Foundations Network Security

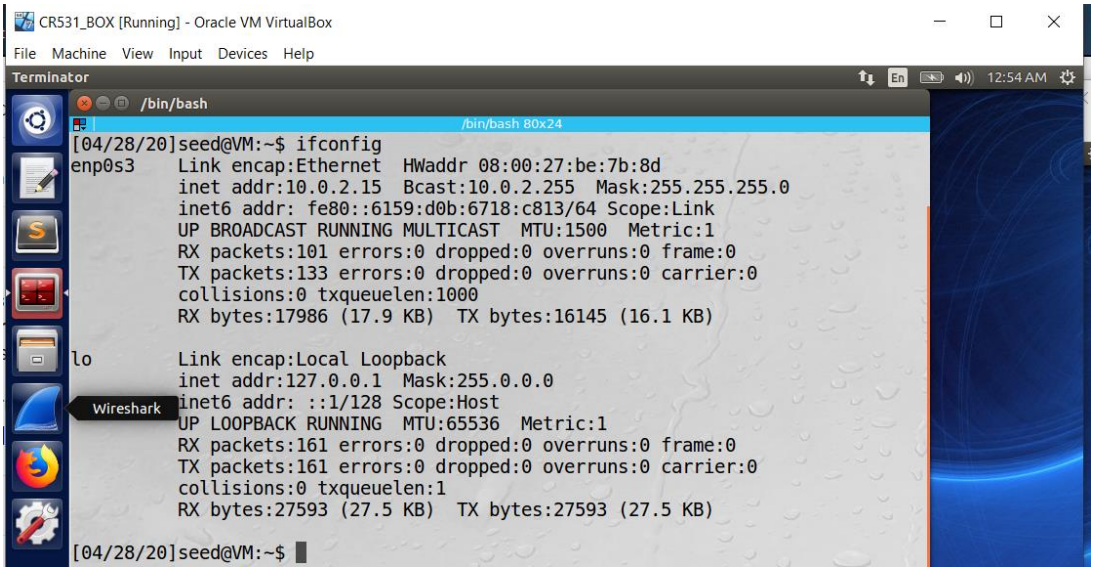
Linux Firewall Exploration Lab

Chakradhar Reddy Donuri

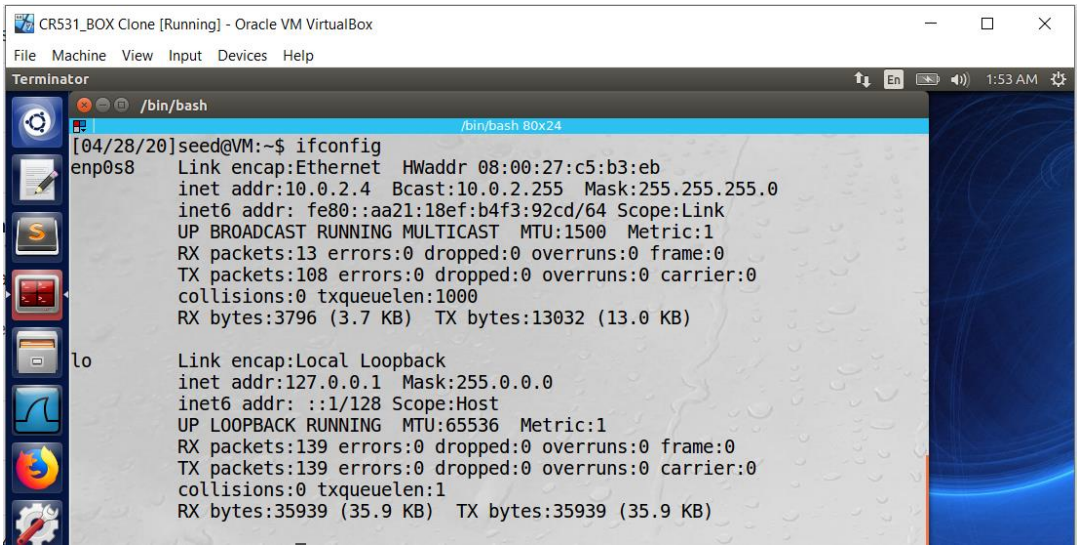
E949F496

Task 1: Using a Firewall

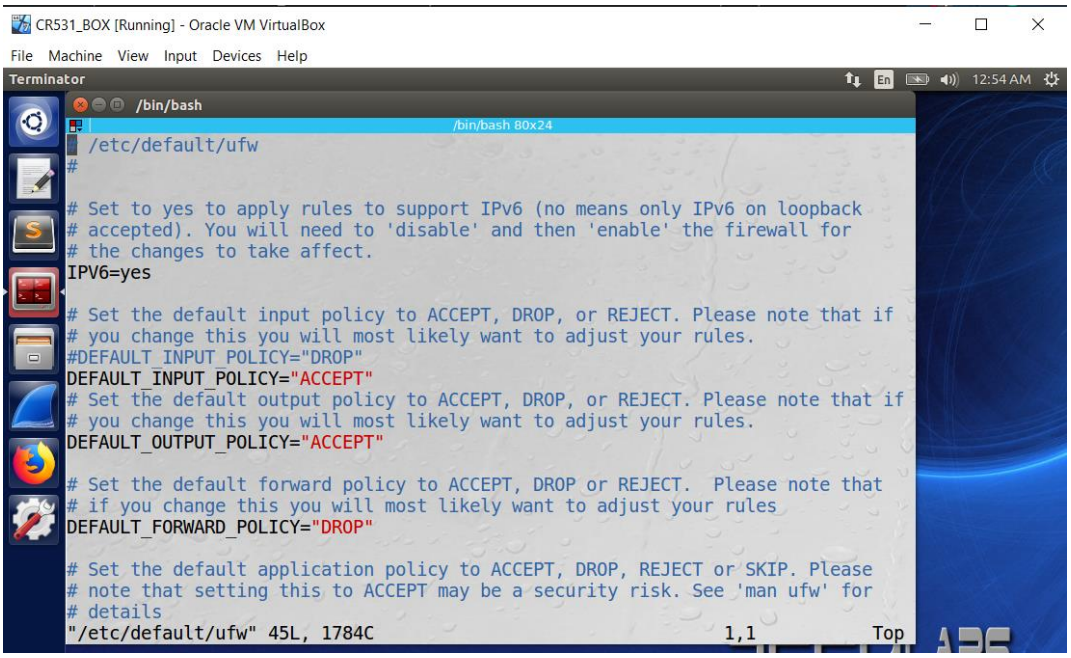
VM1 IP address: 10.0.2.15



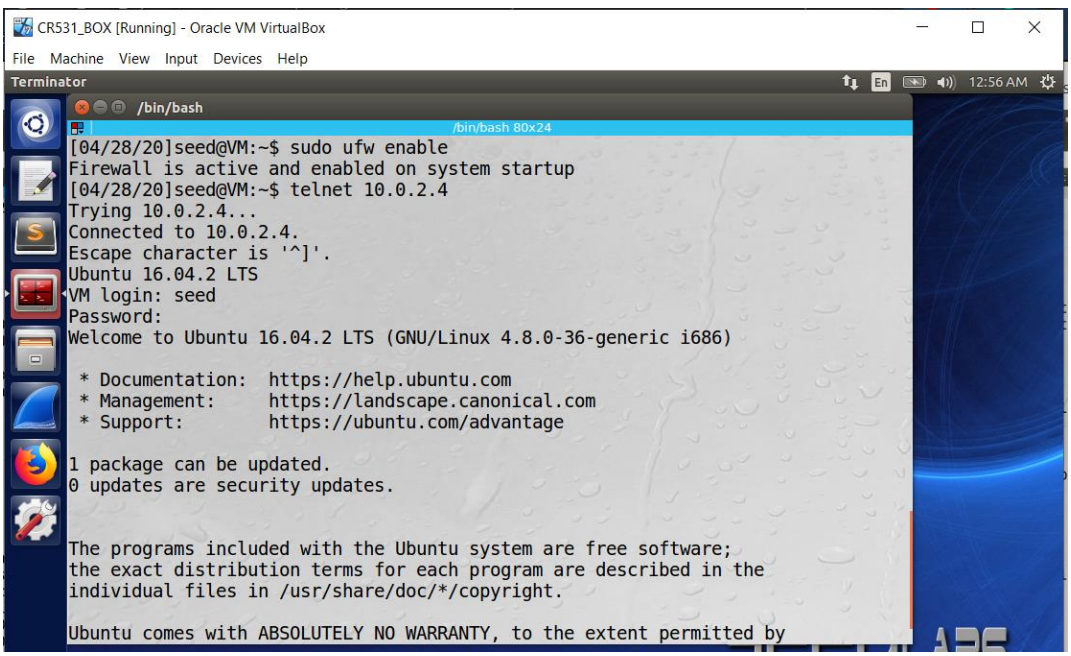
VM2 IP address: 10.0.2.4



