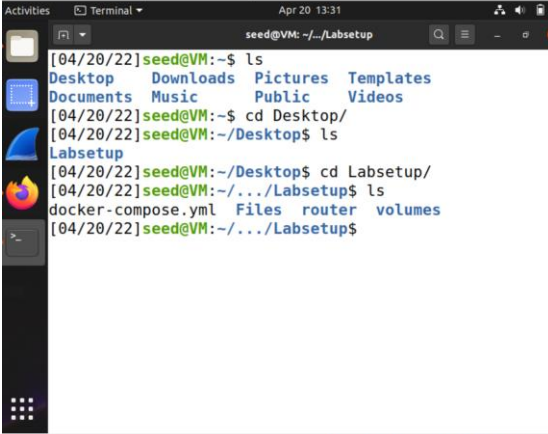


Lab 5 Firewall Exploration

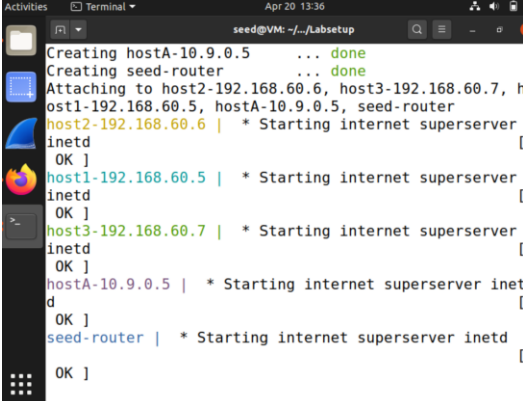
I. Lab set up

- Prebuild 20.04 Seed image on VirtualBox
- Download Labsetup.zip on the VM



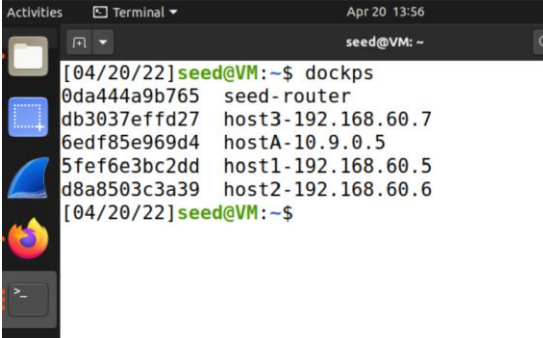
```
SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 13:31
seed@VM: ~/Labsetup
[04/20/22]seed@VM:~$ ls
Desktop Downloads Pictures Templates
Documents Music Public Videos
[04/20/22]seed@VM:~$ cd Desktop/
[04/20/22]seed@VM:~/Desktop$ ls
Labsetup
[04/20/22]seed@VM:~/Desktop$ cd Labsetup/
[04/20/22]seed@VM:~/.../Labsetup$ ls
docker-compose.yml Files router volumes
[04/20/22]seed@VM:~/.../Labsetup$
```

- Run dcbuild and dcup to build and start the container.



```
SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 13:36
seed@VM: ~/Labsetup
Creating hostA-10.9.0.5 ... done
Creating seed-router ... done
Attaching to host2-192.168.60.6, host3-192.168.60.7, host1-192.168.60.5, hostA-10.9.0.5, seed-router
host2-192.168.60.6 | * Starting internet superserver [
inetd
OK ]
host1-192.168.60.5 | * Starting internet superserver [
inetd
OK ]
host3-192.168.60.7 | * Starting internet superserver [
inetd
OK ]
hostA-10.9.0.5 | * Starting internet superserver inetd
OK ]
seed-router | * Starting internet superserver inetd
OK ]
```

- Open another terminal to run dockps to check for IDs.



```
SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 13:56
seed@VM: ~
[04/20/22]seed@VM:~$ dockps
0da444a9b765 seed-router
db3037effd27 host3-192.168.60.7
6edf85e969d4 hostA-10.9.0.5
5fef6e3bc2dd host1-192.168.60.5
d8a8503c3a39 host2-192.168.60.6
[04/20/22]seed@VM:~$
```

g.

