FIREWALL LAB

Introduction:

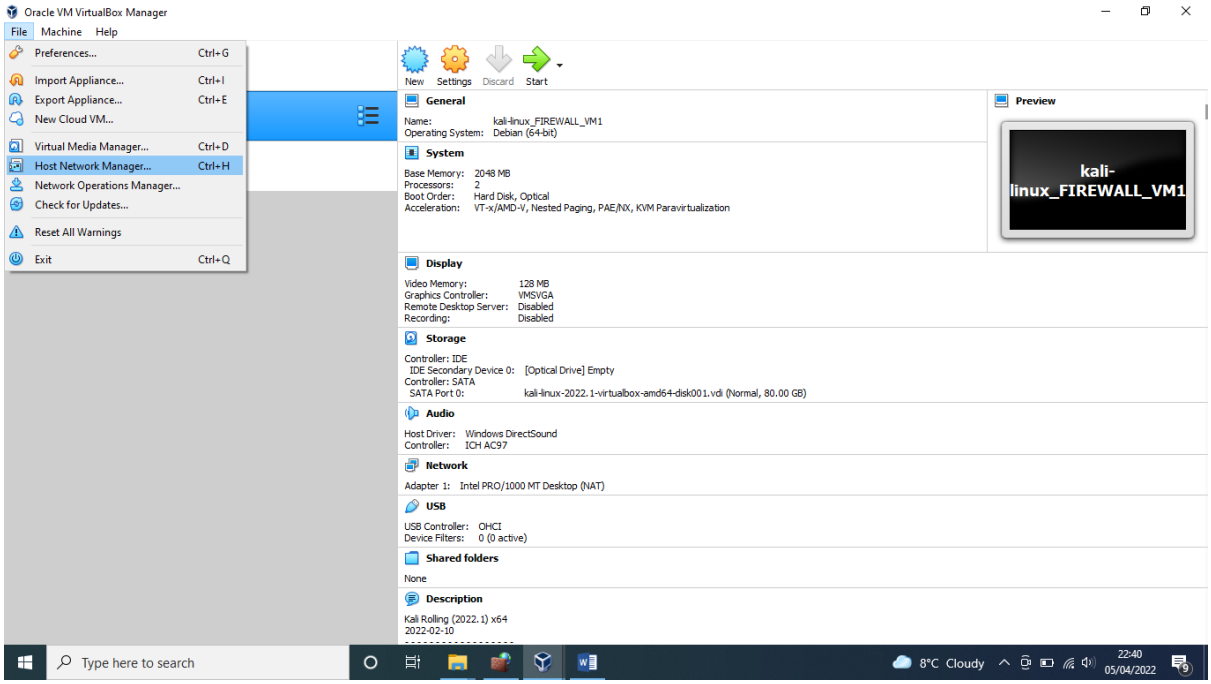
This serves as a comprehensive guide outlining the process of setting up a firewall on a virtual machine and configuring a corresponding firewall rule. Additionally, visual assistance in the form of screenshots is included to offer guidance for those interested in following the steps.

Pre-steps

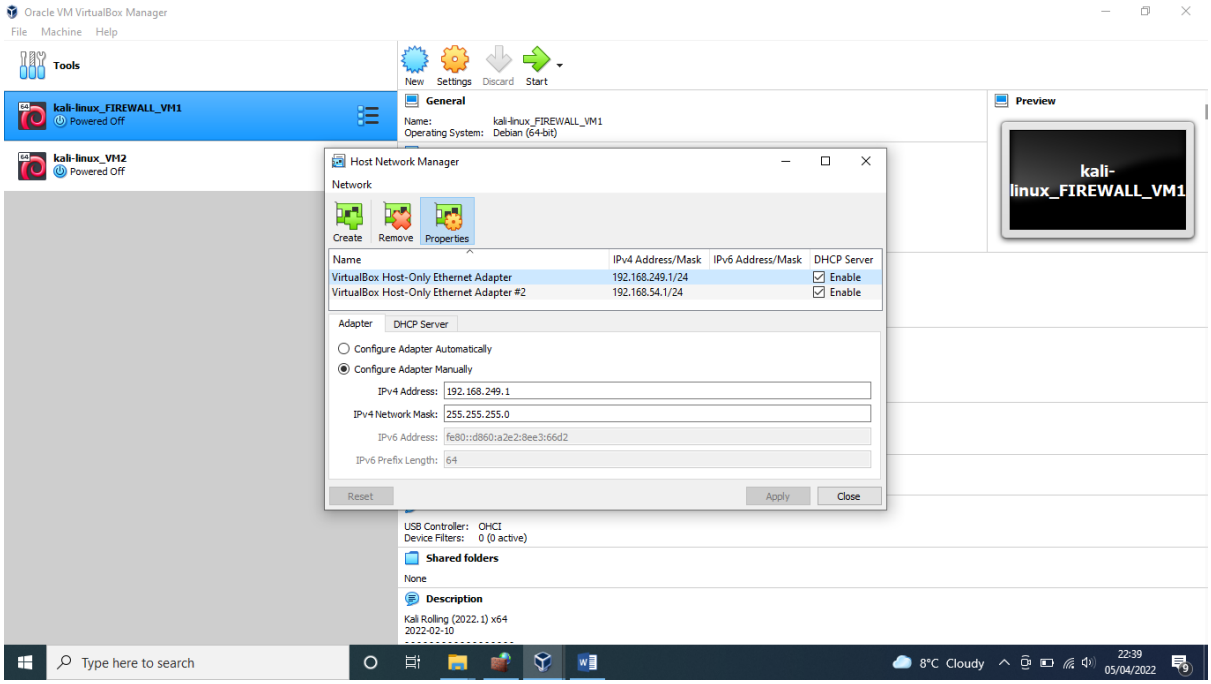
1. Install Oracle Virtualbox/ Vmware on your host system(here my host is a windows machine)
2. Download Kali Linux OS for virtualbox and import it and save as firewall VM1
3. Clone the VM1 and save new Virtualbox as VM2

Step 1- Create Network Adapters in the virtual box

-On VM1, go to File->Host Network Manager (see screenshot below)



Create 2 host only adapters (with DHCP enabled –this allocates IPV4 address automatically) as shown below



