# FIREWALL EXPLORATION LAB

SEED 2.0

# Contents

## Environment Setup

Building docker containers.

```
[11/17/23]seed@VM:~/.../Labsetup$ dcbuild
HostA uses an image, skipping
Host1 uses an image, skipping
Host2 uses an image, skipping
Host3 uses an image, skipping
Building Router
Step 1/2 : FROM handsonsecurity/seed-ubuntu:large
 ---> cecb04fbf1dd
Step 2/2 : RUN apt-get update     && apt-get install -y kmod
& apt-get clean
 ---> Running in b96bd895d231
Get:1 http://archive.ubuntu.com/ubuntu focal InRelease [265 kB]
Get:2 http://security.ubuntu.com/ubuntu focal-security InReleas
14 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease
 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security/restrict
md64 Packages [3017 kB]
```

Setting up dockers.

```
[11/17/23]seed@VM:~/.../Labsetup$ dcup
Creating network "net-10.9.0.0" with the default driver
Creating network "net-192.168.60.0" with the default driver
Creating host3-192.168.60.7 ... done
Creating seed-router        ... done
Creating hostA-10.9.0.5     ... done
Creating host1-192.168.60.5 ... done
Creating host2-192.168.60.6 ... done
Attaching to hostA-10.9.0.5, host3-192.168.60.7, host1-192.168.60.5
, host2-192.168.60.6, seed-router
host3-192.168.60.7 |  * Starting internet superserver inetd       [
 OK ]
hostA-10.9.0.5 |  * Starting internet superserver inetd           [
 OK ]
seed-router |  * Starting internet superserver inetd              [
 OK ]
host2-192.168.60.6 |  * Starting internet superserver inetd       [
 OK ]
host1-192.168.60.5 |  * Starting internet superserver inetd       [
 OK ]
```

Setting the docker for Host A.

```
[11/17/23]seed@VM:~/.../Labsetup$ dockps
8767380c8913  host2-192.168.60.6
5b0f054f8e66  host1-192.168.60.5
b8deea797b11  seed-router
316b4f1f38b7  host3-192.168.60.7
a448fb46a5ce  hostA-10.9.0.5
[11/17/23]seed@VM:~/.../Labsetup$ docksh a44
root@a448fb46a5ce:/#
```

Setting up docker for Seed Router and following is the IP address of Seed Router.

```
[11/17/23]seed@VM:~$ docksh b8d
root@b8deea797b11:/# ipaddr
bash: ipaddr: command not found
root@b8deea797b11:/# ifconfi
bash: ifconfi: command not found
root@b8deea797b11:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.11  netmask 255.255.255.0  broadcast 10.9.0.255
```

Setting up Host1 docker.

```
[11/17/23]seed@VM:~$ dockps
8767380c8913  host2-192.168.60.6
5b0f054f8e66  host1-192.168.60.5
b8deea797b11  seed-router
316b4f1f38b7  host3-192.168.60.7
a448fb46a5ce  hostA-10.9.0.5
[11/17/23]seed@VM:~$ docksh 5b0
root@5b0f054f8e66:/#
```

Setting up Host2 docker.

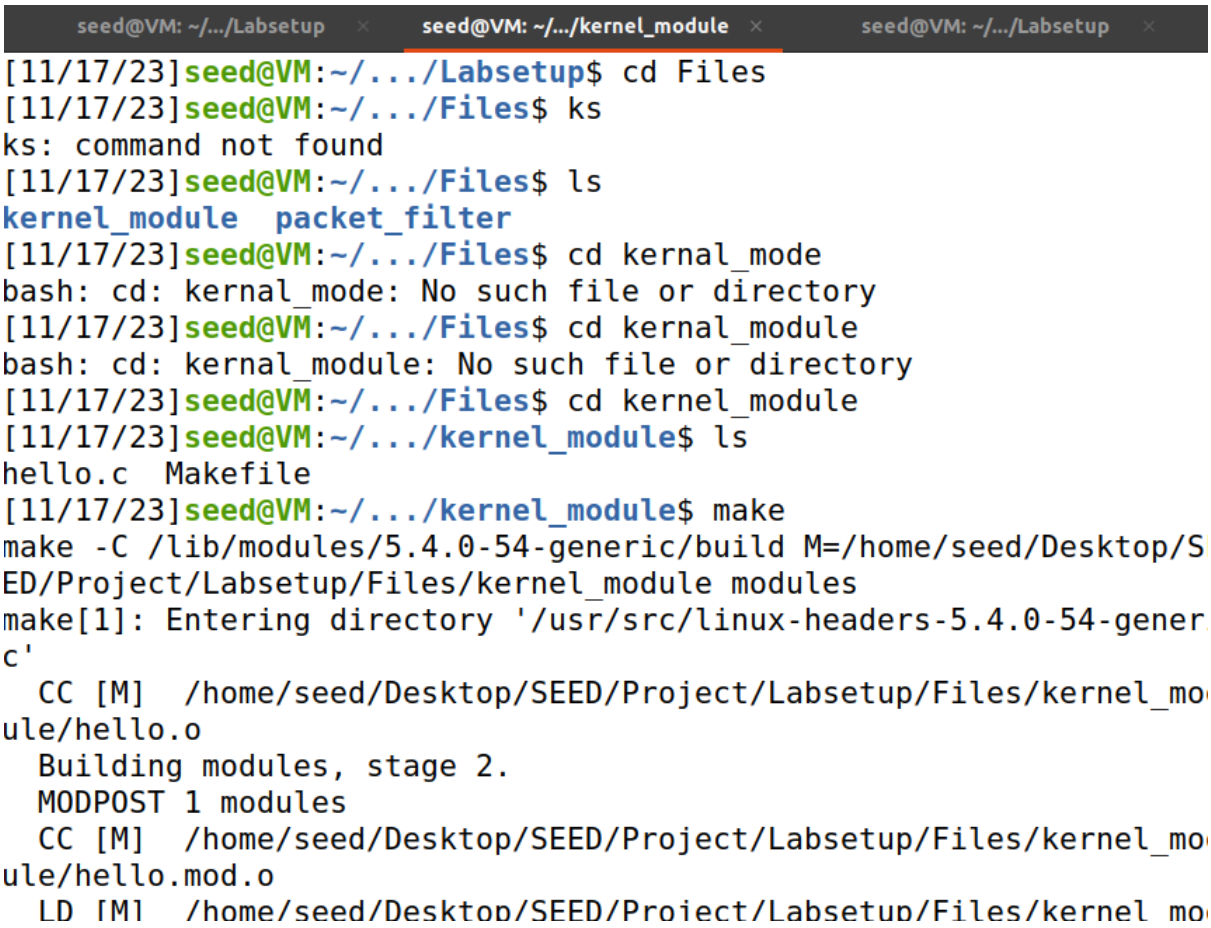
```
[11/17/23]seed@VM:~/.../Labsetup$ dockps
8767380c8913  host2-192.168.60.6
5b0f054f8e66  host1-192.168.60.5
b8deea797b11  seed-router
316b4f1f38b7  host3-192.168.60.7
a448fb46a5ce  hostA-10.9.0.5
[11/17/23]seed@VM:~/.../Labsetup$ docksh 8767
root@8767380c8913:/#
```

Setting up Host3 docker.

```
[11/17/23]seed@VM:~/.../Labsetup$ docksh 85
root@85498c1f767c:/#
```

