**Task 1.A**

**Terminal:**

```
-rw-rw-r-- 1 seed seed   80 Feb 20 13:26 modules.order
-rw-rw-r-- 1 seed seed    0 Feb 20 13:26 Module.symvers
[02/20/23]seed@VM:~/.../kernel_module$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/LabTa
/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'
[02/20/23]seed@VM:~/.../kernel_module$ sudo insmod hello.ko
[02/20/23]seed@VM:~/.../kernel_module$ lsmod | grep hello
hello                  16384  0
[02/20/23]seed@VM:~/.../kernel_module$ dmesg
[    0.000000] Linux version 5.4.0-54-generic (buildd@lcy01-amd64-024)
0-17ubuntu1~20.04)) #60-Ubuntu SMP Fri Nov 6 10:37:59 UTC 2020 (Ubuntu
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.4.0-54-generic
```

```
[  395.682833] veth335971c: renamed from eth1
[  395.706370] br-6fcc59cd8866: port 4(veth2e3aba3) entered disabled state
[  395.706926] device veth2e3aba3 left promiscuous mode
[  395.706928] br-6fcc59cd8866: port 4(veth2e3aba3) entered disabled state
[ 1086.475750] hello: module verification failed: signature and/or required key m
nel
[ 1086.475838] Hello World!
[02/20/23]seed@VM:~/.../kernel_module$
```

```
[  395.706370] br-6fcc59cd8866: port 4(veth2e3aba3) entered disabled state
[  395.706926] device veth2e3aba3 left promiscuous mode
[  395.706928] br-6fcc59cd8866: port 4(veth2e3aba3) entered disabled state
[ 1086.475750] hello: module verification failed: signature and/or required key mi
nel
[ 1086.475838] Hello World!
[ 1460.534604] Bye-bye World!.
[02/20/23]seed@VM:~/.../kernel_module$
```

**Description:**

We just compile and execute the c code to create simple firewall.

**Task 1.B.1**

**Terminal:**

```
^C[02/20/23]seed@VM:~$ dig @8.8.4.4 pfw.edu

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.4.4 pfw.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61818
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;pfw.edu.                       IN      A

;; ANSWER SECTION:
pfw.edu.                21600   IN      A       104.18.18.143
pfw.edu.                21600   IN      A       104.18.19.143

;; Query time: 55 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Mon Feb 20 18:35:02 EST 2023
;; MSG SIZE  rcvd: 68
```

```
[02/20/23]seed@VM:~$ cd Desktop/LabTasks/Lab5_Firewall/Labsetup/F
[02/20/23]seed@VM:~/.../packet_filter$ ll
total 8
-rw-rw-r-- 1 seed seed  236 Jan 13  2021 Makefile
-rw-rw-r-- 1 seed seed 2746 Jan 13  2021 seedFilter.c
[02/20/23]seed@VM:~/.../packet_filter$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-gene
  CC [M]  /home/seed/Desktop/LabTasks/Lab5_Firewall/Labsetup/File
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/Desktop/LabTasks/Lab5_Firewall/Labsetup/File
  LD [M]  /home/seed/Desktop/LabTasks/Lab5_Firewall/Labsetup/File
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-gener
[02/20/23]seed@VM:~/.../packet_filter$ make ins
sudo dmesg -C
sudo insmod seedFilter.ko
[02/20/23]seed@VM:~/.../packet_filter$ lsmod | grep seed
seedFilter             16384  0
[02/20/23]seed@VM:~/.../packet_filter$ dmesg
[ 3695.936977] Registering filters.
[02/20/23]seed@VM:~/.../packet_filter$ dig @8.8.4.4 pfw.edu
```

