Networks and Systems Security (CSE5NSS)

LAB-2 Report

Kaustav Vats (2016048), Sushant Kumar Singh (2016103)

Following IPs are assigned to additional interfaces added to the VMs:
VM1 - 10.0.0.5 (enp0s8)
VM2 - 10.0.0.9 for bridge (br0) and 0.0.0.0 for (enp0s8, enp0s9)
VM3 - 10.0.0.6 (enp0s8)
VM4 - 10.0.0.7 (enp0s8)
VM5 - 10.0.0.8 (enp0s8)

Task 1 We assigned IP 0.0.0.0 to enp0s8, enp0s9 on VM2 using ifconfig
Task 2 We then added bridge on VM2 as shown below using 'brctl addbr br0'
Task 3 Then using 'brctl addif enp0s8', 'brctl addif enp0s9' we added interfaces to the bridge
Task 4 Now VM2 is bridging as required
Task 5 We added IP addresses as mentioned above to the respective interfaces on VM1, 3,4 and 5 in the same subnet 10.0.0.0/24
VM2 Bridge is as added as shown below

Task 6 Now VMs were able to ping as required.

Following snapshot shows that VM1 is able to ping VM5

VM_1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
kvats@kvats:~$ ifconfig 10.0.0.8
10.0.0.8: error fetching interface information: Device not found
kvats@kvats:~$ ping 10.0.0.8
PING 10.0.0.8 (10.0.0.8) 56(84) bytes of data.
64 bytes from 10.0.0.8: icmp_seq=1 ttl=64 time=1.22 ms
64 bytes from 10.0.0.8: icmp_seq=2 ttl=64 time=1.18 ms
64 bytes from 10.0.0.8: icmp_seq=3 ttl=64 time=1.19 ms
64 bytes from 10.0.0.8: icmp_seq=4 ttl=64 time=1.21 ms
64 bytes from 10.0.0.8: icmp_seq=5 ttl=64 time=1.49 ms
64 bytes from 10.0.0.8: icmp_seq=6 ttl=64 time=1.19 ms
^C
--- 10.0.0.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 1.181/1.251/1.499/0.117 ms
kvats@kvats:~$ ifconfig 10.0.0.8
10.0.0.8: error fetching interface information: Device not found
kvats@kvats:~$ ping 10.0.0.8
PING 10.0.0.8 (10.0.0.8) 56(84) bytes of data.
64 bytes from 10.0.0.8: icmp_seq=1 ttl=64 time=0.706 ms
64 bytes from 10.0.0.8: icmp_seq=2 ttl=64 time=1.20 ms
64 bytes from 10.0.0.8: icmp_seq=3 ttl=64 time=1.22 ms
64 bytes from 10.0.0.8: icmp_seq=4 ttl=64 time=1.31 ms
64 bytes from 10.0.0.8: icmp_seq=5 ttl=64 time=1.27 ms
64 bytes from 10.0.0.8: icmp_seq=6 ttl=64 time=1.33 ms
^C
--- 10.0.0.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5010ms
rtt min/avg/max/mdev = 0.706/1.174/1.332/0.218 ms
kvats@kvats:~$ traceroute 10.0.0.8
traceroute to 10.0.0.8 (10.0.0.8), 30 hops max, 60 byte packets
 1  10.0.0.8 (10.0.0.8)  0.479 ms  0.419 ms  0.378 ms
kvats@kvats:~$
```

Following snapshot shows that VM4 is able to ping VM1

VM_4 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.7  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::a00:27ff:fe0c:1695  prefixlen 64  scopeid 0x20<
        ether 08:00:27:0c:16:95  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9  bytes 726 (726.0 B)
        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 116  bytes 8444 (8.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 116  bytes 8444 (8.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kvats@kvats:~$ ping 10.0.0.5
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
64 bytes from 10.0.0.5: icmp_seq=1 ttl=64 time=1.12 ms
64 bytes from 10.0.0.5: icmp_seq=2 ttl=64 time=1.21 ms
64 bytes from 10.0.0.5: icmp_seq=3 ttl=64 time=1.15 ms
64 bytes from 10.0.0.5: icmp_seq=4 ttl=64 time=1.19 ms
64 bytes from 10.0.0.5: icmp_seq=5 ttl=64 time=1.15 ms
^C
--- 10.0.0.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 1.124/1.167/1.213/0.049 ms
```

