

FIREWALL LAB

Introduction:

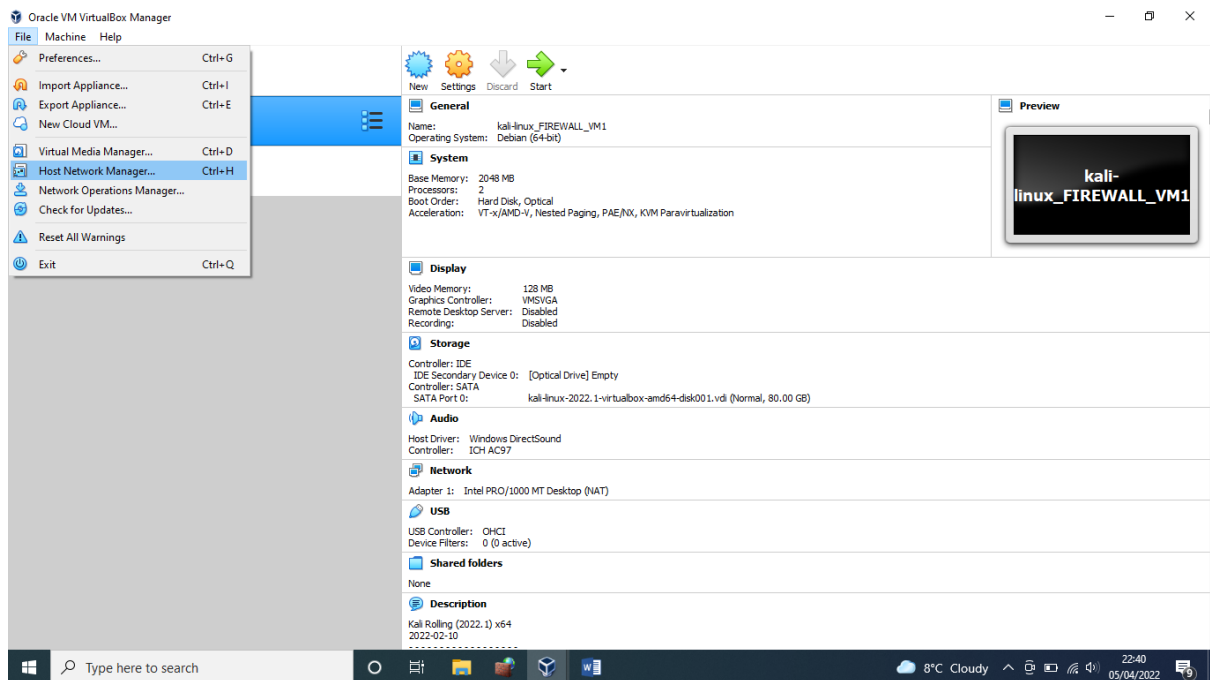
This serves as a comprehensive guide outlining the process of setting up a firewall on a virtual machine and configuring a corresponding firewall rule. Additionally, visual assistance in the form of screenshots is included to offer guidance for those interested in following the steps.

Pre-steps

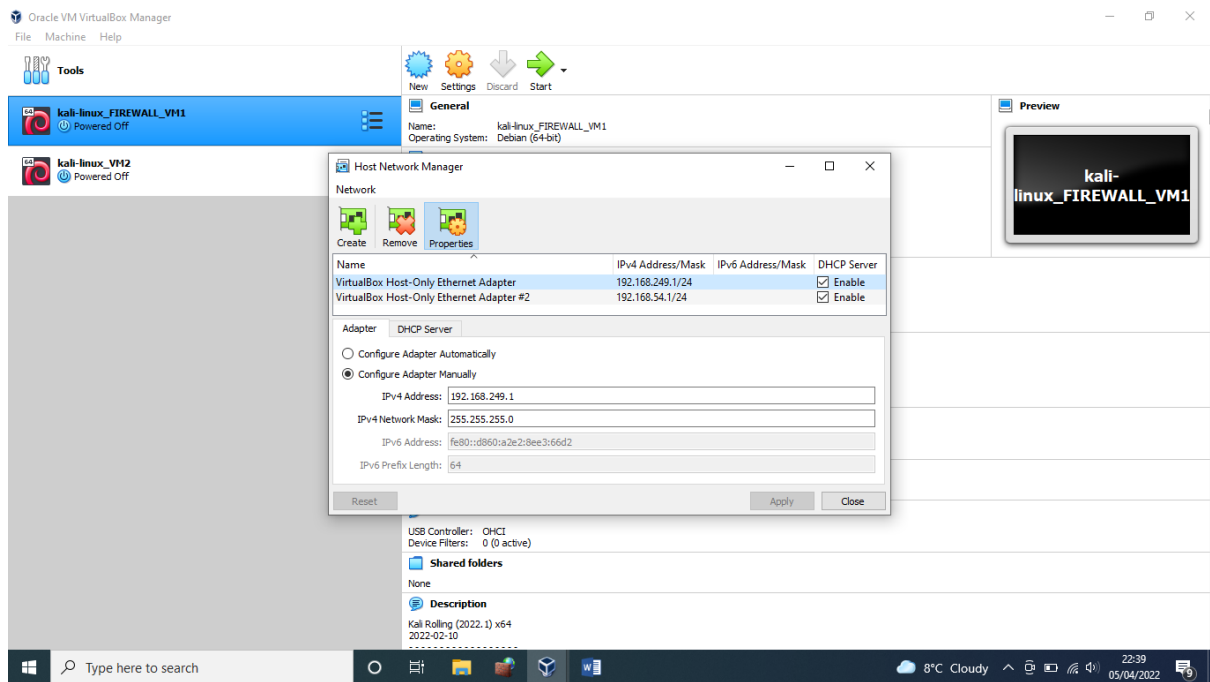
1. Install Oracle Virtualbox/ Vmware on your host system(here my host is a windows machine)
2. Download Kali Linux OS for virtualbox and import it and save as firewall VM1
3. Clone the VM1 and save new Virtualbox as VM2