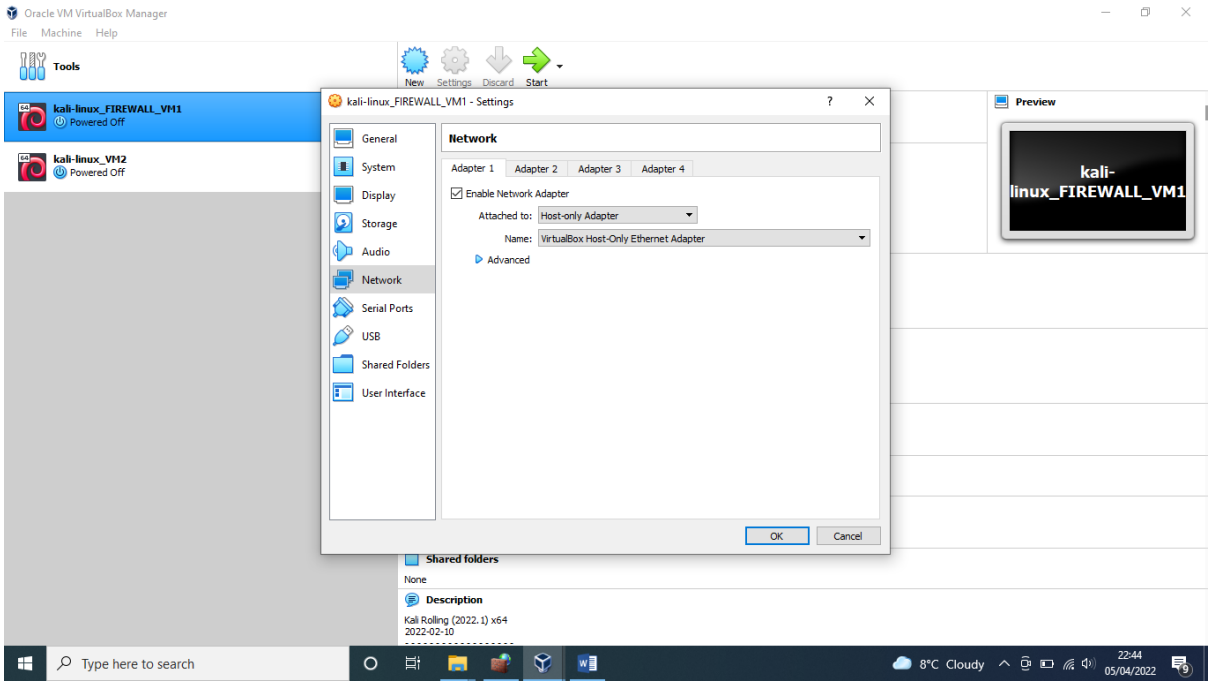
Step 2-

a) Configure network adapter 1 for VM1-Firewall

Select VM1 --> Settings-->Network-->Select Adapter1

Attached to: Host-only adapter

Name: select Virtualbox host-only Ethernet adapter (as shown below)

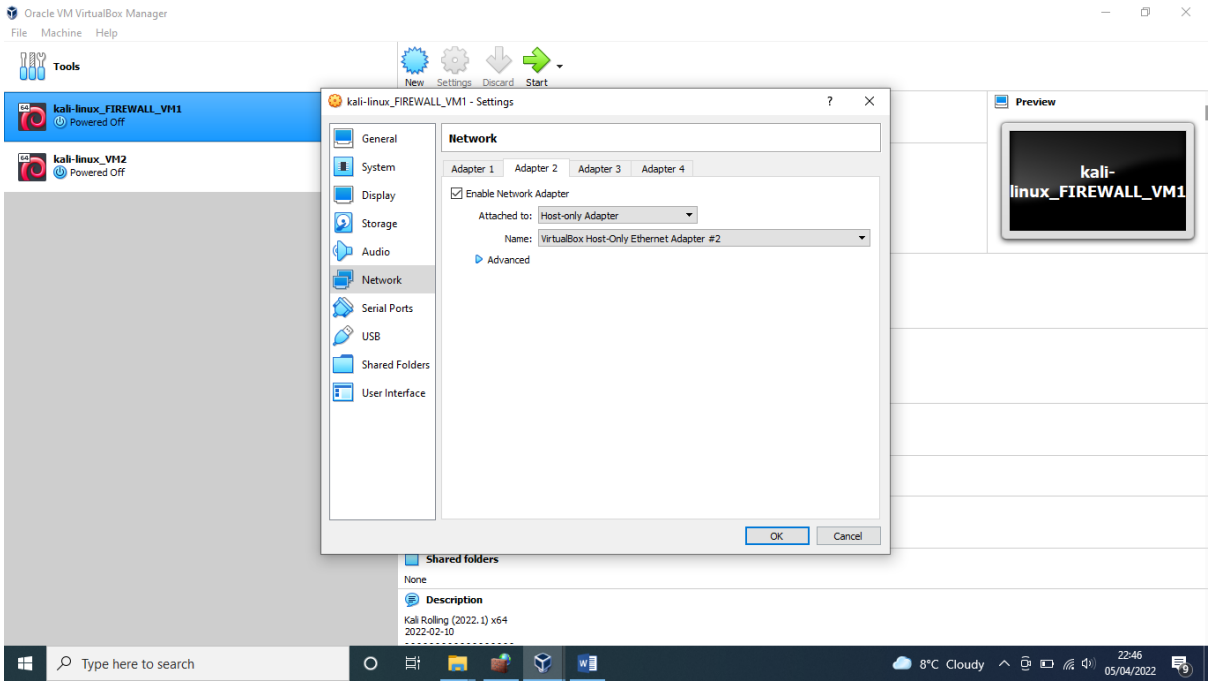


b) Configure network adapter 2 for VM1-Firewall

Select VM1 --> Settings-->Network-->Select Adapter2 (Select enable network adapter)

Attached to: Host-only adapter

Name: select VirtualBox Host-only Ethernet adapter#2 (as shown below)