Task 7 Br0 is assigned IP 10.0.0.9

VM_2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
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 91  bytes 6966 (6.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 91  bytes 6966 (6.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kvats@kvats:~$ sudo ifconfig br0 10.0.0.9 netmask 255.255.255.0 broadcast 10.0.0.255
kvats@kvats:~$ ifconfig
br0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.9  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::a00:27ff:fe7a:a2d6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:7a:a2:d6  txqueuelen 1000  (Ethernet)
        RX packets 17  bytes 6391 (6.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 936 (936.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe77:af35  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:77:af:35  txqueuelen 1000  (Ethernet)
        RX packets 54  bytes 35468 (35.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 52  bytes 4565 (4.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::a00:27ff:fee6:2bfd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e6:2b:fd  txqueuelen 1000  (Ethernet)
        RX packets 58  bytes 10720 (10.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74  bytes 9377 (9.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

As shown below now VM1 is able to ping VM2 using assigned IP

VM_1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

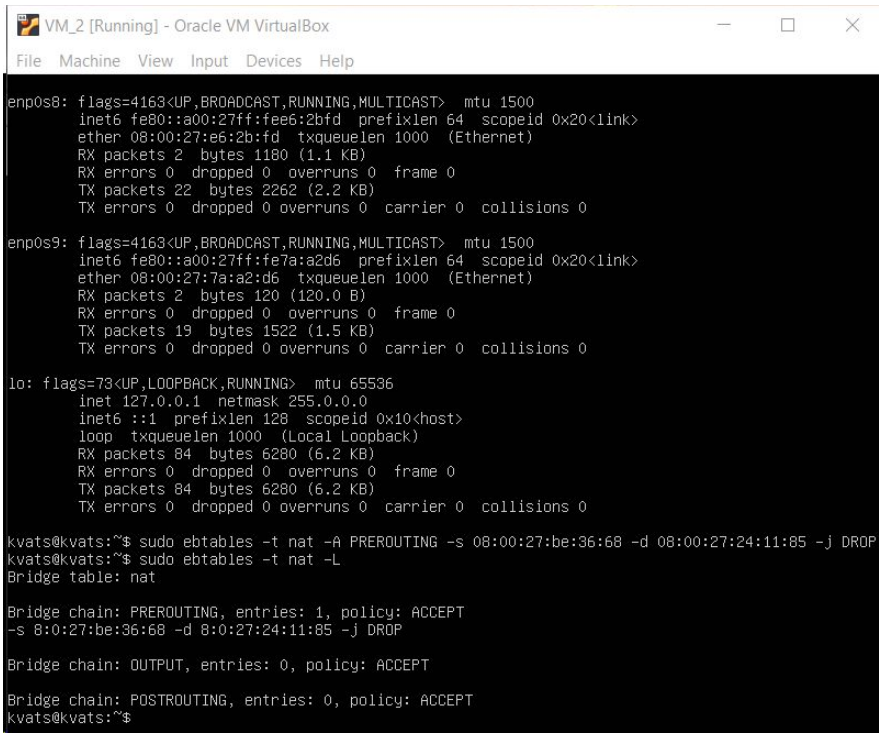
```
64 bytes from 10.0.0.8: icmp_seq=3 ttl=64 time=1.19 ms
64 bytes from 10.0.0.8: icmp_seq=4 ttl=64 time=1.21 ms
64 bytes from 10.0.0.8: icmp_seq=5 ttl=64 time=1.49 ms
64 bytes from 10.0.0.8: icmp_seq=6 ttl=64 time=1.19 ms
^C
--- 10.0.0.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 1.181/1.251/1.499/0.117 ms
kvats@kvats:~$ ifconfig 10.0.0.8
10.0.0.8: error fetching interface information: Device not found
kvats@kvats:~$ ping 10.0.0.8
PING 10.0.0.8 (10.0.0.8) 56(84) bytes of data.
64 bytes from 10.0.0.8: icmp_seq=1 ttl=64 time=0.706 ms
64 bytes from 10.0.0.8: icmp_seq=2 ttl=64 time=1.20 ms
64 bytes from 10.0.0.8: icmp_seq=3 ttl=64 time=1.22 ms
64 bytes from 10.0.0.8: icmp_seq=4 ttl=64 time=1.31 ms
64 bytes from 10.0.0.8: icmp_seq=5 ttl=64 time=1.27 ms
64 bytes from 10.0.0.8: icmp_seq=6 ttl=64 time=1.33 ms
^C
--- 10.0.0.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5010ms
rtt min/avg/max/mdev = 0.706/1.174/1.332/0.218 ms
kvats@kvats:~$ traceroute 10.0.0.8
traceroute to 10.0.0.8 (10.0.0.8), 30 hops max, 60 byte packets
 1  10.0.0.8 (10.0.0.8)  0.479 ms  0.419 ms  0.378 ms
kvats@kvats:~$ ping 10.0.0.9
PING 10.0.0.9 (10.0.0.9) 56(84) bytes of data.
64 bytes from 10.0.0.9: icmp_seq=1 ttl=64 time=0.451 ms
64 bytes from 10.0.0.9: icmp_seq=2 ttl=64 time=0.741 ms
64 bytes from 10.0.0.9: icmp_seq=3 ttl=64 time=0.676 ms
64 bytes from 10.0.0.9: icmp_seq=4 ttl=64 time=1.00 ms
64 bytes from 10.0.0.9: icmp_seq=5 ttl=64 time=0.916 ms
^C
--- 10.0.0.9 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4021ms
rtt min/avg/max/mdev = 0.451/0.758/1.006/0.193 ms
kvats@kvats:~$ _
```

