

Lab-06: Firewall Exploration Lab

First let setup the environment. Volumes is a shared folder between the virtual machine & the containers. This lab we are going to use kernel modules and Iptables to set up the firewall. Bringing up and building up the containers.

```
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/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
--> Using cache
--> 431fee32e22b

Successfully built 431fee32e22b
Successfully tagged seed-router-image:latest
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup$ dcup
Starting host3-192.168.60.7 ... done
Starting seed-router      ... done
Starting host2-192.168.60.6 ... done
Starting host1-192.168.60.5 ... done
Starting hostA-10.9.0.5    ... done
Attaching to host1-192.168.60.5, host3-192.168.60.7, hostA-10.9.0.5, seed-router, host2-192.168.60.6
host3-192.168.60.7 | * Starting internet superserver inetd          [ OK ]
hostA-10.9.0.5 | * Starting internet superserver inetd          [ OK ]
host1-192.168.60.5 | * Starting internet superserver inetd          [ OK ]
host2-192.168.60.6 | * Starting internet superserver inetd          [ OK ]
seed-router | * Starting internet superserver inetd          [ OK ]
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup$ docker container ls
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/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
--> Using cache
--> 431fee32e22b

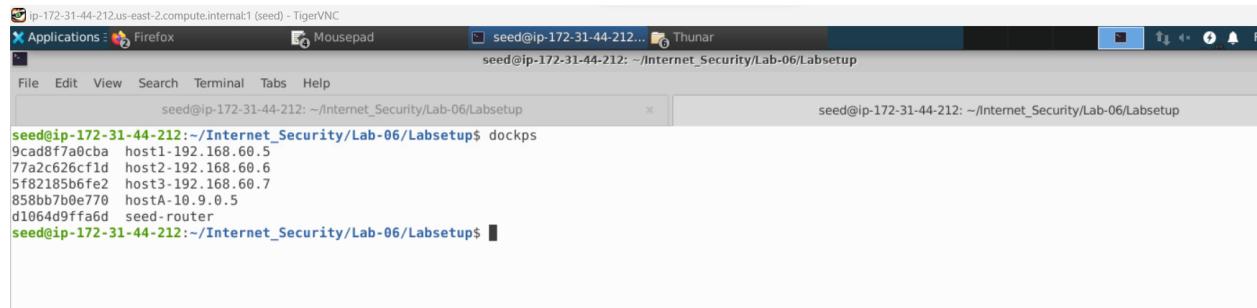
Successfully built 431fee32e22b
Successfully tagged seed-router-image:latest
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup$ dcup
Creating host3-192.168.60.7 ... done
Creating seed-router      ... done
Creating host2-192.168.60.6 ... done
Creating host1-192.168.60.5 ... done
Creating hostA-10.9.0.5    ... done
Attaching to host3-192.168.60.7, host1-192.168.60.5, host2-192.168.60.6, hostA-10.9.0.5, seed-router
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 ]
host1-192.168.60.5 | * Starting internet superserver inetd          [ OK ]
seed-router | * Starting internet superserver inetd          [ OK ]
```

```

seed@ip-172-31-44-212:~/Internet_Security/Lab-06/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
--> cecb04fb1dd
Step 2/2 : RUN apt-get update      && apt-get install -y kmod      && apt-get clean
--> Using cache
--> 431fee32e22b

Successfully built 431fee32e22b
Successfully tagged seed-router-image:latest
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup$ dcup
Creating host3-192.168.60.7 ... done
Creating seed-router ... done
Creating host2-192.168.60.6 ... done
Creating host1-192.168.60.5 ... done
Creating hostA-10.9.0.5 ... done
Attaching to host3-192.168.60.7, host1-192.168.60.5, host2-192.168.60.6, hostA-10.9.0.5, seed-router
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 ]
host1-192.168.60.5 | * Starting internet superserver inetd      [ OK ]
seed-router | * Starting internet superserver inetd      [ OK ]

```



Attacker is the virtual machine among this IP address- Attacker IP address-10.9.0.1

Most of the task will be carried out in the host machine the virtual machine.

Task 1: Implementing a Simple Firewall

SubTask 1.A: Implement a Simple Kernel Module

Here we will be seeing.

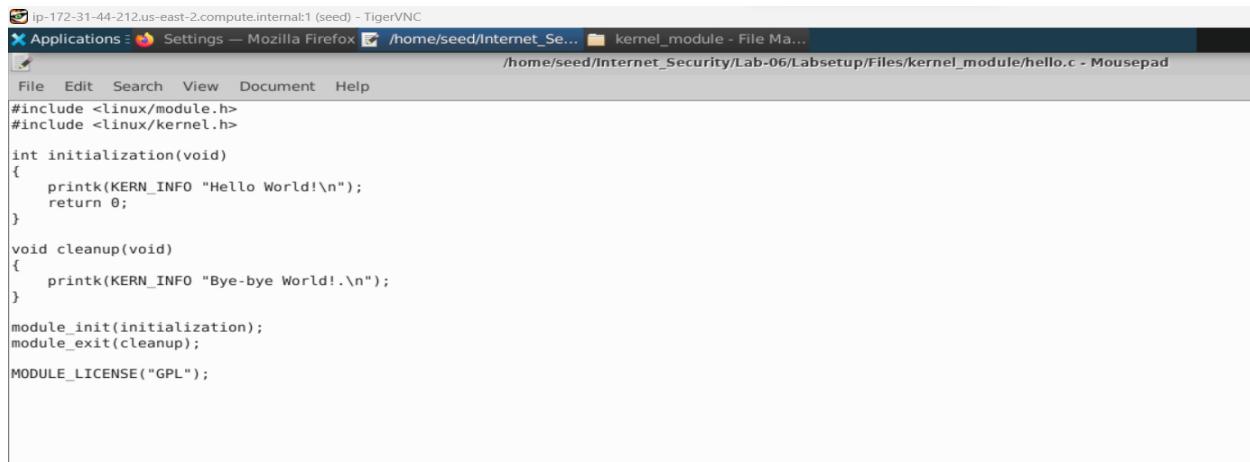
1. How to compile Kernel module
2. How to load Kernel module.
3. How to remove Kernel module
4. How to check it.

In the kernel_module we have hello.c and make file

We open hello.c and make file from kernel module

Make file: - Make file helps us to how to compile kernel module(Learned in lecture module_init and module_exit)

We have module init and module exit functions for the entry into the module and the other one for exiting from the module initialization and clean up.



```
#include <linux/module.h>
#include <linux/kernel.h>

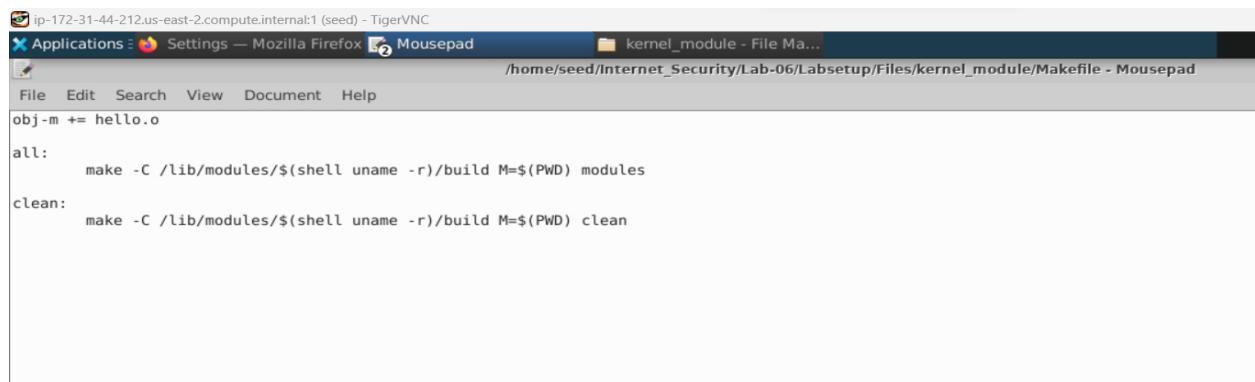
int initialization(void)
{
    printk(KERN_INFO "Hello World!\n");
    return 0;
}

void cleanup(void)
{
    printk(KERN_INFO "Bye-bye World!.\n");
}

module_init(initialization);
module_exit(cleanup);

MODULE_LICENSE("GPL");
```

We will be able to see this module information printed into the kernel buffer.

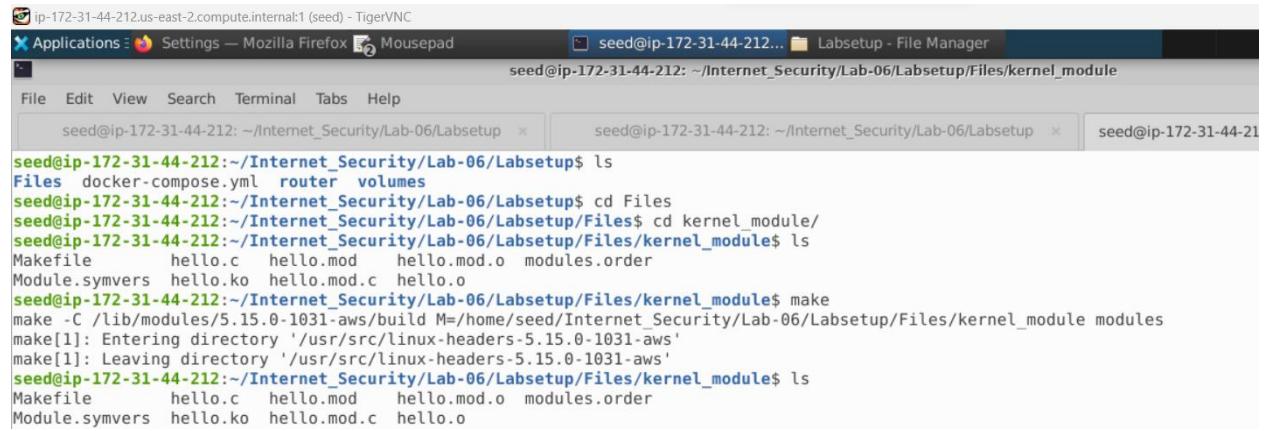


```
obj-m += hello.o

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

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

Here below we are able to see kernel module is built named as “hello.ko”



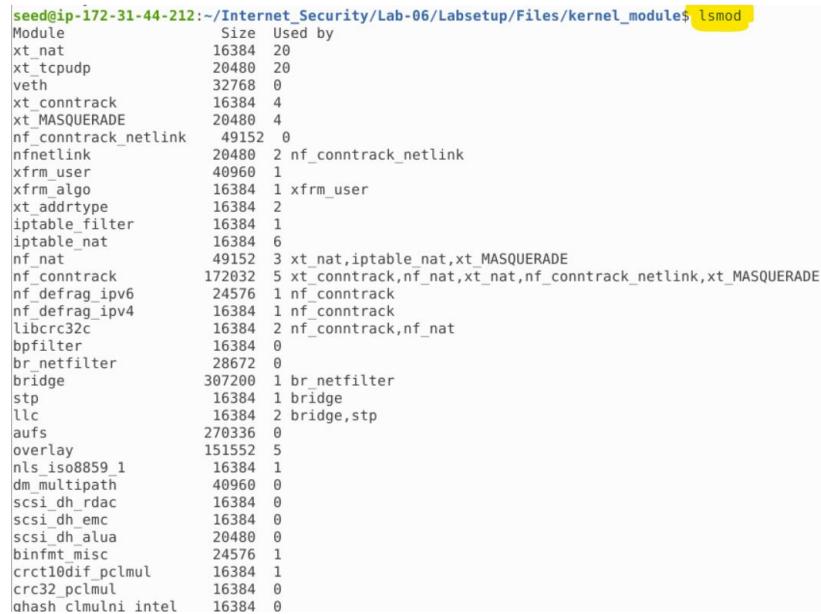
```
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup$ ls
Files docker-compose.yml router volumes
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup$ cd Files
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files$ cd kernel_module/
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ ls
Makefile hello.c hello.mod hello.mod.o modules.order
Module.symvers hello.ko hello.mod.c hello.o
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ make
make -C /lib/modules/5.15.0-1031-aws build M=/home/seed/Internet_Security/Lab-06/Labsetup/Files/kernel_module modules
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-1031-aws'
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-1031-aws'
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ ls
Makefile hello.c hello.mod hello.mod.o modules.order
Module.symvers hello.ko hello.mod.c hello.o
```

lsmod: - lsmod is a Unix-like operating system command which is used to display the status of modules in the Linux kernel. It results in a list of loaded modules.

We are able to see kernel module in built up hello.ko

make clean- To clean hello.ko

Now, for all the modules inside the system you can use **ls** model list or the modules. Here below in the screenshot we are able to see all the current modules inside the kernel.



```
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ lsmod
Module Size Used by
xt_nat 16384 20
xt_tcpudp 20480 20
veth 32768 0
xt_conntrack 16384 4
xt_MASQUERADE 20480 4
nf_conntrack_netlink 49152 0
nfnetlink 20480 2 nf_conntrack_netlink
xfrm_user 40960 1
xfrm_algo 16384 1 xfrm_user
xt_addrtype 16384 2
iptable_filter 16384 1
iptable_nat 16384 6
nf_nat 49152 3 xt_nat,iptable_nat,xt_MASQUERADE
nf_conntrack 172032 5 xt_conntrack,nf_nat,xt_nat,nf_conntrack_netlink,xt_MASQUERADE
nf_defrag_ipv6 24576 1 nf_conntrack
nf_defrag_ipv4 16384 1 nf_conntrack
libcrc32c 16384 2 nf_conntrack,nf_nat
bpfilter 16384 0
br_nfnetfilter 28672 0
bridge 307200 1 br_nfnetfilter
stp 16384 1 bridge
llc 16384 2 bridge,stp
aufs 270336 0
overlay 151552 5
nls_iso8859_1 16384 1
dm_multipath 40960 0
scsi_dh_rdac 16384 0
scsi_dh_emc 16384 0
scsi_dh_alua 20480 0
binfmt_misc 24576 1
crc32_pclmul 16384 1
crc32_pclmul 16384 0
qhash_clmulni_intel 16384 0
```

Now we are only interested in the kernel module we built. To insert the module into the kernel we use **insmod** by the kernel name.

“**sudo insmod hello.ko**”

Run another command by opening the other terminal tab.

dmesg- to check the kernel buffer. It can specify the supported local networks and so on. The kernel message and supported local facilities.

```
seed@ip-172-31-44-212: ~/Internet_Security/Lab-06/Labsetup/Files/kernel_module
File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212: ~/Internet_Security/... seed@ip-172-31-44-212: ~/Internet_Security/... seed@ip-172-31-44-212: ~/Internet_Security/... seed@ip-172-31-44-212:
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ dmesg --help

Usage:
dmesg [options]

Display or control the kernel ring buffer.

Options:
-C, --clear           clear the kernel ring buffer
-c, --read-clear     read and clear all messages
-D, --console-off    disable printing messages to console
-E, --console-on     enable printing messages to console
-F, --file <file>    use the file instead of the kernel log buffer
-f, --facility <list> restrict output to defined facilities
-H, --human          human readable output
-K, --kernel          display kernel messages
-L, --color[=<when>] colorize messages (auto, always or never)
                     colors are enabled by default
-l, --level <list>   restrict output to defined levels
-n, --console-level <level> set level of messages printed to console
-P, --nopager         do not pipe output into a pager
-p, --force-prefix   force timestamp output on each line of multi-line messages
-r, --raw             print the raw message buffer
-S, --syslog          force to use syslog(2) rather than /dev/kmsg
-s, --buffer-size <size> buffer size to query the kernel ring buffer
-U, --userspace       display userspace messages
-w, --follow          wait for new messages
-x, --decode          decode facility and level to readable string
-d, --show-delta      show time delta between printed messages
-e, --reltime         show local time and time delta in readable format
-T, --ctime            show human-readable timestamp (may be inaccurate!)
-t, --notime          don't show any timestamp with messages
                     show timestamp using the given format:
                     [delta|reltime|ctime|notime|iso]
--time-format <format>
SUSPENDING/RESUME WILL MAKE CTIME AND ISO TIMESTAMPS INACCURATE.

SUSPENDING/RESUME WILL MAKE CTIME AND ISO TIMESTAMPS INACCURATE.

-h, --help            display this help
-V, --version         display version

Supported log facilities:
kern - kernel messages
user - random user-level messages
mail - mail system
daemon - system daemons
auth - security/authorization messages
syslog - messages generated internally by syslogd
lpr - line printer subsystem
news - network news subsystem

Supported log levels (priorities):
emerg - system is unusable
alert - action must be taken immediately
crit - critical conditions
err - error conditions
warn - warning conditions
notice - normal but significant condition
info - informational
debug - debug-level messages

