Name: Priyadharshini Stalin

Practical validation

SEED Labs-iptables Tables and Chains

```
C:\Users\priya\Downloads\Labsetup (1)\Labsetup>docker exec -it bash seed-router
Error response from daemon: No such container: bash

C:\Users\priya\Downloads\Labsetup (1)\Labsetup>docker exec -it seed-router bash
root@1f6682ef938e:/# iptables -t filter -L -n
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
root@1f6682ef938e:/# iptables -t nat -L -n
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
DOCKER_OUTPUT  all  --  0.0.0.0/0            127.0.0.11

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
DOCKER_POSTROUTING  all  --  0.0.0.0/0            127.0.0.11

Chain DOCKER_OUTPUT (1 references)
target     prot opt source               destination
DNAT       tcp  --  0.0.0.0/0            127.0.0.11           tcp dpt:53 to:127.0.0.11:33243
DNAT       udp  --  0.0.0.0/0            127.0.0.11           udp dpt:53 to:127.0.0.11:55042

Chain DOCKER_POSTROUTING (1 references)
target     prot opt source               destination
SNAT       tcp  --  127.0.0.11           0.0.0.0/0            tcp spt:33243 to::53
SNAT       udp  --  127.0.0.11           0.0.0.0/0            udp spt:55042 to::53
```

```
root@1f6682ef938e:/# iptables -t nat -L -n --list-numbers
iptables v1.8.4 (legacy): unknown option "--list-numbers"
Try `iptables -h' or 'iptables --help' for more information.
root@1f6682ef938e:/# iptables -t nat -L -n --line-numbers
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination

Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DOCKER_OUTPUT  all  --  0.0.0.0/0            127.0.0.11

Chain POSTROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    DOCKER_POSTROUTING  all  --  0.0.0.0/0            127.0.0.11

Chain DOCKER_OUTPUT (1 references)
num  target     prot opt source               destination
1    DNAT       tcp  --  0.0.0.0/0            127.0.0.11           tcp dpt:53 to:127.0.0.11:33243
2    DNAT       udp  --  0.0.0.0/0            127.0.0.11           udp dpt:53 to:127.0.0.11:55042

Chain DOCKER_POSTROUTING (1 references)
num  target     prot opt source               destination
1    SNAT       tcp  --  127.0.0.11           0.0.0.0/0            tcp spt:33243 to::53
2    SNAT       udp  --  127.0.0.11           0.0.0.0/0            udp spt:55042 to::53
```

Protecting the Router

Protecting the Router In this task, we will set up rules to prevent outside machines from accessing the router machine, except ping. Please execute the following iptables command on the router container, and then try to access it from 10.9.0.5.

(1) Can you ping the router?

```
PS C:\Users\priya> docker exec -it hostA-10.9.0.5 bash
root@4598a8865c51:/# 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=1.20 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.091 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.090 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.189 ms
64 bytes from 10.9.0.11: icmp_seq=5 ttl=64 time=0.111 ms
64 bytes from 10.9.0.11: icmp_seq=6 ttl=64 time=0.118 ms
64 bytes from 10.9.0.11: icmp_seq=7 ttl=64 time=0.134 ms
64 bytes from 10.9.0.11: icmp_seq=8 ttl=64 time=0.111 ms
64 bytes from 10.9.0.11: icmp_seq=9 ttl=64 time=0.184 ms
64 bytes from 10.9.0.11: icmp_seq=10 ttl=64 time=0.092 ms
64 bytes from 10.9.0.11: icmp_seq=11 ttl=64 time=0.424 ms
64 bytes from 10.9.0.11: icmp_seq=12 ttl=64 time=0.121 ms
64 bytes from 10.9.0.11: icmp_seq=13 ttl=64 time=0.097 ms
64 bytes from 10.9.0.11: icmp_seq=14 ttl=64 time=0.097 ms
64 bytes from 10.9.0.11: icmp_seq=15 ttl=64 time=0.207 ms
64 bytes from 10.9.0.11: icmp_seq=16 ttl=64 time=0.115 ms
64 bytes from 10.9.0.11: icmp_seq=17 ttl=64 time=0.090 ms
64 bytes from 10.9.0.11: icmp_seq=18 ttl=64 time=0.149 ms
64 bytes from 10.9.0.11: icmp_seq=19 ttl=64 time=0.303 ms
64 bytes from 10.9.0.11: icmp_seq=20 ttl=64 time=0.297 ms
64 bytes from 10.9.0.11: icmp_seq=21 ttl=64 time=0.131 ms
^C
--- 10.9.0.11 ping statistics ---
21 packets transmitted, 21 received, 0% packet loss, time 20764ms
rtt min/avg/max/mdev = 0.090/0.206/1.195/0.236 ms
root@4598a8865c51:/# telnet seed@10.9.0.11
telnet: could not resolve seed@10.9.0.11/telnet: Name or service not known
root@4598a8865c51:/# telnet 10.9.0.11
Trying 10.9.0.11...
Connected to 10.9.0.11.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
```