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



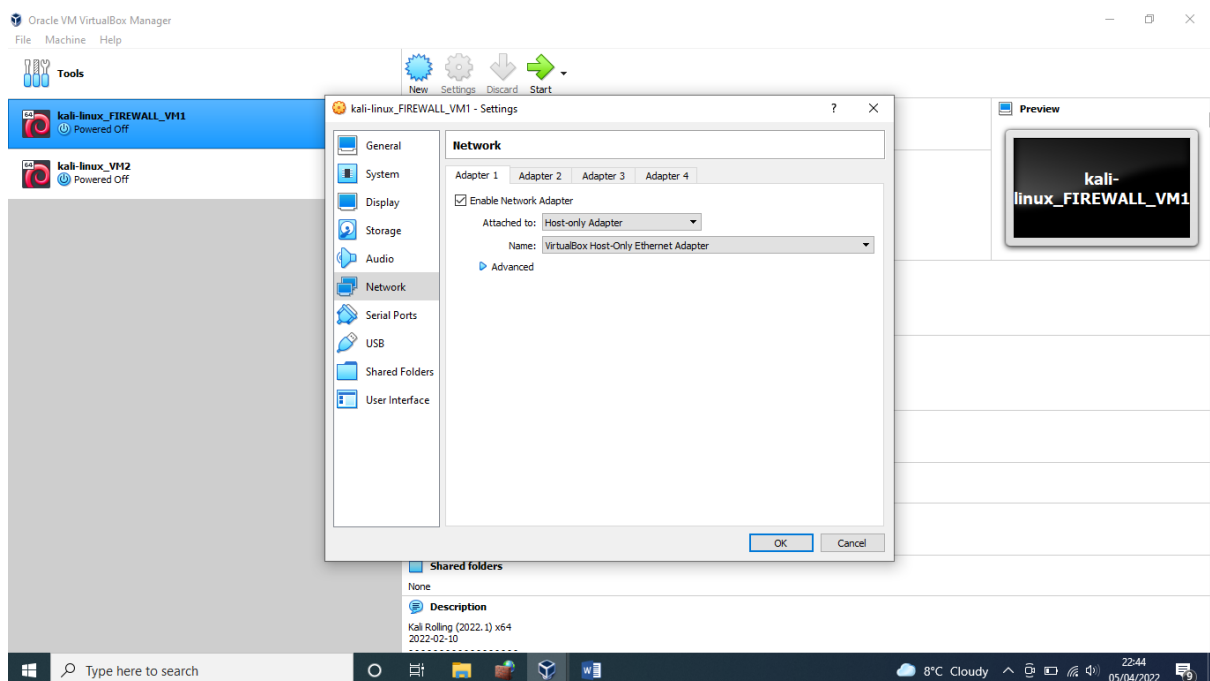
Step 2-

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)

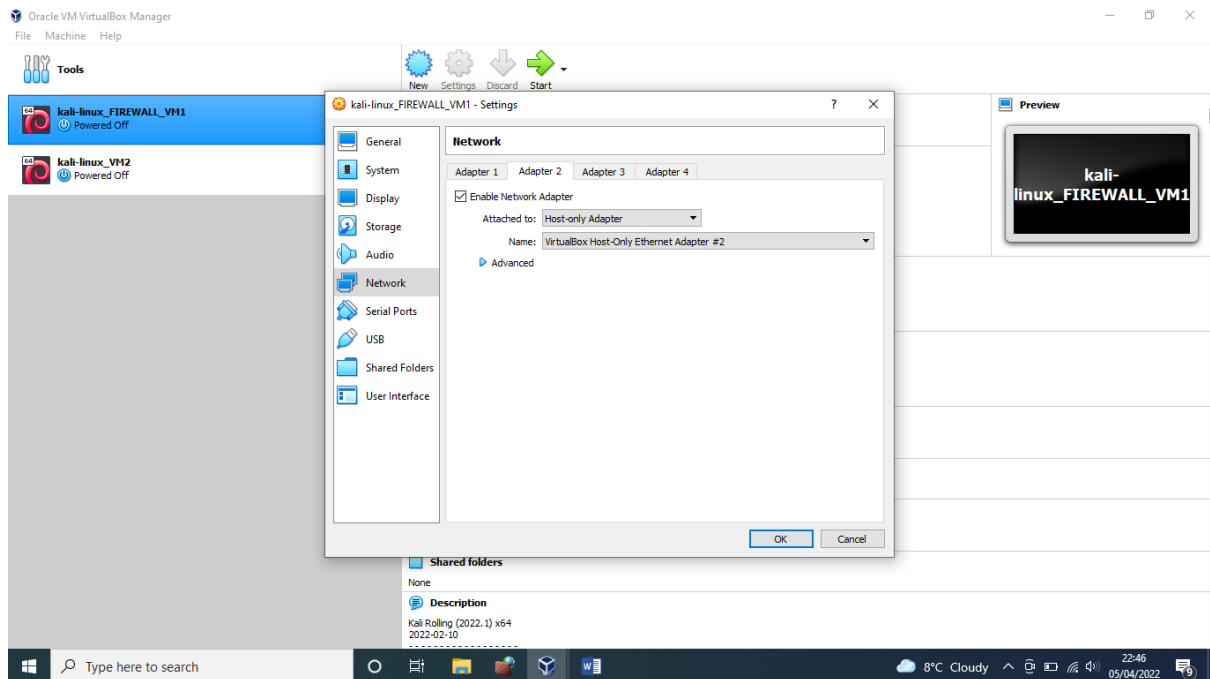


b) Configure network adapter 2 for VM1-Firewall

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)

