Week 7

Firewall Evasion Lab: BypassingFirewalls using VPN

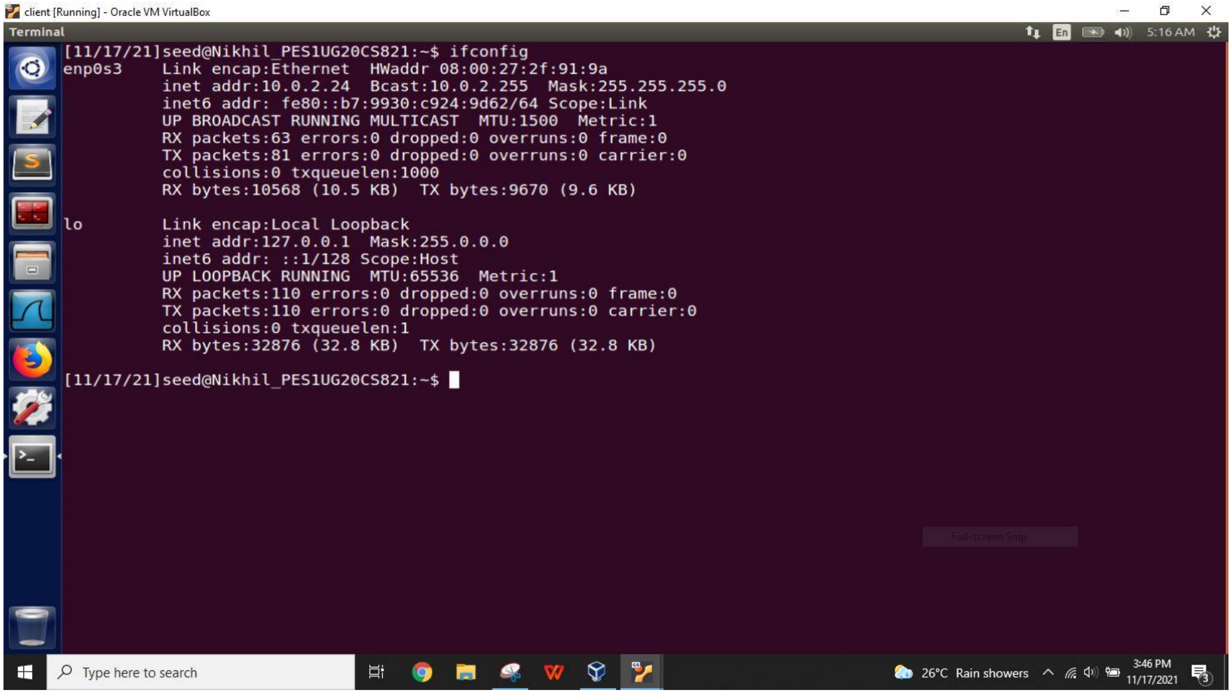
Name:Nikhil T M

SRN:PES1UG20CS821

Lab Setup:

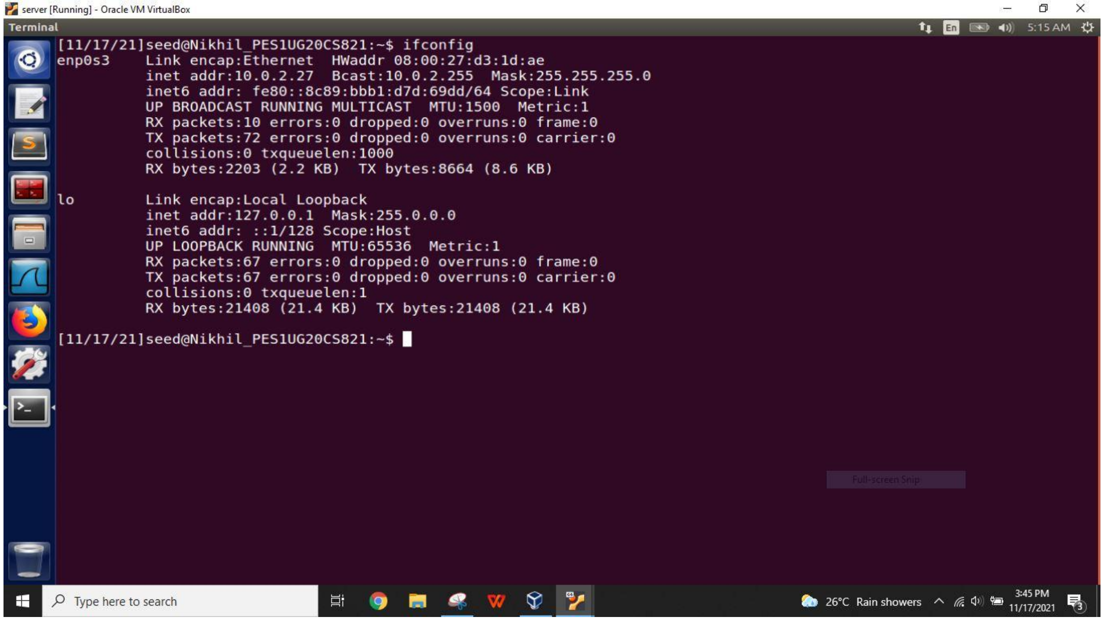
In this lab we use 2 vm's named as client and server

VM1: VPN Client (IP: 10.0.2.24)



```
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:2f:91:9a
          inet addr:10.0.2.24  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::b7:9930:c924:9d62/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:63 errors:0 dropped:0 overruns:0 frame:0
          TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10568 (10.5 KB)  TX bytes:9670 (9.6 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:110 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:32876 (32.8 KB)  TX bytes:32876 (32.8 KB)

[11/17/21]seed@Nikhil_PES1UG20CS821:~$
```