Q1

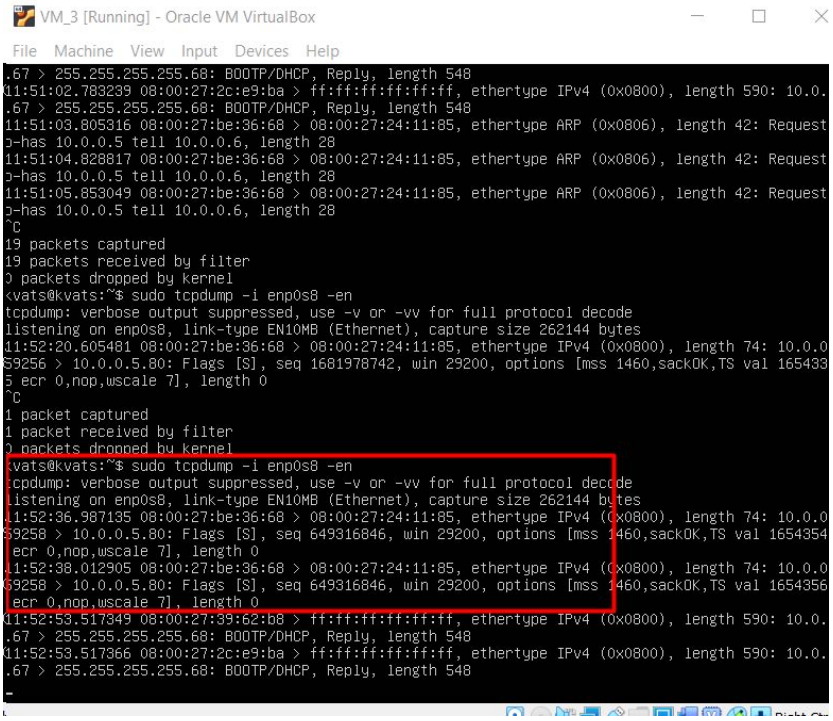
Using ebtables we added a rule on VM2 to drop packets from MAC of VM3 to MAC of VM1 at PREROUTING hook.

The ARP requests are successful and VM3 receives the MAC address of VM1 (ARP packets are not dropped as they bear the destination MAC of broadcast and not that of VM1) but finally the packet from VM3 to VM1 is dropped by VM2 bridge as it bears the destination MAC of VM1 and source MAC of VM3.