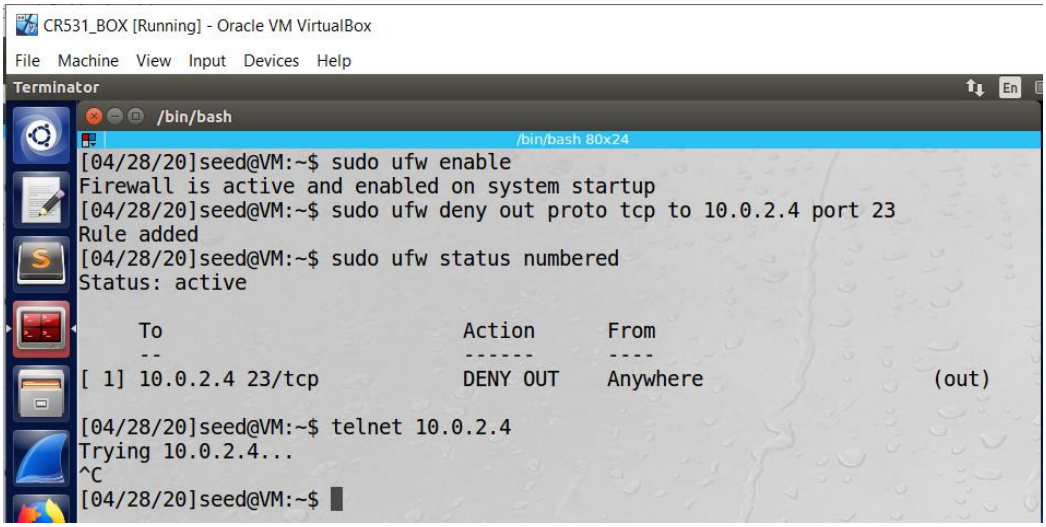
Change DEFAULT_INPUT_POLICY="ACCEPT" in /etc/default/ufw



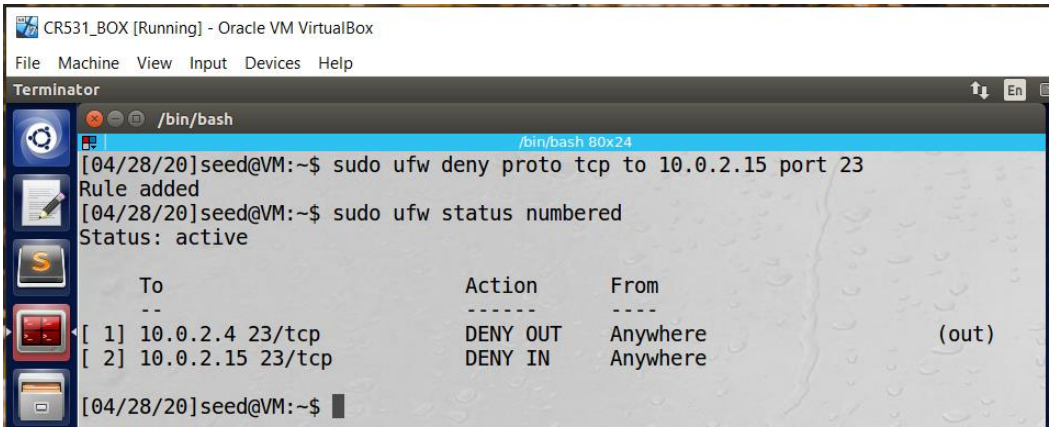
Making sure that VM1 is connecting to VM2



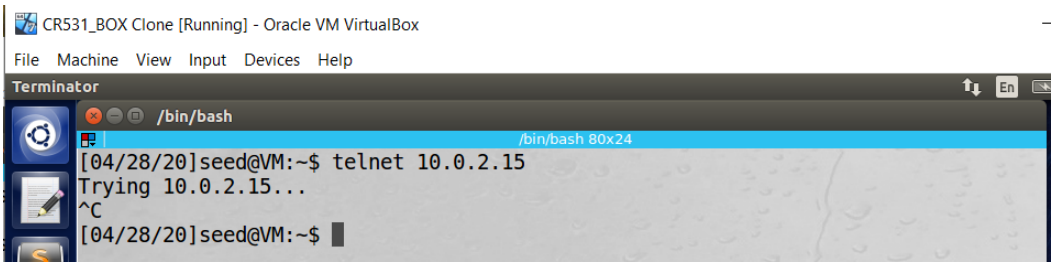
Prevent A from using telnet to connect Machine B.



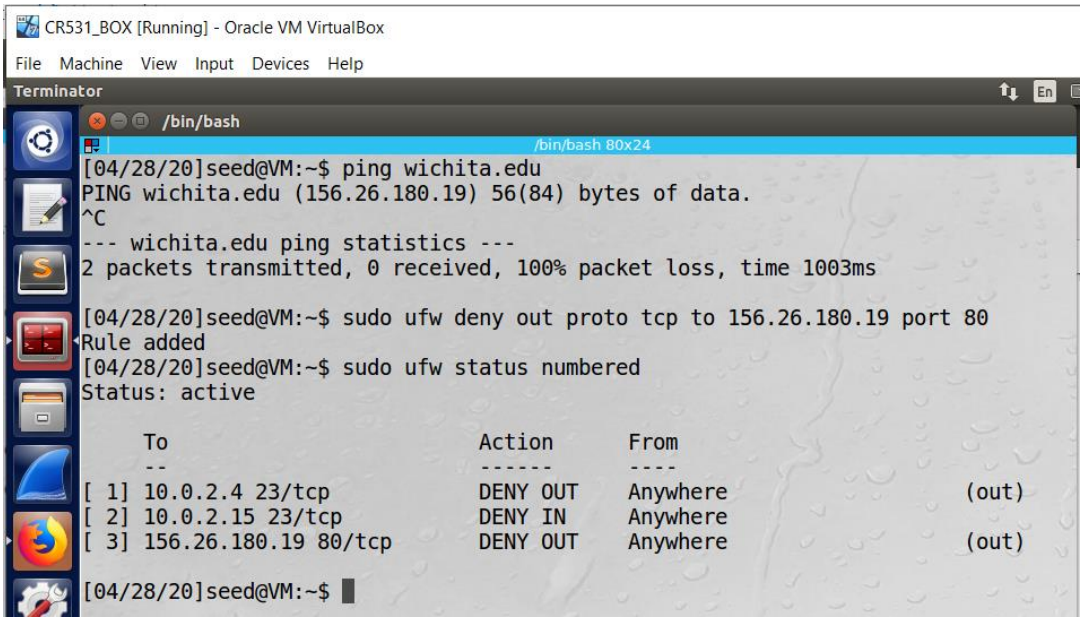
Prevent B from doing telnet to Machine A.



