

# 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

```
5503.313000 Registering filters.
5527.307475 *** LOCAL_OUT
5527.307476 127.0.0.1 --> 127.0.0.1 (UDP)
5527.311003 *** LOCAL_OUT
5527.311004 10.0.2.15 --> 8.8.8.8 (UDP)
5527.311011 *** Dropping 8.8.8.8 (UDP), port 53
5532.318249 *** LOCAL_OUT
5532.318250 10.0.2.15 --> 8.8.8.8 (UDP)
5532.318249 *** Dropping 8.8.8.8 (UDP), port 53
5537.361881 *** LOCAL_OUT
5537.361882 10.0.2.15 --> 8.8.8.8 (UDP)
5537.361895 *** Dropping 8.8.8.8 (UDP), port 53

[10/29/22]seed@VM:~/.../packet_filters$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/lab7/Codes/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
CC [M] /home/seed/Desktop/lab7/Codes/packet_filter/seedFilter.o
Building modules, stage 2.
MODPOST 1 modules
CC [M] /home/seed/Desktop/lab7/Codes/packet_filter/seedFilter.mod.o
LD [M] /home/seed/Desktop/lab7/Codes/packet_filter/seedFilter.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[10/29/22]seed@VM:~/.../packet_filters$ sudo insmod seedFilter.ko
insmod: can't insert file seedFilter.ko: 16384 0
[10/29/22]seed@VM:~/.../packet_filters$ lsmod | grep seedFilter
seedFilter                16384 0
[10/29/22]seed@VM:~/.../packet_filters$ dnf @8.8.8.8 www.example.com
[10/29/22]seed@VM:~/.../packet_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

```
10/29/22]seed@VM:~/.../packet_filters$ sudo dmesg -k -w
5503.313000 Registering filters.
5527.307475 *** LOCAL_OUT
5527.307476 127.0.0.1 --> 127.0.0.1 (UDP)
5527.311003 *** POST_ROUTING
5527.311004 10.0.2.15 --> 172.20.10.1 (UDP)
5527.311011 *** PRE_ROUTING
5527.311012 172.20.10.1 --> 10.0.2.15 (UDP)
5527.311013 *** LOCAL_IN
5527.311014 172.20.10.1 --> 10.0.2.15 (UDP)
5527.311015 *** LOCAL_OUT
5527.311016 127.0.0.1 --> 127.0.0.53 (UDP)
5527.311017 *** POST_ROUTING
5527.311018 127.0.0.1 --> 127.0.0.53 (UDP)
5527.311019 *** PRE_ROUTING
5527.311020 127.0.0.1 --> 127.0.0.53 (UDP)
5527.311021 *** LOCAL_IN
5527.311022 127.0.0.1 --> 127.0.0.53 (UDP)
5527.311023 *** LOCAL_OUT
5527.311024 10.0.2.15 --> 172.20.10.1 (UDP)
5527.311025 *** POST_ROUTING
5527.311026 10.0.2.15 --> 172.20.10.1 (UDP)
5527.311027 *** PRE_ROUTING
5527.311028 172.20.10.1 --> 10.0.2.15 (UDP)
5527.311029 *** LOCAL_IN
5527.311030 172.20.10.1 --> 10.0.2.15 (UDP)
5527.311031 *** LOCAL_OUT
5527.311032 127.0.0.53 --> 127.0.0.1 (UDP)
5527.311033 *** POST_ROUTING
5527.311034 127.0.0.53 --> 127.0.0.1 (UDP)
5527.311035 *** PRE_ROUTING
5527.311036 127.0.0.53 --> 127.0.0.1 (UDP)
5527.311037 *** LOCAL_IN
5527.311038 127.0.0.53 --> 127.0.0.1 (UDP)
5527.311039 *** POST_ROUTING
5527.311040 127.0.0.53 --> 127.0.0.1 (UDP)
5527.311041 *** PRE_ROUTING
5527.311042 127.0.0.53 --> 127.0.0.1 (UDP)
5527.311043 *** LOCAL_OUT
5527.311044 10.0.2.15 --> 8.8.8.8 (UDP)
5527.311045 *** POST_ROUTING
5527.311046 10.0.2.15 --> 8.8.8.8 (UDP)
5527.311047 *** PRE_ROUTING
5527.311048 8.8.8.8 --> 10.0.2.15 (UDP)
5527.311049 *** LOCAL_IN
5527.311050 10.0.2.15 --> 10.0.2.15 (UDP)