For more details see dmesg(1).
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$
```

The kernel message supported local facilities and you can show it.
We are able to see all the below messages in kernel

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo dmseg
[ 0.000000] Linux version 5.15.0-1033-aws (build@lcy02-amd64-026) (gcc (Ubuntu 9.4.0-1ubuntu1-20.04.1) 9.4.0, GNU ld (G
ntu SMP Fri Mar 17 11:39:30 UTC 2023 (Ubuntu 5.15.0-1033.37-20.04.1-aws 5.15.87)
[ 0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.15.0-1033-aws root=PARTUUID=645de17b-5f40-4fe7-8854-1cc9c4847270 ro
out=4294967295 panic=-1
[ 0.000000] KERNEL supported cpus:
[ 0.000000]   Intel GenuineIntel
[ 0.000000]   AMD AuthenticAMD
[ 0.000000]   Hygon HygonGenuine
[ 0.000000]   Centaur CentaurHauls
[ 0.000000]   zhaoxin Shanghai
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x008: 'MPX bounds registers'
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x010: 'MPX CSR'
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x020: 'AVX-512 opmask'
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x040: 'AVX-512 Hi256'
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x080: 'AVX-512 ZMM_Hi256'
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x200: 'Protection Keys User registers'
[ 0.000000] x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
[ 0.000000] x86/fpu: xstate_offset[3]: 832, xstate_sizes[3]: 64
[ 0.000000] x86/fpu: xstate_offset[4]: 896, xstate_sizes[4]: 64
[ 0.000000] x86/fpu: xstate_offset[5]: 960, xstate_sizes[5]: 64
[ 0.000000] x86/fpu: xstate_offset[6]: 1024, xstate_sizes[6]: 512
[ 0.000000] x86/fpu: xstate_offset[7]: 1536, xstate_sizes[7]: 1024
[ 0.000000] x86/fpu: xstate_offset[8]: 2048, xstate_sizes[8]: 1024
[ 0.000000] x86/fpu: xstate_offset[9]: 2560, xstate_sizes[9]: 1024
[ 0.000000] x86/fpu: xstate_offset[10]: 3072, xstate_sizes[10]: 1024
[ 0.000000] x86/fpu: xstate_offset[11]: 3584, xstate_sizes[11]: 1024
[ 0.000000] x86/fpu: xstate_offset[12]: 4104, xstate_sizes[12]: 1024
[ 0.000000] x86/fpu: xstate_offset[13]: 4624, xstate_sizes[13]: 1024
[ 0.000000] x86/fpu: xstate_offset[14]: 5144, xstate_sizes[14]: 1024
[ 0.000000] x86/fpu: xstate_offset[15]: 5664, xstate_sizes[15]: 1024
[ 0.000000] x86/fpu: xstate_offset[16]: 6184, xstate_sizes[16]: 1024
[ 0.000000] x86/fpu: xstate_offset[17]: 6704, xstate_sizes[17]: 1024
[ 0.000000] x86/fpu: xstate_offset[18]: 7224, xstate_sizes[18]: 1024
[ 0.000000] x86/fpu: xstate_offset[19]: 7744, xstate_sizes[19]: 1024
[ 0.000000] x86/fpu: xstate_offset[20]: 8264, xstate_sizes[20]: 1024
[ 0.000000] x86/fpu: xstate_offset[21]: 8784, xstate_sizes[21]: 1024
[ 0.000000] x86/fpu: xstate_offset[22]: 9304, xstate_sizes[22]: 1024
[ 0.000000] x86/fpu: xstate_offset[23]: 9824, xstate_sizes[23]: 1024
[ 0.000000] x86/fpu: xstate_offset[24]: 10344, xstate_sizes[24]: 1024
[ 0.000000] x86/fpu: xstate_offset[25]: 10864, xstate_sizes[25]: 1024
[ 0.000000] x86/fpu: xstate_offset[26]: 11384, xstate_sizes[26]: 1024
[ 0.000000] x86/fpu: xstate_offset[27]: 11904, xstate_sizes[27]: 1024
[ 0.000000] x86/fpu: xstate_offset[28]: 12424, xstate_sizes[28]: 1024
[ 0.000000] x86/fpu: xstate_offset[29]: 12944, xstate_sizes[29]: 1024
[ 0.000000] x86/fpu: xstate_offset[30]: 13464, xstate_sizes[30]: 1024
[ 0.000000] x86/fpu: xstate_offset[31]: 13984, xstate_sizes[31]: 1024
[ 0.000000] x86/fpu: xstate_offset[32]: 14504, xstate_sizes[32]: 1024
[ 0.000000] x86/fpu: xstate_offset[33]: 15024, xstate_sizes[33]: 1024
[ 0.000000] x86/fpu: xstate_offset[34]: 15544, xstate_sizes[34]: 1024
[ 0.000000] x86/fpu: xstate_offset[35]: 16064, xstate_sizes[35]: 1024
[ 0.000000] x86/fpu: xstate_offset[36]: 16584, xstate_sizes[36]: 1024
[ 0.000000] x86/fpu: xstate_offset[37]: 17104, xstate_sizes[37]: 1024
[ 0.000000] x86/fpu: xstate_offset[38]: 17624, xstate_sizes[38]: 1024
[ 0.000000] x86/fpu: xstate_offset[39]: 18144, xstate_sizes[39]: 1024
[ 0.000000] x86/fpu: xstate_offset[40]: 18664, xstate_sizes[40]: 1024
[ 0.000000] x86/fpu: xstate_offset[41]: 19184, xstate_sizes[41]: 1024
[ 0.000000] x86/fpu: xstate_offset[42]: 19704, xstate_sizes[42]: 1024
[ 0.000000] x86/fpu: xstate_offset[43]: 20224, xstate_sizes[43]: 1024
[ 0.000000] x86/fpu: xstate_offset[44]: 20744, xstate_sizes[44]: 1024
[ 0.000000] x86/fpu: xstate_offset[45]: 21264, xstate_sizes[45]: 1024
[ 0.000000] x86/fpu: xstate_offset[46]: 21784, xstate_sizes[46]: 1024
[ 0.000000] x86/fpu: xstate_offset[47]: 22304, xstate_sizes[47]: 1024
[ 0.000000] x86/fpu: xstate_offset[48]: 22824, xstate_sizes[48]: 1024
[ 0.000000] x86/fpu: xstate_offset[49]: 23344, xstate_sizes[49]: 1024
[ 0.000000] x86/fpu: xstate_offset[50]: 23864, xstate_sizes[50]: 1024
[ 0.000000] x86/fpu: xstate_offset[51]: 24384, xstate_sizes[51]: 1024
[ 0.000000] x86/fpu: xstate_offset[52]: 24904, xstate_sizes[52]: 1024
[ 0.000000] x86/fpu: xstate_offset[53]: 25424, xstate_sizes[53]: 1024
[ 0.000000] x86/fpu: xstate_offset[54]: 25944, xstate_sizes[54]: 1024
[ 0.000000] x86/fpu: xstate_offset[55]: 26464, xstate_sizes[55]: 1024
[ 0.000000] x86/fpu: xstate_offset[56]: 26984, xstate_sizes[56]: 1024
[ 0.000000] x86/fpu: xstate_offset[57]: 27504, xstate_sizes[57]: 1024
[ 0.000000] x86/fpu: xstate_offset[58]: 27024, xstate_sizes[58]: 1024
[ 0.000000] x86/fpu: xstate_offset[59]: 27544, xstate_sizes[59]: 1024
[ 0.000000] x86/fpu: xstate_offset[60]: 28064, xstate_sizes[60]: 1024
[ 0.000000] x86/fpu: xstate_offset[61]: 28584, xstate_sizes[61]: 1024
[ 0.000000] x86/fpu: xstate_offset[62]: 29104, xstate_sizes[62]: 1024
[ 0.000000] x86/fpu: xstate_offset[63]: 29624, xstate_sizes[63]: 1024
[ 0.000000] x86/fpu: xstate_offset[64]: 30144, xstate_sizes[64]: 1024
[ 0.000000] x86/fpu: xstate_offset[65]: 30664, xstate_sizes[65]: 1024
[ 0.000000] x86/fpu: xstate_offset[66]: 31184, xstate_sizes[66]: 1024
[ 0.000000] x86/fpu: xstate_offset[67]: 31704, xstate_sizes[67]: 1024
[ 0.000000] x86/fpu: xstate_offset[68]: 32224, xstate_sizes[68]: 1024
[ 0.000000] x86/fpu: xstate_offset[69]: 32744, xstate_sizes[69]: 1024
[ 0.000000] x86/fpu: xstate_offset[70]: 33264, xstate_sizes[70]: 1024
[ 0.000000] x86/fpu: xstate_offset[71]: 33784, xstate_sizes[71]: 1024
[ 0.000000] x86/fpu: xstate_offset[72]: 34304, xstate_sizes[72]: 1024
[ 0.000000] x86/fpu: xstate_offset[73]: 34824, xstate_sizes[73]: 1024
[ 0.000000] x86/fpu: xstate_offset[74]: 35344, xstate_sizes[74]: 1024
[ 0.000000] x86/fpu: xstate_offset[75]: 35864, xstate_sizes[75]: 1024
[ 0.000000] x86/fpu: xstate_offset[76]: 36384, xstate_sizes[76]: 1024
[ 0.000000] x86/fpu: xstate_offset[77]: 36904, xstate_sizes[77]: 1024
[ 0.000000] x86/fpu: xstate_offset[78]: 37424, xstate_sizes[78]: 1024
[ 0.000000] x86/fpu: xstate_offset[79]: 37944, xstate_sizes[79]: 1024
[ 0.000000] x86/fpu: xstate_offset[80]: 38464, xstate_sizes[80]: 1024
[ 0.000000] x86/fpu: xstate_offset[81]: 38984, xstate_sizes[81]: 1024
[ 0.000000] x86/fpu: xstate_offset[82]: 39504, xstate_sizes[82]: 1024
[ 0.000000] x86/fpu: xstate_offset[83]: 40024, xstate_sizes[83]: 1024
[ 0.000000] x86/fpu: xstate_offset[84]: 40544, xstate_sizes[84]: 1024
[ 0.000000] x86/fpu: xstate_offset[85]: 41064, xstate_sizes[85]: 1024
[ 0.000000] x86/fpu: xstate_offset[86]: 41584, xstate_sizes[86]: 1024
[ 0.000000] x86/fpu: xstate_offset[87]: 42104, xstate_sizes[87]: 1024
[ 0.000000] x86/fpu: xstate_offset[88]: 42624, xstate_sizes[88]: 1024
[ 0.000000] x86/fpu: xstate_offset[89]: 43144, xstate_sizes[89]: 1024
[ 0.000000] x86/fpu: xstate_offset[90]: 43664, xstate_sizes[90]: 1024
[ 0.000000] x86/fpu: xstate_offset[91]: 44184, xstate_sizes[91]: 1024
[ 0.000000] x86/fpu: xstate_offset[92]: 44704, xstate_sizes[92]: 1024
[ 0.000000] x86/fpu: xstate_offset[93]: 45224, xstate_sizes[93]: 1024
[ 0.000000] x86/fpu: xstate_offset[94]: 45744, xstate_sizes[94]: 1024
[ 0.000000] x86/fpu: xstate_offset[95]: 46264, xstate_sizes[95]: 1024
[ 0.000000] x86/fpu: xstate_offset[96]: 46784, xstate_sizes[96]: 1024
[ 0.000000] x86/fpu: xstate_offset[97]: 47304, xstate_sizes[97]: 1024
[ 0.000000] x86/fpu: xstate_offset[98]: 47824, xstate_sizes[98]: 1024
[ 0.000000] x86/fpu: xstate_offset[99]: 48344, xstate_sizes[99]: 1024
[ 0.000000] x86/fpu: xstate_offset[100]: 48864, xstate_sizes[100]: 1024
[ 0.000000] x86/fpu: xstate_offset[101]: 49384, xstate_sizes[101]: 1024
[ 0.000000] x86/fpu: xstate_offset[102]: 49904, xstate_sizes[102]: 1024
[ 0.000000] x86/fpu: xstate_offset[103]: 50424, xstate_sizes[103]: 1024
[ 0.000000] x86/fpu: xstate_offset[104]: 50944, xstate_sizes[104]: 1024
[ 0.000000] x86/fpu: xstate_offset[105]: 51464, xstate_sizes[105]: 1024
[ 0.000000] x86/fpu: xstate_offset[106]: 51984, xstate_sizes[106]: 1024
[ 0.000000] x86/fpu: xstate_offset[107]: 52504, xstate_sizes[107]: 1024
[ 0.000000] x86/fpu: xstate_offset[108]: 53024, xstate_sizes[108]: 1024
[ 0.000000] x86/fpu: xstate_offset[109]: 53544, xstate_sizes[109]: 1024
[ 0.000000] x86/fpu: xstate_offset[110]: 54064, xstate_sizes[110]: 1024
[ 0.000000] x86/fpu: xstate_offset[111]: 54584, xstate_sizes[111]: 1024
[ 0.000000] x86/fpu: xstate_offset[112]: 55104, xstate_sizes[112]: 1024
[ 0.000000] x86/fpu: xstate_offset[113]: 55624, xstate_sizes[113]: 1024
[ 0.000000] x86/fpu: xstate_offset[114]: 56144, xstate_sizes[114]: 1024
[ 0.000000] x86/fpu: xstate_offset[115]: 56664, xstate_sizes[115]: 1024
[ 0.000000] x86/fpu: xstate_offset[116]: 57184, xstate_sizes[116]: 1024
[ 0.000000] x86/fpu: xstate_offset[117]: 57704, xstate_sizes[117]: 1024
[ 0.000000] x86/fpu: xstate_offset[118]: 58224, xstate_sizes[118]: 1024
[ 0.000000] x86/fpu: xstate_offset[119]: 58744, xstate_sizes[119]: 1024
[ 0.000000] x86/fpu: xstate_offset[120]: 59264, xstate_sizes[120]: 1024
[ 0.000000] x86/fpu: xstate_offset[121]: 59784, xstate_sizes[121]: 1024
[ 0.000000] x86/fpu: xstate_offset[122]: 60304, xstate_sizes[122]: 1024
[ 0.000000] x86/fpu: xstate_offset[123]: 60824, xstate_sizes[123]: 1024
[ 0.000000] x86/fpu: xstate_offset[124]: 61344, xstate_sizes[124]: 1024
[ 0.000000] x86/fpu: xstate_offset[125]: 61864, xstate_sizes[125]: 1024
[ 0.000000] x86/fpu: xstate_offset[126]: 62384, xstate_sizes[126]: 1024
[ 0.000000] x86/fpu: xstate_offset[127]: 62904, xstate_sizes[127]: 1024
[ 0.000000] x86/fpu: xstate_offset[128]: 63424, xstate_sizes[128]: 1024
[ 0.000000] x86/fpu: xstate_offset[129]: 63944, xstate_sizes[129]: 1024
[ 0.000000] x86/fpu: xstate_offset[130]: 64464, xstate_sizes[130]: 1024
[ 0.000000] x86/fpu: xstate_offset[131]: 64984, xstate_sizes[131]: 1024
[ 0.000000] x86/fpu: xstate_offset[132]: 65504, xstate_sizes[132]: 1024
[ 0.000000] x86/fpu: xstate_offset[133]: 66024, xstate_sizes[133]: 1024
[ 0.000000] x86/fpu: xstate_offset[134]: 66544, xstate_sizes[134]: 1024
[ 0.000000] x86/fpu: xstate_offset[135]: 67064, xstate_sizes[135]: 1024
[ 0.000000] x86/fpu: xstate_offset[136]: 67584, xstate_sizes[136]: 1024
[ 0.000000] x86/fpu: xstate_offset[137]: 68104, xstate_sizes[137]: 1024
[ 0.000000] x86/fpu: xstate_offset[138]: 68624, xstate_sizes[138]: 1024
[ 0.000000] x86/fpu: xstate_offset[139]: 69144, xstate_sizes[139]: 1024
[ 0.000000] x86/fpu: xstate_offset[140]: 69664, xstate_sizes[140]: 1024
[ 0.000000] x86/fpu: xstate_offset[141]: 70184, xstate_sizes[141]: 1024
[ 0.000000] x86/fpu: xstate_offset[142]: 70704, xstate_sizes[142]: 1024
[ 0.000000] x86/fpu: xstate_offset[143]: 71224, xstate_sizes[143]: 1024
[ 0.000000] x86/fpu: xstate_offset[144]: 71744, xstate_sizes[144]: 1024
[ 0.000000] x86/fpu: xstate_offset[145]: 72264, xstate_sizes[145]: 1024
[ 0.000000] x86/fpu: xstate_offset[146]: 72784, xstate_sizes[146]: 1024
[ 0.000000] x86/fpu: xstate_offset[147]: 73304, xstate_sizes[147]: 1024
[ 0.000000] x86/fpu: xstate_offset[148]: 73824, xstate_sizes[148]: 1024
[ 0.000000] x86/fpu: xstate_offset[149]: 74344, xstate_sizes[149]: 1024
[ 0.000000] x86/fpu: xstate_offset[150]: 74864, xstate_sizes[150]: 1024
[ 0.000000] x86/fpu: xstate_offset[151]: 75384, xstate_sizes[151]: 1024
[ 0.000000] x86/fpu: xstate_offset[152]: 75904, xstate_sizes[152]: 1024
[ 0.000000] x86/fpu: xstate_offset[153]: 76424, xstate_sizes[153]: 1024
[ 0.000000] x86/fpu: xstate_offset[154]: 76944, xstate_sizes[154]: 1024
[ 0.000000] x86/fpu: xstate_offset[155]: 77464, xstate_sizes[155]: 1024
[ 0.000000] x86/fpu: xstate_offset[156]: 77984, xstate_sizes[156]: 1024
[ 0.000000] x86/fpu: xstate_offset[157]: 78504, xstate_sizes[157]: 1024
[ 0.000000] x86/fpu: xstate_offset[158]: 79024, xstate_sizes[158]: 1024
[ 0.000000] x86/fpu: xstate_offset[159]: 79544, xstate_sizes[159]: 1024
[ 0.000000] x86/fpu: xstate_offset[160]: 80064, xstate_sizes[160]: 1024
[ 0.000000] x86/fpu: xstate_offset[161]: 80584, xstate_sizes[161]: 1024
[ 0.000000] x86/fpu: xstate_offset[162]: 81104, xstate_sizes[162]: 1024
[ 0.000000] x86/fpu: xstate_offset[163]: 81624, xstate_sizes[163]: 1024
[ 0.000000] x86/fpu: xstate_offset[164]: 82144, xstate_sizes[164]: 1024
[ 0.000000] x86/fpu: xstate_offset[165]: 82664, xstate_sizes[165]: 1024
[ 0.000000] x86/fpu: xstate_offset[166]: 83184, xstate_sizes[166]: 1024
[ 0.000000] x86/fpu: xstate_offset[167]: 83704, xstate_sizes[167]: 1024
[ 0.000000] x86/fpu: xstate_offset[168]: 84224, xstate_sizes[168]: 1024
[ 0.000000] x86/fpu: xstate_offset[169]: 84744, xstate_sizes[169]: 1024
[ 0.000000] x86/fpu: xstate_offset[170]: 85264, xstate_sizes[170]: 1024
[ 0.000000] x86/fpu: xstate_offset[171]: 85784, xstate_sizes[171]: 1024
[ 0.000000] x86/fpu: xstate_offset[172]: 86304, xstate_sizes[172]: 1024
[ 0.000000] x86/fpu: xstate_offset[173]: 86824, xstate_sizes[173]: 1024
[ 0.000000] x86/fpu: xstate_offset[174]: 87344, xstate_sizes[174]: 1024
[ 0.000000] x86/fpu: xstate_offset[175]: 87864, xstate_sizes[175]: 1024
[ 0.000000] x86/fpu: xstate_offset[176]: 88384, xstate_sizes[176]: 1024
[ 0.000000] x86/fpu: xstate_offset[177]: 88904, xstate_sizes[177]: 1024
[ 0.000000] x86/fpu: xstate_offset[178]: 89424, xstate_sizes[178]: 1024
[ 0.000000] x86/fpu: xstate_offset[179]: 89944, xstate_sizes[179]: 1024
[ 0.000000] x86/fpu: xstate_offset[180]: 90464, xstate_sizes[180]: 1024
[ 0.000000] x86/fpu: xstate_offset[181]: 90984, xstate_sizes[181]: 1024
[ 0.000000] x86/fpu: xstate_offset[182]: 91504, xstate_sizes[182]: 1024
[ 0.000000] x86/fpu: xstate_offset[183]: 917  loading out-of-tree module taints kernel.
[ 0.000000] x86/fpu: module verification failed: signature and/or required key missing - tainting kernel
[ 0.000000] 750.291555 Hello World!
```

To clear the above messages we are going to use

“**`sudo dmesg --clear`**”

```
[11:30:27.721] Hello world:  
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo dmesg --clear  
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ dmesg  
dmesg: read kernel buffer failed: Operation not permitted  
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo dmesg  
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$  
  
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg --clear  
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ dmesg  
dmesg: read kernel buffer failed: Operation not permitted  
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg  
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$
```

To show the message in real time we use “**`sudo dmesg -k -e`**”

```
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg  
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ dmesg -k -e  
dmesg: read kernel buffer failed: Operation not permitted  
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg -k -e  
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ █  
  
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ dmesg -k -w  
dmesg: read kernel buffer failed: Operation not permitted  
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg -k -w
```

Now lets insert our module

In the 2nd tab we use

By typing dmesg we are able to see the current modules inside the kernel

```
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg --kernel
[ 3360.308914] hello: loading out-of-tree module taints kernel.
[ 3360.308948] hello: module verification failed: signature and/or required key missing - tainting kernel
[ 3360.309076] Hello World!
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg
[ 3360.308914] hello: loading out-of-tree module taints kernel.
[ 3360.308948] hello: module verification failed: signature and/or required key missing - tainting kernel
[ 3360.309076] Hello World!
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg --clear
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmseg
sudo: dmseg: command not found
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ dmesg --version
dmseg from util-linux 2.34
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ dmesg --reltime
dmesg: read kernel buffer failed: Operation not permitted
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg --kernel
[ 3360.308914] hello: loading out-of-tree module taints kernel.
[ 3360.308948] hello: module verification failed: signature and/or required key missing - tainting kernel
[ 3360.309076] Hello World!
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg
[ 3360.308914] hello: loading out-of-tree module taints kernel.
[ 3360.308948] hello: module verification failed: signature and/or required key missing - tainting kernel
[ 3360.309076] Hello World!
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg --clear
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmseg
sudo: dmseg: command not found
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ dmesg --version
dmseg from util-linux 2.34
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ dmesg --reltime
dmesg: read kernel buffer failed: Operation not permitted
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$
```

```
insmod: ERROR: could not insert module hello.ko: File exists
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo insmod hello.ko
insmod: ERROR: could not insert module hello.ko: File exists
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ lsmod | grep -i hello
hello           16384  0
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$
```

Now we need to use **lsmod** to find the hello model

We can see here hello model is in the list of the ls module.

To remove it we have used “**sudo rmmod hello**”, we get nothing from the list

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ lsmod | grep -i hello
hello           16384  0
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo rmmod hello
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ lsmod | grep -i hello
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg --kernel
[ 3360.308914] hello: loading out-of-tree module taints kernel.
[ 3360.308948] hello: module verification failed: signature and/or required key missing - tainting kernel
[ 3360.309076] Hello World!
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ sudo dmesg
[ 3360.308914] hello: loading out-of-tree module taints kernel.
[ 3360.308948] hello: module verification failed: signature and/or required key missing - tainting kernel
[ 3360.309076] Hello World!
```

When we remove the model we see the “Bye-bye World” information, printed into the kernel buffer.

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo dmesg --kernel
[ 1794.118767] Bye-bye World!
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo dmesg -k -e
[Mar31 01:46] Bye-bye World!
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$
```

This is how we compare, insert list and remove kernel module and check the messages printed into the kernel buffer.

