



Clemson University

Lab-5: Firewall Exploration Lab.
CPSC:8570
Spring- 2022

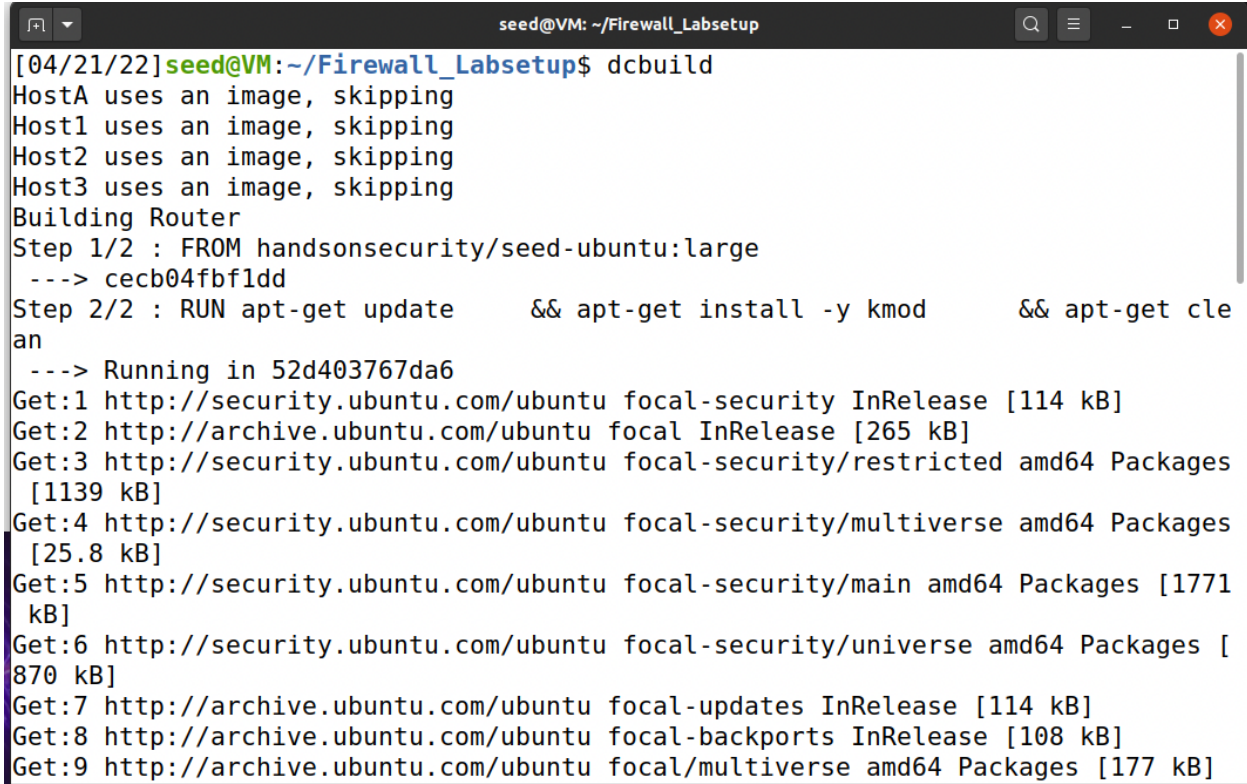
Course Instructor: Dr. Long Cheng

by:
Sai Vinay Nandigam
CUID: C17742253

Description:

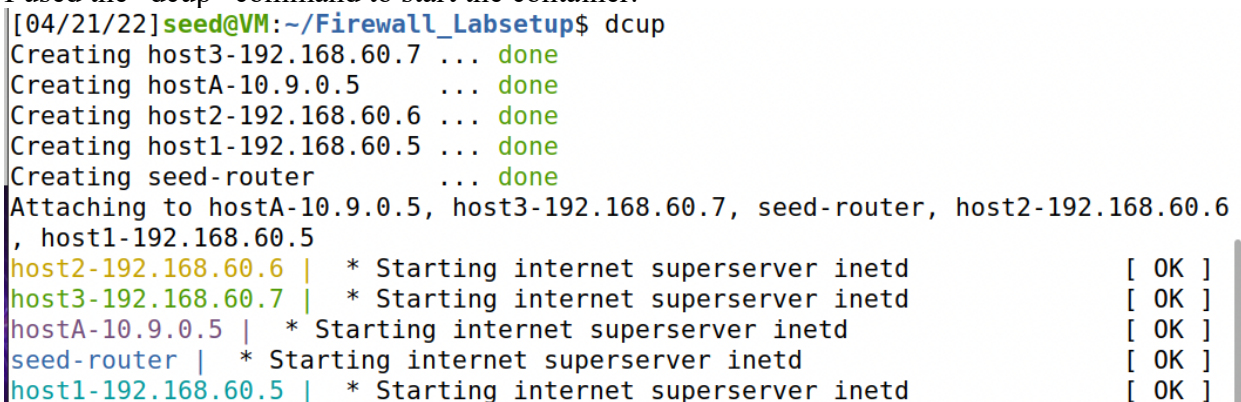
In this lab, I learned how firewalls work and set up a simple firewall for a network. Linux already has a built-in firewall based on Netfilter, and This firewall is also called iptables. I used iptables to set up firewall rules to protect the network. I have downloaded the labsetup.zip file from the seed lab website, and used the docker-compose.yml file to setup the lab environment. Later, I have completed both Task-1A&1B and its sub-tasks successfully.

I used the “**dcbuild**” command to build the container.



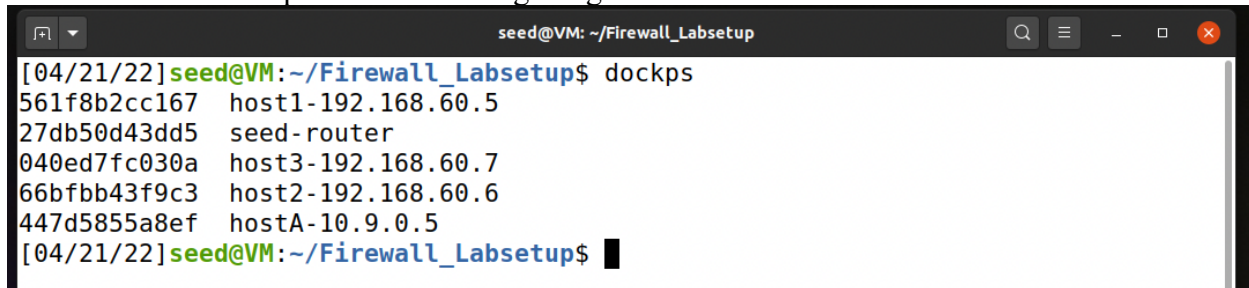
```
[04/21/22]seed@VM:~/Firewall_Labsetup$ dcbuild
HostA uses an image, skipping
Host1 uses an image, skipping
Host2 uses an image, skipping
Host3 uses an image, skipping
Building Router
Step 1/2 : FROM handsonsecurity/seed-ubuntu:large
---> cecb04fbf1dd
Step 2/2 : RUN apt-get update      && apt-get install -y kmod      && apt-get cle
an
---> Running in 52d403767da6
Get:1 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:2 http://archive.ubuntu.com/ubuntu focal InRelease [265 kB]
Get:3 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages
[1139 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Packages
[25.8 kB]
Get:5 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [1771
kB]
Get:6 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [
870 kB]
Get:7 http://archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:8 http://archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:9 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [177 kB]
```

I used the “**dcup**” command to start the container.



```
[04/21/22]seed@VM:~/Firewall_Labsetup$ dcup
Creating host3-192.168.60.7 ... done
Creating hostA-10.9.0.5      ... done
Creating host2-192.168.60.6 ... done
Creating host1-192.168.60.5 ... done
Creating seed-router         ... done
Attaching to hostA-10.9.0.5, host3-192.168.60.7, seed-router, host2-192.168.60.6
, host1-192.168.60.5
host2-192.168.60.6 | * Starting internet superserver inetd          [ OK ]
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 ]
host1-192.168.60.5 | * Starting internet superserver inetd          [ OK ]
```

I have used the “dockps” command for getting the ID’s of the container.