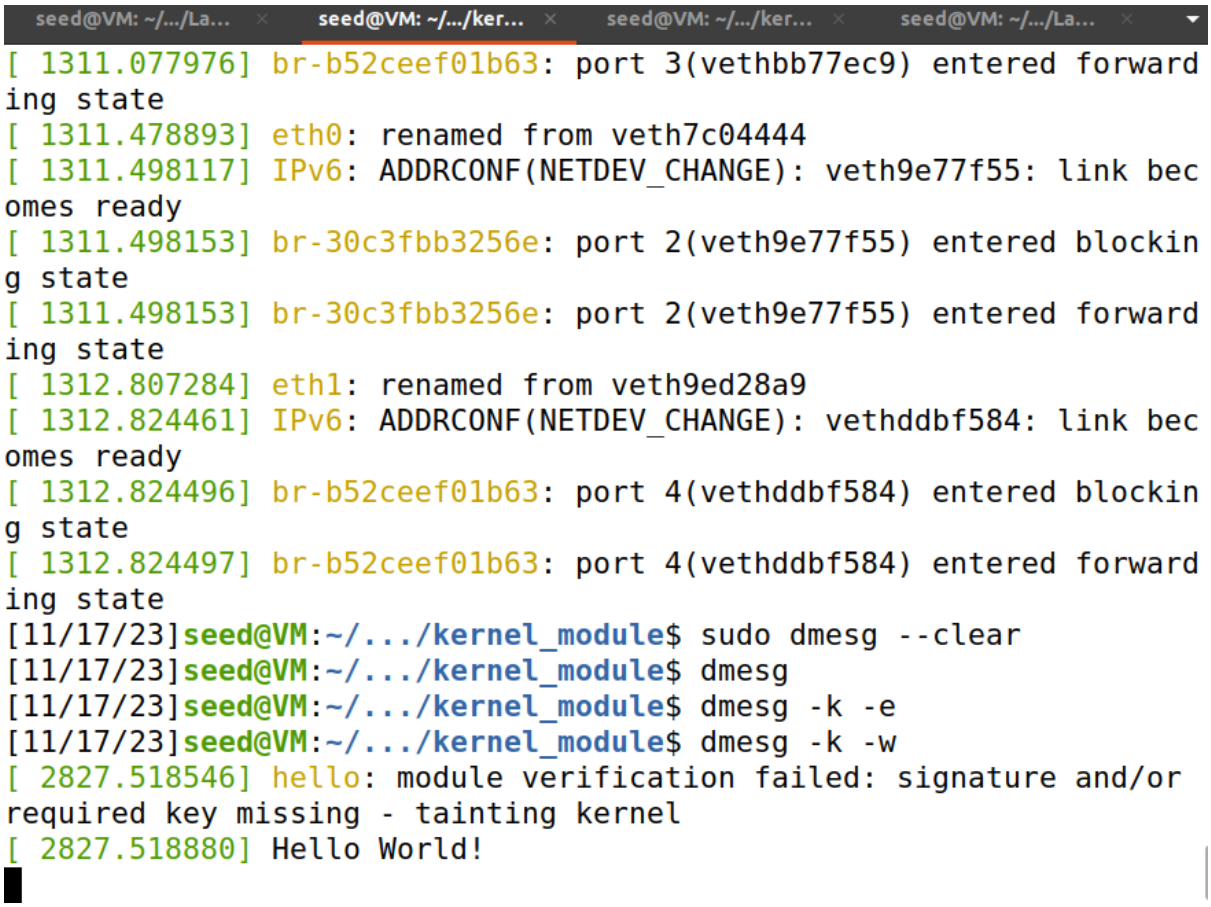
## Task 1

Compiling the program.

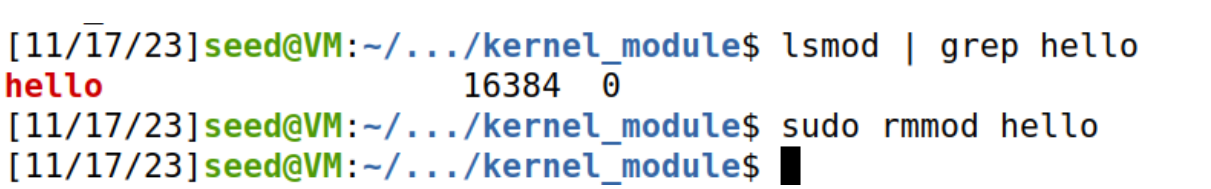


## Task 1.A

I checked the messages with dmesg and then proceeded to checking messages for kernal modules on wait where when I ran ‘sudo insmod hello.ko’ so I received this message from the given kernal module.




Then I performed the next command which lists the module and after that I removed the hello module.



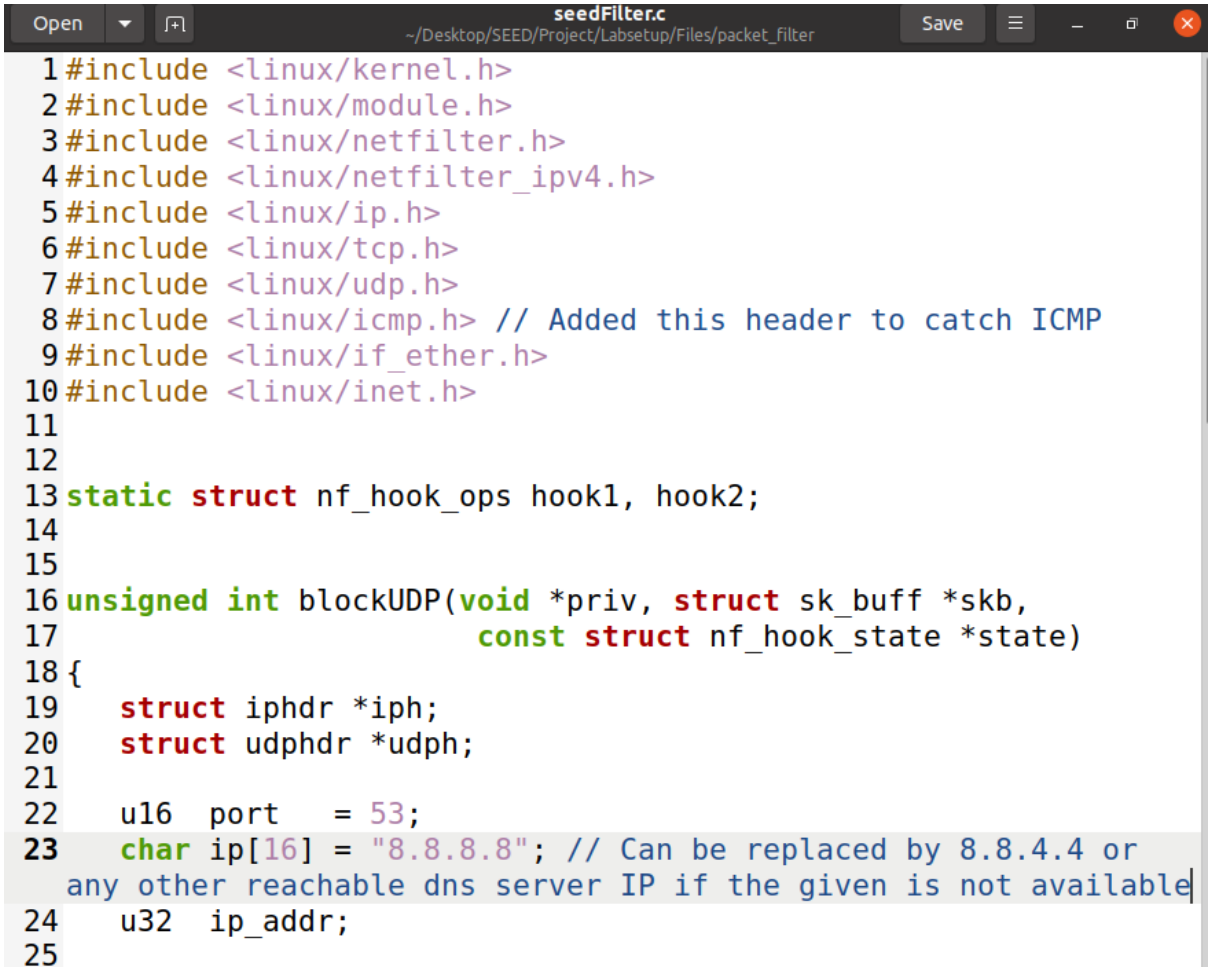
As a result, I can see the Bye World message where I have put the terminal to wait for kernal module messages.