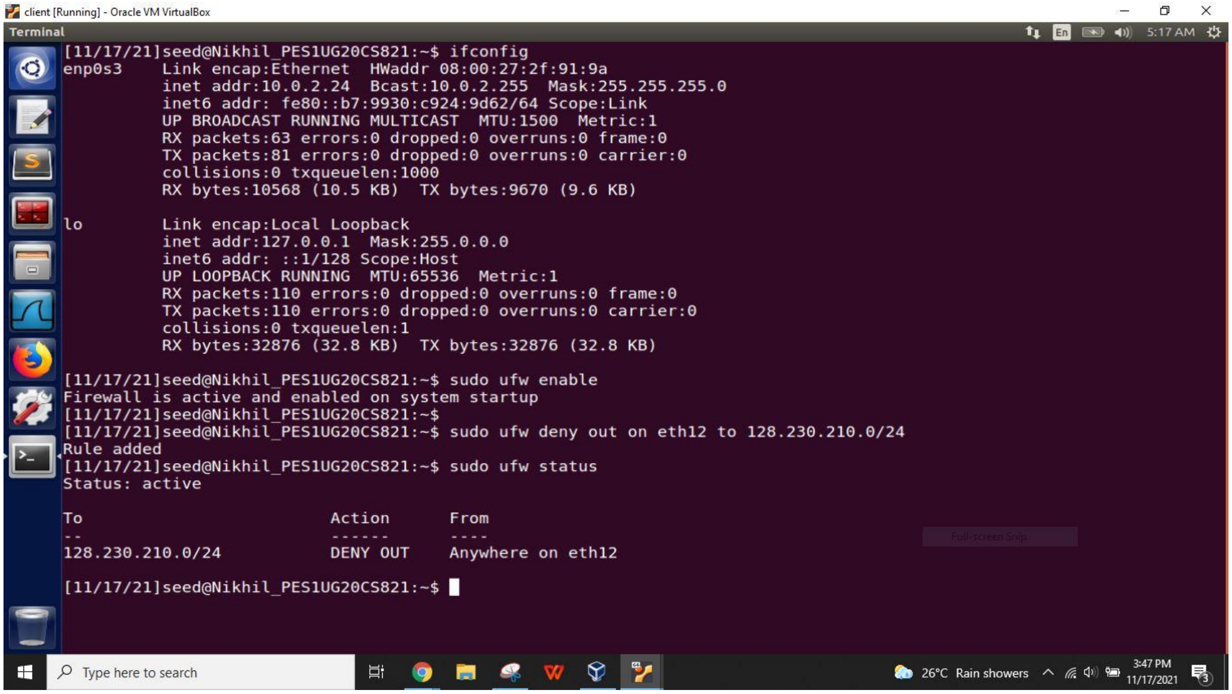
VM2: VPN Server (IP: 10.0.2.27)



```
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:d3:1d:ae
          inet addr:10.0.2.27  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::8c89:bbb1:d7d:69dd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2203 (2.2 KB)  TX bytes:8664 (8.6 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:67 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:21408 (21.4 KB)  TX bytes:21408 (21.4 KB)

[11/17/21]seed@Nikhil_PES1UG20CS821:~$
```

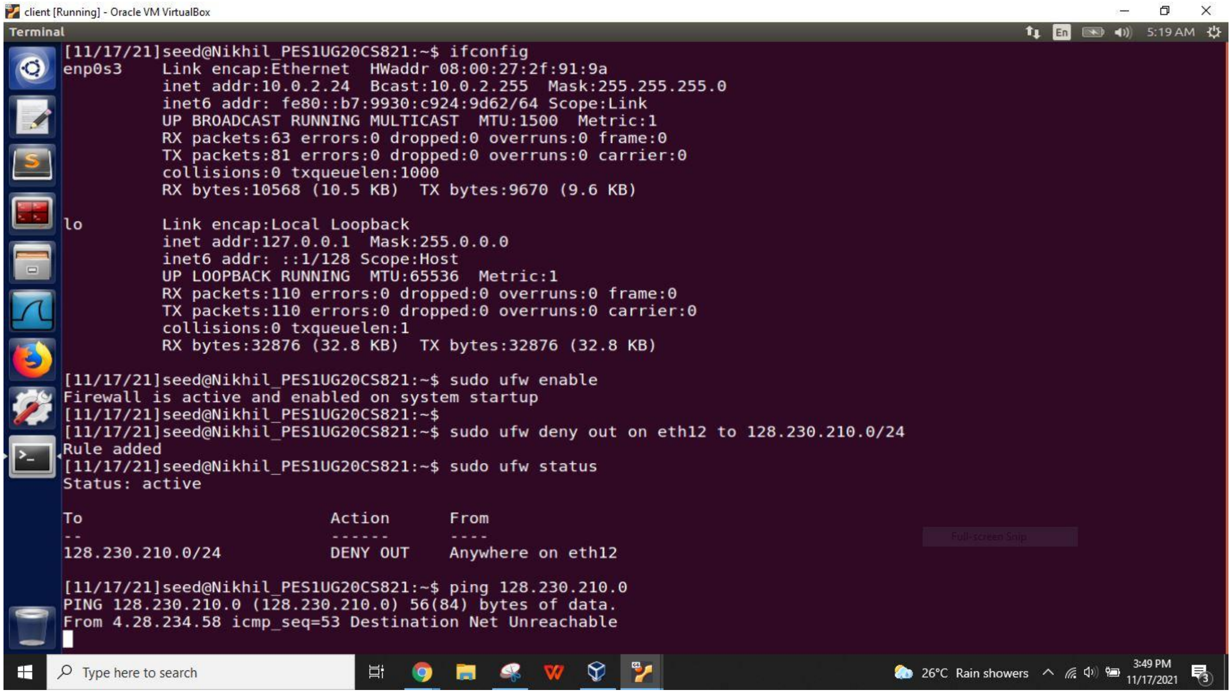
Task 2: Set up Firewall

In this task we will setup the firewall in the client vm to block the website containing the ip address 128.230.210.0



```
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:2f:91:9a
          inet addr:10.0.2.24  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::b7:9930:c924:9d62/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:63 errors:0 dropped:0 overruns:0 frame:0
          TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10568 (10.5 KB)  TX bytes:9670 (9.6 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:110 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:32876 (32.8 KB)  TX bytes:32876 (32.8 KB)

[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw enable
Firewall is active and enabled on system startup
[11/17/21]seed@Nikhil_PES1UG20CS821:~$
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw deny out on eth12 to 128.230.210.0/24
Rule added
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
128.230.210.0/24           DENY OUT    Anywhere on eth12

[11/17/21]seed@Nikhil_PES1UG20CS821:~$
```

We check whether the site is blocked or not by pinging its ip address and we can see that the ping is unsuccessful