A terminal window titled 'seed@VM: ~/Firewall_Labsetup' showing the output of the 'dockps' command. The output lists five containers with their IDs and IP addresses: host1-192.168.60.5, seed-router, host3-192.168.60.7, host2-192.168.60.6, and hostA-10.9.0.5.

```
[04/21/22]seed@VM:~/Firewall_Labsetup$ dockps
561f8b2cc167    host1-192.168.60.5
27db50d43dd5    seed-router
040ed7fc030a    host3-192.168.60.7
66bfbb43f9c3    host2-192.168.60.6
447d5855a8ef    hostA-10.9.0.5
[04/21/22]seed@VM:~/Firewall_Labsetup$
```

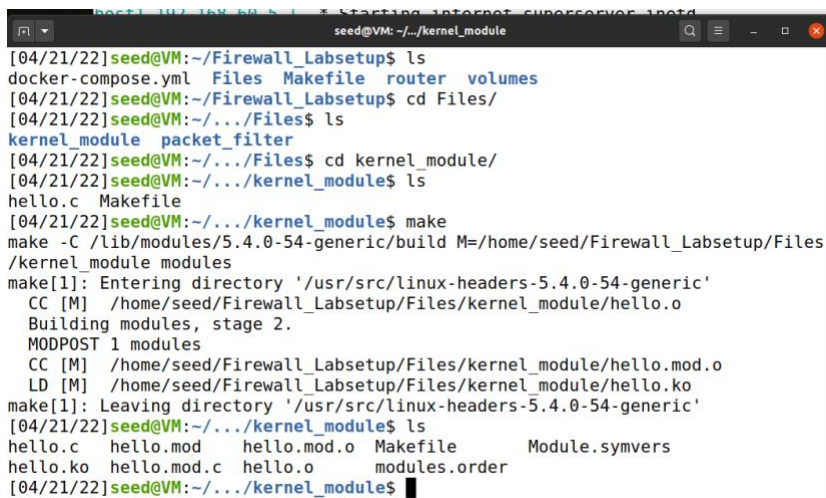
Compare with the figure in the manual.

Task-1 Implementing a Simple Firewall.

In this task I have implemented a simple packet filtering type of firewall, which inspects each incoming and outgoing packets. Since the packet processing is done within the kernel, i have done the filtering also in the kernel. I have modified the kernel by rebuilding the kernel.

Task-1A: Implement a simple kernel module.

I have implemented a simple loadable kernel module, when it is loaded it displays the “Hello World!” message. When the module is removed, it prints “Bye-bye World”. These both the messages were displayed when I use “dmesg” command. The following screenshots are the step by step executions.

A terminal window titled 'seed@VM: ~/kernel_module' showing the steps to build and install a kernel module. The user navigates to the 'Files' directory, then to 'kernel_module', and runs 'make' to build the module. The output shows the compilation process and the resulting files: hello.c, hello.mod, hello.mod.c, hello.o, and modules.order.

```
[04/21/22]seed@VM:~/Firewall_Labsetup$ ls
docker-compose.yml  Files  Makefile  router  volumes
[04/21/22]seed@VM:~/Firewall_Labsetup$ cd Files/
[04/21/22]seed@VM:~/Files$ ls
kernel_module  packet_filter
[04/21/22]seed@VM:~/Files$ cd kernel_module/
[04/21/22]seed@VM:~/kernel_module$ ls
hello.c  Makefile
[04/21/22]seed@VM:~/kernel_module$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Firewall_Labsetup/Files
/kernel_module modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
CC [M] /home/seed/Firewall_Labsetup/Files/kernel_module/hello.o
Building modules, stage 2.
MODPOST 1 modules
CC [M] /home/seed/Firewall_Labsetup/Files/kernel_module/hello.mod.o
LD [M] /home/seed/Firewall_Labsetup/Files/kernel_module/hello.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[04/21/22]seed@VM:~/kernel_module$ ls
hello.c  hello.mod  hello.mod.o  Makefile      Module.symvers
hello.ko  hello.mod.c  hello.o      modules.order
[04/21/22]seed@VM:~/kernel_module$
```

