Tanmay Fadnavis

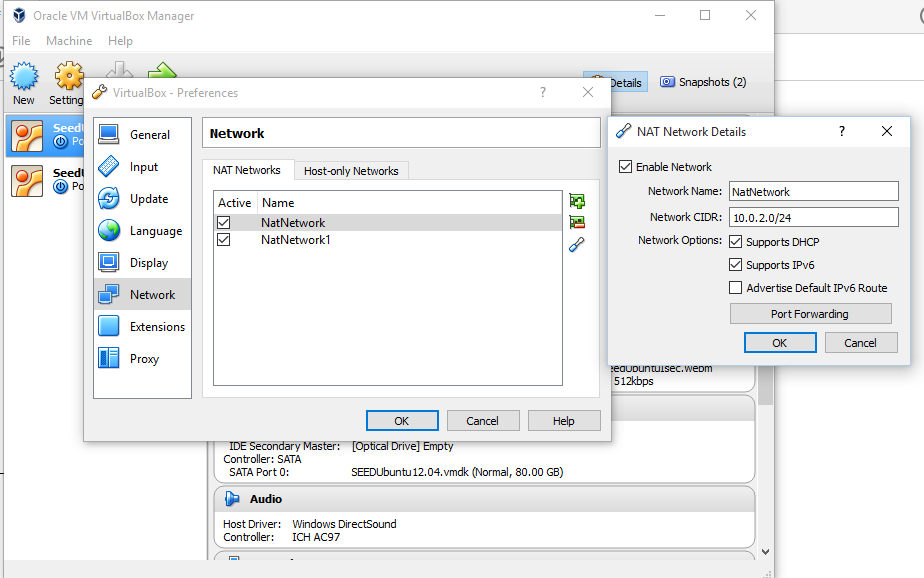
SUID: 971141760

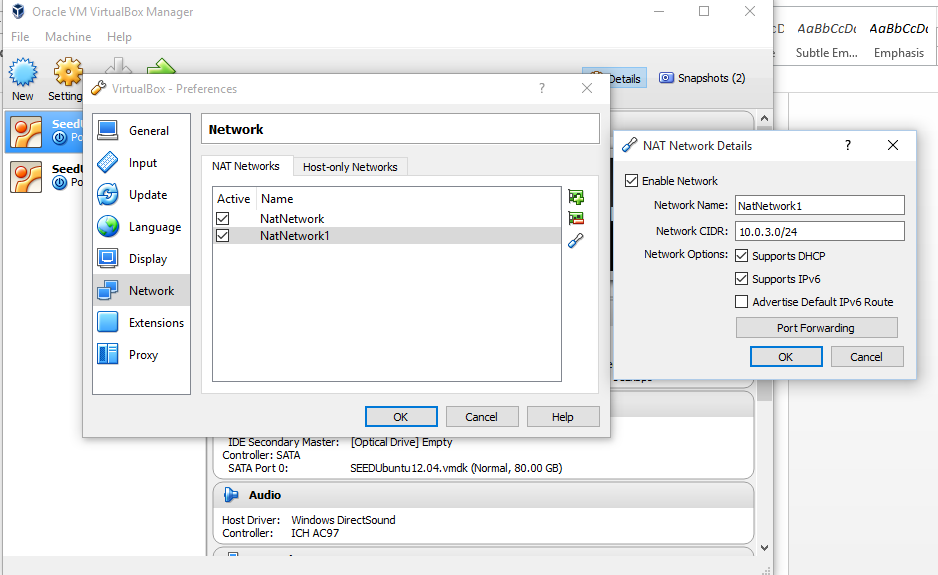
INTERNET Security

Lab - 3

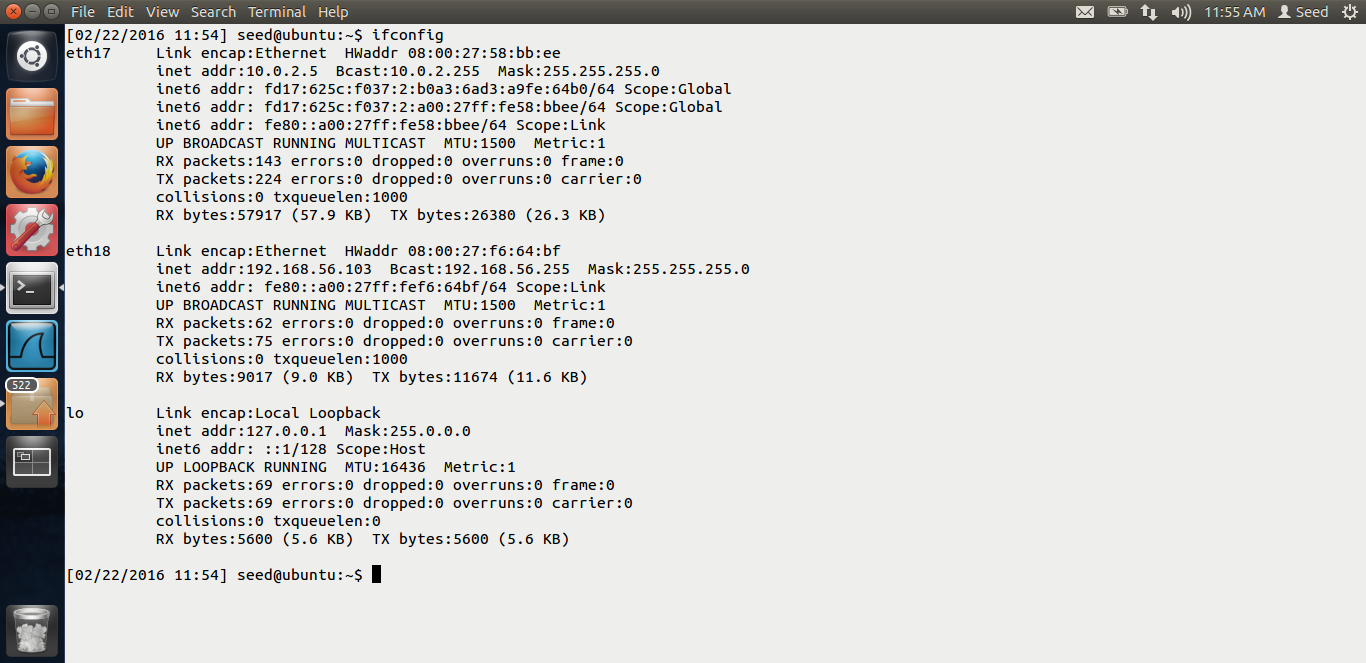
# LAB ENVIRONMENT

Below are the screen shots for lab environment setup.