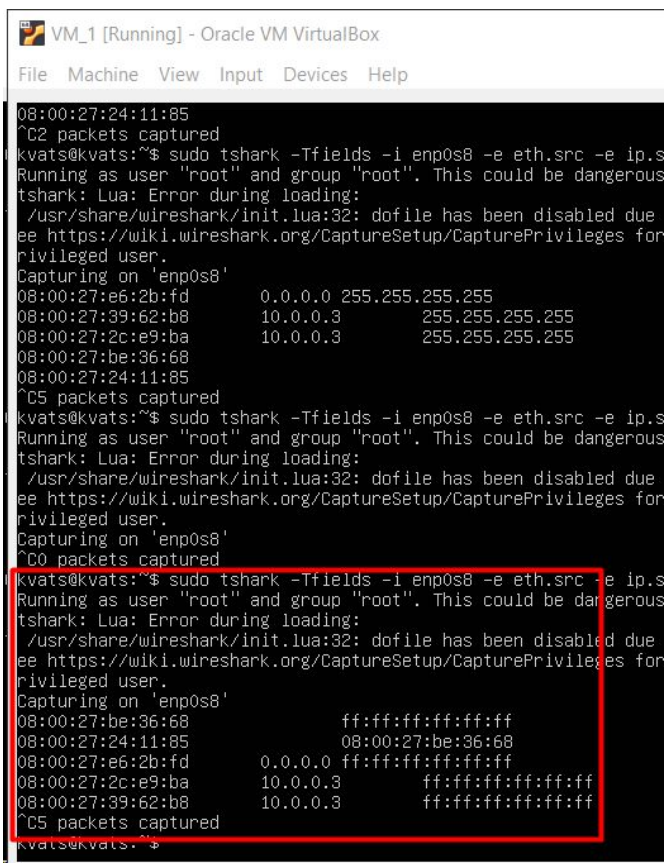
Following snapshot shows the added rule on VM2



Following snapshot shows that request was sent to vm1 from VM3



Following snapshot shows that VM1 received a broadcast request from VM3



Following snapshot shows that VM4 was able to ping VM1

alBox

es Help

elds -i enp0s8 -e eth.src -
o "root". This could be dan
ng:
32: dofile has been disable
aptureSetup/CapturePrivileg

255.255.255.255
3 255.255.255.255
3 255.255.255.255

elds -i enp0s8 -e eth.src -
o "root". This could be dan
ng:
32: dofile has been disable
aptureSetup/CapturePrivileg

elds -i enp0s8 -e eth.src -
o "root". This could be dan
ng:
32: dofile has been disable
aptureSetup/CapturePrivileg

ff:ff:ff:ff:ff:ff
08:00:27:be:36:68
ff:ff:ff:ff:ff:ff
3 ff:ff:ff:ff:ff:f
3 ff:ff:ff:ff:ff:ff

VM_4 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.
        inet6 fe80::a00:27ff:fe19:5ca4  prefixlen 64  scopeid 0x
        ether 08:00:27:19:5c:a4  txqueuelen 1000  (Ethernet)
        RX packets 1524  bytes 1598167 (1.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 425  bytes 33463 (33.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.7  netmask 255.255.255.0  broadcast 10.0.0.2
        inet6 fe80::a00:27ff:fe0c:1695  prefixlen 64  scopeid 0x
        ether 08:00:27:0c:16:95  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 2030 (2.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 656 (656.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions

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 106  bytes 7946 (7.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 106  bytes 7946 (7.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions

kvats@kvats:~$ ping 10.0.0.5
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
64 bytes from 10.0.0.5: icmp_seq=1 ttl=64 time=1.10 ms
64 bytes from 10.0.0.5: icmp_seq=2 ttl=64 time=0.599 ms
64 bytes from 10.0.0.5: icmp_seq=3 ttl=64 time=0.988 ms
64 bytes from 10.0.0.5: icmp_seq=4 ttl=64 time=0.839 ms
^C
--- 10.0.0.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3023ms
rtt min/avg/max/mdev = 0.599/0.881/1.100/0.189 ms
kvats@kvats:~$ _
```

Following snapshot shows VM3 is now not able to ping VM1

```
VM_3 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 199  bytes 15292 (15.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.6  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::a00:27ff:febe:3668  prefixlen 64  scopeid 0x20
        ether 08:00:27:be:36:68  txqueuelen 1000  (Ethernet)
        RX packets 63  bytes 22508 (22.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 62  bytes 6003 (6.0 KB)
        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 140  bytes 10346 (10.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 140  bytes 10346 (10.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kvats@kvats:~$ ping 10.0.0.5
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
^C
--- 10.0.0.5 ping statistics ---
94 packets transmitted, 0 received, 100% packet loss, time 95234ms

kvats@kvats:~$ ping 10.0.0.5
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
^C
--- 10.0.0.5 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4090ms

kvats@kvats:~$ ping 10.0.0.5
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
```

Q2 (assuming earlier ebtables rules are flushed)
Using ebtables we added a rule on VM2 to change the source MAC to that of VM2 for all packets destined t0 VM1
Following shows the added MAC address SNAT rule