I have opened a new terminal and checked the kernel buffer, there are messages so I have cleaned them.

```
seed@VM: ~/.../kernel_module
ined" name="snap.snap-store.ubuntu-software" pid=3822 comm="apparmor_parser"
[ 321.172479] audit: type=1400 audit(1650559048.974:47): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="snap.snap-store.ubuntu-software-local-file" pid=3823 comm="apparmor_parser"
[ 323.059711] audit: type=1400 audit(1650559050.862:48): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/snap/snapd/15534/usr/lib/snapd/snap-confine" pid=3892 comm="apparmor_parser"
[ 323.073981] audit: type=1400 audit(1650559050.878:49): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/snap/snapd/15534/usr/lib/snapd/snap-confine//mount-namespace-capture-helper" pid=3892 comm="apparmor_parser"
[ 323.276966] audit: type=1400 audit(1650559051.078:50): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.hook.configur" pid=3895 comm="apparmor_parser"
[ 405.841371] ohci-pci 0000:00:06.0: frame counter not updating; disabled
[ 405.841377] ohci-pci 0000:00:06.0: HC died; cleaning up
[ 405.841881] usb 1-1: USB disconnect, device number 2
[04/21/22]seed@VM:~/.../kernel_module$ dmesg -clear
dmesg: unknown level 'ear'
[04/21/22]seed@VM:~/.../kernel_module$ dmesg --clear
dmesg: klogctl failed: Operation not permitted
[04/21/22]seed@VM:~/.../kernel_module$ sudo dmesg --clear
[04/21/22]seed@VM:~/.../kernel_module$ dmesg
[04/21/22]seed@VM:~/.../kernel_module$
```

I have executed “sudo insmod hello.ko” command and checked the kernel buffer, then it displayed “Hello World!”. Later I dropped it by using “sudo rmmod hello” command and displayed “Bye-bye World!” in the kernel buffer.

```
seed@VM:~/.../kernel_module$ sudo insmod hello.ko
seed@VM:~/.../kernel_module$ sudo rmmod hello
```

```
seed@VM: ~/.../kernel_module
parser"
[ 323.059711] audit: type=1400 audit(1650559050.862:48): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/snap/snapd/15534/usr/lib/snapd/snap-confine" pid=3892 comm="apparmor_parser"
[ 323.073981] audit: type=1400 audit(1650559050.878:49): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/snap/snapd/15534/usr/lib/snapd/snap-confine//mount-namespace-capture-helper" pid=3892 comm="apparmor_parser"
[ 323.276966] audit: type=1400 audit(1650559051.078:50): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap.snap-store.hook.configur" pid=3895 comm="apparmor_parser"
[ 405.841371] ohci-pci 0000:00:06.0: frame counter not updating; disabled
[ 405.841377] ohci-pci 0000:00:06.0: HC died; cleaning up
[ 405.841881] usb 1-1: USB disconnect, device number 2
[04/21/22]seed@VM:~/.../kernel_module$ dmesg -clear
dmesg: unknown level 'ear'
[04/21/22]seed@VM:~/.../kernel_module$ dmesg --clear
dmesg: klogctl failed: Operation not permitted
[04/21/22]seed@VM:~/.../kernel_module$ sudo dmesg --clear
[04/21/22]seed@VM:~/.../kernel_module$ dmesg
[04/21/22]seed@VM:~/.../kernel_module$ dmesg -k -w
[ 1229.683664] hello: module verification failed: signature and/or required key missing - tainting kernel
[ 1229.684799] Hello World!
```

```
] Hello World!
```

```
] Bye-bye World!.
```

```
d@VM:~/.../kernel_module$
```


I first executed `dmesg -k -w` and later I executed the file. Then I came back to the kernel buffer. It displays “Hello World!”. When I dropped it displayed “Bye-bye World!”. Hence Task-1A completed.