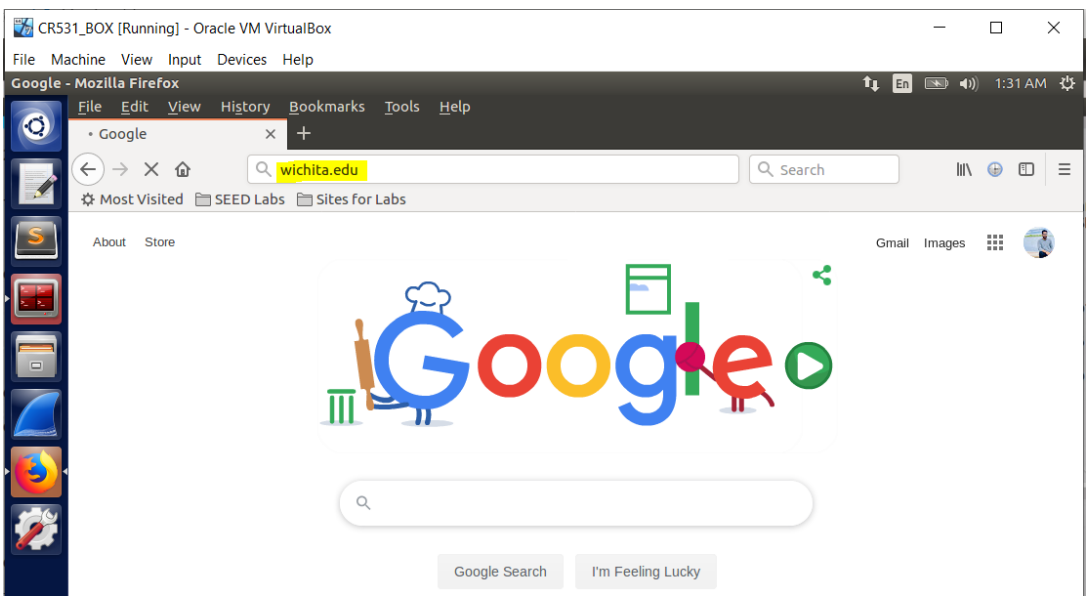
Checking



Prevent A from visiting an external web site (Wichita.edu)

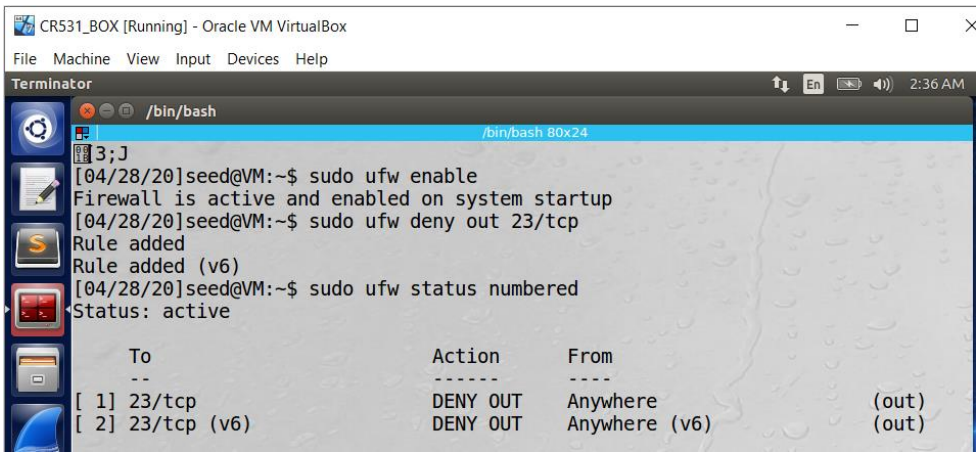


Checking Wichita.edu in browser

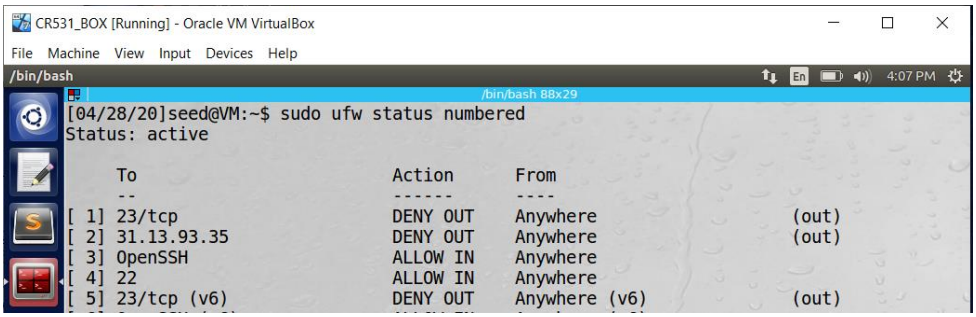


Task 2: Evading Egress Filtering

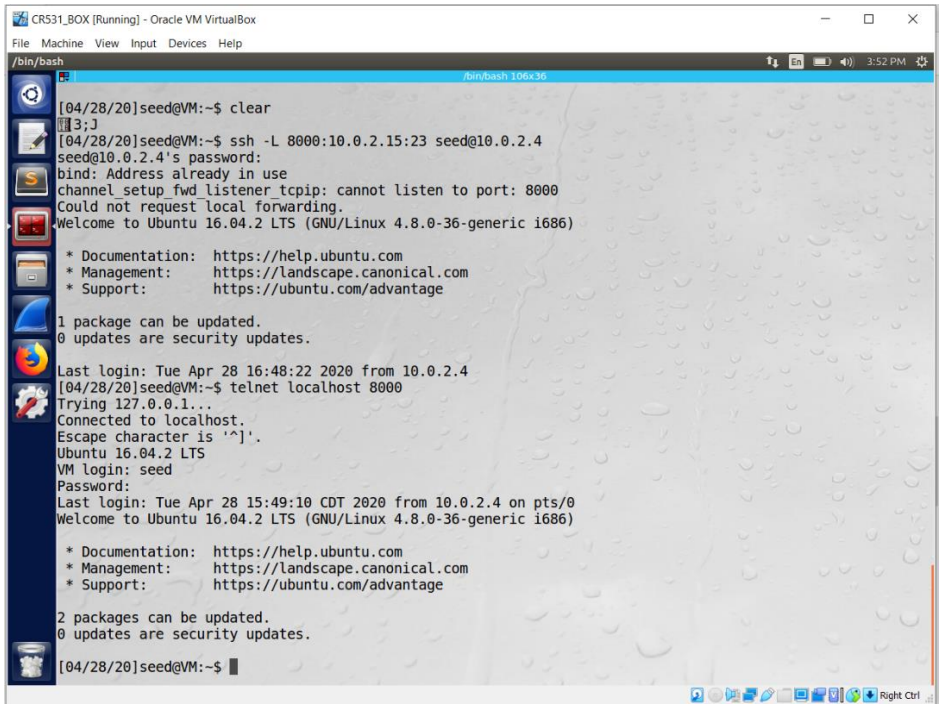
Step 1: blocking outgoing traffic 23/tcp