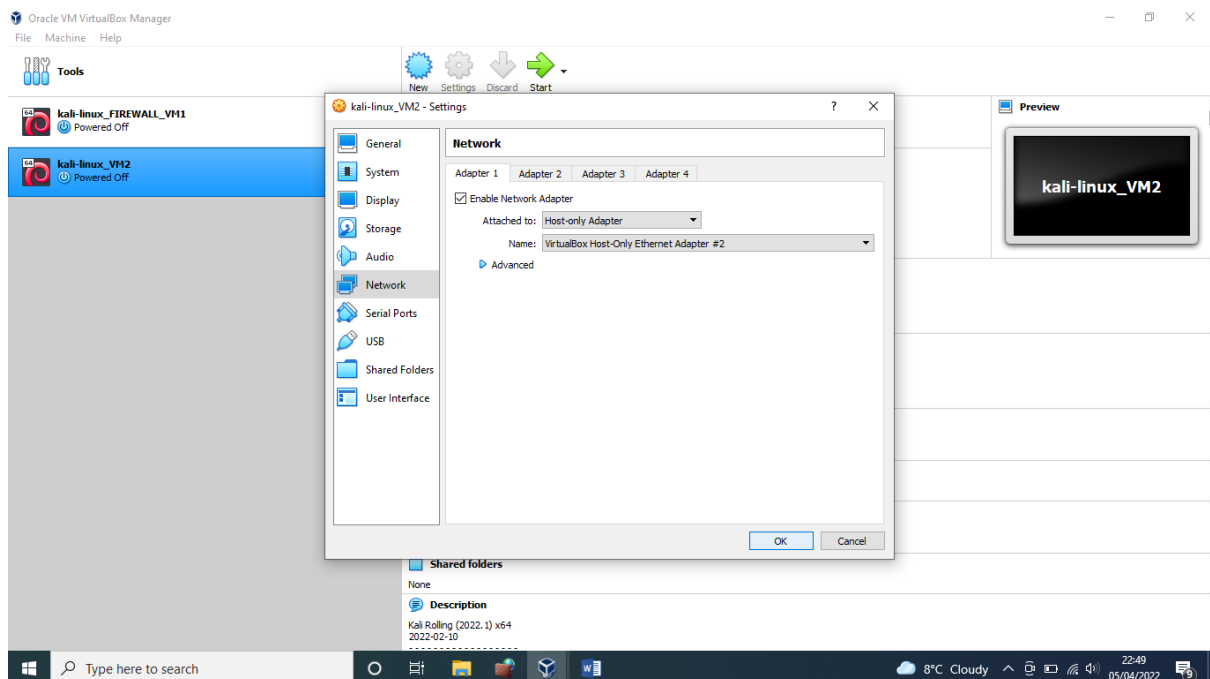


c) Configure network adapter for VM2

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

Attached to: Host-only adapter

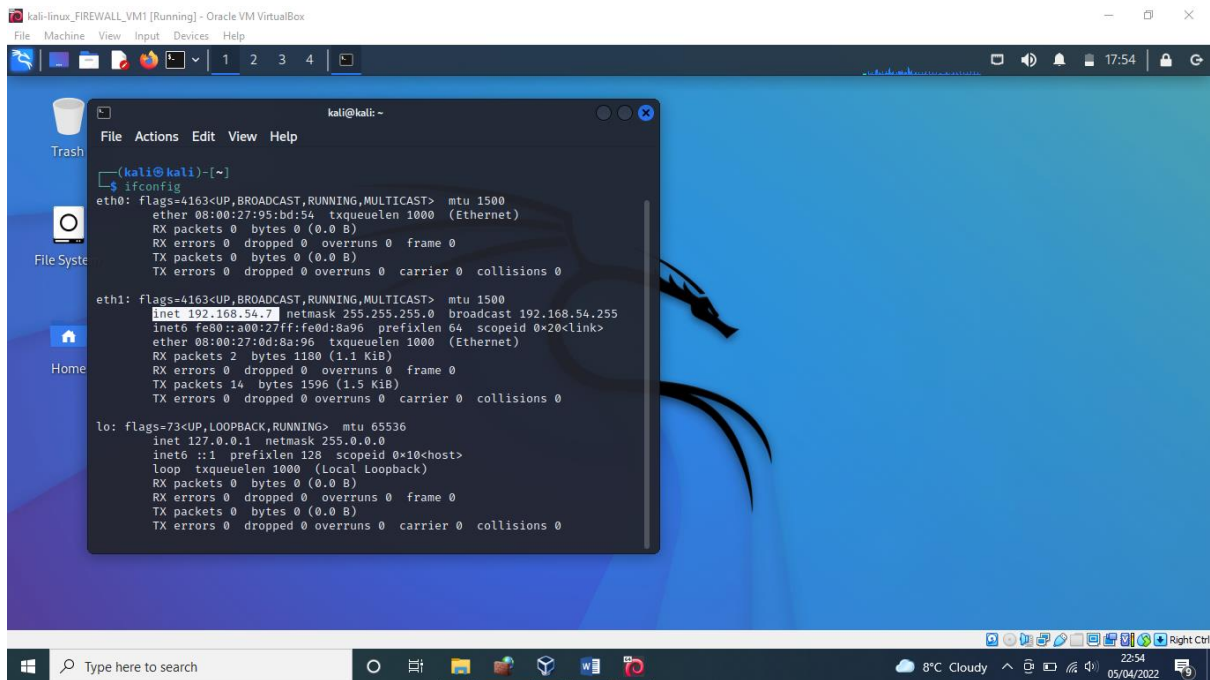
Name: select VirtualBox Host-only Ethernet adapter#2 (as shown below)



Step 3:

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

Go to terminal emulator and type ifconfig

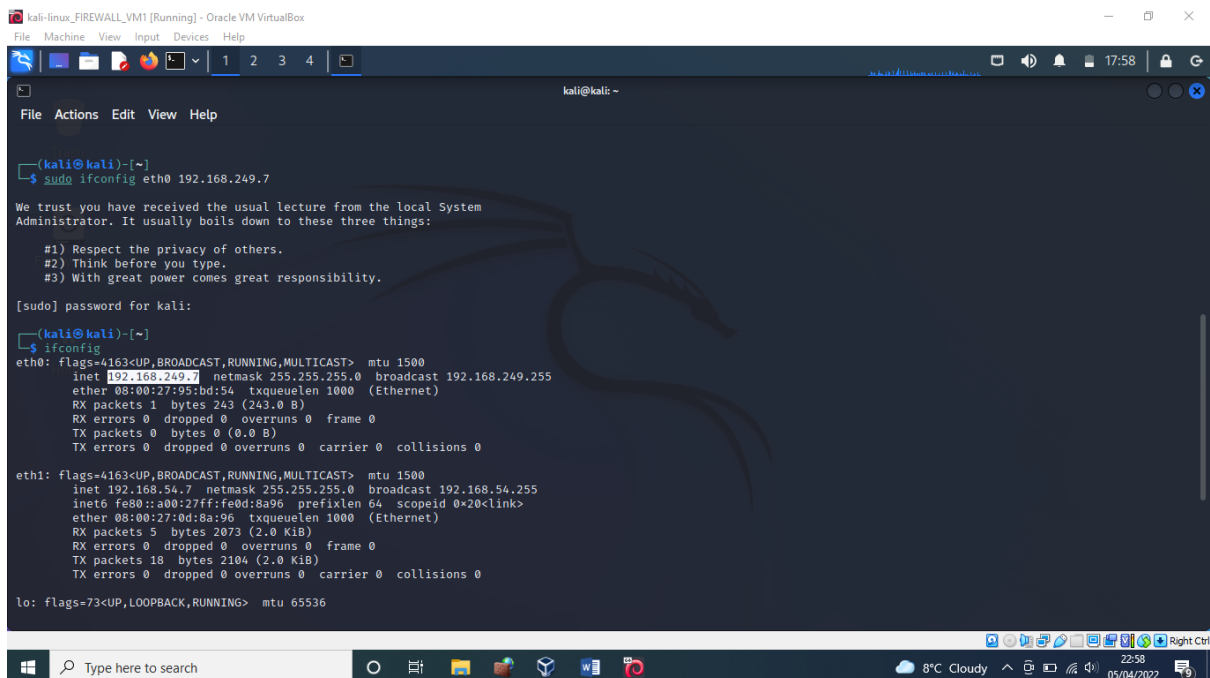


```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.54.7 netmask 255.255.255.0 broadcast 192.168.54.255
    inet6 fe80::a00:27ff:fe0d:8a96 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0d:8a:96 txqueuelen 1000 (Ethernet)
    RX packets 2 bytes 1180 (1.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14 bytes 1596 (1.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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)



```
kali@kali:~$ sudo ifconfig eth0 192.168.249.7
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

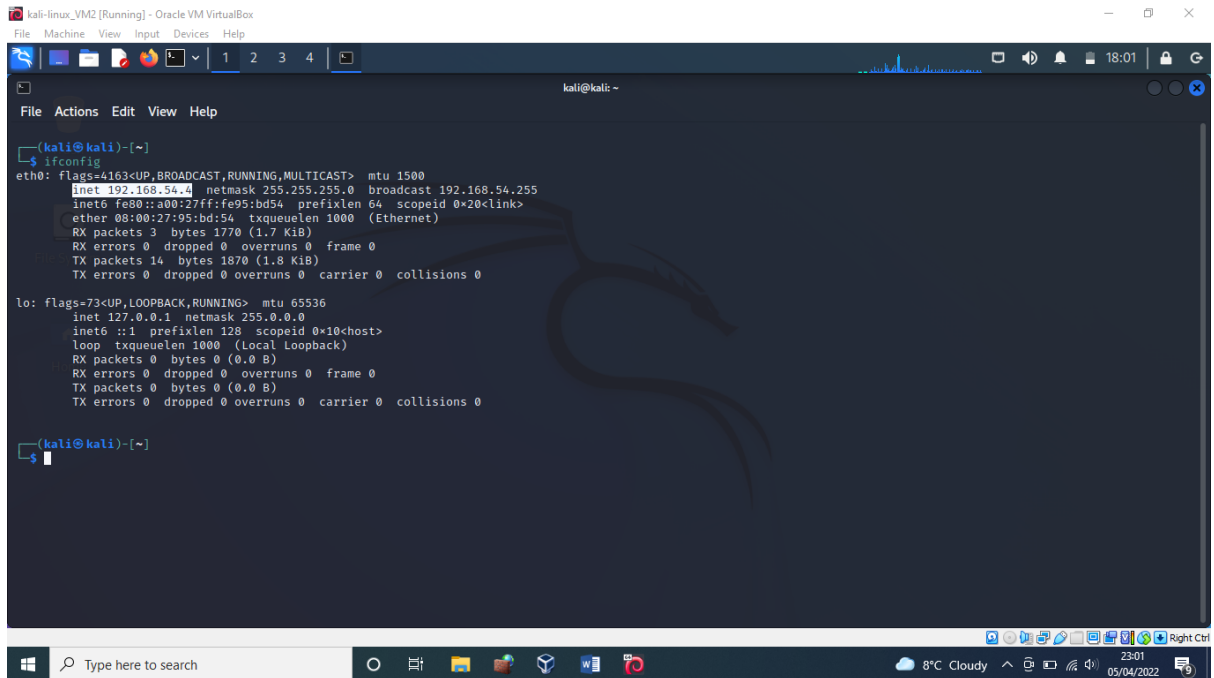
[sudo] password for kali:
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.249.7 netmask 255.255.255.0 broadcast 192.168.249.255
    ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 243 (243.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.54.7 netmask 255.255.255.0 broadcast 192.168.54.255
    inet6 fe80::a00:27ff:fe0d:8a96 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0d:8a:96 txqueuelen 1000 (Ethernet)
    RX packets 5 bytes 2073 (2.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 2104 (2.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
```

b) Power the VM2 and check the IP address

Go to terminal emulator and type ifconfig