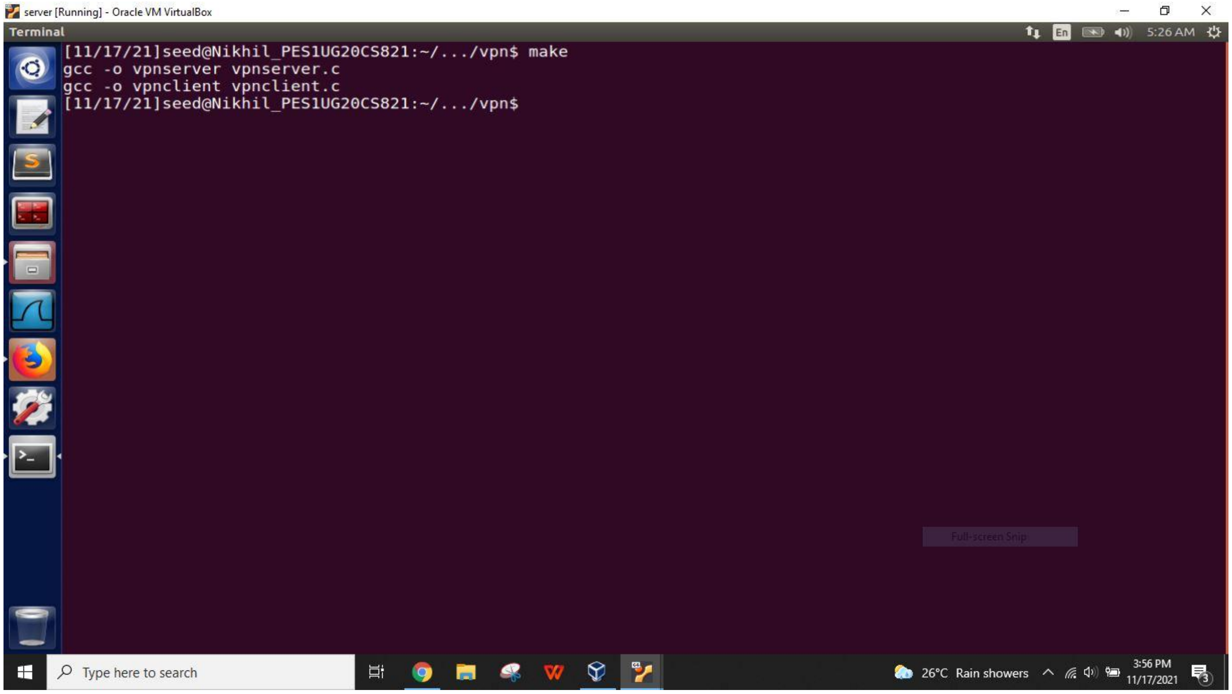
```
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:2f:91:9a
          inet addr:10.0.2.24  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::b7:9930:c924:9d62/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:63 errors:0 dropped:0 overruns:0 frame:0
          TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10568 (10.5 KB)  TX bytes:9670 (9.6 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:110 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:32876 (32.8 KB)  TX bytes:32876 (32.8 KB)

[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw enable
Firewall is active and enabled on system startup
[11/17/21]seed@Nikhil_PES1UG20CS821:~$
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw deny out on eth12 to 128.230.210.0/24
Rule added
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
128.230.210.0/24           DENY OUT    Anywhere on eth12

[11/17/21]seed@Nikhil_PES1UG20CS821:~$ ping 128.230.210.0
PING 128.230.210.0 (128.230.210.0) 56(84) bytes of data.
From 4.28.234.58 icmp_seq=53 Destination Net Unreachable
```

Task 3: Bypassing Firewall using VPN

In this task we establish the VPN tunnel between server and client VM’s that is when client tries to access the blocked site it will not directly pass through the network adapter as it is blocked so the packets to the blocked site from client will be routed to the VPN tunnel and reaches at Server VM after it reaches the Server VM will route them to the destination site when it reply it follows the same path in reverse order.

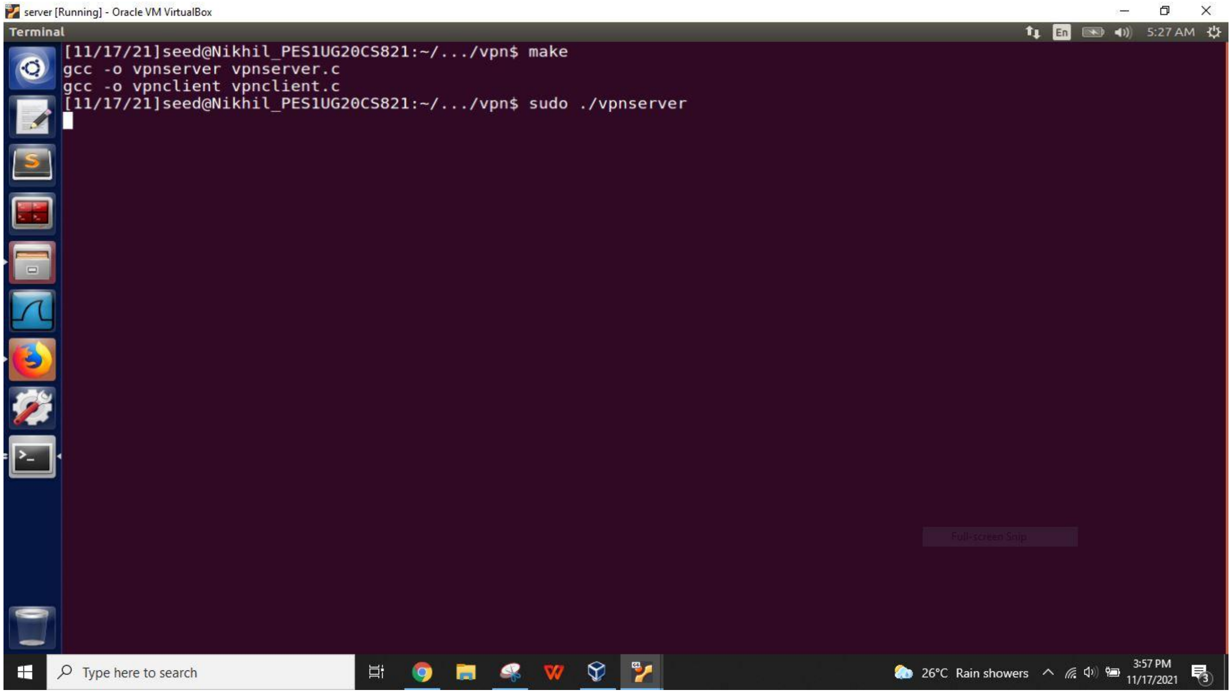
Step 1: Run VPN Server:

We first build the make file on the server VM



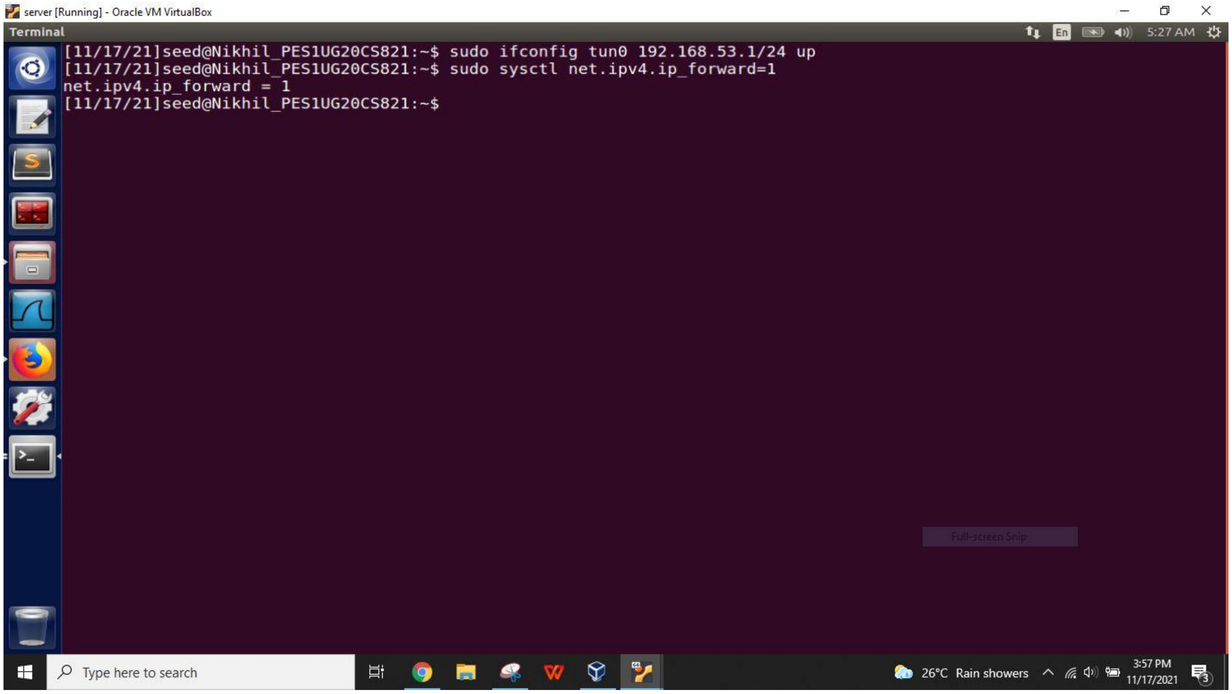
```
[11/17/21]seed@Nikhil_PES1UG20CS821:~/.../vpn$ make
gcc -o vpnserver vpnserver.c
gcc -o vpnclient vpnclient.c
[11/17/21]seed@Nikhil_PES1UG20CS821:~/.../vpn$
```

Then we run the VPN server program vpnserver on the Server VM.



```
[11/17/21]seed@Nikhil_PES1UG20CS821:~/.../vpn$ make
gcc -o vpnserver vpnserver.c
gcc -o vpnclient vpnclient.c
[11/17/21]seed@Nikhil_PES1UG20CS821:~/.../vpn$ sudo ./vpnserver
```

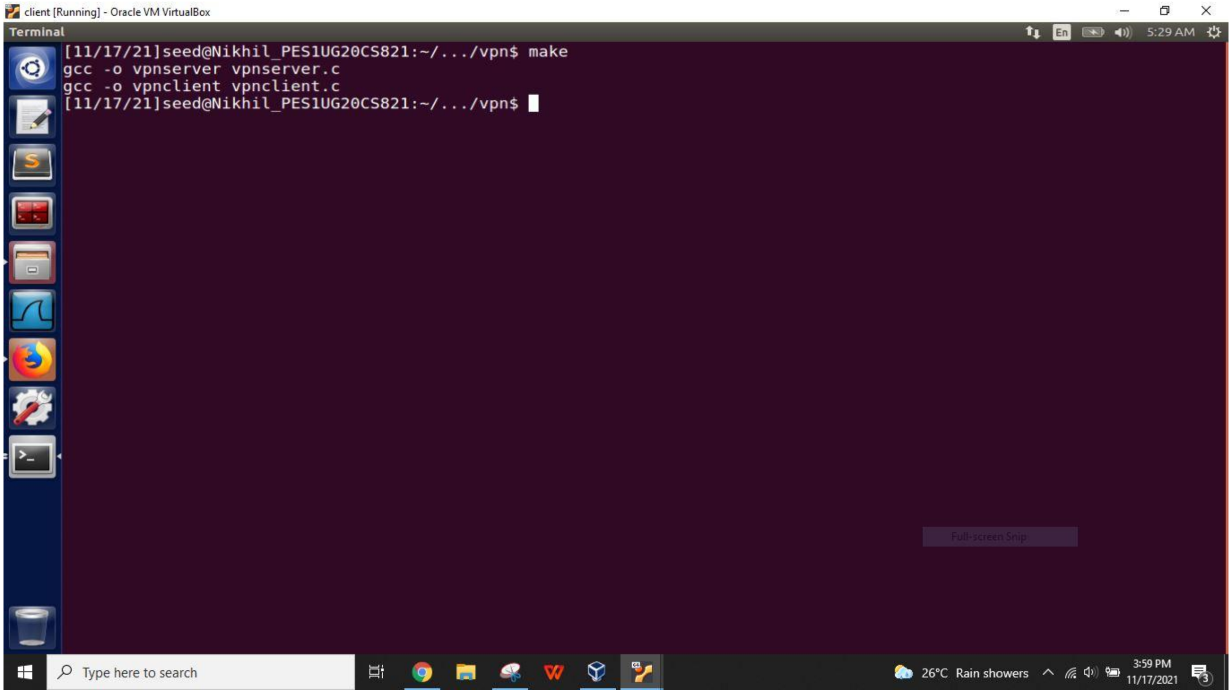
The server VM need to forward the packets so we set the forward to 1 by enabling it



```
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ifconfig tun0 192.168.53.1/24 up
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
[11/17/21]seed@Nikhil_PES1UG20CS821:~$
```

