WEEK 7 - Firewall Exploration 2022

Name: Adarsh Kumar	SRN No: PES2UG20CS016	Assignment No: 07
	Section: B	Date: 21/10/2022

Task 1:	Implementing a Simple Firewall
Task 1.A:	Implement a Simple Kernel Module
Screenshot	Loading and removing a moduole to kernel.

```
Host-VM/PES2UG20CS016/AdarshKumar/>$make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/cns/Labsetup/volumes/Codes/kernel_module modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  Building modules, stage 2.
  MODPOST 1 modules
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
Host-VM/PES2UG20CS016/AdarshKumar/>$sudo insmod hello.ko
Host-VM/PES2UG20CS016/AdarshKumar/>$lsmod | grep hello
hello                  16384  0
Host-VM/PES2UG20CS016/AdarshKumar/>$sudo rmmod hello
Host-VM/PES2UG20CS016/AdarshKumar/>$
```

We can see that our inserted kernel module is printing message to in the /var/log/syslog file.

```
[ 1316.085662] br-d493d6eeb794: port 4(veth9f3d5c8) entered blocking state
[ 1316.085663] br-d493d6eeb794: port 4(veth9f3d5c8) entered forwarding state
[ 2881.651093] hello: module verification failed: signature and/or required key missing - tainting kernel
[ 2881.652375] Hello World!
[ 2914.404819] Bye-bye World!.
```

Task 1.B:	Implement a Simple Firewall Using Netfilter.
1.)	

```
VM/PES2UG20CS016/AdasrhKumar/>$dig @8.8.8.8 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41690
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        21042   IN      A       93.184.216.34

;; Query time: 12 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Oct 27 06:04:34 EDT 2022
;; MSG SIZE  rcvd: 60

VM/PES2UG20CS016/AdasrhKumar/>$
```

```
VM/PES2UG20CS016/AdasrhKumar/>$make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/cns/Labsetup/volumes/Codes/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CC [M]  /home/seed/Desktop/cns/Labsetup/volumes/Codes/packet_filter/seedFilter.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/Desktop/cns/Labsetup/volumes/Codes/packet_filter/seedFilter.mod.o
  LD [M]  /home/seed/Desktop/cns/Labsetup/volumes/Codes/packet_filter/seedFilter.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
VM/PES2UG20CS016/AdasrhKumar/>$sudo ismod seedFilter.ko
sudo: ismod: command not found
VM/PES2UG20CS016/AdasrhKumar/>$sudo insmod seedFilter.ko
```

The above screenshot shows that the module is successfully compiled and loaded in the kernel.

```
VM/PES2UG20CS016/AdasrhKumar/>$lsmod | grep seedFilter
seedFilter             16384  0
VM/PES2UG20CS016/AdasrhKumar/>$dig @8.8.8.8 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 www.example.com
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached

VM/PES2UG20CS016/AdasrhKumar/>$sudo rmmod seedFilter
VM/PES2UG20CS016/AdasrhKumar/>$
```

We can see that is says that the connection time out no server could be reached.

```
[  940.163915] seedFilter: module verification failed: signature and/or required key missing - tainting kernel
[  940.164746] Registering filters.
[ 1031.032801] *** LOCAL_OUT
[ 1031.032803]     127.0.0.1  --> 224.0.0.251 (UDP)
[ 1032.549440] *** LOCAL_OUT
[ 1032.549443]     10.0.2.5  --> 224.0.0.251 (UDP)
[ 1038.211178] *** LOCAL_OUT
[ 1038.211183]     172.17.0.1  --> 224.0.0.251 (UDP)
[ 1041.275578] *** LOCAL_OUT
[ 1041.275580]     127.0.0.1  --> 127.0.0.1 (UDP)
[ 1041.276080] *** LOCAL_OUT
[ 1041.276082]     10.0.2.5  --> 8.8.8.8 (UDP)
[ 1041.276088] *** Dropping 8.8.8.8 (UDP), port 53
[ 1046.276905] *** LOCAL_OUT
[ 1046.276910]     10.0.2.5  --> 8.8.8.8 (UDP)
[ 1046.276937] *** Dropping 8.8.8.8 (UDP), port 53
[ 1051.274944] *** LOCAL_OUT
[ 1051.275518]     10.0.2.5  --> 8.8.8.8 (UDP)
[ 1051.275549] *** Dropping 8.8.8.8 (UDP), port 53
[ 1090.920284] *** LOCAL_OUT
[ 1090.920290]     10.9.0.1  --> 224.0.0.251 (UDP)
[ 1091.066183] *** LOCAL_OUT
[ 1091.066188]     192.168.60.1  --> 224.0.0.251 (UDP)
[ 1100.638414] The filters are being removed.
```