```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.54.4 netmask 255.255.255.0 broadcast 192.168.54.255
    inet6 fe80::a00:27ff:fe95:bd54 prefixlen 64 scopeid 0<link>
    ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)
    RX packets 3 bytes 1770 (1.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14 bytes 1870 (1.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

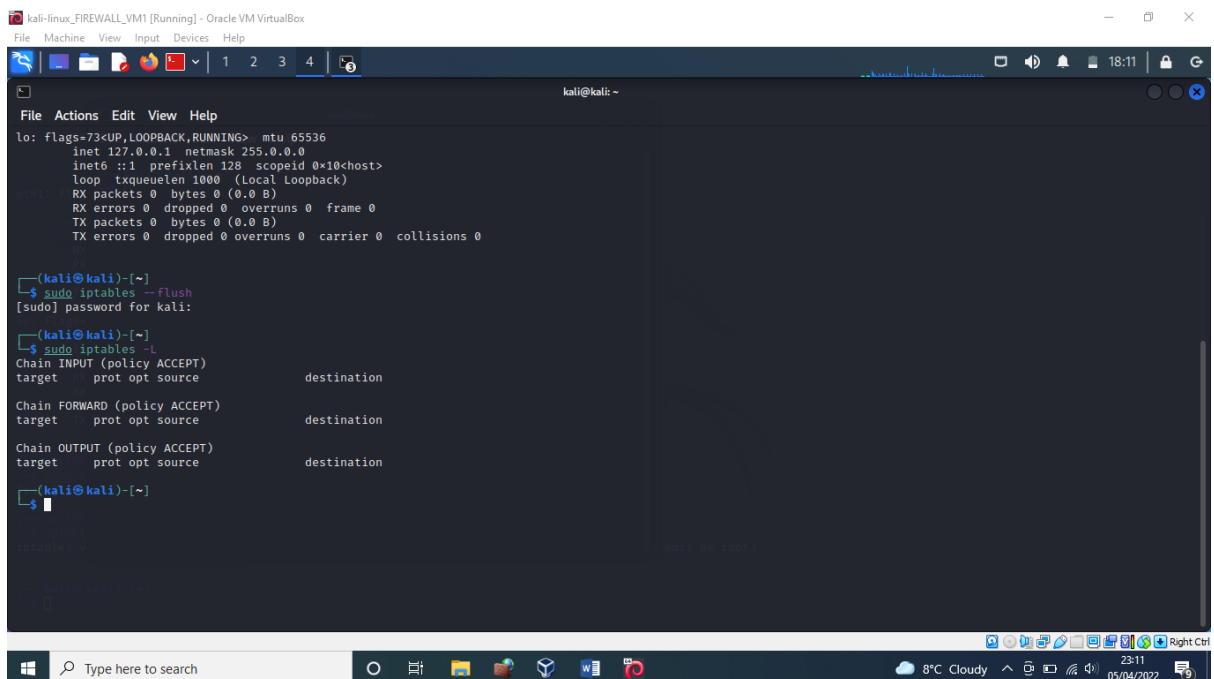
kali@kali:~$
```

Step 4 Delete firewall rules on VM1

On VM1, type:

`sudo iptables --flush` (and type password)

`sudo iptables -L`



```
kali@kali:~$ sudo iptables --flush
[sudo] password for kali:
kali@kali:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination

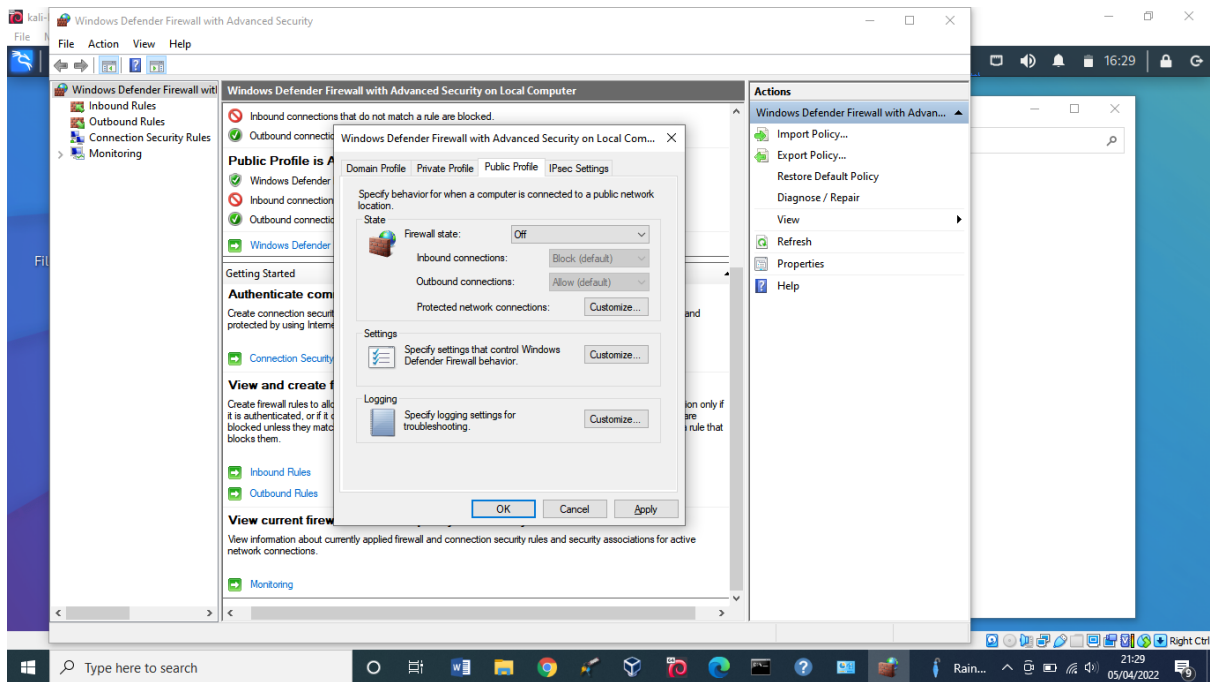
Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