**Code:**

```
#include <linux/kernel.h>
#include <linux/module.h>
#include <linux/netfilter.h>
#include <linux/netfilter_ipv4.h>
#include <linux/ip.h>
#include <linux/tcp.h>
#include <linux/udp.h>
#include <linux/if_ether.h>
#include <linux/inet.h>


static struct nf_hook_ops hook1, hook2;


unsigned int blockUDP(void *priv, struct sk_buff *skb,
                      const struct nf_hook_state *state)
{
   struct iphdr *iph;
   struct udphdr *udph;

   u16  port   = 53;
   char ip[16] = "8.8.4.4";
   u32  ip_addr;

   if (!skb) return NF_ACCEPT;

   iph = ip_hdr(skb);
   // Convert the IPv4 address from dotted decimal to 32-bit binary
   in4_pton(ip, -1, (u8 *)&ip_addr, '\0', NULL);

   if (iph->protocol == IPPROTO_UDP) {
       udph = udp_hdr(skb);
       if (iph->daddr == ip_addr && ntohs(udph->dest) == port){
           printk(KERN_WARNING "*** Dropping %pI4 (UDP), port %d\n",
&(iph->daddr), port);
           return NF_DROP;
```

**Description:**

Firewall is working as expected

**Task 1.B.2**
**Code:**

```
#include <linux/kernel.h>
#include <linux/module.h>
#include <linux/netfilter.h>
#include <linux/netfilter_ipv4.h>
#include <linux/ip.h>
#include <linux/tcp.h>
#include <linux/udp.h>
#include <linux/if_ether.h>
#include <linux/inet.h>

static struct nf_hook_ops hook1, hook2, hook3, hook4, hook5, hook6;

unsigned int blockUDP(void *priv, struct sk_buff *skb,
                      const struct nf_hook_state *state)
{
    struct iphdr *iph;
    struct udphdr *udph;

    u16 port = 53;
    char ip[16] = "8.8.4.4";
    u32 ip_addr;

    if (!skb)
        return NF_ACCEPT;

    iph = ip_hdr(skb);
    // Convert the IPv4 address from dotted decimal to 32-bit binary
    in4_pton(ip, -1, (u8 *)&ip_addr, '\0', NULL);

    if (iph->protocol == IPPROTO_UDP)
    {
        udph = udp_hdr(skb);
        if (iph->daddr == ip_addr && ntohs(udph->dest) == port)
        {
            printk(KERN_WARNING "*** Dropping %pI4 (UDP), port %d\n",
&(iph->daddr), port);
```

**Terminal:**

```
[ 3935.398277] *** LOCAL_OUT
[ 3935.398279]     127.0.0.1  --> 127.0.0.1 (UDP)
[ 3935.398390] *** LOCAL_OUT
[ 3935.398391]     10.0.2.4  --> 8.8.8.8 (UDP)
[ 3935.398395] *** Dropping 8.8.8.8 (UDP), port 53
[ 3940.399891] *** LOCAL_OUT
[ 3940.399897]     10.0.2.4  --> 8.8.8.8 (UDP)
[ 3940.399923] *** Dropping 8.8.8.8 (UDP), port 53
```

**Description:**

We successfully check info of all hocks.

**Task 1.B.3**

**Code:**

```c
#include <linux/kernel.h>
#include <linux/module.h>
#include <linux/netfilter.h>
#include <linux/netfilter_ipv4.h>
#include <linux/ip.h>
#include <linux/tcp.h>
#include <linux/udp.h>
#include <linux/icmp.h>
#include <linux/if_ether.h>
#include <linux/inet.h>

static struct nf_hook_ops hook1, hook2, hook3, hook4, hook5, hook6;

unsigned int blockICMP(void *priv, struct sk_buff *skb, const struct
nf_hook_state *state)
{
    struct iphdr *iph;
    struct icmphdr *icmph;

    u16 type = 8;
    char ip[16] = "10.9.0.1";
    u32 ip_addr;

    if (!skb)
        return NF_ACCEPT;

    iph = ip_hdr(skb);
    // Convert the IPv4 address from dotted decimal to 32-bit binary
    in4_pton(ip, -1, (u8 *)&ip_addr, '\0', NULL);

    if (iph->protocol == IPPROTO_ICMP)
    {
        icmph = icmp_hdr(skb);
        if (iph->daddr == ip_addr && icmph->type == type)
        {
            printk(KERN_WARNING "*** Dropping %pI4 (ICMP), type
```