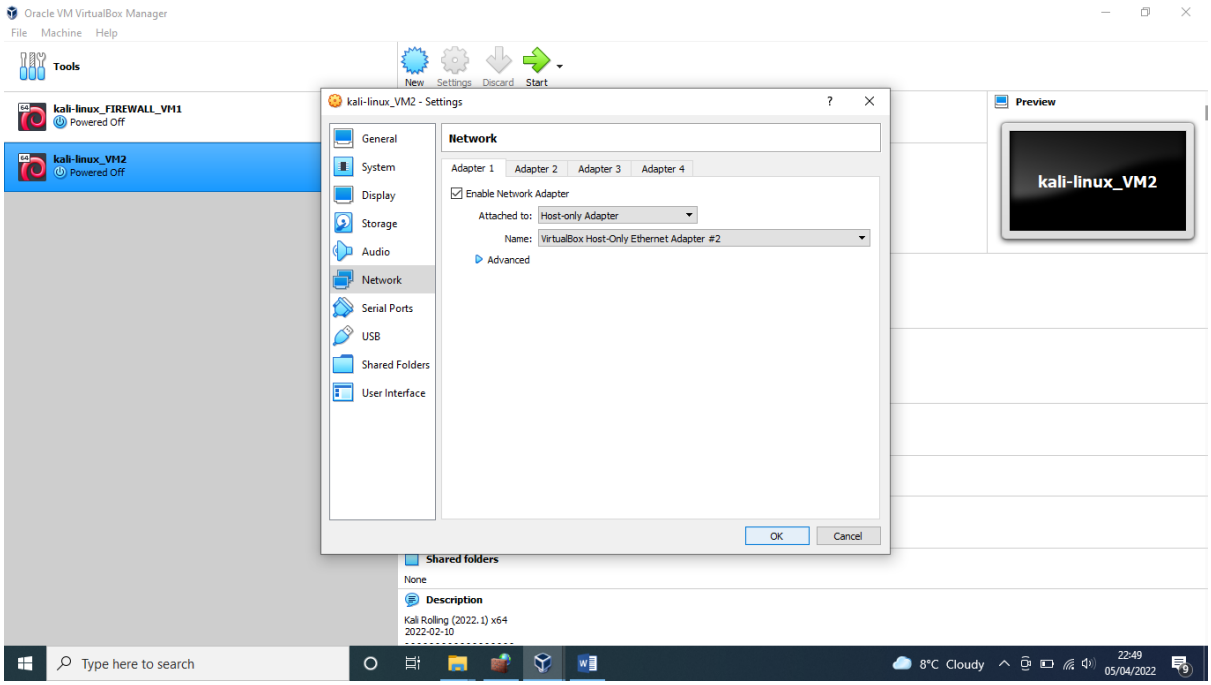


c) Configure network adapter for VM2

Select VM2 --> Settings-->Network-->Select Adapter1 (Select enable network adapter)

Attached to: Host-only adapter

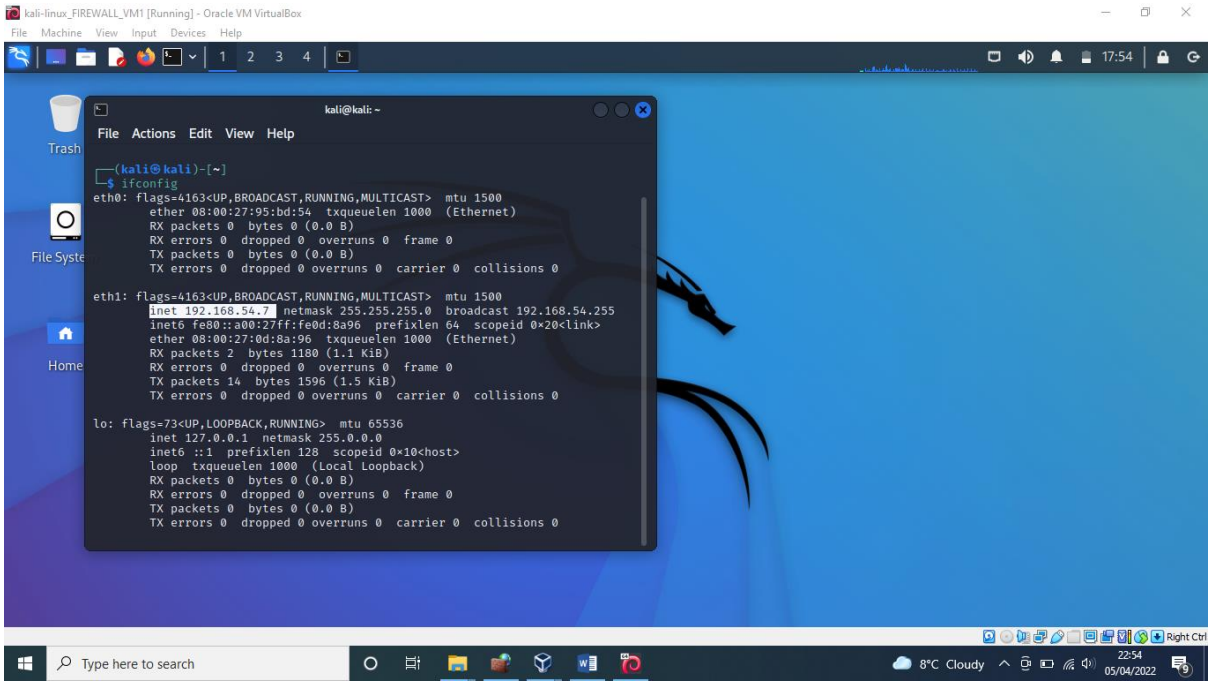
Name: select VirtualBox Host-only Ethernet adapter#2 (as shown below)



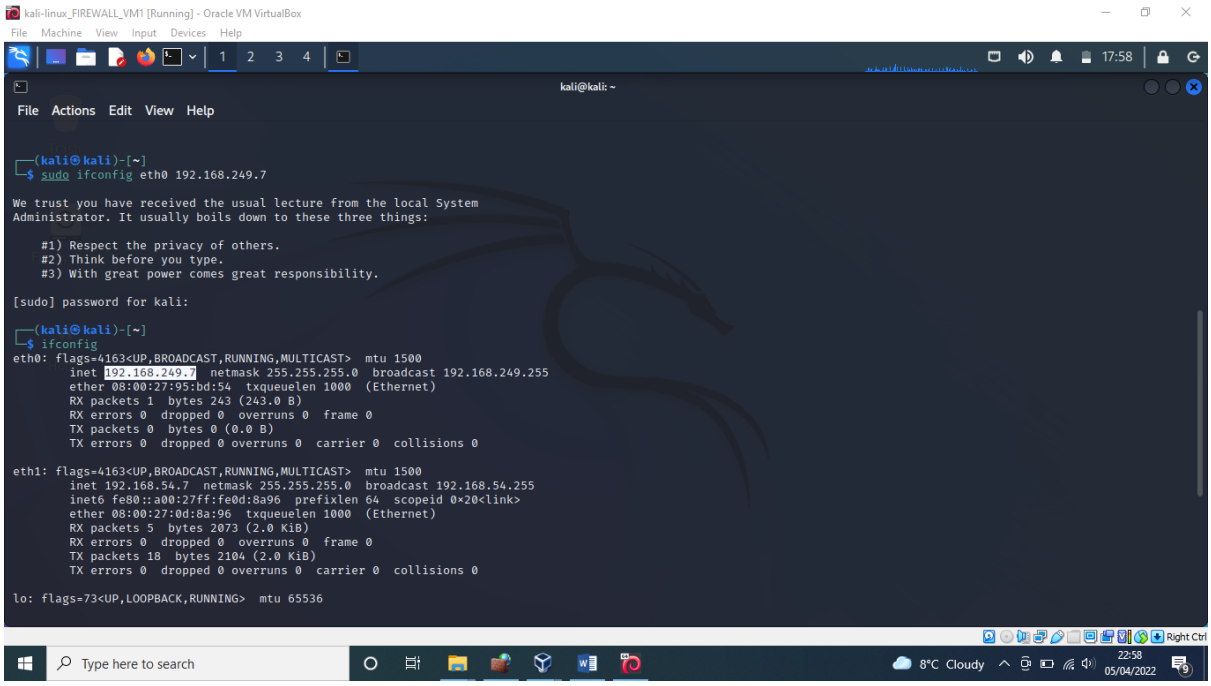
Step 3:

a) Power the VM1 and check the IP addresses of the VM1 (Firewall)

