CNS Lab 7 Firewall Exploration

PES1UG20CS084

Aryansh Bhargavan

Task 1: Implementing a Simple Firewall

Task 1.A: Implement a Simple Kernel Module

```
[10/29/22]seed@VM:~/.../kernel_module$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/lab7/Codes/kernel_module modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CC [M]  /home/seed/Desktop/lab7/Codes/kernel_module/hello.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/Desktop/lab7/Codes/kernel_module/hello.mod.o
  LD [M]  /home/seed/Desktop/lab7/Codes/kernel_module/hello.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[10/29/22]seed@VM:~/.../kernel_module$ sudo insmod hello.ko
[10/29/22]seed@VM:~/.../kernel_module$ lsmod | grep hello
hello                  16384  0
[10/29/22]seed@VM:~/.../kernel_module$ sudo rmmod hello
[10/29/22]seed@VM:~/.../kernel_module$
```

```
[ 4208.742745] Hello World!
[ 4228.585534] Bye-bye World!.
```

Explanation:

Task 1.B: Implement a Simple Firewall Using Netfilter

1. `dig @8.8.8.8 www.example.com`

```
[10/29/22]seed@VM:~/.../packet_filter$ 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: 48823
;; 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.        21108   IN      A       93.184.216.34

;; Query time: 60 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sat Oct 29 06:19:41 EDT 2022
;; MSG SIZE  rcvd: 60
```

On another terminal:

```
[10/29/22]seed@VM:~/.../kernel_module$ sudo dmesg -k -w
```

```
obj-m += seedFilter.o
#obj-m += seedPrint.o
#obj-m += seedBlock.o
all:
	make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules

clean:
	make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean

ins:
	sudo dmesg -C
	sudo insmod seedFilter.ko

rm:
	sudo rmmod seedFilter
```

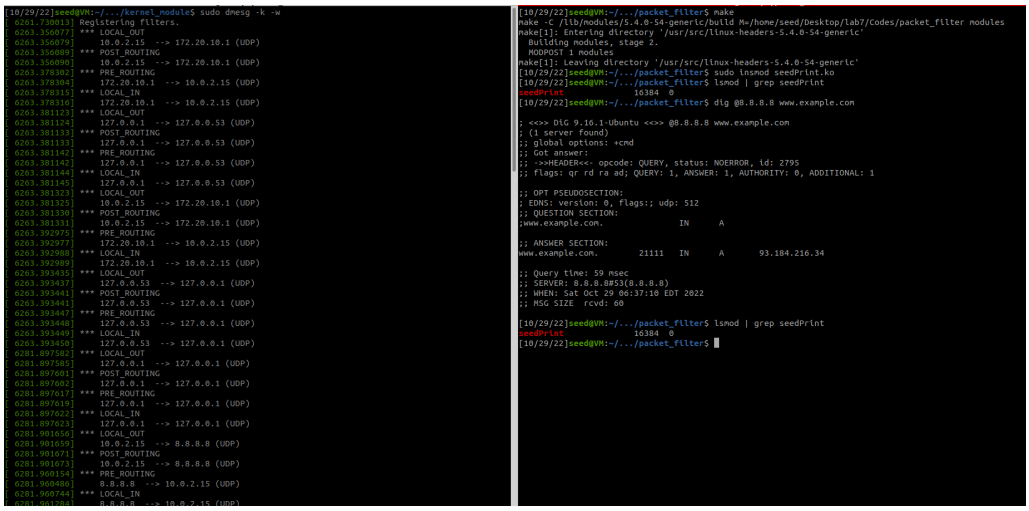
Adding filters

We can see that packet is being dropped since filter was added against `google.com` hence dig does not show any response

2. **Uncommenting - `obj-m += seedPrint.o` and commenting the other two**

```
#obj-m += seedFilter.o
obj-m += seedPrint.o
#obj-m += seedBlock.o
all:
	make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules

clean:
	make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean

ins:
	sudo dmesg -C
	sudo insmod seedFilter.ko

rm:
	sudo rmmod seedFilter
```