Task-1B: Implement a Simple Firewall using Netfilter:

First I have pinged to 8.8.8.8 and checked whether it's working or not.

```
[04/21/22]seed@VM:~/.../packet_filter$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=63 time=83.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=63 time=161 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=63 time=72.2 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=63 time=66.3 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=63 time=86.9 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=63 time=113 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=63 time=106 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=63 time=110 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=63 time=95.6 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=63 time=97.8 ms
```

I also pinged the www.example.com to check whether it's working or not.

```
[04/21/22]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=63 time=48.1 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=2 ttl=63 time=65.9 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=3 ttl=63 time=62.0 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=4 ttl=63 time=61.5 ms
^C
--- www.example.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 48.059/59.378/65.909/6.752 ms
[04/21/22]seed@VM:~/.../packet_filter$ dig 8.8.8.8 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> 8.8.8.8 www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 24910
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 65494
;; QUESTION SECTION:
;8.8.8.8.                IN      A

;; Query time: 152 msec
```

Here we got the IP address.

```
;; Query time: 152 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu Apr 21 14:27:27 EDT 2022
;; MSG SIZE rcvd: 36

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51415
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.example.com.                IN      A

;; ANSWER SECTION:
www.example.com.                662     IN      A      93.184.216.34

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu Apr 21 14:27:27 EDT 2022
;; MSG SIZE rcvd: 60
```

I used the command “sudo insmod seedFilter.ko” command to run the file.

```
[04/21/22]seed@VM:~/.../packet_filter$ ls
Makefile  seedFilter.c
[04/21/22]seed@VM:~/.../packet_filter$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Firewall_Labsetup/Files
/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CC [M]  /home/seed/Firewall_Labsetup/Files/packet_filter/seedFilter.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/Firewall_Labsetup/Files/packet_filter/seedFilter.mod.o
  LD [M]  /home/seed/Firewall_Labsetup/Files/packet_filter/seedFilter.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[04/21/22]seed@VM:~/.../packet_filter$ ls
Makefile      Module.symvers  seedFilter.ko   seedFilter.mod.c  seedFilter.o
modules.order seedFilter.c    seedFilter.mod  seedFilter.mod.o
[04/21/22]seed@VM:~/.../packet_filter$ sudo insmod seedFilter.ko
[04/21/22]seed@VM:~/.../packet_filter$
```

```
[04/21/22]seed@VM:~/.../packet_filter$ sudo insmod seedFilter.ko
[04/21/22]seed@VM:~/.../packet_filter$ lsmod | grep -i seed
seedFilter                16384  0
[04/21/22]seed@VM:~/.../packet_filter$
```

In the buffer it display's that the filters are getting registered.

```
50 560 804 093 737 000 ns fSetTimeLastLoop=true )
[ 3355.969854] Registering filters.
```

```
change: 3 6/6 806 611 000ns (GuestNow=1 650 564 480 900 348 000 ns GuestLas
50 560 804 093 737 000 ns fSetTimeLastLoop=true )
[ 3355.969854] Registering filters.
[ 3516.330503] *** LOCAL_OUT
[ 3516.330505] 10.0.2.15 --> 67.202.185.122 (UDP)
[ 3516.405755] *** LOCAL_OUT
[ 3516.405757] 127.0.0.1 --> 127.0.0.53 (UDP)
[ 3516.406107] *** LOCAL_OUT
[ 3516.406108] 10.0.2.15 --> 67.202.185.122 (UDP)
[ 3516.487380] *** LOCAL_OUT
[ 3516.487385] 127.0.0.53 --> 127.0.0.1 (UDP)
[ 3519.267348] *** LOCAL_OUT
[ 3519.267351] 127.0.0.1 --> 127.0.0.53 (UDP)
[ 3519.267784] *** LOCAL_OUT
[ 3519.267786] 10.0.2.15 --> 67.202.185.122 (UDP)
[ 3519.325967] *** LOCAL_OUT
[ 3519.325970] 127.0.0.1 --> 127.0.0.53 (UDP)
[ 3519.337778] *** LOCAL_OUT
[ 3519.337782] 127.0.0.53 --> 127.0.0.1 (UDP)
[ 3519.337842] *** LOCAL_OUT
[ 3519.337844] 127.0.0.53 --> 127.0.0.1 (UDP)
```