If you want to develop drivers for hardware for linux, you need to know kernel development this just show you a very simple example.

Here it explains the so called make file and tell you how to insert it and how to list it, how to remove it, how to check the messages demonstrated, we can also use “modinfo” to show the information about the linux kernel module.

Since the hello kernel module is removed we can check the other modules.

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ modinfo video
filename: /lib/modules/5.15.0-1033-aws/kernel/drivers/acpi/video.ko
license: GPL
description: ACPI Video Driver
author: Bruno Ducrot
srcversion: 3FB8E0D0EEBEB51FE3059225
alias: acpi*:LNXVIDEO:*
depends:
retpoline: Y
intree: Y
name: video
vermagic: 5.15.0-1033-aws SMP mod_unload modversions
sig_id: PKCS#7
signer: Build time autogenerated kernel key
sig_key: 39:89:97:37:A4:55:14:5A:B2:BD:8C:99:D4:2A:D0:23:4D:D5:63:50
sig_hashalgo: sha512
signature: 70:F1:6B:83:2A:23:49:2F:5F:2E:C2:8F:5A:60:A3:5B:10:14:63:6C:
65:0C:9B:59:94:A4:D4:F8:94:9D:1D:1E:3B:D0:2E:D7:51:6C:7F:67:
41:ED:BB:C5:54:09:9E:5C:2E:17:C3:C7:81:20:10:52:BD:4D:9F:D2:
EB:C4:B7:88:37:B4:73:93:35:AF:C7:B3:E1:00:FF:80:BE:21:81:A9:
46:5C:97:81:7E:72:78:23:82:43:13:F8:E1:5A:12:B2:1A:E3:E1:CA:
41:91:B3:D6:F3:A9:5E:BC:6C:F4:75:FA:1C:DE:F0:9C:94:A0:BB:D8:
D0:A8:02:1F:D1:93:8B:89:82:EF:40:F7:AF:57:D0:FE:F4:C2:6B:BF:
F3:90:EA:DD:7F:C4:3A:DA:D2:BE:A8:25:F3:57:03:CE:B2:0C:46:52:
F6:66:5B:B6:36:E4:BE:75:F7:37:5E:B0:CF:08:C6:6D:E8:A5:77:86:
47:5A:93:EF:8D:73:6B:FA:3E:EF:07:2C:A0:EF:A2:A7:8B:78:C2:BC:
0B:8C:ED:6B:2F:30:D2:50:73:26:B7:B1:34:0B:EC:B5:17:18:98:D2:
6A:48:2E:43:63:F5:49:F6:4B:65:1E:1F:18:30:C3:DF:26:17:1B:B0:
D0:33:73:03:04:47:61:7A:AB:CD:0B:EE:AE:0A:11:3B:64:0C:EN:0B:
```

We can see the information for the video module. In the below image we are able to see the filename, location, license cpr description, the video driver.

So to develop like these a video driver, we need a lots of knowledge.

How to design parameters for kernel module in linux kind of programming(We can find detail information from the guide in github “ The Linux Kernel Module Programming guide”)

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo insmod hello.ko
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ modinfo hello.ko
filename: /home/seed/Internet_Security/Lab6/Labsetup/Files/kernel_module/hello.ko
license: GPL
srcversion: 717A72281ACFAA8385B33A8
depends:
retpoline: Y
name: hello
vermagic: 5.15.0-1033-aws SMP mod_unload modversions
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ modelinfo hello.ko -n
modelinfo: command not found
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ modelinfo hello -n
modelinfo: command not found
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ modeinfo hello.ko

Command 'modeinfo' not found, did you mean:

  command 'modinfo' from deb kmod (27-lubuntu2.1)

Try: apt install <deb name>

seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ modinfo hello.ko
filename:      /home/seed/Internet_Security/Lab-06/Labsetup/Files/kernel_module/hello.ko
license:       GPL
srcversion:    717A72281ACFAA8385B33A8
depends:
retpoline:     Y
name:          hello
vermagic:      5.15.0-1031-aws SMP mod_unload modversions
seed@ip-172-31-44-212:~/Internet_Security/Lab-06/Labsetup/Files/kernel_module$ █
```

Task 1.B Implement a Simple firewall using Netfilter

Subtask-1

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ cd ..
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files$ ls
kernel_module packet_filter
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files$ cd packet_filter/
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ cd ..
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files$ ls
kernel_module packet_filter
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files$ cd packet_filter/
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ ls
Makefile seedFilter.c
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ gedit * &
[1] 3912
```

There are two hooks we need to initialize the hook

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/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=110 time=10.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=10.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=10.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=10.8 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 10.803/10.841/10.911/0.042 ms
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ ls
Makefile seedFilter.c
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ make
make -C /lib/modules/5.15.0-1033-aws/build M=/home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-1033-aws'
  CC [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.o
  MODPOST /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/Module.symvers
  CC [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.mod.o
  LD [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.ko
  BTF [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.ko
Skipping BTF generation for /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.ko due to unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-1033-aws'
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$
```

Here the kernel module is generated

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ make
make -C /lib/modules/5.15.0-1033-aws/build M=/home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-1033-aws'
  CC [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.o
  MODPOST /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/Module.symvers
  CC [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.mod.o
  LD [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.ko
  BTF [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.ko
Skipping BTF generation for /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.ko due to unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-1033-aws'
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ ls
Makefile Module.symvers modules.order seedFilter.c seedFilter.ko seedFilter.mod seedFilter.mod.c seedFilter.mod.o seedFilter.o
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$
```

Above kernel module is generated

```

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ make
make -C /lib/modules/5.15.0-1033-aws/build M=/home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-1033-aws'
  CC [M]  /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.o
  MODPOST /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/Module.symvers
  CC [M]  /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.mod.o
  LD [M]  /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.ko
  BTF [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.ko
Skipped BTF generation for /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.ko due to unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-1033-aws'
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ ls
Makefile Module.symvers modules.order seedFilter.o seedFilter.mod seedFilter.mod.c seedFilter.mod.o seedFilter.o
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ sudo insmod seedFilter.ko
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ lsmod | grep -i seed
seedFilter           16384  0
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$
```

```

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo dmesg -k -w
[ 1794.118767] Bye-bye World!
[ 2159.338373] Hello World!
[ 4053.829387] Registering filters.
[ 4053.858450] *** LOCAL_OUT
[ 4053.858454]    172.31.44.212 --> 71.176.66.85 (TCP)
[ 4053.858478] *** LOCAL_OUT
[ 4053.858479]    172.31.44.212 --> 71.176.66.85 (TCP)
[ 4053.858507] *** LOCAL_OUT
[ 4053.858507]    172.31.44.212 --> 71.176.66.85 (TCP)
[ 4053.858756] *** LOCAL_OUT
[ 4053.858757] *** LOCAL_OUT
[ 4053.858761] *** LOCAL_OUT
[ 4053.858762] *** LOCAL_OUT
[ 4053.897413] *** LOCAL_OUT
[ 4053.897417] *** LOCAL_OUT
[ 4053.897433] *** LOCAL_OUT
[ 4053.897434]    172.31.44.212 --> 71.176.66.85 (TCP)
```

```

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo dmesg -k -w
[ 1794.118767] Bye-bye World!
[ 2159.338373] Hello World!
[ 4053.829387] Registering filters.
```

We are able to see hook information, prototype udp and IP address for source to destination and the hook where it is hooked and which hook it has triggered.

We are getting as timeout when we try to dig because it's opened by our filter

```

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ 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: 41794
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.com.  20833   IN      A      93.184.216.34

;; Query time: 12 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Mar 31 02:19:39 UTC 2023
;; MSG SIZE rcvd: 60

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ 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

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$
```

We want to see that the dig was dropped, that the dna's credit was dropped

```
[ 4728.406355]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4728.447819] *** LOCAL_OUT
[ 4728.447823]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4728.447886] *** LOCAL_OUT
[ 4728.447890]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4728.484296] *** LOCAL_OUT
[ 4728.484301]    172.31.44.212  --> 8.8.8.8 (UDP)
[ 4728.484312] *** Dropping 8.8.8.8 (UDP), port 53
[ 4728.488400] *** LOCAL_OUT
[ 4728.488403]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4728.536241] *** LOCAL_OUT
[ 4728.536245]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4728.575240] *** LOCAL_OUT
[ 4728.575243]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4728.611115] *** LOCAL_OUT
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo dmesg -k -w
[ 4835.483363] *** LOCAL_OUT
[ 4835.483364]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4835.483377] *** LOCAL_OUT
[ 4835.483378]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4835.498836] *** LOCAL_OUT
[ 4835.498839]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4835.499281] *** LOCAL_OUT
[ 4835.499283]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4835.499339] *** LOCAL_OUT
[ 4835.499340]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4835.499497] *** LOCAL_OUT
[ 4835.499497]    172.31.44.212  --> 71.176.66.85 (TCP)

[ 4723.480862]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4723.481016] *** LOCAL_OUT
[ 4723.481017]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4723.481084] *** LOCAL_OUT
[ 4723.481085]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4723.481154] *** LOCAL_OUT
[ 4723.481155]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4723.484469] *** LOCAL_OUT
[ 4723.484472]    172.31.44.212  --> 8.8.8.8 (UDP)
[ 4723.484486] *** Dropping 8.8.8.8 (UDP), port 53
[ 4723.486384] *** LOCAL_OUT
[ 4723.486386]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4723.486565] *** LOCAL_OUT
[ 4723.486566]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4723.486611] *** LOCAL_OUT
[ 4723.486612]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 4723.491159] *** LOCAL_OUT
[ 4723.491162]    172.31.44.212  --> 71.176.66.85 (TCP)
```

We are able to see the packets which are dropped for number 53

Let's remove the module, in remote we can see the message

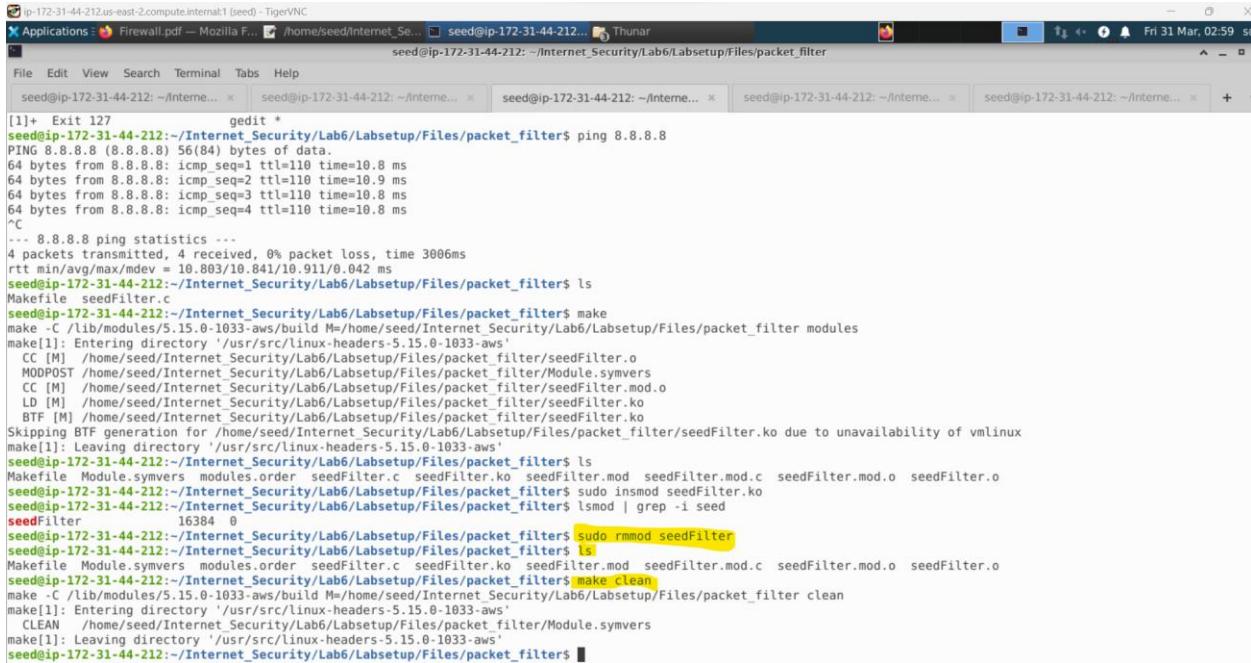
```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo dmesg -k -w
[ 5268.746650] *** LOCAL_OUT
[ 5268.746653]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 5268.771662] *** LOCAL_OUT
[ 5268.771666]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 5268.775191] *** LOCAL_OUT
[ 5268.775195]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 5268.775257] *** LOCAL_OUT
[ 5268.775258]    172.31.44.212  --> 71.176.66.85 (TCP)
[ 5268.775268] *** LOCAL_OUT
[ 5268.775269]    172.31.44.212  --> 71.176.66.85 (TCP)
```

```
[ 5655.001832] *** LOCAL_OUT
[ 5655.001834]    127.0.0.1 --> 127.0.0.53 (UDP)
[ 5655.002064] *** LOCAL_OUT
[ 5655.002065]    172.31.44.212 --> 172.31.0.2 (UDP)
[ 5655.002154] *** LOCAL_OUT
[ 5655.002155]    172.31.44.212 --> 172.31.0.2 (UDP)
[ 5655.003052] *** LOCAL_OUT
[ 5655.003054]    127.0.0.53 --> 127.0.0.1 (UDP)
[ 5655.003113] *** LOCAL_OUT
[ 5655.003115]    127.0.0.53 --> 127.0.0.1 (UDP)
[ 5655.011933] The filters are being removed.
```

Subtask-2

Here we need to modify the seedFilter

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ sudo rmmod seedFilter
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ ls
Makefile Module.symvers modules.order seedFilter.c seedFilter.ko seedFilter.mod seedFilter.mod.c seedFilter.mod.o seedFilter.o
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ make clean
make -C /lib/modules/5.15.0-1033-aws/build M=/home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter clean
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-1033-aws'
  CLEAN  /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-1033-aws'
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$
```



```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/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=110 time=10.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=10.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=10.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=10.8 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 10.803/10.841/10.911/0.042 ms
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ ls
Makefile seedFilter.c
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ make
make -C /lib/modules/5.15.0-1033-aws/build M=/home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-1033-aws'
  CC [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.o
  MODPOST /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/Module.symvers
  CC [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter/mod.o
  LD [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.ko
  BTF [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.ko
Skipping BTF generation for /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedFilter.ko due to unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-1033-aws'
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ ls
Makefile Module.symvers modules.order seedFilter.c seedFilter.ko seedFilter.mod seedFilter.mod.c seedFilter.mod.o seedFilter.o
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filters$ sudo insmod seedFilter.ko
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filters$ lsmod | grep -i seed
seedFilter           16384  0
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filters$ sudo rmmod seedFilter
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filters$ ls
Makefile Module.symvers modules.order seedFilter.c seedFilter.ko seedFilter.mod seedFilter.mod.c seedFilter.mod.o seedFilter.o
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filters$ make clean
make -C /lib/modules/5.15.0-1033-aws/build M=/home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter clean
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-1033-aws'
  CLEAN  /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-1033-aws'
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filters$
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filters$ sudo rmmod seedFilter
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filters$ ls
Makefile Module.symvers modules.order seedFilter.c seedFilter.ko seedFilter.mod seedFilter.mod.c seedFilter.mod.o seedFilter.o
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filters$ make clean
make -C /lib/modules/5.15.0-1033-aws/build M=/home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter clean
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-1033-aws'
  CLEAN  /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-1033-aws'
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filters$ make clean
make -C /lib/modules/5.15.0-1033-aws/build M=/home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter clean
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-1033-aws'
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-1033-aws'
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filters$
```

We can use the seedFilter as our Template

```
#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;

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] = "8.8.8.8";
    u32 ip_addr;

    if (!skb) return NF_ACCEPT;

    iph = ip_hdr(skb);
```

MakeFile:-



```
# obj-m += seedFilter.o
obj-m += seedPrint.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 total we need 5 hooks

These are the register features with register file focus



```
File Edit Search View Document Help
Makefile × seedFilter.c × seedPrint.c ×

nf_register_net_hook(&init_net, &hook1);

//NF_INET_LOCAL_IN
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);

//NF_INET_FORWARD
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);

//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;
}

void 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);
}

return 0;
}

void 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);
}
```

We need to unregister all the networks. Lets make seedPrint.ko

```
[11142.213615] *** POST_ROUTING
[11142.213616] 172.31.44.212 --> 71.176.66.85 (TCP)
[11142.213748] *** LOCAL_OUT
[11142.213750] 172.31.44.212 --> 71.176.66.85 (TCP)
[11142.213752] *** POST_ROUTING
[11142.213754] 172.31.44.212 --> 71.176.66.85 (TCP)
[11142.213924] *** LOCAL_OUT
[11142.213925] 172.31.44.212 --> 71.176.66.85 (TCP)
[11142.213928] *** POST_ROUTING
[11142.213929] 172.31.44.212 --> 71.176.66.85 (TCP)
[11142.213949] *** LOCAL_OUT
[11142.213950] 172.31.44.212 --> 71.176.66.85 (TCP)
[11142.213952] *** POST_ROUTING
[11142.213953] 172.31.44.212 --> 71.176.66.85 (TCP)
[11142.223761] *** PRE_ROUTING
[11142.223779] 71.176.66.85 --> 172.31.44.212 (TCP)
[11142.223790] *** PRE_ROUTING
[11142.223792] 71.176.66.85 --> 172.31.44.212 (TCP)
[11142.223801] *** LOCAL_IN
[11142.223802] 71.176.66.85 --> 172.31.44.212 (TCP)
[11142.223816] *** LOCAL_IN
[11142.223818] 71.176.66.85 --> 172.31.44.212 (TCP)
[11142.234090] *** LOCAL_OUT
[11142.234093] 172.31.44.212 --> 71.176.66.85 (TCP)
[11142.234101] *** POSTROUTING

[ 4723.480862] 172.31.44.212 --> 71.176.66.85 (TCP)
[ 4723.481016] *** LOCAL_OUT
[ 4723.481017] 172.31.44.212 --> 71.176.66.85 (TCP)
[ 4723.481084] *** LOCAL_OUT
[ 4723.481085] 172.31.44.212 --> 71.176.66.85 (TCP)
[ 4723.481154] *** LOCAL_OUT
[ 4723.481155] 172.31.44.212 --> 71.176.66.85 (TCP)
[ 4723.484469] *** LOCAL_OUT
[ 4723.484472] 172.31.44.212 --> 8.8.8.8 (UDP)
[ 4723.484486] *** Dropping 8.8.8.8 (UDP), port 53
[ 4723.486384] *** LOCAL_OUT
[ 4723.486386] 172.31.44.212 --> 71.176.66.85 (TCP)
[ 4723.486565] *** LOCAL_OUT
[ 4723.486566] 172.31.44.212 --> 71.176.66.85 (TCP)
[ 4723.486611] *** LOCAL_OUT
[ 4723.486612] 172.31.44.212 --> 71.176.66.85 (TCP)
[ 4723.491159] *** LOCAL_OUT
[ 4723.491162] 172.31.44.212 --> 71.176.66.85 (TCP)

[ 3112.842092] *** LOCAL_OUT
[ 3112.842094] 10.20.30.13 --> 54.192.121.83 (TCP)
[ 3112.852603] *** LOCAL_OUT
[ 3112.852615] 10.20.30.13 --> 54.192.121.83 (TCP)
[ 3130.642747] The filters are being removed.
[ 3726.258025] seedPrint: Registering filters.
```

```

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ make
make -C /lib/modules/5.15.0-1033-aws/build M=/home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-1033-aws'
  CC [M]  /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedPrint.o
  MODPOST /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/Module.symvers
  CC [M]  /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedPrint.mod.o
  LD [M]  /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedPrint.ko
  BTF [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedPrint.ko
Skipping BTF generation for /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/seedPrint.ko due to unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-1033-aws'
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ sudo insmod seedPrint.ko
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ sudo insmod seedPrint.ko
insmod: ERROR: could not insert module seedPrint.ko: File exists
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ sudo rmmod seedPrint
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ 

```