Go to terminal emulator and type ifconfig

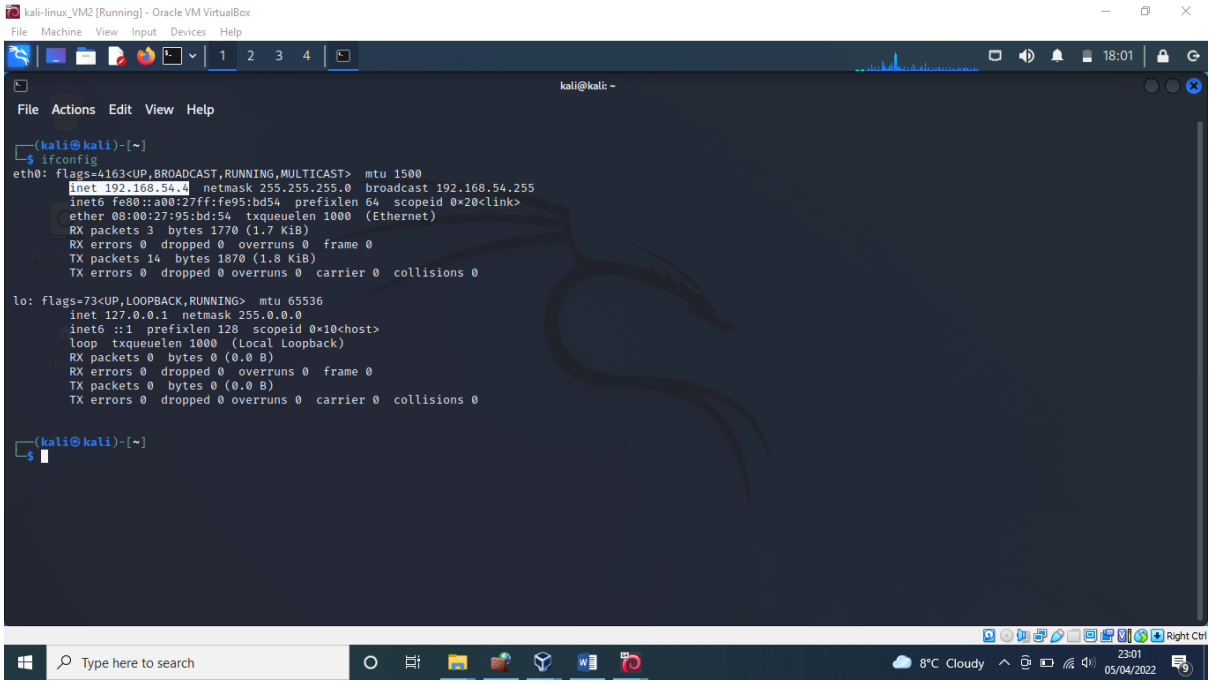


Note that if your eth0 does not have an IP address, it can be manually added with the command sudo ifconfig eth0 192.168.249.7 and check the IP addresses again to confirm that eth0 has been captured (see details below)



b) Power the VM2 and check the IP address

Go to terminal emulator and type ifconfig

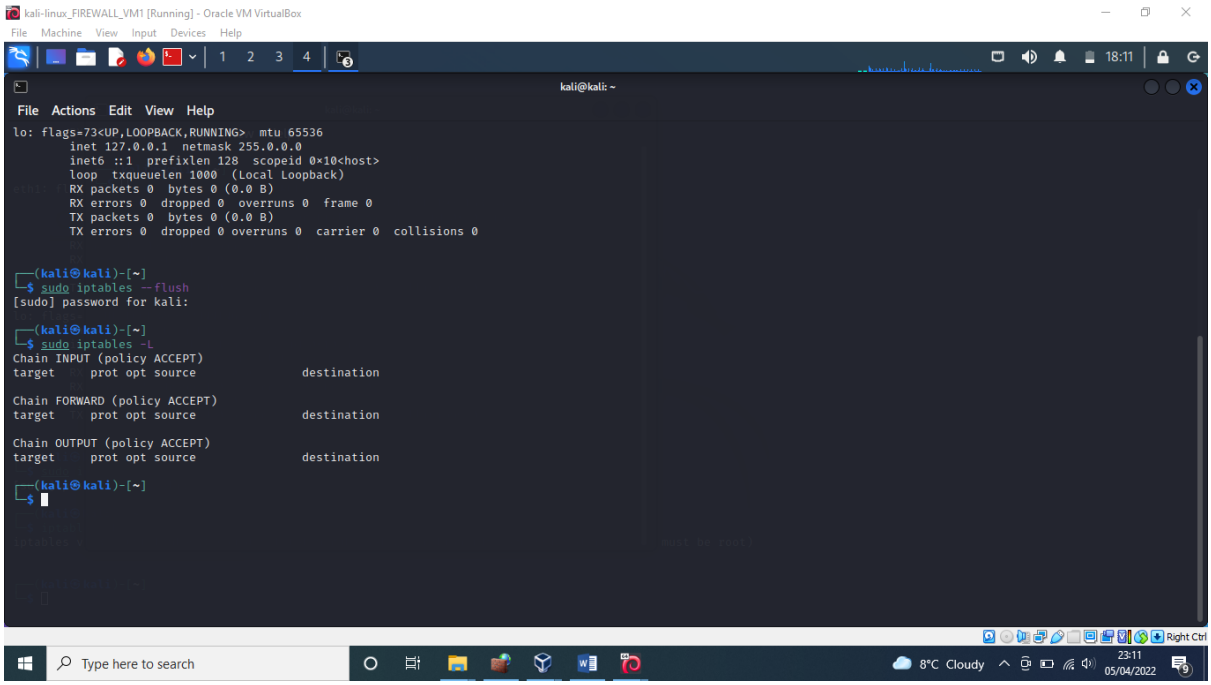


Step 4 Delete firewall rules on VM1

On VM1, type:

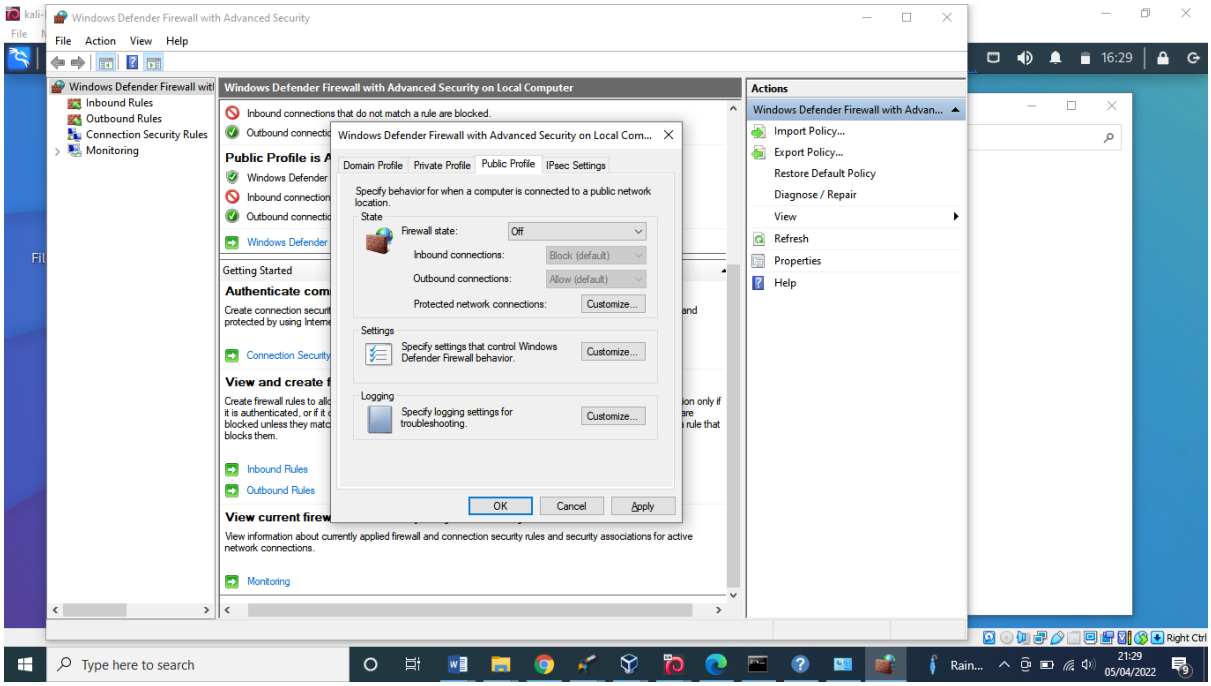
sudo iptables --flush (and type password)

sudo iptables –L

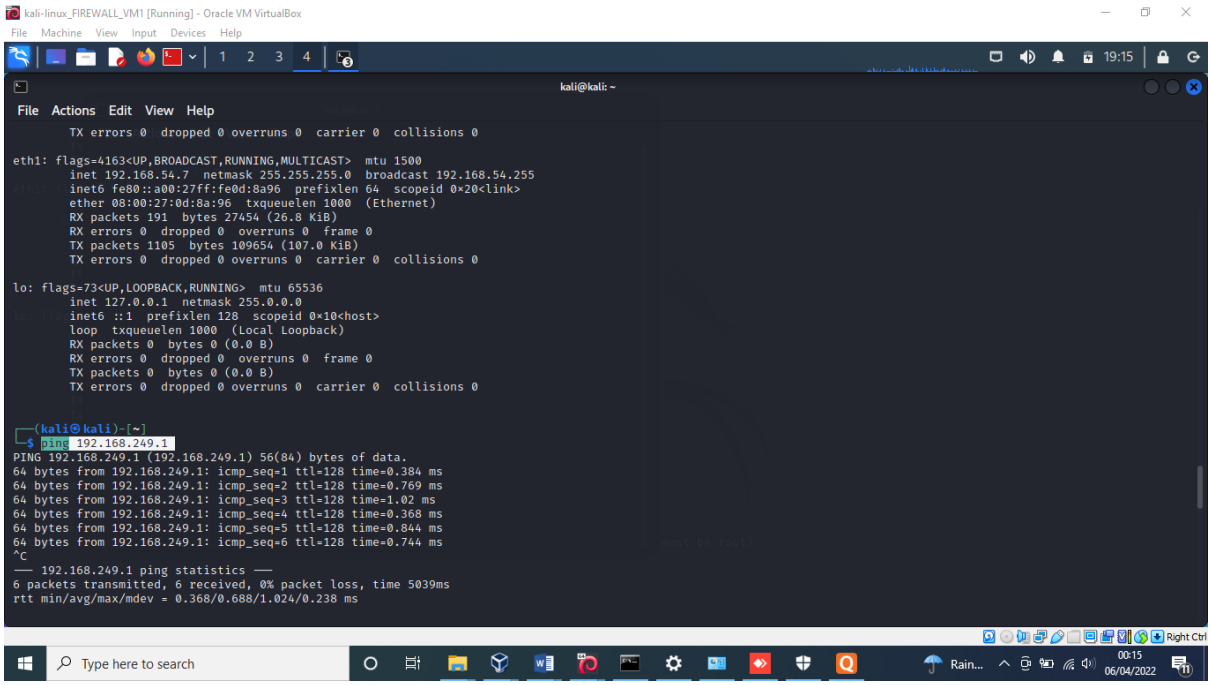


Step 5: Ping host from VM1

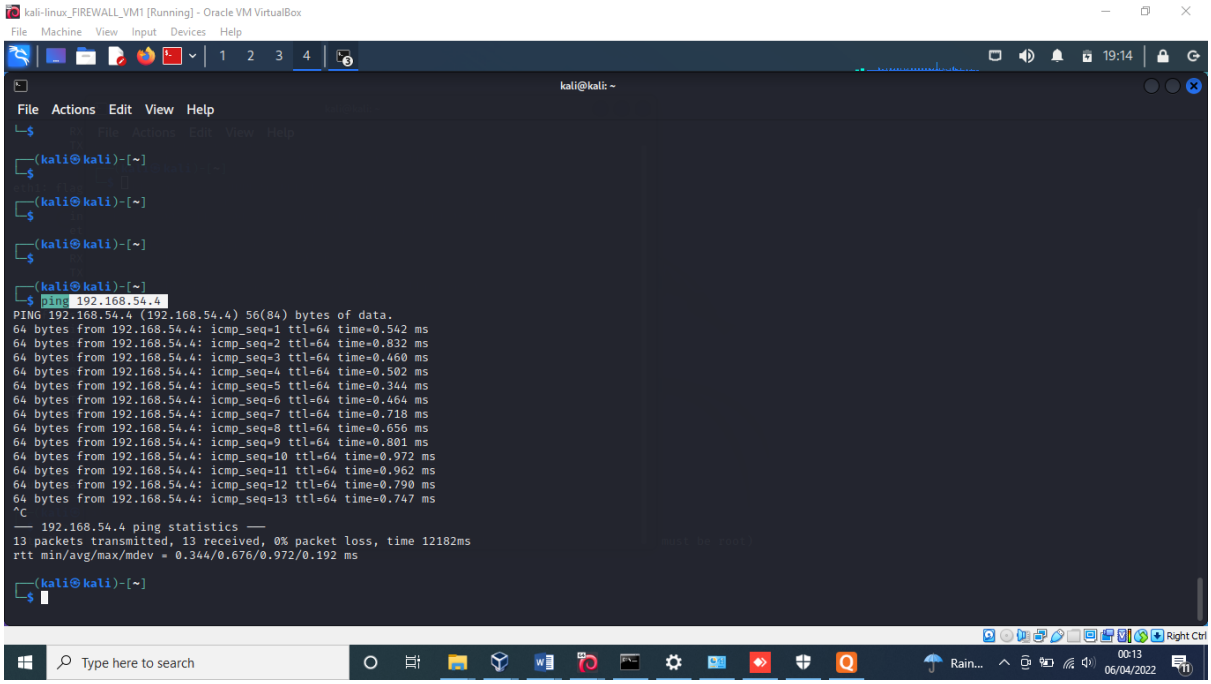
Remember to turn off your host system firewall