Next block www.facebook.com i.e. 31.13.93.35

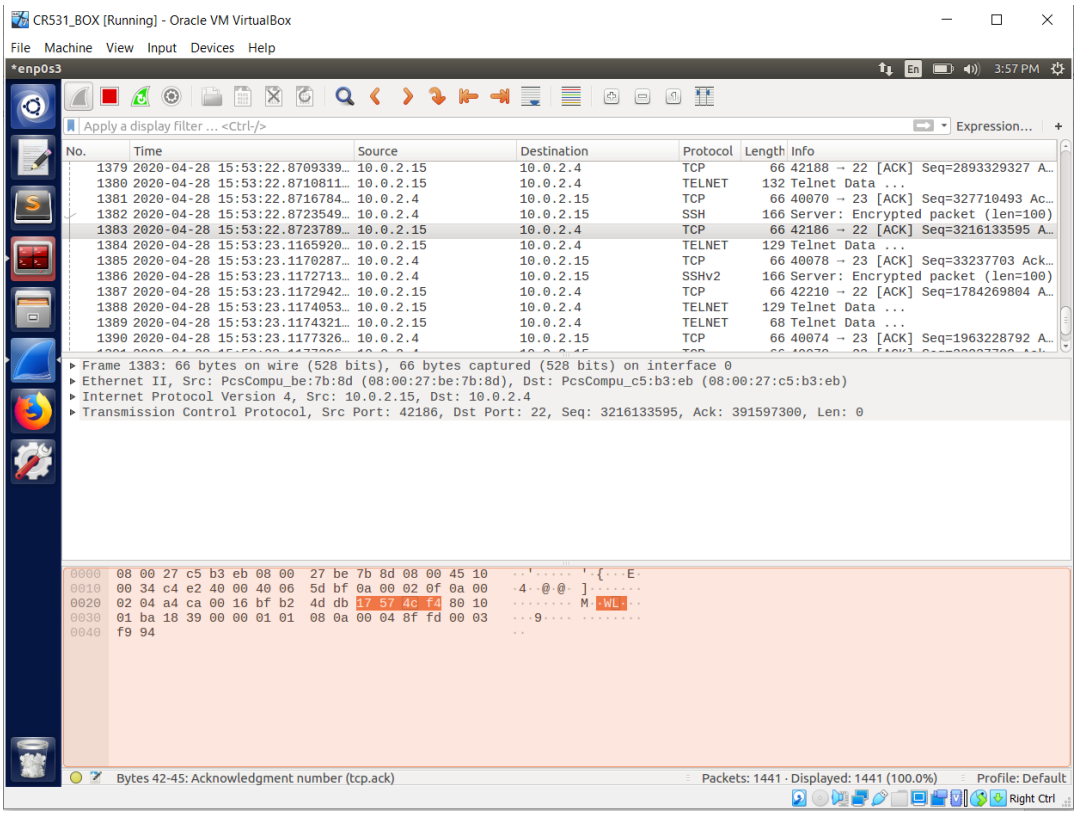


Task 2.a) Deliverable Explain what the ”-L” option does in the ssh command. Explain how the tunneling approach allows us to bypass the egress filtering. A screen shot of the packet traffic provided by Wireshark on Machine A showing the packet traffic when connecting to the telnet server on machine B

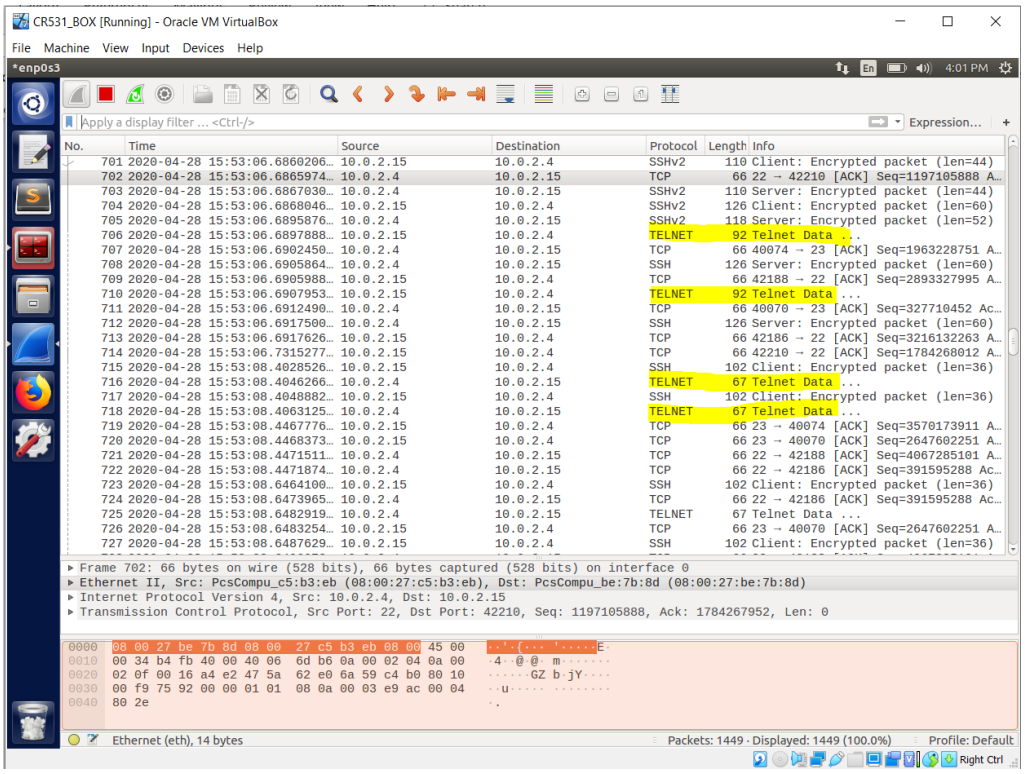


Answer) We set up an SSH tunnel through which all telnet communications can pass. The -L flag stands for the local host. i.e. Specifies that the given port on the local (client) host is to be forwarded to the given host and port on the remote side.
Now, if we point the VM to localhost 8000, first it gets forwarded to 10.0.2.4:23 (i.e. telnet port of machine_B) through after going 10.0.2.4:22 (ssh port of machine_B) known as port forwarding.

Below is the screen shot of the packet traffic provided by Wireshark on Machine .A showing the packet traffic when connecting to the telnet server on machine B

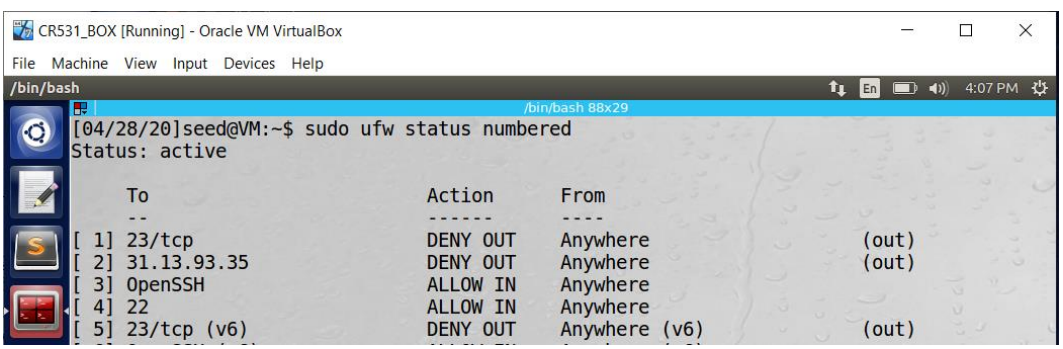


Observation: After CR531 i.e. VM1 gains access to CR531_Clone i.e. VM2 it telnet to localhost and gains access to localhost. Information regarding localhost is passed to VM1 through VM2 and SSH tunnel