Making and running `dig @8.8.8.8 www.example.com`

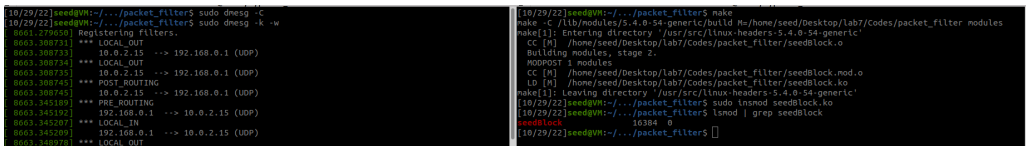


This does not drop the packets, instead it just prints filtered packets

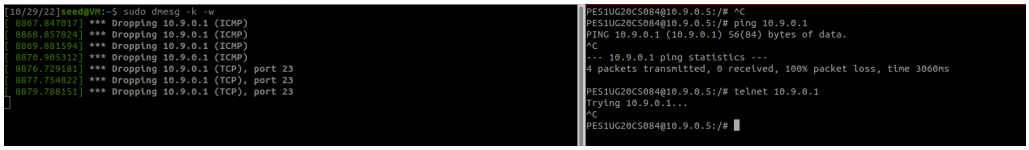
3. **Uncommenting - `obj-m += seedBlock.o` and commenting the other two**

```
#obj-m += seedFilter.o
#obj-m += seedPrint.o
obj-m += seedBlock.o
all:
	make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules

clean:
	make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean

ins:
	sudo dmesg -C
	sudo insmod seedFilter.ko

rm:
	sudo rmmod seedFilter
```

Preforming Make and loading the Module



Attempting to Ping and telnet into `10.9.0.1`

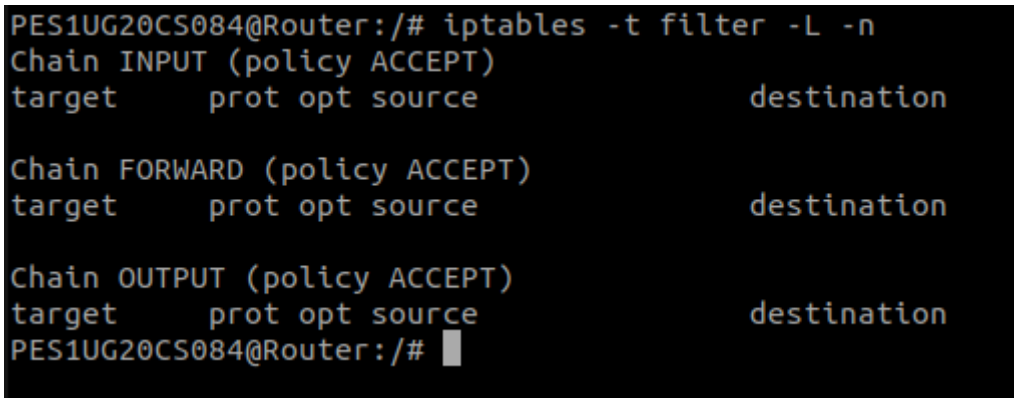


Due to the addition of the filter, ping and telnet have been dropped

Task 2: Experimenting with Stateless Firewall Rules

Task 2.A: Protecting the Router

`iptables -t filter -L -n`



`# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT`

`# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT`

`# iptables -P OUTPUT DROP`

`# iptables -P INPUT DROP`

`# iptables -t filter -L -n`

```
PES1UG20CS084@Router:/#  iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
PES1UG20CS084@Router:/#  iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
PES1UG20CS084@Router:/# iptables -P OUTPUT DROP
PES1UG20CS084@Router:/# iptables -P INPUT DROP
PES1UG20CS084@Router:/#  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
PES1UG20CS084@Router:/#
```

`ping seed-router`

```
PES1UG20CS084@10.9.0.5:/# 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=2.84 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=2 ttl=64 time=0.219 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=3 ttl=64 time=0.216 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=4 ttl=64 time=0.074 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=5 ttl=64 time=0.083 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=6 ttl=64 time=0.128 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=7 ttl=64 time=0.165 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=8 ttl=64 time=0.221 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=9 ttl=64 time=0.158 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=10 ttl=64 time=0.333 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=11 ttl=64 time=0.171 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=12 ttl=64 time=0.252 ms
^C
--- seed-router ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11240ms
rtt min/avg/max/mdev = 0.074/0.404/2.839/0.737 ms
PES1UG20CS084@10.9.0.5:/#
```

`telnet seed-router`

```
PES1UG20CS084@10.9.0.5:/# telnet seed-router
Trying 10.9.0.11...
telnet: Unable to connect to remote host: Connection timed out
PES1UG20CS084@10.9.0.5:/#
```

We are able to ping the router since ICMP request and reply have been allowed but since there is no rule for TCP (Used by telnet) it is filtered; i.e packets are being blocked