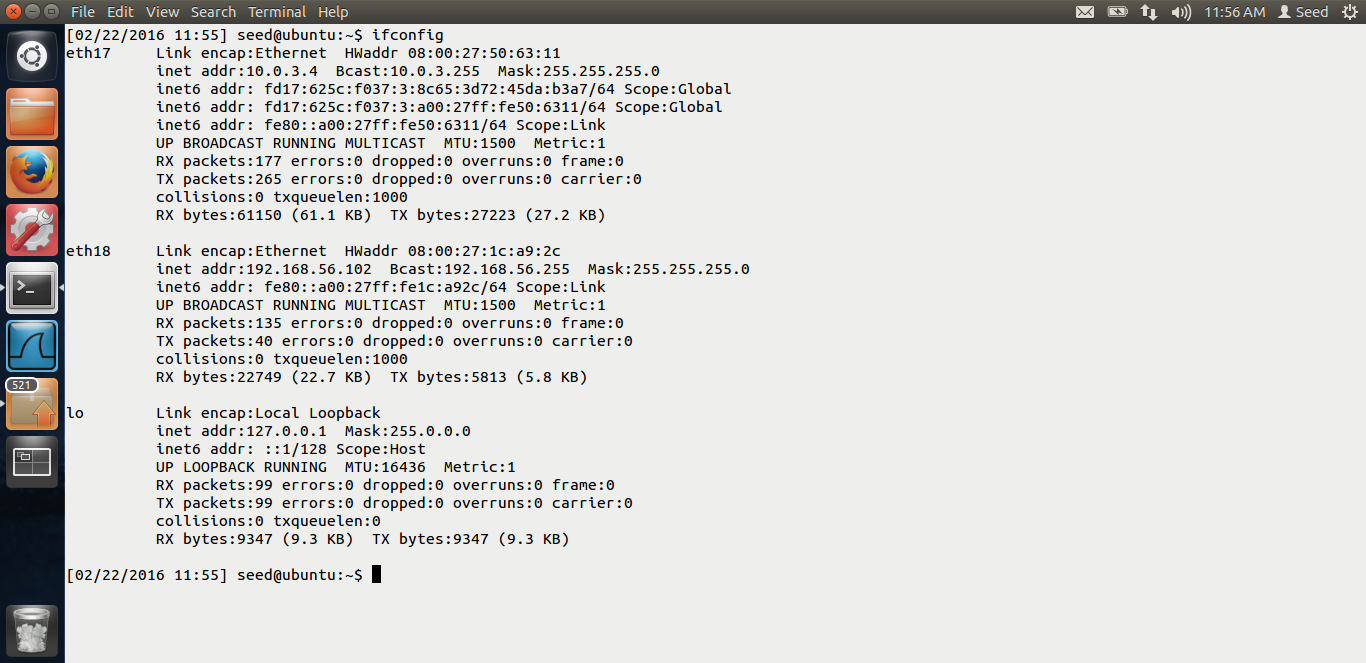




You can see in the above screen shots, I have set-up two NAT networks and a host only network.



Above is the screen shot for my original VM, The ip address is 10.0.2.5 and the host-network ip is 192.168.56.103 I am using my original VM as the VM behind the firewall. I will use this as the VPN client.

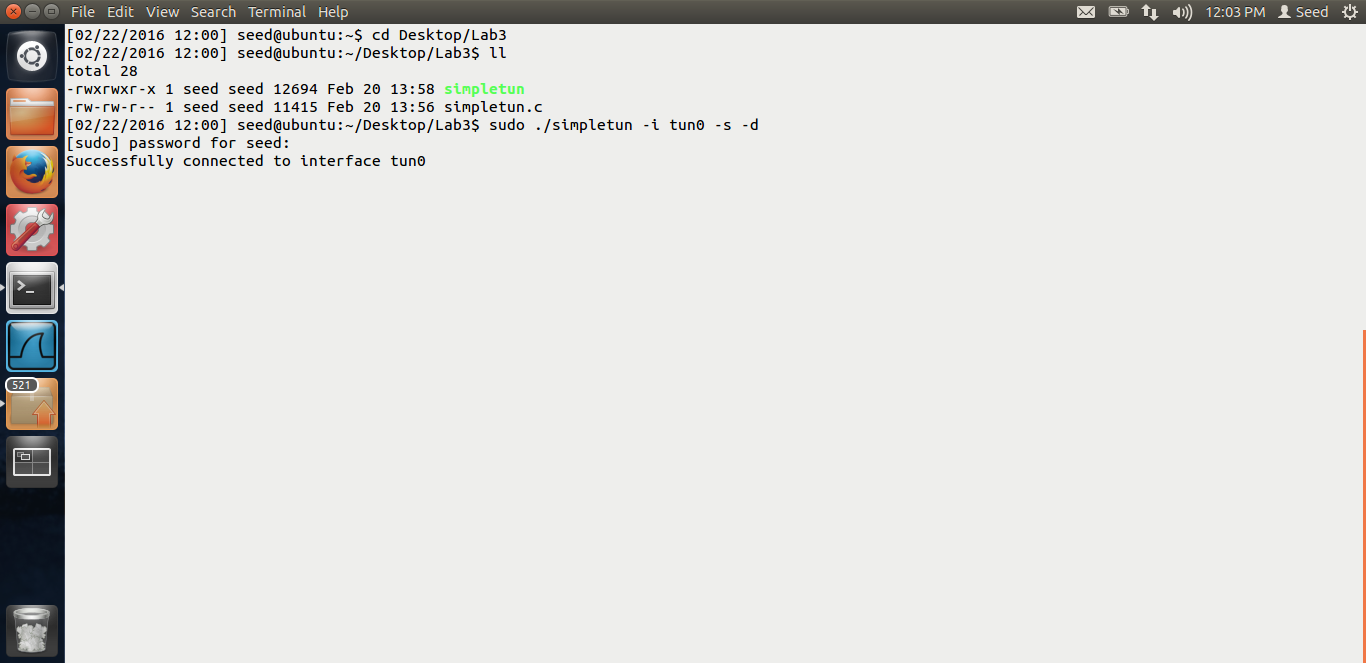


This is the screen shot for my clone VM. The ip is 10.0.3.4 The host network IP is 192.168.56.102 I will be using this clone VM as my VPN server.