I have used the `dig @8.8.8.8 www.example.com` command, and then immediately in the buffer the packets are dropping.

```
[04/21/22]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
```

The packets are dropping.

```
[ 5229.531183] 127.0.0.1 --> 127.0.0.1 (UDP)
[ 5229.531442] *** LOCAL_OUT
[ 5229.531444] 10.0.2.15 --> 8.8.8.8 (UDP)
[ 5229.531449] *** Dropping 8.8.8.8 (UDP), port 53
[ 5234.532521] *** LOCAL_OUT
[ 5234.532524] 10.0.2.15 --> 8.8.8.8 (UDP)
[ 5234.532538] *** Dropping 8.8.8.8 (UDP), port 53
[ 5239.549658] *** LOCAL_OUT
[ 5239.549663] 10.0.2.15 --> 8.8.8.8 (UDP)
[ 5239.549702] *** Dropping 8.8.8.8 (UDP), port 53
```

When I executed the command `sudo rmod seedFilter` command, in the buffer the filters are being removed.

```
[04/21/22] seed@VM:~/.../packet_filter$ sudo rmmod seedFilter
[04/21/22] seed@VM:~/.../packet_filter$
```

```
[ 5327.429871] The filters are being removed.
```

TASK-1B- Subtask-1 completed.

Subtask-2

For this task I have hooked printInfo function to the netfilter hooks(NF_INET_PRE_ROUTING NF_INET_LOCAL_IN NF_INET_FORWARD NF_INET_LOCAL_OUT NF_INET_POST_ROUTING). I have modified the code by adding additional hooks and netfilters and executed the code. The filters are registered in the buffer and when I removed the filters are removed.

```
[04/21/22] seed@VM:~/.../packet_filter$ cp seedFilter.c seedPrint.c
[04/21/22] seed@VM:~/.../packet_filter$ gedit seedPrint.c
[04/21/22] seed@VM:~/.../packet_filter$ gedit seedPrint.c &
[2] 6775
[04/21/22] seed@VM:~/.../packet_filter$
```

I made changes to make file

Makefile	seedFilter.c
1#obj-m += seedFilter.o	
2obj-m += seedPrint.o	
3all:	
4 make -C /lib/modules/\$(shell uname -r)/build M=\$(PWD) modules	
5	

I have added 3 more hooks to the code because as mentioned in the task

```
11
12
13 static struct nf_hook_ops hook1, hook2, hook3, hook4, hook5;
14
15
```



```

78 hook1.hook = printInfo;
79 hook1.hooknum = NF_INET_LOCAL_OUT;
80 hook1.pf = PF_INET;
81 hook1.priority = NF_IP_PRI_FIRST;
82 nf_register_net_hook(&init_net, &hook1);
83
84 hook2.hook = printInfo;
85 hook2.hooknum = NF_INET_POST_ROUTING;
   nf_register_net_hook(&init_net, &hook3);

```

NF_INET_LOCAL_OUT

```

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);

```

NF_INET_POST_ROUTING

```

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);

```

```

return 0;

```

```

id removeFilter(void) {
   printk(KERN_INFO "The filters are being removed.\n");
   nf_unregister_net_hook(&init_net, &hook1);
   nf_unregister_net_hook(&init_net, &hook2);
   nf_unregister_net_hook(&init_net, &hook3);
   nf_unregister_net_hook(&init_net, &hook4);
   nf_unregister_net_hook(&init_net, &hook5);
}

```

```

[04/21/22] seed@VM:~/.../packet_filter$ sudo insmod seedPrint.ko
[04/21/22] seed@VM:~/.../packet_filter$ █
[ 5327.429871] The filters are being removed.
[ 7065.594005] SeedPrint:Registering filters.
█
[04/21/22] seed@VM:~/.../packet_filter$ sudo rmmod seedPrint
[04/21/22] seed@VM:~/.../packet_filter$ █
[ 7122.072489]      8.8.8.8 --> 10.0.2.15 (UDP)
[ 7191.843753] SeedPrint: The filters are being removed.
█

```

Subtask-2 completed.....