Now just for a good measure I used the command as visible below which shows information of the hello.ko kernal module.

```
[11/17/23]seed@VM:~/.../kernel_module$ modinfo hello.ko
filename:       /home/seed/Desktop/SEED/Project/Labsetup/Files/kern
el_module/hello.ko
license:        GPL
srcversion:     717A72281ACFAA8385B33A8
depends:
retpoline:      Y
name:           hello
vermagic:       5.4.0-54-generic SMP mod_unload
[11/17/23]seed@VM:~/.../kernel_module$
```

## Task 1.B

I made the changes in the given code for this task which are visible along the comments.




```
1 #include <linux/kernel.h>
2 #include <linux/module.h>
3 #include <linux/netfilter.h>
4 #include <linux/netfilter_ipv4.h>
5 #include <linux/ip.h>
6 #include <linux/tcp.h>
7 #include <linux/udp.h>
8 #include <linux/icmp.h> // Added this header to catch ICMP
9 #include <linux/if_ether.h>
10 #include <linux/inet.h>
11
12
13 static struct nf_hook_ops hook1, hook2;
14
15
16 unsigned int blockUDP(void *priv, struct sk_buff *skb,
17                       const struct nf_hook_state *state)
18 {
19    struct iphdr *iph;
20    struct udphdr *udph;
21
22    u16  port   = 53;
23    char ip[16] = "8.8.8.8"; // Can be replaced by 8.8.4.4 or
   any other reachable dns server IP if the given is not available
24    u32  ip_addr;
25
```

## Subtask 1

In my case the dns server at 8.8.8.8 is available and the link provided. Moreover I can dig to this so it is alright.

```
[11/17/23]seed@VM:~/.../packet_filter$ ping www.example.com
PING www.example.com (93.184.216.34) 56(84) bytes of data.
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=1 ttl=42 time
=249 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=2 ttl=42 time
=258 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=3 ttl=42 time
=256 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=4 ttl=42 time
=252 ms
^C
--- www.example.com ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4005ms
rtt min/avg/max/mdev = 248.646/253.913/258.206/3.679 ms
[11/17/23]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: 26206
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONA
L: 1

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

;; ANSWER SECTION:
www.example.com.        7563    IN      A       93.184.216.34

;; Query time: 151 msec
```

After I make the files I ran this kernal module and ensured if the module is there now in working.

```
[11/17/23]seed@VM:~/.../packet_filter$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/SE
ED/Project/Labsetup/Files/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generi
c'
  CC [M]  /home/seed/Desktop/SEED/Project/Labsetup/Files/packet_fil
ter/seedFilter.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/Desktop/SEED/Project/Labsetup/Files/packet_fil
ter/seedFilter.mod.o
  LD [M]  /home/seed/Desktop/SEED/Project/Labsetup/Files/packet_fil
ter/seedFilter.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic
'
[11/17/23]seed@VM:~/.../packet_filter$ sudo insmod seedFilter.ko
[11/17/23]seed@VM:~/.../packet_filter$  lsmod | grep seed
seedFilter             16384  0
[11/17/23]seed@VM:~/.../packet_filter$
```

Here I can see the new kernel module message caught proving it to be in progress along with the packets it is capturing now.

```
[11/17/23]seed@VM:~/.../kernel_module$ dmesg -k -w
[ 2827.518546] hello: module verification failed: signature and/or
required key missing - tainting kernel
[ 2827.518880] Hello World!
[ 3187.959226] Bye-bye World!.
[ 3744.934488] Hello World!
[ 3765.694932] Bye-bye World!.
[ 4437.191251] Registering filters.
[ 4437.987443] *** LOCAL_OUT
[ 4437.987447]     10.0.2.15  --> 192.168.1.1 (UDP)
[ 4518.027793] *** LOCAL_OUT
[ 4518.027794]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 4518.027925] *** LOCAL_OUT
[ 4518.027926]     10.0.2.15  --> 192.168.1.1 (UDP)
[ 4518.089473] *** LOCAL_OUT
[ 4518.089476]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 4518.137866] *** LOCAL_OUT
[ 4518.137867]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 4518.138012] *** LOCAL_OUT
[ 4518.138012]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 4551.391180] *** LOCAL_OUT
[ 4551.391182]     10.0.2.15  --> 192.168.1.1 (UDP)
[ 4551.435752] *** LOCAL_OUT
[ 4551.435754]     10.0.2.15  --> 185.125.190.48 (TCP)
```

When I digged again the module started dropping these packets which means it is being blocked.

```
[ 5186.196950]      10.0.2.15  --> 8.8.8.8 (UDP)
[ 5186.196953] *** Dropping 8.8.8.8 (UDP), port 53
[ 5191.366856] *** LOCAL_OUT
[ 5191.366858]      10.0.2.15  --> 8.8.8.8 (UDP)
[ 5191.366867] *** Dropping 8.8.8.8 (UDP), port 53
[ 5196.371382] *** LOCAL_OUT
[ 5196.371384]      10.0.2.15  --> 8.8.8.8 (UDP)
[ 5196.371396] *** Dropping 8.8.8.8 (UDP), port 53
```

And now I can see that the digging got timed out.

```
[11/17/23]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
;; connection timed out; no servers could be reached

[11/17/23]seed@VM:~/.../packet_filter$
```

Removing the module.

```
[11/17/23]seed@VM:~/.../packet_filter$ sudo rmmod seedFilter.ko
[11/17/23]seed@VM:~/.../packet_filter$
```

## Subtask 2

Now cleaning the compiled program and copying the provided code to a new file to make modifications for this task.

```
[11/17/23]seed@VM:~/.../packet_filter$ make clean
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/SE
ED/Project/Labsetup/Files/packet_filter clean
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generi
c'
  CLEAN   /home/seed/Desktop/SEED/Project/Labsetup/Files/packet_fil
ter/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic
'
[11/17/23]seed@VM:~/.../packet_filter$ cp seedFilter.c seedPrint.c
[11/17/23]seed@VM:~/.../packet_filter$
```

Then I added more hooks.

```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> // Added this header to catch ICMP
#include <linux/if_ether.h>
#include <linux/inet.h>


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


unsigned int blockUDP(void *priv, struct sk_buff *skb,
                      const struct nf_hook_state *state)
{
```

Then I added the filters to be registered according to the hooks and instructions provided.

seedPrint.c

```c
int registerFilter(void) {
   printk(KERN_INFO "Registering filters.\n");

   hook1.hook = printInfo;
   hook1.hooknum = NF_INET_PRE_ROUTING;
   hook1.pf = PF_INET;
   hook1.priority = NF_IP_PRI_FIRST;
   nf_register_net_hook(&init_net, &hook1);

   hook2.hook = printInfo;
   hook2.hooknum = NF_INET_LOCAL_IN;
   hook2.pf = PF_INET;
   hook2.priority = NF_IP_PRI_FIRST;
   nf_register_net_hook(&init_net, &hook2);

   hook3.hook = printInfo;
   hook3.hooknum = NF_INET_FORWARD;
   hook3.pf = PF_INET;
   hook3.priority = NF_IP_PRI_FIRST;
   nf_register_net_hook(&init_net, &hook3);

   hook4.hook = printInfo;
   hook4.hooknum = NF_INET_LOCAL_OUT;
   hook4.pf = PF_INET;
   hook4.priority = NF_IP_PRI_FIRST;
   nf_register_net_hook(&init_net, &hook4);

   hook5.hook = printInfo;
   hook5.hooknum = NF_INET_POST_ROUTING;
   hook5.pf = PF_INET;
   hook5.priority = NF_IP_PRI_FIRST;
   nf_register_net_hook(&init_net, &hook5);
```

As well the unregistering for the filters accordingly.

```
111 void removeFilter(void) {
112     printk(KERN_INFO "The filters are being removed.\n");
113     nf_unregister_net_hook(&init_net, &hook1);
114     nf_unregister_net_hook(&init_net, &hook2);
115     nf_unregister_net_hook(&init_net, &hook3);
116     nf_unregister_net_hook(&init_net, &hook4);
117     nf_unregister_net_hook(&init_net, &hook5);
118 }
119
120 module_init(registerFilter);
121 module_exit(removeFilter);
122
123 MODULE_LICENSE("GPL");
124
```

Made the following changes in the MakeFile as seen on the first two lines.

```
1 #obj-m += seedFilter.o
2 obj-m += seedPrint.o
3 all:
4         make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules
5
6 clean:
7         make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean
8
9 ins:
10        sudo dmesg -C
11        sudo insmod seedFilter.ko
12
13 rm:
14        sudo rmmod seedFilter
15
```