---

Task 2.B: Protecting the Internal Network

Setting Rules

```
PES1UG20CS084@Router:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DROP
PES1UG20CS084@Router:/# iptables -A FORWARD -i eth1 -p icmp --icmp-type echo-request -j ACCEPT
PES1UG20CS084@Router:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-reply -j ACCEPT
PES1UG20CS084@Router:/# iptables -P FORWARD DROP
PES1UG20CS084@Router:/# 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
PES1UG20CS084@Router:/#
```

Testing

1. Outside hosts cannot ping internal hosts.

```
PES1UG20CS084@10.9.0.5:/# 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 ---
465 packets transmitted, 0 received, 100% packet loss, time 475550ms

PES1UG20CS084@10.9.0.5:/#
```

2. Outside hosts can ping the router

```
PES1UG20CS084@10.9.0.5:/# 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=3.21 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=2 ttl=64 time=0.068 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=3 ttl=64 time=0.305 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=4 ttl=64 time=0.062 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=5 ttl=64 time=0.167 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=6 ttl=64 time=0.062 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=7 ttl=64 time=0.090 ms
^C
--- seed-router ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6132ms
rtt min/avg/max/mdev = 0.062/0.565/3.205/1.080 ms
PES1UG20CS084@10.9.0.5:/#
```

3. Internal hosts can ping Outside Hosts

```
PES1UG20CS084@192.168.60.5:/# 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=0.196 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.220 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.219 ms
^C
--- 10.9.0.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2030ms
rtt min/avg/max/mdev = 0.196/0.211/0.220/0.011 ms
PES1UG20CS084@192.168.60.5:/#
```

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

```
PES1UG20CS084@192.168.60.5:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
```

Task 2.C: Protecting Internal Servers

Setting the rules

```
PES1UG20CS084@Router:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 -j ACCEPT
PES1UG20CS084@Router:/# iptables -A FORWARD -i eth1 -s 192.168.60.5 -p tcp --sport 23 -j ACCEPT
PES1UG20CS084@Router:/#  iptables -P FORWARD DROP
PES1UG20CS084@Router:/# 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
PES1UG20CS084@Router:/#
```

1. Checking Telnet

```
PES1UG20CS084@10.9.0.5:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
seed
Ubuntu 20.04.1 LTS
seed
c37fb9afb47f 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.
```

2. Outside hosts cannot access other internal servers.

```
PES1UG20CS084@10.9.0.5:/# telnet 192.168.60.6
Trying 192.168.60.6...
telnet: Unable to connect to remote host: Connection timed out
PES1UG20CS084@10.9.0.5:/# telnet 192.168.60.7
Trying 192.168.60.7...
telnet: Unable to connect to remote host: Connection timed out
PES1UG20CS084@10.9.0.5:/#
```

3. Internal hosts can access all the internal servers.

```
PES1UG20CS084@192.168.60.6:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c37fb9afb47f 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: Sat Oct 29 12:20:28 UTC 2022 on pts/2
seed@c37fb9afb47f:~$
```

```
PES1UG20CS084@192.168.60.6:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
283d3f27289c 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.
```

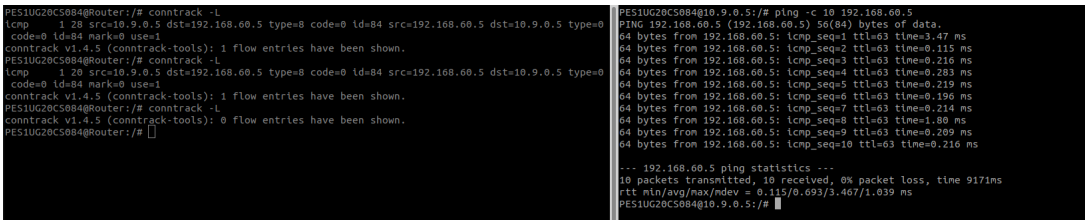
4. Internal hosts cannot access external servers

```
PES1UG20CS084@192.168.60.6:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
PES1UG20CS084@192.168.60.6:/#
```