(2) Can you telnet into the router (a telnet server is running on all the containers

```
1f6682ef938e login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.133.1-microsoft-standard-WSL2 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@1f6682ef938e:~$ EXIT
-bash: EXIT: command not found
seed@1f6682ef938e:~$ exit
logout
Connection closed by foreign host.
root@4598a8865c51:/# exit
```

Setting the rules in seed machines

```
root@4598a8865c51:/# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
root@4598a8865c51:/# iptables -A INPUT -p icmp --icmp-type echo-reqly -j ACCEPT
iptables v1.8.4 (legacy): Invalid ICMP type `echo-reqly'

Try `iptables -h' or 'iptables --help' for more information.
root@4598a8865c51:/# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@4598a8865c51:/# iptables -P OUTPUT DROP
root@4598a8865c51:/# iptables -P INPUT DROP
root@4598a8865c51:/#
```

Trying to ping seed machine from host A

```
root@4598a8865c51:/# 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=182 ttl=64 time=0.194 ms
64 bytes from 10.9.0.11: icmp_seq=183 ttl=64 time=0.130 ms
64 bytes from 10.9.0.11: icmp_seq=184 ttl=64 time=0.128 ms
64 bytes from 10.9.0.11: icmp_seq=185 ttl=64 time=0.142 ms
64 bytes from 10.9.0.11: icmp_seq=186 ttl=64 time=0.302 ms
64 bytes from 10.9.0.11: icmp_seq=187 ttl=64 time=0.189 ms
64 bytes from 10.9.0.11: icmp_seq=188 ttl=64 time=0.132 ms
64 bytes from 10.9.0.11: icmp_seq=189 ttl=64 time=0.173 ms
64 bytes from 10.9.0.11: icmp_seq=190 ttl=64 time=0.130 ms
64 bytes from 10.9.0.11: icmp_seq=191 ttl=64 time=0.158 ms
64 bytes from 10.9.0.11: icmp_seq=192 ttl=64 time=0.194 ms
64 bytes from 10.9.0.11: icmp_seq=193 ttl=64 time=0.148 ms
64 bytes from 10.9.0.11: icmp_seq=194 ttl=64 time=0.148 ms
64 bytes from 10.9.0.11: icmp_seq=195 ttl=64 time=0.136 ms
64 bytes from 10.9.0.11: icmp_seq=196 ttl=64 time=0.121 ms
64 bytes from 10.9.0.11: icmp_seq=197 ttl=64 time=0.136 ms
64 bytes from 10.9.0.11: icmp_seq=198 ttl=64 time=0.135 ms
64 bytes from 10.9.0.11: icmp_seq=199 ttl=64 time=0.136 ms
64 bytes from 10.9.0.11: icmp_seq=200 ttl=64 time=0.129 ms
64 bytes from 10.9.0.11: icmp_seq=201 ttl=64 time=0.160 ms
64 bytes from 10.9.0.11: icmp_seq=202 ttl=64 time=0.136 ms
64 bytes from 10.9.0.11: icmp_seq=203 ttl=64 time=0.233 ms
^C
--- 10.9.0.11 ping statistics ---
203 packets transmitted, 22 received, 89.1626% packet loss, time 210095ms
rtt min/avg/max/mdev = 0.121/0.158/0.302/0.041 ms
```

Trying to telnet to seed from host A

```
root@4598a8865c51:/# Telnet 10.9.0.11
bash: Telnet: command not found
root@4598a8865c51:/# telnet 10.9.0.11
Trying 10.9.0.11...
telnet: Unable to connect to remote host: Connection timed out
root@4598a8865c51:/#
```