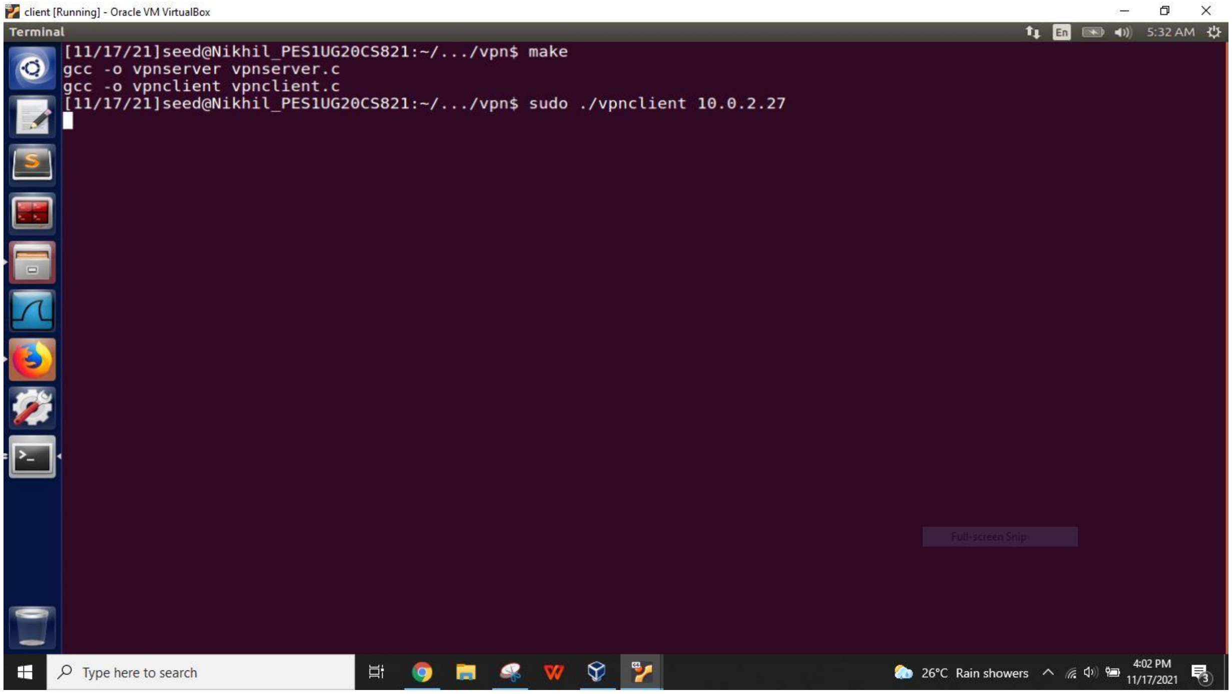
Step 2: Run VPN Client:

In client VM also we build the make file



```
[11/17/21]seed@Nikhil_PES1UG20CS821:~/.../vpn$ make
gcc -o vpnserver vpnserver.c
gcc -o vpnclient vpnclient.c
[11/17/21]seed@Nikhil_PES1UG20CS821:~/.../vpn$ 
```

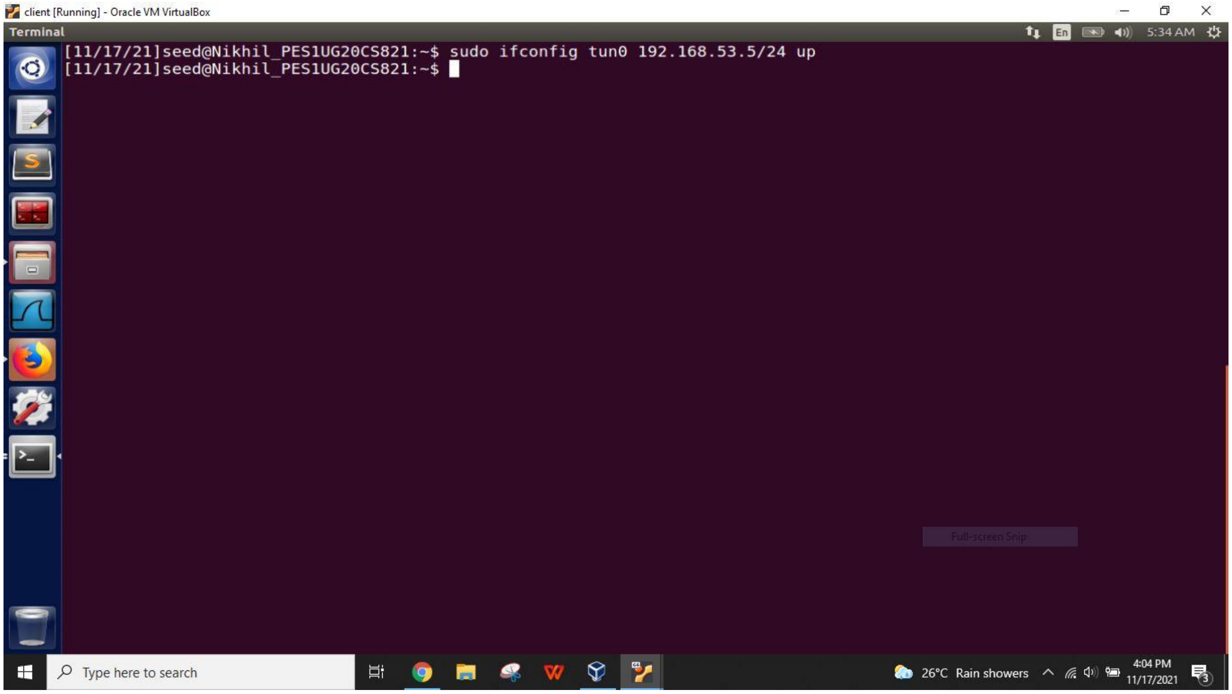
Next we run the VPN client program on the Client VM



```
[11/17/21]seed@Nikhil_PES1UG20CS821:~/.../vpn$ make
gcc -o vpnserver vpnserver.c
gcc -o vpnclient vpnclient.c
[11/17/21]seed@Nikhil_PES1UG20CS821:~/.../vpn$ sudo ./vpnclient 10.0.2.27
```