**Terminal:**

```
[ 7180.218669]      127.0.0.53  --> 127.0.0.1 (UDP)
[ 7196.205393] *** Dropping 10.9.0.5 (ICMP), type 8
[ 7197.229874] *** Dropping 10.9.0.5 (ICMP), type 8
[ 7198.252718] *** Dropping 10.9.0.5 (ICMP), type 8
[ 7199.276551] *** Dropping 10.9.0.5 (ICMP), type 8
[ 7200.301351] *** Dropping 10.9.0.5 (ICMP), type 8
[ 7201.325160] *** Dropping 10.9.0.5 (ICMP), type 8
[ 7202.348706] *** Dropping 10.9.0.5 (ICMP), type 8
[ 7203.372814] *** Dropping 10.9.0.5 (ICMP), type 8
[ 7204.396651] *** Dropping 10.9.0.5 (ICMP), type 8
[ 7205.420703] *** Dropping 10.9.0.5 (ICMP), type 8
```

```
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data.
^C
--- 10.9.0.1 ping statistics ---
165 packets transmitted, 0 received, 100% packet loss, time 167935ms

root@96c403782607:/# ping 10.9.0.1
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data.
```

```
[02/20/23]seed@VM:~/.../packet_filter$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Deskto
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-ge
  CC [M]  /home/seed/Desktop/LabTasks/Lab5_Firewall/Labsetup/Fi
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/Desktop/LabTasks/Lab5_Firewall/Labsetup/Fi
  LD [M]  /home/seed/Desktop/LabTasks/Lab5_Firewall/Labsetup/Fi
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-ger
[02/20/23]seed@VM:~/.../packet_filter$ make ins
sudo dmesg -C
sudo insmod seedFilter.ko
[02/20/23]seed@VM:~/.../packet_filter$ sudo dmesg
[ 7159.322278] Registering filters.
[02/20/23]seed@VM:~/.../packet_filter$ sudo dmesg
[ 7159.322278] Registering filters.
```

**Description:**

I Implemented two more hooks to achieve preventing other computers to ping and telnet into the VM.

**Task 2.A**

**Terminal:**

```
root@53dbb5c5914f:/# iptables -t filter -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

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

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

```
root@53dbb5c5914f:/# iptables -A INPUT  -p icmp --icmp-type echo-request -j ACCEPT
root@53dbb5c5914f:/# iptables -A OUTPUT -p icmp --icmp-type echo-reply   -j ACCEPT
root@53dbb5c5914f:/# iptables -P INPUT  DROP
root@53dbb5c5914f:/# iptables -P OUTPUT DROP
```

```
root@53dbb5c5914f:/# iptables -t filter -L -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0            icmptype 8

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

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

```
root@60ad9dbae4b3:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data.
64 bytes from 10.9.0.11: icmp_seq=1 ttl=64 time=0.060 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.132 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.129 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.128 ms
64 bytes from 10.9.0.11: icmp_seq=5 ttl=64 time=0.122 ms
^C
--- 10.9.0.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4075ms
rtt min/avg/max/mdev = 0.060/0.114/0.132/0.027 ms
root@60ad9dbae4b3:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
64 bytes from 192.168.60.11: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 192.168.60.11: icmp_seq=2 ttl=64 time=0.127 ms
64 bytes from 192.168.60.11: icmp_seq=3 ttl=64 time=0.043 ms
64 bytes from 192.168.60.11: icmp_seq=4 ttl=64 time=0.045 ms
64 bytes from 192.168.60.11: icmp_seq=5 ttl=64 time=0.068 ms
^C
--- 192.168.60.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4079ms
rtt min/avg/max/mdev = 0.043/0.067/0.127/0.031 ms
```

```
root@60ad9dbae4b3:/# telnet 10.9.0.11
Trying 10.9.0.11...
```

**Description:**

I was able to prevent anything to go through except ping like we can see telnet didnot go through.