Nmap

```
root@4598a8865c51:/# nmap -p 1-100 10.9.0.1-15
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-30 00:48 UTC
Nmap scan report for 10.9.0.1
Host is up (0.000056s latency).
All 100 scanned ports on 10.9.0.1 are closed
MAC Address: 02:42:3C:22:12:92 (Unknown)

Nmap scan report for seed-router.net-10.9.0.0 (10.9.0.11)
Host is up (0.00012s latency).
All 100 scanned ports on seed-router.net-10.9.0.0 (10.9.0.11) are filtered
MAC Address: 02:42:0A:09:00:0B (Unknown)

Nmap scan report for 4598a8865c51 (10.9.0.5)
Host is up (0.0000060s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
```

Protecting the Internal Network

to enforce the following restrictions on the ICMP traffic: 1. Outside hosts cannot ping internal hosts. 2. Outside hosts can ping the router. 3. Internal hosts can ping outside hosts. 4. All other packets between the internal and external networks should be blocked.

ROUTER

```
root@1f6682ef938e:/# iptables -P INPUT DROP
root@1f6682ef938e:/# iptables -P OUTPUT DROP
root@1f6682ef938e:/# iptables -t filter -L -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source               destination

Chain FORWARD (policy DROP)
num  target     prot opt source               destination

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
```

1. Outside hosts cannot ping internal hosts- HOST A

```
254 packets transmitted, 186 received, 58.2677% packet loss, time 263097ms
rtt min/avg/max/mdev = 0.103/0.157/0.304/0.031 ms
root@4598a8865c51:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
```

ROUTER:

```
root@1f6682ef938e:/# iptables -t filter -L -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0            icmptype 8

Chain FORWARD (policy DROP)
num  target     prot opt source               destination

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0            icmptype 0
root@1f6682ef938e:/#
```

HOST A:

```
root@4598a8865c51:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data.
^C
--- 10.9.0.11 ping statistics ---
55 packets transmitted, 0 received, 100% packet loss, time 56197ms

root@4598a8865c51:/# 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=149 ttl=64 time=0.164 ms
64 bytes from 10.9.0.11: icmp_seq=150 ttl=64 time=0.179 ms
64 bytes from 10.9.0.11: icmp_seq=151 ttl=64 time=0.147 ms
64 bytes from 10.9.0.11: icmp_seq=152 ttl=64 time=0.162 ms
64 bytes from 10.9.0.11: icmp_seq=153 ttl=64 time=0.126 ms
64 bytes from 10.9.0.11: icmp_seq=154 ttl=64 time=0.156 ms
64 bytes from 10.9.0.11: icmp_seq=155 ttl=64 time=0.185 ms
64 bytes from 10.9.0.11: icmp_seq=156 ttl=64 time=0.157 ms
64 bytes from 10.9.0.11: icmp_seq=157 ttl=64 time=0.152 ms
64 bytes from 10.9.0.11: icmp_seq=158 ttl=64 time=0.184 ms
64 bytes from 10.9.0.11: icmp_seq=159 ttl=64 time=0.127 ms
64 bytes from 10.9.0.11: icmp_seq=160 ttl=64 time=0.144 ms
64 bytes from 10.9.0.11: icmp_seq=161 ttl=64 time=0.204 ms
```

Nmap

```
root@4598a8865c51:/# nmap -p 1-100 10.9.0.1-15
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-30 00:48 UTC
Nmap scan report for 10.9.0.1
Host is up (0.000056s latency).
All 100 scanned ports on 10.9.0.1 are closed
MAC Address: 02:42:3C:22:12:92 (Unknown)

Nmap scan report for seed-router.net-10.9.0.0 (10.9.0.11)
Host is up (0.00012s latency).
All 100 scanned ports on seed-router.net-10.9.0.0 (10.9.0.11) are filtered
MAC Address: 02:42:0A:09:00:0B (Unknown)

Nmap scan report for 4598a8865c51 (10.9.0.5)
Host is up (0.0000060s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 15 IP addresses (3 hosts up) scanned in 15.76 seconds
root@4598a8865c51:/#
```

Router

```
root@1f6682ef938e:/# iptables -A FORWARD -i eth1 -p icmp --icmp-type echo-request -j ACCEPT
root@1f6682ef938e:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-reply -j ACCEPT
root@1f6682ef938e:/# iptables -A INPUT -i eth0 -p icmp --icmp-type echo-request -j ACCEPT
root@1f6682ef938e:/# iptables -A OUTPUT -o eth0 -p icmp --icmp-type echo-reply -j ACCEPT
root@1f6682ef938e:/# iptables -t filter -L -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0            icmptype 8

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

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0            icmptype 0
root@1f6682ef938e:/#
```

from 192.168.60.5

```
PS C:\Users\priya> docker exec -it host1-192.168.60.5 bash
root@74cd48bf81e4:/# PING 10.9.0.5
bash: PING: command not found
root@74cd48bf81e4:/# 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=0.320 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.163 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.170 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.187 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.243 ms
```