II. Task 2.A

- Get a shell on seed-router.

```
Activities Terminal Apr 20 13:58
seed@VM: ~
[04/20/22]seed@VM:~$ dockps
0da444a9b765 seed-router
db3037effd27 host3-192.168.60.7
6edf85e969d4 hostA-10.9.0.5
5fef6e3bc2dd host1-192.168.60.5
d8a8503c3a39 host2-192.168.60.6
[04/20/22]seed@VM:~$ docksh 0d
root@0da444a9b765:/#
```

- b.
- c. Execute the provided commands and check the rules in the table.

```
SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 14:07
seed@VM: ~
root@0da444a9b765:/# iptables -A INPUT -p icmp --icmp-
type echo-request -j ACCEPT
root@0da444a9b765:/# iptables -A INPUT -p icmp --icmp-
type echo-reply -j ACCEPT
root@0da444a9b765:/# iptables -P OUTPUT DROP
root@0da444a9b765:/# iptables -P INPUT DROP
root@0da444a9b765:/# iptables -t filter -L -n
Chain INPUT (policy DROP)
target prot opt source destination
ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0
icmp type 8
ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0
icmp type 0
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy DROP)
```

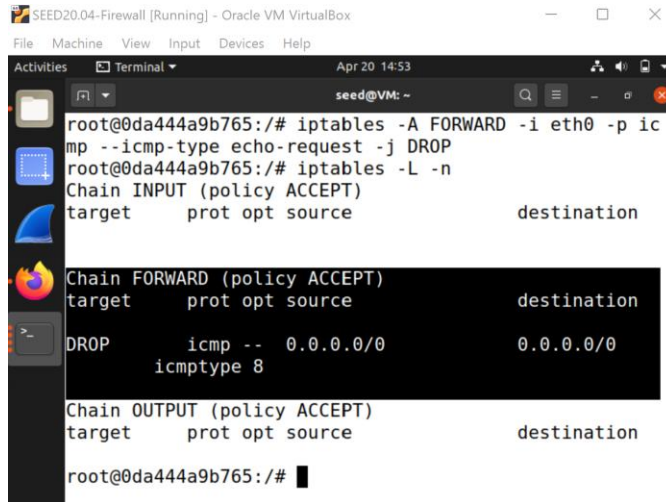
- d.
- e. On the shell of 10.9.0.5 try telnet and ping the server. Telnet does not work anymore yet ping would still work since the commands filtered all incoming and outgoing traffic except ping (ICMP packets).

```
SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 14:28
seed@VM: ~
root@6edf85e969d4:/# telnet 192.168.60.11
Trying 192.168.60.11...
^C
root@6edf85e969d4:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of dat
a.
64 bytes from 192.168.60.11: icmp_seq=1 ttl=64 time=0.
182 ms
64 bytes from 192.168.60.11: icmp_seq=2 ttl=64 time=0.
130 ms
64 bytes from 192.168.60.11: icmp_seq=3 ttl=64 time=0.
124 ms
64 bytes from 192.168.60.11: icmp_seq=4 ttl=64 time=0.
127 ms
64 bytes from 192.168.60.11: icmp_seq=5 ttl=64 time=0.
125 ms
^Z
[7]+ Stopped ping 192.168.60.11
root@6edf85e969d4:/#
```

- f.
- g. Restart the container to restore states of all tables.

III. Task 2.B

- a. Run the command in router's shell and check the table.



```
SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 14:53
seed@VM: ~
root@0da444a9b765:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DROP
root@0da444a9b765:/# iptables -L -n
Chain INPUT (policy ACCEPT)
target    prot opt source                destination

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination
DROP      icmp -- 0.0.0.0/0              0.0.0.0/0
           icmp -- 0.0.0.0/0              0.0.0.0/0
           icmp -- 0.0.0.0/0              0.0.0.0/0

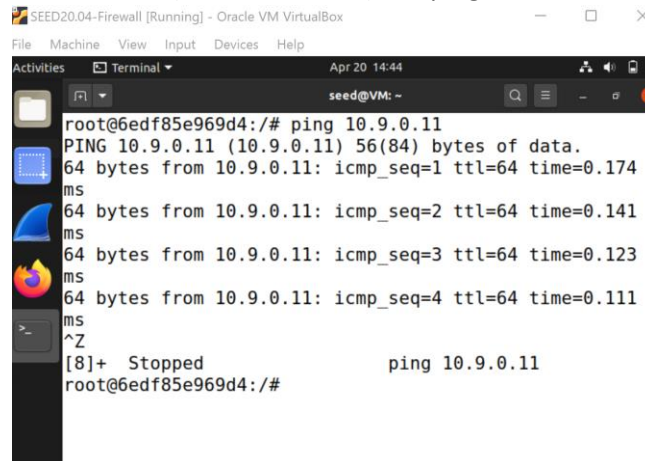
Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination

root@0da444a9b765:/#
```

- b.