```
VM_2 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
kvats@kvats:~$ sudo ebtables -t nat -L --Ln
Bridge table: nat

Bridge chain: PREROUTING, entries: 0, policy: ACCEPT

Bridge chain: OUTPUT, entries: 0, policy: ACCEPT

Bridge chain: POSTROUTING, entries: 1, policy: ACCEPT
1. -d 8:0:27:24:11:85 -j snat --to-src 8:0:27:e6:2b:fd --snat-target ACCEPT
kvats@kvats:~$ _
```

Ping from VM3 to VM1 is successful as shown below

VM_3 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
kvats@kvats:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe83:1ef6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:83:1e:f6  txqueuelen 1000  (Ethernet)
        RX packets 81640  bytes 100423849 (100.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14478  bytes 893068 (893.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.6  netmask 255.255.255.0  broadcast 10.0.0.0
        inet6 fe80::a00:27ff:febe:3668  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:be:36:68  txqueuelen 1000  (Ethernet)
        RX packets 75  bytes 23054 (23.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 73  bytes 7872 (7.8 KB)
        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 176  bytes 13478 (13.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 176  bytes 13478 (13.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kvats@kvats:~$ ping 10.0.0.5
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
64 bytes from 10.0.0.5: icmp_seq=1 ttl=64 time=0.607 ms
64 bytes from 10.0.0.5: icmp_seq=2 ttl=64 time=1.40 ms
^C
--- 10.0.0.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.607/1.008/1.409/0.401 ms
kvats@kvats:~$ _
```

Following snapshot is the tshark packets capture on VM1 for requests from VM3 showing that source ip is of VM3 but the source MAC has been changed to that of VM2.