From external host A to internal hosts

```
root@4598a8865c51:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
```

```
root@4598a8865c51:/# telnet 192.168.60.5
Trying 192.168.60.5...
```

Nmap scan from external host

```
root@4598a8865c51:/# nmap -p 1-100 10.9.0.1-20
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-30 03:21 UTC
Nmap scan report for 10.9.0.1
Host is up (0.00010s latency).
All 100 scanned ports on 10.9.0.1 are closed
MAC Address: 02:42:3C:22:12:92 (Unknown)

Nmap scan report for seed-router.net-10.9.0.0 (10.9.0.11)
Host is up (0.000010s latency).
All 100 scanned ports on seed-router.net-10.9.0.0 (10.9.0.11) are filtered
MAC Address: 02:42:0A:09:00:0B (Unknown)

Nmap scan report for 4598a8865c51 (10.9.0.5)
Host is up (0.0000020s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 20 IP addresses (3 hosts up) scanned in 3.97 seconds
root@4598a8865c51:/#
```

Protecting Internal Servers

Router

```
root@1f6682ef938e:/# iptables -F
root@1f6682ef938e:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 -j ACCEPT
root@1f6682ef938e:/# iptables -A FORWARD -i eth1 -s 192.168.60.5 -p tcp --sport 23 -j ACCEPT
root@1f6682ef938e:/# iptables -t filter -L -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source               destination

Chain FORWARD (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  0.0.0.0/0            192.168.60.5         tcp dpt:23
2    ACCEPT     tcp  --  192.168.60.5         0.0.0.0/0            tcp spt:23

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
root@1f6682ef938e:/#
```

Host A is able to access 192.168.60.5-internal host but another internal host are not accessible:

```
^C
root@4598a8865c51:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
74cd48bf81e4 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.133.1-microsoft-standard-WSL2 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.
Last login: Thu Nov 30 03:38:21 UTC 2023 on pts/3
seed@74cd48bf81e4:~$ exit
logout
Connection closed by foreign host.
root@4598a8865c51:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
root@4598a8865c51:/# telnet 192.168.60.7
Trying 192.168.60.7...
^C
root@4598a8865c51:/# ping 192.168.60.7
PING 192.168.60.7 (192.168.60.7) 56(84) bytes of data.
```

Nmap:

```
root@4598a8865c51:/# nmap -p 1-100 10.9.0.1-20
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-30 03:57 UTC
Nmap scan report for 10.9.0.1
Host is up (0.000025s latency).
All 100 scanned ports on 10.9.0.1 are closed
MAC Address: 02:42:3C:22:12:92 (Unknown)

Nmap scan report for seed-router.net-10.9.0.0 (10.9.0.11)
Host is up (0.0000070s latency).
All 100 scanned ports on seed-router.net-10.9.0.0 (10.9.0.11) are filtered
MAC Address: 02:42:0A:09:00:0B (Unknown)

Nmap scan report for 4598a8865c51 (10.9.0.5)
Host is up (0.0000020s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 20 IP addresses (3 hosts up) scanned in 4.00 seconds
root@4598a8865c51:/#
```

Host 192.168.60.5 is accessing 192.168.60.6

```
Connection closed by foreign host.
root@74cd48bf81e4:/# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
bddbb020f91c login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.133.1-microsoft-standard-WSL2 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@bddbb020f91c:~$
```