Stopping the UDP packet of part 53

2.)

```
VM/PES2UG20CS016/AdasrhKumar/>$pwd
/home/seed/Desktop/cns/Labsetup/volumes/Codes/packet_filter
VM/PES2UG20CS016/AdasrhKumar/>$make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/cns/Labsetup/volumes/Codes/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CC [M]  /home/seed/Desktop/cns/Labsetup/volumes/Codes/packet_filter/seedPrint.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/Desktop/cns/Labsetup/volumes/Codes/packet_filter/seedPrint.mod.o
  LD [M]  /home/seed/Desktop/cns/Labsetup/volumes/Codes/packet_filter/seedPrint.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
VM/PES2UG20CS016/AdasrhKumar/>$sudo insmode seedPrint.ko
sudo: insmode: command not found
VM/PES2UG20CS016/AdasrhKumar/>$sudo insmod seedPrint.ko
VM/PES2UG20CS016/AdasrhKumar/>$lsmod | grep seedPrint
seedPrint              16384  0
```

```
VM/PES2UG20CS016/AdasrhKumar/>$dig @8.8.8.8 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29646
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        20240   IN      A       93.184.216.34

;; Query time: 12 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Oct 27 06:53:50 EDT 2022
;; MSG SIZE  rcvd: 60

VM/PES2UG20CS016/AdasrhKumar/>$sudo rmmod seedPrint
```

```
VM/PES2UG20CS016/AdasrhKumar/>$sudo dmesg -k -w
[ 3696.026249] Registering filters.
[ 3710.160332] *** LOCAL_OUT
[ 3710.160337]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 3710.160360] *** POST_ROUTING
[ 3710.160362]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 3710.160381] *** PRE_ROUTING
[ 3710.160383]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 3710.160386] *** LOCAL_IN
[ 3710.160388]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 3710.162053] *** LOCAL_OUT
[ 3710.162057]     10.0.2.5  --> 202.138.96.2 (UDP)
[ 3710.162076] *** POST_ROUTING
[ 3710.162078]     10.0.2.5  --> 202.138.96.2 (UDP)
[ 3710.754317] *** PRE_ROUTING
[ 3710.754786]     202.138.96.2  --> 10.0.2.5 (UDP)
[ 3710.755109] *** LOCAL_IN
[ 3710.755546]     202.138.96.2  --> 10.0.2.5 (UDP)
[ 3710.756329] *** LOCAL_OUT
[ 3710.756330]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 3710.756334] *** POST_ROUTING
[ 3710.756334]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 3710.756342] *** PRE_ROUTING
[ 3710.756342]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 3710.756343] *** LOCAL_IN
[ 3710.756344]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 3710.756568] *** LOCAL_OUT
[ 3710.756572]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 3710.756587] *** POST_ROUTING
[ 3710.756588]     127.0.0.1  --> 127.0.0.53 (UDP)
```

```
[ 3780.025108] *** LOCAL_IN
[ 3780.025258]     35.224.170.84  --> 10.0.2.5 (TCP)
[ 3780.026144] *** LOCAL_OUT
[ 3780.026145]     10.0.2.5  --> 35.224.170.84 (TCP)
[ 3780.026148] *** POST_ROUTING
[ 3780.026149]     10.0.2.5  --> 35.224.170.84 (TCP)
[ 3780.027937] *** PRE_ROUTING
[ 3780.027939]     35.224.170.84  --> 10.0.2.5 (TCP)
[ 3780.027945] *** LOCAL_IN
[ 3780.027946]     35.224.170.84  --> 10.0.2.5 (TCP)
[ 3788.196611] The filters are being removed.
```

We can see that TCP, UDP Connections are working.

