and not on one of the endpoints itself.