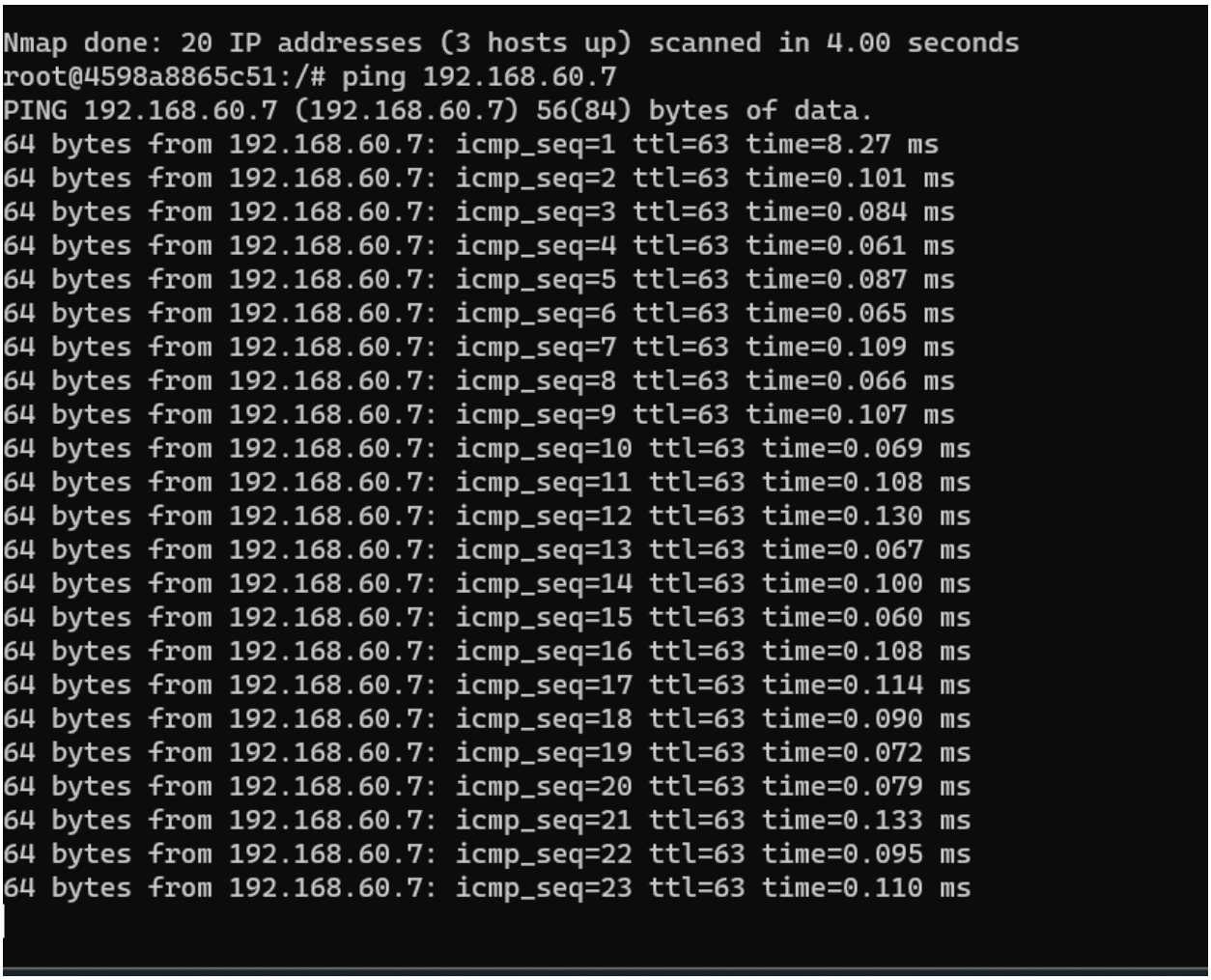
Tried to access the external server from internal host.

```
root@74cd48bf81e4:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

In the previous task, we have only set up stateless firewalls.

Connection Tracking and Stateful Firewall

pinging from external host to internal host



Output from router

```
root@1f6682ef938e:/# conntrack -L -O EXTENDED
conntrack v1.4.5 (conntrack-tools): unknown option `-O'
Try `conntrack -h' or 'conntrack --help' for more information.
root@1f6682ef938e:/# conntrack -L -o extended
ipv4     2 icmp     1 29 src=192.168.60.5 dst=10.9.0.5 type=8 code=0 id=22 s
rc=10.9.0.5 dst=192.168.60.5 type=0 code=0 id=22 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@1f6682ef938e:/# conntrack -L -o extended
ipv4     2 icmp     1 29 src=192.168.60.5 dst=10.9.0.5 type=8 code=0 id=22 s
rc=10.9.0.5 dst=192.168.60.5 type=0 code=0 id=22 mark=0 use=1
ipv4     2 icmp     1 29 src=10.9.0.5 dst=192.168.60.7 type=8 code=0 id=26 s
rc=192.168.60.7 dst=10.9.0.5 type=0 code=0 id=26 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@1f6682ef938e:/#
```