3.)

```
VM/PES2UG20CS016/AdasrhKumar/>$make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/cns/Labsetup/volumes/Codes/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CC [M]  /home/seed/Desktop/cns/Labsetup/volumes/Codes/packet_filter/seedBlock.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/Desktop/cns/Labsetup/volumes/Codes/packet_filter/seedBlock.mod.o
  LD [M]  /home/seed/Desktop/cns/Labsetup/volumes/Codes/packet_filter/seedBlock.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
VM/PES2UG20CS016/AdasrhKumar/>$sudo insmod seedBlock.ko
VM/PES2UG20CS016/AdasrhKumar/>$lsmod | grep seedBlock
seedBlock              16384  0
VM/PES2UG20CS016/AdasrhKumar/>$sudo rmmod seedBlock
VM/PES2UG20CS016/AdasrhKumar/>$sudo dmesg -C
VM/PES2UG20CS016/AdasrhKumar/>$
```

```
root@a9bf42ea63af:/# export PS1="Host-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$"
Host-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$ping 10.9.0.1
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data.
^C
--- 10.9.0.1 ping statistics ---
13 packets transmitted, 0 received, 100% packet loss, time 12277ms

Host-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$telnet 10.9.0.1
Trying 10.9.0.1...
^C
Host-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$
```

```
VM/PES2UG20CS016/AdasrhKumar/>$sudo dmesg -k -w
[ 5009.114265] Registering filters.
[ 5015.179571] *** LOCAL_OUT
[ 5015.179576]     10.0.2.5  --> 224.0.0.251 (UDP)
[ 5050.996792] *** Dropping 10.9.0.1 (ICMP)
[ 5052.007051] *** Dropping 10.9.0.1 (ICMP)
[ 5053.029388] *** Dropping 10.9.0.1 (ICMP)
[ 5054.057494] *** Dropping 10.9.0.1 (ICMP)
[ 5055.076847] *** Dropping 10.9.0.1 (ICMP)
[ 5056.101558] *** Dropping 10.9.0.1 (ICMP)
[ 5057.123422] *** Dropping 10.9.0.1 (ICMP)
[ 5058.146914] *** Dropping 10.9.0.1 (ICMP)
[ 5059.170312] *** Dropping 10.9.0.1 (ICMP)
[ 5060.194772] *** Dropping 10.9.0.1 (ICMP)
[ 5061.217734] *** Dropping 10.9.0.1 (ICMP)
[ 5062.241548] *** Dropping 10.9.0.1 (ICMP)
[ 5063.267969] *** Dropping 10.9.0.1 (ICMP)
[ 5067.774034] *** LOCAL_OUT
[ 5067.774037]     10.0.2.5  --> 10.0.2.3 (UDP)
[ 5088.378007] *** Dropping 10.9.0.1 (TCP), port 23
[ 5089.396043] *** Dropping 10.9.0.1 (TCP), port 23
[ 5091.410338] *** Dropping 10.9.0.1 (TCP), port 23
[ 5095.601952] *** Dropping 10.9.0.1 (TCP), port 23
[ 5126.559885] The filters are being removed.
```

Here we can see that All our ICMP Packets as well as Telnet Packets are dropped.