**Task 2.B**

**Terminal:**

```
root@53dbb5c5914f:/#
root@53dbb5c5914f:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DROP
root@53dbb5c5914f:/# iptables -A FORWARD -i eth1 -p icmp --icmp-type echo-request -j ACCEPT
root@53dbb5c5914f:/# iptables -A FORWARD -p icmp --icmp-type echo-reply -j ACCEPT
root@53dbb5c5914f:/# iptables -P FORWARD DROP
root@53dbb5c5914f:/# iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

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

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

```
root@60ad9dbae4b3:/# 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=0.090 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.162 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.160 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.075 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.052 ms
^C
--- 10.9.0.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4075ms
rtt min/avg/max/mdev = 0.052/0.107/0.162/0.045 ms
```

```
[02/21/23]seed@VM:~/.../Labsetup$ docksh 96
root@96c403782607:/# 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 ---
5 packets transmitted, 0 received, 100% packet loss, time 4078ms
```

```
root@96c403782607:/# telnet 192.168.60.5
Trying 192.168.60.5...
^C
root@96c403782607:/#
```

Description:
I was able to implement a firewall to protect the internal network 192.168.60.0/24. More specifically, to enforce the restrictions on the ICMP traffic using all the four rules stated in the documentation.

**Task 2.C**
**Terminal:**

```
root@53dbb5c5914f:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -
p tcp --dport 23 -j ACCEPT
root@53dbb5c5914f:/# iptables -A FORWARD -i eth1 -s 192.168.60.5 -
p tcp --sport 23 -j ACCEPT
root@53dbb5c5914f:/# iptables -P FORWARD DROP
root@53dbb5c5914f:/# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

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

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@53dbb5c5914f:/#
```

**Outside hosts:**

```
root@96c403782607:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
60ad9dbae4b3 login: ^CConnection closed by foreign host.
root@96c403782607:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
root@96c403782607:/#
```

**Internal hosts:**

```
root@60ad9dbae4b3:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
root@60ad9dbae4b3:/#
```

```
root@8f33e887bda6:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
root@8f33e887bda6:/#
```

```
root@dfb005a05b8d:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
root@dfb005a05b8d:/#
```

**Descriptions:**

I was able to protect the TCP servers inside the internal network (192.168.60.0/24). This includes the
router, outside host and the internal servers.

1. All the internal hosts run a telnet server (listening to port23). Outside hosts can only access the telnet
server on192.168.60.5, not the other internal hosts.
2. Outside hosts cannot access other internal servers.
3. Internal hosts can access all the internal servers.
4. Internal hosts cannot access external servers.

**Task 3.A**

**Terminal:**

```
root@53dbb5c5914f:/# conntrack -L
conntrack v1.4.5 (conntrack-tools): 0 flow entries have been shown
.
root@53dbb5c5914f:/#
```

```
root@96c403782607:/# 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=0.115 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.164 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.167 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.160 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.057 ms
^C
--- 192.168.60.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4083ms
rtt min/avg/max/mdev = 0.057/0.132/0.167/0.042 ms
```

```
root@96c403782607:/# nc -u 192.168.60.5 9090
vksvsss
```

```
root@60ad9dbae4b3:/# nc -lu 9090
vksvsss
```

```
root@60ad9dbae4b3:/# nc -l 9090
gddg
```

```
root@96c403782607:/# nc 192.168.60.5 9090
gddg
```

**Description:**
I checked the connection tracking information on the router container. Then, I tried ICMP, UDP and TCP experiment.

**Task 3.B**
**Terminal:**

```
root@53dbb5c5914f:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -
p tcp --dport 23 --syn -j ACCEPT
root@53dbb5c5914f:/# iptables -A FORWARD -i eth1 -p tcp --syn -j A
CCEPT
root@53dbb5c5914f:/# iptables -A FORWARD -p tcp -m conntrack --cts
tate RELATED,ESTABLISHED -j ACCEPT
root@53dbb5c5914f:/# iptables -A FORWARD -p tcp -j DROP
```

```
root@53dbb5c5914f:/# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            192.168.60.5         tcp
dpt:23 flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp
flags:0x17/0x02
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            ctst
ate RELATED,ESTABLISHED
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

**External Host:**

```
root@96c403782607:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
root@96c403782607:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
60ad9dbae4b3 login:
```

**Internal Host:**

```
root@60ad9dbae4b3:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
96c403782607 login: ^CConnection closed by foreign host.
root@60ad9dbae4b3:/#
```

```
root@8f33e887bda6:/# telnet 10.9.0.11
Trying 10.9.0.11...
Connected to 10.9.0.11.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
53dbb5c5914f login: ^CConnection closed by foreign host.
root@8f33e887bda6:/#
```

```
root@dfb005a05b8d:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
96c403782607 login: ^CConnection closed by foreign host.
root@dfb005a05b8d:/#
```

**Description:**

I set up firewall rules based on connections. The rule allows TCP packets belonging to an existing connection to pass through as you can see above.