Now I compiled this code.

```
[11/17/23]seed@VM:~/.../packet_filter$ make clean
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/SE
ED/Project/Labsetup/Files/packet_filter clean
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generi
c'
  CLEAN   /home/seed/Desktop/SEED/Project/Labsetup/Files/packet_fil
ter/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic
'
[11/17/23]seed@VM:~/.../packet_filter$ cp seedFilter.c seedPrint.c
[11/17/23]seed@VM:~/.../packet_filter$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/SE
ED/Project/Labsetup/Files/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generi
c'
  CC [M]  /home/seed/Desktop/SEED/Project/Labsetup/Files/packet_fil
ter/seedPrint.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/Desktop/SEED/Project/Labsetup/Files/packet_fil
ter/seedPrint.mod.o
  LD [M]  /home/seed/Desktop/SEED/Project/Labsetup/Files/packet_fil
ter/seedPrint.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic
'
[11/17/23]seed@VM:~/.../packet_filter$
```

I initiated the kernal module.

```
[11/17/23]seed@VM:~/.../packet_filter$ sudo insmod seedPrint.ko
[11/17/23]seed@VM:~/.../packet_filter$
```

As visible the hooks are working.

```
[ 6937.777562] The filters are being removed.
[ 7440.083923] Registering filters.
[ 7518.041077] *** LOCAL_OUT
[ 7518.041079]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 7518.041086] *** POST_ROUTING
[ 7518.041087]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 7518.041093] *** PRE_ROUTING
[ 7518.041094]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 7518.041095] *** LOCAL_IN
[ 7518.041096]     127.0.0.1  --> 127.0.0.53 (UDP)
[ 7518.041239] *** LOCAL_OUT
[ 7518.041241]     10.0.2.15  --> 192.168.1.1 (UDP)
[ 7518.041245] *** POST_ROUTING
[ 7518.041246]     10.0.2.15  --> 192.168.1.1 (UDP)
[ 7518.095071] *** PRE_ROUTING
[ 7518.095073]     192.168.1.1  --> 10.0.2.15 (UDP)
[ 7518.095083] *** LOCAL_IN
[ 7518.095084]     192.168.1.1  --> 10.0.2.15 (UDP)
[ 7518.095297] *** LOCAL_OUT
[ 7518.095299]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 7518.095301] *** POST_ROUTING
[ 7518.095302]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 7518.095307] *** PRE_ROUTING
[ 7518.095308]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 7518.095308] *** LOCAL_IN
[ 7518.095309]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 7518.147433] *** LOCAL_OUT
```

Now to see if it is also going to get information when we target our target.

```
[11/17/23]seed@VM:~/.../packet_filter$ sudo insmod seedPrint.ko
[11/17/23]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: 63416
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONA
L: 1

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

;; ANSWER SECTION:
www.example.com.        4274    IN      A       93.184.216.34

;; Query time: 92 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Nov 17 08:31:20 EST 2023
;; MSG SIZE  rcvd: 60

[11/17/23]seed@VM:~/.../packet_filter$
```

LOCAL_OUT is the spot from where we dig the target then POST_ROUTING is when the packet is going from our machine to dns server then PRE_ROUTING is when the packet comes back from the server to the machine and then we get a LOCAL_IN. There is no FORWARD as it is on the loader but basically it is useful for forwarding the packets to another destination.

```
[ 7518.147629] *** PRE_ROUTING
[ 7518.147630]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 7518.147631] *** LOCAL_IN
[ 7518.147631]     127.0.0.53  --> 127.0.0.1 (UDP)
[ 7551.401202] *** LOCAL_OUT
[ 7551.401203]     10.0.2.15  --> 192.168.1.1 (UDP)
[ 7551.401212] *** POST_ROUTING
[ 7551.401213]     10.0.2.15  --> 192.168.1.1 (UDP)
[ 7551.442745] *** PRE_ROUTING
[ 7551.442764]     192.168.1.1  --> 10.0.2.15 (UDP)
[ 7551.442777] *** LOCAL_IN
[ 7551.442780]     192.168.1.1  --> 10.0.2.15 (UDP)
[ 7551.443575] *** LOCAL_OUT
[ 7551.443576]     10.0.2.15  --> 185.125.190.48 (TCP)
[ 7551.443588] *** POST_ROUTING
[ 7551.443589]     10.0.2.15  --> 185.125.190.48 (TCP)
[ 7551.692568] *** PRE_ROUTING
[ 7551.692599]     185.125.190.48  --> 10.0.2.15 (TCP)
[ 7551.692617] *** LOCAL_IN
[ 7551.692622]     185.125.190.48  --> 10.0.2.15 (TCP)
[ 7551.692648] *** LOCAL_OUT
[ 7551.692654]     10.0.2.15  --> 185.125.190.48 (TCP)
[ 7551.692661] *** POST_ROUTING
[ 7551.692666]     10.0.2.15  --> 185.125.190.48 (TCP)
[ 7551.693159] *** LOCAL_OUT
[ 7551.693160]     10.0.2.15  --> 185.125.190.48 (TCP)
[ 7551.693163] *** POST_ROUTING
[ 7551.693164]     10.0.2.15  --> 185.125.190.48 (TCP)
[ 7551.693613] *** PRE_ROUTING
[ 7551.693615]     185.125.190.48  --> 10.0.2.15 (TCP)
[ 7551.693618] *** LOCAL_IN
[ 7551.693619]     185.125.190.48  --> 10.0.2.15 (TCP)
[ 7551.965844] *** PRE_ROUTING
```

```
[ 7551.965886] *** LOCAL_OUT
[ 7551.965889]     10.0.2.15  --> 185.125.190.48 (TCP)
[ 7551.965894] *** POST_ROUTING
[ 7551.965898]     10.0.2.15  --> 185.125.190.48 (TCP)
[ 7551.965920] *** PRE_ROUTING
[ 7551.965924]     185.125.190.48  --> 10.0.2.15 (TCP)
[ 7551.965928] *** LOCAL_IN
[ 7551.965932]     185.125.190.48  --> 10.0.2.15 (TCP)
[ 7551.966219] *** LOCAL_OUT
[ 7551.966220]     10.0.2.15  --> 185.125.190.48 (TCP)
[ 7551.966223] *** POST_ROUTING
[ 7551.966223]     10.0.2.15  --> 185.125.190.48 (TCP)
[ 7551.966335] *** PRE_ROUTING
[ 7551.966336]     185.125.190.48  --> 10.0.2.15 (TCP)
[ 7551.966338] *** LOCAL_IN
[ 7551.966339]     185.125.190.48  --> 10.0.2.15 (TCP)
[ 7586.509137] *** LOCAL_OUT
[ 7586.509139]     127.0.0.1  --> 127.0.0.1 (UDP)
[ 7586.509147] *** POST_ROUTING
[ 7586.509147]     127.0.0.1  --> 127.0.0.1 (UDP)
[ 7586.509155] *** PRE_ROUTING
[ 7586.509155]     127.0.0.1  --> 127.0.0.1 (UDP)
[ 7586.509156] *** LOCAL_IN
[ 7586.509157]     127.0.0.1  --> 127.0.0.1 (UDP)
[ 7586.509364] *** LOCAL_OUT
[ 7586.509365]     10.0.2.15  --> 8.8.8.8 (UDP)
[ 7586.509368] *** POST_ROUTING
[ 7586.509369]     10.0.2.15  --> 8.8.8.8 (UDP)
[ 7586.595873] *** PRE_ROUTING
[ 7586.595891]     8.8.8.8  --> 10.0.2.15 (UDP)
[ 7586.595906] *** LOCAL_IN
[ 7586.595911]     8.8.8.8  --> 10.0.2.15 (UDP)
```

I removed the module now.

```
[11/17/23]seed@VM:~/.../packet_filter$ sudo rmmod seedPrint.ko
[11/17/23]seed@VM:~/.../packet_filter$
```

And the filters are cleared by the above step.

```
[ 7737.947328]     10.0.2.15  --> 192.168.1.1 (UDP)
[ 7738.007024] *** PRE_ROUTING
[ 7738.007044]     192.168.1.1  --> 10.0.2.15 (UDP)
[ 7738.007056] *** LOCAL_IN
[ 7738.007060]     192.168.1.1  --> 10.0.2.15 (UDP)
[ 7740.251456] The filters are being removed.
```

## Subtask 3

I pinged from HOST A to the SEED VM.

```
[11/17/23]seed@VM:~/.../Labsetup$ docksh a44
root@a448fb46a5ce:/# ping 10.9.0.1
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data.
64 bytes from 10.9.0.1: icmp_seq=1 ttl=64 time=0.070 ms
64 bytes from 10.9.0.1: icmp_seq=2 ttl=64 time=0.053 ms
64 bytes from 10.9.0.1: icmp_seq=3 ttl=64 time=0.051 ms
64 bytes from 10.9.0.1: icmp_seq=4 ttl=64 time=0.050 ms
^C
--- 10.9.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.050/0.056/0.070/0.008 ms
```