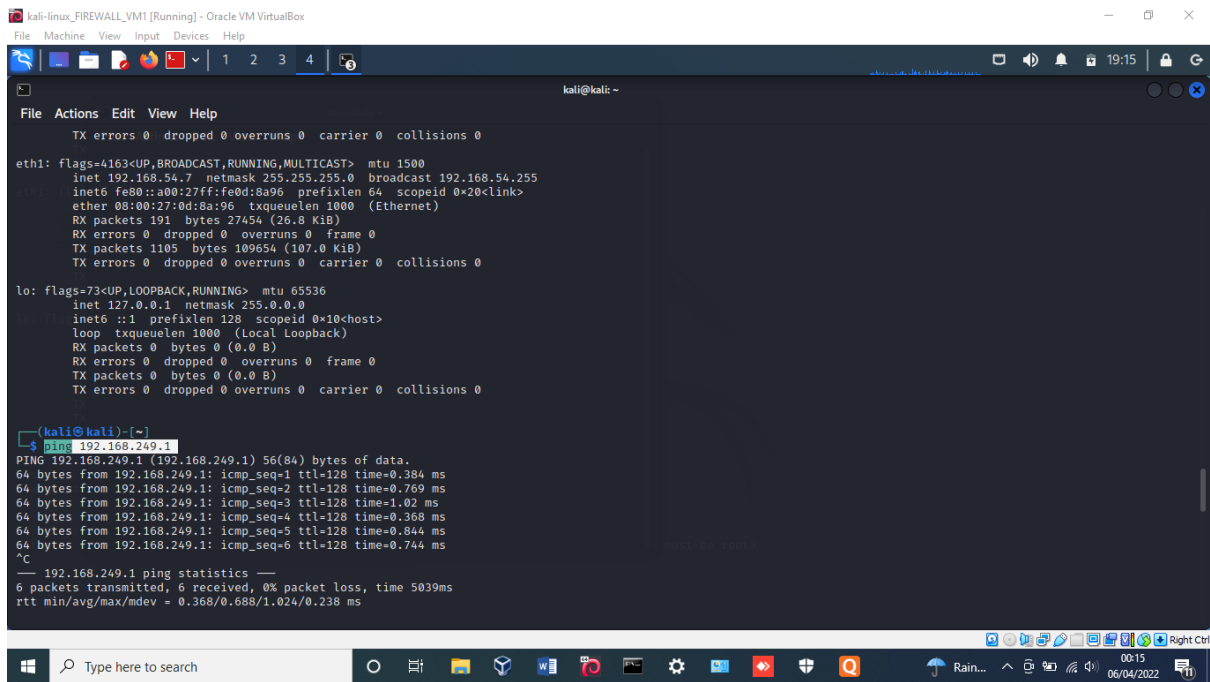
kali@kali:~$
```

Step 5: Ping host from VM1

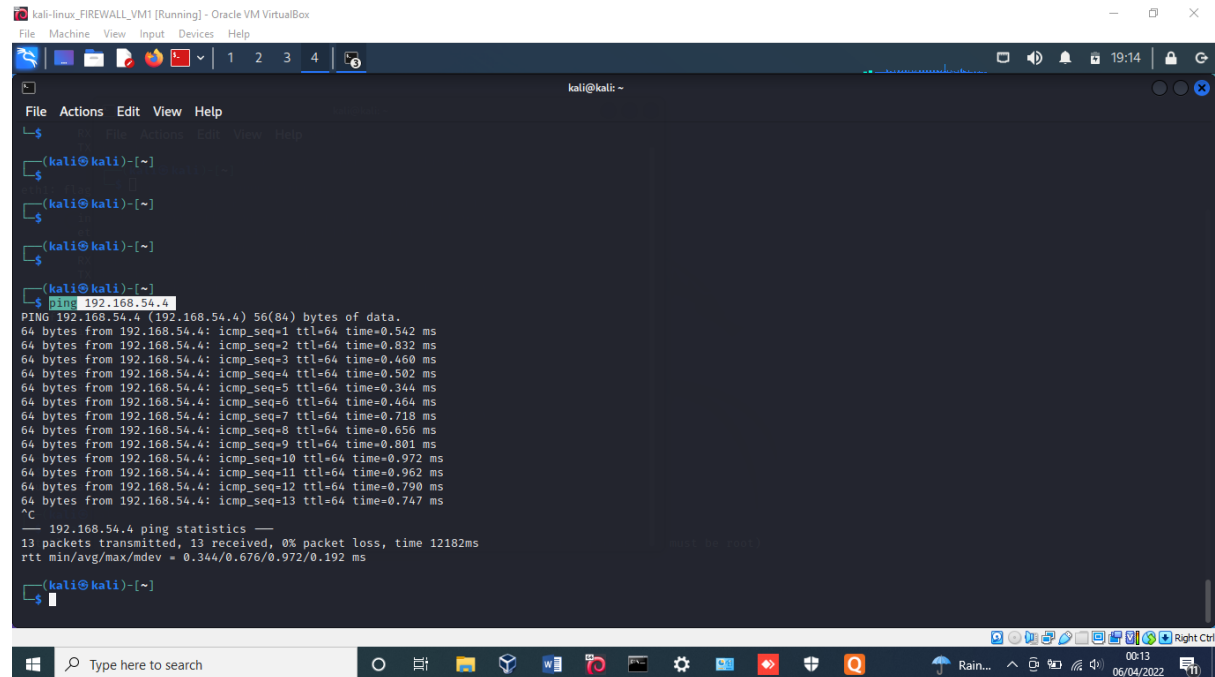
Remember to turn off your host system firewall



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



And from VM1 also ping VM2

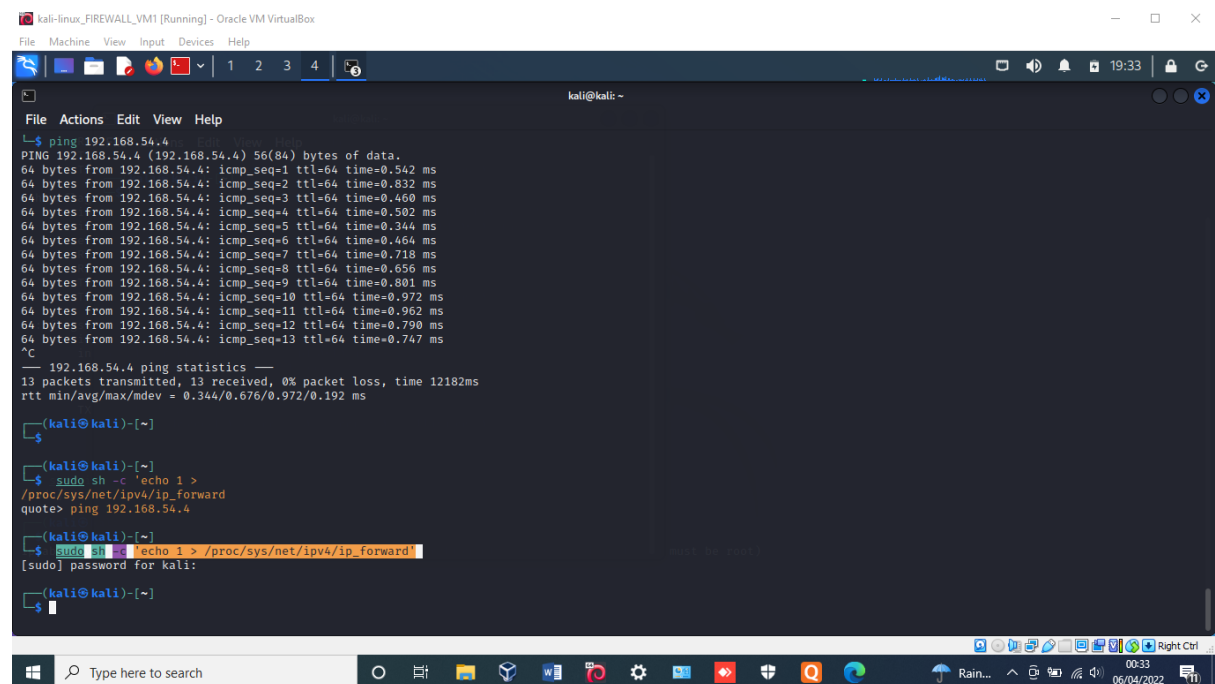