[10/29/22]seed@VM:~/.../packet_filters$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/lab7/Codes/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
CC [M] /home/seed/Desktop/lab7/Codes/packet_filter/seedPrint.o
Building modules, stage 2.
MODPOST 1 modules
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[10/29/22]seed@VM:~/.../packet_filters$ sudo insmod seedPrint.ko
insmod: can't insert file seedPrint.ko: 16384 0
[10/29/22]seed@VM:~/.../packet_filters$ 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: 2795
; 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.                21111  IN      A      93.184.216.34

;; Query time: 59 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sat Oct 29 06:37:10 EDT 2022
;; MSG SIZE rcvd: 60

[10/29/22]seed@VM:~/.../packet_filters$ lsmod | grep seedPrint
seedPrint                16384 0
[10/29/22]seed@VM:~/.../packet_filters$
```

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

```
[10/29/22]seed@VM:~/packet_filters$ sudo dmesg -C
[10/29/22]seed@VM:~/packet_filters$ sudo dmesg -k -w
8661.779050 Registering filters.
8661.308731 *** LOCAL OUT
8661.308733 10.0.2.15 --> 192.168.0.1 (UDP)
8661.308734 *** LOCAL OUT
8661.308735 10.0.2.15 --> 192.168.0.1 (UDP)
8661.308745 *** POST_ROUTING
8661.308745 10.0.2.15 --> 192.168.0.1 (UDP)
8661.345189 *** PRE_ROUTING
8661.345192 192.168.0.1 --> 10.0.2.15 (UDP)
8661.345207 *** LOCAL IN
8661.345209 192.168.0.1 --> 10.0.2.15 (UDP)
8661.345210 *** LOCAL OUT

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

## Attempting to Ping and telnet into 10.9.0.1

```
[10/29/22]seed@VM:~$ sudo dmesg -k -w
8867.847017 *** Dropping 10.9.0.1 (ICMP)
8868.857824 *** Dropping 10.9.0.1 (ICMP)
8869.881594 *** Dropping 10.9.0.1 (ICMP)
8870.905132 *** Dropping 10.9.0.1 (ICMP)
8876.729181 *** Dropping 10.9.0.1 (TCP), port 23
8877.754822 *** Dropping 10.9.0.1 (TCP), port 23
8879.788151 *** Dropping 10.9.0.1 (TCP), port 23

PES1UG20CS084@10.9.0.5:/# ^C
PES1UG20CS084@10.9.0.5:/# 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 ---
4 packets transmitted, 0 received, 100% packet loss, time 3060ms

PES1UG20CS084@10.9.0.5:/# telnet 10.9.0.1
Trying 10.9.0.1...
^C
PES1UG20CS084@10.9.0.5:/#
```

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
```

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

```
# 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            icmptype
ACCEPT    icmp -- 0.0.0.0/0              0.0.0.0/0              8

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy DROP)
target    prot opt source                destination            icmptype
ACCEPT    icmp -- 0.0.0.0/0              0.0.0.0/0              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            icmptype
0      0 DROP      icmp -- eth0   *      0.0.0.0/0             0.0.0.0/0              8
0      0 ACCEPT    icmp -- eth1   *      0.0.0.0/0             0.0.0.0/0              8
0      0 ACCEPT    icmp -- eth0   *      0.0.0.0/0             0.0.0.0/0              0

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

<pre> PES1UG20CS084@Router:/# conntrack -L tcp 1 28 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=84 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 id=84 mark=0 use=1 conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown. PES1UG20CS084@Router:/# conntrack -L tcp 1 20 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=84 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 id=84 mark=0 use=1 conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown. PES1UG20CS084@Router:/# conntrack -L tcp 1 20 src=10.9.0.5 dst=192.168.60.5 type=8 code=0 id=84 src=192.168.60.5 dst=10.9.0.5 type=0 code=0 id=84 mark=0 use=1 conntrack v1.4.5 (conntrack-tools): 0 flow entries have been shown. PES1UG20CS084@Router:/# █ </pre>	<pre> PES1UG20CS084@10.9.0.5:/# ping -c 10 192.168.60.5 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=3.47 ms 64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.115 ms 64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.216 ms 64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.283 ms 64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.219 ms 64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.196 ms 64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.214 ms 64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=1.80 ms 64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.209 ms 64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.216 ms  --- 192.168.60.5 ping statistics --- 10 packets transmitted, 10 received, 0% packet loss, time 917ms rtt min/avg/max/ndev = 0.115/0.693/3.467/1.039 ms PES1UG20CS084@10.9.0.5:/# █ </pre>
---	--

TTL decreases from 28 to 0.