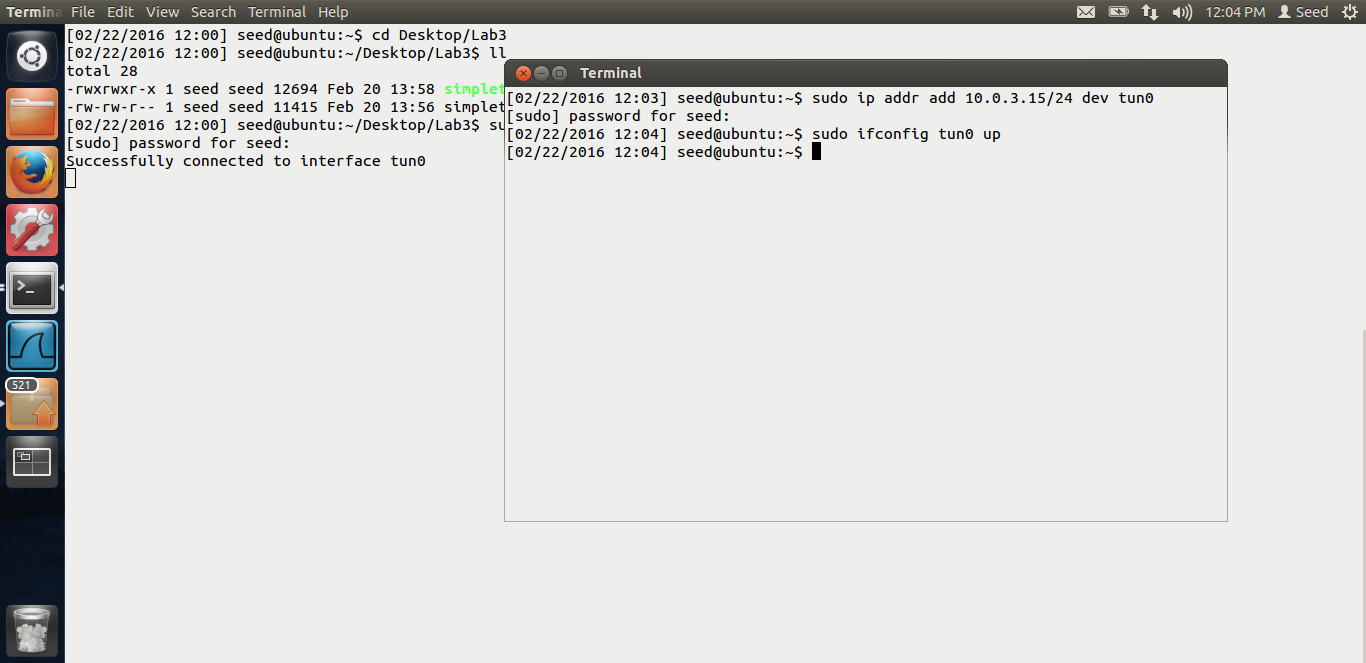
# TASK 1: HOST TO HOST TUNNEL USING TUN/TAP

I have downloaded the simpleton program and compiled it.

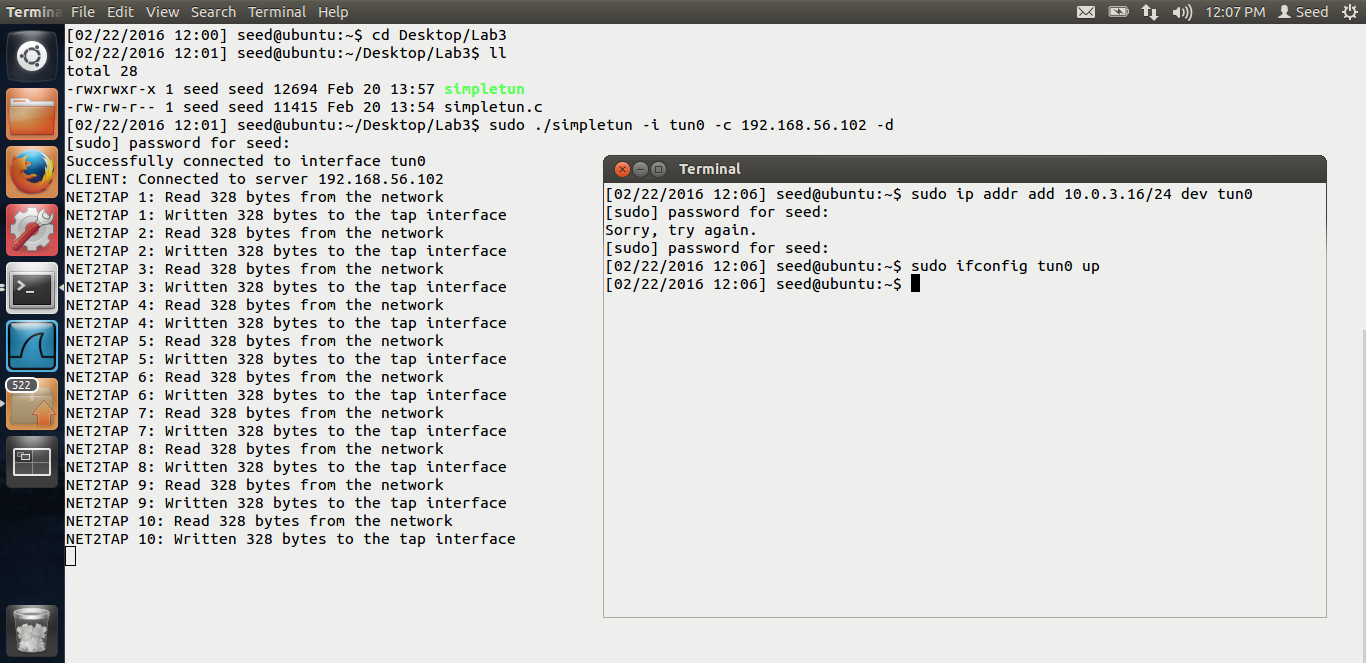
The screen shots for task-1 are below.