```
root@1f6682ef938e:/# conntrack -L -o extended
ipv4     2 icmp     1 29 src=192.168.60.5 dst=10.9.0.5 type=8 code=0 id=22 s
rc=10.9.0.5 dst=192.168.60.5 type=0 code=0 id=22 mark=0 use=1
ipv4     2 icmp     1 25 src=10.9.0.5 dst=192.168.60.7 type=8 code=0 id=26 s
rc=192.168.60.7 dst=10.9.0.5 type=0 code=0 id=26 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@1f6682ef938e:/# conntrack -L
icmp     1 29 src=192.168.60.5 dst=10.9.0.5 type=8 code=0 id=22 src=10.9.0.5
 dst=192.168.60.5 type=0 code=0 id=22 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@1f6682ef938e:/#
```

Experiment with the Connection Tracking

On host 10.9.0.5, send ICMP packets to 192.168.60.5

```
root@4598a8865c51:/# 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=0.171 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.092 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.099 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.104 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.109 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.123 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.087 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.072 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.094 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.108 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.098 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.079 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.104 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.099 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.114 ms
64 bytes from 192.168.60.5: icmp_seq=16 ttl=63 time=0.093 ms
64 bytes from 192.168.60.5: icmp_seq=17 ttl=63 time=0.193 ms
64 bytes from 192.168.60.5: icmp_seq=18 ttl=63 time=0.304 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.100 ms
64 bytes from 192.168.60.5: icmp_seq=20 ttl=63 time=0.068 ms
64 bytes from 192.168.60.5: icmp_seq=21 ttl=63 time=0.068 ms
64 bytes from 192.168.60.5: icmp_seq=22 ttl=63 time=0.133 ms
```

How long is the ICMP connection state be kept?

According to my observation tcp connection state kept is kept around 30 sec

On the router container,

```
root@1f6682ef938e:/# conntrack -L
icmp     1 29 src=192.168.60.5 dst=10.9.0.5 type=8 code=0 id=22 src=10.9.0.5 dst=192.168.60.5 type=0 code=0 id=22 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@1f6682ef938e:/#
```

On 192.168.60.5, start a netcat UDP server

```
root@74cd48bf81e4:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
root@74cd48bf81e4:/# nc -lu 9090
^C
root@74cd48bf81e4:/# # nc -lu 9090
root@74cd48bf81e4:/# nc -lu 9090
hi
hello
^C
root@74cd48bf81e4:/#
```

On host 10.9.0.5, send UDP packets to 192.168.60.5

```
root@4598a8865c51:/# # nc -lu 9090
root@4598a8865c51:/# nc -u 192.168.60.5 9090
hi
root@4598a8865c51:/#
```

How long is the UDP connection state be kept?
According to my observation tcp connection state kept is kept about a min

Router:

```
udp      17 26 src=10.9.0.5 dst=192.168.60.5 sport=40109 dport=9090 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=40109 mark=0 use=1
icmp     1 29 src=192.168.60.5 dst=10.9.0.5 type=8 code=0 id=22 src=10.9.0.5 dst=192.168.60.5 type=0 code=0 id=22 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@1f6682ef938e:/# conntrack -L
udp      17 23 src=10.9.0.5 dst=192.168.60.5 sport=40109 dport=9090 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=40109 mark=0 use=1
icmp     1 29 src=192.168.60.5 dst=10.9.0.5 type=8 code=0 id=22 src=10.9.0.5 dst=192.168.60.5 type=0 code=0 id=22 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@1f6682ef938e:/#
```

TCP Experiment:

On 192.168.60.5, start a netcat TCP server:

```
root@74cd48bf81e4:/# nc -l 9090
hihellooooo
^C
root@74cd48bf81e4:/#
```

On host 10.9.0.5, send TCP packets to 192.168.60.5:

```
root@4598a8865c51:/# nc 192.168.60.5 9090
hihellooooo
PS C:\Users\priya>
```

On the router container

```
root@1f6682ef938e:/# conntrack -L -o extended
ipv4     2 icmp     1 29 src=192.168.60.5 dst=10.9.0.5 type=8 code=0 id=22 src=10.9.0.5 dst=192.168.60.5 type=0 code=0 id=22 mark=0 use=1
ipv4     2 tcp      6 431991 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=45470 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=45470 [ASSURED]
 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@1f6682ef938e:/#
```

Nmap:

```
root@4598a8865c51:/# nmap -p 1-100 10.9.0.1-10.9.0.15
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-30 05:41 UTC
Failed to resolve "10.9.0.1-10.9.0.15".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.20 seconds
root@4598a8865c51:/# nmap -p 1-100 10.9.0.1-15
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-30 05:42 UTC
Nmap scan report for 10.9.0.1
Host is up (0.0000030s latency).
All 100 scanned ports on 10.9.0.1 are closed
MAC Address: 02:42:3C:22:12:92 (Unknown)

Nmap scan report for seed-router.net-10.9.0.0 (10.9.0.11)
Host is up (0.0000050s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 02:42:0A:09:00:0B (Unknown)

Nmap scan report for 4598a8865c51 (10.9.0.5)
Host is up (0.0000020s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 15 IP addresses (3 hosts up) scanned in 1.81 seconds
root@4598a8865c51:/#
```

Describe your observation. How long is the TCP connection state kept?
According to my observation tcp connection state kept is kept more 1min

Setting Up a Stateful Firewall

```
root@1f6682ef938e:/# iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
root@1f6682ef938e:/# iptables -A FORWARD -p tcp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
root@1f6682ef938e:/# iptables -A FORWARD -p tcp -i eth1 -o eth0 --dport 8080 --syn -m conntrack --ctstate NEW -j ACCEPT
root@1f6682ef938e:/# iptables -P FORWARD DROP
root@1f6682ef938e:/# iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:8080 flags:0x17/0x02 ctstate NEW

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@1f6682ef938e:/#
```

using the connection tracking mechanism

```
root@1f6682ef938e:/# iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
root@1f6682ef938e:/# iptables -A FORWARD -p tcp --sport 8080 -m state --state ESTABLISHED -j ACCEPT
root@1f6682ef938e:/# iptables -A FORWARD -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
root@1f6682ef938e:/# iptables -A FORWARD -p tcp -i eth1 -o eth0 --dport 8080 --syn -m state --state NEW -j ACCEPT
root@1f6682ef938e:/# iptables -P FORWARD DROP
root@1f6682ef938e:/# iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:8080 state ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:80 state ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:8080 flags:0x17/0x02 state NEW

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@1f6682ef938e:/#
```

The connection tracking mechanism provides a more straightforward and automated way to handle stateful firewall rules, while the non-tracking mechanism might be used in resource-constrained environments

Load Balancing

Using the nth mode (round-robin)

Router

```
C:\Users\priya\OneDrive\Documents\Labsetup\Labsetup>docker exec -it seed-router bash
root@5473c66651f3:/# iptables -F
root@5473c66651f3:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --packet 0 -j DNAT --to-destination 192.168.60.5:80
80
root@5473c66651f3:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --packet 1 -j DNAT --to-destination 192.168.60.6:80
80
root@5473c66651f3:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --packet 2 -j DNAT --to-destination 192.168.60.7:80
80
root@5473c66651f3:/#
```

HOST A:

```
root@60581c8284a5:/# echo hello | nc -u 10.9.0.11 8080
hello
^C
root@60581c8284a5:/# echo hello1 | nc -u 10.9.0.11 8080
hello1
^C
root@60581c8284a5:/# echo hello2 | nc -u 10.9.0.11 8080
root@60581c8284a5:/# echo hello2 | nc -u 10.9.0.11 8080
hello2
```

HOST1:

```
PS C:\Users\priya\OneDrive\Documents\Labsetup\Labsetup> docker exec -it host1-192.168.60.5 bash
root@a91a712e2196:/# nc -luk 8080
hello1
hello1
^C
root@a91a712e2196:/# nc -luk 8080
hello
```

Host2:

```
PS C:\Users\priya> cd C:\Users\priya\OneDrive\Documents\Labsetup\Labsetup
PS C:\Users\priya\OneDrive\Documents\Labsetup\Labsetup> docker exec -it host2-192.168.60.6 bash
root@5d9e3edf8b5e:/# nc -luk 8080
hello
^C
root@5d9e3edf8b5e:/# nc -luk 8080
hell1
```

Host3:

```
PS C:\Users\priya> cd C:\Users\priya\OneDrive\Documents\Labsetup\Labsetup
PS C:\Users\priya\OneDrive\Documents\Labsetup\Labsetup> docker exec -it host3-192.168.60.7 bash
root@ba24a1cb306a:/# nc -luk 8080
hello2
^C
root@ba24a1cb306a:/# nc -luk 8080
```

Using the random mode

Seed router:

Explanation:

First rule Uses the statistic module with the random mode and sets the probability to 0.33. Third rule it uses the statistic module with the random mode, but the probability is set to 0.50 (50%). Second rule It matches UDP packets with destination port 8080 and directs them to the IP address 192.168.60.6 on port 8080.

