CNS LAB

LAB - 7

Firewall Evasion Lab:
Bypassing Firewalls using VPN

NAME : SIRI S

SEMESTER : 5

SECTION :H

SRN : PES1UG19CS485

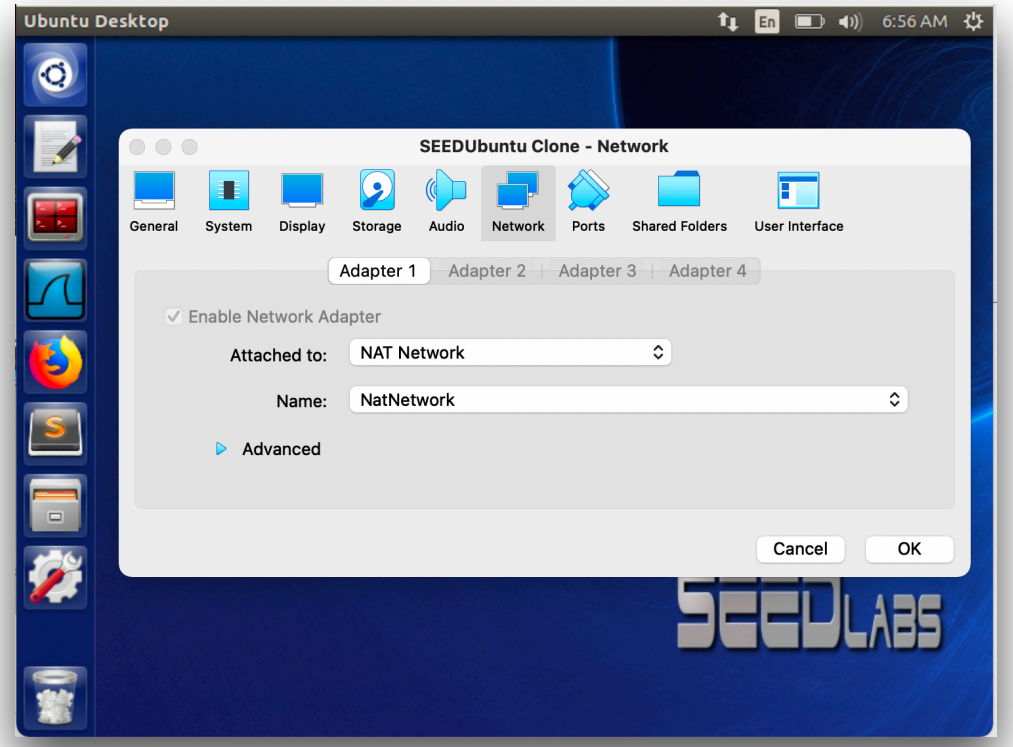
LAB SETUP:

VPN SERVER: 10. 0. 2. 5

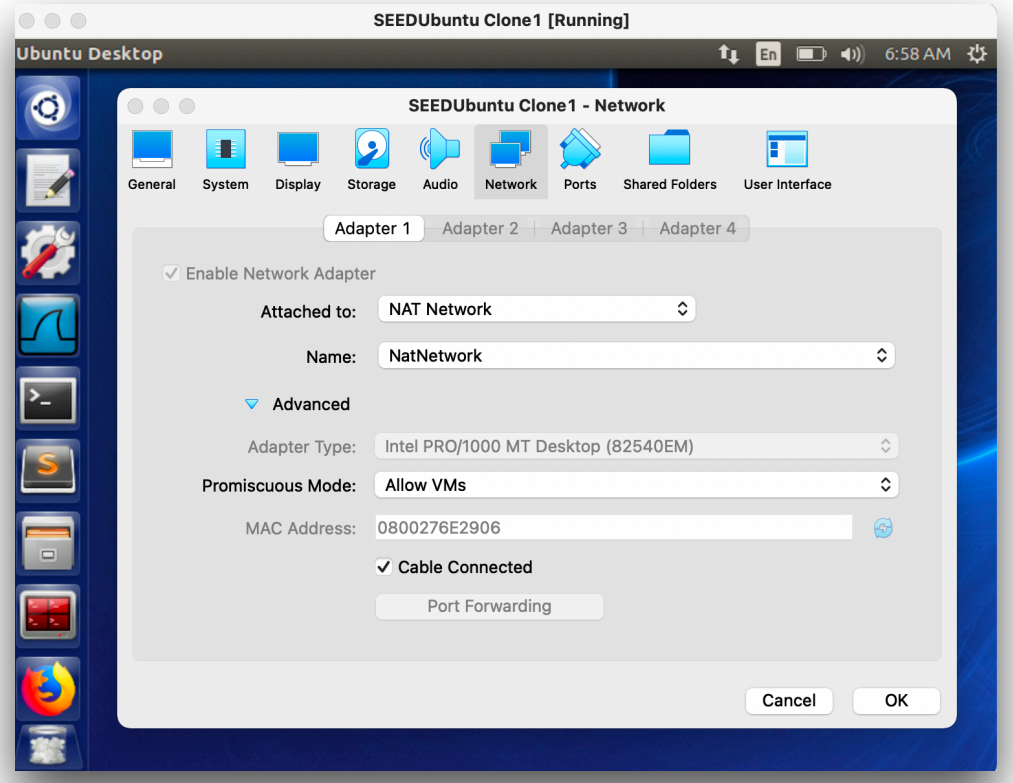
VPN CLIENT: 10. 0. 2. 6

Task 1: VM Setup

Both the VMs need to have the "NAT Network" Adapter enabled on them:



Server machine network configuration



Client machine network configuration

Task 2: Set up Firewall

We have identified '**www.facebook.com**' as a website to be blocked on the client machine. The client machine is inside the firewall.

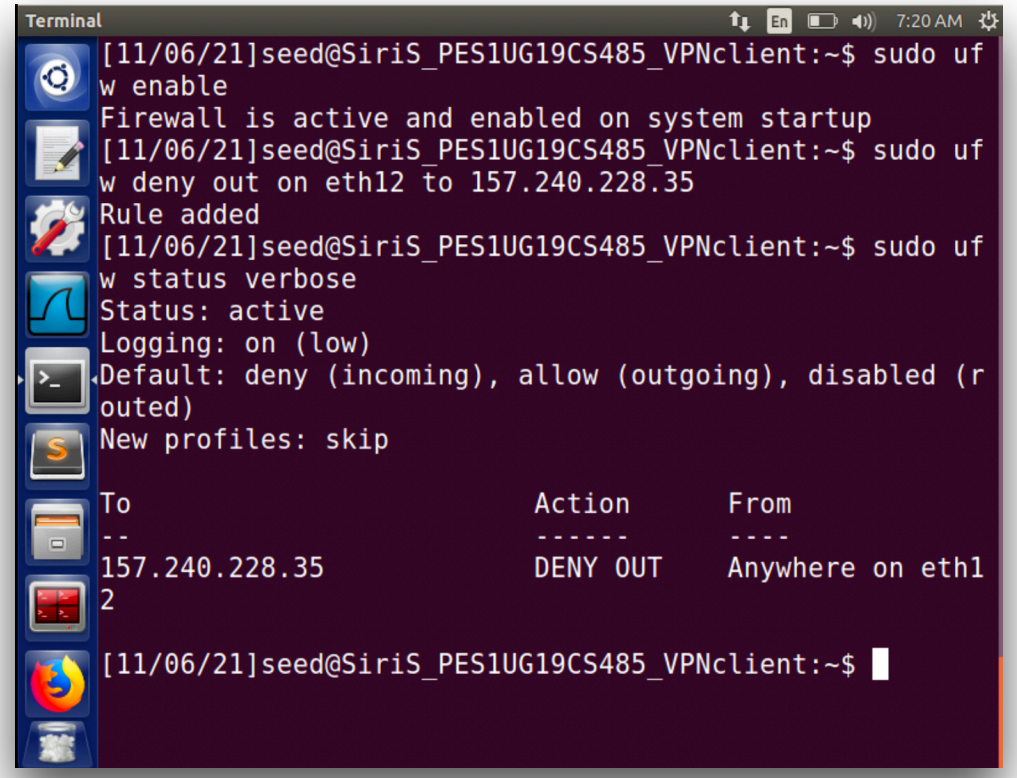
The website is able to be pinged from the client machine:

IP Address: 157. 240. 228. 35

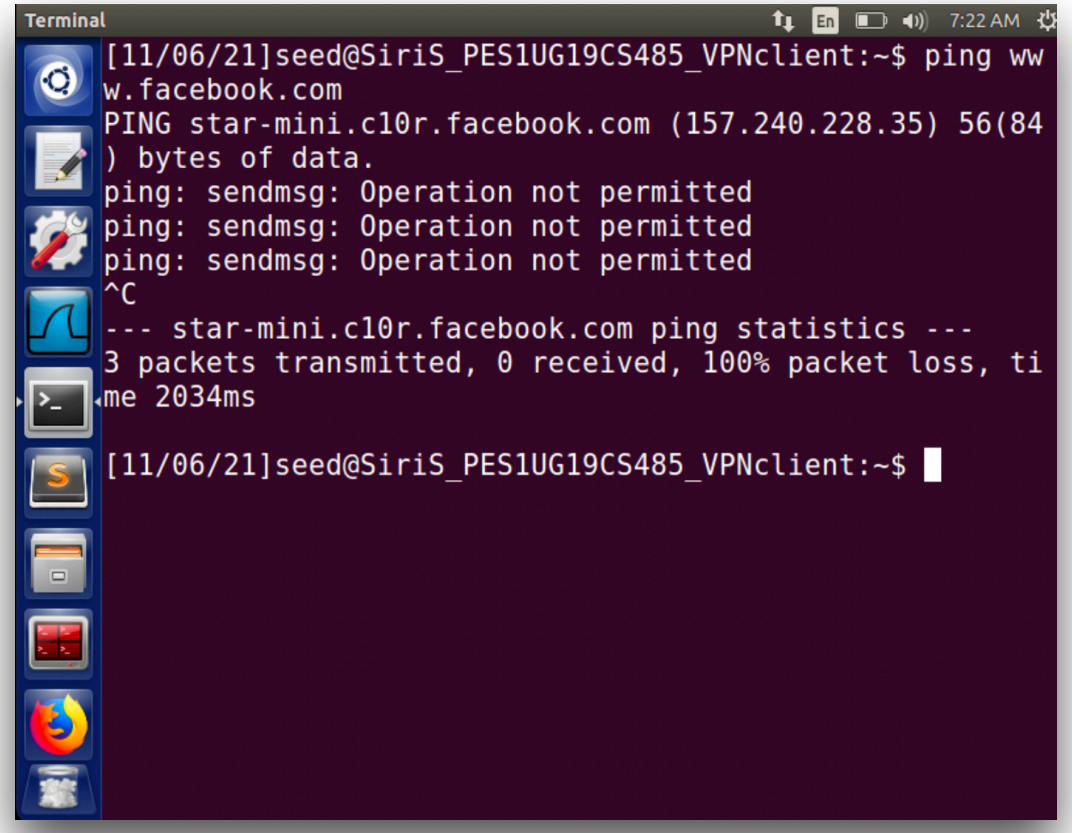
Therefore we can see that Facebook has a fixed IP Address.

Now, we will set up a firewall to block this website from being accessed.

We can see that www.facebook.com is blocked:



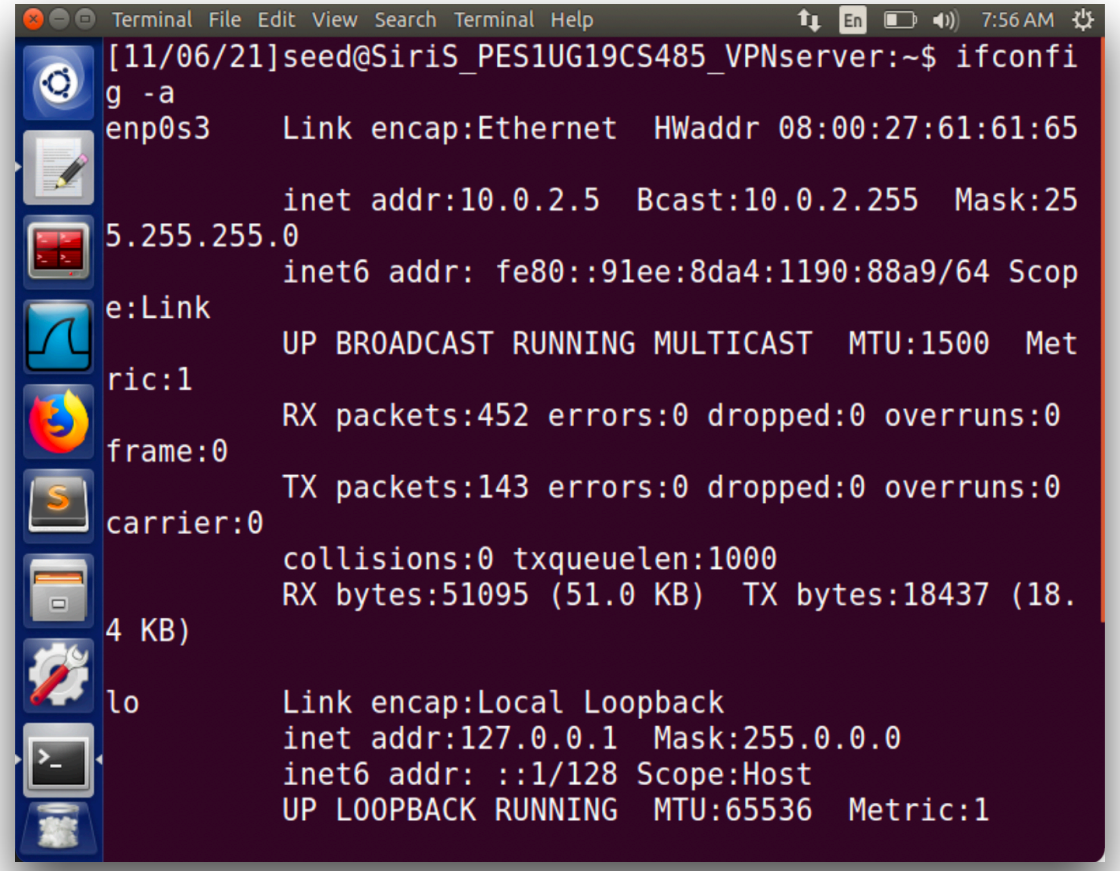
Now, we are unable to ping the website:



Task 3: Bypassing Firewall using VPN

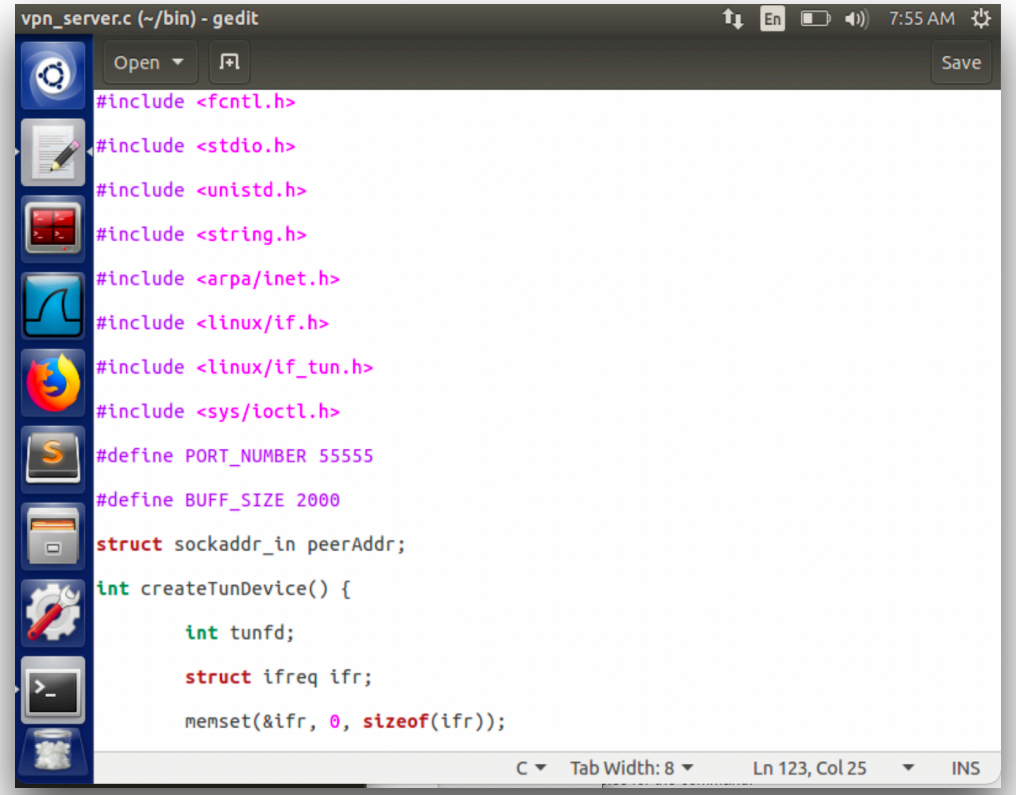
Step 1: Run VPN Server:

Before running the server code we can see that when we run *ifconfig -a*, tun0 (the name of the interface that establishes a VPN tunnel) Is inactive:

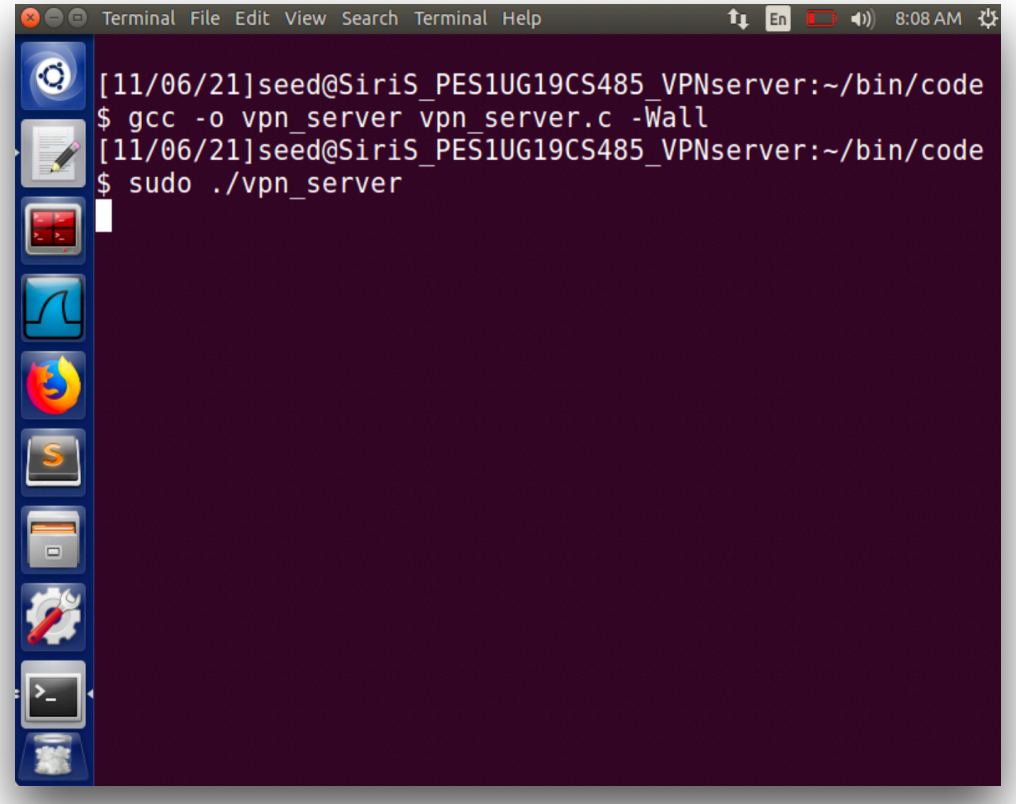


There is no mention of *tun0*.

The code that is run on the server to establish the tunnel:

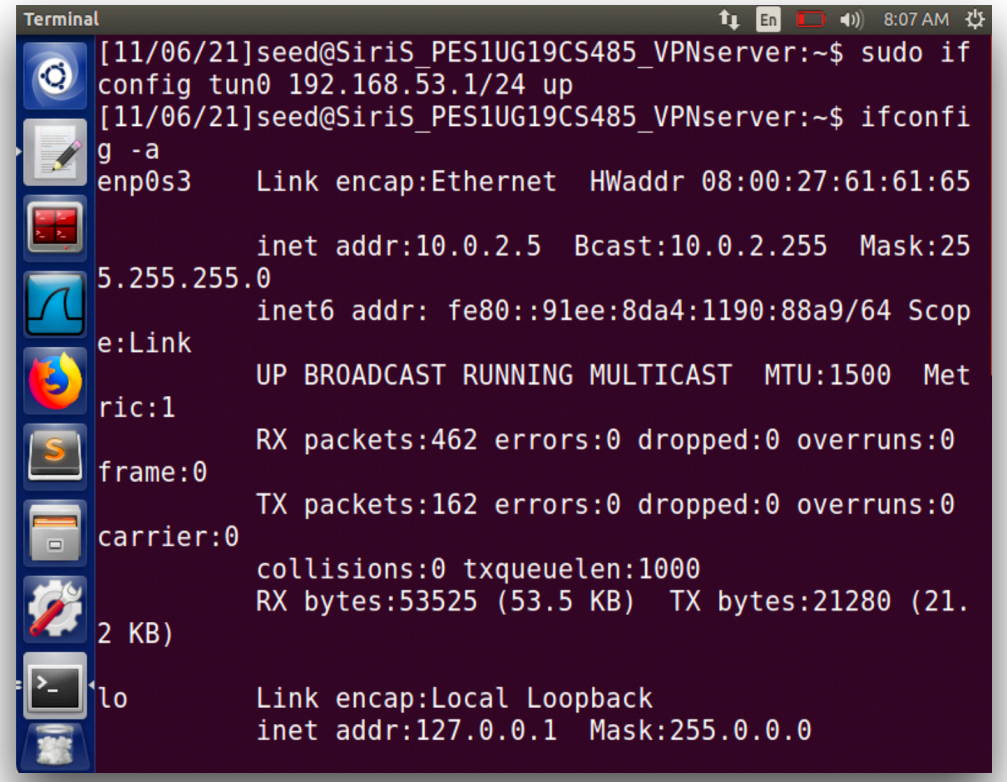


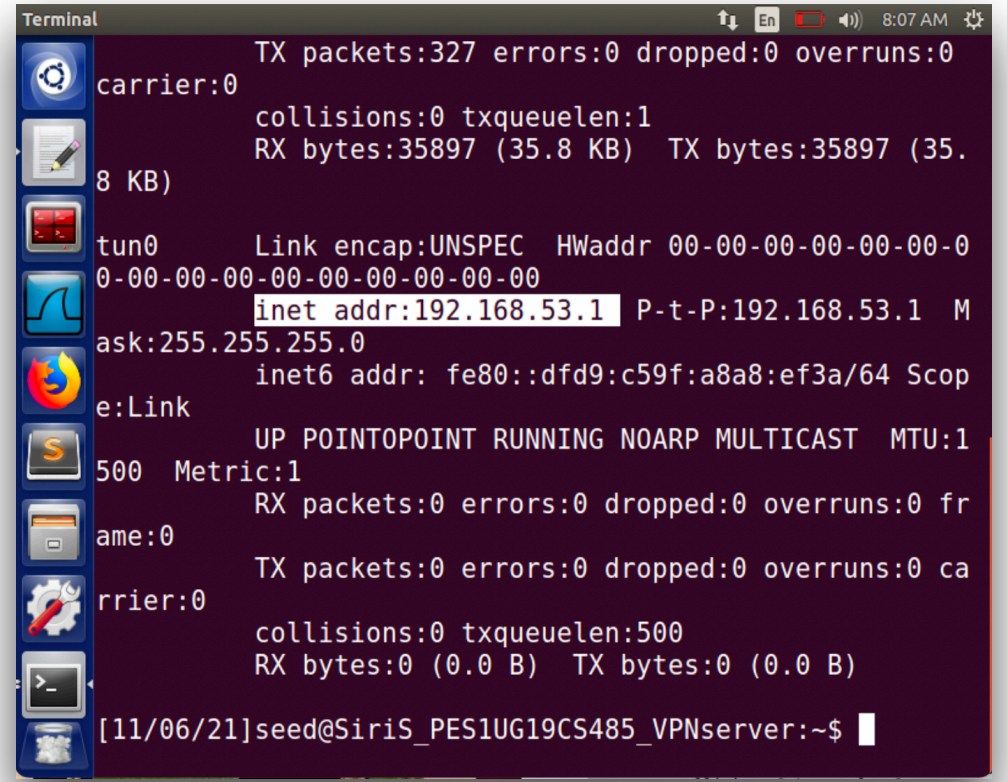
Now, we run the above code:



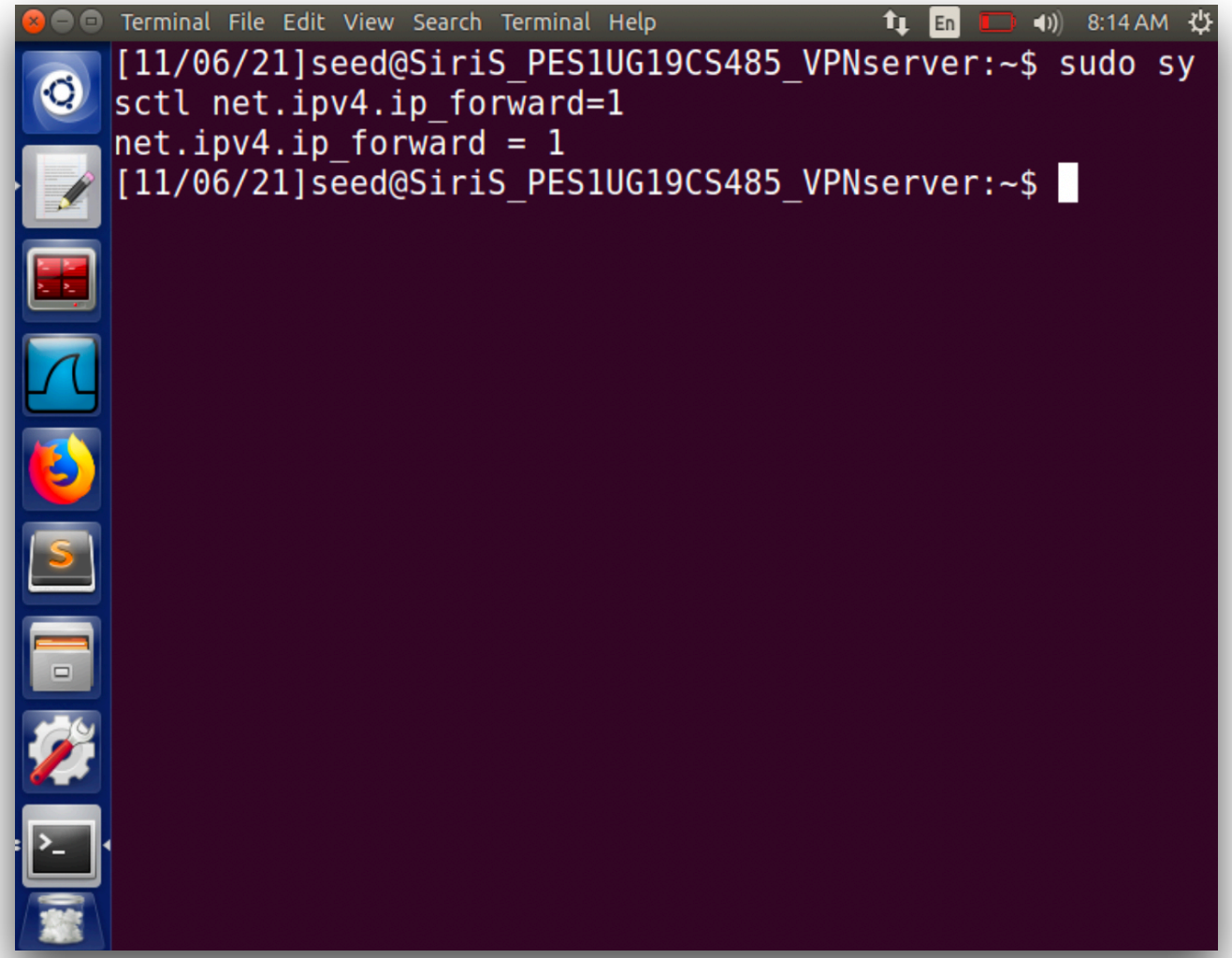
Then we assign an IP address to the tun0 inferface and activate it. IP Address assigned: 192.168.53.1/25

Upon checking ifconfig -a : we have an established tunnel:



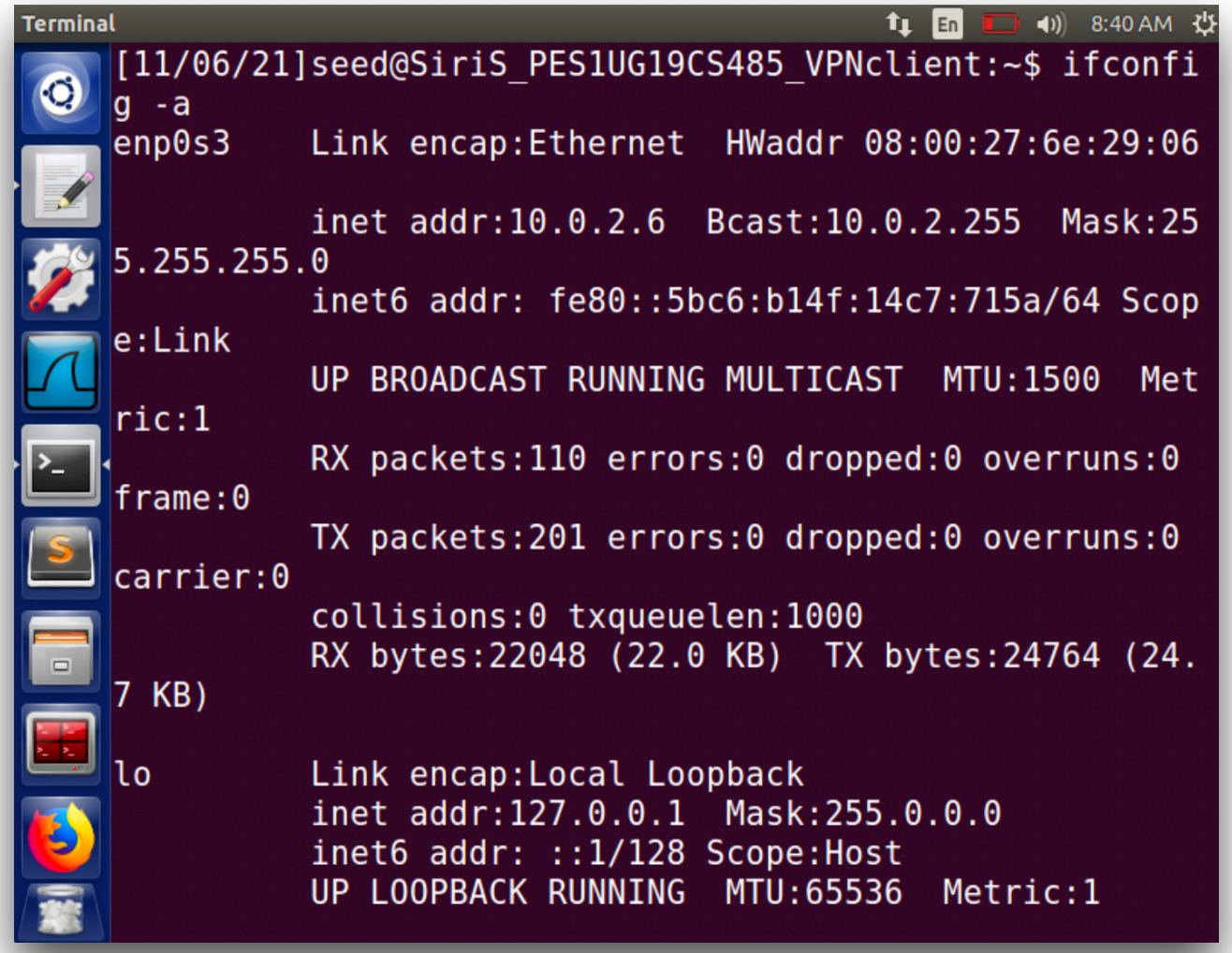


Now the VPN Server needs to forward packets to other destinations, so it needs to function as a gateway. We need to enable the IP forwarding for a computer to behave like a gateway.