```

[11449.425536]      127.0.0.53  --> 127.0.0.1 (UDP)
[11449.450092] *** PRE_ROUTING
[11449.450095]    71.176.66.85  --> 172.31.44.212 (TCP)
[11449.450102] *** PRE_ROUTING
[11449.450103]    71.176.66.85  --> 172.31.44.212 (TCP)
[11449.450110] *** LOCAL_IN
[11449.450110]    71.176.66.85  --> 172.31.44.212 (TCP)
[11449.450122] *** LOCAL_IN
[11449.450123]    71.176.66.85  --> 172.31.44.212 (TCP)
[11449.450714] *** LOCAL_OUT
[11449.450716]    172.31.44.212  --> 71.176.66.85 (TCP)
[11449.450724] *** POST_ROUTING
[11449.450725]    172.31.44.212  --> 71.176.66.85 (TCP)
[11449.450739] seedPrint: The filters are being removed.

```

Subtask-3

To create a kernel module to hook into this netfilter to block just to attempt the ping and the ethernet

```

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firewall.pdf - Mozilla F... /home/seed/Internet_Sec... seed@ip-172-31-44-212 Thunar
File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ make
make -C /lib/modules/5.15.0-1033-aws/build M=/home/seed/Internet_Security/Lab6/Labsetup/Files/kernel_module modules
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-1033-aws'
  CC [M]  /home/seed/Internet_Security/Lab6/Labsetup/Files/kernel_module/kernel.o
  MODPOST /home/seed/Internet_Security/Lab6/Labsetup/Files/kernel_module/Module.symvers
  CC [M]  /home/seed/Internet_Security/Lab6/Labsetup/Files/kernel_module/kernel.mod.o
  LD [M]  /home/seed/Internet_Security/Lab6/Labsetup/Files/kernel_module/kernel.ko
  BTF [M] /home/seed/Internet_Security/Lab6/Labsetup/Files/kernel_module/kernel.ko
Skipping BTF generation for /home/seed/Internet_Security/Lab6/Labsetup/Files/kernel_module/kernel.ko due to unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-1033-aws'
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo insmod kernel.ko
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo insmod kernel.ko
insmod: ERROR: could not insert module kernel.ko: File exists
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ sudo rmmod kernel
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ 
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ dig @8.8.8.8 www.example.com
;; Query time: 12 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Mar 31 02:19:39 UTC 2023
;; MSG SIZE rcvd: 60
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ 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
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ 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: 63933
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 512
;; QUESTION SECTION:
;www.example.com.           IN      A
;; ANSWER SECTION:
www.example.com.        19362   IN      A      93.184.216.34
;; Query time: 12 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Mar 31 04:26:12 UTC 2023
;; MSG SIZE rcvd: 60
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ docksh hostA-10.9.0.5
root@6470af2d65:/#

```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ docksh hostA-10.9.0.5
root@86470afd2d65:/# 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=0.130 ms
64 bytes from 10.9.0.1: icmp_seq=2 ttl=64 time=0.089 ms
64 bytes from 10.9.0.1: icmp_seq=3 ttl=64 time=0.059 ms
64 bytes from 10.9.0.1: icmp_seq=4 ttl=64 time=0.055 ms
64 bytes from 10.9.0.1: icmp_seq=5 ttl=64 time=0.178 ms
^C
--- 10.9.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4076ms
rtt min/avg/max/mdev = 0.055/0.102/0.178/0.046 ms
root@86470afd2d65:/# telnet 10.9.0.1
Trying 10.9.0.1...
Connected to 10.9.0.1.
Escape character is '^]'.
Ubuntu 20.04.5 LTS
ip-172-31-44-212 login: seed
Password:

Login incorrect
ip-172-31-44-212 login: seed
Password:

Login incorrect
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ sudo insmod seedPrint.ko
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ sudo insmod seedPrint.ko
insmod: ERROR: could not insert module seedPrint.ko: File exists
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ sudo rmmod seedPrint
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filters ls
Makefile Module.symvers modules.order seedFilter.c seedPrint.c seedPrint.mod seedPrint.mod.c seedPrint.mod.o seedPrint.o
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ make clean
make -C /lib/modules/5.15.0-1033-aws/build M=/home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter clean
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-1033-aws'
  CLEAN  /home/seed/Internet_Security/Lab6/Labsetup/Files/packet_filter/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-1033-aws'
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ ls
Makefile seedFilter.c seedPrint.c
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ cp seedFilter.c seedBlock.c
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$
```

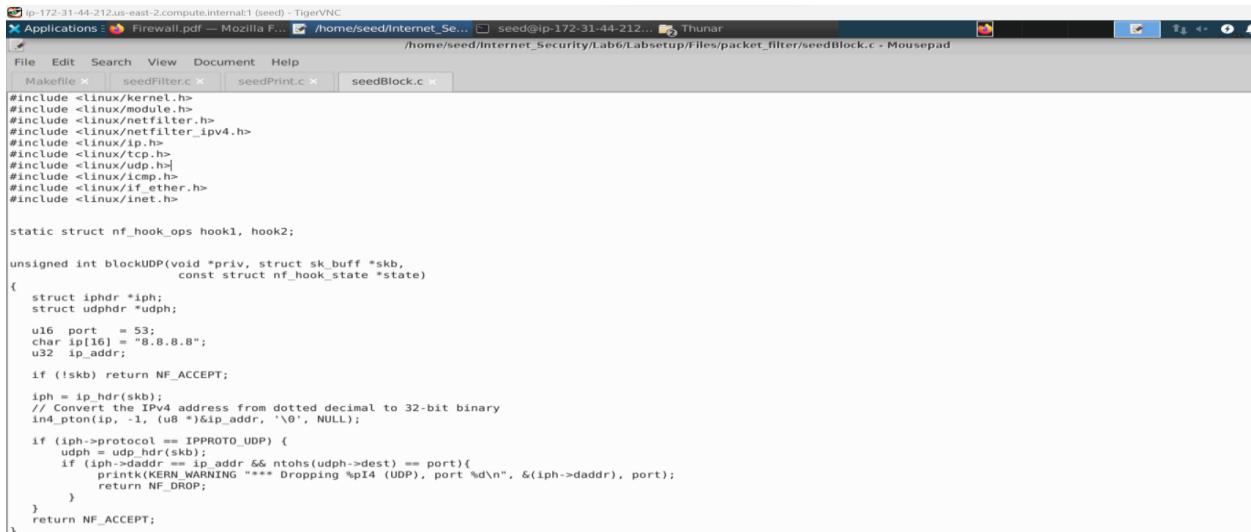
```
Login incorrect
ip-172-31-44-212 login:
Login timed out after 60 seconds.
Connection closed by foreign host.
root@86470afd2d65:/# telnet 10.9.0.1
Trying 10.9.0.1...
Connected to 10.9.0.1.
Escape character is '^]'.
Ubuntu 20.04.5 LTS
ip-172-31-44-212 login: seed
Password:

Login incorrect
ip-172-31-44-212 login: seed
Password:

Login incorrect
ip-172-31-44-212 login: seed
Password:

Login incorrect
ip-172-31-44-212 login:
Login timed out after 60 seconds.
Connection closed by foreign host.
root@86470afd2d65:/# telnet 10.9.0.1
Trying 10.9.0.1...
Connected to 10.9.0.1.
Escape character is '^]'.
Ubuntu 20.04.5 LTS
```

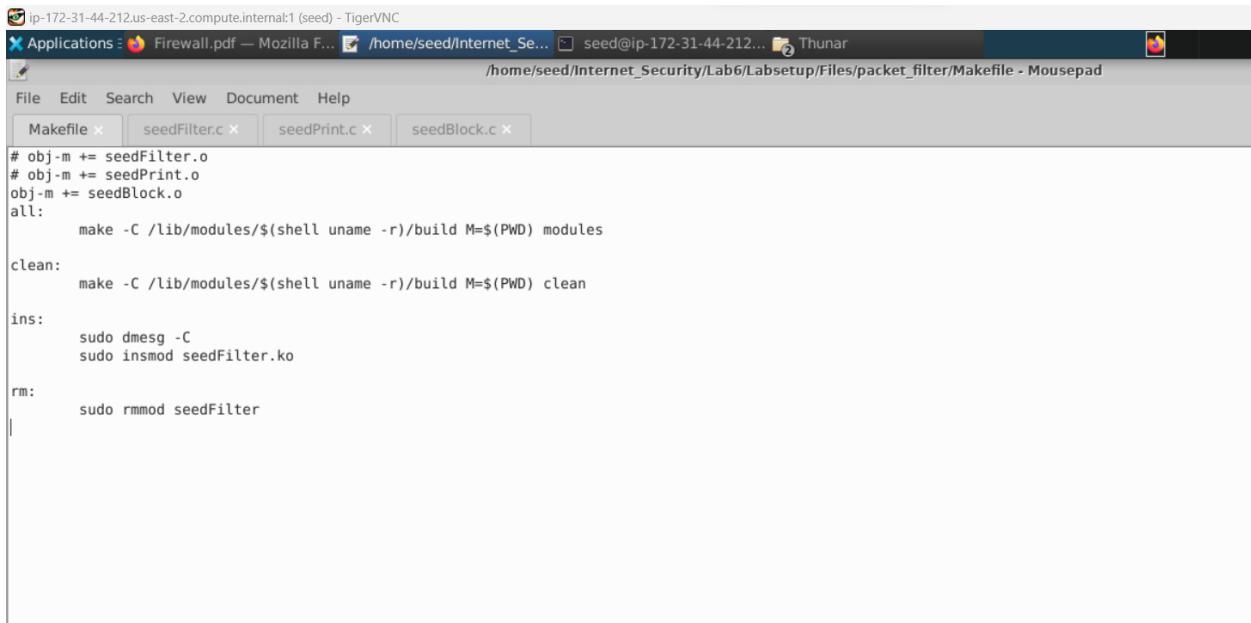
seedBlock.c



```
#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/if.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] = "8.8.8.8";
    u32 ip_addr;
    if (!skb) return NF_ACCEPT;
    ip = iph->dst;
    // 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;
        }
    }
    return NF_ACCEPT;
}
```



```
# 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
```

Task 1 is to block ping to our virtual machine

Now check the virtual machine IP address if it equals virtual machine IP address

Task-2 Experimenting with Stateless Firewall Rules

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ man iptables
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ iptables -t nat -L -n
Fatal: can't open lock file /run/xtables.lock: Permission denied
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ 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 L
OCALE

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 L
OCALE

Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
MASQUERADE all   --  172.17.0.0/16  0.0.0.0/0
MASQUERADE all   --  10.9.0.0/24   0.0.0.0/0
MASQUERADE all   --  192.168.60.0/24 0.0.0.0/0
MASQUERADE all   --  192.168.50.0/24 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
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ sudo iptables -t filter -L -n
--line-numbers
Chain INPUT (policy ACCEPT)
num target    prot opt source          destination

Chain FORWARD (policy DROP)
num target    prot opt source          destination
1  DOCKER-USER  all   --  0.0.0.0/0      0.0.0.0/0
2  DOCKER-ISOLATION-STAGE-1 all   --  0.0.0.0/0      0.0.0.0/0
3  ACCEPT     all   --  0.0.0.0/0      0.0.0.0/0          ctstate RELATED,ESTA
BLISHED
4  DOCKER     all   --  0.0.0.0/0      0.0.0.0/0
5  ACCEPT     all   --  0.0.0.0/0      0.0.0.0/0
6  ACCEPT     all   --  0.0.0.0/0      0.0.0.0/0
7  ACCEPT     all   --  0.0.0.0/0      0.0.0.0/0          ctstate RELATED,ESTA
```

```

File Edit View Search Terminal Help
14 ACCEPT all -- 0.0.0.0/0 0.0.0.0/0 ctstate RELATED,ESTA
15 ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
BLISHED
16 DOCKER all -- 0.0.0.0/0 0.0.0.0/0
17 ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
18 ACCEPT all -- 0.0.0.0/0 0.0.0.0/0

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

Chain DOCKER (4 references)
num target prot opt source destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
num target prot opt source destination
1 DOCKER-ISOLATION-STAGE-2 all -- 0.0.0.0/0 0.0.0.0/0
2 DOCKER-ISOLATION-STAGE-2 all -- 0.0.0.0/0 0.0.0.0/0
3 DOCKER-ISOLATION-STAGE-2 all -- 0.0.0.0/0 0.0.0.0/0
4 DOCKER-ISOLATION-STAGE-2 all -- 0.0.0.0/0 0.0.0.0/0
5 RETURN all -- 0.0.0.0/0 0.0.0.0/0

Chain DOCKER-ISOLATION-STAGE-2 (4 references)
num target prot opt source destination
1 DROP all -- 0.0.0.0/0 0.0.0.0/0
2 DROP all -- 0.0.0.0/0 0.0.0.0/0
3 DROP all -- 0.0.0.0/0 0.0.0.0/0
4 DROP all -- 0.0.0.0/0 0.0.0.0/0
5 RETURN all -- 0.0.0.0/0 0.0.0.0/0

Chain DOCKER-USER (1 references)
num target prot opt source destination
1 RETURN all -- 0.0.0.0/0 0.0.0.0/0
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ █

```

```

seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module
File Edit View Search Terminal Tabs Help
seed@ip... seed@ip... seed@ip... seed@ip... seed@ip... seed@ip...
Escape character is '^]'.
Ubuntu 20.04.5 LTS
ip-172-31-44-212 login: seed
Password:

Login incorrect
ip-172-31-44-212 login:
Login timed out after 60 seconds.
Connection closed by foreign host.
root@86470af2d65:/# telnet 10.9.0.1
Trying 10.9.0.1...
Connected to 10.9.0.1.
Escape character is '^]'.
Ubuntu 20.04.5 LTS
ip-172-31-44-212 login: seed
Password:

Login incorrect
ip-172-31-44-212 login:
Login timed out after 60 seconds.
Connection closed by foreign host.
root@86470af2d65:/# 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@86470af2d65:/# █

```

```

root@86470afd2d65:/# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
          prot opt source          destination

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

Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination
          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
          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
          prot opt source          destination
DNAT     tcp   --  0.0.0.0/0      127.0.0.11      tcp dpt:53 to:127.0.0.11:
44617


```

Task-2A Protecting the Router

As a router it has 2 ip addresses

```

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filters$ docksh seed-router
root@ad423d4610e:/# ip link
1: lo: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.0.0.1 scope host lo
        valid_lft forever preferred_lft forever
9: eth0@if10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:00:00:00:00 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.11 brd 10.9.0.255 scope global eth0
        valid_lft forever preferred_lft forever
17: eth1@if18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:ab:3c:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.11/24 brd 192.168.60.255 scope global eth1
        valid_lft forever preferred_lft forever
root@ad423d4610e:#

```

Use telnet to save as an example. The ping has worked how about we set an other interface

```

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ 
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... seed...
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ 
Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination
DOCKER_OUTPUT all  --  0.0.0.0/0      127.0.0.11

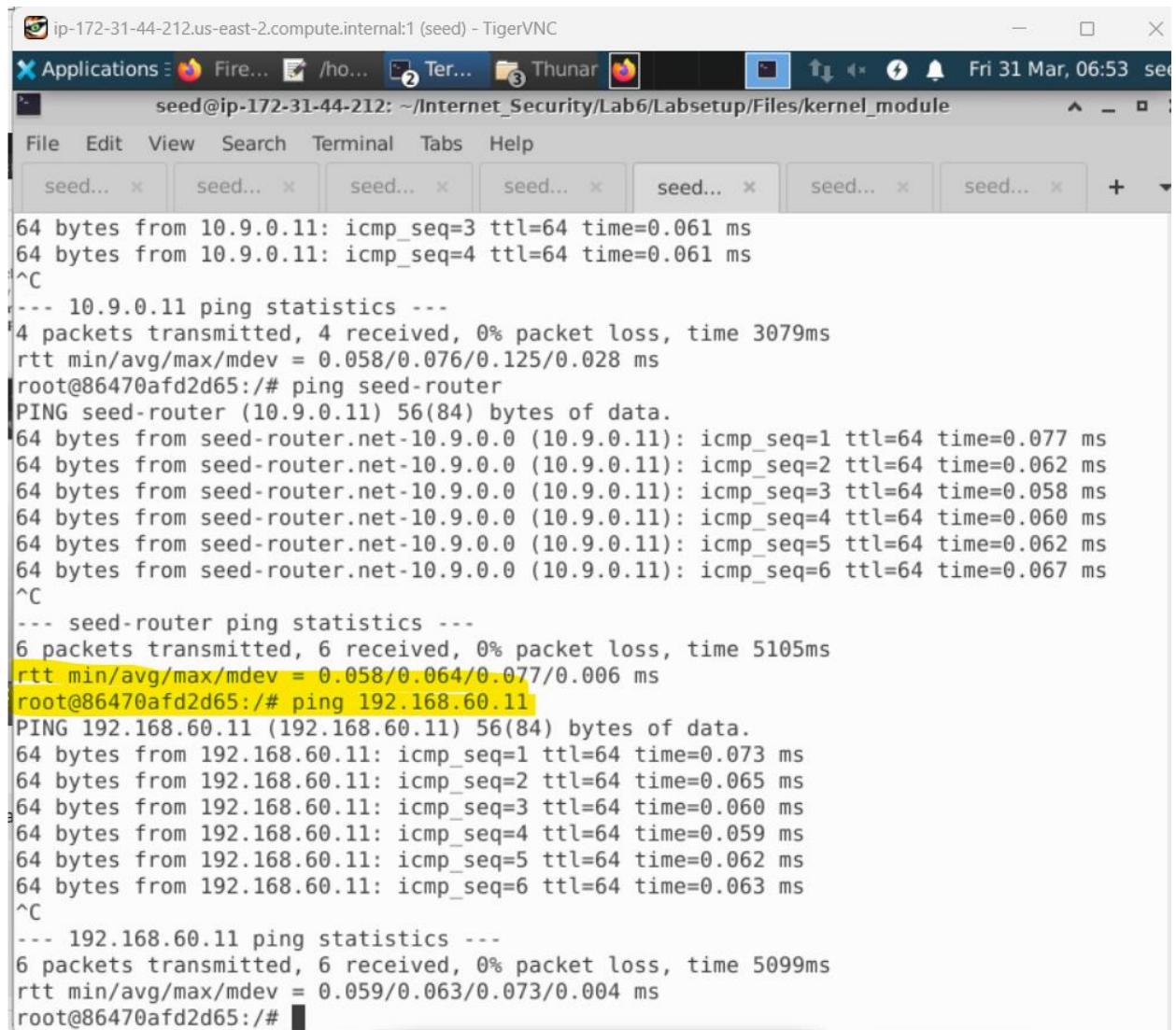
Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
DOCKER_POSTROUTING all  --  0.0.0.0/0      127.0.0.11

Chain DOCKER_OUTPUT (1 references)
target    prot opt source          destination
          prot opt source          destination
DNAT     tcp   --  0.0.0.0/0      127.0.0.11      tcp dpt:53 to:127.0.0.11:
44617
DNAT     udp   --  0.0.0.0/0      127.0.0.11      udp dpt:53 to:127.0.0.11:
35947

Chain DOCKER_POSTROUTING (1 references)
target    prot opt source          destination
          prot opt source          destination
SNAT     tcp   --  127.0.0.11      0.0.0.0/0      tcp spt:44617 to::53
SNAT     udp   --  127.0.0.11      0.0.0.0/0      udp spt:35947 to::53
root@86470afd2d65:/# 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=0.125 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.061 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.061 ms
^C
--- 10.9.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3079ms
rtt min/avg/max/mdev = 0.058/0.076/0.125/0.028 ms
root@86470afd2d65:/# 

```

```
root@86470afd2d65:/# ping seed-router
PING seed-router (10.9.0.11) 56(84) bytes of data.
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=1 ttl=64 time=0.077 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=2 ttl=64 time=0.062 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=3 ttl=64 time=0.058 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=4 ttl=64 time=0.060 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=5 ttl=64 time=0.062 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=6 ttl=64 time=0.067 ms
^C
--- seed-router ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5105ms
rtt min/avg/max/mdev = 0.058/0.064/0.077/0.006 ms
root@86470afd2d65:/#
```



The screenshot shows a TigerVNC session with multiple tabs open in the background. The active terminal window has the following details:

- Title bar: Applications, Fire..., /ho..., Terminal, Thunar, Fri 31 Mar, 06:53 seed
- Terminal title: seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module
- Terminal content:

```
File Edit View Search Terminal Tabs Help
seed... × + ×

64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.061 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.061 ms
^C
--- 10.9.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3079ms
rtt min/avg/max/mdev = 0.058/0.076/0.125/0.028 ms
root@86470afd2d65:/# ping seed-router
PING seed-router (10.9.0.11) 56(84) bytes of data.
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=1 ttl=64 time=0.077 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=2 ttl=64 time=0.062 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=3 ttl=64 time=0.058 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=4 ttl=64 time=0.060 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=5 ttl=64 time=0.062 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=6 ttl=64 time=0.067 ms
^C
--- seed-router ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5105ms
rtt min/avg/max/mdev = 0.058/0.064/0.077/0.006 ms
root@86470afd2d65:/# 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=0.073 ms
64 bytes from 192.168.60.11: icmp_seq=2 ttl=64 time=0.065 ms
64 bytes from 192.168.60.11: icmp_seq=3 ttl=64 time=0.060 ms
64 bytes from 192.168.60.11: icmp_seq=4 ttl=64 time=0.059 ms
64 bytes from 192.168.60.11: icmp_seq=5 ttl=64 time=0.062 ms
64 bytes from 192.168.60.11: icmp_seq=6 ttl=64 time=0.063 ms
^C
--- 192.168.60.11 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5099ms
rtt min/avg/max/mdev = 0.059/0.063/0.073/0.004 ms
root@86470afd2d65:/#
```

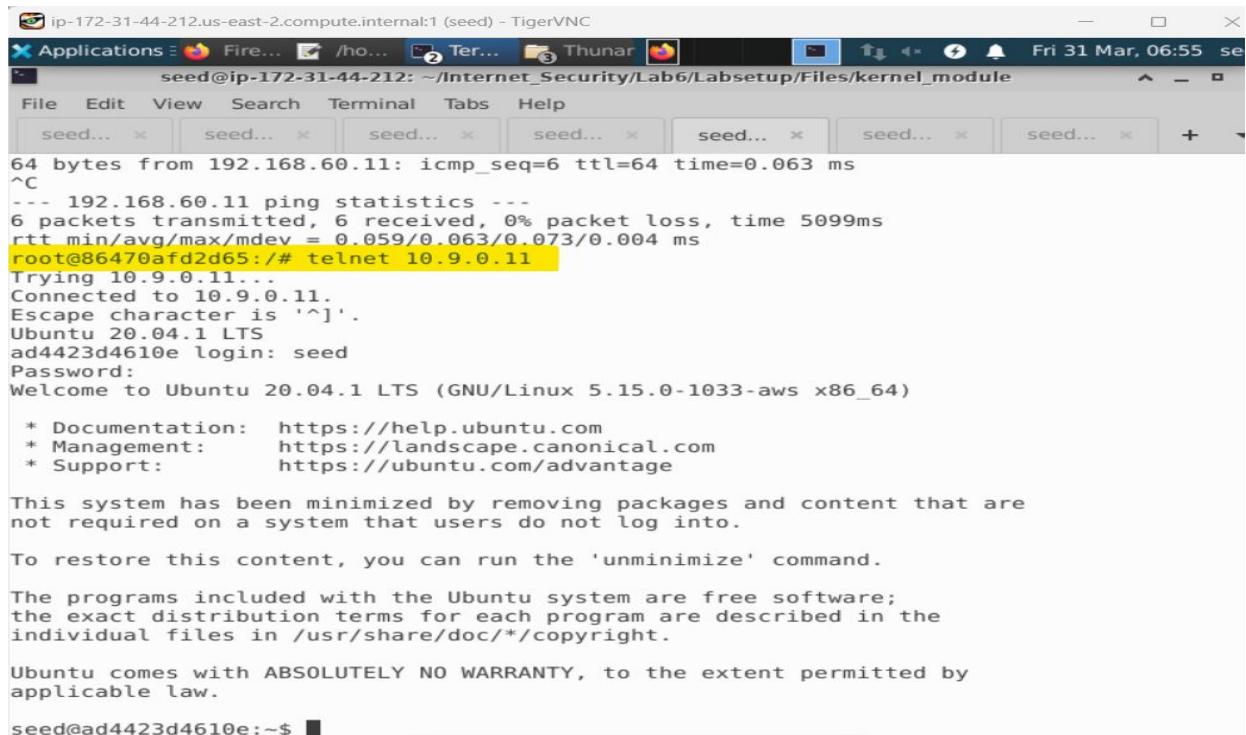
We can also use telnet to turn into this router

Before we run the active commands we can print it we can telnet it, now it asks us to execute those ip tips command and try it again by pinging and telnetting it.

Telnet service is running on all the containers, the core seat was created on them with the panel ds as I jus demonstrated

Report your observation and explain the problems of each row.

Here we need to setup these rows in the router inside the router



```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications   Fire...   /ho...   2 Ter...   3 Thunar   Fri 31 Mar, 06:55 seed...
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module
File Edit View Search Terminal Tabs Help
seed... × + ×
64 bytes from 192.168.60.11: icmp_seq=6 ttl=64 time=0.063 ms
^C
--- 192.168.60.11 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5099ms
rtt min/avg/max/mdev = 0.059/0.063/0.073/0.004 ms
root@86470afed2d65:/# telnet 10.9.0.11
Trying 10.9.0.11...
Connected to 10.9.0.11.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
ad4423d4610e login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@ad4423d4610e:~$
```

```

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Fire... /ho... Terminal Thunar Fri 31 Mar, 06:57 seed...
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... seed... + ...
rtt min/avg/max/mdev = 0.059/0.063/0.073/0.004 ms
root@ad4423d4610e:~# telnet 10.9.0.11
Trying 10.9.0.11...
Connected to 10.9.0.11.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
ad4423d4610e login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@ad4423d4610e:~$ ls
seed@ad4423d4610e:~$ exit
logout
Connection closed by foreign host.
root@ad4423d4610e:#

```

Before we run the active commands we can print it we can telnet it, now it asks us to execute those ip tips command and try it again by pinging and telnetting it.

Telnet service is running on all the containers, the core seat was created on them with the panel ds as I jus demonstrated

Report your observation and explain the problems of each row.

Here we need to setup these rows in the router inside the router

It lists out this field table

```

root@ad4423d4610e:/# 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@ad4423d4610e:#

```

We can use the check command to see whether the ICMP rule is added here

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) ~ TigerVNC
Applications Firef... /ho... 2 Ter... Thunar Fri 31 Mar, 07:17
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... + 

64 bytes from 192.168.60.11: icmp_seq=4 ttl=64 time=0.041 ms
64 bytes from 192.168.60.11: icmp_seq=5 ttl=64 time=0.040 ms
64 bytes from 192.168.60.11: icmp_seq=6 ttl=64 time=0.039 ms
^C
--- 192.168.60.11 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5106ms
rtt min/avg/max/mdev = 0.037/0.040/0.046/0.002 ms
root@ad4423d4610e:/# 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@ad4423d4610e:/# iptables -A INPUT -p icmp --icmp-type echo-request -j
iptables v1.8.4 (legacy): option "-j" requires an argument
Try `iptables -h` or 'iptables --help' for more information.
root@ad4423d4610e:/# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
root@ad4423d4610e:/# iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
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 ACCEPT)
target     prot opt source          destination
root@ad4423d4610e:/#
```

For the echo reply we also accept the reply which means we let the reply go back to the accessor and we set the default rules of the output to be job and input to job which means other protocols cannot access our router.

To specify the default rule touch p, on this output chain drop everything

```

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications ③ Firef... ② /ho... ② Ter... ③ Thunar ③ Fri 31 Mar, 07:29
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... seed...
64 bytes from 192.168.60.11: icmp_seq=6 ttl=64 time=0.039 ms
^C
--- 192.168.60.11 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5106ms
rtt min/avg/max/mdev = 0.037/0.040/0.046/0.002 ms
root@ad4423d4610e:/# 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@ad4423d4610e:/# iptables -A INPUT -p icmp --icmp-type echo-request -j
iptables v1.8.4 (legacy): option "-j" requires an argument
Try `iptables -h` or `iptables --help` for more information.
root@ad4423d4610e:/# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
root@ad4423d4610e:/# iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
ACCEPT    icmp -- 0.0.0.0/0          0.0.0.0/0           icmp type 8
Chain FORWARD (policy ACCEPT)
target     prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
root@ad4423d4610e:/# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@ad4423d4610e:/# iptables -P OUTPUT DROP
root@ad4423d4610e:/# iptables -P INPUT DROP

```

```

root@ad4423d4610e:/# iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
ACCEPT    icmp -- 0.0.0.0/0          0.0.0.0/0           icmp type 8
Chain FORWARD (policy ACCEPT)
target     prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
root@ad4423d4610e:/# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@ad4423d4610e:/# iptables -P OUTPUT DROP
root@ad4423d4610e:/# iptables -P INPUT DROP
root@ad4423d4610e:/# 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           icmp type 8
ACCEPT    icmp -- 0.0.0.0/0          0.0.0.0/0           icmp type 0
Chain FORWARD (policy ACCEPT)
target     prot opt source          destination
Chain OUTPUT (policy DROP)
target     prot opt source          destination
root@ad4423d4610e:/#

```

Now we should test it here ping should work and telnet should deny

Here below the ping does not work

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Fire... /ho... Ter... Thunar Fri 31 Mar, 07:34 seed...
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... seed...
ad4423d4610e login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@ad4423d4610e:~$ ls
seed@ad4423d4610e:~$ exit
logout
Connection closed by foreign host.
root@86470af2d65:~# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
^C
--- 192.168.60.11 ping statistics ---
14 packets transmitted, 0 received, 100% packet loss, time 13301ms
root@86470af2d65:~#
```

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Fire... /ho... Ter... Thunar Fri 31 Mar, 07:34 seed...
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed...
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

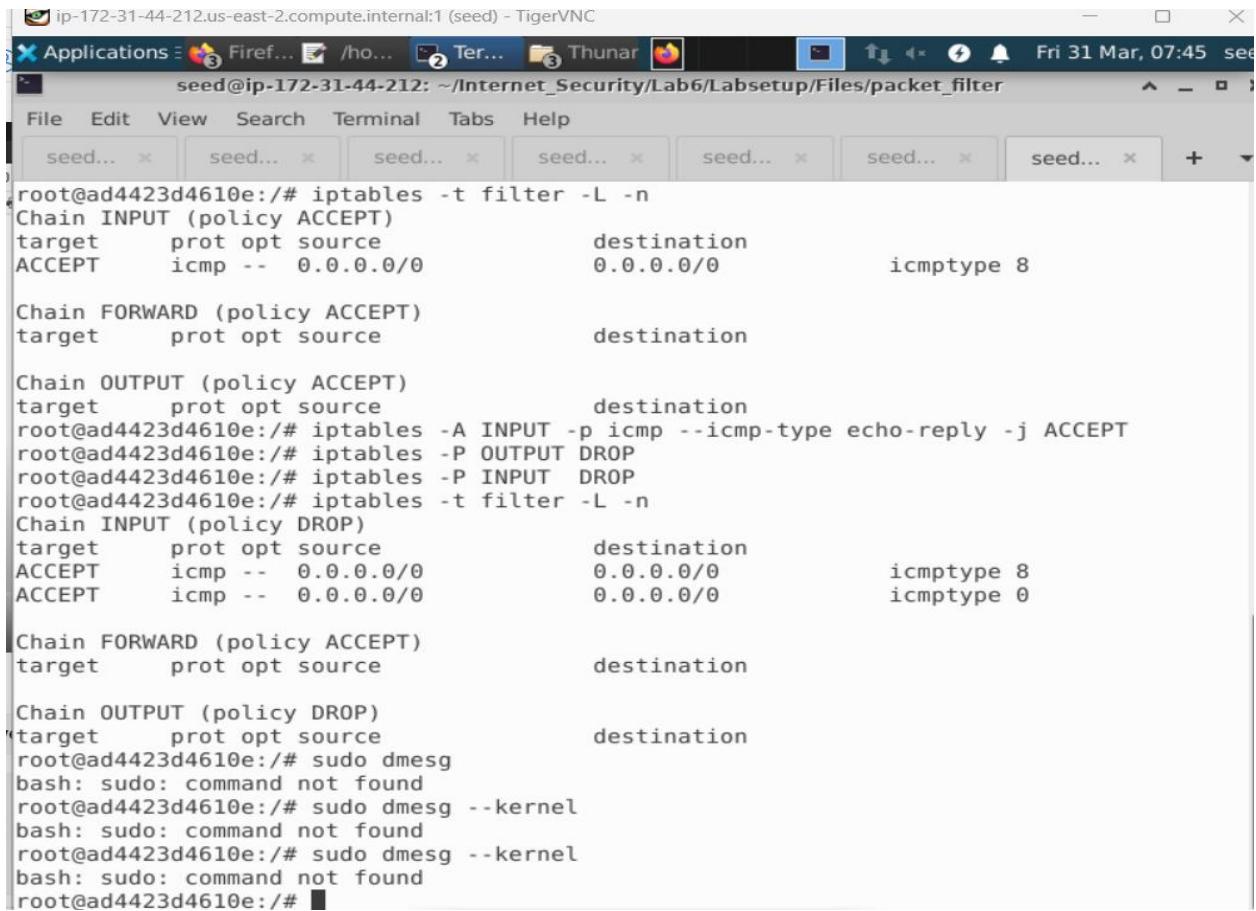
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@ad4423d4610e:~$ ls
seed@ad4423d4610e:~$ exit
logout
Connection closed by foreign host.
root@86470af2d65:~# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
^C
--- 192.168.60.11 ping statistics ---
14 packets transmitted, 0 received, 100% packet loss, time 13301ms
root@86470af2d65:~# telnet 10.9.0.11
Trying 10.9.0.11...
^C
root@86470af2d65:~#
```

We can check whether we are able to see any kernel information from here

The information which we got in our virtual machine and the kernel message they share same kind of buffer between these containers and virtual machine and we didn't see any new messages printed out here

We get the output as **seedBlock:The filter are being removed.**



```

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications   Fire... /ho... Ter... Thunar
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... seed... + -
root@ad4423d4610e:/# iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
target    prot opt source          destination
ACCEPT    icmp -- 0.0.0.0/0        0.0.0.0/0           icmp type 8

Chain FORWARD (policy ACCEPT)
target    prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination
root@ad4423d4610e:/# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@ad4423d4610e:/# iptables -P OUTPUT DROP
root@ad4423d4610e:/# iptables -P INPUT DROP
root@ad4423d4610e:/# 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           icmp type 8
ACCEPT    icmp -- 0.0.0.0/0        0.0.0.0/0           icmp type 0

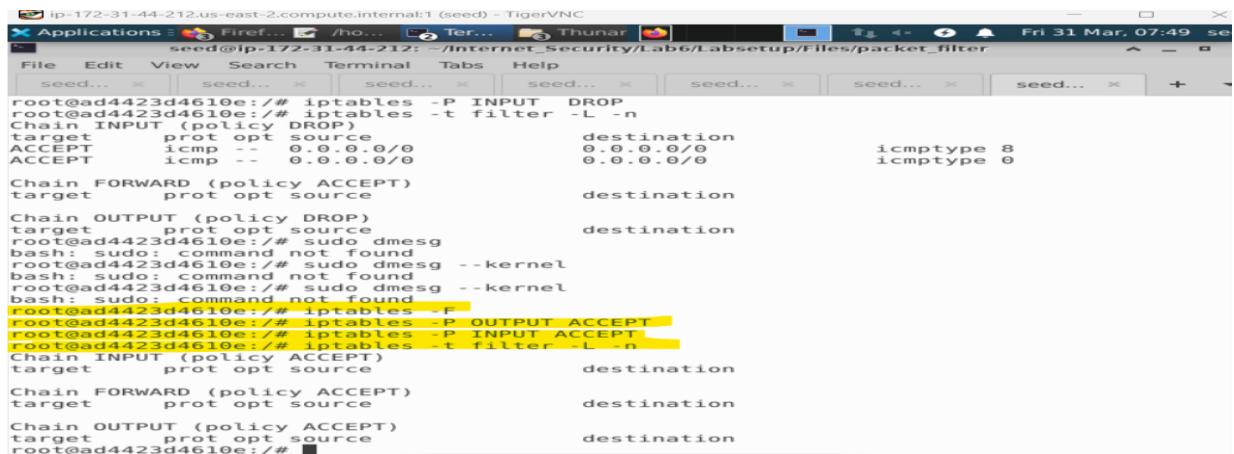
Chain FORWARD (policy ACCEPT)
target    prot opt source          destination

Chain OUTPUT (policy DROP)
target    prot opt source          destination
root@ad4423d4610e:/# sudo dmesg
bash: sudo: command not found
root@ad4423d4610e:/# sudo dmesg --kernel
bash: sudo: command not found
root@ad4423d4610e:/# sudo dmesg --kernel
bash: sudo: command not found
root@ad4423d4610e:/# ■

```

Restoring the filter table to it's original state with the following commands

The policy rules as removed now



```

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications   Fire... /ho... Ter... Thunar
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... seed... seed... + -
root@ad4423d4610e:/# iptables -P INPUT DROP
root@ad4423d4610e:/# 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           icmp type 8
ACCEPT    icmp -- 0.0.0.0/0        0.0.0.0/0           icmp type 0

Chain FORWARD (policy ACCEPT)
target    prot opt source          destination

Chain OUTPUT (policy DROP)
target    prot opt source          destination
root@ad4423d4610e:/# sudo dmesg
bash: sudo: command not found
root@ad4423d4610e:/# sudo dmesg --kernel
bash: sudo: command not found
root@ad4423d4610e:/# sudo dmesg --kernel
bash: sudo: command not found
root@ad4423d4610e:/# ■
root@ad4423d4610e:/# iptables -F
root@ad4423d4610e:/# iptables -P OUTPUT ACCEPT
root@ad4423d4610e:/# iptables -P INPUT ACCEPT
root@ad4423d4610e:/# 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@ad4423d4610e:/# ■

```

Another way to restore the states of all the tables is to restart the container. Here we need to find the ID docker restore command id

Task 2.B: Protecting the Internal Network

Here we make use of internal network we have 3 containers

192.168.60.5/6/7

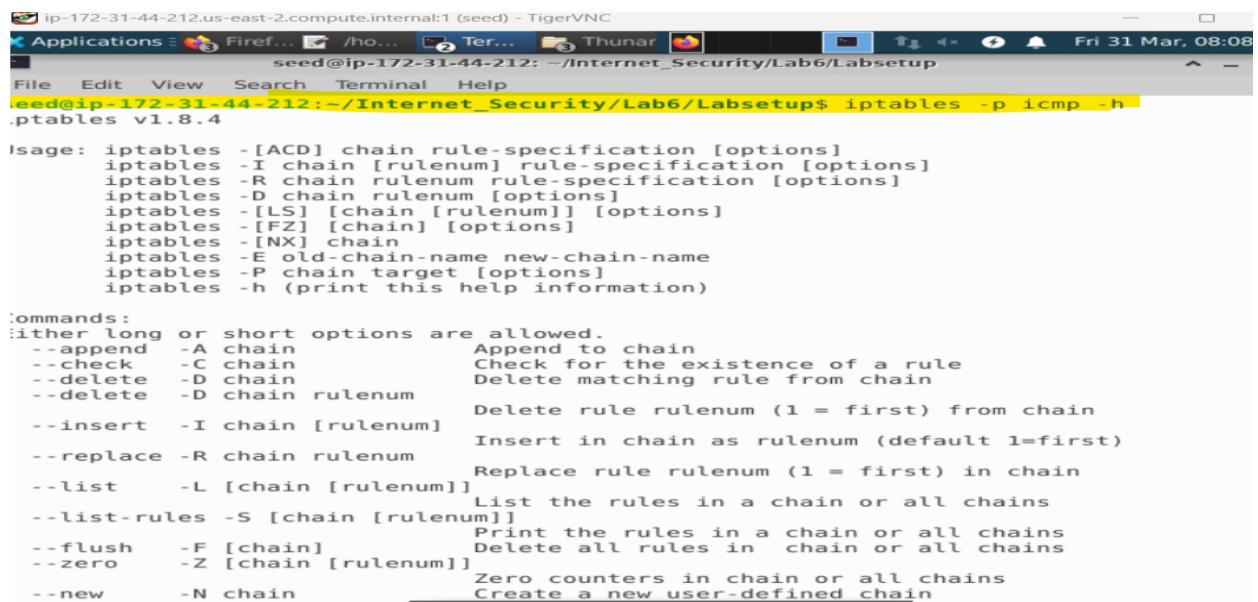
We need to use the forward chain for this purpose because the router sit between the outside and this this internal network so we need the forward chain in the router

The directions of the packet in the input and output chains are clear effects are either coming into for the input or going out for the output it's not true for the forward check because its bi-directional, because going into the internal network or going out to the external network or go through this forward chain.