```
root@320d762bdeff:/# iptables -F
root@320d762bdeff:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 0.33 -j DNAT --to-destination 192.168.60.5:8
080
root@320d762bdeff:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -j DNAT --to-destination 192.168.60.6:8080
root@320d762bdeff:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 0.50 -j DNAT --to-destination 192.168.60.7:8
080
```

External host:

```
root@6d4d0563a590:/# nc -u 10.9.0.11 8080
123
456
789
901
902
1210
1012
11122233654
14789655644412358
77777777777777777777777777777777
888888888888888888888888888888888888888888
789878
77777777777779999999999999999999999999999999999999999999999999999777777777777777777777777777
15151515
48484847888
48484848
1212121212
14454545454
45845121
1515151515151
151515151515151515151
12646848684684
555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555
46464646
```

Internal host 1

```
root@3a354333236b:/# nc -luk 8080
123
456
789
901
902
1210
1012
11122233654
14789655644412358
777777777777777777777777777777777
888888888888888888888888888888888888888888
789878
7777777777777799999999999999999999999999999999999999999999999999999777777777777777777777777777
```

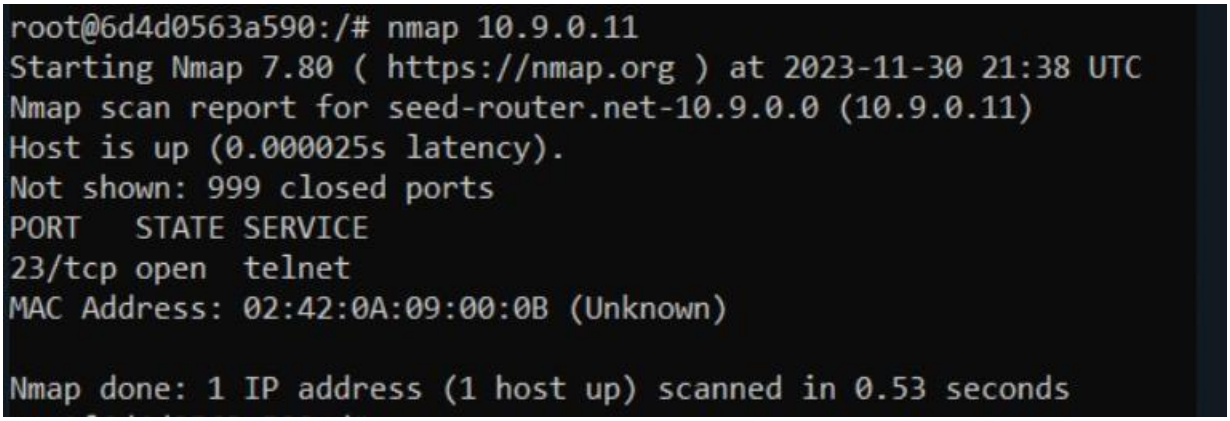
Internal host 2:

```
root@441ca4d4f7b6:/# nc -luk 8080
46464646
```

Internal host 3:

```
root@ff6fc7a6c43b:/# nc -luk 8080
15151515
48484847888
48484848
1212121212
14454545454
45845121
1515151515151
151515151515151515l
12646848684684
55555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555
55555555555555555555555555555555555555555
S
```

Nmap:



Purpose of nth Mode (Round-Robin):

Distributes incoming traffic evenly in a sequential manner among the available servers.

Use Cases:
For uniform distribution without load not considering server load.
Advantages:
1.It's simple to implement
2.All the servers will get equal share of request.

Disadvantages:

1. It Doesn't consider server load.

Purpose Random Mode:

Assigns incoming requests randomly to available servers.
For scenarios where you want to distribute traffic without considering the current load on servers.
Advantages:
1.it's straightforward to implement.
2.Useful in the case where a bit of unpredictability in load distribution is acceptable.
Disadvantages:
1.Unequal Distribution
2.Lack of Consideration for Server Load

My opinion:
The choice between Round Robin and Random modes for load balancing depends on the specific requirements and both have their own merits and demerits. Depending on the applications requirement we need the one which best suits the requirements.

Interesting facts:
The concept of setting up a stateful firewall is more interesting. The transformation from stateless to stateful firewall shows the evolution in network security.