I tried to telnet into SEED VM from HOST A which I was successful at after which I closed the connection.

```
[11/17/23]seed@VM:~/.../Labsetup$ docksh a44
root@a448fb46a5ce:/# ping 10.9.0.1
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data.
64 bytes from 10.9.0.1: icmp_seq=1 ttl=64 time=0.070 ms
64 bytes from 10.9.0.1: icmp_seq=2 ttl=64 time=0.053 ms
64 bytes from 10.9.0.1: icmp_seq=3 ttl=64 time=0.051 ms
64 bytes from 10.9.0.1: icmp_seq=4 ttl=64 time=0.050 ms
^C
--- 10.9.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.050/0.056/0.070/0.008 ms
root@a448fb46a5ce:/# telnet 10.9.0.1
Trying 10.9.0.1...
Connected to 10.9.0.1.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: dees
Password: Connection closed by foreign host.
root@a448fb46a5ce:/# telnet 10.9.0.1
Trying 10.9.0.1...
Connected to 10.9.0.1.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM 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

0 updates can be installed immediately.
```

I copied the file to a new file to use it for this subtask.

```
[11/17/23]seed@VM:~/.../packet_filter$ make clean
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/SEED/Project/Labsetup/Files/packet_filter clean
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CLEAN   /home/seed/Desktop/SEED/Project/Labsetup/Files/packet_filter/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[11/17/23]seed@VM:~/.../packet_filter$ cp seedFilter.c seedBlock.c
[11/17/23]seed@VM:~/.../packet_filter$ gedit seedBlock.c
[11/17/23]seed@VM:~/.../packet_filter$
```

I added the hooks and added these details for hooks.

```
 1 #include <linux/kernel.h>
 2 #include <linux/module.h>
 3 #include <linux/netfilter.h>
 4 #include <linux/netfilter_ipv4.h>
 5 #include <linux/ip.h>
 6 #include <linux/tcp.h>
 7 #include <linux/udp.h>
 8 #include <linux/icmp.h> // Added this header to catch ICMP
 9 #include <linux/if_ether.h>
10 #include <linux/inet.h>
11
12
13 static struct nf_hook_ops hook1, hook2, hook3, hook4;
14
```

```
128 int registerFilter(void) {
129    printk(KERN_INFO "Registering filters.\n");
130
131    hook1.hook = printInfo;
132    hook1.hooknum = NF_INET_LOCAL_OUT;
133    hook1.pf = PF_INET;
134    hook1.priority = NF_IP_PRI_FIRST;
135    nf_register_net_hook(&init_net, &hook1);
136
137    hook2.hook = blockUDP;
138    hook2.hooknum = NF_INET_POST_ROUTING;
139    hook2.pf = PF_INET;
140    hook2.priority = NF_IP_PRI_FIRST;
141    nf_register_net_hook(&init_net, &hook2);
142
143    hook3.hook = blockICMP;
144    hook3.hooknum = NF_INET_PRE_ROUTING;
145    hook3.pf = PF_INET;
146    hook3.priority = NF_IP_PRI_FIRST;
147    nf_register_net_hook(&init_net, &hook3);
148
149    hook4.hook = blockTCP;
150    hook4.hooknum = NF_INET_PRE_ROUTING;
151    hook4.pf = PF_INET;
152    hook4.priority = NF_IP_PRI_FIRST;
153    nf_register_net_hook(&init_net, &hook4);
154
155    return 0;
156 }
157
```

```
158 void removeFilter(void) {
159     printk(KERN_INFO "The filters are being removed.\n");
160     nf_unregister_net_hook(&init_net, &hook1);
161     nf_unregister_net_hook(&init_net, &hook2);
162     nf_unregister_net_hook(&init_net, &hook3);
163     nf_unregister_net_hook(&init_net, &hook4);
164 }
165
```

And I added the following functions.

```
41 // blocking ping to vm 10.9.0.1
42 unsigned int blockICMP(void *priv, struct sk_buff *skb,
43                        const struct nf_hook_state *state)
44 {
45     struct iphdr *iph;
46     struct icmphdr *icmph;
47
48     //u16  port   = 53;
49     char ip[16] = "10.9.0.1";
50     u32  ip_addr;
51
52     if (!skb) return NF_ACCEPT;
53
54     iph = ip_hdr(skb);
55     // Convert the IPv4 address from dotted decimal to 32-bit binary
56     in4_pton(ip, -1, (u8 *)&ip_addr, '\0', NULL);
57
58     if (iph->protocol == IPPROTO_ICMP) {
59         icmph = icmp_hdr(skb);
60         if (iph->daddr == ip_addr && icmph->type == ICMP_ECHO){
61             printk(KERN_WARNING "*** Dropping %pI4 (ICMP)\n", &(iph->daddr));
62             return NF_DROP;
63          }
64     }
65     return NF_ACCEPT;
66 }
67
68 // blocking telnet to 10.9.0.1 23
69 unsigned int blockTCP(void *priv, struct sk_buff *skb,
70                       const struct nf_hook_state *state)
71 {
72     struct iphdr *iph;
73     struct tcphdr *tcph;
74
75     u16  port   = 23;
76     char ip[16] = "10.9.0.1";
77     u32  ip_addr;
78
79     if (!skb) return NF_ACCEPT;
80
81     iph = ip_hdr(skb);
82     // Convert the IPv4 address from dotted decimal to 32-bit binary
83     in4_pton(ip, -1, (u8 *)&ip_addr, '\0', NULL);
84
85     if (iph->protocol == IPPROTO_TCP) {
86         tcph = tcp_hdr(skb);
87         if (iph->daddr == ip_addr && ntohs(tcph->dest) == port){
88             printk(KERN_WARNING "*** Dropping %pI4 (TCP), port %d\n", &(iph->daddr), port);
89             return NF_DROP;
90          }
91     }
92     return NF_ACCEPT;
93 }
94
```

I changed the MakeFile.

```
#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
```

Now I compiled the program.

```
[11/17/23]seed@VM:~/.../packet_filter$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Desktop/SE
ED/Project/Labsetup/Files/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generi
c'
  CC [M]  /home/seed/Desktop/SEED/Project/Labsetup/Files/packet_fil
ter/seedBlock.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/Desktop/SEED/Project/Labsetup/Files/packet_fil
ter/seedBlock.mod.o
  LD [M]  /home/seed/Desktop/SEED/Project/Labsetup/Files/packet_fil
ter/seedBlock.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic
'
[11/17/23]seed@VM:~/.../packet_filter$
```

Now initiating kernel module.

```
[11/17/23]seed@VM:~/.../packet_filter$ sudo insmod seedBlock.ko
[11/17/23]seed@VM:~/.../packet_filter$
```

Module has started.

```
[ 7740.251456] The filters are being removed.
[14416.896351] Registering filters.
[14418.063536] *** LOCAL_OUT
[14418.063537]     127.0.0.1  --> 127.0.0.53 (UDP)
[14418.063644] *** LOCAL_OUT
[14418.063645]     10.0.2.15  --> 192.168.1.1 (UDP)
[14418.133037] *** LOCAL_OUT
[14418.133039]     127.0.0.53  --> 127.0.0.1 (UDP)
[14418.170268] *** LOCAL_OUT
[14418.170270]     127.0.0.1  --> 127.0.0.53 (UDP)
[14418.170423] *** LOCAL_OUT
[14418.170424]     127.0.0.53  --> 127.0.0.1 (UDP)
```