Subtask-3:

To prevent other computers to ping VM and prevent other computers to telnet into VM. I have implemented the two different functions and registered them to the same netfilter hook. I set the telnet tcp port to 23.

```
[04/21/22]seed@VM:~/.../packet_filter$ docksh hostA-10.9.0.5
root@447d5855a8ef:/# 
root@447d5855a8ef:/# 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=0.542 ms
64 bytes from 10.9.0.1: icmp_seq=2 ttl=64 time=0.067 ms
64 bytes from 10.9.0.1: icmp_seq=3 ttl=64 time=0.103 ms
64 bytes from 10.9.0.1: icmp_seq=4 ttl=64 time=0.068 ms
64 bytes from 10.9.0.1: icmp_seq=5 ttl=64 time=0.115 ms
^C
--- 10.9.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4079ms
rtt min/avg/max/mdev = 0.067/0.179/0.542/0.182 ms
root@447d5855a8ef:/# 
root@447d5855a8ef:/# 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.
0 of these updates are security updates.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
```

I have modified the code I gave 2 new hooks one is for telnet and the other is for the HOST A machine

```
hook3.hook = blockICMP;
hook3.hooknum = NF_INET_PRE_ROUTING;
hook3.pf = PF_INET;
hook3.priority = NF_IP_PRI_FIRST;
nf_register_net_hook(&init_net, &hook3);
```

```
hook4.hook = blockTelnet;
hook4.hooknum = NF_INET_PRE_ROUTING;
hook4.pf = PF_INET;
hook4.priority = NF_IP_PRI_FIRST;
nf_register_net_hook(&init_net, &hook4);
```

```
return 0;
```

```
void removeFilter(void) {
    printk(KERN_INFO "SeedBlock: The filters are being removed.\n");
    nf_unregister_net_hook(&init_net, &hook1);
    nf_unregister_net_hook(&init_net, &hook2);
    nf_unregister_net_hook(&init_net, &hook3);
    nf_unregister_net_hook(&init_net, &hook4);
}
```

```
[04/21/22]seed@VM:~/.../packet_filter$ ls
Makefile      seedBlock.c  seedBlock.mod.c  seedFilter.c
modules.order seedBlock.ko  seedBlock.mod.o  seedPrint.c
Module.symvers seedBlock.mod seedBlock.o
[04/21/22]seed@VM:~/.../packet_filter$ sudo insmod seedBlock.ko
[04/21/22]seed@VM:~/.../packet_filter$ 
[04/21/22]seed@VM:~/.../packet_filter$ sudo insmod seedBlock.ko
[04/21/22]seed@VM:~/.../packet_filter$ sudo rmmod seedBlock
[04/21/22]seed@VM:~/.../packet_filter$
```

In buffer the filters are being removed when I executed the command “rmmod seedBlock”.

```
[10118.660010] 127.0.0.53 --> 127.0.0.1 (UDP)
[10118.660048] *** LOCAL_OUT
[10118.660049] 127.0.0.53 --> 127.0.0.1 (UDP)
[10153.832221] The filters are being removed.
```

```
host1 192.168.60.5.1 * Starting internet superserver inetd
seed@VM: ~/.../kernel_module
ppdev                24576  0
lp                   20480  0
parport              53248  3 parport_pc,lp,ppdev
drm                  491520  6 vmwgfx,drm_kms_helper,ttm
ip_tables            32768  2 iptable_filter,iptable_nat
x_tables             40960  7 xt_contrack,iptable_filter,xt_tcpudp,xt_addrtyp
e,xt_nat,ip_tables,xt_MASQUERADE
autofs4              45056  2
hid_generic          16384  0
usbhid               57344  0
hid                  131072  2 usbhid,hid_generic
crc32_pclmul         16384  0
ahci                  40960  2
psmouse              155648  0
i2c_piix4            28672  0
libahci              32768  1 ahci
e1000                147456  0
pata_acpi            16384  0
video                49152  0
[04/21/22] seed@VM: ~/.../kernel_module$ ls
hello.c  hello.mod  hello.mod.o  Makefile      Module.symvers
hello.ko hello.mod.c  hello.o      modules.order
[04/21/22] seed@VM: ~/.../kernel_module$ sudo insmod hello.ko
[04/21/22] seed@VM: ~/.../kernel_module$
```