```
kali@kali: ~  
File Actions Edit View Help  
└─$  
└─$  
└─$  
└─$  
└─$ ping 192.168.54.4  
PING 192.168.54.4 (192.168.54.4) 56(84) bytes of data:  
64 bytes from 192.168.54.4: icmp_seq=1 ttl=64 time=0.542 ms  
64 bytes from 192.168.54.4: icmp_seq=2 ttl=64 time=0.832 ms  
64 bytes from 192.168.54.4: icmp_seq=3 ttl=64 time=0.460 ms  
64 bytes from 192.168.54.4: icmp_seq=4 ttl=64 time=0.502 ms  
64 bytes from 192.168.54.4: icmp_seq=5 ttl=64 time=0.344 ms  
64 bytes from 192.168.54.4: icmp_seq=6 ttl=64 time=0.464 ms  
64 bytes from 192.168.54.4: icmp_seq=7 ttl=64 time=0.718 ms  
64 bytes from 192.168.54.4: icmp_seq=8 ttl=64 time=0.656 ms  
64 bytes from 192.168.54.4: icmp_seq=9 ttl=64 time=0.801 ms  
64 bytes from 192.168.54.4: icmp_seq=10 ttl=64 time=0.972 ms  
64 bytes from 192.168.54.4: icmp_seq=11 ttl=64 time=0.962 ms  
64 bytes from 192.168.54.4: icmp_seq=12 ttl=64 time=0.790 ms  
64 bytes from 192.168.54.4: icmp_seq=13 ttl=64 time=0.747 ms  
^C  
--- 192.168.54.4 ping statistics ---  
13 packets transmitted, 13 received, 0% packet loss, time 12182ms  
rtt min/avg/max/mdev = 0.344/0.676/0.972/0.192 ms  
└─$
```

These successful ping means that

Step

Enable IP forward on VM1



```
kali@kali: ~  
File Actions Edit View Help  
└─$ ping 192.168.54.4  
PING 192.168.54.4 (192.168.54.4) 56(84) bytes of data:  
64 bytes from 192.168.54.4: icmp_seq=1 ttl=64 time=0.542 ms  
64 bytes from 192.168.54.4: icmp_seq=2 ttl=64 time=0.832 ms  
64 bytes from 192.168.54.4: icmp_seq=3 ttl=64 time=0.460 ms  
64 bytes from 192.168.54.4: icmp_seq=4 ttl=64 time=0.502 ms  
64 bytes from 192.168.54.4: icmp_seq=5 ttl=64 time=0.344 ms  
64 bytes from 192.168.54.4: icmp_seq=6 ttl=64 time=0.464 ms  
64 bytes from 192.168.54.4: icmp_seq=7 ttl=64 time=0.718 ms  
64 bytes from 192.168.54.4: icmp_seq=8 ttl=64 time=0.656 ms  
64 bytes from 192.168.54.4: icmp_seq=9 ttl=64 time=0.801 ms  
64 bytes from 192.168.54.4: icmp_seq=10 ttl=64 time=0.972 ms  
64 bytes from 192.168.54.4: icmp_seq=11 ttl=64 time=0.962 ms  
64 bytes from 192.168.54.4: icmp_seq=12 ttl=64 time=0.790 ms  
64 bytes from 192.168.54.4: icmp_seq=13 ttl=64 time=0.747 ms  
^C  
--- 192.168.54.4 ping statistics ---  
13 packets transmitted, 13 received, 0% packet loss, time 12182ms  
rtt min/avg/max/mdev = 0.344/0.676/0.972/0.192 ms  
└─$  
└─$ sudo sh -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'  
quote> ping 192.168.54.4  
└─$  
└─$ sudo sh -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'  
[sudo] password for kali:  
└─$
```

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)