Task 2 — Experimenting with Stateless Firewall Rules

Task 2.A: Protecting the Router

```
Router/PES2UG20CS016/AdasrhKumar/>$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
Router/PES2UG20CS016/AdasrhKumar/>$
```

```
Router/PES2UG20CS016/AdasrhKumar/>$iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
Router/PES2UG20CS016/AdasrhKumar/>$iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
Router/PES2UG20CS016/AdasrhKumar/>$iptables -P OUTPUT DROP
Router/PES2UG20CS016/AdasrhKumar/>$iptables -P INPUT DROP
Router/PES2UG20CS016/AdasrhKumar/>$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            icmptype 8

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0            icmptype 0
Router/PES2UG20CS016/AdasrhKumar/>$
```

Here we are accepting the ICMP Packet In, Out.

```
Host_A-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$ping seed-router
PING seed-router (10.9.0.11) 56(84) bytes of data.
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=1 ttl=64 time=0.241 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=2 ttl=64 time=0.099 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=3 ttl=64 time=0.096 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=4 ttl=64 time=0.066 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=5 ttl=64 time=0.084 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=6 ttl=64 time=0.117 ms
^C
--- seed-router ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5117ms
rtt min/avg/max/mdev = 0.066/0.117/0.241/0.057 ms
Host_A-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$telnet seed-router
Trying 10.9.0.11...
^C
Host_A-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$
```

Questions:

(1) Can you ping the router?
ANS: Yes, I can ping to the router

(2) Can you telnet into the router?
ANS: No, I can't able to telnet to the router because Telnet connection blocked.

Restoring the filter table to its original state

```
Router/PES2UG20CS016/AdasrhKumar/>$iptables -F
Router/PES2UG20CS016/AdasrhKumar/>$iptables -P OUTPUT ACCEPT
Router/PES2UG20CS016/AdasrhKumar/>$iptables -P INPUT ACCEPT
Router/PES2UG20CS016/AdasrhKumar/>$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
Router/PES2UG20CS016/AdasrhKumar/>$
```

Task 2.B:	Protecting the Internal Network

```
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DROP
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -A FORWARD -i eth1 -p icmp --icmp-type echo-request -j ACCEPT
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-reply -j ACCEPT
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -P FORWARD DROP
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       icmp --  eth0   *       0.0.0.0/0            0.0.0.0/0           icmptype 8
    0     0 ACCEPT     icmp --  eth1   *       0.0.0.0/0            0.0.0.0/0           icmptype 8
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0            0.0.0.0/0           icmptype 0

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
seed-router/PES2UG20CS016/AdasrhKumar/>$
```

1. Outside hosts cannot ping internal hosts.

```
Host_A-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$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 ---
118 packets transmitted, 0 received, 100% packet loss, time 119820ms

Host_A-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$
```

2. Outside hosts can ping the router.

```
Host_A-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$ping seed-router
PING seed-router (10.9.0.11) 56(84) bytes of data.
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=1 ttl=64 time=0.043 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=2 ttl=64 time=0.087 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=3 ttl=64 time=0.112 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=4 ttl=64 time=0.084 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=5 ttl=64 time=0.104 ms
^C
--- seed-router ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4083ms
rtt min/avg/max/mdev = 0.043/0.086/0.112/0.023 ms
Host_A-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$
```

3. Internal hosts can ping Outside Hosts.

```
host1/PES2UG20CS016/AdasrhKumar/>$ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=63 time=0.174 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.150 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.176 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.130 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.133 ms
64 bytes from 10.9.0.5: icmp_seq=6 ttl=63 time=0.053 ms
^C
--- 10.9.0.5 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5119ms
rtt min/avg/max/mdev = 0.053/0.136/0.176/0.041 ms
host1/PES2UG20CS016/AdasrhKumar/>$
```

4. All other packets between the internal and external networks should be blocked.

```
host1/PES2UG20CS016/AdasrhKumar/>$telnet 10.9.0.5
Trying 10.9.0.5...
^C
host1/PES2UG20CS016/AdasrhKumar/>$
```

Cleaning iptables:

```
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -F
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -P OUTPUT ACCEPT
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -P INPUT ACCEPT
seed-router/PES2UG20CS016/AdasrhKumar/>$
```