TO find the hello model.

```
[04/21/22] seed@VM: ~/.../kernel_module$ lsmod | grep -i hello
hello                16384  0
[04/21/22] seed@VM: ~/.../kernel_module$
```

Now the hello do not display.

```
[04/21/22] seed@VM: ~/.../kernel_module$ lsmod | grep -i hello
hello                16384  0
[04/21/22] seed@VM: ~/.../kernel_module$ sudo rmmod hello
[04/21/22] seed@VM: ~/.../kernel_module$ lsmod | grep -i hello
[04/21/22] seed@VM: ~/.../kernel_module$
```


When I executed the remove command, it displayed “Bye-bye World!” here

```
[ 1229.683664] hello: module verification failed: signature and/or required key
missing - tainting kernel
[ 1229.684799] Hello World!
[ 1564.581047] Bye-bye World!.
```

```
[10377.870450] SeedBlock: Registering filters.
[10385.633892] *** LOCAL_OUT
[10385.633895]      10.0.2.15  --> 54.230.31.66 (TCP)
```

I have used the ping command in the Host A machine.

```
rtt min/avg/max/mdev = 0.057/0.088/0.143/0.020 ms
root@447d5855a8ef:/# ping 10.9.0.1
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data.
```

```
[10403.903439] *** Dropping 10.9.0.1 (UDP) -202890752
[10404.988894] *** Dropping 10.9.0.1 (UDP) -202890752
[10406.013305] *** Dropping 10.9.0.1 (UDP) -202890752
[10407.038032] *** Dropping 10.9.0.1 (UDP) -202890752
[10408.062160] *** Dropping 10.9.0.1 (UDP) -202890752
[10409.085131] *** Dropping 10.9.0.1 (UDP) -202889216
[10410.110336] *** Dropping 10.9.0.1 (UDP) -202889216
[10411.134231] *** Dropping 10.9.0.1 (UDP) -202889216
[10412.158107] *** Dropping 10.9.0.1 (UDP) -202889216
[10413.190443] *** Dropping 10.9.0.1 (UDP) -202889216
[10414.205469] *** Dropping 10.9.0.1 (UDP) -202889216
```

I tried to establish connection with the VM.

```
root@447d5855a8ef:/# 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: █
```

The result displayed here

```
[10437.759862] *** Dropping 10.9.0.1 (UDP) -202888704
[10438.782830] *** Dropping 10.9.0.1 (UDP) -202888704
[10493.201449] *** LOCAL_OUT
[10493.201451] 10.9.0.1 --> 10.9.0.5 (TCP)
[10493.201843] *** LOCAL_OUT
[10493.201845] 10.9.0.1 --> 10.9.0.5 (TCP)
[10493.211129] *** LOCAL_OUT
[10493.211131] 10.9.0.1 --> 10.9.0.5 (TCP)
[10493.211194] *** LOCAL_OUT
[10493.211201] 10.9.0.1 --> 10.9.0.5 (TCP)
[10493.211257] *** LOCAL_OUT
```

I removed the seedBlock

```
[04/21/22] seed@VM:~/.../packet_filter$ sudo insmod seedBlock.ko
[04/21/22] seed@VM:~/.../packet_filter$ sudo rmmmod seedBlock
```

The status that the filters are being removed was displayed.

```
[10546.483294] *** LOCAL_OUT
[10546.483296] 10.0.2.15 --> 35.224.170.84 (TCP)
[10583.195041] *** LOCAL_OUT
[10583.195088] 10.0.2.15 --> 35.82.230.35 (TCP)
[10583.195520] *** LOCAL_OUT
[10583.195523] 10.0.2.15 --> 35.82.230.35 (TCP)
[10646.592908] SeedBlock: The filters are being removed.
```

The **Subtask-3** completed and the whole task-1B completed.