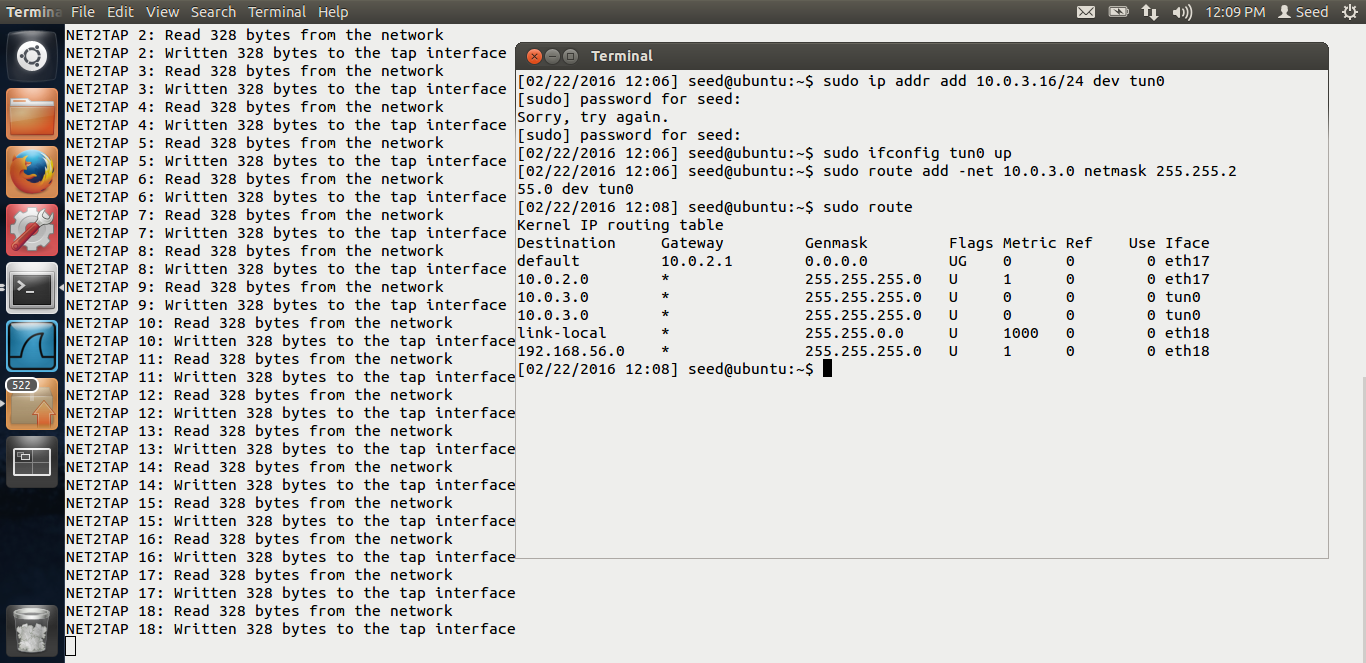
Above is the screen shot for the tuntap server. I am running this on my VM clone.



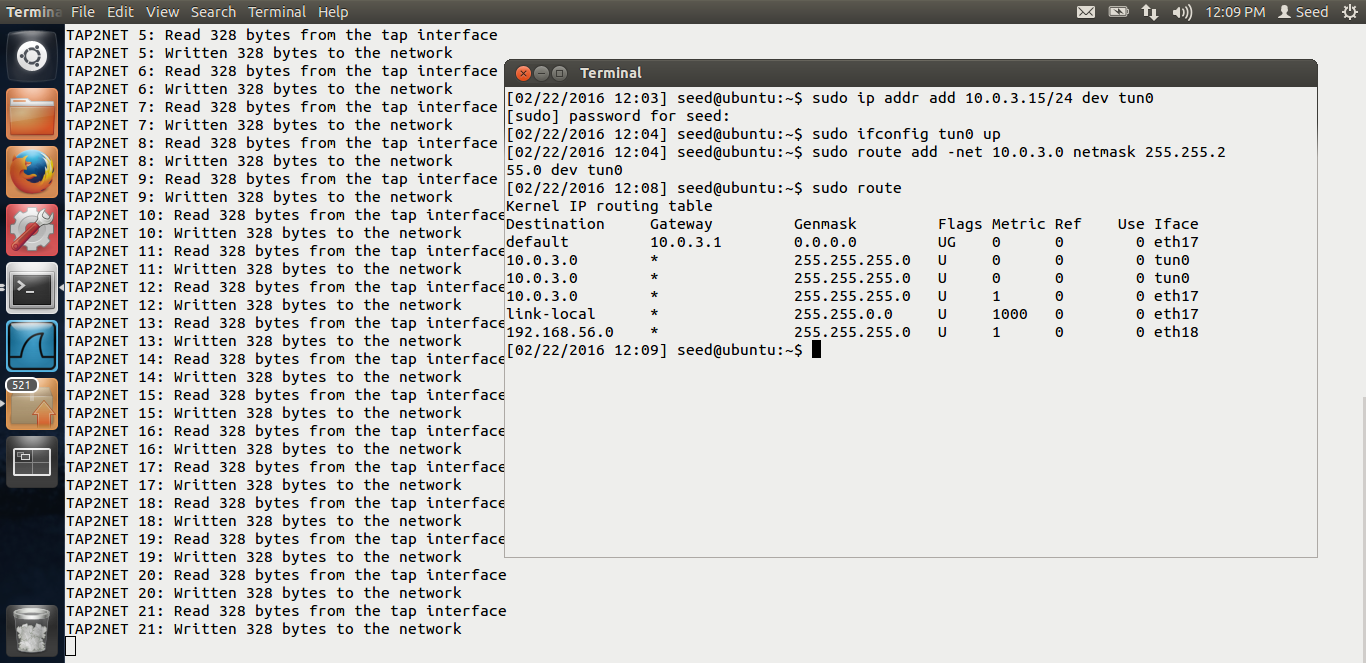
Above is the screen shot for the tun/tap server. I am giving the interface ip as 10.0.3.15 and running the commands in the lab.



Above is the screen shot for my client, my original vm. The tun interface ip I am giving as 10.0.3.16