VM_1 [Running] - Oracle VM VirtualBox

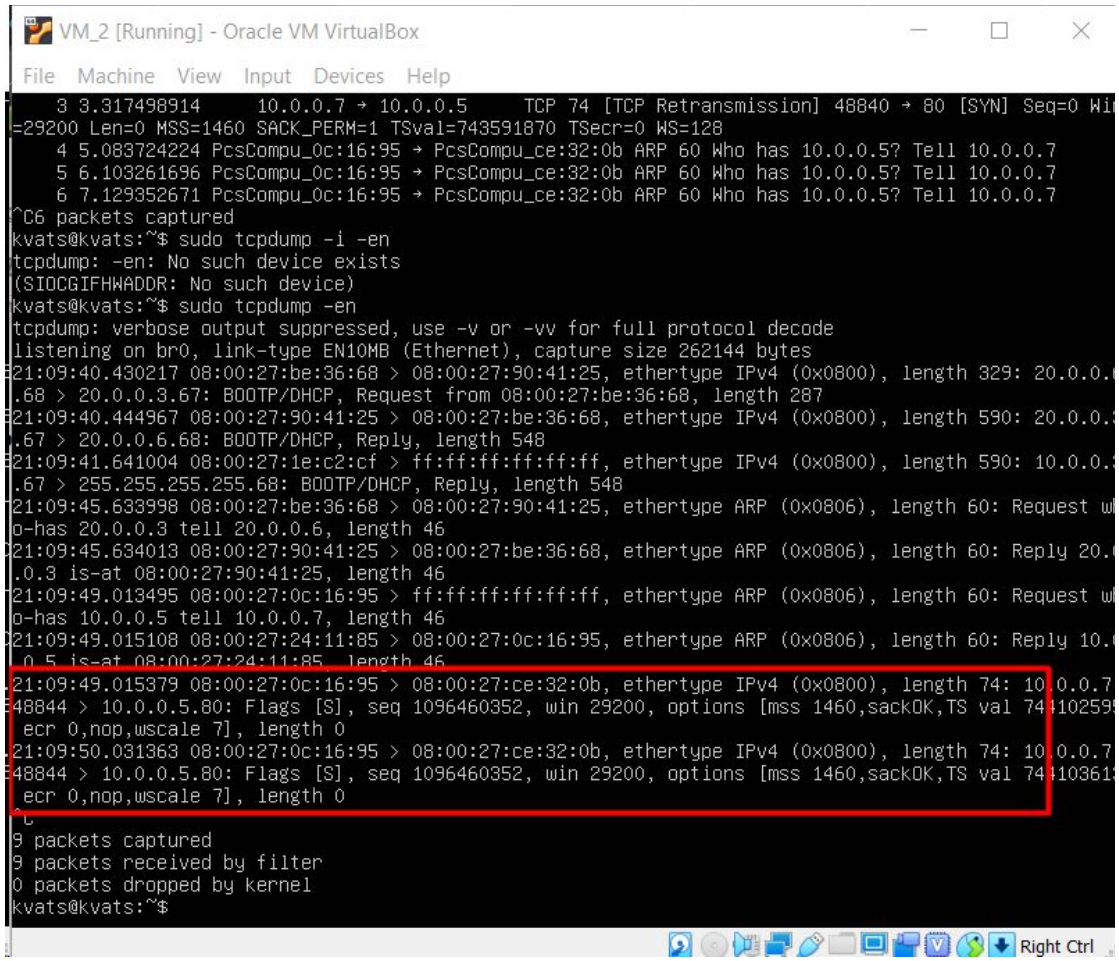
File Machine View Input Devices Help

```
tshark: Lua: Error during loading:
 /usr/share/wireshark/init.lua:32: dofile has been disabled due to
ee https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for h
rivileged user.
Capturing on 'enp0s3'
^[[A^C0 packets captured
kvats@kvats:~$ sudo tshark -Tfields -i enp0s8 -e eth.src -e ip.src
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
 /usr/share/wireshark/init.lua:32: dofile has been disabled due to
ee https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for h
rivileged user.
Capturing on 'enp0s8'
08:00:27:e6:2b:fd       10.0.0.6
08:00:27:24:11:85       10.0.0.5
08:00:27:e6:2b:fd       10.0.0.6
08:00:27:24:11:85       10.0.0.5
08:00:27:e6:2b:fd       10.0.0.6
08:00:27:24:11:85       10.0.0.5
^C6 packets captured
kvats@kvats:~$ sudo tshark -Tfields -i enp0s8 -e eth.src -e ip.src
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
 /usr/share/wireshark/init.lua:32: dofile has been disabled due to
ee https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for h
rivileged user.
Capturing on 'enp0s8'
08:00:27:e6:2b:fd       10.0.0.6
08:00:27:24:11:85       10.0.0.5
08:00:27:e6:2b:fd       10.0.0.6
08:00:27:24:11:85       10.0.0.5
08:00:27:24:11:85
08:00:27:e6:2b:fd
08:00:27:e6:2b:fd
08:00:27:24:11:85
c^C8 packets captured
kvats@kvats:~$ _
```

Q3

We used ebtables to add rules on VM2 for changing the destination MAC to that of VM5 for packets coming from source MAC VM4 to destination MAC VM1.
Now VM4 was **not** able to receive response to wget http://10.0.0.5. This is due to the fact that the source and destination ip of the request remains the same hence even after having destination MAC of VM5, VM5 probably discards the packet as it does not have the ip destination of VM5. Also the packets coming to br0 destination NATted to the same internal network are not send back again.

Snapshot of packet capture on VM2 using tcpdump -en



VM1 Mac Address is shown below

VM_1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
21:09:49.027444 08:00:27:0c:16:95 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x
o-has 10.0.0.5 tell 10.0.0.7, length 46
21:09:49.027466 08:00:27:24:11:85 > 08:00:27:0c:16:95, ethertype ARP (0x
.0.5 is-at 08:00:27:24:11:85, length 28
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
kvats@kvats:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe16:250b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:16:25:0b  txqueuelen 1000  (Ethernet)
        RX packets 2136  bytes 2291883 (2.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 633  bytes 49318 (49.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.5  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::a00:27ff:fe24:1185  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:24:11:85  txqueuelen 1000  (Ethernet)
        RX packets 275  bytes 98463 (98.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86  bytes 23669 (23.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Vm5 mac is shown below