- c. Check

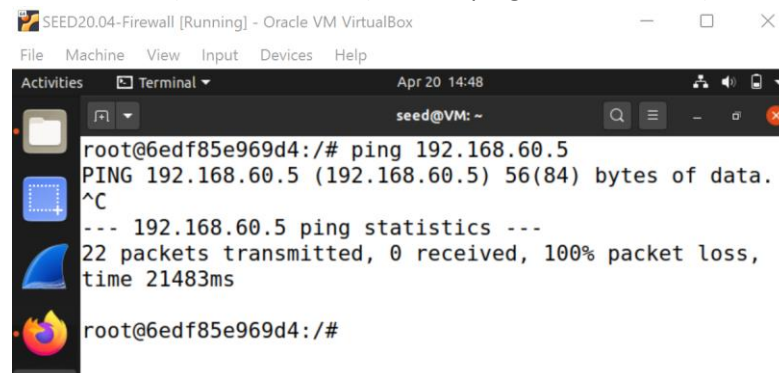
- i. Outside host (host A: 10.9.0.5) can ping the router.



```
SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 14:44
seed@VM: ~
root@6edf85e969d4:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data:
64 bytes from 10.9.0.11: icmp_seq=1 ttl=64 time=0.174 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.141 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.123 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.111 ms
^Z
[8]+  Stopped                  ping 10.9.0.11
root@6edf85e969d4:/#
```

- ii.

- iii. Outside host (host A: 10.9.0.5) cannot ping internal hosts (host 1: 192.168.60.5).



```
SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 14:48
seed@VM: ~
root@6edf85e969d4:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data:
^C
--- 192.168.60.5 ping statistics ---
22 packets transmitted, 0 received, 100% packet loss,
time 21483ms

root@6edf85e969d4:/#
```

- iv.

- v. Internal host (host 1: 192.168.60.5) can ping outside host (host A: 10.9.0.5).

```

SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 14:53
seed@VM: ~
root@5fef6e3bc2dd:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=63 time=0.150 m
s
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.163 m
s
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.152 m
s
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.198 m
s
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.167 m
s
^Z
[2]+  Stopped                  ping 10.9.0.5
root@5fef6e3bc2dd:/#

```

vi.

vii. To prevent other packets between internal and external host, added more rules to the table.

```

SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 15:05
seed@VM: ~
root@0da444a9b765:/# iptables -A FORWARD -i eth1 -p ic
mp --icmp-type echo-request -j ACCEPT
root@0da444a9b765:/# iptables -A FORWARD -i eth0 -p ic
mp --icmp-type echo-reply -j DROP

```

viii.

ix. Also set the default policy for Forward to DROP, and check the table.

```

SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 15:06
seed@VM: ~
root@0da444a9b765:/# iptables -P FORWARD DROP
root@0da444a9b765:/# iptables -L -n
Chain INPUT (policy ACCEPT)
target    prot opt source               destination

Chain FORWARD (policy DROP)
target    prot opt source               destination
DROP      icmp -- 0.0.0.0/0             0.0.0.0/0
          icmptype 8
ACCEPT    icmp -- 0.0.0.0/0             0.0.0.0/0
          icmptype 8
DROP      icmp -- 0.0.0.0/0             0.0.0.0/0
          icmptype 0

Chain OUTPUT (policy ACCEPT)
target    prot opt source               destination

root@0da444a9b765:/#

```

x.

xi. Telnet outside host (host A: 10.9.0.5) from Internal host (host 1: 192.168.60.5). Packets should be dropped, and telnet should not work.

```
SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 15:03
seed@VM: ~
[04/20/22]seed@VM:~$ docksh 5f
root@5fef6e3bc2dd:~# telnet 10.9.0.5
Trying 10.9.0.5...
^C
root@5fef6e3bc2dd:~#
```

- xii.
- xiii. The firewall works as expected. Restart the container to clean up the rules.