**Task 4**

**Terminal:**

I used it to load balance three UDP servers running in the internal network. Starting the server on each of the hosts:192.168.60.6, and 192.168.60.7.

```
[02/21/23]seed@VM:~/.../Labsetup$
[02/21/23]seed@VM:~/.../Labsetup$ iptables -m limit -h
iptables v1.8.4

Usage: iptables -[ACD] chain rule-specification [options]
       iptables -I chain [rulenum] rule-specification [options]
       iptables -R chain rulenum rule-specification [options]
```

```
[02/21/23]seed@VM:~/.../Labsetup$ docksh 53d
root@53dbb5c5914f:/# iptables -A FORWARD -s 192.168.60.5 -m limit
--limit 20/minute --limit-burst 4 -j ACCEPT
root@53dbb5c5914f:/# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  192.168.60.5         0.0.0.0/0            limi
t: avg 20/min burst 4

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

```
root@53dbb5c5914f:/# iptables -A FORWARD -s 192.168.60.5 -j DROP
root@53dbb5c5914f:/# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  192.168.60.5         0.0.0.0/0            limi
t: avg 20/min burst 4
DROP       all  --  192.168.60.5         0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

```
root@60ad9dbae4b3:/# 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=0.071 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.056 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.057 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.064 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.090 ms
64 bytes from 10.9.0.5: icmp_seq=7 ttl=63 time=0.304 ms
64 bytes from 10.9.0.5: icmp_seq=10 ttl=63 time=0.117 ms
64 bytes from 10.9.0.5: icmp_seq=13 ttl=63 time=0.156 ms
64 bytes from 10.9.0.5: icmp_seq=16 ttl=63 time=0.060 ms
^C
--- 10.9.0.5 ping statistics ---
17 packets transmitted, 9 received, 47.0588% packet loss, time 16374ms
rtt min/avg/max/mdev = 0.056/0.108/0.304/0.076 ms
```

**Description:**

I used this module to limit how many packets from10.9.0.5 are allowed to get into the internal

network to accept each packet message every three (3) minutes, then 1 packet results drop after 3 sec each.

**Task 5**
**Terminal:**

```
root@8f33e887bda6:/# nc -luk 8080
```

**Using the nth mode (round-robin)**

```
[02/22/23]seed@VM:~/.../Labsetup$ docksh 53d
root@53dbb5c5914f:/# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

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

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


Chain DOCKER_OUTPUT (1 references)
target     prot opt source               destination
DNAT       tcp  --  0.0.0.0/0            127.0.0.11           tcp
dpt:53 to:127.0.0.11:39915
DNAT       udp  --  0.0.0.0/0            127.0.0.11           udp
dpt:53 to:127.0.0.11:53559

Chain DOCKER_POSTROUTING (1 references)
target     prot opt source               destination
SNAT       tcp  --  127.0.0.11           0.0.0.0/0            tcp
spt:39915 to::53
SNAT       udp  --  127.0.0.11           0.0.0.0/0            udp
spt:53559 to::53
```

**This for UDP server 192.168.60.6**

```
root@53dbb5c5914f:/# iptables -t nat -A PREROUTING -p udp --dport
8080 -m statistic --mode nth --every 2 --packet 0 -j DNAT --to-des
tination 192.168.60.6:8080
root@53dbb5c5914f:/# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp
dpt:8080 statistic mode nth every 2 to:192.168.60.6:8080

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

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

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


Chain DOCKER_OUTPUT (1 references)
target     prot opt source               destination
DNAT       tcp  --  0.0.0.0/0            127.0.0.11           tcp
dpt:53 to:127.0.0.11:39915
DNAT       udp  --  0.0.0.0/0            127.0.0.11           udp
dpt:53 to:127.0.0.11:53559
```

```
Chain DOCKER_POSTROUTING (1 references)
target     prot opt source               destination
SNAT       tcp  --  127.0.0.11           0.0.0.0/0            tcp
spt:39915 to::53
SNAT       udp  --  127.0.0.11           0.0.0.0/0            udp
spt:53559 to::53
root@53dbb5c5914f:/#
```