Task 3: Connection Tracking and Stateful Firewall

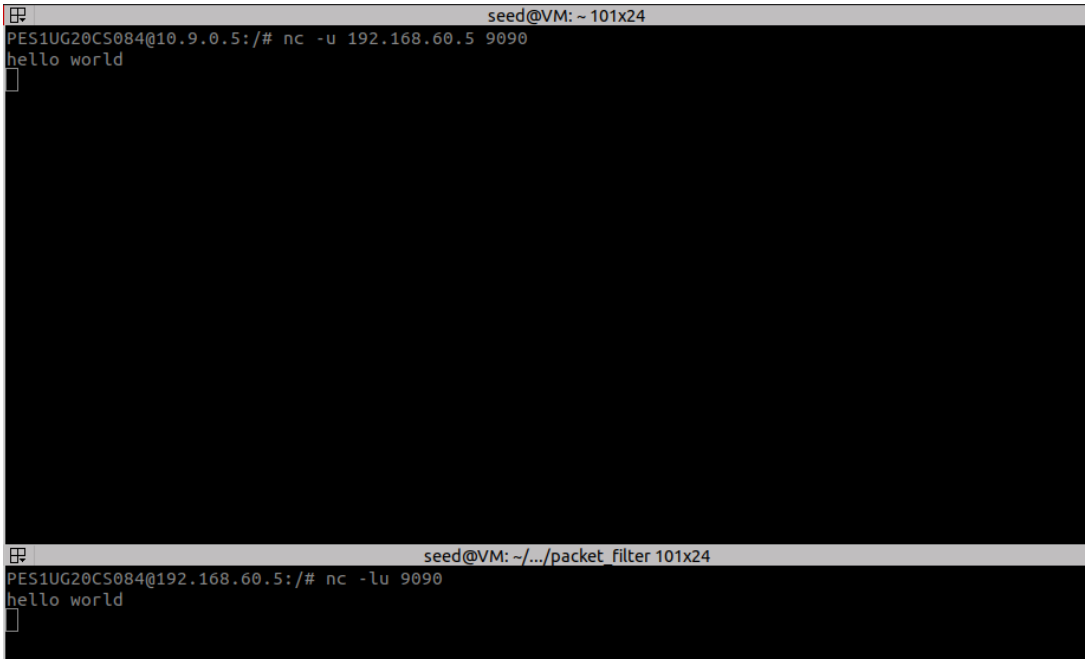
Task 3.A: Experiment with the Connection Tracking

ICMP



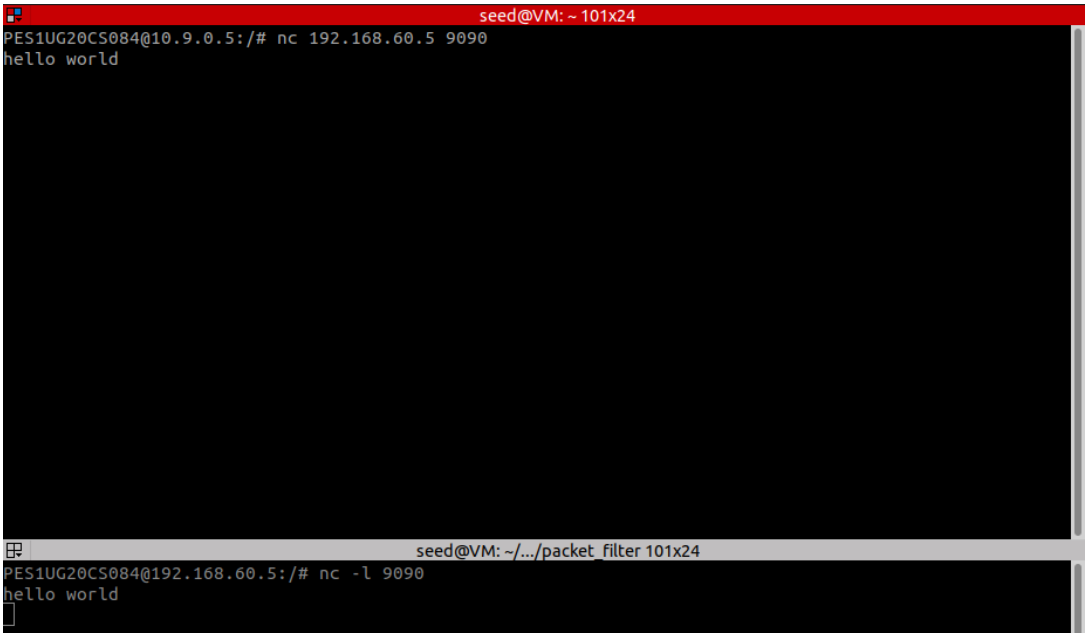
TTL decreases from 28 to 0.