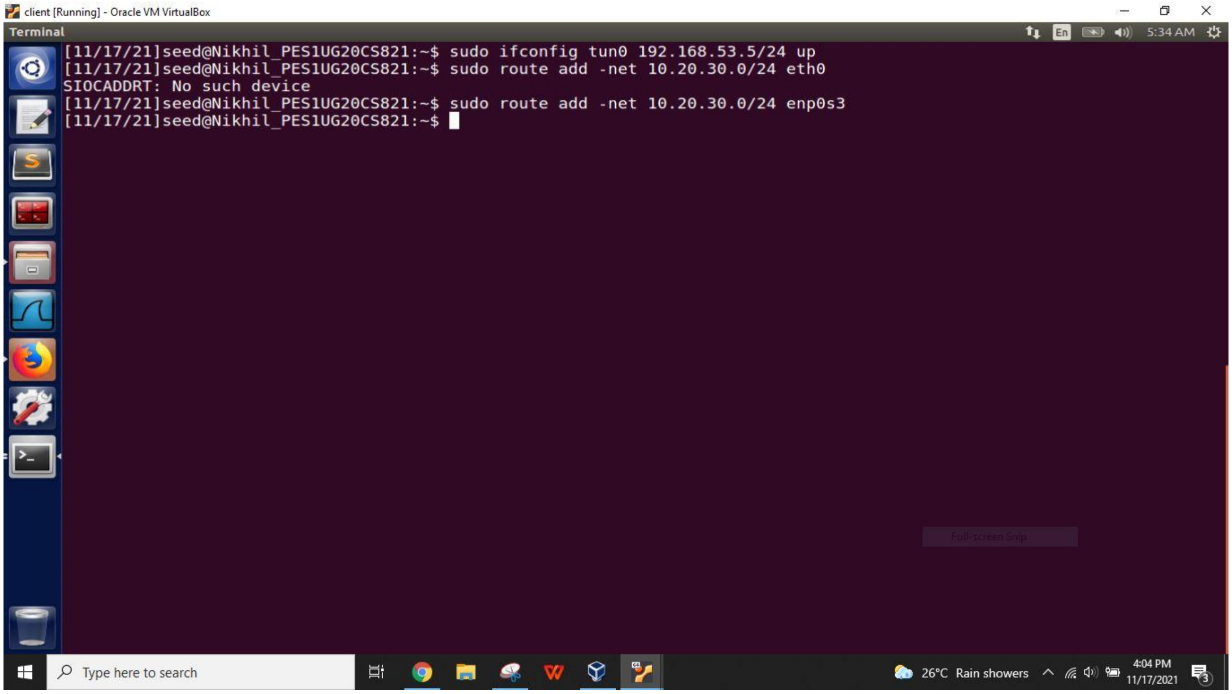
Step 3: Set Up Routing on Client and Server VMs:

we assign IP address 192.168.53.5 to the tun0 interface



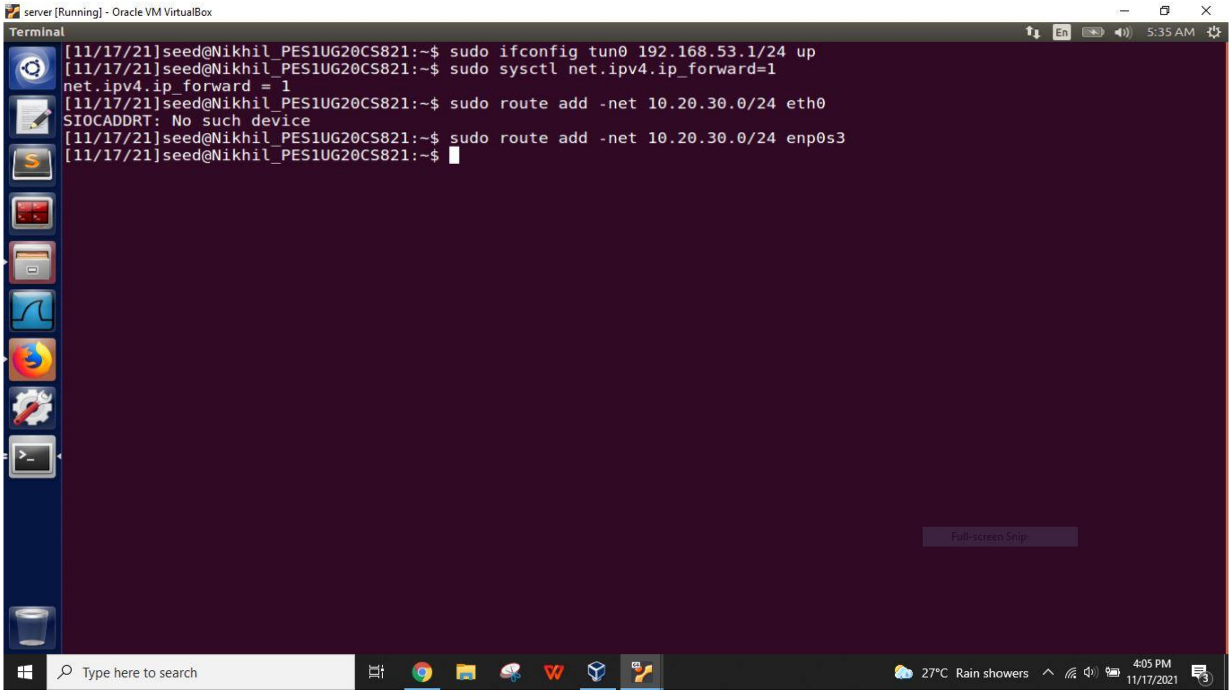
```
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ifconfig tun0 192.168.53.5/24 up
[11/17/21]seed@Nikhil_PES1UG20CS821:~$
```

We add the ip route in both client and server VM



```
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ifconfig tun0 192.168.53.5/24 up
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo route add -net 10.20.30.0/24 eth0
SIOCADDRT: No such device
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo route add -net 10.20.30.0/24 enp0s3
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ 
```