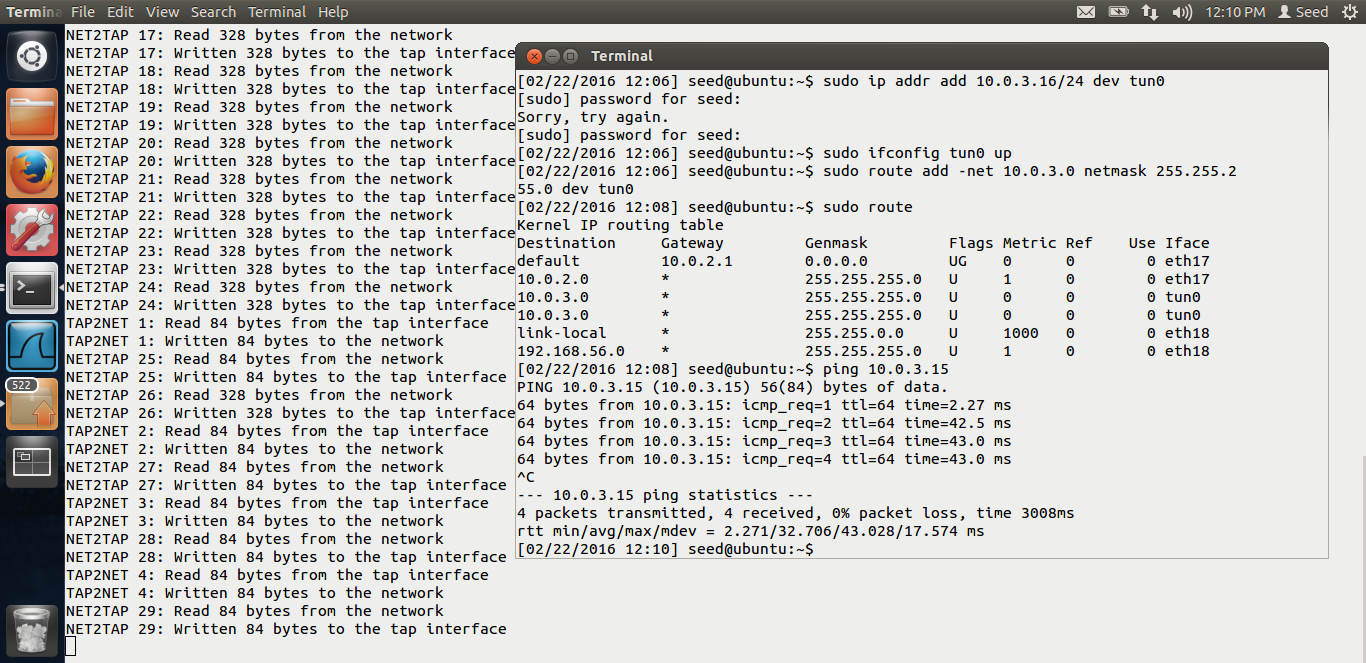


Above is the screen shot for my routing table after the interface has been set-up This is the route table for my original VM.



Above is the route table for my clone VM. After the tunnel has been set-up.

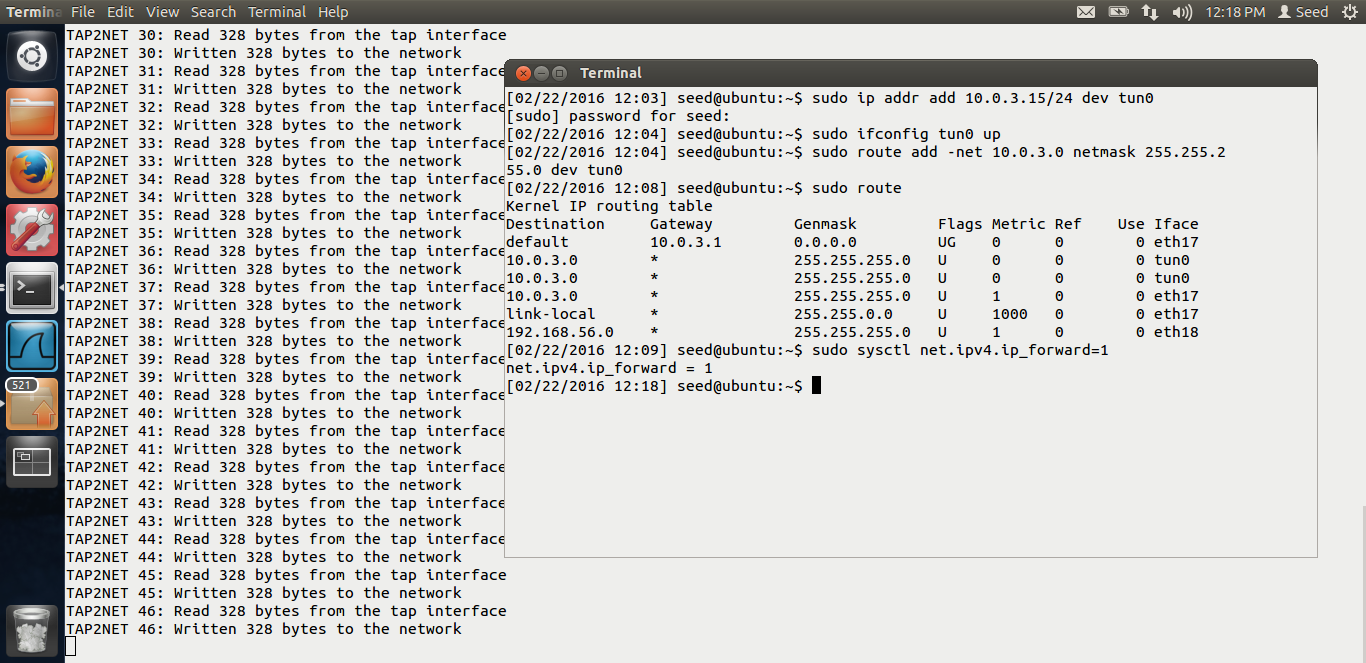
Thus the tunnel has been set-up. Let us ping and check if the tunnel works.



I am pinging my clone from my original vm. In the screen shot, you can see that the tunnel has been successfully set-up as my ping works. Thus host to host tunnel has been set-up.