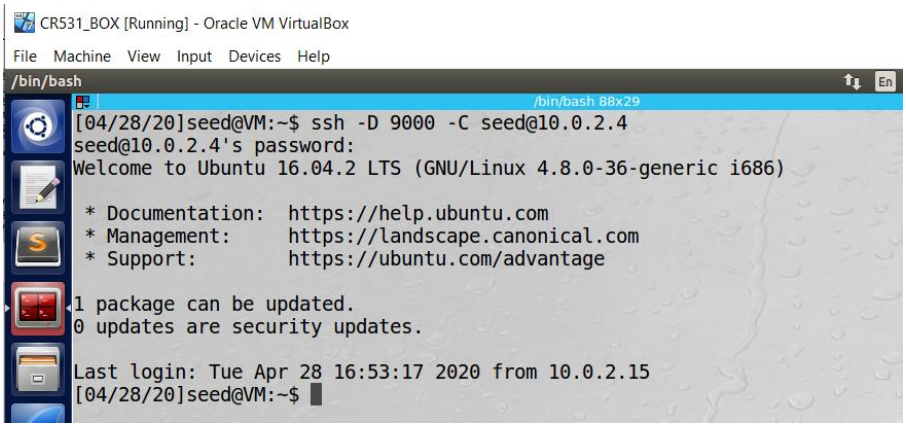


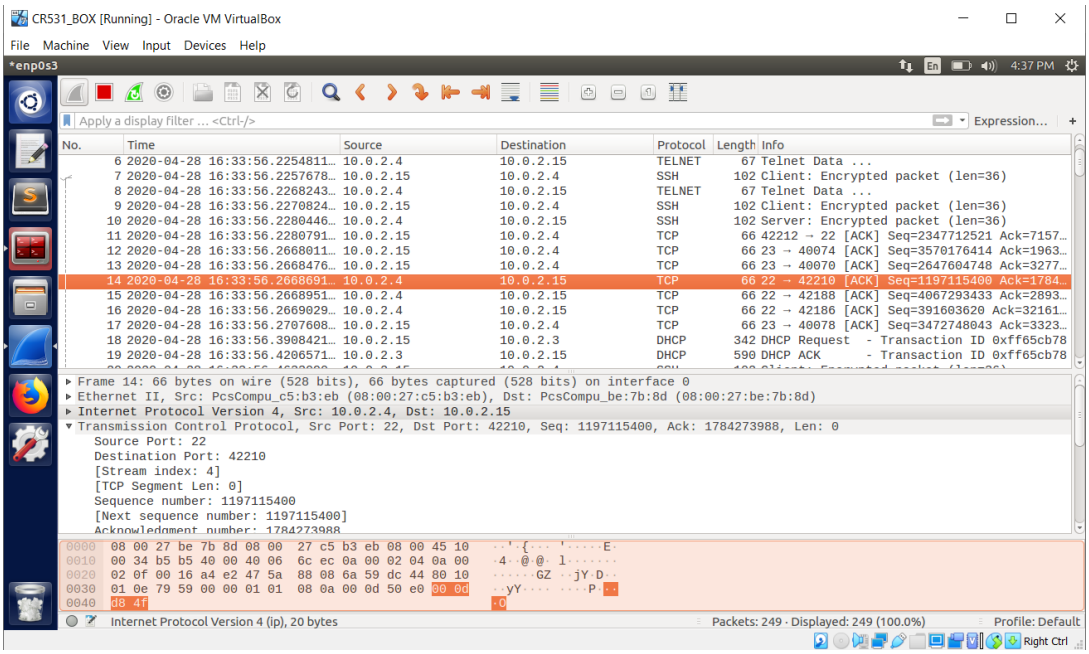
Task 2.b Connect to Facebook using SSH Tunnel

We have already denied out to facebook.com i.e 31.13.93.35



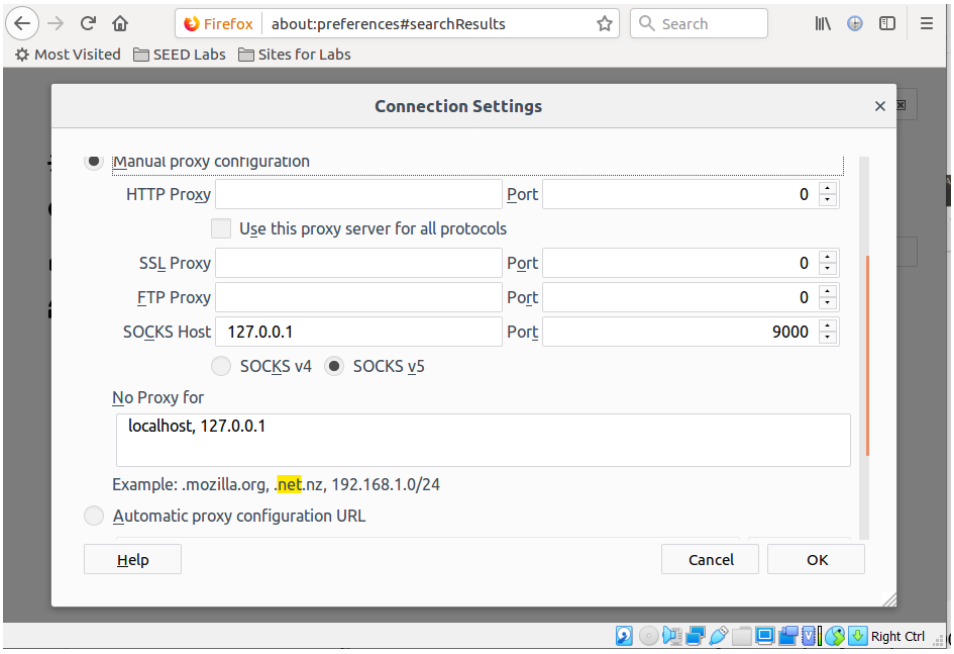
VM1(10.0.2.15) creates a SSH tunnel to VM2 (10.0.2.4) through port 9000.



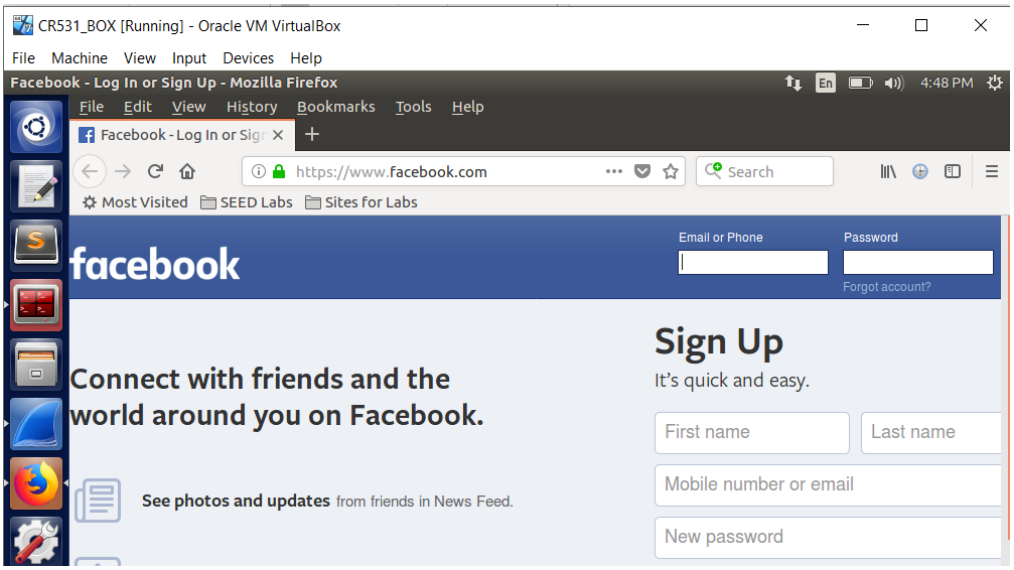


Observation: VM1(10.0.2.15) and VM2 (10.0.2.4) performs 3-way handshake and establishes connection using the SSH port 22. After establishing the connection they communicate through TCP protocol.