When I pinged from HOST A to SEED VM the packets were dropped.

```
[14451.721341] *** LOCAL_OUT
[14451.721359]     10.0.2.15  --> 185.125.190.48 (TCP)
[14451.721623] *** LOCAL_OUT
[14451.721624]     10.0.2.15  --> 185.125.190.48 (TCP)
[14451.981849] *** LOCAL_OUT
[14451.981870]     10.0.2.15  --> 185.125.190.48 (TCP)
[14451.982103] *** LOCAL_OUT
[14451.982104]     10.0.2.15  --> 185.125.190.48 (TCP)
[14454.216508] *** Dropping 10.9.0.1 (ICMP)
[14455.235645] *** Dropping 10.9.0.1 (ICMP)
[14456.259722] *** Dropping 10.9.0.1 (ICMP)
[14457.283381] *** Dropping 10.9.0.1 (ICMP)
[14458.307597] *** Dropping 10.9.0.1 (ICMP)
[14459.331308] *** Dropping 10.9.0.1 (ICMP)
[14460.355406] *** Dropping 10.9.0.1 (ICMP)
[14461.380146] *** Dropping 10.9.0.1 (ICMP)
[14462.403282] *** Dropping 10.9.0.1 (ICMP)
[14463.428184] *** Dropping 10.9.0.1 (ICMP)
[14464.452226] *** Dropping 10.9.0.1 (ICMP)
[14465.477591] *** Dropping 10.9.0.1 (ICMP)
[14466.502953] *** Dropping 10.9.0.1 (ICMP)
[14467.523319] *** Dropping 10.9.0.1 (ICMP)
[14468.547970] *** Dropping 10.9.0.1 (ICMP)
[14469.571524] *** Dropping 10.9.0.1 (ICMP)
[14470.595315] *** Dropping 10.9.0.1 (ICMP)
[14471.619661] *** Dropping 10.9.0.1 (ICMP)
[14472.643610] *** Dropping 10.9.0.1 (ICMP)
[14473.675007] *** Dropping 10.9.0.1 (ICMP)
[14474.691433] *** Dropping 10.9.0.1 (ICMP)
```

Then I tried to establish telnet connection from HOST A to SEED VM.

```
root@a448fb46a5ce:/# 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 ---
37 packets transmitted, 0 received, 100% packet loss, time 36923ms

root@a448fb46a5ce:/# telnet 10.9.0.1
Trying 10.9.0.1...
```

Which evidently got dropped and tells that I have succeeded in this task. After this I removed the module and the filters got removed like the end of the last subtask.

```
[14470.595315] *** Dropping 10.9.0.1 (ICMP)
[14471.619661] *** Dropping 10.9.0.1 (ICMP)
[14472.643610] *** Dropping 10.9.0.1 (ICMP)
[14473.675007] *** Dropping 10.9.0.1 (ICMP)
[14474.691433] *** Dropping 10.9.0.1 (ICMP)
[14475.719582] *** Dropping 10.9.0.1 (ICMP)
[14476.739378] *** Dropping 10.9.0.1 (ICMP)
[14477.763660] *** Dropping 10.9.0.1 (ICMP)
[14478.807939] *** Dropping 10.9.0.1 (ICMP)
[14479.821991] *** Dropping 10.9.0.1 (ICMP)
[14480.878496] *** Dropping 10.9.0.1 (ICMP)
[14481.892566] *** Dropping 10.9.0.1 (ICMP)
[14482.915931] *** Dropping 10.9.0.1 (ICMP)
[14483.942518] *** Dropping 10.9.0.1 (ICMP)
[14484.964176] *** Dropping 10.9.0.1 (ICMP)
[14485.987405] *** Dropping 10.9.0.1 (ICMP)
[14487.014530] *** Dropping 10.9.0.1 (ICMP)
[14488.036026] *** Dropping 10.9.0.1 (ICMP)
[14489.098465] *** Dropping 10.9.0.1 (ICMP)
[14490.116125] *** Dropping 10.9.0.1 (ICMP)
[14491.139978] *** Dropping 10.9.0.1 (ICMP)
[14496.026140] *** Dropping 10.9.0.1 (TCP), port 23
[14497.043571] *** Dropping 10.9.0.1 (TCP), port 23
[14499.075814] *** Dropping 10.9.0.1 (TCP), port 23
[14503.181754] *** Dropping 10.9.0.1 (TCP), port 23
[14511.395759] *** Dropping 10.9.0.1 (TCP), port 23
```

And I stopped the dmesg -k -w as it is no longer needed.

## Task 2

These are the docker rules currently where it tells 127.0.0.0/8 is not the address of the docker. To check with line number just add –line numbers on the end of the command shown in the screenshot below.

```
[11/17/23]seed@VM:~/.../packet_filter$ sudo iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DOCKER     all  --  0.0.0.0/0            0.0.0.0/0            ADDRTYPE match dst-type LOCAL

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DOCKER     all  --  0.0.0.0/0           !127.0.0.0/8          ADDRTYPE match dst-type LOCAL

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  192.168.60.0/24      0.0.0.0/0
MASQUERADE  all  --  10.9.0.0/24          0.0.0.0/0
MASQUERADE  all  --  172.17.0.0/16        0.0.0.0/0

Chain DOCKER (2 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
[11/17/23]seed@VM:~/.../packet_filter$
```

Host A has this for IPTables which is empty.

```
root@a448fb46a5ce:/# iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@a448fb46a5ce:/#
```

In Host A the nat tables are as follows.

```
root@a448fb46a5ce:/# 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:127.0.0.11:37145
DNAT       udp  --  0.0.0.0/0            127.0.0.11           udp dpt:53 to:127.0.0.11:32914

Chain DOCKER_POSTROUTING (1 references)
target     prot opt source               destination
SNAT       tcp  --  127.0.0.11           0.0.0.0/0            tcp spt:37145 to::53
SNAT       udp  --  127.0.0.11           0.0.0.0/0            udp spt:32914 to::53
root@a448fb46a5ce:/#
```

For confirmation I checked if the Seed Router is working so I tried pinging and establishing telnet connection which I closed after successfully checking.

```
root@a448fb46a5ce:/# 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=0.076 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.056 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.051 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.068 ms
^C
--- 10.9.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.051/0.062/0.076/0.009 ms
root@a448fb46a5ce:/# telnet 10.9.0.11
Trying 10.9.0.11...
Connected to 10.9.0.11.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
b8deea797b11 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 th
t 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.
```

## Task 2.A

Now I set the IPTables for the Seed Router.

```
root@b8deea797b11:/# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
root@b8deea797b11:/# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@b8deea797b11:/# iptables -P OUTPUT DROP
root@b8deea797b11:/# iptables -P INPUT DROP
root@b8deea797b11:/# 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
root@b8deea797b11:/#
```

Now when testing pinging it was successful, but telnet connection wasn't established.

```
root@a448fb46a5ce:/# 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=0.101 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.051 ms
^C
--- 10.9.0.11 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1012ms
rtt min/avg/max/mdev = 0.051/0.076/0.101/0.025 ms
root@a448fb46a5ce:/# telnet 10.9.0.11
Trying 10.9.0.11...
telnet: Unable to connect to remote host: Connection timed out
root@a448fb46a5ce:/#
```

I cleared the IPTables for the next task.

```
root@b8deea797b11:/# iptables -F
root@b8deea797b11:/# iptables -P OUTPUT ACCEPT
root@b8deea797b11:/# iptables -P INPUT ACCEPT
root@b8deea797b11:/# iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@b8deea797b11:/#
```

## Task 2.B

After setting the rule in Seed Router IPTables look like this.

```
root@b8deea797b11:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DROP
root@b8deea797b11:/# iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

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

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@b8deea797b11:/#
```

I can ping the Seed Router from HostA but I can't ping the inner Host1.

```
root@a448fb46a5ce:/# 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=0.055 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.047 ms
^C
--- 10.9.0.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2035ms
rtt min/avg/max/mdev = 0.047/0.052/0.055/0.003 ms
root@a448fb46a5ce:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
```

I can ping to outer HostA from inner Host1.

```
root@5b0f054f8e66:/# 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=0.113 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.168 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.074 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.059 ms
```

I made further modifications by setting more rules.

```
root@b8deea797b11:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-reply -j ACCEPT
root@b8deea797b11:/# iptables -A FORWARD -i eth1 -p icmp --icmp-type echo-request -j ACCEPT
root@b8deea797b11:/# iptables -P FORWARD DROP
root@b8deea797b11:/# 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 0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0            icmptype 8

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@b8deea797b11:/#
```

Now I can ping to the Seed Router but can't ping or telnet Host1.

```
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=0.148 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.056 ms
^C
--- 10.9.0.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2050ms
rtt min/avg/max/mdev = 0.047/0.083/0.148/0.045 ms
root@a448fb46a5ce:/# 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 ---
6 packets transmitted, 0 received, 100% packet loss, time 5129ms

root@a448fb46a5ce:/# telnet 192.168.60.5
Trying 192.168.60.5...
```

I can ping from Host1 to HostA but I can't establish telnet connection from Host1 to HostA.

```
root@5b0f054f8e66:/# 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=0.172 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.073 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.062 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.077 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.061 ms
64 bytes from 10.9.0.5: icmp_seq=6 ttl=63 time=0.081 ms
64 bytes from 10.9.0.5: icmp_seq=7 ttl=63 time=0.061 ms
64 bytes from 10.9.0.5: icmp_seq=8 ttl=63 time=0.071 ms
^C
--- 10.9.0.5 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7176ms
rtt min/avg/max/mdev = 0.061/0.082/0.172/0.034 ms
root@5b0f054f8e66:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

As the task has been successfully done now, I cleared the IPTables of the Seed Router.