IV. Task 2.c

- a. Add the following rule so that all the internal hosts run a telnet server (listening to port 23). Outside hosts can only access the telnet server on 192.168.60.5, not the other internal hosts.

```
SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 15:21
seed@VM: ~
root@0da444a9b765:~# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 -j ACCEPT
```

- b.
- c. Add the following rule so that internal hosts can access all the internal servers and internal hosts cannot access external servers.

```
SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 15:21
seed@VM: ~
root@0da444a9b765:~# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 -j ACCEPT
root@0da444a9b765:~# iptables -A FORWARD -i eth1 -s 192.168.60.5 -p tcp --sport 23 -j ACCEPT
root@0da444a9b765:~# iptables -P FORWARD DROP
root@0da444a9b765:~#
```

- d.
- e. Check
 - i. Outside hosts (host A: 10.9.0.5) can only access the telnet server on 192.168.60.5, not the other internal hosts.

```
SEED20.04-Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Apr 20 15:28
seed@VM: ~
root@6edf85e969d4:~# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^'.
Ubuntu 20.04.1 LTS
5fef6e3bc2dd login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize'
command.
```

- ii.
- iii.

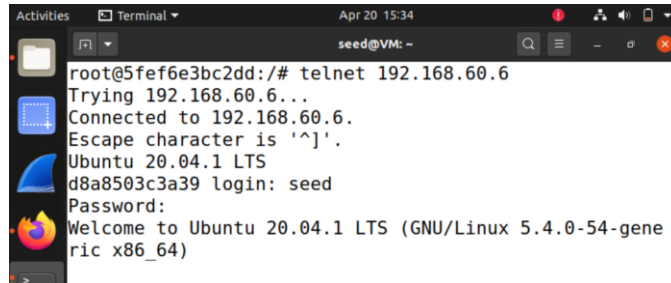
- iv. Outside hosts (host A: 10.9.0.5) cannot access other internal servers.



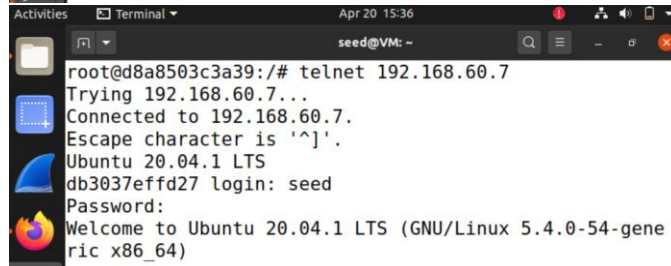
```
root@6edf85e969d4:/# telnet 192.168.60.7
Trying 192.168.60.7...
```

- v.

- vi. . Internal hosts can access all the internal servers. Here I will check if internal host 1 (192.168.60.5) can access host 2 (192.168.60.6) and host 2 can access host 3 (192.168.60.7).



- vii.



- viii.

- ix. Internal hosts cannot access external servers. Here I will check if internal host 1(192.168.60.5) host2(192.168.60.6) and host 3(192.168.60.7) can access host A(10.9.0.5).



- x.



- xi.



- xii.

- xiii. The rules to protect the TCP server was set up successfully. Restart the docker to clean up the tables.

V. Task 4

- a. In the router shell, add the first rule only.

```
Activities Terminal Apr 22 09:32 seed@VM: ~
root@0da444a9b765:/# iptables -A FORWARD -s 10.9.0.5 -
m limit --limit 10/minute --limit-burst 5 -j ACCEPT
root@0da444a9b765:/#
```

b.

c. On shell of 10.9.0.5, ping 192.168.60.5. The packets were transmitted.

```
Activities Terminal Apr 22 09:33 seed@VM: ~
root@6edf85e969d4:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.2
28 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.1
70 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.1
81 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.1
66 ms
^Z
[1]+  Stopped                  ping 192.168.60.5
root@6edf85e969d4:/#
```

d.

e. Add the second rule.

```
Activities Terminal Apr 22 09:35 seed@VM: ~
root@0da444a9b765:/# iptables -A FORWARD -s 10.9.0.5 -
m limit --limit 10/minute --limit-burst 5 -j ACCEPT
root@0da444a9b765:/# iptables -A FORWARD -s 10.9.0.5 -
j DROP
root@0da444a9b765:/#
```

f.

g. Ping again, and with second rule, the limit takes effect as the icmp_seq are not consecutive since the rule limits to 10 packets per minute. The second rule is needed since it specifies the default rule for forward is to drop the packets.

```
Activities Terminal Apr 22 09:37 seed@VM: ~
root@6edf85e969d4:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.1
69 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.1
74 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.
224 ms
64 bytes from 192.168.60.5: icmp_seq=18 ttl=63 time=0.
121 ms
64 bytes from 192.168.60.5: icmp_seq=24 ttl=63 time=0.
159 ms
^Z
[4]+  Stopped                  ping 192.168.60.5
root@6edf85e969d4:/#
```

h.