Task 2.C: Protecting Internal Servers

```
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 -j ACCEPT
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -A FORWARD -i eth1 -s 192.168.60.5 -p tcp --sport 23 -j ACCEPT
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -P FORWARD DROP
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0            192.168.60.5         tcp dpt:23
    0     0 ACCEPT     tcp  --  eth1   *       192.168.60.5         0.0.0.0/0            tcp spt:23

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
seed-router/PES2UG20CS016/AdasrhKumar/>$
```

1. 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

```
Host_A-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
sUbuntu 20.04.1 LTS
s92ac4401b752 login: dees
Password:

Login incorrect
92ac4401b752 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.

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@92ac4401b752:~$ exit
logout
Connection closed by foreign host.
```

2. Outside hosts cannot access other internal servers.

```
Host_A-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$telnet 192.168.60.6
Trying 192.168.60.6...
^C
Host_A-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$telnet 192.168.60.7
Trying 192.168.60.7...
^C
Host_A-10.9.0.5/PES2UG20CS016/AdasrhKumar/>$
```

3. Internal hosts can access all the internal servers.

```
host2/PES2UG20CS016/AdasrhKumar/>$telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
2df667178bf7 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.

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@2df667178bf7:~$ exit
logout
Connection closed by foreign host.
```

```
host2/PES2UG20CS016/AdasrhKumar/>$telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
92ac4401b752 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.
Last login: Thu Oct 27 12:26:24 UTC 2022 on pts/2
seed@92ac4401b752:~$ exit
logout
Connection closed by foreign host.
host2/PES2UG20CS016/AdasrhKumar/>$
```

4. Internal hosts cannot access external servers

```
host2/PES2UG20CS016/AdasrhKumar/>$telnet 10.9.0.5
Trying 10.9.0.5...
^C
host2/PES2UG20CS016/AdasrhKumar/>$
```

Cleaning iptables:

```
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -F
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -P OUTPUT ACCEPT
seed-router/PES2UG20CS016/AdasrhKumar/>$iptables -P INPUT ACCEPT
seed-router/PES2UG20CS016/AdasrhKumar/>$
```

Task 3:	**Connection Tracking and Stateful Firewall**
Task 3.A:	Experiment with the Connection Tracking

ICMP experiment:

```
host_A/PES2UG20CS016/AdarshKumar/>$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=0.069 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.069 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.076 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.132 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.071 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.100 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.075 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.068 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.072 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.103 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.072 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.112 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.065 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.072 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.137 ms
^C
--- 192.168.60.5 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14314ms
rtt min/avg/max/mdev = 0.065/0.086/0.137/0.023 ms
```

```
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
icmp     1 27 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=28 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 id=28 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
icmp     1 29 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=29 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 id=29 mark=0 use=1
icmp     1 20 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=28 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 id=28 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
icmp     1 29 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=29 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 id=29 mark=0 use=1
icmp     1 14 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=28 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 id=28 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
icmp     1 29 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=29 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 id=29 mark=0 use=1
icmp     1 11 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=28 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 id=28 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$
```

How long can the ICMP connection state be kept?

Ans: ICMP requests has a default timeout of 30 seconds,
which you can change in the /proc/sys/net/ipv4/netfilter/ip_ct_icmp_timeout entry.

UDP experiment:

```
host_1/PES2UG20CS016/AdarshKumar/>$nc -lu 9090
hello
how are you
me fine
^C
host_1/PES2UG20CS016/AdarshKumar/>$
```

```
host_A/PES2UG20CS016/AdarshKumar/>$nc -u 192.168.60.5 9090
hello
how are you
me fine
^C
host_A/PES2UG20CS016/AdarshKumar/>$
```

```
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
udp      17 17 src=10.9.0.5 dst=192.168.60.5 sport=39305 dport=9090 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=39305 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
udp      17 13 src=10.9.0.5 dst=192.168.60.5 sport=39305 dport=9090 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=39305 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
udp      17 5 src=10.9.0.5 dst=192.168.60.5 sport=39305 dport=9090 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=39305 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
conntrack v1.4.5 (conntrack-tools): 0 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
conntrack v1.4.5 (conntrack-tools): 0 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$
```

How long can the UDP connection state be kept?