Step-1) Changing preferences of firefox

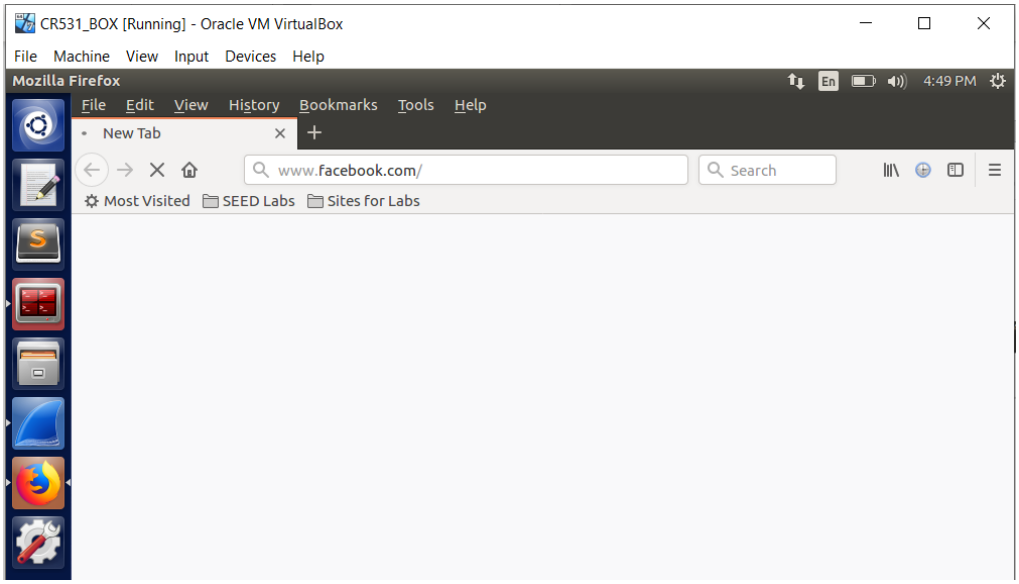


Testing www.facebook.com



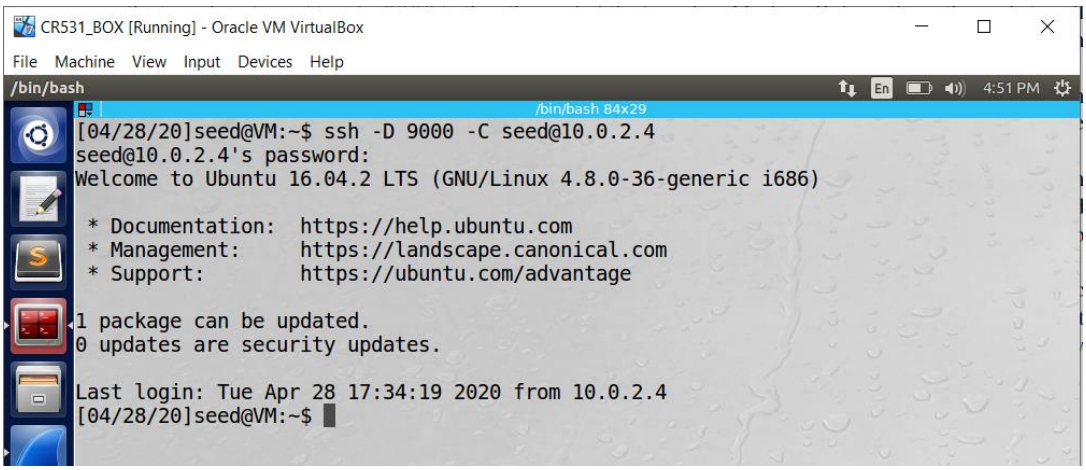
Observation: We can see that website is working.

Step-2) Now, VM1 (10.0.2.15) breaks the SSH connection from VM2 (10.0.2.4) by exiting VM2



Observation: After breaking SSH connection when VM1(10.0.2.15) tries to access facebook.com the proxy and port 9000 refuses the connection since it cannot connect to VM2 (10.0.2.4).

Step-3) Now, again VM1 (10.0.2.15) establishes SSH connection to VM2 (10.0.2.4).



After establishing the SSH tunnel between 10.0.2.15 and 10.0.2.4 again performs 3-way handshake. Further communication is done through SSH

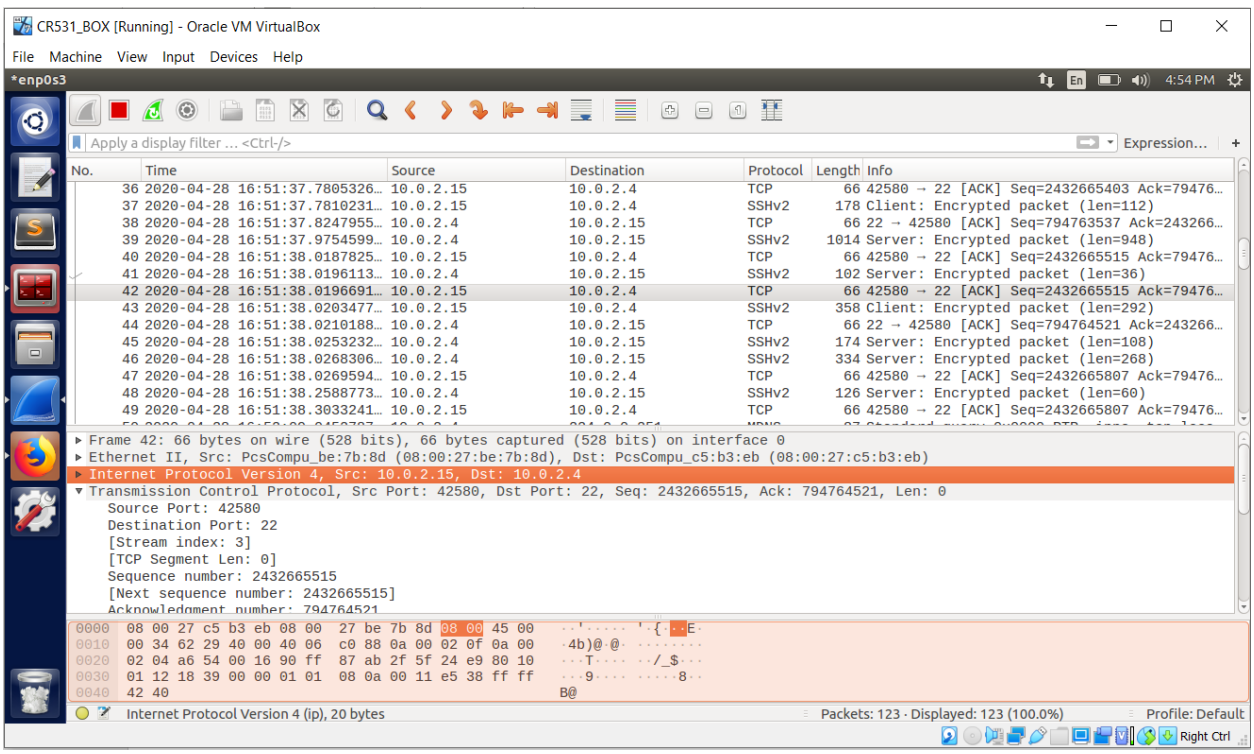
Explain what the -D and -C options do in the ssh command

The -D flag stands for dynamic port forwarding which will basically turn your SSH client into a proxy server (SOCKS). i.e. Specifies a local “dynamic” application-level port forwarding.
-C i.e. Requests compression of all data (including stdin, stdout, stderr, and data for forwarded X11 and TCP connections)

Explain how this approach helps you bypass the firewall rules?