```
kali-linux_FIREWALL_VM1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali ~
File Actions Edit View Help
rtt min/avg/max/mdev = 0.344/0.676/0.972/0.192 ms
kali@kali-[-~]
$
kali@kali-[-~]
$ sudo sh -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'
quote> ping 192.168.54.4
kali@kali-[-~]
$ sudo sh -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'
[sudo] password for kali:
kali@kali-[-~]
$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
kali@kali-[-~]
$ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain POSTROUTING (policy ACCEPT)
target prot opt source destination
MASQUERADE all -- anywhere anywhere
kali@kali-[-~]
$
```

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

```
kali-linux_VM2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali ~
File Actions Edit View Help
472 packets transmitted, 315 received, 33.2627% packet loss, time 479817ms
rtt min/avg/max/mdev = 0.304/0.675/4.207/0.335 ms
kali@kali-[-~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.54.4 netmask 255.255.255.0 broadcast 192.168.54.255
    inet6 fe80::a00:27ff:fe95:bd54 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)
    RX packets 483 bytes 55127 (53.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 553 bytes 56236 (54.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali-[-~]
$ ping 192.168.249.1
ping: connect: Network is unreachable
kali@kali-[-~]
$ ping 192.168.249.1
ping: connect: Network is unreachable
kali@kali-[-~]
$
```

Step: Next add route on VM2 and ping host again


```
kali-linux_VM2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali ~
File Actions Edit View Help

RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ ping 192.168.249.1
ping: connect: Network is unreachable

(kali@kali)-[~]
$ ping 192.168.249.1
ping: connect: Network is unreachable

(kali@kali)-[~]
$ sudo route add -net 192.168.249.0 netmask 255.255.255.0 gw 192.168.54.7

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for kali:
(kali@kali)-[~]
$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.54.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
192.168.249.0 192.168.54.7 255.255.255.0 UG 0 0 0 eth0

(kali@kali)-[~]
$
```

The ping result to the host is now successful

```
kali-linux_VM2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali ~
File Actions Edit View Help

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for kali:
(kali@kali)-[~]
$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.54.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
192.168.249.0 192.168.54.7 255.255.255.0 UG 0 0 0 eth0

(kali@kali)-[~]
$ ping 192.168.249.1
PING 192.168.249.1 (192.168.249.1) 56(84) bytes of data:
64 bytes from 192.168.249.1: icmp_seq=1 ttl=127 time=1.09 ms
64 bytes from 192.168.249.1: icmp_seq=2 ttl=127 time=1.58 ms
64 bytes from 192.168.249.1: icmp_seq=3 ttl=127 time=1.88 ms
64 bytes from 192.168.249.1: icmp_seq=4 ttl=127 time=1.89 ms
64 bytes from 192.168.249.1: icmp_seq=5 ttl=127 time=1.52 ms
64 bytes from 192.168.249.1: icmp_seq=6 ttl=127 time=1.92 ms
64 bytes from 192.168.249.1: icmp_seq=7 ttl=127 time=1.45 ms
^C
--- 192.168.249.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6012ms
rtt min/avg/max/mdev = 1.085/1.618/1.923/0.282 ms

(kali@kali)-[~]
$
```

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

```
kali-linux_FIREWALL_VM1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali ~
File Actions Edit View Help
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain POSTROUTING (policy ACCEPT)
target prot opt source destination
MASQUERADE all -- anywhere
(kali@kali)-[~]
$
(kali@kali)-[~]
$ sudo iptables -A FORWARD -p icmp --icmp-type echo-request -j DROP
[sudo] password for kali:
(kali@kali)-[~]
$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
DROP icmp -- anywhere anywhere icmp echo-request
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
(kali@kali)-[~]
$
```

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

```
kali-linux_VM2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali ~
File Actions Edit View Help
(kali@kali)-[~]
$ ping 192.168.249.1
PING 192.168.249.1 (192.168.249.1) 56(84) bytes of data:
64 bytes from 192.168.249.1: icmp_seq=1 ttl=127 time=1.09 ms
64 bytes from 192.168.249.1: icmp_seq=2 ttl=127 time=1.58 ms
64 bytes from 192.168.249.1: icmp_seq=3 ttl=127 time=1.88 ms
64 bytes from 192.168.249.1: icmp_seq=4 ttl=127 time=1.89 ms
64 bytes from 192.168.249.1: icmp_seq=5 ttl=127 time=1.52 ms
64 bytes from 192.168.249.1: icmp_seq=6 ttl=127 time=1.92 ms
64 bytes from 192.168.249.1: icmp_seq=7 ttl=127 time=1.45 ms
^C
--- 192.168.249.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6012ms
rtt min/avg/max/mdev = 1.085/1.618/1.923/0.282 ms
(kali@kali)-[~]
$ ping 192.168.249.1
PING 192.168.249.1 (192.168.249.1) 56(84) bytes of data.
^C
--- 192.168.249.1 ping statistics ---
42 packets transmitted, 0 received, 100% packet loss, time 42004ms

(kali@kali)-[~]
$
(kali@kali)-[~]
$
(kali@kali)-[~]
$
(kali@kali)-[~]
$
```

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