Outside host cannot ping internal hosts

We are inside the router now as in containers the autocomplete does not work.

We use the below command to find the other match options. The match options are for the snmp protocol.



```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications = Firef... /ho... Ter... Thunar Fri 31 Mar, 08:08
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup
File Edit View Search Terminal Help
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ iptables -p icmp -h
iptables v1.8.4

Usage: iptables [-ACD] chain rule-specification [options]
iptables -I chain [rulenumber] rule-specification [options]
iptables -R chain rulenumber rule-specification [options]
iptables -D chain rulenumber [options]
iptables -[LS] [chain [rulenumber]] [options]
iptables -[FZ] [chain] [options]
iptables -[NX] chain
iptables -E old-chain-name new-chain-name
iptables -P chain target [options]
iptables -h (print this help information)

Commands:
:either long or short options are allowed.
--append -A chain          Append to chain
--check -C chain            Check for the existence of a rule
--delete -D chain           Delete matching rule from chain
--delete -D chain rulenumber Delete rule rulenumber (1 = first) from chain
--insert -I chain [rulenumber] Insert in chain as rulenumber (default 1=first)
--replace -R chain rulenumber Replace rule rulenumber (1 = first) in chain
--list -L [chain [rulenumber]] List the rules in a chain or all chains
--list-rules -S [chain [rulenumber]] Print the rules in a chain or all chains
--flush -F [chain]           Delete all rules in chain or all chains
--zero -Z [chain [rulenumber]] Zero counters in chain or all chains
--new -N chain               Create a new user-defined chain
```

```

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firefo... /ho... Ter... Thunar Fri 31 Mar, 08:12
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... seed...
seed... seed... seed... seed... seed... seed... seed... + 

bash: sudo: command not found
root@ad4423d4610e:/# sudo dmesg --kernel
bash: sudo: command not found
root@ad4423d4610e:/# sudo dmesg --kernel
bash: sudo: command not found
root@ad4423d4610e:/# iptables -F
root@ad4423d4610e:/# iptables -P OUTPUT ACCEPT
root@ad4423d4610e:/# iptables -P INPUT ACCEPT
root@ad4423d4610e:/# 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@ad4423d4610e:/# iptables -t forward -L -n
iptables v1.8.4 (legacy): can't initialize iptables table `forward': Table does not exist (do you need to insmod?)
Perhaps iptables or your kernel needs to be upgraded.
root@ad4423d4610e:/# 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@ad4423d4610e:/#

```

The outside host will be able to ping inner host because they were also dropped when they come to the router

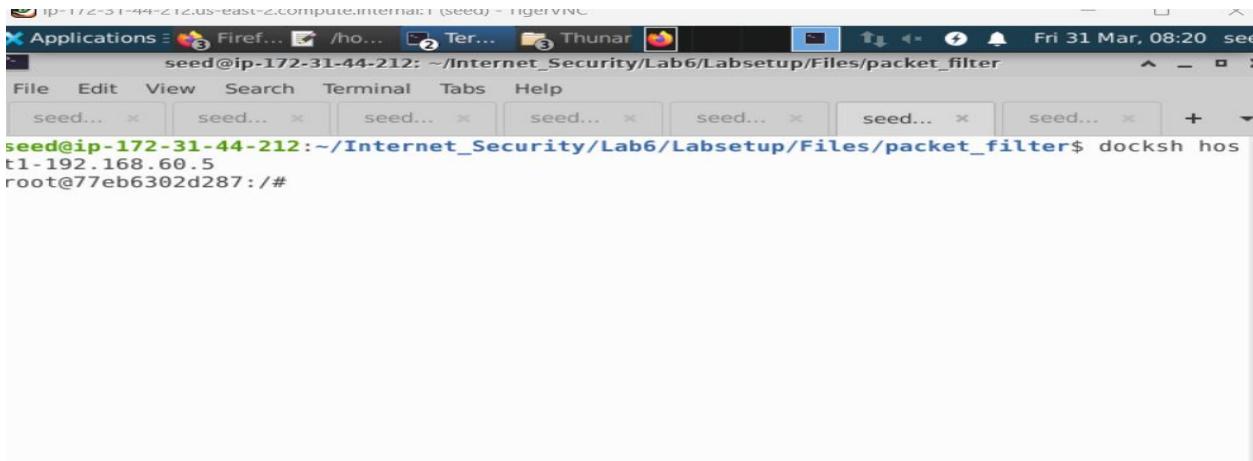
```

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firefo... /ho... Ter... Thunar Fri 31 Mar, 08:18 se
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... seed...
seed... seed... seed... seed... seed... seed... seed... seed... + 

root@ad4423d4610e:/# iptables -t forward -L -n
iptables v1.8.4 (legacy): can't initialize iptables table `forward': Table does not exist (do you need to insmod?)
Perhaps iptables or your kernel needs to be upgraded.
root@ad4423d4610e:/# 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@ad4423d4610e:/# iptables -A FORWARD -p icmp --icmp-type echo-request -j DROP
root@ad4423d4610e:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DR
OP
root@ad4423d4610e:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DR
OP
root@ad4423d4610e:/# iptables -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           icmp type 8
DROP     icmp -- 0.0.0.0/0                 0.0.0.0/0           icmp type 8
DROP     icmp -- 0.0.0.0/0                 0.0.0.0/0           icmp type 8
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ad4423d4610e:/#

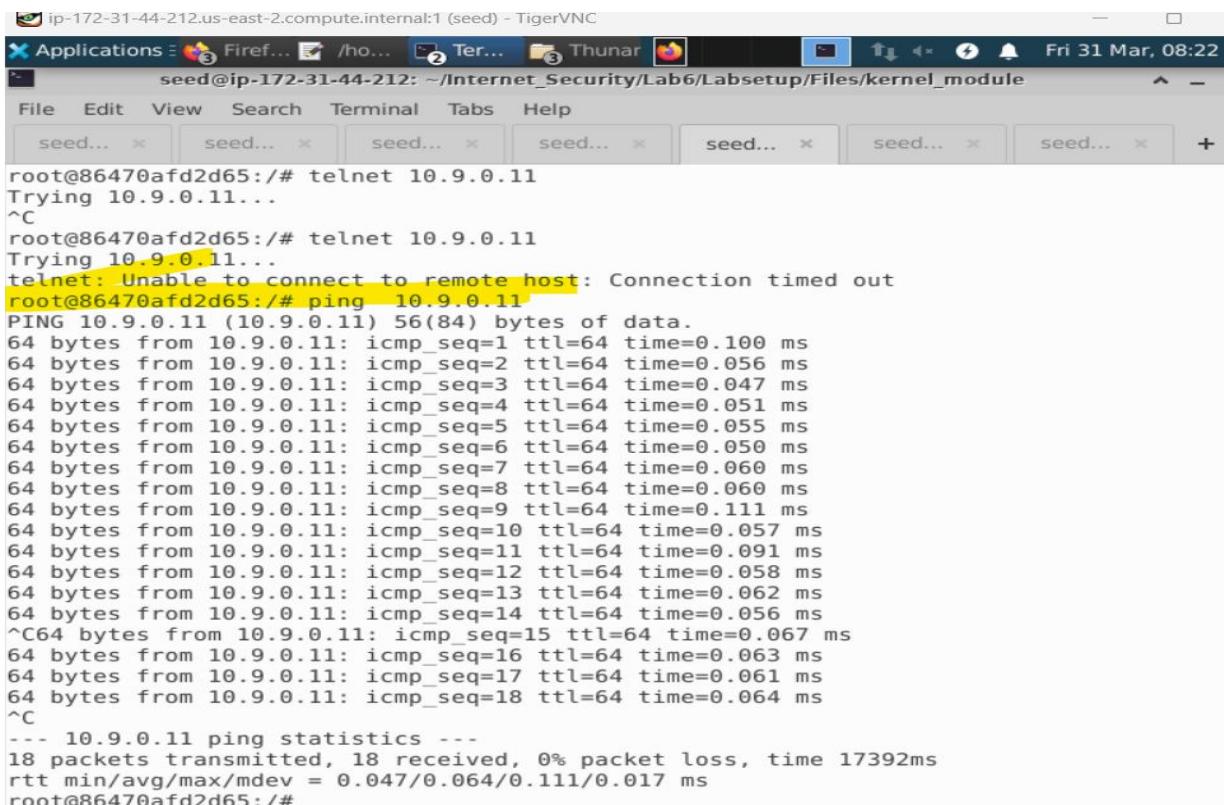
```

Inside network below



```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ docksh host1-192.168.60.5
root@77eb6302d287:/#
```

1. Outside hosts cannot ping internal hosts



```
root@86470af2d65:/# telnet 10.9.0.11
Trying 10.9.0.11...
^C
root@86470af2d65:/# telnet 10.9.0.11
Trying 10.9.0.11...
telnet: Unable to connect to remote host: Connection timed out
root@86470af2d65:/# 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=0.100 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=0.047 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.051 ms
64 bytes from 10.9.0.11: icmp_seq=5 ttl=64 time=0.055 ms
64 bytes from 10.9.0.11: icmp_seq=6 ttl=64 time=0.050 ms
64 bytes from 10.9.0.11: icmp_seq=7 ttl=64 time=0.060 ms
64 bytes from 10.9.0.11: icmp_seq=8 ttl=64 time=0.060 ms
64 bytes from 10.9.0.11: icmp_seq=9 ttl=64 time=0.111 ms
64 bytes from 10.9.0.11: icmp_seq=10 ttl=64 time=0.057 ms
64 bytes from 10.9.0.11: icmp_seq=11 ttl=64 time=0.091 ms
64 bytes from 10.9.0.11: icmp_seq=12 ttl=64 time=0.058 ms
64 bytes from 10.9.0.11: icmp_seq=13 ttl=64 time=0.062 ms
64 bytes from 10.9.0.11: icmp_seq=14 ttl=64 time=0.056 ms
^C64 bytes from 10.9.0.11: icmp_seq=15 ttl=64 time=0.067 ms
64 bytes from 10.9.0.11: icmp_seq=16 ttl=64 time=0.063 ms
64 bytes from 10.9.0.11: icmp_seq=17 ttl=64 time=0.061 ms
64 bytes from 10.9.0.11: icmp_seq=18 ttl=64 time=0.064 ms
^C
--- 10.9.0.11 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17392ms
rtt min/avg/max/mdev = 0.047/0.064/0.111/0.017 ms
root@86470af2d65:/#
```

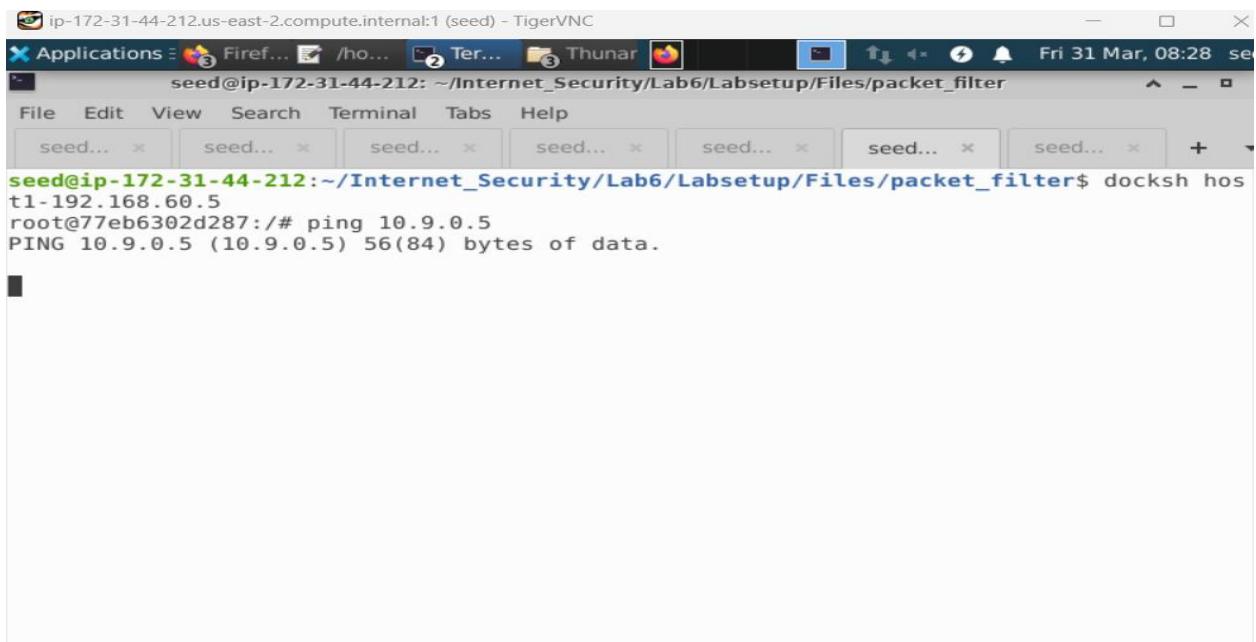
Now is able to ping the router.

When we ping the inner host it has stopped, it cannot ping the inner host.

2) Outside host can ping the router

The inner host can ping outside host.

Internal host can ping the outside host



```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications   Firef... /ho... 2 Ter... 3 Thunar Firefox Fri 31 Mar, 08:28 seed
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter
File Edit View Search Terminal Tabs Help
seed... x + -
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ docksh host1-192.168.60.5
root@77eb6302d287:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
```

```
root@77eb6302d287:/# 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=0.093 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.095 ms
```

```

Applications Firefox /ho... Terminal Thunar Fri 31 Mar, 08:23 seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module
File Edit View Search Terminal Tabs Help
seed... < > + < >
^C
root@86470af2d65:/# telnet 10.9.0.11
Trying 10.9.0.11...
telnet: Unable to connect to remote host: Connection timed out
root@86470af2d65:/# 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=0.100 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=0.047 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.051 ms
64 bytes from 10.9.0.11: icmp_seq=5 ttl=64 time=0.055 ms
64 bytes from 10.9.0.11: icmp_seq=6 ttl=64 time=0.050 ms
64 bytes from 10.9.0.11: icmp_seq=7 ttl=64 time=0.060 ms
64 bytes from 10.9.0.11: icmp_seq=8 ttl=64 time=0.060 ms
64 bytes from 10.9.0.11: icmp_seq=9 ttl=64 time=0.111 ms
64 bytes from 10.9.0.11: icmp_seq=10 ttl=64 time=0.057 ms
64 bytes from 10.9.0.11: icmp_seq=11 ttl=64 time=0.091 ms
64 bytes from 10.9.0.11: icmp_seq=12 ttl=64 time=0.058 ms
64 bytes from 10.9.0.11: icmp_seq=13 ttl=64 time=0.062 ms
64 bytes from 10.9.0.11: icmp_seq=14 ttl=64 time=0.056 ms
^C64 bytes from 10.9.0.11: icmp_seq=15 ttl=64 time=0.067 ms
64 bytes from 10.9.0.11: icmp_seq=16 ttl=64 time=0.063 ms
64 bytes from 10.9.0.11: icmp_seq=17 ttl=64 time=0.061 ms
64 bytes from 10.9.0.11: icmp_seq=18 ttl=64 time=0.064 ms
^C
-- 10.9.0.11 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17392ms
rtt min/avg/max/mdev = 0.047/0.064/0.111/0.017 ms
root@86470af2d65:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.

```

```

Applications Firefox /home/seed/Internet_Sec... Terminal Thunar Fri 31 Mar, 08:23 seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter
File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-2... < > seed@ip-172-31-44-2... < >
root@ad4423d4610e:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DROP
root@ad4423d4610e:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DROP
root@ad4423d4610e:/# iptables -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
DROP      icmp -- 0.0.0.0/0        0.0.0.0/0           icmptype 8
DROP      icmp -- 0.0.0.0/0        0.0.0.0/0           icmptype 8
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
root@ad4423d4610e:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j ACCEPT
root@ad4423d4610e:/# iptables -A FORWARD -i eth1 -p icmp --icmp-type echo-request -j ACCEPT
root@ad4423d4610e:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-reply -j ACCEPT
root@ad4423d4610e:/# iptables -P FORWARD DROP
iptables: warning: (loopback) --P requires a chain and a policy.
Try 'iptables -h' or 'iptables -P --help' for more information.
root@ad4423d4610e:/# iptables -P FORWARD DROP
root@ad4423d4610e:/# iptables -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
DROP      icmp -- 0.0.0.0/0        0.0.0.0/0           icmptype 8
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 8
ACCEPT    icmp -- 0.0.0.0/0        0.0.0.0/0           icmptype 8
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
root@ad4423d4610e:/#

```

```

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications: ③ Firef... ④ /ho... ② Ter... ③ Thunar ⑤ Fri 31 Mar, 08:41 seed
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter
File Edit View Search Terminal Tabs Help
seed... × + ▾
ACCEPT    icmp -- 0.0.0.0/0      0.0.0.0/0      icmp type 8
ACCEPT    icmp -- 0.0.0.0/0      0.0.0.0/0      icmp type 8
ACCEPT    icmp -- 0.0.0.0/0      0.0.0.0/0      icmp type 0

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
root@ad4423d4610e:/# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in      out      source          destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in      out      source          destination
  918 77112 DROP       icmp   --  *      *      0.0.0.0/0      0.0.0.0/0
  icmp type 8
  0     0 DROP       icmp   --  eth0   *      0.0.0.0/0      0.0.0.0/0
  icmp type 8
  0     0 DROP       icmp   --  eth0   *      0.0.0.0/0      0.0.0.0/0
  icmp type 8
  0     0 ACCEPT     icmp   --  eth0   *      0.0.0.0/0      0.0.0.0/0
  icmp type 8
  0     0 ACCEPT     icmp   --  eth1   *      0.0.0.0/0      0.0.0.0/0
  icmp type 8
  0     0 ACCEPT     icmp   --  eth0   *      0.0.0.0/0      0.0.0.0/0
  icmp type 0

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in      out      source          destination
root@ad4423d4610e:/#

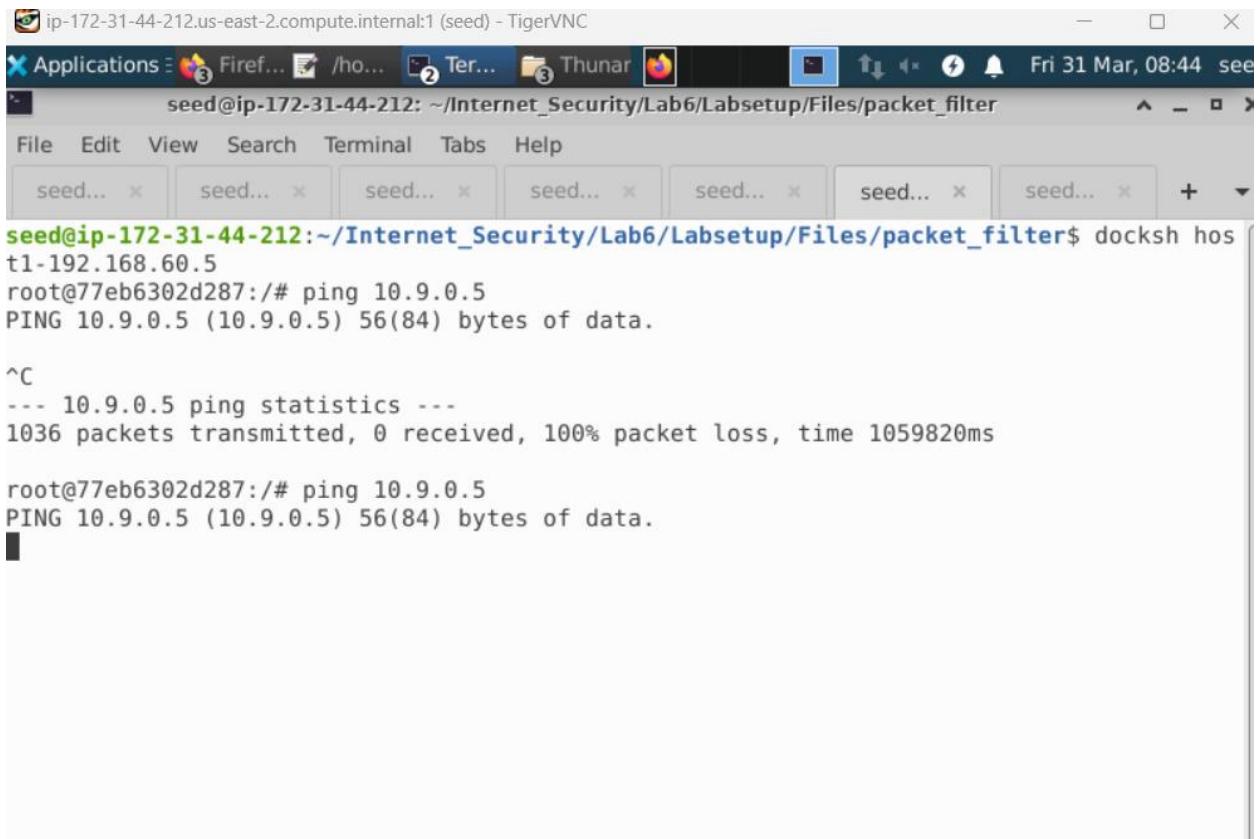
```