Now go to VM1 Firewall and ping the host (which is 192.168.249.1)



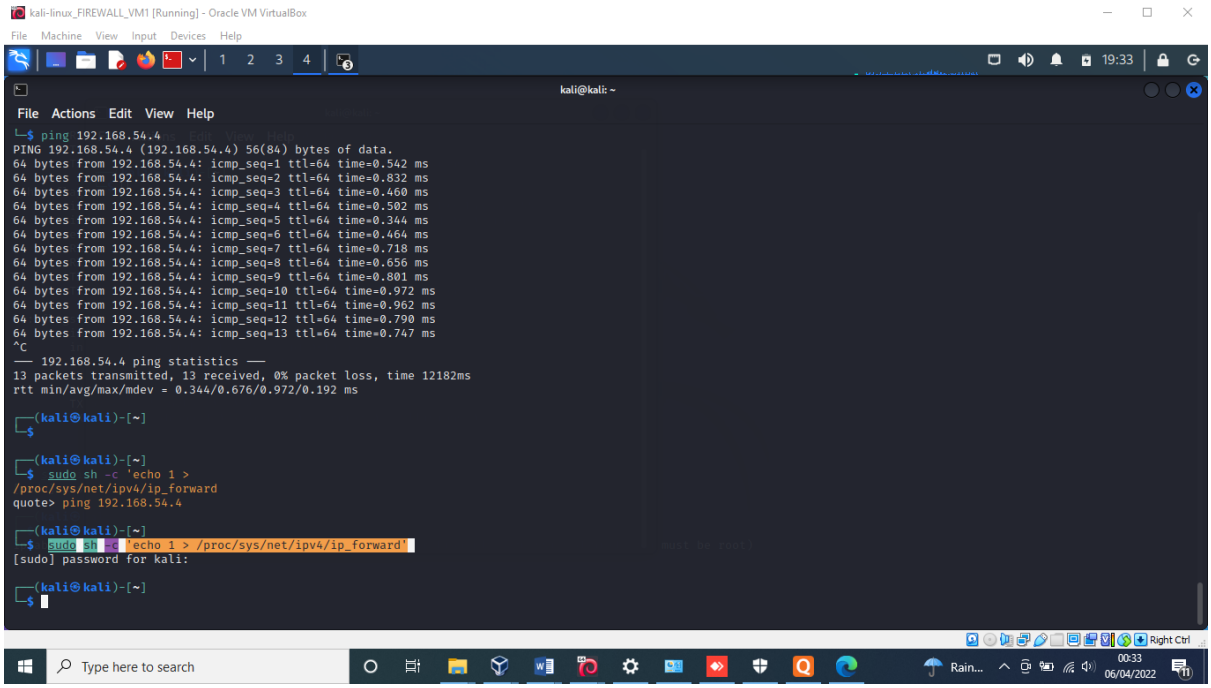
And from VM1 also ping VM2



These successful ping means that

Step

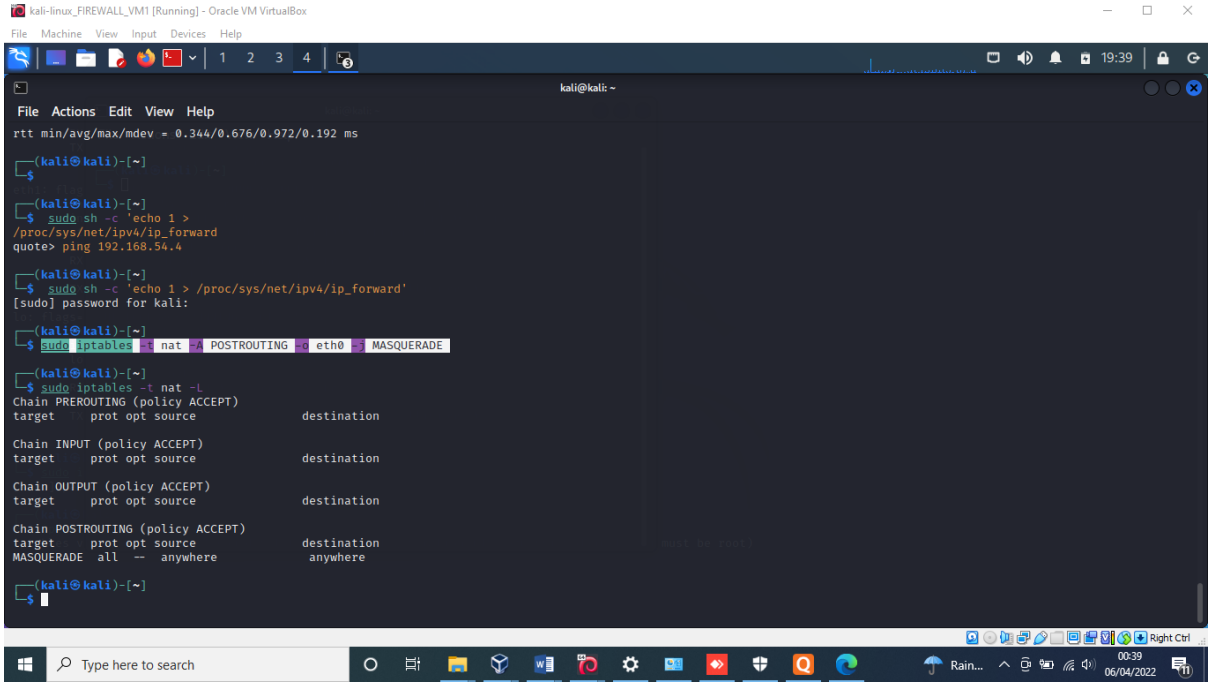
Enable IP forward on VM1



Step

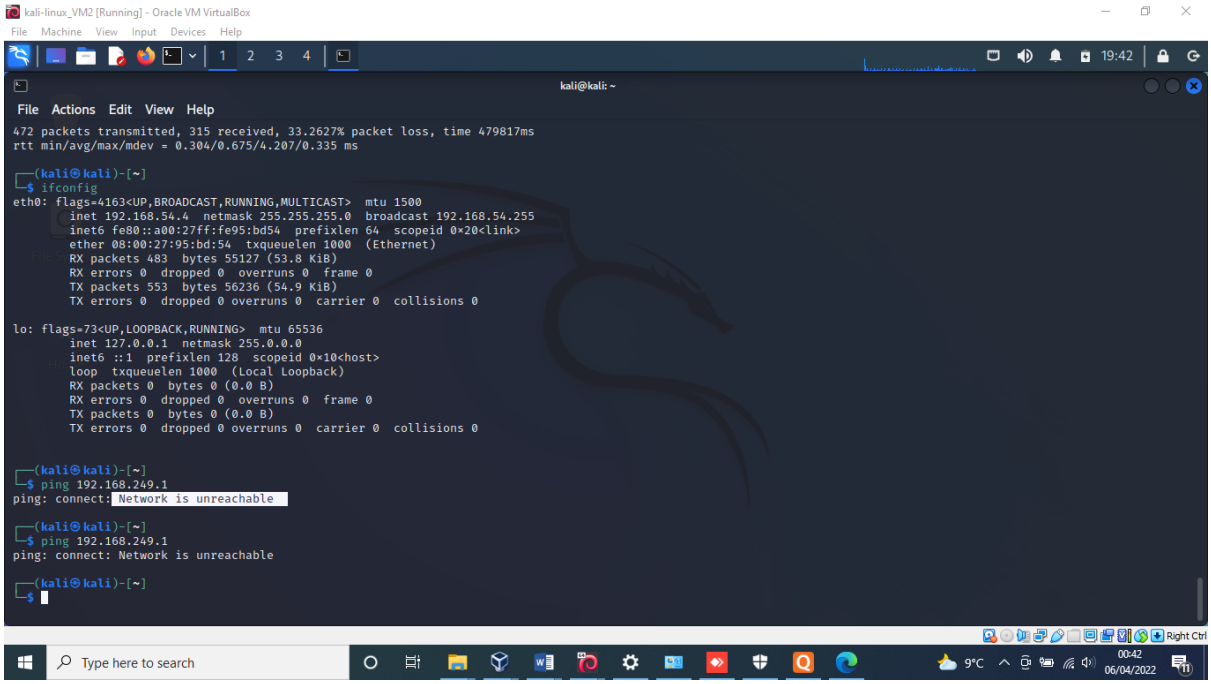
Enable NAT on VM1

Note that NAT (Network Address Translation) to change the source IP of