#### UDP



```
seed@VM: ~ 101x24
PES1UG20CS084@10.9.0.5:/# nc -u 192.168.60.5 9090
hello world
█

seed@VM: ~/.../packet_filter 101x24
PES1UG20CS084@192.168.60.5:/# nc -lu 9090
hello world
█
```

```
PES1UG20CS084@Router:/# conntrack -L
udp      17 28 src=10.9.0.5 dst=192.168.60.5 sport=47030 dport=9090 [UNREPLIED] src=192.168.60.5 dst=
=10.9.0.5 sport=9090 dport=47030 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
PES1UG20CS084@Router:/# conntrack -L
udp      17 16 src=10.9.0.5 dst=192.168.60.5 sport=47030 dport=9090 [UNREPLIED] src=192.168.60.5 dst=
=10.9.0.5 sport=9090 dport=47030 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
PES1UG20CS084@Router:/# conntrack -L
udp      17 5 src=10.9.0.5 dst=192.168.60.5 sport=47030 dport=9090 [UNREPLIED] src=192.168.60.5 dst=
=10.9.0.5 sport=9090 dport=47030 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
PES1UG20CS084@Router:/# conntrack -L
conntrack v1.4.5 (conntrack-tools): 0 flow entries have been shown.
PES1UG20CS084@Router:/# █
```

TTL decreases from 28 until it is expired

## TCP

```
seed@VM: ~ 101x24
PES1UG20CS084@10.9.0.5:/# nc 192.168.60.5 9090
hello world
█

seed@VM: ~/.../packet_filter 101x24
PES1UG20CS084@192.168.60.5:/# nc -l 9090
hello world
█
```



```
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 conntrack --ctstate NEW -j ACCEPT
PES1UG20CS084@Router:/# iptables -A FORWARD -i eth1 -p tcp --syn -m conntrack --ctstate NEW -j ACCEPT
PES1UG20CS084@Router:/# iptables -A FORWARD -p tcp -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
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

```

PES1UG20CS084@Router:~# iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/minute --limit-burst 5 -j ACCEPT
PES1UG20CS084@Router:~# iptables -A FORWARD -s 10.9.0.5 -j 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 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
PES1UG20CS084@Router:~#
PES1UG20CS084@10.9.0.5:~# 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=0.247 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.288 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.215 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.200 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.113 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.272 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.209 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.404 ms
64 bytes from 192.168.60.5: icmp_seq=25 ttl=63 time=0.228 ms
64 bytes from 192.168.60.5: icmp_seq=31 ttl=63 time=0.090 ms
64 bytes from 192.168.60.5: icmp_seq=37 ttl=63 time=0.356 ms
64 bytes from 192.168.60.5: icmp_seq=43 ttl=63 time=0.231 ms
^C
--- 192.168.60.5 ping statistics ---
46 packets transmitted, 12 received, 73.913% packet loss, time 46065ms
rtt min/avg/max/mdev = 0.090/0.237/0.404/0.084 ms
PES1UG20CS084@10.9.0.5:~#

```

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

```

PES1UG20CS084@Router:~# iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/minute --limit-burst 5 -j 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    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
PES1UG20CS084@Router:~#
PES1UG20CS084@10.9.0.5:~# 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=0.129 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.218 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.132 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.211 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.298 ms
^C
--- 192.168.60.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4049ms
rtt min/avg/max/mdev = 0.129/0.435/1.322/0.446 ms
PES1UG20CS084@10.9.0.5:~#

```

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

```

seed@VM: ~ 101x24
PES1UG20CS084@10.9.0.5:~# nc -u 10.9.0.11 8080
hello1
hello2
hello3
^C

seed@VM: ~ 33x24
PES1UG20CS084@192.168.60.5:~# nc
-luk 8080
hello1
^C

seed@VM: ~ 32x24
PES1UG20CS084@192.168.60.6:~# nc
-luk 8080
hello2
^C

seed@VM: ~ 32x24
PES1UG20CS084@192.168.60.7:~# nc
-luk 8080
hello3
^C

```

### 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