The default, UDP connection timeout 30 seconds. As soon we close the connection after 30 seconds router container 0 flow entries as shown.

TCP experiment:

```
host_1/PES2UG20CS016/AdarshKumar/>$nc -l 9090
hi bro
how are you
i am in PESU
ok
nice
exit
^C
host_1/PES2UG20CS016/AdarshKumar/>$
```

```
host_A/PES2UG20CS016/AdarshKumar/>$nc 192.168.60.5 9090
hi bro
how are you
i am in PESU
ok
nice
exit
^C
host_A/PES2UG20CS016/AdarshKumar/>$
```

```
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
tcp      6 431986 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=59414 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=59414 [ASSURED]
mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
tcp      6 431997 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=59414 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=59414 [ASSURED]
mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
tcp      6 431998 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=59414 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=59414 [ASSURED]
mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
tcp      6 117 TIME_WAIT src=10.9.0.5 dst=192.168.60.5 sport=59414 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=59414 [ASSURED] mark=
0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
tcp      6 117 TIME_WAIT src=10.9.0.5 dst=192.168.60.5 sport=59414 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=59414 [ASSURED] mark=
0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
tcp      6 108 TIME_WAIT src=10.9.0.5 dst=192.168.60.5 sport=59414 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=59414 [ASSURED] mark=
0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$conntrack -L
tcp      6 76 TIME_WAIT src=10.9.0.5 dst=192.168.60.5 sport=59414 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=59414 [ASSURED] mark=0
 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
seed-router/PES2UG20CS016/AdarshKumar/>$
```

Do you spot any difference?

Ans: In UDP, as soon as we close connection flow entries become 0 but in TCP flow entries doesn't become 0 as we close our connection

How long can the TCP connection state be kept?

The default, the TCP connection timeout is 15 minutes it is a very long period of time so I haven't waited to show that here, it is because the TCP have a three-way hand shake function

Task 3.B:	Setting Up a Stateful Firewall

On seed-router

```
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -A FORWARD -p tcp -i eth0 -d 192.168.60.5 --dport 23 --syn -m conntrack --ctstate NEW -j ACCEPT
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -A FORWARD -i eth1 -p tcp --syn -m conntrack --ctstate NEW -j ACCEPT
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -A FORWARD -p tcp -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -A FORWARD -p tcp -j DROP
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -P FORWARD ACCEPT
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  eth0   *      0.0.0.0/0            192.168.60.5        tcp dpt:23 flags:0x17/0x02 ctstate NEW
    0     0 ACCEPT     tcp  --  eth0   *      0.0.0.0/0            192.168.60.5        tcp dpt:23 flags:0x17/0x02 ctstate NEW
    0     0 ACCEPT     tcp  --  eth1   *      0.0.0.0/0            0.0.0.0/0           tcp flags:0x17/0x02 ctstate NEW
    0     0 ACCEPT     tcp  --  *      *      0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED
    0     0 DROP       tcp  --  *      *      0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
seed-router/PES2UG20CS016/AdarshKumar/>$
```

1. 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.

```
host_A/PES2UG20CS016/AdarshKumar/>$telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
8b1ff7e85654 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.

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@8b1ff7e85654:~$ exit
logout
Connection closed by foreign host.
host_A/PES2UG20CS016/AdarshKumar/>$
```

We are able to see that HOST -A can telnet to Host 1 internal server.

2. Outside hosts cannot access other internal servers.

```
host_A/PES2UG20CS016/AdarshKumar/>$telnet 192.168.60.6
Trying 192.168.60.6...
^C
host_A/PES2UG20CS016/AdarshKumar/>$telnet 192.168.60.7
Trying 192.168.60.7...
^C
host_A/PES2UG20CS016/AdarshKumar/>$
```

We are able to see that HOST -A can't able to telnet of Host 2 & Host 3 internal server.