UDP



TTL decreases from 28 until it is expired

TCP



```
PES1UG20CS084@Router:/# conntrack -L
tcp      6 431998 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=41862 dport=9090 src=192.168.60.5
dst=10.9.0.5 sport=9090 dport=41862 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
PES1UG20CS084@Router:/# conntrack -L
tcp      6 431991 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=41862 dport=9090 src=192.168.60.5
dst=10.9.0.5 sport=9090 dport=41862 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
PES1UG20CS084@Router:/# conntrack -L
tcp      6 431932 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=41862 dport=9090 src=192.168.60.5
dst=10.9.0.5 sport=9090 dport=41862 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
PES1UG20CS084@Router:/#
```

TTL for TCP is 5 days, but decreases the same way

Task 3.B: Setting Up a Stateful Firewall

Setting Rules

```
PES1UG20CS084@Router:/# iptables -A FORWARD -p tcp -i eth0 -d 192.168.60.5 --dport 23 --syn -m connt
rack --ctstate NEW -j ACCEPT
PES1UG20CS084@Router:/# iptables -A FORWARD -i eth1 -p tcp --syn -m conntrack --ctstate NEW -j ACCEP
T
PES1UG20CS084@Router:/# iptables -A FORWARD -p tcp -m conntrack --ctstate RELATED,ESTABLISHED -j ACC
EPT
PES1UG20CS084@Router:/# iptables -A FORWARD -p tcp -j DROP
PES1UG20CS084@Router:/# iptables -P FORWARD ACCEPT
PES1UG20CS084@Router:/# 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  --  eth1   *       0.0.0.0/0            0.0.0.0/0            tcp flags:0
x17/0x02 ctstate NEW
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            ctstate REL
ATED,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
```

Checking rules

1. Checking telnet

```
PES1UG20CS084@10.9.0.5:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c37fb9afb47f 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: Sat Oct 29 12:28:50 UTC 2022 from host2-192.168.60.6.net-192.168.60.0 on pts/2
seed@c37fb9afb47f:~$
```

2. Outside hosts cannot access other internal servers.

```
PES1UG20CS084@10.9.0.5:/# telnet 192.168.60.6
Trying 192.168.60.6...
telnet: Unable to connect to remote host: Connection timed out
PES1UG20CS084@10.9.0.5:/# telnet 192.168.60.7
Trying 192.168.60.7...
telnet: Unable to connect to remote host: Connection timed out
PES1UG20CS084@10.9.0.5:/#
```

3. a

```
PES1UG20CS084@192.168.60.6:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c37fb9afb47f 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: Sat Oct 29 13:31:24 UTC 2022 on pts/2
seed@c37fb9afb47f:~$
```

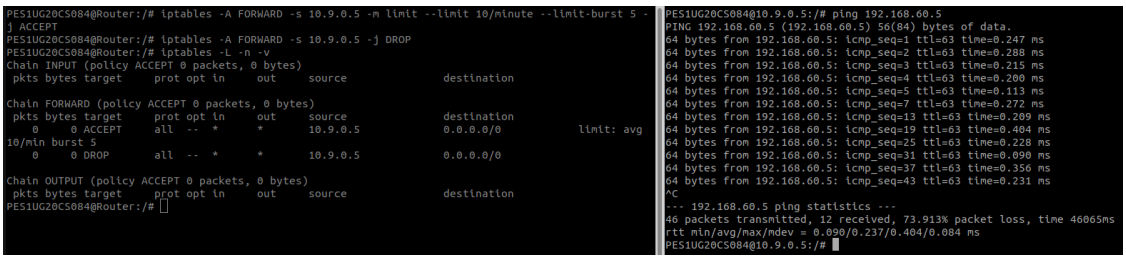
```
PES1UG20CS084@192.168.60.6:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
283d3f27289c login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * 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: Sat Oct 29 12:29:26 UTC 2022 from host2-192.168.60.6.net-192.168.60.0 on pts/1
seed@283d3f27289c:~$
```

4. Internal hosts can access all the internal servers

```
PES1UG20CS084@192.168.60.6:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
2092284a5d2c 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.
```

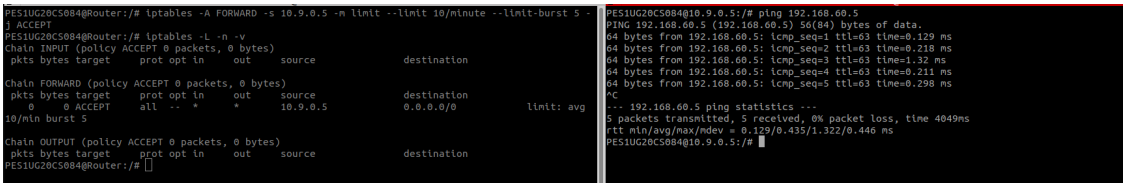
Task 4: Limiting Network Traffic

Setting Rules and pinging host `192.168.60.5`



Some packets not following the rule are dropped, hence we can see the 73.9% packet loss