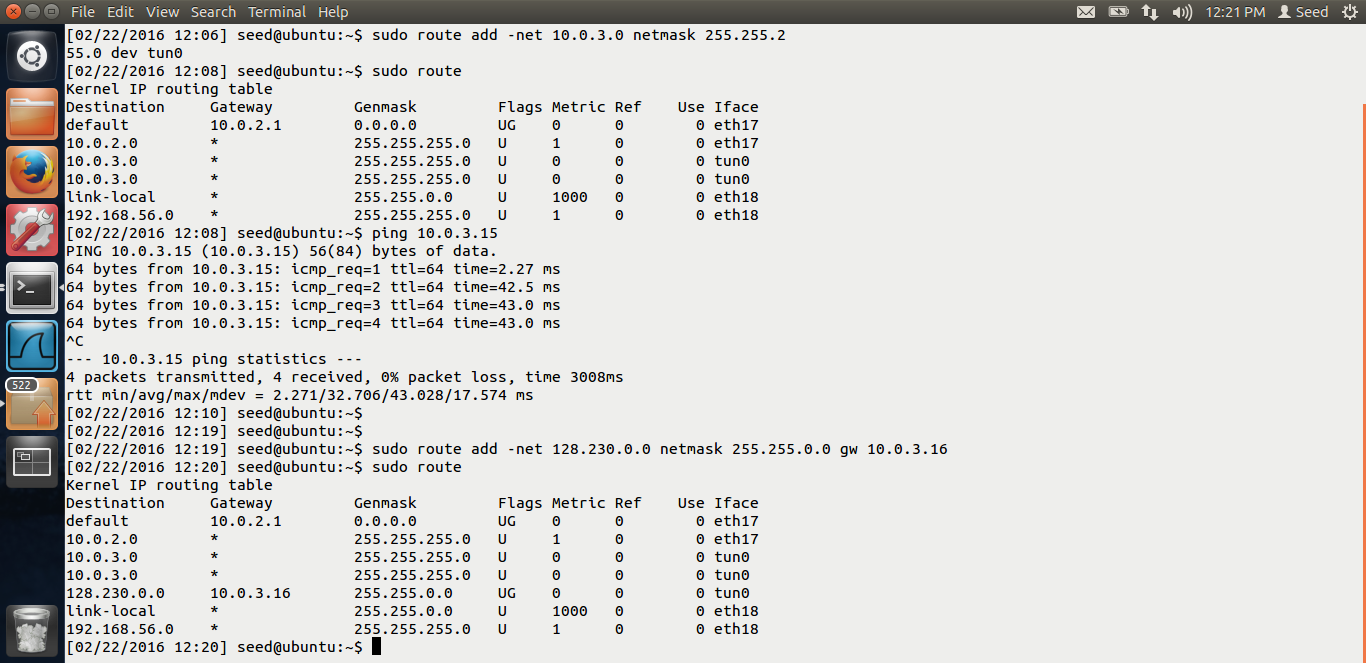
# TASK 2: HOST TO GATEWAY TUNNEL

The screen shots for task2 are below.

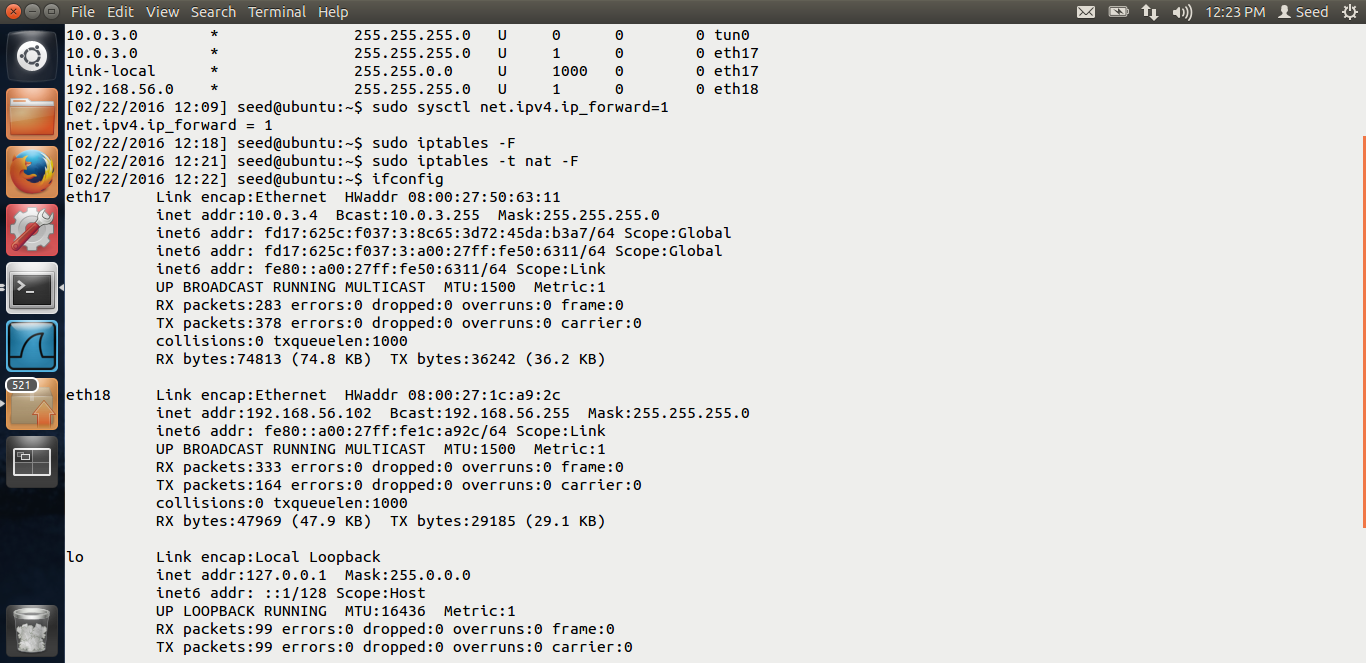


In the above screen shot, we can see that on my clone vm, I have enabled the ip forwarding.

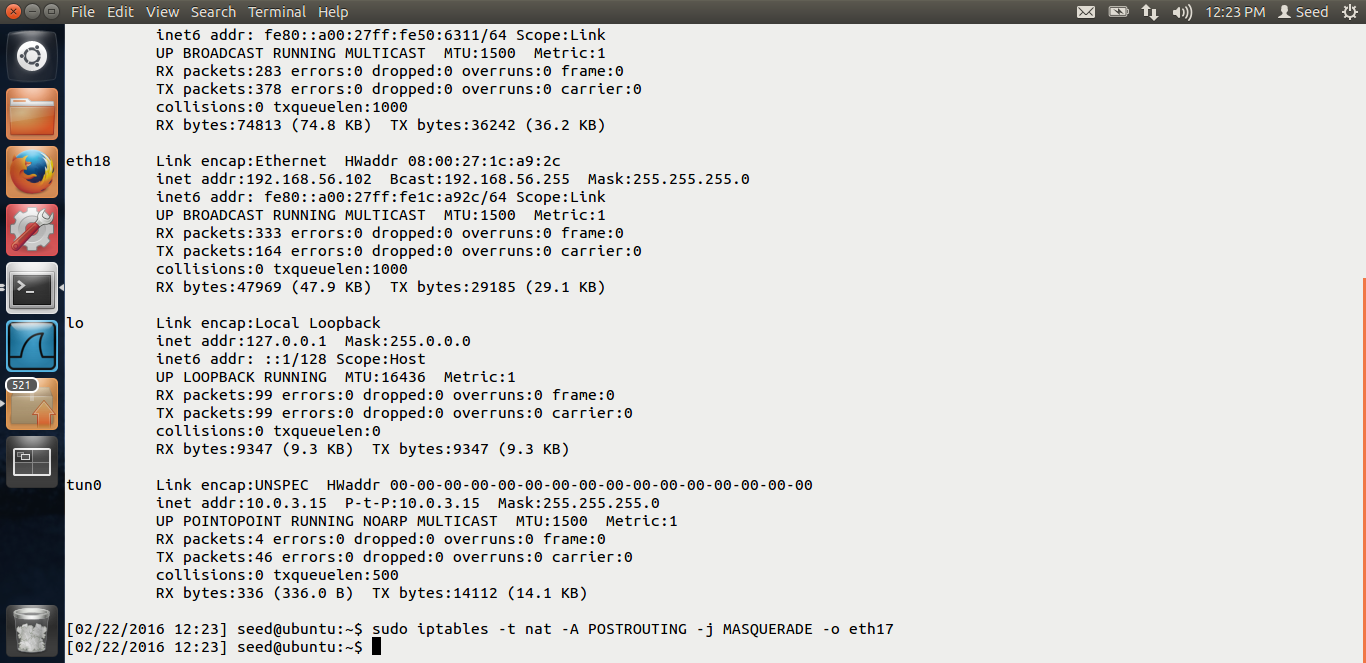
Now, we have to redirect all the traffic on my original vm, for Syracuse network, 128.230.0.0 to my vpn tunnel.