VM_5 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

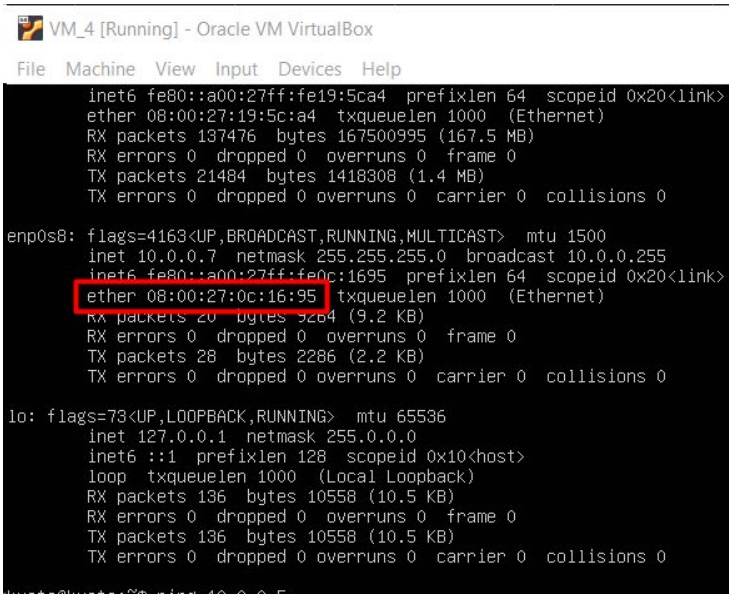
```
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 342  bytes 23284 (23.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 342  bytes 23284 (23.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kvats@kvats:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe19:5ca4  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:19:5c:a4  txqueuelen 1000  (Ethernet)
        RX packets 155376  bytes 186938112 (186.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26884  bytes 1742306 (1.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.8  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::a00:27ff:fece:320b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ce:32:0b  txqueuelen 1000  (Ethernet)
        RX packets 85  bytes 38088 (36.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 36  bytes 19584 (19.5 KB)
        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 342  bytes 23284 (23.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 342  bytes 23284 (23.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

VM4’s MAC address is shown below



Q4

We first enabled the packets coming to the bridge on VM2 to traverse through the iptables rules by using following command:

Sudo modprobe br_netfilter

sudo sysctl net.bridge.bridge-nf-call-iptables = 1

sudo sysctl -p

After that we added the iptables rule to do the destination NAT at post routing hook and changed dest ip address of packets from VM4 directed towards VM1 to that of VM5.

sudo iptables -t nat -A PREROUTING -i br0 -d 10.0.0.5 -s 10.0.0.7 -j DNAT --to-destination 10.0.0.8

Even after this, it was not possible to achieve the desired results. The packets had their IP destinations changed to that of VM5 but not the destination MAC, thus VM4 was still sending the packets to the VM1's MAC received in ARP packets. But they were being discarded by VM1 and were not reaching VM5.

We then tried even tried both ebtables and iptables to change the destination MAC and IP both at the same time. Even this was not giving the results. A reason could be that the packets were not being resent to same side of br0 after destination MAC NAT.

Following snapshot shows that VM2 has changed the destination IP to that of VM5 but as VM4 as received the MAC of VM1 from ARP, it sends the packet with destination MAC as of VM1.

VM4

```
VM_4 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
Setting up libwsutil9:amd64 (2.6.6-1~ubuntu18.04.0) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Setting up libsnappy1v5:amd64 (1.1.7-1) ...
Setting up libwireshark-data (2.6.6-1~ubuntu18.04.0) ...
Processing triggers for man-db (2.8.3-2) ...
Processing triggers for shared-mime-info (1.9-2) ...
Setting up liblua5.2-0:amd64 (5.2.4-1.1build1) ...
Setting up libc-ares2:amd64 (1.14.0-1) ...
Setting up libmaxminddb0:amd64 (1.3.1-1) ...
Setting up libjpeg8:amd64 (8c-2ubuntu8) ...
Setting up libtiff5:amd64 (4.0.9-5ubuntu0.1) ...
Setting up libwiretap8:amd64 (2.6.6-1~ubuntu18.04.0) ...
Setting up libspandsp2:amd64 (0.0.6+dfsg-0.1) ...
Setting up libwscodecs2:amd64 (2.6.6-1~ubuntu18.04.0) ...
Setting up libwireshark11:amd64 (2.6.6-1~ubuntu18.04.0) ...
Setting up wireshark-common (2.6.6-1~ubuntu18.04.0) ...
Setting up tshark (2.6.6-1~ubuntu18.04.0) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
kvats@kvats:~$ sudo tshark -i enp0s8
Running as user "root" and group "root". This could be dange
tshark: Lua: Error during loading:
/usr/share/wireshark/init.lua:32: dofile has been disabled due to running Wireshark as superuser.
ee https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an un
rivileged user.
Capturing on 'enp0s8'
    1 0.000000000      10.0.0.3 → 255.255.255.255 DHCP 590 DHCP Offer    - Transaction ID 0xfd082ef
    2 0.000014097      10.0.0.3 → 255.255.255.255 DHCP 590 DHCP Offer    - Transaction ID 0xfd082ef
    3 0.323083047      10.0.0.7 → 10.0.0.5      TCP 74 42512 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=146
SACK_PERM=1 TSval=640043885 TSecr=0 WS=128
    4 1.335471130      10.0.0.7 → 10.0.0.5      TCP 74 [TCP Retransmission] 42512 → 80 [SYN] Seq=0 Wi
29200 Len=0 MSS=1460 SACK_PERM=1 TSval=640044897 TSecr=0 WS=128
    5 3.351806752      10.0.0.7 → 10.0.0.5      TCP 74 [TCP Retransmission] 42512 → 80 [SYN] Seq=0 Wi
29200 Len=0 MSS=1460 SACK_PERM=1 TSval=640046914 TSecr=0 WS=128
    6 5.432180683 PcsCompu_0c:16:95 → PcsCompu_24:11:85 ARP 42 Who has 10.0.0.5? Tell 10.0.0.7
    7 5.433395017 PcsCompu_24:11:85 → PcsCompu_0c:16:95 ARP 60 10.0.0.5 is at 08:00:27:24:11:85
^C7 packets captured
```