3. Internal hosts can access all the internal servers

```
host_2/PES2UG20CS016/AdarshKumar/>$telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
8b1ff7e85654 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.
Last login: Thu Oct 27 17:15:59 UTC 2022 on pts/2
seed@8b1ff7e85654:~$ exit
logout
Connection closed by foreign host.
host_2/PES2UG20CS016/AdarshKumar/>$telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
f5392521a468 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.

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@f5392521a468:~$ exit
logout
Connection closed by foreign host.
```

Taking internal Host 2 we can establish telnet connection to Host 1 & Host 3.

4. Internal hosts can access external servers.

```
host_2/PES2UG20CS016/AdarshKumar/>$telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
8b1ff7e85654 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.
Last login: Thu Oct 27 17:17:27 UTC 2022 from host2-192.168.60.6.net-192.168.60.0 on pts/2
seed@8b1ff7e85654:~$ exit
logout
Connection closed by foreign host.
host_2/PES2UG20CS016/AdarshKumar/>$
```

Internal Host can even make tell net connection to external server Host-A.

Clean-up of Firewall rules

```
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -F
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -P OUTPUT ACCEPT
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -P INPUT ACCEPT
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

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

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
seed-router/PES2UG20CS016/AdarshKumar/>$
```

Task 4: Limiting Network Traffic

On seed-Router

```
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/minute --limit-burst 5 -j ACCEPT
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -A FORWARD -s 10.9.0.5 -j DROP
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       10.9.0.5             0.0.0.0/0           limit: avg 10/min burst 5
    0     0 DROP       all  --  *      *       10.9.0.5             0.0.0.0/0

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
seed-router/PES2UG20CS016/AdarshKumar/>$
```

```
host_A/PES2UG20CS016/AdarshKumar/>$ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.241 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.094 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.071 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.142 ms
64 bytes from 192.168.60.5: icmp_seq=18 ttl=63 time=0.085 ms
64 bytes from 192.168.60.5: icmp_seq=24 ttl=63 time=0.068 ms
64 bytes from 192.168.60.5: icmp_seq=29 ttl=63 time=0.134 ms
64 bytes from 192.168.60.5: icmp_seq=35 ttl=63 time=0.126 ms
64 bytes from 192.168.60.5: icmp_seq=41 ttl=63 time=0.089 ms
64 bytes from 192.168.60.5: icmp_seq=47 ttl=63 time=0.097 ms
64 bytes from 192.168.60.5: icmp_seq=53 ttl=63 time=0.090 ms
64 bytes from 192.168.60.5: icmp_seq=59 ttl=63 time=0.094 ms
64 bytes from 192.168.60.5: icmp_seq=65 ttl=63 time=0.118 ms
64 bytes from 192.168.60.5: icmp_seq=71 ttl=63 time=0.133 ms
64 bytes from 192.168.60.5: icmp_seq=76 ttl=63 time=0.129 ms
64 bytes from 192.168.60.5: icmp_seq=82 ttl=63 time=0.088 ms
^C
--- 192.168.60.5 ping statistics ---
83 packets transmitted, 17 received, 79.5181% packet loss, time 83967ms
rtt min/avg/max/mdev = 0.060/0.109/0.241/0.040 ms
host_A/PES2UG20CS016/AdarshKumar/>$
```

Here we can clearly see that initial 5 packets sequence no as regular but after that we were receiving ICMP_Sequence of jump 5 because we set constraint 10/packet per minute and but limit 5.