From the outside host ping the inside host

```

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications: ③ Firef... ④ /ho... ② Ter... ③ Thunar ⑤ Fri 31 M...
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module
File Edit View Search Terminal Tabs Help
seed... × + ▾
64 bytes from 10.9.0.11: icmp_seq=1 ttl=64 time=0.100 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=0.047 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.051 ms
64 bytes from 10.9.0.11: icmp_seq=5 ttl=64 time=0.055 ms
64 bytes from 10.9.0.11: icmp_seq=6 ttl=64 time=0.050 ms
64 bytes from 10.9.0.11: icmp_seq=7 ttl=64 time=0.060 ms
64 bytes from 10.9.0.11: icmp_seq=8 ttl=64 time=0.060 ms
64 bytes from 10.9.0.11: icmp_seq=9 ttl=64 time=0.111 ms
64 bytes from 10.9.0.11: icmp_seq=10 ttl=64 time=0.057 ms
64 bytes from 10.9.0.11: icmp_seq=11 ttl=64 time=0.091 ms
64 bytes from 10.9.0.11: icmp_seq=12 ttl=64 time=0.058 ms
64 bytes from 10.9.0.11: icmp_seq=13 ttl=64 time=0.062 ms
64 bytes from 10.9.0.11: icmp_seq=14 ttl=64 time=0.056 ms
^C64 bytes from 10.9.0.11: icmp_seq=15 ttl=64 time=0.067 ms
64 bytes from 10.9.0.11: icmp_seq=16 ttl=64 time=0.063 ms
64 bytes from 10.9.0.11: icmp_seq=17 ttl=64 time=0.061 ms
64 bytes from 10.9.0.11: icmp_seq=18 ttl=64 time=0.064 ms
^C
--- 10.9.0.11 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17392ms
rtt min/avg/max/mdev = 0.047/0.064/0.111/0.017 ms
root@86470af2d65:/# 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 ---
83 packets transmitted, 0 received, 100% packet loss, time 83957ms
root@86470af2d65:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.

```



A screenshot of a Linux desktop environment showing a terminal window. The terminal window title is "seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter". The terminal content shows a ping test from a host (t1-192.168.60.5) to another host (10.9.0.5). The output indicates 1036 packets transmitted, 0 received, and 100% packet loss.

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ docksh host1-192.168.60.5
root@77eb6302d287:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.

^C
--- 10.9.0.5 ping statistics ---
1036 packets transmitted, 0 received, 100% packet loss, time 1059820ms

root@77eb6302d287:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
```

```
root@77eb6302d287:/# 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=0.073 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.079 ms
```

Telnet to inside host does not work

```

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Fire... /ho... Ter... Thunar Fri 31 M
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed...
seed... seed... seed... seed... seed... seed... seed...

64 bytes from 10.9.0.11: icmp_seq=7 ttl=64 time=0.060 ms
64 bytes from 10.9.0.11: icmp_seq=8 ttl=64 time=0.060 ms
64 bytes from 10.9.0.11: icmp_seq=9 ttl=64 time=0.111 ms
64 bytes from 10.9.0.11: icmp_seq=10 ttl=64 time=0.057 ms
64 bytes from 10.9.0.11: icmp_seq=11 ttl=64 time=0.091 ms
64 bytes from 10.9.0.11: icmp_seq=12 ttl=64 time=0.058 ms
64 bytes from 10.9.0.11: icmp_seq=13 ttl=64 time=0.062 ms
64 bytes from 10.9.0.11: icmp_seq=14 ttl=64 time=0.056 ms
^C64 bytes from 10.9.0.11: icmp_seq=15 ttl=64 time=0.067 ms
64 bytes from 10.9.0.11: icmp_seq=16 ttl=64 time=0.063 ms
64 bytes from 10.9.0.11: icmp_seq=17 ttl=64 time=0.061 ms
64 bytes from 10.9.0.11: icmp_seq=18 ttl=64 time=0.064 ms
^C
--- 10.9.0.11 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17392ms
rtt min/avg/max/mdev = 0.047/0.064/0.111/0.017 ms
root@86470af2d65:/# 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 ---
83 packets transmitted, 0 received, 100% packet loss, time 83957ms
root@86470af2d65:/# 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 ---
184 packets transmitted, 0 received, 100% packet loss, time 187381ms
root@86470af2d65:/# telnet 192.168.60.5
Trying 192.168.60.5...

```

Telnet from inside to outside host

```

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Fire... /ho... Ter... Thunar Fri 31 Mar, 08:49 se
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... + -
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ docksh hos
t1-192.168.60.5
root@77eb6302d287:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.

^C
--- 10.9.0.5 ping statistics ---
1036 packets transmitted, 0 received, 100% packet loss, time 1059820ms
root@77eb6302d287:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
^C
--- 10.9.0.5 ping statistics ---
67 packets transmitted, 0 received, 100% packet loss, time 67585ms
root@77eb6302d287:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
root@77eb6302d287:/

```

To clean and restore

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC

Applications: Fire... /ho... Ter... Thunar Fri 31 Mar, 08:52 seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter

```
File Edit View Search Terminal Tabs Help
seed... * seed... * seed... * seed... * seed... * seed... * seed... *
918 77112 DROP      icmp -- * * 0.0.0.0/0          0.0.0.0/0
icmptype 8          0 0 DROP      icmp -- eth0 * 0.0.0.0/0          0.0.0.0/0
icmptype 8          0 0 DROP      icmp -- eth0 * 0.0.0.0/0          0.0.0.0/0
icmptype 8          0 0 ACCEPT   icmp -- eth0 * 0.0.0.0/0          0.0.0.0/0
icmptype 8          0 0 ACCEPT   icmp -- eth1 * 0.0.0.0/0          0.0.0.0/0
icmptype 8          0 0 ACCEPT   icmp -- eth0 * 0.0.0.0/0          0.0.0.0/0
icmptype 0          0 0          0.0.0.0/0          0.0.0.0/0

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target    prot opt in     out    source          destination
root@ad4423d4610e:/# iptables -F
root@ad4423d4610e:/# iptables -P FORWARD ACCEPT
root@ad4423d4610e:/# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target    prot opt in     out    source          destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target    prot opt in     out    source          destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target    prot opt in     out    source          destination
root@ad4423d4610e:/#
```

Task 2.C Protecting Internal Servers

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications   Firef... /ho... 2 Ter... 3 Thunar
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... seed...
Trying 192.168.60.5...
telnet: Unable to connect to remote host: Connection timed out
root@86470afdf2d65:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
77eb6302d287 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@77eb6302d287:~$ exit
logout
Connection closed by foreign host.
root@86470afdf2d65:/#
```

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications   Firef... /ho... 2 Ter... 3 Thunar
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... seed...
logout
Connection closed by foreign host.
root@86470afdf2d65:/# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
b11c982b0c89 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@b11c982b0c89:~$ exit
logout
Connection closed by foreign host.
root@86470afdf2d65:/#
```

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firef... /ho... Ter... Thunar Fri 31 Mar, 08:5
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... seed...
applicable law.

seed@b11c982b0c89:~$ exit
logout
Connection closed by foreign host.
root@86470af2d65:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
See4fbca3e25 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@5ee4fbca3e25:~$
```

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firef... /ho... Ter... Thunar Fri 31 Mar, 09:00 se
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter
File Edit View Search Terminal Tabs Help
seed... seed... seed... seed... seed... seed... seed... +
67 packets transmitted, 0 received, 100% packet loss, time 67585ms

root@77eb6302d287:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
root@77eb6302d287:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
86470af2d65 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@86470af2d65:~$
```

Inside the router lets set up the rule

1. All the internal hosts run a telnet server (listening to port 23). Outside hosts can only access the telnet server on 192.168.60.5, 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.

```

root@ad4423d4610e:~# iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 23 -j ACCEPT
iptables v1.8.4 (legacy): multiple -d flags not allowed
Try 'iptables -h' or 'iptables --help' for more information.
root@ad4423d4610e:~# iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 23 -j ACCEPT
root@ad4423d4610e:~# iptables -A FORWARD -i eth1 -o eth0 -p tcp --sport 23 -j ACCEPT
root@ad4423d4610e:~# iptables -P FORWARD DROP
root@ad4423d4610e:~# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source          destination
      0     0 ACCEPT      tcp   --  eth0    *       0.0.0.0/0      192.168.60.5
      0     0 ACCEPT      tcp   --  eth1    *       0.0.0.0/0      192.168.60.5
      0     0 ACCEPT      tcp   --  eth1    o      0.0.0.0/0      192.168.60.5
      0     0 ACCEPT      tcp   --  eth0    o      0.0.0.0/0      192.168.60.5
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source          destination
      0     0 ACCEPT      tcp   --  eth0    *       0.0.0.0/0      192.168.60.5
      0     0 ACCEPT      tcp   --  eth1    *       0.0.0.0/0      192.168.60.5
      0     0 ACCEPT      tcp   --  eth1    o      0.0.0.0/0      192.168.60.5
      0     0 ACCEPT      tcp   --  eth0    o      0.0.0.0/0      192.168.60.5
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source          destination
root@ad4423d4610e:~#

```

```

root@ad4423d4610e:~# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
b11c982b0c89 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)

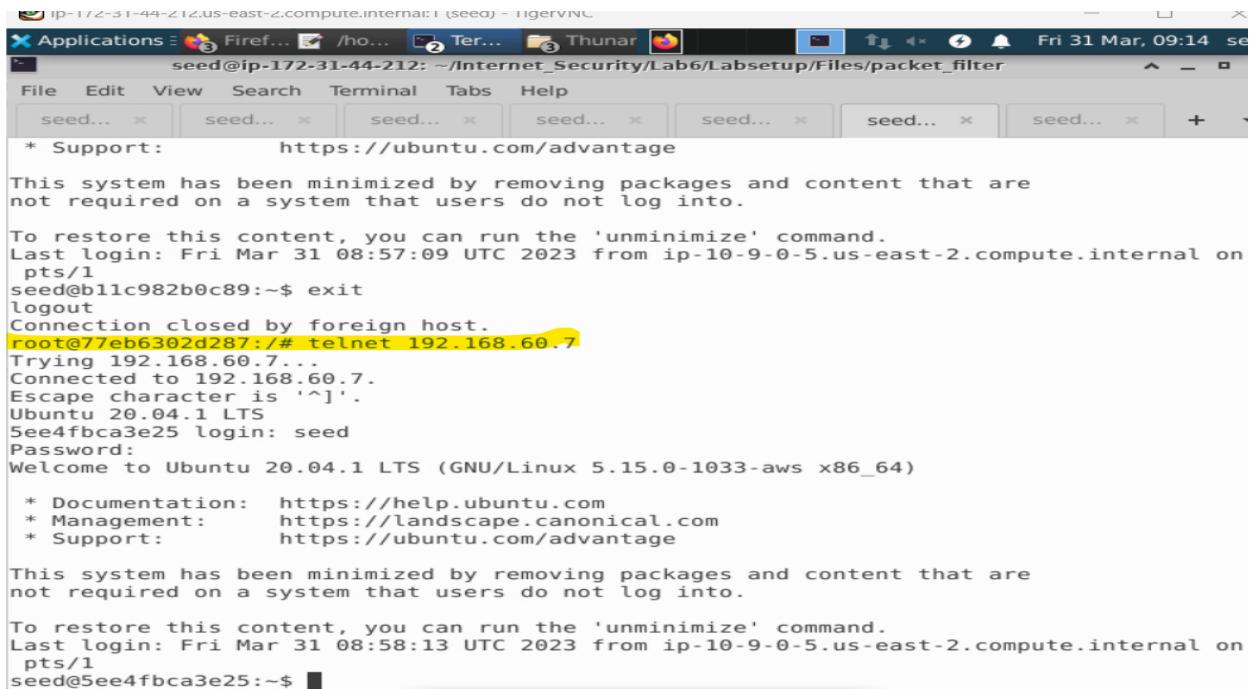
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Mar 31 08:57:09 UTC 2023 from ip-10-9-0-5.us-east-2.compute.internal on
pts/1
seed@b11c982b0c89:~$ exit
logout
Connection closed by foreign host.
root@ad4423d4610e:~#

```

Need to check whether other internal host can access other internal servers



The screenshot shows a terminal window titled "seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter". The terminal content is as follows:

```
* Support: https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Mar 31 08:57:09 UTC 2023 from ip-10-9-0-5.us-east-2.compute.internal on
pts/1
seed@b11c982b0c89:~$ exit
logout
Connection closed by foreign host.
root@77eb6302d287:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^].
Ubuntu 20.04.1 LTS
See4fbca3e25 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Mar 31 08:58:13 UTC 2023 from ip-10-9-0-5.us-east-2.compute.internal on
pts/1
seed@5ee4fbca3e25:~$
```

We didn't specify any rules to drop packets from one internal machine to another internal machine

```
root@77eb6302d287:/# telnet 192.168.60.7
Trying 192.168.60.7...
^C
root@77eb6302d287:/#
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ docksh hostA-10.9.0.5
root@86470af2d65:/# telnet 192.168.60.7
Trying 192.168.60.7...
^C
root@86470af2d65:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
root@86470af2d65:/# telnet 192.168.60.5
Trying 192.168.60.5...
```

There is a longer interface to that subnetwork so there is a source destination, there is also a ping from the router to the target

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ docksh hostA-10.9.0.5
root@86470af2d65:/# telnet 192.168.60.7
Trying 192.168.60.7...
^C
root@86470af2d65:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
root@86470af2d65:/# telnet 192.168.60.5
Trying 192.168.60.5...
^C
root@86470af2d65:/# nc -lt 9090
```

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications: Fire... /ho... Ter... Thunar
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module
File Edit View Search Terminal Tabs Help
see... see... see... see... see... see... see... see... see... see...
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ docksh ho
sta-10.9.0.5
root@86470af2d65:/# telnet 192.168.60.7
Trying 192.168.60.7...
^C
root@86470af2d65:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
root@86470af2d65:/# telnet 192.168.60.5
Trying 192.168.60.5...
^C
root@86470af2d65:/# nc -lt 9090
^C
root@86470af2d65:/# nc 192.168.60.5 9090
hello
^C
root@86470af2d65:/# nc -lu 9090
^C
root@86470af2d65:/# nc -u 192.168.60.5 9090
```

We are unable to connect

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications: Fire... /ho... Ter... Thunar
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module
File Edit View Search Terminal Tabs Help
see... see... see... see... see... see... see... see... see... see...
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ docksh h
sta-10.9.0.5
root@86470af2d65:/# telnet 192.168.60.7
Trying 192.168.60.7...
^C
root@86470af2d65:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
root@86470af2d65:/# telnet 192.168.60.5
Trying 192.168.60.5...
^C
root@86470af2d65:/# nc -lt 9090
^C
root@86470af2d65:/# nc 192.168.60.5 9090
hello
^C
root@86470af2d65:/# nc -lu 9090
^C
root@86470af2d65:/# nc -u 192.168.60.5 9090
^C
root@86470af2d65:/# nc -lu 9090

hello
```

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firef... /ho... ② Ter... ③ Thunar
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/packet_filter Fri 31 Mar, 09:32 see
File Edit View Terminal Tabs Help
se... se... se... se... se... se... se... se... se... se...
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ docksh host
t2-192.168.60.6
root@b11c982b0c89:/# nc -u 192.168.60.5 9090
hello
root@b11c982b0c89:/#
```

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firef... /ho... ② Ter... ③ Thunar
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup/Files/kernel_module Fri 31 Mar, 09:36 see
File Edit View Terminal Tabs Help
se... se... se... se... se... se... se... se... se... se...
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/kernel_module$ docksh host
sta-10.9.0.5
root@86470af2d65:/# telnet 192.168.60.7
Trying 192.168.60.7...
^C
root@86470af2d65:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
root@86470af2d65:/# telnet 192.168.60.5
Trying 192.168.60.5...
^C
root@86470af2d65:/# nc -lt 9090
^C
root@86470af2d65:/# nc 192.168.60.5 9090
hello
^C
root@86470af2d65:/# nc -lu 9090
^C
root@86470af2d65:/# nc -u 192.168.60.5 9090
^C
root@86470af2d65:/# nc -lu 9090

hello
^C
root@86470af2d65:/# nc -t 192.168.60.5 9090
hello
```

Terminal Emulator
Use the command line

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC

Applications: Firef... /ho... Ter... Thunar Fri 31 Mar, 09:36 seed

File Edit View Search Terminal Tabs Help

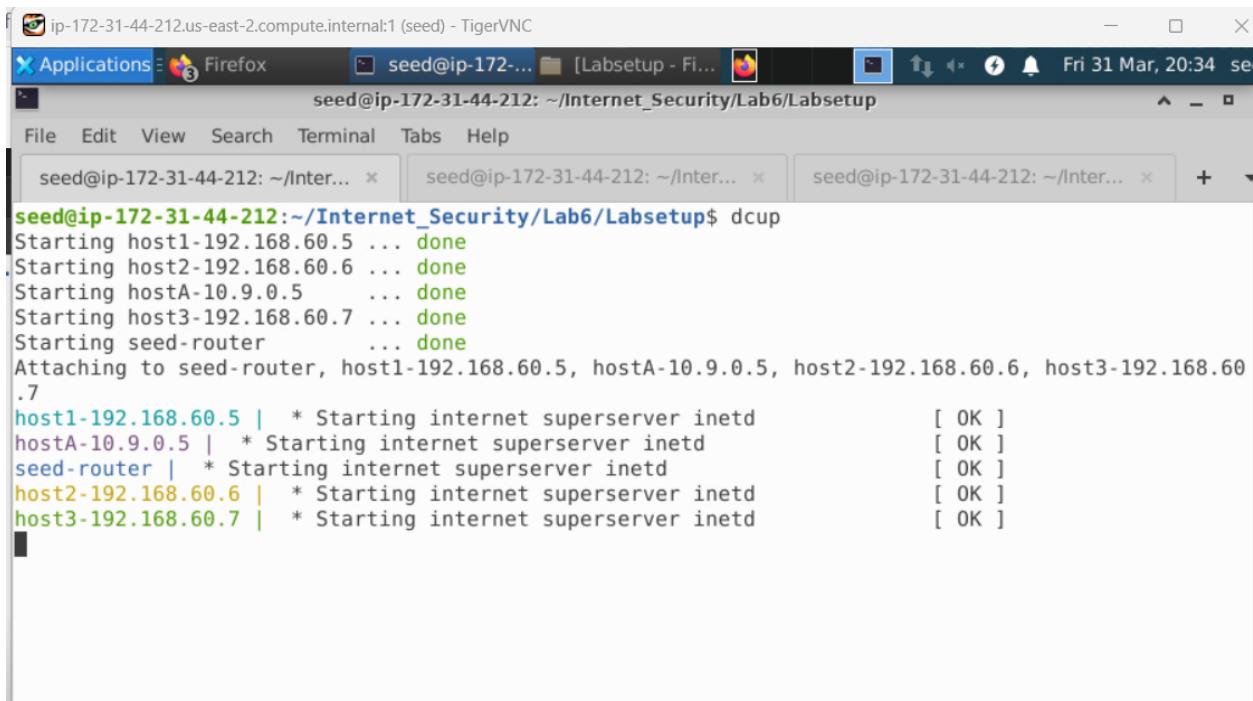
se... se... se... se... se... se... se... se... se... +