the packets going through the firewall, so that the destination knows where to send the response (to the firewall)

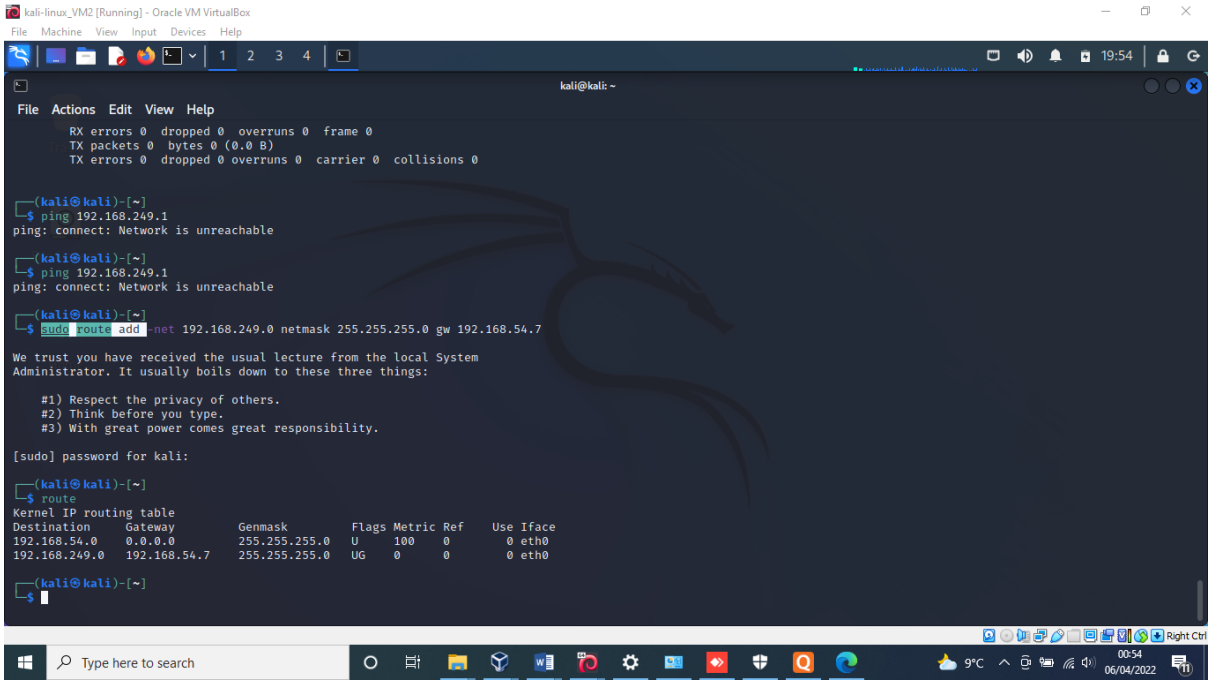


Step: Try to ping the host from VM2

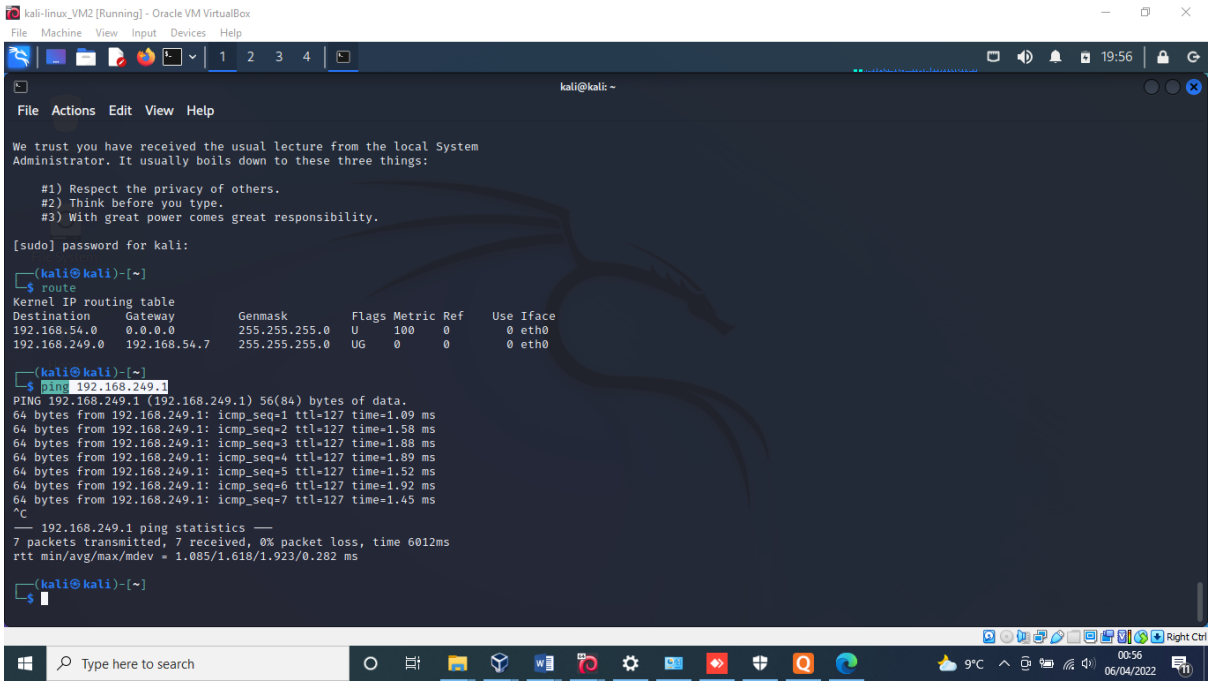
The Network is unreachable as show below. This is because host and VM2 are not on the same network and there is no route to reach host from VM2 yet