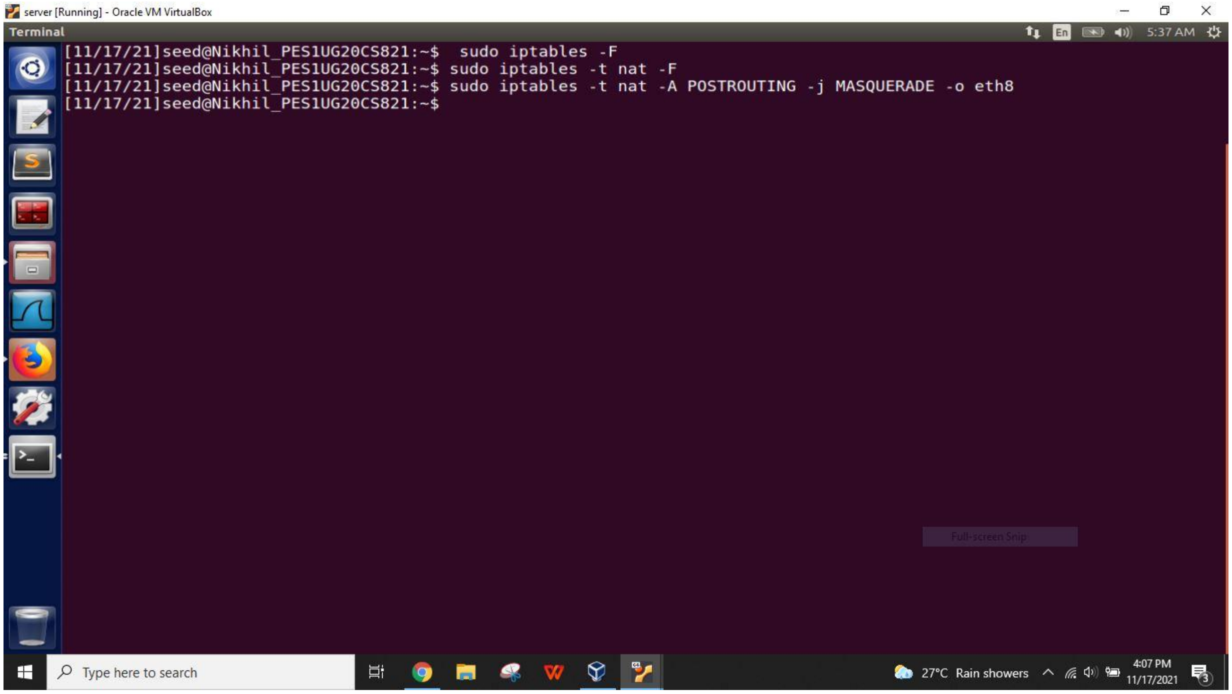
Same thing is done on the server VM



```
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ifconfig tun0 192.168.53.1/24 up
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo route add -net 10.20.30.0/24 eth0
SIOCADDRT: No such device
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo route add -net 10.20.30.0/24 enp0s3
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ 
```

Step 4: Set Up NAT on Server VM:

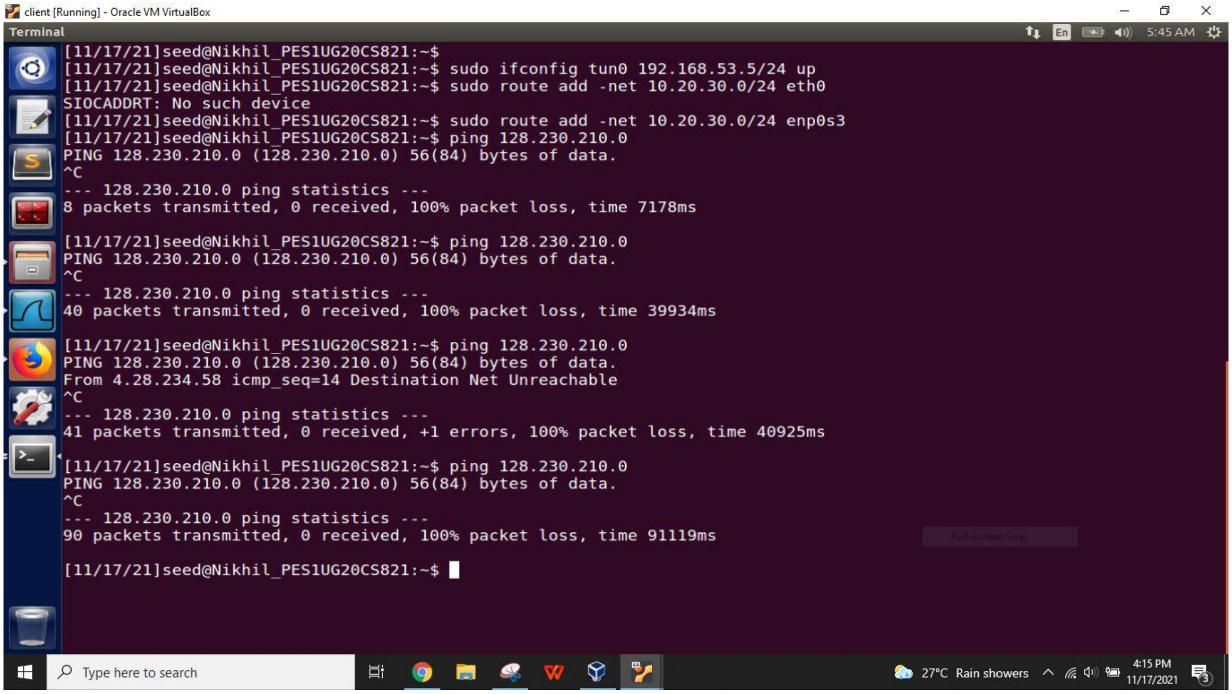
We enable the NAT on the Server VM so that the packet can travel from Server VM to client VM



```
[11/17/21]seed@Nikhil_PES1UG20CS821:~$  sudo iptables -F
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo iptables -t nat -F
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo iptables -t nat -A POSTROUTING -j MASQUERADE -o eth8
[11/17/21]seed@Nikhil_PES1UG20CS821:~$
```