same task without the second rule –

On seed-Router

```
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/minute --limit-burst 5 -j ACCEPT
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       10.9.0.5             0.0.0.0/0           limit: avg 10/min burst 5

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
seed-router/PES2UG20CS016/AdarshKumar/>$
```

```
host_A/PES2UG20CS016/AdarshKumar/>$ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.222 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.125 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.109 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.100 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.085 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.080 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.072 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.128 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.121 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.104 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.148 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.156 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.147 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.202 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.101 ms
64 bytes from 192.168.60.5: icmp_seq=16 ttl=63 time=0.128 ms
64 bytes from 192.168.60.5: icmp_seq=17 ttl=63 time=1.18 ms
64 bytes from 192.168.60.5: icmp_seq=18 ttl=63 time=0.080 ms
^C
--- 192.168.60.5 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17369ms
rtt min/avg/max/mdev = 0.072/0.182/1.178/0.244 ms
host_A/PES2UG20CS016/AdarshKumar/>$
```

If second rule is omitted then we are able to get all the packet in ascending order

Please report your observation with screenshots and explain the purpose for each rule?

- 1st rule help to maintain 10 packet/minute and give a burst of 5 initial packet
- 2nd rule gives a jump of 5 packet after bust time.

Task 5: Load Balancing

Using the nth mode (round-robin) –

```
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --packet 0 -j DNAT --to-destination 192.168.60.5:8080
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 2 --packet 0 -j DNAT --to-destination 192.168.60.6:8080
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 1 --packet 0 -j DNAT --to-destination 192.168.60.7:8080
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

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

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
seed-router/PES2UG20CS016/AdarshKumar/>$
```

Implemented policies to equally divide the incoming packets between the three interval servers.

Host A

```
host_A/PES2UG20CS016/AdarshKumar/>$nc -u 10.9.0.11 8080
Hello 1
Hello 2
Hello 3
Adarsh
Kumar
PES2UG20CS016
```

HOST 1 - 192.168.60.5

```
host_1/PES2UG20CS016/AdarshKumar/>$nc -luk 8080
Hello 1
Adarsh
```

HOST 2 - 192.168.60.6

```
host_2/PES2UG20CS016/AdarshKumar/>$nc -luk 8080
Hello 2
Kumar
```

HOST 3 - 192.168.60.7

```
host_3/PES2UG20CS016/AdarshKumar/>$nc -luk 8080
Hello 3
PES2UG20CS016
```

We can observe that when we enter in the text message in the HOST-A machine the message (the incoming packets) gets equally divided between the three interval servers, hence balancing the load on overall machine. The order of message is first one reaches to HOST 1 then HOST 2, then HOST 3 and next message again the next message reaches to HOST 1

Using the random mode-

```
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 0.3333 -j DNAT
--to-destination 192.168.60.5:8080
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 0.5 -j DNAT --t
o-destination 192.168.60.6:8080
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 1 -j DNAT --to-
destination 192.168.60.6:8080
seed-router/PES2UG20CS016/AdarshKumar/>$iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

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

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
seed-router/PES2UG20CS016/AdarshKumar/>$
```

The following rule will select a matching packet with the probability P.

Host A

```
host_A/PES2UG20CS016/AdarshKumar/>$nc -u 10.9.0.11 8080
Adarsh_Hello1
Kumar_Hello2
PES2UG20CS016_Hello3
```

HOST 1 - 192.168.60.5

```
host_1/PES2UG20CS016/AdarshKumar/>$nc -luk 8080
Adarsh_Hello1
```

HOST 2 - 192.168.60.6

```
host_2/PES2UG20CS016/AdarshKumar/>$nc -luk 8080
Kumar_Hello2
```

HOST 3 - 192.168.60.7

```
host_3/PES2UG20CS016/AdarshKumar/>$nc -luk 8080
PES2UG20CS016_Hello3
```

Here, in this rule unlike Round Robbin method this method selects the internal server based on probability it could be completely random no order is followed. In my case the arrival of the first packet is completely random and it(algorithm) could choose any internal server and the probability of getting selected is 33.33%. As you can see that the algorithm choice was HOST 1 for first packet so the next packet algorithm has 2 choices each having 50% chance of getting selected. In my case the algo choice was HOST 2, at the end algorithm got only one choice of HOST 3 with 100% probability of being selected.

THE END