Using and pinging host `192.168.60.5`



Packets not dropped since there is no rule telling the firewall to drop them even though the ping is a burst request

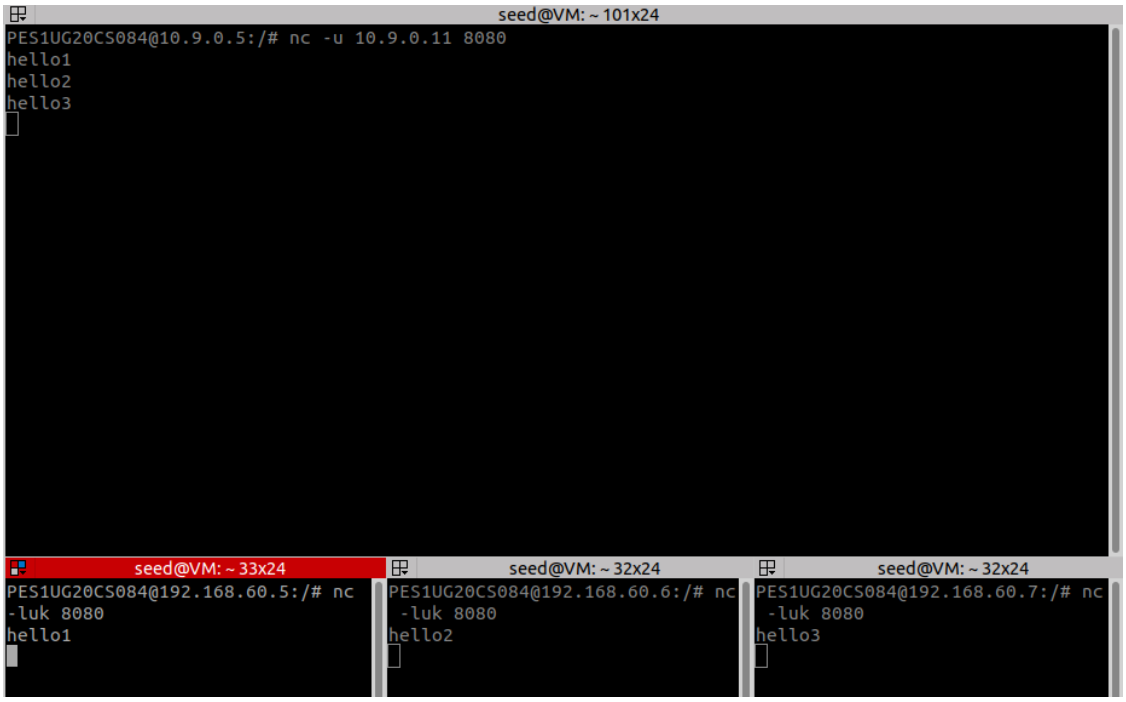
---

Task 5: Load Balancing

Setting up the rules

```
PES1UG20CS084@Router:/# 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
PES1UG20CS084@Router:/# 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
PES1UG20CS084@Router:/# 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
PES1UG20CS084@Router:/# 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
PES1UG20CS084@Router:/#
```

Round Robin



Random Mode

Rules:

```
PES1UG20CS084@Router:/# 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
PES1UG20CS084@Router:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random
 --probability 0.5 -j DNAT --to-destination 192.168.60.6:8080
PES1UG20CS084@Router:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random
 --probability 1 -j DNAT --to-destination 192.168.60.6:8080
PES1UG20CS084@Router:/# 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
PES1UG20CS084@Router:/#
```

```
PES1UG20CS084@10.9.0.5:/# nc -u 10.9.0.11 8080
hello1
hello2
hello3
hello4
hello5
```

seed@VM: ~ 33x24

```
PES1UG20CS084@192.168.60.5:/# nc
-luk 8080
hello1
```

seed@VM: ~ 32x24

```
PES1UG20CS084@192.168.60.6:/# nc
 -luk 8080
hello2
hello3
hello4
hello5
```

seed@VM: ~ 32x24

```
PES1UG20CS084@192.168.60.7:/# nc
 -luk 8080
```

Packets are sent randomly