**This for UDP server 192.168.60.7**

```
root@53dbb5c5914f:/# iptables -t nat -A PREROUTING -p udp --dport
8080  -j DNAT --to-destination 192.168.60.7:8080
root@53dbb5c5914f:/# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp
dpt:8080 statistic mode nth every 2 to:192.168.60.6:8080
DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp
dpt:8080 to:192.168.60.7:8080

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

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

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

```
Chain DOCKER_OUTPUT (1 references)
target     prot opt source               destination
DNAT       tcp  --  0.0.0.0/0            127.0.0.11           tcp
dpt:53 to:127.0.0.11:39915
DNAT       udp  --  0.0.0.0/0            127.0.0.11           udp
dpt:53 to:127.0.0.11:53559

Chain DOCKER_POSTROUTING (1 references)
target     prot opt source               destination
SNAT       tcp  --  127.0.0.11           0.0.0.0/0            tcp
spt:39915 to::53
SNAT       udp  --  127.0.0.11           0.0.0.0/0            udp
spt:53559 to::53
root@53dbb5c5914f:/#
```

**Echoing packages to external servers**

```
root@96c403782607:/# echo 1 | nc -u 10.9.0.11 8080
^C
root@96c403782607:/#
```

```
root@8f33e887bda6:/# nc -luk 8080
1
```

```
root@96c403782607:/# echo 2 | nc -u 10.9.0.11 8080
^C
root@96c403782607:/#
```

```
root@dfb005a05b8d:/# nc -luk 8080
2
```

**192.168.60.6 takes the odd numbers, while 192.168.60.7 takes the even numbers.**

```
root@96c403782607:/# echo 1 | nc -u 10.9.0.11 8080
^C
root@96c403782607:/# echo 2 | nc -u 10.9.0.11 8080
^C
root@96c403782607:/# echo 3 | nc -u 10.9.0.11 8080

^C
root@96c403782607:/# echo 4 | nc -u 10.9.0.11 8080
^C
root@96c403782607:/# echo 5 | nc -u 10.9.0.11 8080
^C
root@96c403782607:/# echo 6 | nc -u 10.9.0.11 8080
```

```
root@8f33e887bda6:/# nc -luk 8080
1
1
3
5
```

```
root@dfb005a05b8d:/# nc -luk 8080
2
4
6
```

**Using random mode**

```
root@53dbb5c5914f:/# iptables -t nat -A PREROUTING -p udp --dport
8080 -m statistic --mode random --probability 0.5 -j DNAT --to-des
tination 192.168.60.6:8080
root@53dbb5c5914f:/# iptables -t nat -A PREROUTING -p udp --dport
8080  -j DNAT --to-destination 192.168.60.7:8080
root@53dbb5c5914f:/#
```

```
root@96c403782607:/# echo 1 | nc -u 10.9.0.11 8080
^C
root@96c403782607:/# echo 2 | nc -u 10.9.0.11 8080
^C
root@96c403782607:/# echo 3 | nc -u 10.9.0.11 8080
^C
root@96c403782607:/# echo 4 | nc -u 10.9.0.11 8080
^C
root@96c403782607:/# echo 5 | nc -u 10.9.0.11 8080
^C
root@96c403782607:/# echo 6 | nc -u 10.9.0.11 8080
^C
root@96c403782607:/# echo 7 | nc -u 10.9.0.11 8080
^C
root@96c403782607:/# echo 8 | nc -u 10.9.0.11 8080
```

```
root@8f33e887bda6:/# nc -luk 8080
2
3
4
8
```

```
root@dfb005a05b8d:/# nc -luk 8080
1
5
6
7
```