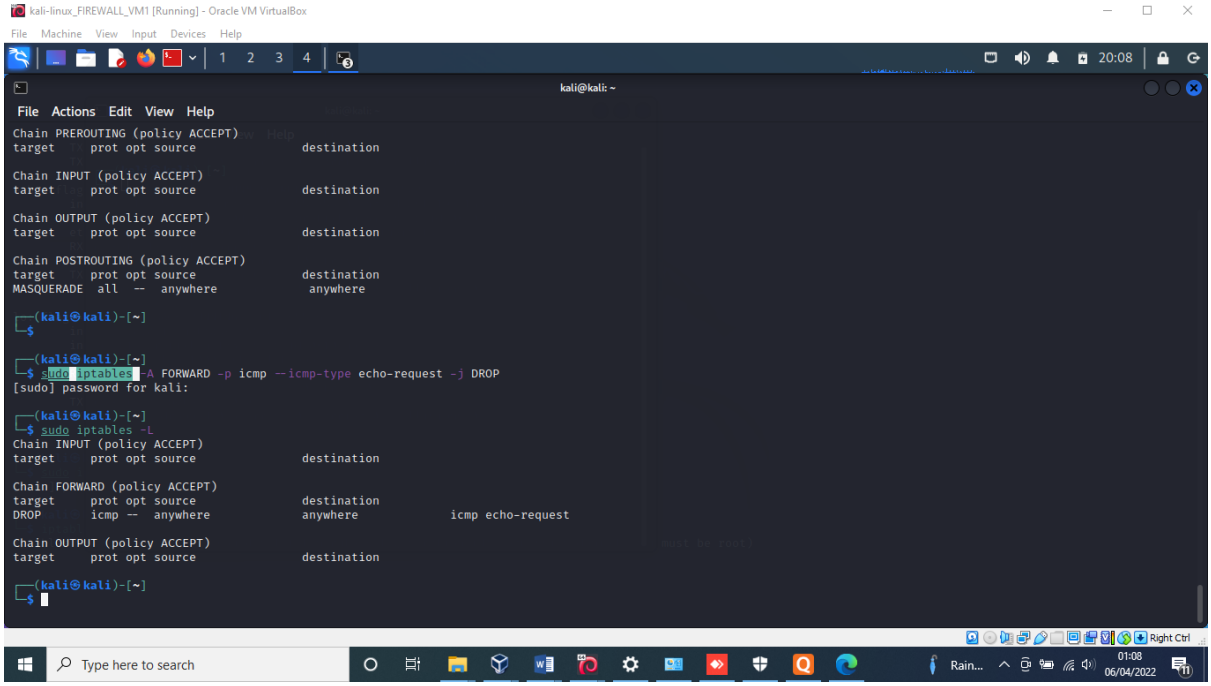
Step: Next add route on VM2 and ping host again



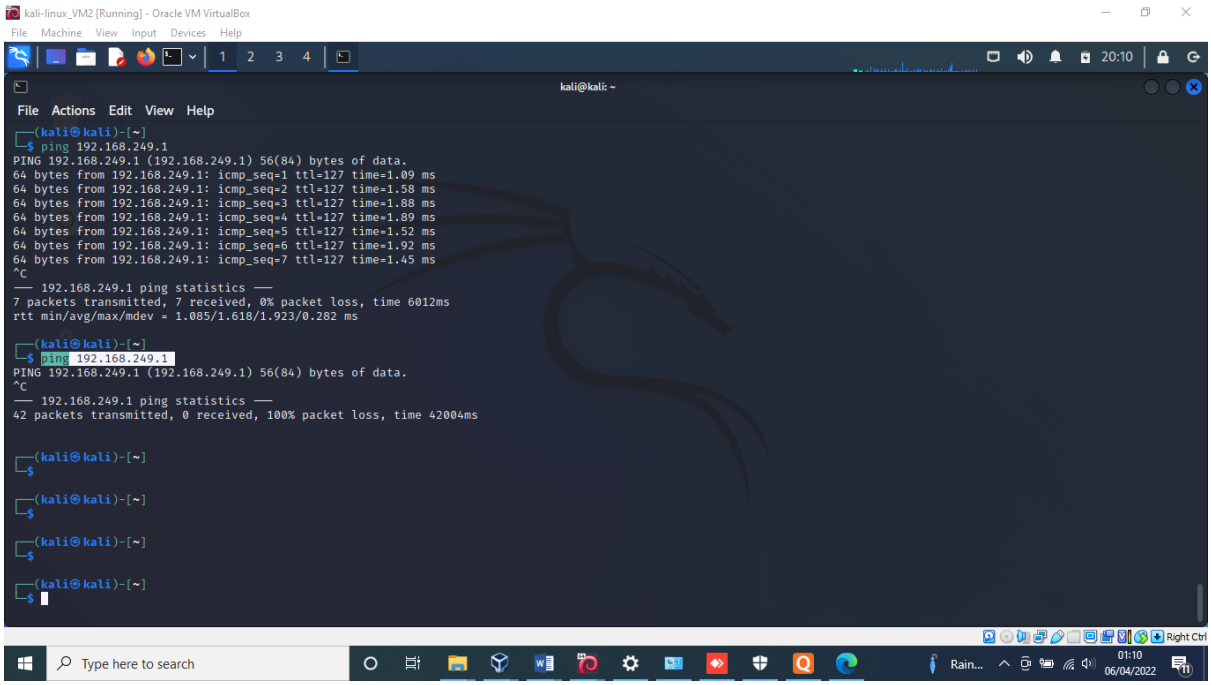
The ping result to the host is now successful



Step: The next step is to create a firewall rule on VM1 to deny ICMP messages



Step: Final step is to try to ping the host from VM2 again



The ICMP request is dropped, confirming that our firewall rule is active