```
root@b8deea797b11:/# iptables -F
root@b8deea797b11:/# iptables -P OUTPUT ACCEPT
root@b8deea797b11:/# iptables -P INPUT ACCEPT
root@b8deea797b11:/# iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@b8deea797b11:/#
```

## Task 2.C

External HostA can't telnet Internal Host2 nor Host3

```
root@a448fb46a5ce:/# telnet 192.168.60.6
Trying 192.168.60.6...
```

Internal Host1 can't ping External HostA.

```
root@5b0f054f8e66:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
```

Nor can Internal Host1 telnet External HostA.

```
root@5b0f054f8e66:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

Internal Host1 can telnet and ping Internal Host2 which means this task has achieved all its goals.

```
root@5b0f054f8e66:/# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
8767380c8913 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 tha
t 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 b
y
applicable law.
```

```
root@5b0f054f8e66:/# ping 192.168.60.6
PING 192.168.60.6 (192.168.60.6) 56(84) bytes of data.
64 bytes from 192.168.60.6: icmp_seq=1 ttl=64 time=0.165 ms
64 bytes from 192.168.60.6: icmp_seq=2 ttl=64 time=0.048 ms
64 bytes from 192.168.60.6: icmp_seq=3 ttl=64 time=0.086 ms
64 bytes from 192.168.60.6: icmp_seq=4 ttl=64 time=0.085 ms
```

# Task 3

## Task 3.A

### ICMP Experiment

Pinging from Seed Router to Host1 and I found out that the connection remains for 5 to 6 seconds icmp connection can be kept after the job is killed.

```
root@8282f3f499fc:/# ping 192.168.60.5 &> /dev/null &
[1] 30
root@8282f3f499fc:/# kill %1
root@8282f3f499fc:/# conntrack -L
icmp     1 11 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=30 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=30 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
[1]+  Terminated              ping 192.168.60.5 &> /dev/null
root@8282f3f499fc:/# conntrack -L
icmp     1 8 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=30 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=30 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
icmp     1 6 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=30 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=30 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
icmp     1 3 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=30 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=30 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
icmp     1 0 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=30 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=30 mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
conntrack v1.4.5 (conntrack-tools): 0 flow entries have been shown.
root@8282f3f499fc:/#
```

### UDP Experiment

Put Host1 to starting a netcat UDP server.

```
[11/17/23]seed@VM:~/.../Labsetup$ docksh ef0
root@ef09d6ef87bd:/# nc -lu 9090
```

Then sending UDP packets from HostA.

```
root@6b88eaae6a1b:/# nc -u 192.168.60.5 9090
hello
hi
```

Where I observed about 8 to 13 seconds of udp connection being kept.

```
root@8282f3f499fc:/# conntrack -L
udp      17 26 src=10.9.0.5 dst=192.168.60.5 sport=33637 dport=9090
 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=33637 m
ark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
udp      17 24 src=10.9.0.5 dst=192.168.60.5 sport=33637 dport=9090
 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=33637 m
ark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
udp      17 22 src=10.9.0.5 dst=192.168.60.5 sport=33637 dport=9090
 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=33637 m
ark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
udp      17 20 src=10.9.0.5 dst=192.168.60.5 sport=33637 dport=9090
 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=33637 m
ark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
udp      17 18 src=10.9.0.5 dst=192.168.60.5 sport=33637 dport=9090
 [UNREPLIED] src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=33637 m
ark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
```

## TCP Experiment

Put Host1 to starting a netcat TCP server.

```
root@ef09d6ef87bd:/# nc -l 9090
```

Then sending UDP packets from HostA.

```
root@6b88eaae6a1b:/# nc 192.168.60.5 9090
hello
```

It is evident that router keeps the connection of TCP for as long as possible.

```
4 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
tcp      6 431959 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=3
8114 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=3811
4 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
tcp      6 431957 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=3
8114 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=3811
4 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
tcp      6 431955 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=3
8114 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=3811
4 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
tcp      6 431923 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=3
8114 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=3811
4 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
tcp      6 431921 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=3
8114 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=3811
4 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/# conntrack -L
tcp      6 431921 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=3
8114 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=3811
4 [ASSURED] mark=0 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@8282f3f499fc:/#
```

## Task 3.B

Configured the IPTables of the router accordingly.

```
root@8282f3f499fc:/# iptables -A FORWARD -p tcp -i eth0 -d 192.168.60.5 --dport 23 --syn -m conntrack --ctstate NEW -j ACCEPT
root@8282f3f499fc:/# iptables -A FORWARD -i eth1 -p tcp --syn -m conntrack --ctstate NEW -j ACCEPT
root@8282f3f499fc:/# iptables -A FORWARD -p tcp -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
root@8282f3f499fc:/# iptables -A FORWARD -p tcp -j DROP
root@8282f3f499fc:/# iptables -P FORWARD ACCEPT
root@8282f3f499fc:/# 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 ctstate NEW
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp flags:0x17/0x02 ctstate NEW
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            ctstate RELATED,ESTABLISHED
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@8282f3f499fc:/#
```

Noticed that connection from Host1 to HostA is allowed.

```
root@ef09d6ef87bd:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
6b88eaae6a1b 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 tha
t 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 b
y
applicable law.

seed@6b88eaae6a1b:~$ ls
seed@6b88eaae6a1b:~$ exit
logout
Connection closed by foreign host.
root@ef09d6ef87bd:/#
```

Connection from HostA to Host1 is not permitted.

```
root@6b88eaae6a1b:/# telnet 192.168.60.6
Trying 192.168.60.6...
telnet: Unable to connect to remote host: Connection timed out
root@6b88eaae6a1b:/#
```

Connection from Host2 to Host1 is allowed.

```
root@c5f9701cc70d:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
ef09d6ef87bd 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 tha
t 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 b
y
applicable law.

seed@ef09d6ef87bd:~$
```

Now flushed the table and made new configurations with rules.

```
root@8282f3f499fc:/# iptables -F
root@8282f3f499fc:/# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@8282f3f499fc:/# iptables -p FORWARD ACCEPT
iptables v1.8.4 (legacy): unknown protocol "forward" specified
Try `iptables -h' or 'iptables --help' for more information.
root@8282f3f499fc:/# iptables -P FORWARD ACCEPT
root@8282f3f499fc:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 --syn -j ACCEPT
root@8282f3f499fc:/# iptables -A FORWARD -i eth0 -p tcp --syn -j DROP
root@8282f3f499fc:/# iptables -A FORWARD -p tcp -j ACCEPT
root@8282f3f499fc:/# iptables -P FORWARD ACCEPT
root@8282f3f499fc:/# 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
DROP       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

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@8282f3f499fc:/#
```

I tried telnetting from HostA to Host2 and it wasn't allowed but it was allowed to Host1.

```
root@6b88eaae6a1b:/# telnet 192.168.60.6
Trying 192.168.60.6...
```

Telnet from Host2 to HostA is allowed and same if for other inner Hosts to outer Hosts.

```
root@c5f9701cc70d:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
6b88eaae6a1b 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 tha
t 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 Nov 18 01:24:36 UTC 2023 from 192.168.60.5 on pts/2
seed@6b88eaae6a1b:~$
```

Flushing these rules for the next task.

```
root@8282f3f499fc:/# iptables -F
root@8282f3f499fc:/# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@8282f3f499fc:/#
```

## Task 4

Made the asked rule configurations on router.

```
root@8282f3f499fc:/# iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/minute --limit-burst 5 -j ACCEPT
root@8282f3f499fc:/# iptables -A FORWARD -s 10.9.0.5 -j DROP
root@8282f3f499fc:/# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  10.9.0.5            0.0.0.0/0            limit: avg 10/min burst 5
DROP       all  --  10.9.0.5            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@8282f3f499fc:/#
```