VI. Task 5

- Run `nc -luk 8080` on host 1-3
- Using round robin:
- On router shell, run following command.

```

root@0da444a9b765:/# iptables -t nat -A PREROUTING -p
udp --dport 8080 -m statistic --mode nth --every 3 --p
acket 0 -j DNAT --to-destination 192.168.60.5:8080
root@0da444a9b765:/#

```

-
- On host A shell, run following command.

```

[04/22/22]seed@VM:~$ docksh 6e
root@6edf85e969d4:/# echo hello | nc -u 10.9.0.11 8080
^C
root@6edf85e969d4:/#

```

-
-
- On host 1, we can see 'hello' printed out.

```

[04/22/22]seed@VM:~$ docksh 5f
root@5fef6e3bc2dd:/# nc -luk 8080
hello

```

-
-
-
- In order to all the three internal hosts get the equal number of packets, two more rules are needed. The rule added previously sent the first packet among three packets to host1. We need to dispatch the 2 packets left. The first added rule specifies that every 2 packets, send the first packet to host 2. The last rule specifies that for the third packet, send to host 3.

```

root@0da444a9b765:/# iptables -t nat -A PREROUTING -p
udp --dport 8080 -m statistic --mode nth --every 3 --p
acket 0 -j DNAT --to-destination 192.168.60.5:8080
root@0da444a9b765:/# iptables -t nat -A PREROUTING -p
udp --dport 8080 -m statistic --mode nth --every 2 --p
acket 0 -j DNAT --to-destination 192.168.60.6:8080
root@0da444a9b765:/# iptables -t nat -A PREROUTING -p
udp --dport 8080 -m statistic --mode nth --every 1 --p
acket 0 -j DNAT --to-destination 192.168.60.7:8080
root@0da444a9b765:/#

```

-
-
-
-
- Check the nat table rules:

```

root@0da444a9b765:/# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target    prot opt source                destination
DNAT      udp  --  0.0.0.0/0             0.0.0.0/0
           udp dpt:8080 statistic mode nth every 3 to:192.168.60.
5:8080
DNAT      udp  --  0.0.0.0/0             0.0.0.0/0
           udp dpt:8080 statistic mode nth every 2 to:192.168.60.
6:8080
DNAT      udp  --  0.0.0.0/0             0.0.0.0/0
           udp dpt:8080 statistic mode nth every 1 to:192.168.60.
7:8080

```

-
-
-
-
-
- Now on host A run `echo hello` three times, and host 1-3 will printout hello.

n.

```
Activities Terminal Apr 22 10:05
seed@VM: ~
[04/22/22]seed@VM:~$ docksh db
root@db3037effd27:/# nc -luk 8080
hello
```

o.

```
Activities Terminal Apr 22 10:06
seed@VM: ~
[04/22/22]seed@VM:~$ docksh d8
root@d8a8503c3a39:/# nc -luk 8080
hello
```

p. Using the random node:

q. Restart router and run following command in router shell. For host 1, the probability is $\frac{1}{3}$ since it is receiving one packets out of three. For host2, the probability is $\frac{1}{2}$, since it is receiving one packets out of two, and for host 3, the probability is 1.

r. On host A, send three packets: packet 1-3 and host 1-3 will receive correspondingly packet 1-3. Load balancing using probability mode was implemented successfully.

```
root@5fef6e3bc2dd:/# nc -luk 8080
hello
hello
packet1
```

s.

```
Activities Terminal Apr 22 10:17
seed@VM: ~
[04/22/22]seed@VM:~$ docksh d8
root@d8a8503c3a39:/# nc -luk 8080
hello
packet2
```

t.

```
root@db3037effd27:/# nc -luk 8080
hello
packet3
```

u.