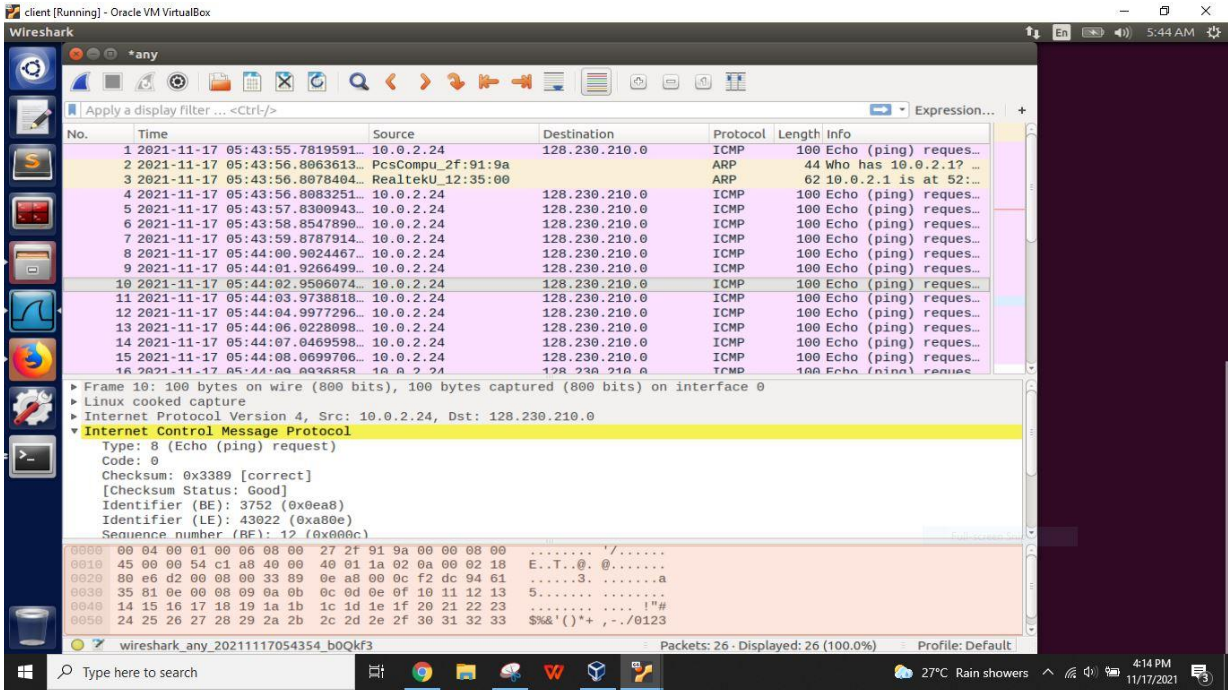
Demonstration

After setting up and configuring the VM's we can able to send the packets form the Client vm and it sent from client to server as it is blocked in the client.



```
[11/17/21]seed@Nikhil_PES1UG20CS821:~$
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo ifconfig tun0 192.168.53.5/24 up
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo route add -net 10.20.30.0/24 eth0
SIOCADDRT: No such device
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ sudo route add -net 10.20.30.0/24 enp0s3
[11/17/21]seed@Nikhil_PES1UG20CS821:~$ ping 128.230.210.0
PING 128.230.210.0 (128.230.210.0) 56(84) bytes of data.
^C
--- 128.230.210.0 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7178ms

[11/17/21]seed@Nikhil_PES1UG20CS821:~$ ping 128.230.210.0
PING 128.230.210.0 (128.230.210.0) 56(84) bytes of data.
^C
--- 128.230.210.0 ping statistics ---
40 packets transmitted, 0 received, 100% packet loss, time 39934ms

[11/17/21]seed@Nikhil_PES1UG20CS821:~$ ping 128.230.210.0
PING 128.230.210.0 (128.230.210.0) 56(84) bytes of data.
From 4.28.234.58 icmp_seq=14 Destination Net Unreachable
^C
--- 128.230.210.0 ping statistics ---
41 packets transmitted, 0 received, +1 errors, 100% packet loss, time 40925ms

[11/17/21]seed@Nikhil_PES1UG20CS821:~$ ping 128.230.210.0
PING 128.230.210.0 (128.230.210.0) 56(84) bytes of data.
^C
--- 128.230.210.0 ping statistics ---
90 packets transmitted, 0 received, 100% packet loss, time 91119ms

[11/17/21]seed@Nikhil_PES1UG20CS821:~$
```

Below we can see the wireshark observation of packets being sent



No.	Time	Source	Destination	Protocol	Length	Info
1	2021-11-17 05:43:55.7819591…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…
2	2021-11-17 05:43:56.8063613…	PcsCompu_2f:91:9a		ARP	44	Who has 10.0.2.1? …
3	2021-11-17 05:43:56.8078404…	RealtekU_12:35:00		ARP	62	10.0.2.1 is at 52:…
4	2021-11-17 05:43:56.8083251…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…
5	2021-11-17 05:43:57.8300943…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…
6	2021-11-17 05:43:58.8547890…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…
7	2021-11-17 05:43:59.8787914…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…
8	2021-11-17 05:44:00.9024467…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…
9	2021-11-17 05:44:01.9266499…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…
10	2021-11-17 05:44:02.9506074…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…
11	2021-11-17 05:44:03.9738818…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…
12	2021-11-17 05:44:04.9977296…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…
13	2021-11-17 05:44:06.0228098…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…
14	2021-11-17 05:44:07.0469598…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…
15	2021-11-17 05:44:08.0699706…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…
16	2021-11-17 05:44:09.0936858…	10.0.2.24	128.230.210.0	ICMP	100	Echo (ping) reques…

```
▸ Frame 10: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.24, Dst: 128.230.210.0
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x3389 [correct]
    [Checksum Status: Good]
    Identifier (BE): 3752 (0x0ea8)
    Identifier (LE): 43022 (0xa80e)
    Sequence number (BE): 12 (0x000c)
```

```
0000  00 04 00 01 00 06 08 00  27 2f 91 9a 00 00 08 00   ........ '/......
0010  45 00 00 54 c1 a8 40 00  40 01 1a 02 0a 00 02 18   E..T..@. @.......
0020  80 e6 d2 00 08 00 33 89  0e a8 00 0c f2 dc 94 61   ......3. .......a
0030  35 81 0e 00 08 09 0a 0b  0c 0d 0e 0f 10 11 12 13   5....... ........
0040  14 15 16 17 18 19 1a 1b  1c 1d 1e 1f 20 21 22 23   ........ .... !"#
0050  24 25 26 27 28 29 2a 2b  2c 2d 2e 2f 30 31 32 33   $%&'()*+ ,-./0123
```

wireshark_any_20211117054354_b0Qkf3 Packets: 26 · Displayed: 26 (100.0%) Profile: Default