```
*** System restart required ***
kvats@kvats:~$ sudo tshark
[sudo] password for kvats:
Running as user "root" and group "root".
tshark: Lua: Error during loading:
 /usr/share/wireshark/init.lua:32: dofil
ee https://wiki.wireshark.org/CaptureSet
rivileged user.
Capturing on 'br0'
    1 0.000000000      10.0.0.3 → 255.255
    2 0.000092859      10.0.0.3 → 255.255
    3 0.323465028      10.0.0.7 → 10.0.0.
 SACK_PERM=1 TSval=640043885 TSecr=0 WS=
    4 1.336123468      10.0.0.7 → 10.0.0.
=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=
    5 3.352511960      10.0.0.7 → 10.0.0.
=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=
    6 5.433140761 PcsCompu_0c:16:95 → Pc
    7 5.433717111 PcsCompu_24:11:85 → Pc
^C7 packets captured
kvats@kvats:~$ _
```

VM2

VM_2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
  Usage of /:   52.5% of 9.78GB   Users logged in:       1
  Memory usage: 11%               IP address for enp0s3: 10.0.2.15
  Swap usage:   0%                IP address for br0:    10.0.0.9

 * 'snap info' now shows the freshness of each channel.
   Try 'snap info microk8s' for all the latest goodness.


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

132 packages can be updated.
0 updates are security updates.


*** System restart required ***
kvats@kvats:~$ sudo tshark
[sudo] password for kvats:
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
/usr/share/wireshark/init.lua:32: dofile has been disabled due to running Wireshark as superuser.
ee https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an un
rivileged user.
Capturing on 'br0'
    1 0.000000000     10.0.0.3 → 255.255.255.255 DHCP 590 DHCP Offer    - Transaction ID 0xfd082ef
    2 0.000092859     10.0.0.3 → 255.255.255.255 DHCP 590 DHCP Offer    - Transaction ID 0xfd082ef
    3 0.323465028     10.0.0.7 → 10.0.0.8     TCP 74 42512 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=146
SACK_PERM=1 TSval=640043885 TSecr=0 WS=128
    4 1.336123468     10.0.0.7 → 10.0.0.8     TCP 74 [TCP Retransmission] 42512 → 80 [SYN] Seq=0 Wi
=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=640044897 TSecr=0 WS=128
    5 3.352511960     10.0.0.7 → 10.0.0.8     TCP 74 [TCP Retransmission] 42512 → 80 [SYN] Seq=0 Wi
=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=640046914 TSecr=0 WS=128
    6 5.433140761 PcsCompu_0c:16:95 → PcsCompu_24:11:85 ARP 60 Who has 10.0.0.5? Tell 10.0.0.7
    7 5.433717111 PcsCompu_24:11:85 → PcsCompu_0c:16:95 ARP 60 10.0.0.5 is at 08:00:27:24:11:85
^C7 packets captured
kvats@kvats:~$ _
```