Many organizations and industries among different countries often block access to some external sites by their internal users. This is called Egrees filtering . These businesses set up their egress firewalls to block social network sites, which ensures that their workers can not access such sites from within their network. Unfortunately, it is easy to bypass these firewalls, and services / products that help users bypass firewalls are widely available on the Internet. The most commonly used technology to bypass egress firewalls is Virtual Private Network (VPN)

Egress filtering controls the traffic that is attempting to leave the network. Before an outbound connection is allowed, it has to pass the filter's rules. Pretty much every firewall provides egress filtering. However, it is not enabled by default. The out-of-the-box setup typically allows any machine on the network to connect to any host over any port. Since it is disabled by default, many small & medium-size organizations never use egress filtering.

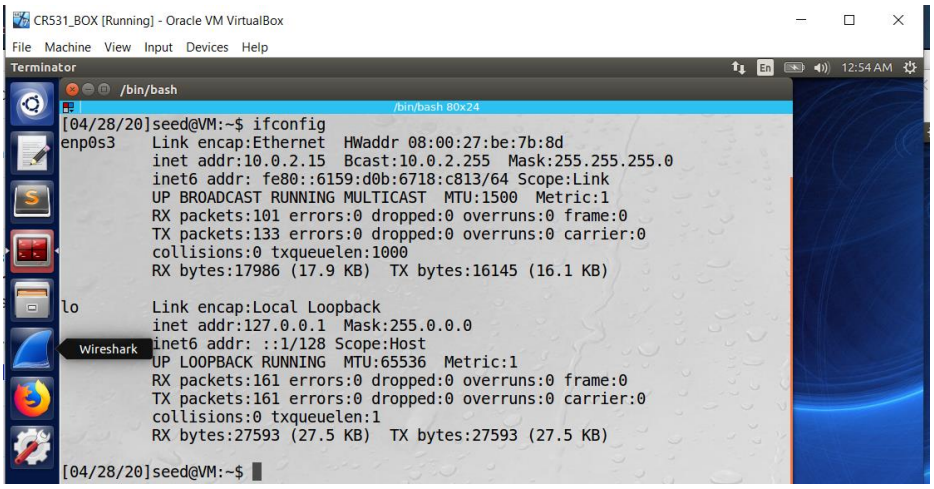


Observation: We can see that packets are sent through SSH which contain information about Ethernet Type, IP, TCP and SSH and with port number 22. There is no information of facebook.com IP address and port 22 is not blocked so the ufw firewall accepts the packet.