In the above screen shot, I have added the route to redirect all the traffic to the tun0 interface.

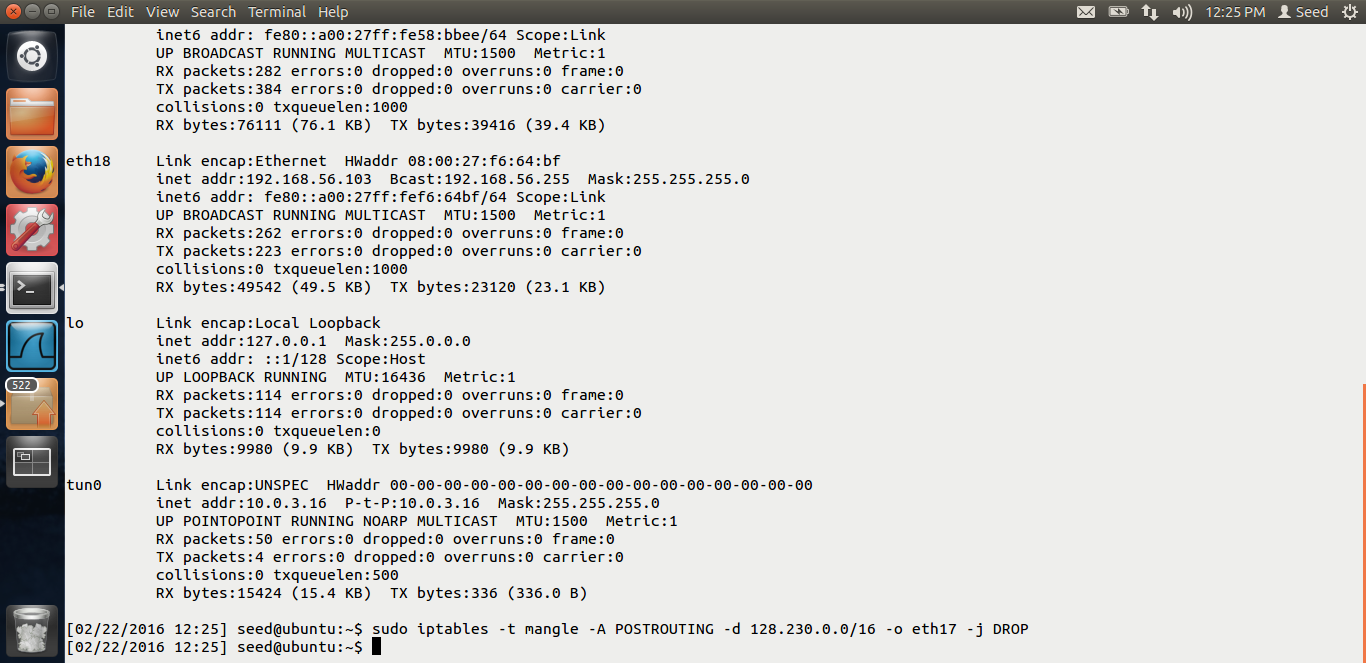


Because of the NAT limitation, I have use the above commands as mentioned in the lab.



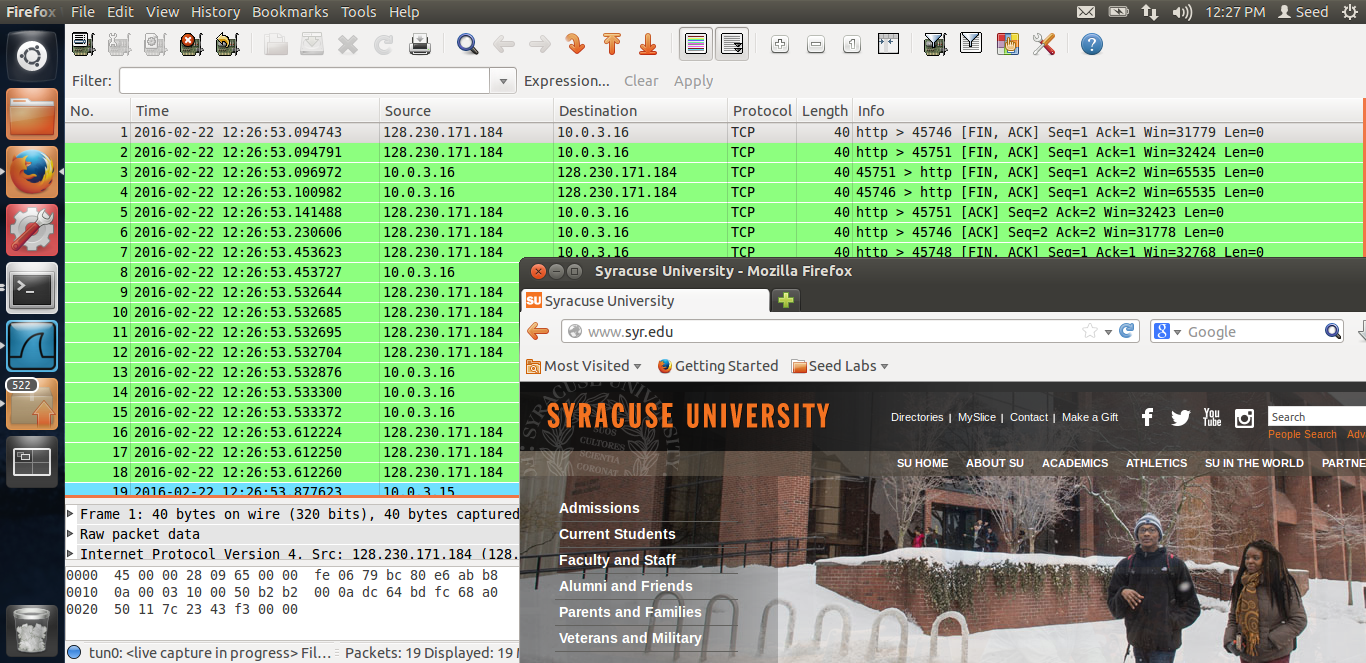
Thus my host to gateway tunnel has been set-up.