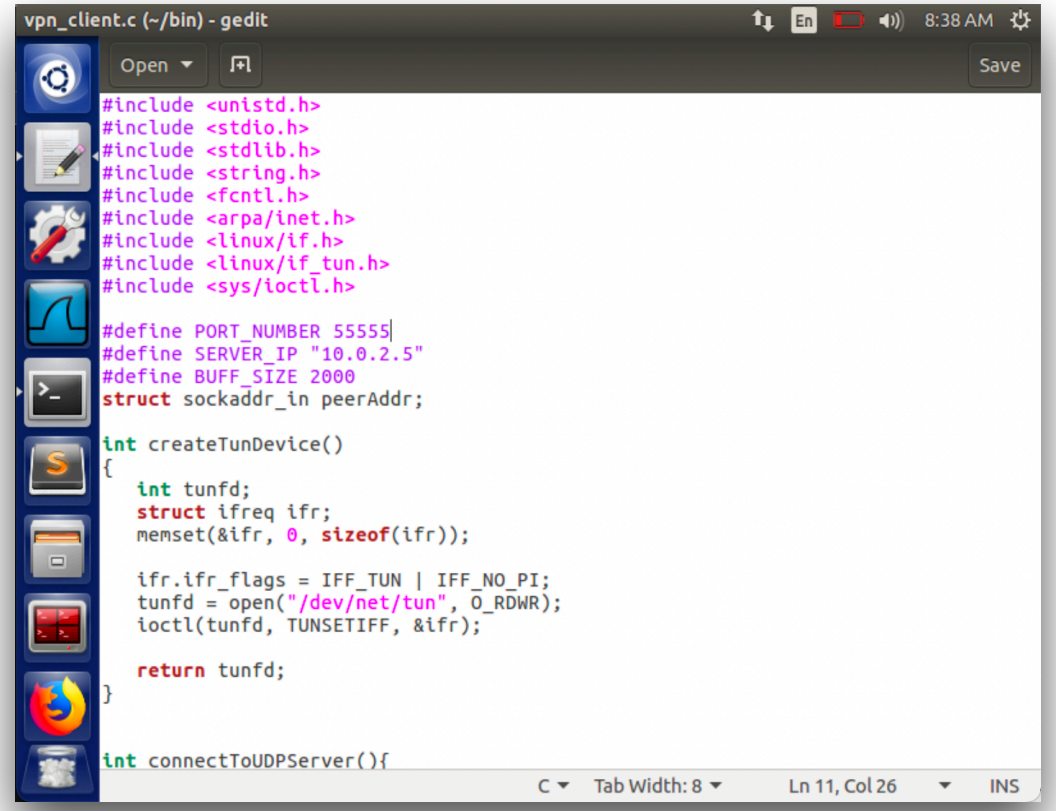
<u>Step 2:</u> Run VPN Client

Before running the client code we can see that when we run *ifconfig -a*, tun0 (the name of the interface that establishes a VPN tunnel) Is inactive:

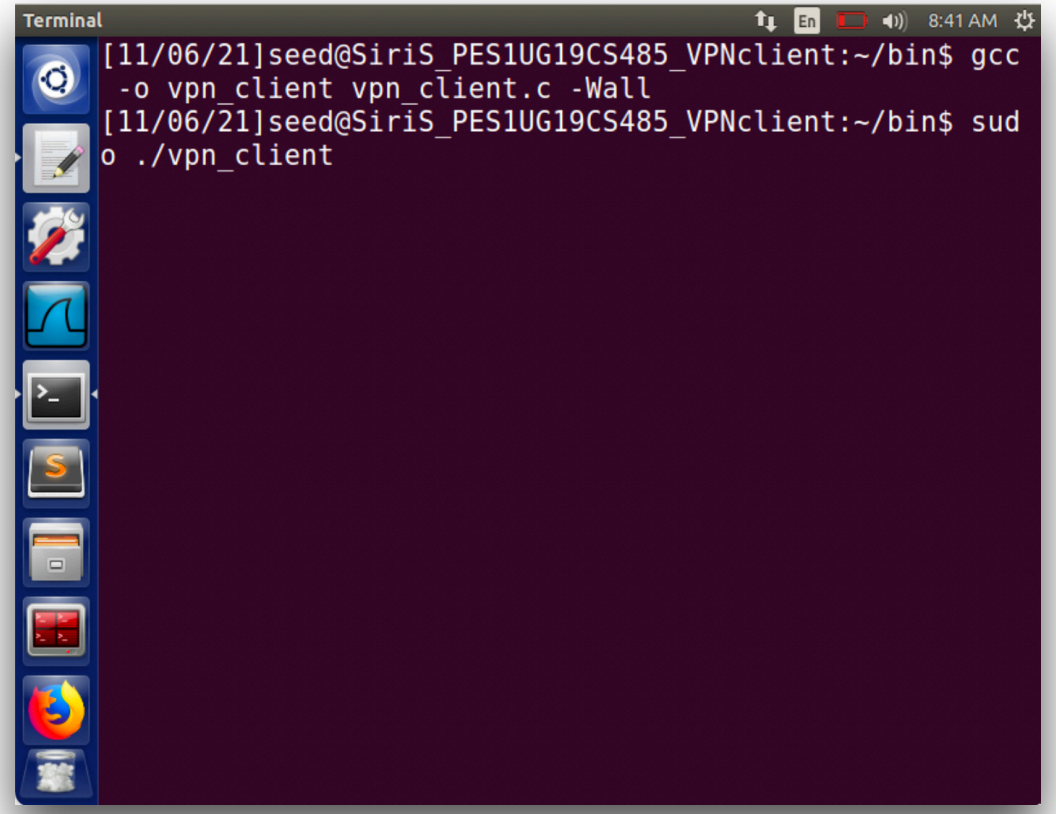


There is no mention of *tun0*.

The code that is run on the server to establish the tunnel:

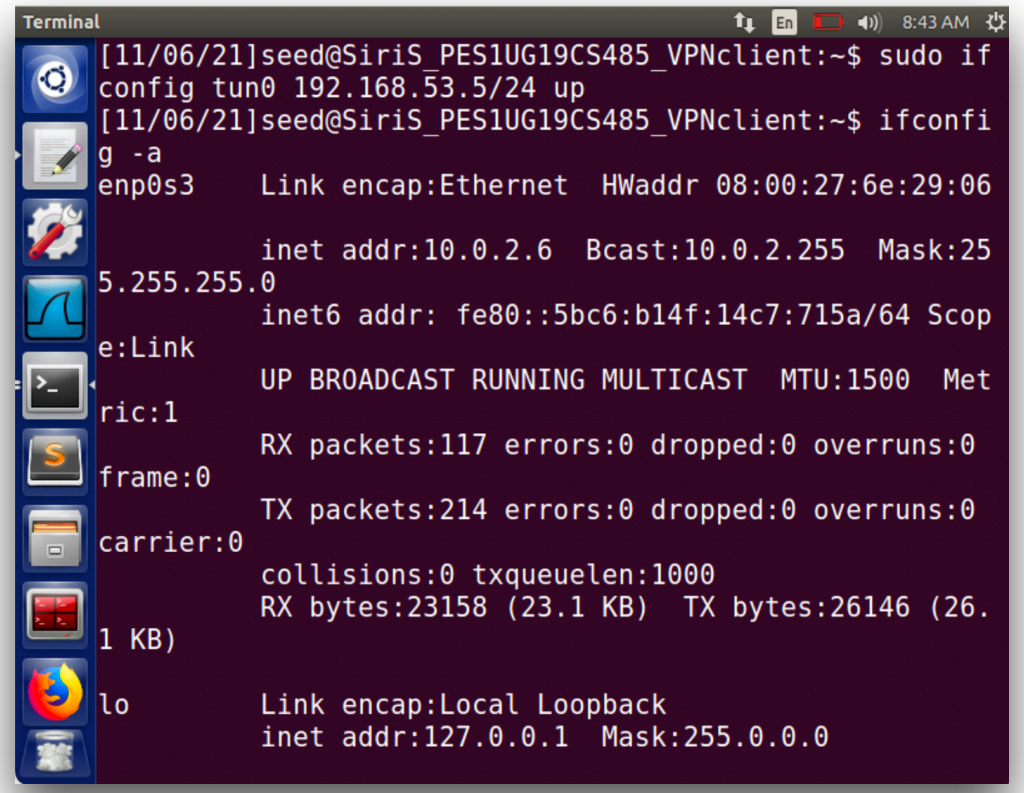


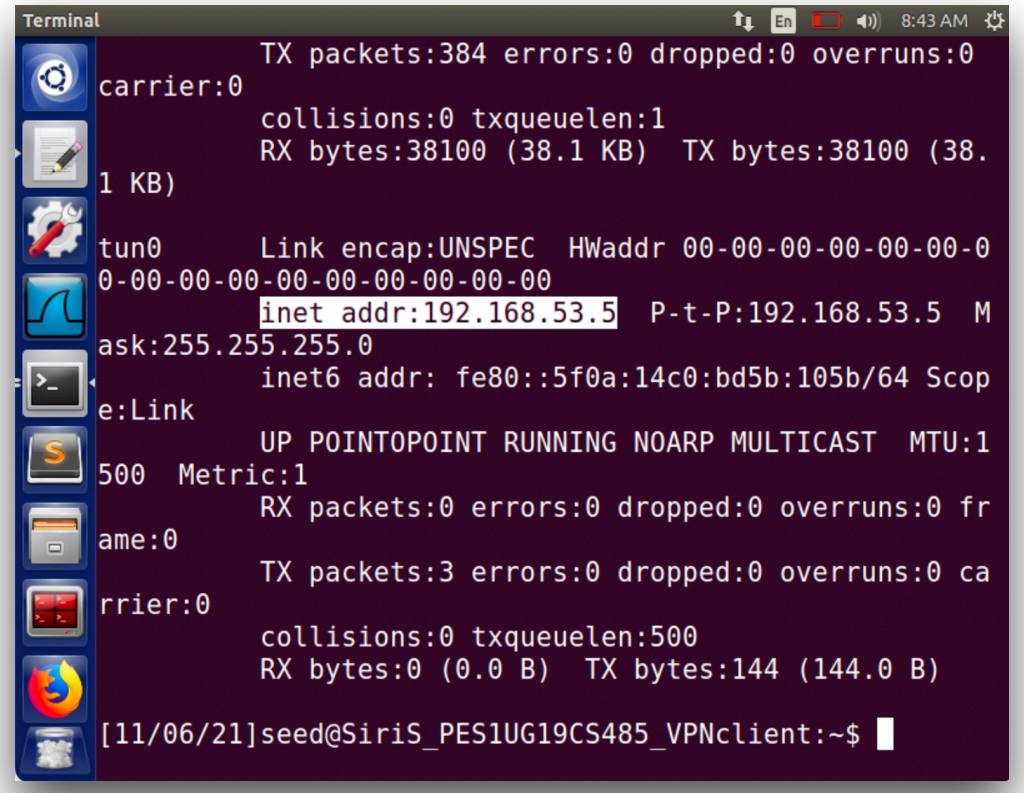
Now, we run the above code:



Then we assign an IP address to the tun0 inferface and activate it. IP Address assigned: 192.168.53.1/25

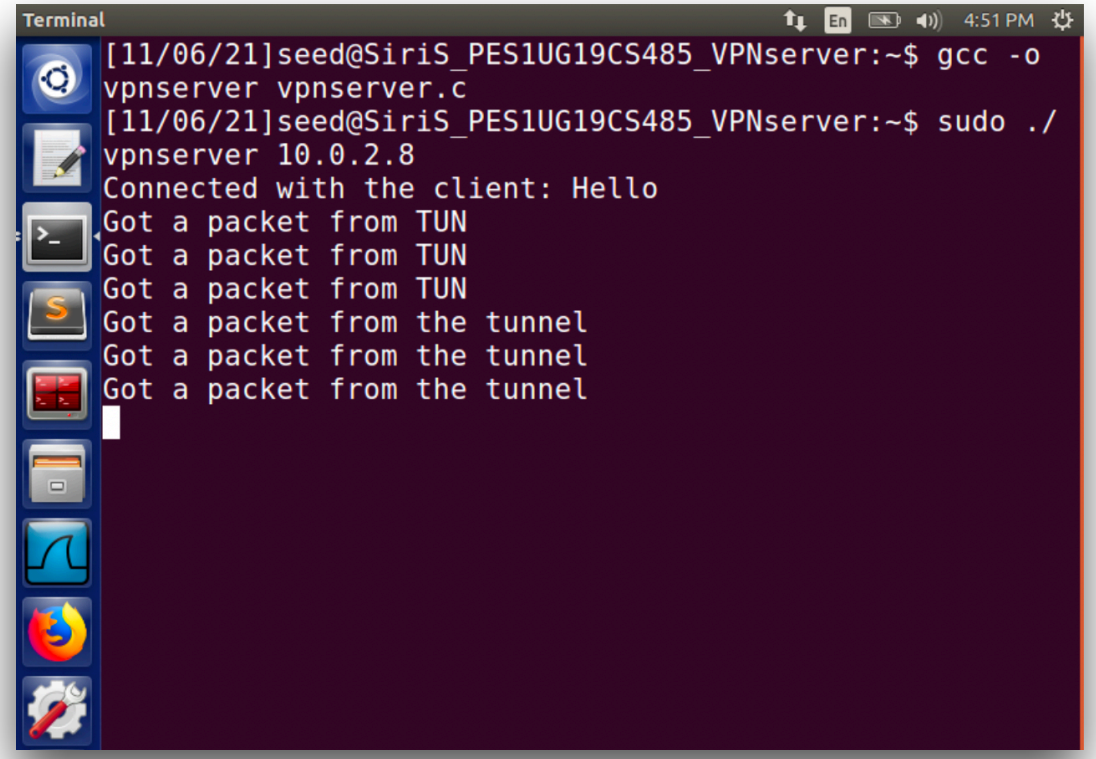
Upon checking ifconfig -a : we have an established tunnel:

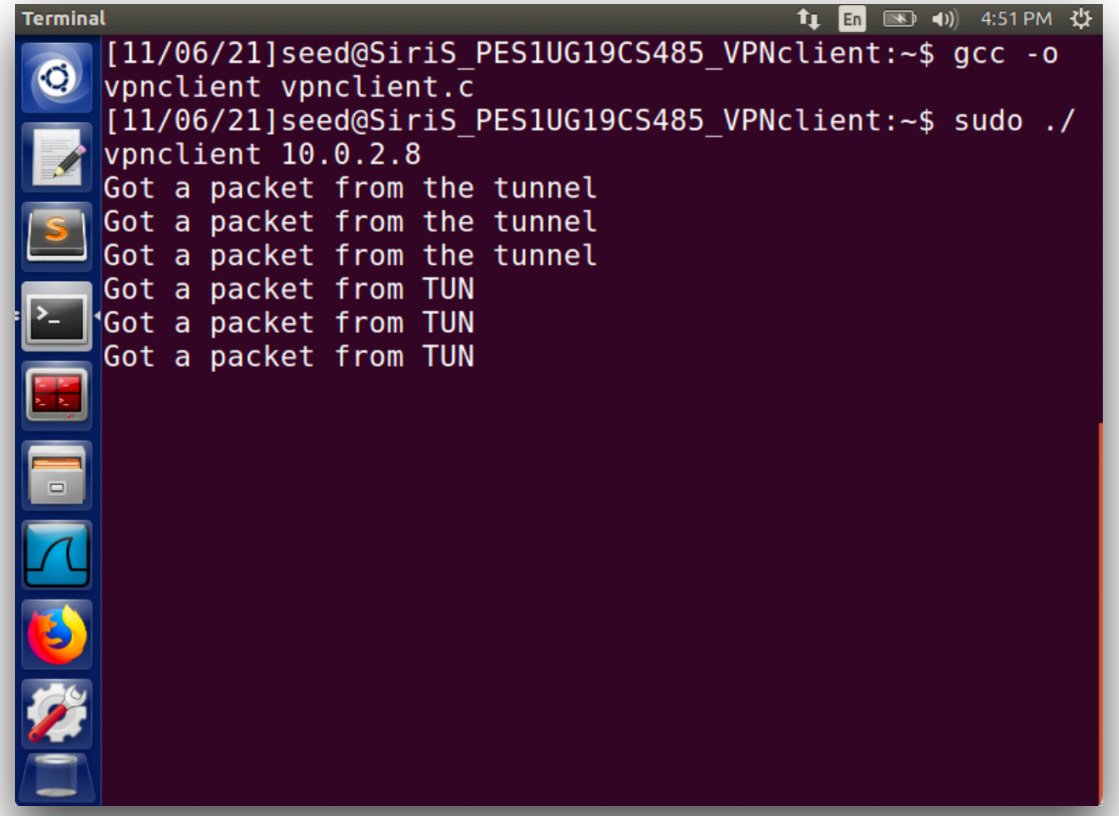




<u>Step 3:</u> Set Up Routing on Client and Server VMs

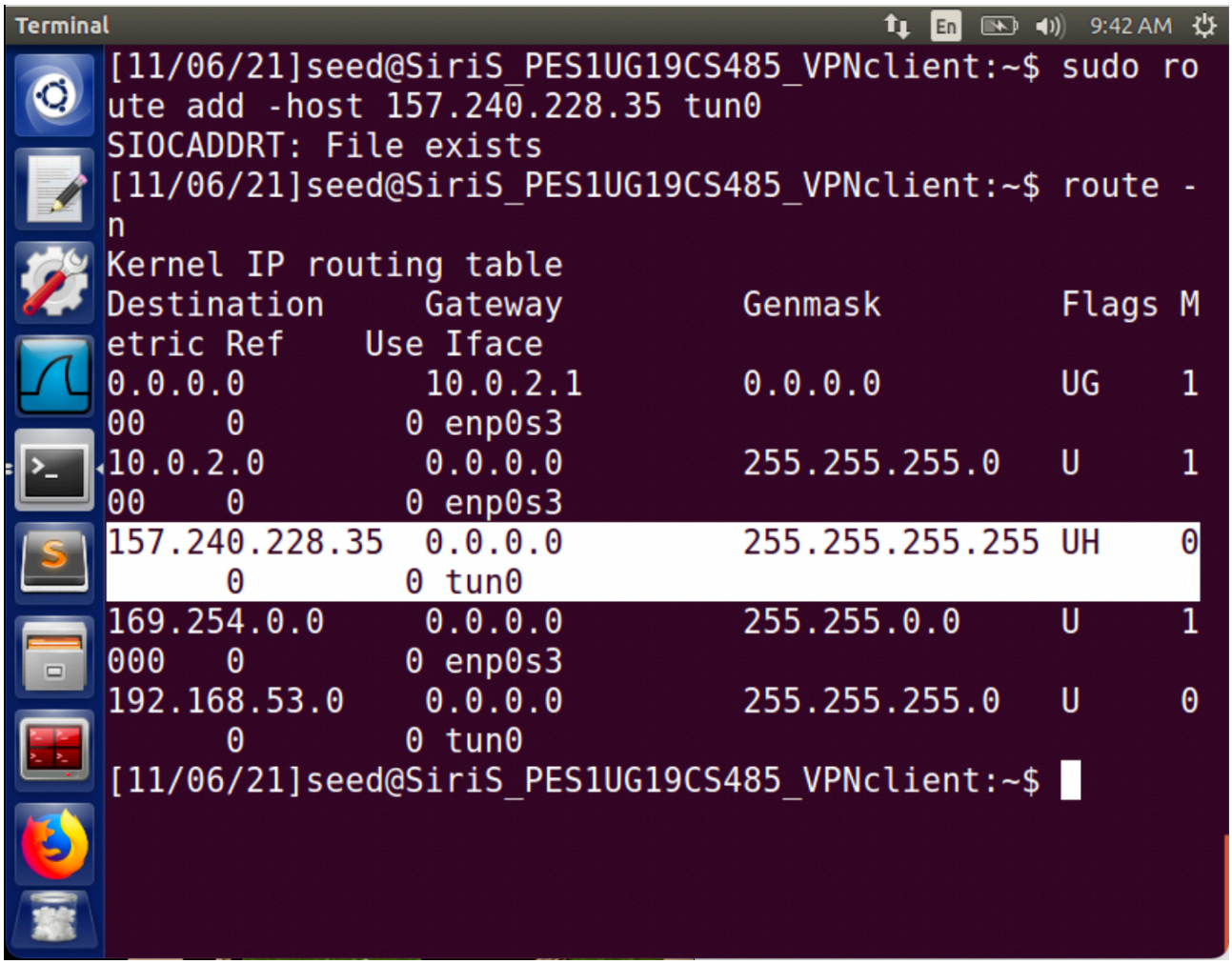
We can now see that the tunnel is established because of the messages displayed like '**Connected with client: Hello**':





We need to set up routing paths on both client and server machines to direct the intended traffic through the tunnel. This is done on the client machine as follows:

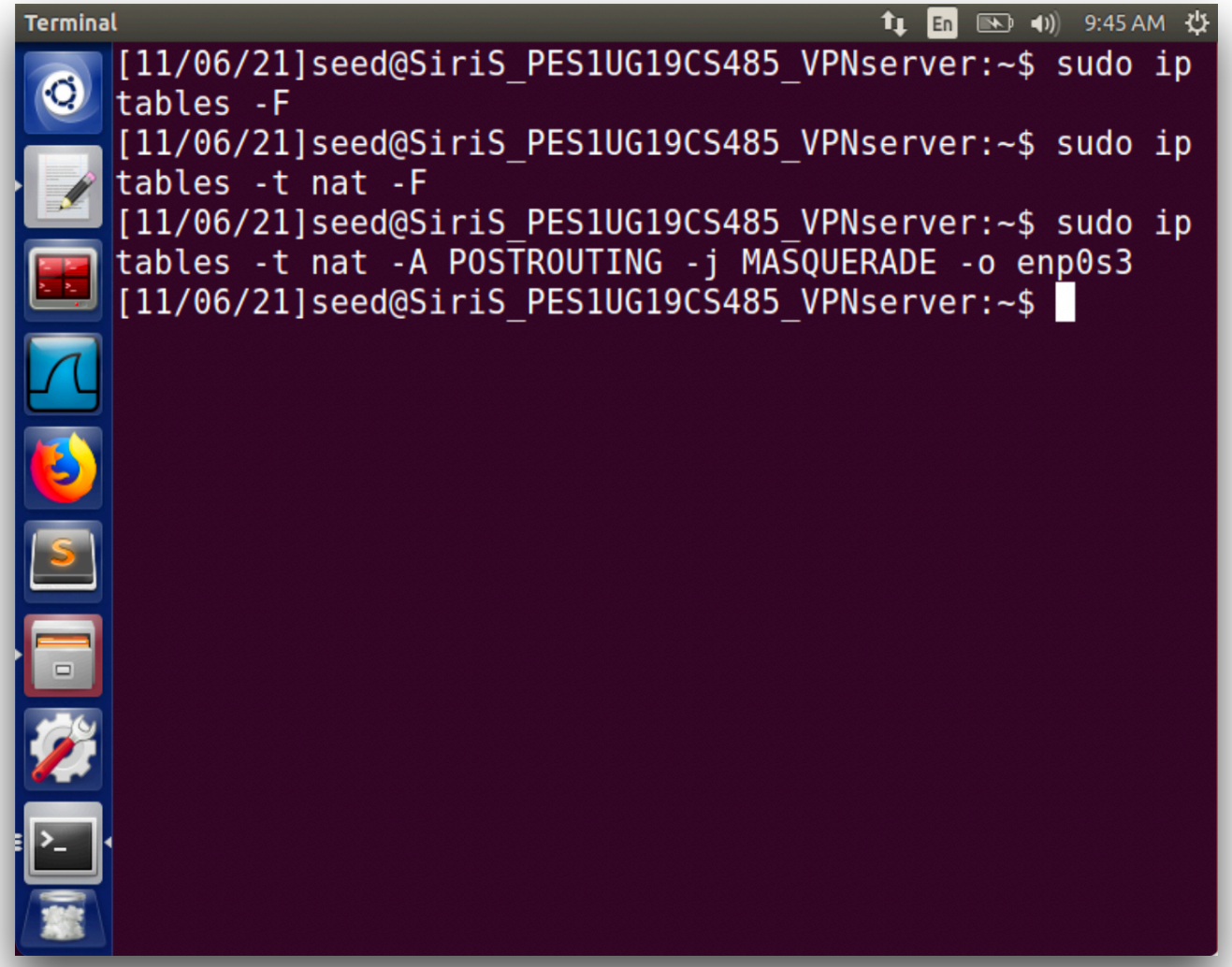
IP Address of Facebook: 157.240.228.35



This ensures that all the packets from the IP address 157.240.228.0/24 (facebook's IP) will be routed to tun0 interface.

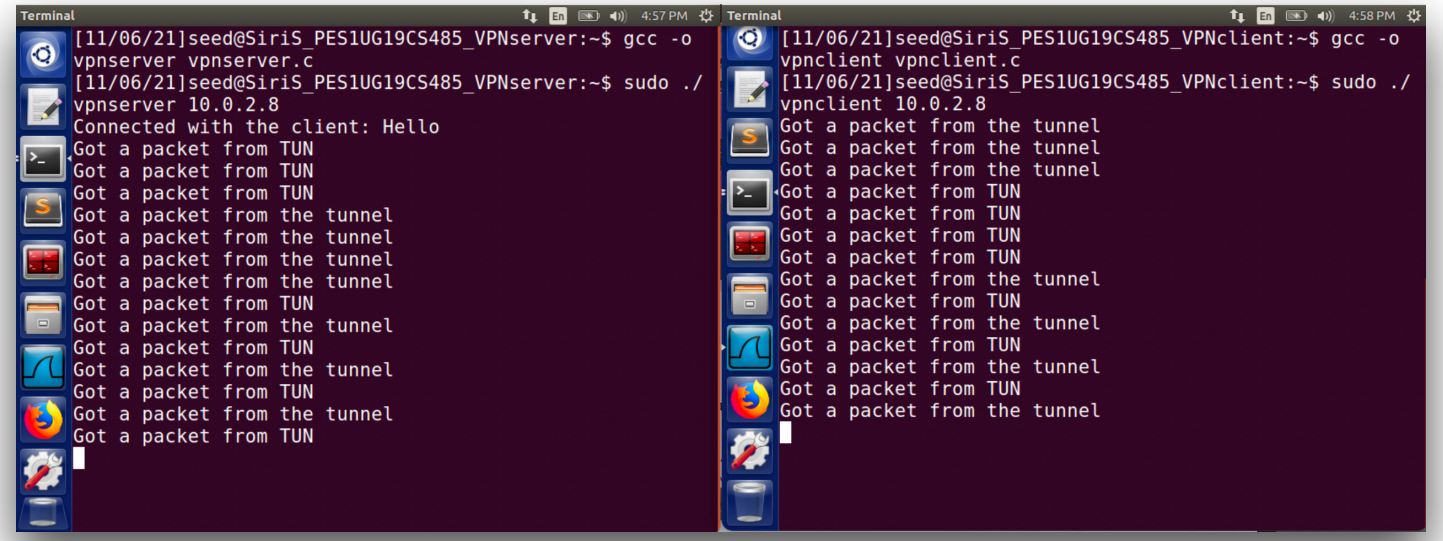
Step 4: Set Up NAT on Server VM

We make NAT to believe that the MAC address of 192.168.53.5 is the VPN server's MAC address. The following commands can enable the NAT on the Server VM:

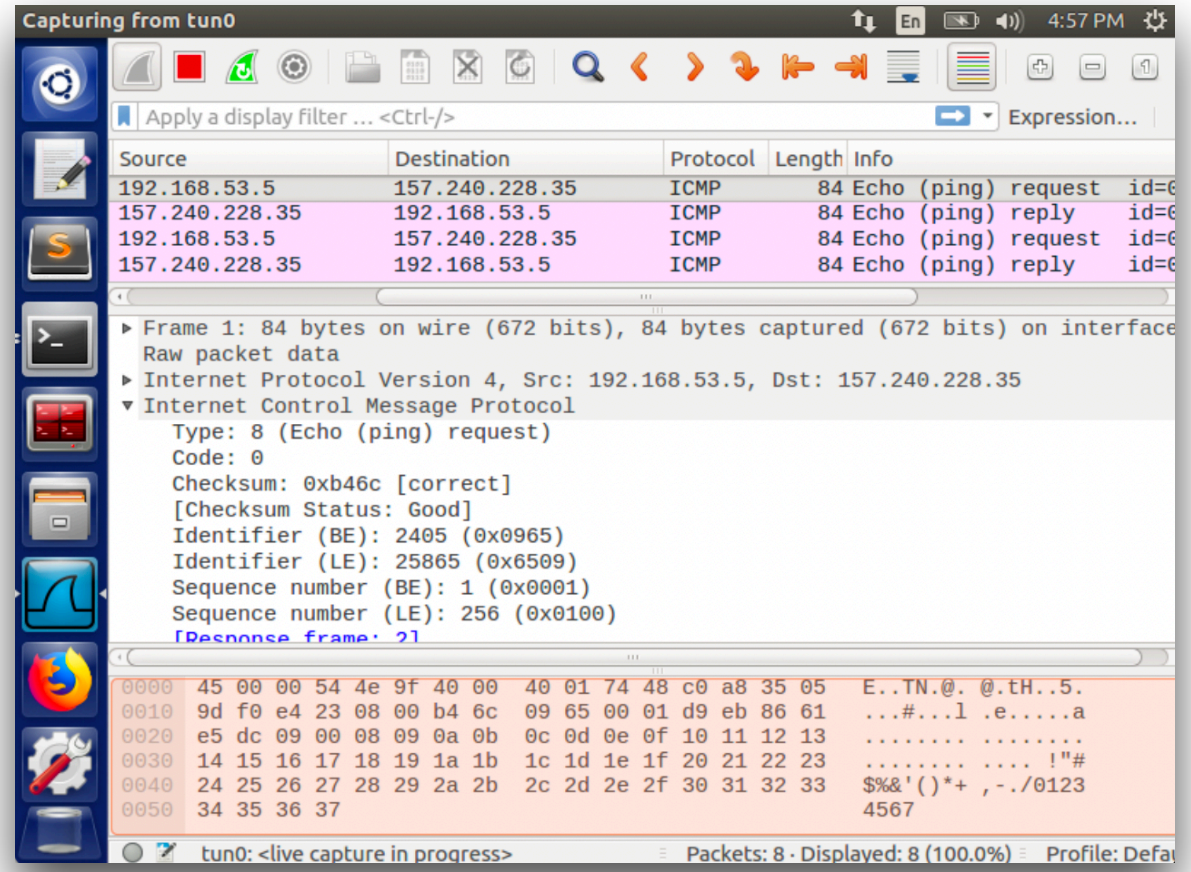


Task 4: Demonstration

Client machine can now access facebook.com through the tunnel established. We can try ping command. Therefore the task has been completed successfully.



Wireshark screenshot that explains the route traversed by the packet:



We can observe that the ICMP request packet from tunnel interface (192.168.53.5) is created to facebook's IP(157.240.228.35), the tunnel writes the packet to the UDP socket which sends the packet to server machine.(10.0.2.5). The ping reply is received back on tun0 interface.Hence, ping works bypassing firewall through the created tunnel.