I tried with the first rule, but it didn't seem to limit the packets but after placing the second rule it started to limit the network traffic from outside HostA.

```
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=0.066 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.058 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.047 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.046 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.056 ms
64 bytes from 10.9.0.5: icmp_seq=7 ttl=63 time=0.064 ms
64 bytes from 10.9.0.5: icmp_seq=13 ttl=63 time=0.065 ms
64 bytes from 10.9.0.5: icmp_seq=19 ttl=63 time=0.046 ms
64 bytes from 10.9.0.5: icmp_seq=25 ttl=63 time=0.047 ms
64 bytes from 10.9.0.5: icmp_seq=31 ttl=63 time=0.050 ms
64 bytes from 10.9.0.5: icmp_seq=37 ttl=63 time=0.061 ms
64 bytes from 10.9.0.5: icmp_seq=42 ttl=63 time=0.058 ms
64 bytes from 10.9.0.5: icmp_seq=48 ttl=63 time=0.049 ms
64 bytes from 10.9.0.5: icmp_seq=54 ttl=63 time=0.059 ms
64 bytes from 10.9.0.5: icmp_seq=60 ttl=63 time=0.048 ms
64 bytes from 10.9.0.5: icmp_seq=66 ttl=63 time=0.053 ms
64 bytes from 10.9.0.5: icmp_seq=72 ttl=63 time=0.048 ms
64 bytes from 10.9.0.5: icmp_seq=78 ttl=63 time=0.056 ms
64 bytes from 10.9.0.5: icmp_seq=84 ttl=63 time=0.047 ms
64 bytes from 10.9.0.5: icmp_seq=89 ttl=63 time=0.067 ms
64 bytes from 10.9.0.5: icmp_seq=95 ttl=63 time=0.050 ms
64 bytes from 10.9.0.5: icmp_seq=101 ttl=63 time=0.057 ms
64 bytes from 10.9.0.5: icmp_seq=107 ttl=63 time=0.048 ms
64 bytes from 10.9.0.5: icmp_seq=113 ttl=63 time=0.045 ms
64 bytes from 10.9.0.5: icmp_seq=119 ttl=63 time=0.055 ms
```

Flushed the routed IPTables for the next task.

```
root@8282f3f499fc:/# iptables -F
root@8282f3f499fc:/# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@8282f3f499fc:/#
```

## Task 5

I put this command in all inner Host1, Host2 and Host3.

```
root@ef09d6ef87bd:/# nc -luk 8080
```

Placing the rule in router.

```
root@8282f3f499fc:/# iptables -t nat -A PREROUTING -p udp --dport 8
080 -m statistic --mode nth --every 3 --packet 0 -j DNAT --to-desti
nation 192.168.60.5:8080
```

From HostA I sent this packet to router.

```
root@6b88eaae6a1b:/# echo hello | nc -u 10.9.0.11 8080
^C
root@6b88eaae6a1b:/#
```

I only received a packet in Host1.

```
root@ef09d6ef87bd:/# nc -luk 8080
hello
```

Added two more rules on the router.

```
root@8282f3f499fc:/# iptables -t nat -A PREROUTING -p udp --dport 8root@8282f3f499fc:/# 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
root@8282f3f499fc:/# 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
```

Now checking the nat IPTables for the rules placed.

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

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@8282f3f499fc:/# 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 3 to:192.168.60.5:8080
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 statistic mode nth every 1 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:127.0.0.11:33839
DNAT       udp  --  0.0.0.0/0            127.0.0.11           udp dpt:53 to:127.0.0.11:59700

Chain DOCKER_POSTROUTING (1 references)
target     prot opt source               destination
SNAT       tcp  --  127.0.0.11           0.0.0.0/0            tcp spt:33839 to::53
SNAT       udp  --  127.0.0.11           0.0.0.0/0            udp spt:59700 to::53
root@8282f3f499fc:/#
```

Again, from HostA I sent this packet to router.

```
root@6b88eaae6a1b:/# echo hello | nc -u 10.9.0.11 8080
^C
root@6b88eaae6a1b:/#
```

I only received a packet in Host1 only.

```
root@ef09d6ef87bd:/# nc -luk 8080
hello
hello
```

Then I send again the packets to router from HostA and I found that each time a packet is sent it is sent to another internal Host which makes load balancing till here a success. So it can be said that if I only put uc -c 10.9.0.11 8080 and not used echo, I would receive packets in only in one of the internal Hosts but when I put delay in typing and entering then I receive packets in all the internal Hosts.

```
root@c5f9701cc70d:/# nc -luk 8080
hello
```

```
root@85498c1f767c:/# nc -luk 8080
hello
```

Now checking the nat IPTable with line numbers.

```
root@8282f3f499fc:/# iptables -t nat -L -n --line-numbers
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0
udp dpt:8080 statistic mode nth every 3 to:192.168.60.5:8080
2    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
3    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0
udp dpt:8080 statistic mode nth every 1 to:192.168.60.7:8080

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

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


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


Chain DOCKER_OUTPUT (1 references)
num  target     prot opt source               destination
1    DNAT       tcp  --  0.0.0.0/0            127.0.0.11
tcp dpt:53 to:127.0.0.11:33839
2    DNAT       udp  --  0.0.0.0/0            127.0.0.11
udp dpt:53 to:127.0.0.11:59700

Chain DOCKER_POSTROUTING (1 references)
num  target     prot opt source               destination
1    SNAT       tcp  --  127.0.0.11           0.0.0.0/0
```

Adding more configurations to the router.

```
root@8282f3f499fc:/# iptables -t nat -D PREROUTING 1
root@8282f3f499fc:/# iptables -t nat -D PREROUTING 2
root@8282f3f499fc:/# iptables -t nat -D PREROUTING 3
iptables: Index of deletion too big.
root@8282f3f499fc:/# iptables -t nat -D PREROUTING 1
```

```
root@8282f3f499fc:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 0.33333 -j DNAT --to-destinat
ion 192.168.60.5:8080
root@8282f3f499fc:/# 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
root@8282f3f499fc:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 1 -j DNAT --to-destination 19
2.168.60.7:8080
root@8282f3f499fc:/#
```

Checking the configurations,

```
root@8282f3f499fc:/# iptables -t nat -L -n --line-numbers
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0
udp dpt:8080 statistic mode random probability 0.33332999982 to:192
.168.60.5:8080
2    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0
udp dpt:8080 statistic mode random probability 0.50000000000 to:192
.168.60.6:8080
3    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0
udp dpt:8080 statistic mode random probability 1.00000000000 to:192
.168.60.7:8080

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

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


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


Chain DOCKER_OUTPUT (1 references)
num  target     prot opt source               destination
1    DNAT       tcp  --  0.0.0.0/0            127.0.0.11
tcp dpt:53 to:127.0.0.11:33839
2    DNAT       udp  --  0.0.0.0/0            127.0.0.11
udp dpt:53 to:127.0.0.11:50700
```

I have sent packets, and it is based on probability now but randomly. Given it is also based on round robin, so it gives it to another process.

```
root@6b88eaae6a1b:/# nc -u 10.9.0.11 8080
hi1
hi2
hi3
hi4
hi5
hi6
^C
root@6b88eaae6a1b:/# echo "hi" | nc -u 10.9.0.11 8080
hi
^[[A^[[A^C
root@6b88eaae6a1b:/# echo "hello" | nc -u 10.9.0.11 8080
^C
root@6b88eaae6a1b:/# echo "hello" | nc -u 10.9.0.11 8080
^C
root@6b88eaae6a1b:/# echo "hello" | nc -u 10.9.0.11 8080
^C
root@6b88eaae6a1b:/# echo "hello" | nc -u 10.9.0.11 8080^C
root@6b88eaae6a1b:/# echo "hello" | nc -u 10.9.0.11 8080
^C
root@6b88eaae6a1b:/#
```

Host1 got these.

```
root@ef09d6ef87bd:/# nc -luk 8080
hi
hello
hello
```

Host2 got these.

```
root@c5f9701cc70d:/# nc -luk 8080
hello
hi1
hi2
hello
```

Host3 got these.

```
root@85498c1f767c:/# nc -luk 8080
hello
hi3
hi4
hi5
hi6
hello
```