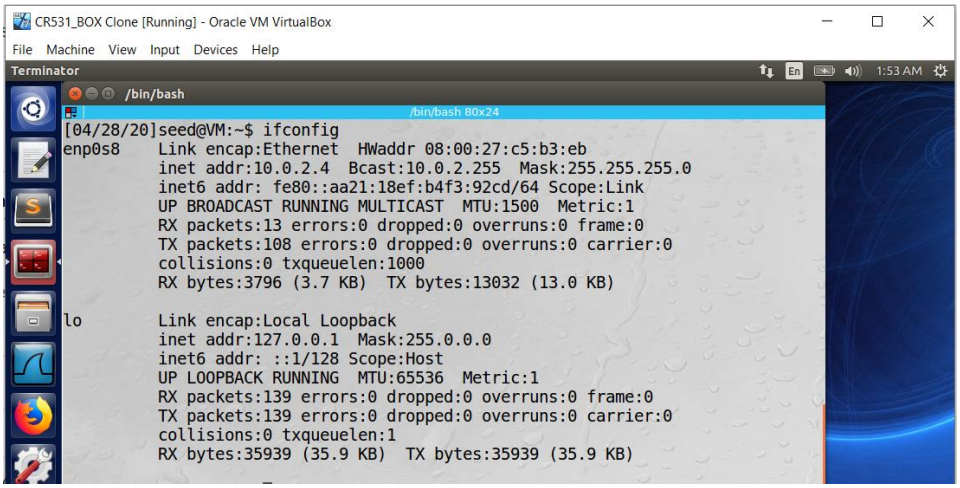
Task 3: Evading Ingress Filtering

Answer) First check the ip address of each VM box

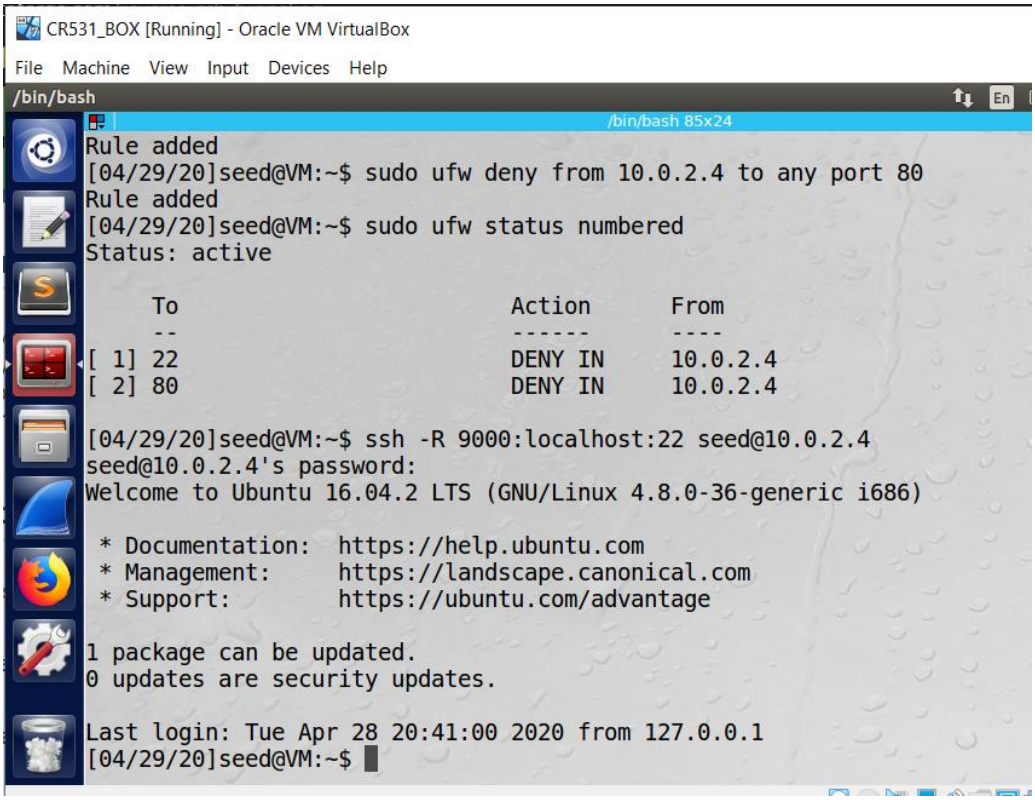
VM1- 10.0.2.15



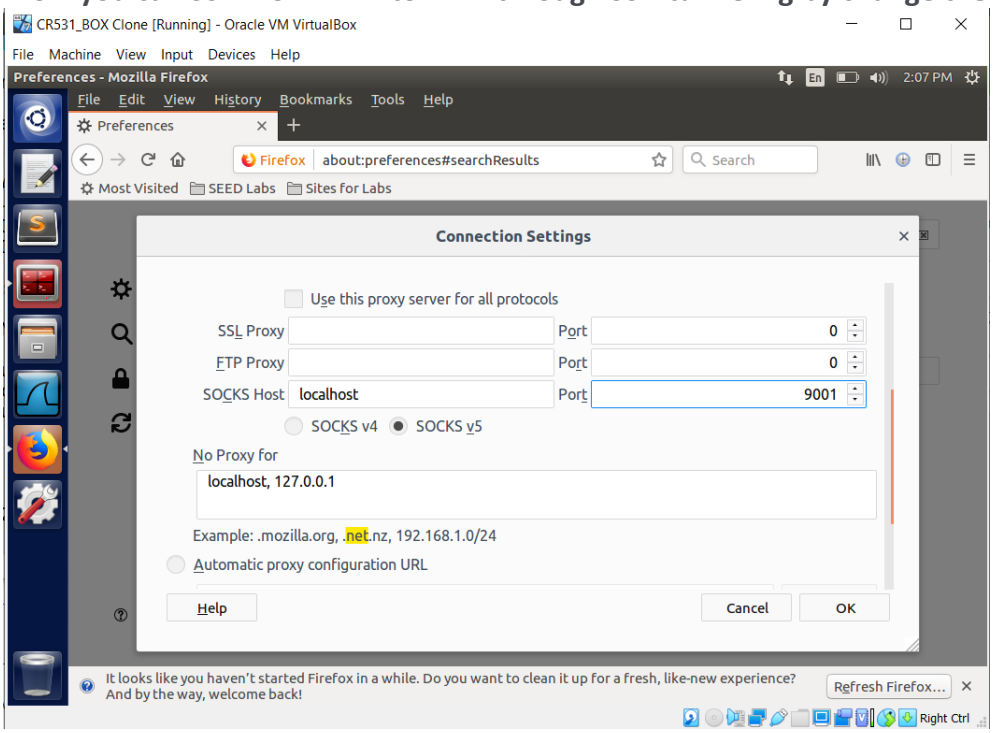
VM-2: 10.0.2.4

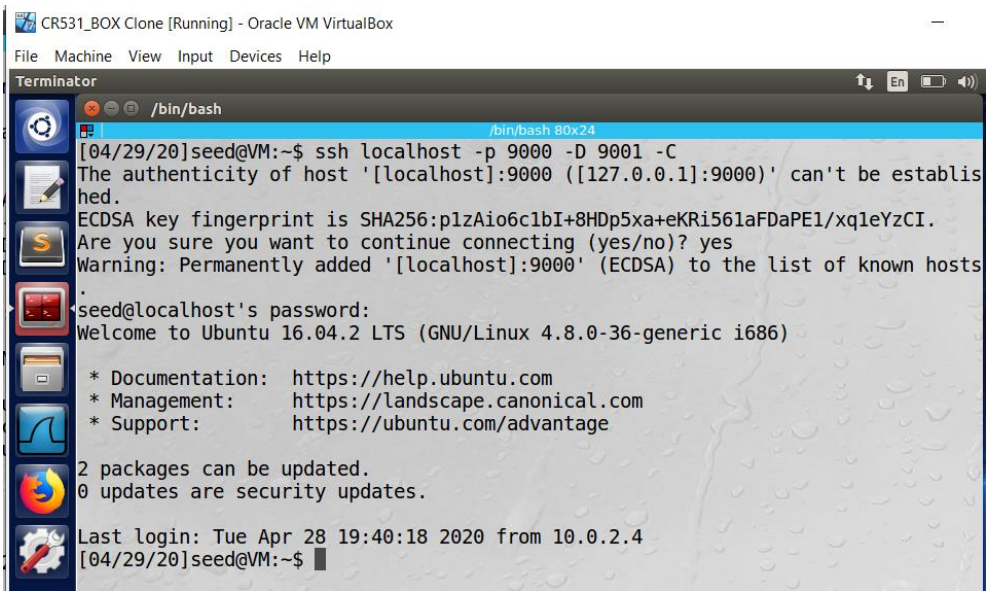


Now, Deny port 22 and 80 from 10.0.2.4 (VM2) and perform reverse ssh tunnel to VM2



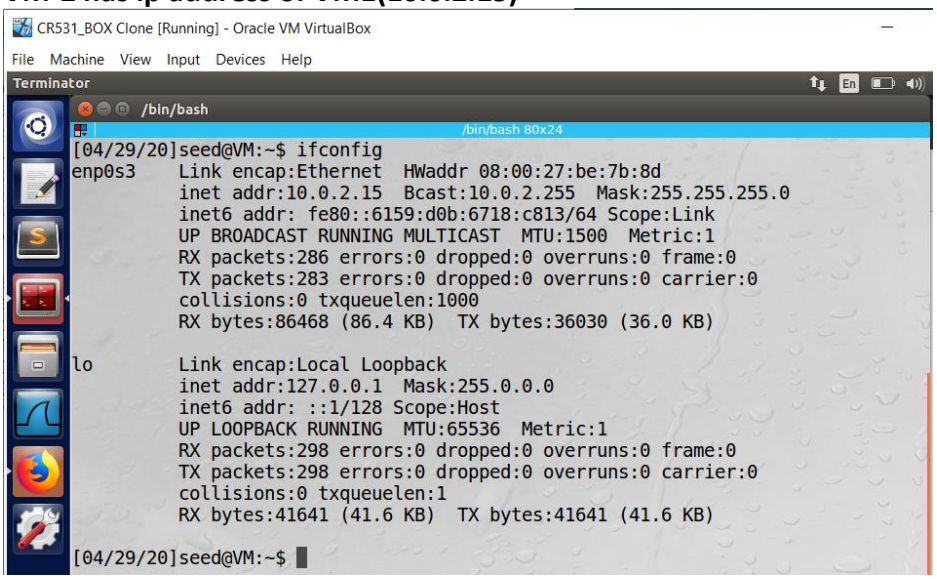
Now you can SSH from VM2 to VM1 through SSH tunneling by change the proxy port to 9001



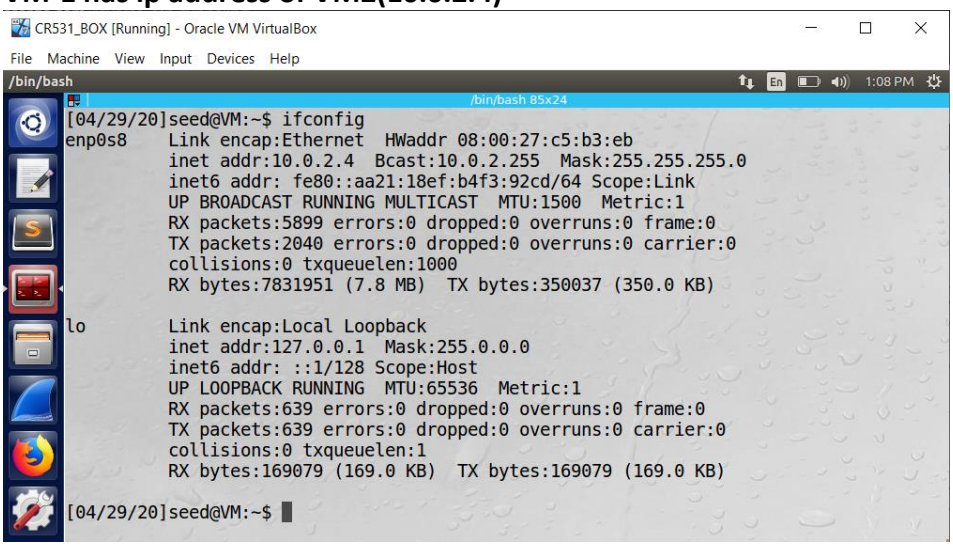


Now we can see from below screenshots the ip address have be altered from VM1 to VM2

VM-2 has ip address of VM1(10.0.2.15)



VM-1 has ip address of VM2(10.0.2.4)



Check the VM1 ip address from browser