# TASK 3: SET UP FIREWALL

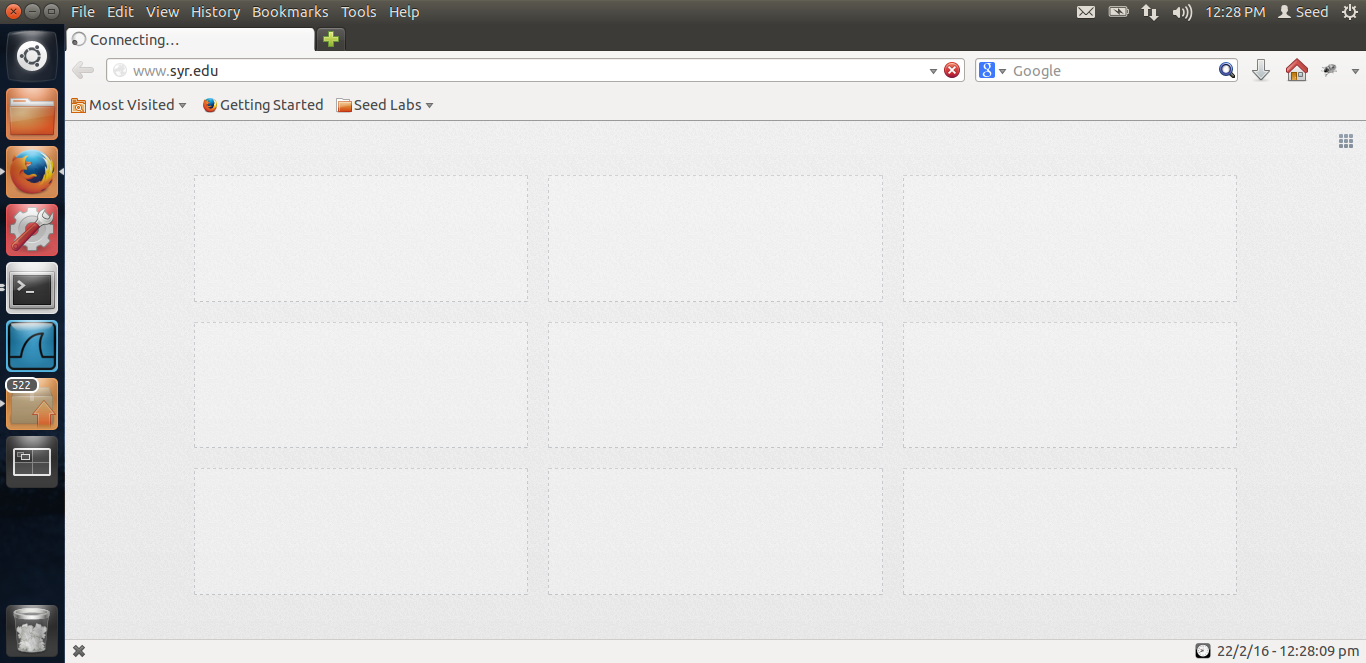


You can see that I am setting up my firewall on my original vm.

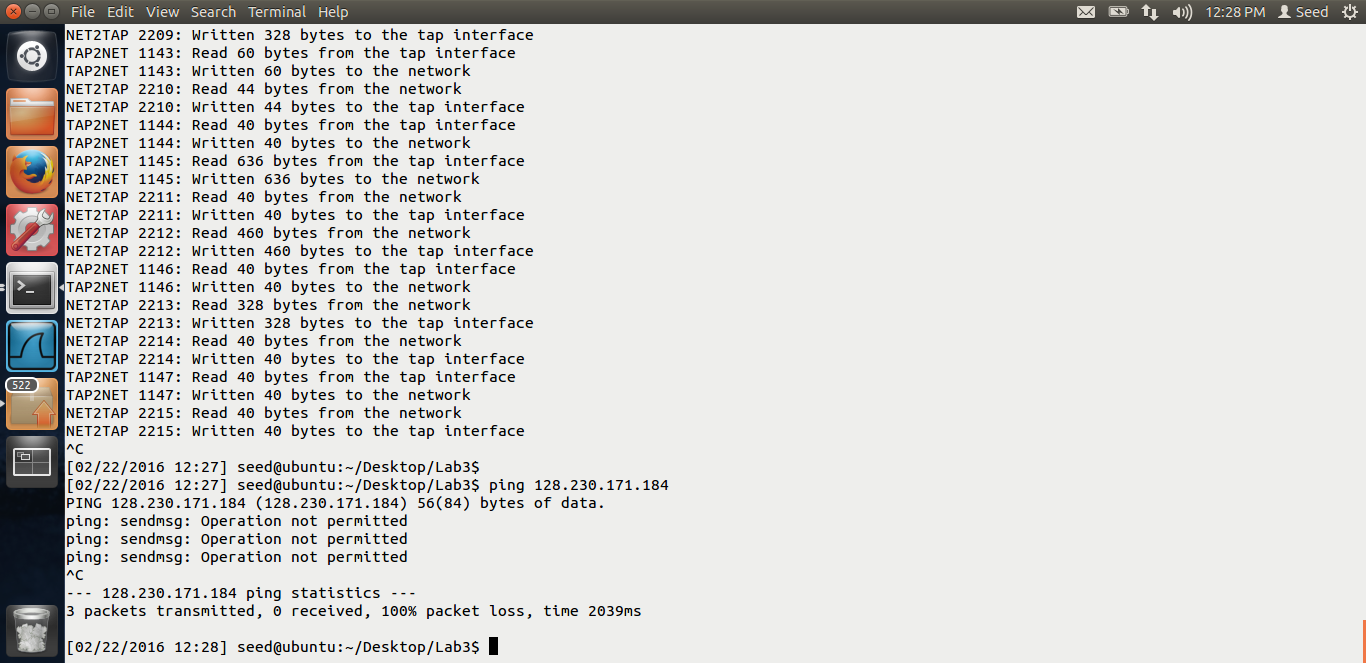
# TASK 4: BYPASSING FIREWALL



Now, as everything has been set-up, even though I access [www.syr.edu](http://www.syr.edu), I am able to access it. From the wireshark, you can see that the traffic is going through 10.0.3.16, which is my tun0 interface. Thus, I am able to bypass the firewall using VPN.



If I cut my VPN, I am not able to bypass the firewall.



You can see that I have cut my VM, even then I am not able to bypass the firewall, and because of the rule, I am not able to ping. Thus the VPN I am using to bypass the firewall.

End of Lab-3.