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup/Files/packet_filter$ docksh host2-192.168.60.6
root@b11c982b0c89:/# nc -u 192.168.60.5 9090
hello
root@b11c982b0c89:/# nc -t 192.168.60.5 9090
root@b11c982b0c89:/#
```

Task 3: Connection Tracking and Stateful Firewall

5.1 Task 3.A: Experiment with the Connection Tracking

Here we will work inside the loader container



```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firefox seed@ip-172-... [Labsetup - Fi...
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup
Fri 31 Mar, 20:34 seed

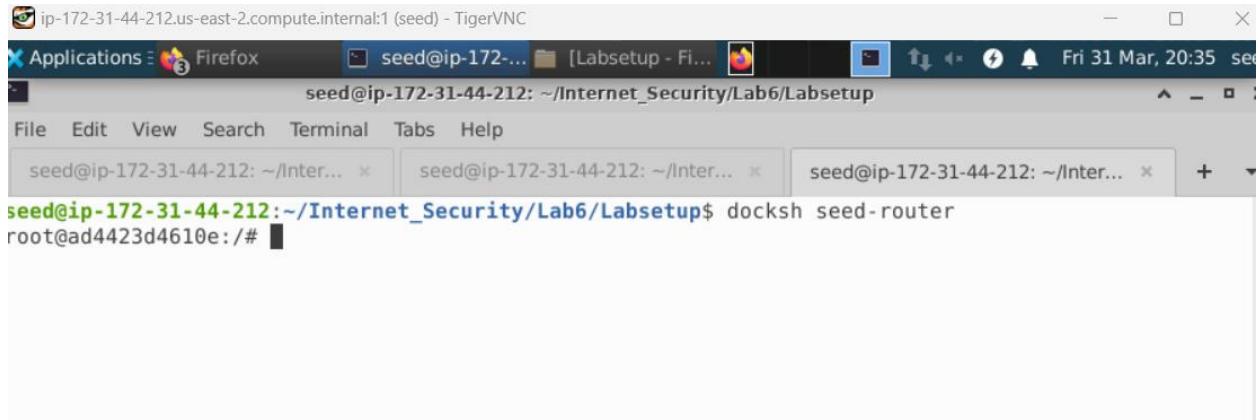
File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup$ dcup
Starting host1-192.168.60.5 ... done
Starting host2-192.168.60.6 ... done
Starting hostA-10.9.0.5 ... done
Starting host3-192.168.60.7 ... done
Starting seed-router ... done
Attaching to seed-router, host1-192.168.60.5, hostA-10.9.0.5, host2-192.168.60.6, host3-192.168.60.7
host1-192.168.60.5 | * 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 ]
host3-192.168.60.7 | * Starting internet superserver inetd [ OK ]
```



```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firefox seed@ip-172-... [Labsetup - Fi...
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup
Fri 31 Mar, 20:34 seed

File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup$ dockps
77eb6302d287 host1-192.168.60.5
b11c982b0c89 host2-192.168.60.6
5ee4fbca3e25 host3-192.168.60.7
86470afd2d65 hostA-10.9.0.5
ad4423d4610e seed-router
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup$
```

We need to go inside the seed router



```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh seed-router
root@ad4423d4610e:/#
```

To check the connection tracking information of any container we need to run this command



```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh seed-router
root@ad4423d4610e:/# conntrack -L
conntrack v1.4.5 (conntrack-tools): 0 flow entries have been shown.
root@ad4423d4610e:/#
```

Here we have 0 flow entries we didn't set up any connection tracking rows

1. ICMP Experiment

ICMP experiment: Run the following command and check the connection tracking information on the router. Describe your observation. How long is the ICMP connection state be kept?

We can put the ping into the background

```
root@ad4423d4610e:/# conntrack --help
Command line interface for the connection tracking system. Version 1.4.5
Usage: conntrack [commands] [options]
```

Commands:

-L [table] [options]	List conntrack or expectation table
-G [table] parameters	Get conntrack or expectation
-D [table] parameters	Delete conntrack or expectation
-I [table] parameters	Create a conntrack or expectation
-U [table] parameters	Update a conntrack
-E [table] [options]	Show events
-F [table]	Flush table
-C [table]	Show counter
-S	Show statistics

Tables: conntrack, expect, dying, unconfirmed

Conntrack parameters and options:

-n, --src-nat ip	source NAT ip
-g, --dst-nat ip	destination NAT ip
-j, --any-nat ip	source or destination NAT ip
-m, --mark mark	Set mark
-c, --secmark secmark	Set selinux secmark
-e, --event-mask eventmask	Event mask, eg. NEW,DESTROY
-z, --zero	Zero counters while listing

```
--label-add table      Delete table

Common parameters and options:
-s, --src, --orig-src ip          Source address from original direction
-d, --dst, --orig-dst ip         Destination address from original direction
-r, --reply-src ip               Source address from reply direction
-q, --reply-dst ip               Destination address from reply direction
-p, --proto num proto           Layer 4 Protocol, eg. 'tcp'
-f, --family proto              Layer 3 Protocol, eg. 'ipv6'
-t, --timeout timeout          Set timeout
-u, --status status             Set status, eg. ASSURED
-w, --zone value                Set conntrack zone
--orig-zone value               Set zone for original direction
--reply-zone value              Set zone for reply direction
-b, --buffer-size                Netlink socket buffer size
--mask-src ip                   Source mask address
--mask-dst ip                   Destination mask address

root@ad4423d4610e:/# 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=64 time=0.136 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=64 time=0.074 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=64 time=0.059 ms
^C
--- 192.168.60.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2054ms
rtt min/avg/max/mdev = 0.059/0.089/0.136/0.033 ms
root@ad4423d4610e:/#
```

We need to ping, ther's a whole screen inside the internal network put it in for the background

```

root@ad4423d4610e:/# 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=64 time=0.136 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=64 time=0.074 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=64 time=0.059 ms
^C
--- 192.168.60.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2054ms
rtt min/avg/max/mdev = 0.059/0.089/0.136/0.033 ms
root@ad4423d4610e:/# ping 192.168.60.5 &
[1] 34
root@ad4423d4610e:/# 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=64 time=0.079 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=64 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=64 time=0.064 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=64 time=0.118 ms
^C
root@ad4423d4610e:/# 64 bytes from 192.168.60.5: icmp_seq=6 ttl=64 time=0.063 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=64 time=0.052 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=64 time=0.056 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=64 time=0.062 ms

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ conntrack -L
conntrack v1.4.5 (conntrack-tools): Operation failed: sorry, you must be root or get CAP_NET_ADMIN capability to do this
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh seed-router
root@ad4423d4610e:/# conntrack -L
icmp 1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@ad4423d4610e:/# 
```

Kill the jobs and show the current status

```

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ conntrack -L
conntrack v1.4.5 (conntrack-tools): Operation failed: sorry, you must be root or get CAP_NET_ADMIN capability to do this
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh seed-router
root@ad4423d4610e:/# conntrack -L
icmp 1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@ad4423d4610e:/# jobs
root@ad4423d4610e:/# ping 192.168.60.5 &> /dev/null &
[1] 43
root@ad4423d4610e:/# conntrack -L
icmp 1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=43 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=43 use=1
icmp 1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@ad4423d4610e:/# jobs
[1]+  Running                  ping 192.168.60.5 &> /dev/null &
root@ad4423d4610e:/# kill %1
root@ad4423d4610e:/# conntrack -L
icmp 1 15 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=43 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=43 use=1
icmp 1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
[1]+  Terminated                 ping 192.168.60.5 &> /dev/null
root@ad4423d4610e:/# conntrack -L
icmp 1 0 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=43 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=43 use=1
icmp 1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@ad4423d4610e:/# 
```

How long we can keep the icmp connection state

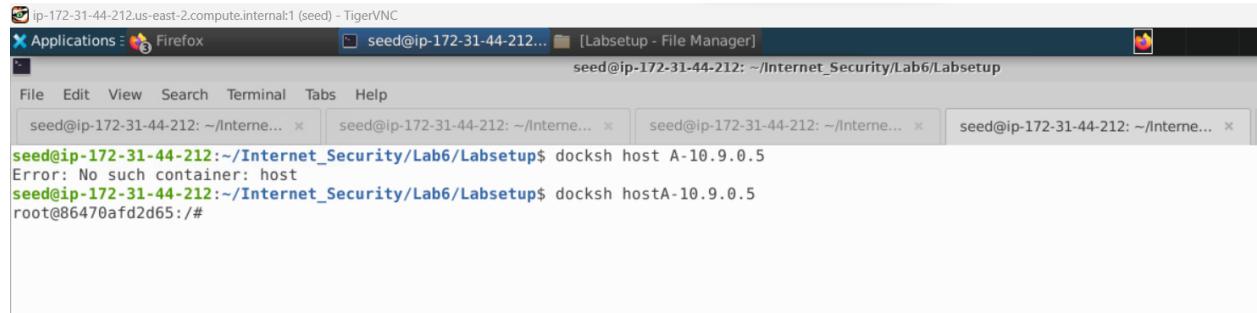
- We can write bash script to check when this connection becomes empty for this contract
- It will keep roughly the icmp connection state for 5 to 6 seconds or in other situations may be different just based on our own estimation

```

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ conntrack -L
conntrack v1.4.5 (conntrack-tools): Operation failed: sorry, you must be root or get CAP_NET_ADMIN capability to do this
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh seed-router
root@ad4423d4610e:/# conntrack -L
icmp 1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@ad4423d4610e:/# jobs
root@ad4423d4610e:/# ping 192.168.60.5 &> /dev/null &
[1] 43
root@ad4423d4610e:/# conntrack -L
icmp 1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=43 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=43 use=1
icmp 1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@ad4423d4610e:/# jobs
[1]+  Running                  ping 192.168.60.5 &> /dev/null
root@ad4423d4610e:/# kill %1
root@ad4423d4610e:/# conntrack -L
icmp 1 15 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=43 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=43 use=1
icmp 1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
[1]+  Terminated                 ping 192.168.60.5 &> /dev/null
root@ad4423d4610e:/# conntrack -L
icmp 1 0 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=43 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=43 use=1
icmp 1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@ad4423d4610e:/# contrack -L
bash: contrack: command not found
root@ad4423d4610e:/#

```

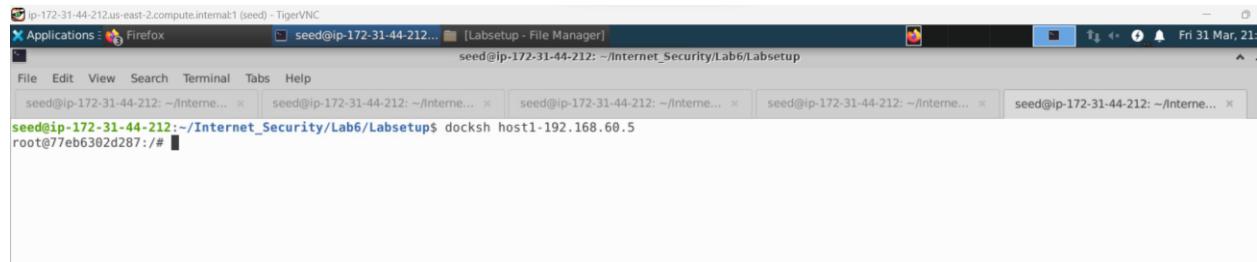
- 2) UDP experiment: Run the following command and check the connection tracking information on the router. Describe your observation. How long is the UDP connection state be kept?



```

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host A-10.9.0.5
Error: No such container: host
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh hostA-10.9.0.5
root@86470afd2d65:/#

```

```

seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host1-192.168.60.5
root@77eb6302d287:/#

```

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications   Fi...  s...  Mail  Firefox  docksh  Fri 31 Mar, 21:30  seed
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup
File Edit View Search Terminal Tabs Help
seed...  seed...  seed...  seed...  seed...  +  -
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh
host A-10.9.0.5
Error: No such container: host
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh
hostA-10.9.0.5
root@86470af2d65:/# nc -u 192.168.60.5 9090
hello
```

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications   Fi...  s...  Mail  Firefox  docksh  Fri 31 Mar, 21:31  seed
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup
File Edit View Search Terminal Tabs Help
seed...  seed...  seed...  seed...  seed...  +  -
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh
host1-192.168.60.5
root@77eb6302d287:/# nc -lu 9090
hello
```

```
root@ad4423d4610e:/# conntrack -L
icmp    1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@ad4423d4610e:/#
```

```

root@ad4423d4610e:/# conntrack -L
icmp      1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@ad4423d4610e:/#

```

The connection is active roughly for 6 to 8 seconds

Now lets stop it

```

File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212:~/Internet_Security/Lab6$ nc -l 9090
root@77eb6302d287:/# nc -lu 9090
hello
^C
root@77eb6302d287:/

```

```

File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212:~/Internet_Security/Lab6$ docksh host1-192.168.60.5
Error: No such container: host
seed@ip-172-31-44-212:~/Internet_Security/Lab6$ docksh hostA-10.9.0.5
root@86470afd2d65:/# nc -u 192.168.60.5 9090
hello
^C
root@86470afd2d65:/

```

3) TCP experiment: Run the following command and check the connection tracking information on the router. Describe your observation. How long is the TCP connection state be kept?

Again on inside host A host 1 we run a netcat tcp server

```

File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212:~/Internet_Security/Lab6$ nc -l 9090
root@77eb6302d287:/# nc -lu 9090
hello
^C
root@77eb6302d287:/

```

```

File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212:~/Internet_Security/Lab6$ docksh host1-192.168.60.5
Error: No such container: host
seed@ip-172-31-44-212:~/Internet_Security/Lab6$ docksh hostA-10.9.0.5
root@86470afd2d65:/# nc -u 192.168.60.5 9090
hello
^C
root@86470afd2d65:/

```

```
root@ad4423d4610e:/# conntrack -L
tcp      6 431972 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=39530 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=39530 [ASSURED] use=1
icmp     1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@ad4423d4610e:/#
```

In TCP we should be able to see the connection. Once we set up the connection we are going to set up a three way handshake.

Connection is set up from source to destination we did not send anything yet, because TCP is a connection oriented

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host A-10.9.0.5
Error: No such container: host
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh hostA-10.9.0.5
root@86470af2d65:/# nc -u 192.168.60.5 9090
hello
^C
root@86470af2d65:/# nc 192.168.60.5 9090
hello
hello
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host1-192.168.60.5
root@7eb6302d287:/# nc -l 9090
hello
^C
root@7eb6302d287:/# nc -l 9090
hello
hello
```

It will be kept as long as the TCP connection is not as broken

```
tcp      6 431972 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=39530 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=39530 [ASSURED] use=1
icmp     1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@ad4423d4610e:/# conntrack -L
tcp      6 431785 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=39530 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=39530 [ASSURED] use=1
icmp     1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@ad4423d4610e:/# conntrack -L
tcp      6 431780 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=39530 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=39530 [ASSURED] use=1
icmp     1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@ad4423d4610e:/# conntrack -L
tcp      6 431765 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=39530 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=39530 [ASSURED] use=1
icmp     1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@ad4423d4610e:/#
```

Now we will see it after the connection broke how long will be able to see it

```

root@ad4423d4610e:/# conntrack -L
tcp      6 431765 ESTABLISHED src=10.9.0.5 dst=192.168.60.5 sport=39530 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=39530 [ASSURED] use=1
icmp   1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@ad4423d4610e:/# conntrack -L
tcp      6 55 TIME_WAIT src=10.9.0.5 dst=192.168.60.5 sport=39530 dport=9090 src=192.168.60.5 dst=10.9.0.5 sport=9090 dport=39530 [ASSURED] use=1
icmp   1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 2 flow entries have been shown.
root@ad4423d4610e:/# conntrack -L
bash: conntrack: command not found
root@ad4423d4610e:/#

```

We are getting time wait means the connection did not stop completely

```

root@ad4423d4610e:/# conntrack -L
icmp   1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@ad4423d4610e:/# conntrack -L
icmp   1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@ad4423d4610e:/# conntrack -L
icmp   1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@ad4423d4610e:/# conntrack -L
icmp   1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@ad4423d4610e:/# conntrack -L
icmp   1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@ad4423d4610e:/# conntrack -L
icmp   1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=192.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@ad4423d4610e:/# conntrack -L

```

We are able to see that the number is decreasing to the local timeout

```

root@ad4423d4610e:/# conntrack -L
icmp 1 29 src=192.168.11 dst=192.168.60.5 type=8 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools):1 flow enteries have been shown.
root@ad4423d4610e:/# conntrack -L
icmp 1 29 src=192.168.11 dst=192.168.60.5 type=8 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools):1 flow enteries have been shown.
root@ad4423d4610e:/# conntrack -L
icmp 1 29 src=192.168.11 dst=192.168.60.5 type=8 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools):1 flow enteries have been shown.
root@ad4423d4610e:/# conntrack -L
icmp 1 29 src=192.168.11 dst=192.168.60.5 type=8 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools):0 flow enteries have been shown.

```

And lastly it becomes 0

Task 3.B: Setting Up a Stateful Firewall

We need to check inside our router to find those interface

```
root@ad4423d4610e:/# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
13: eth0@if14: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
        inet 10.9.0.11/24 brd 10.9.0.255 scope global eth0
            valid_lft forever preferred_lft forever
17: eth1@if18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:a8:3c:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
        inet 192.168.60.11/24 brd 192.168.60.255 scope global eth1
            valid_lft forever preferred_lft forever
root@ad4423d4610e:/#
```

We have two interfaces eth1 and eth0

For task 2 we need to rewrite those rules we need to check our record or task 2 and write the rules in these router, good idea is u may save those rules in the script, here I just type them line by line.

In task 2 there are telnet services, we need to refer to task 2. Firstly we will accept the new sync packet which will accept the tcp connection.

New sync packet used to establish TCP connection

Here we write the rule to accept the tcp connection a three way handshake

```
root@ad4423d4610e:/# iptables -A FORWARD -p
iptables v1.8.4 (legacy): option "-p" requires an argument
Try `iptables -h` or 'iptables --help' for more information.
root@ad4423d4610e:/# iptables -A FORWARD -p tcp -i eth0 -d 192.168.60.5 --dport 23
--syn -m conntrack --ctstate NEW -j ACCEPT
root@ad4423d4610e:/#
```

Now we want to allow to be able to access our cell host. A lot internal host with any external server.

So this allows internal host with any external server we didn't specify any target but for any destination ip and destination port which means any external server

```
.../y iptables -h or iptables --help for more information.
root@ad4423d4610e:/# iptables -A FORWARD -p tcp -i eth0 -d 192.168.60.5 --dport 23
--syn -m conntrack --ctstate NEW -j ACCEPT
root@ad4423d4610e:/# iptables -A FORWARD -i eth1 -p tcp --syn -m conntrack --ctstat
e NEW -j ACCEPT
root@ad4423d4610e:/#
```

Once this connection is established so they are following tcp packets we need to accept them. We want to accept any following tcp packets belong to the established tcp connections related

```
root@ad4423d4610e:/# iptables -A FORWARD -p tcp -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT  
root@ad4423d4610e:/#
```

Any packet other than the rules allowed we will drop them

```
root@ad4423d4610e:/# iptables -A FORWARD -p tcp -j DROP  
root@ad4423d4610e:/#
```

For other packets or ping packets we allow them pass by udp packets. Set up the default policy

```
root@ad4423d4610e:/# iptables -A FORWARD -p tcp -j DROP  
root@ad4423d4610e:/# iptables -P FORWARD ACCEPT  
root@ad4423d4610e:/#
```

Now lets test this one, internal host with any external host. We can confirm this internal host to the telent to the external host. Before that we need to check the rules which are set iptables

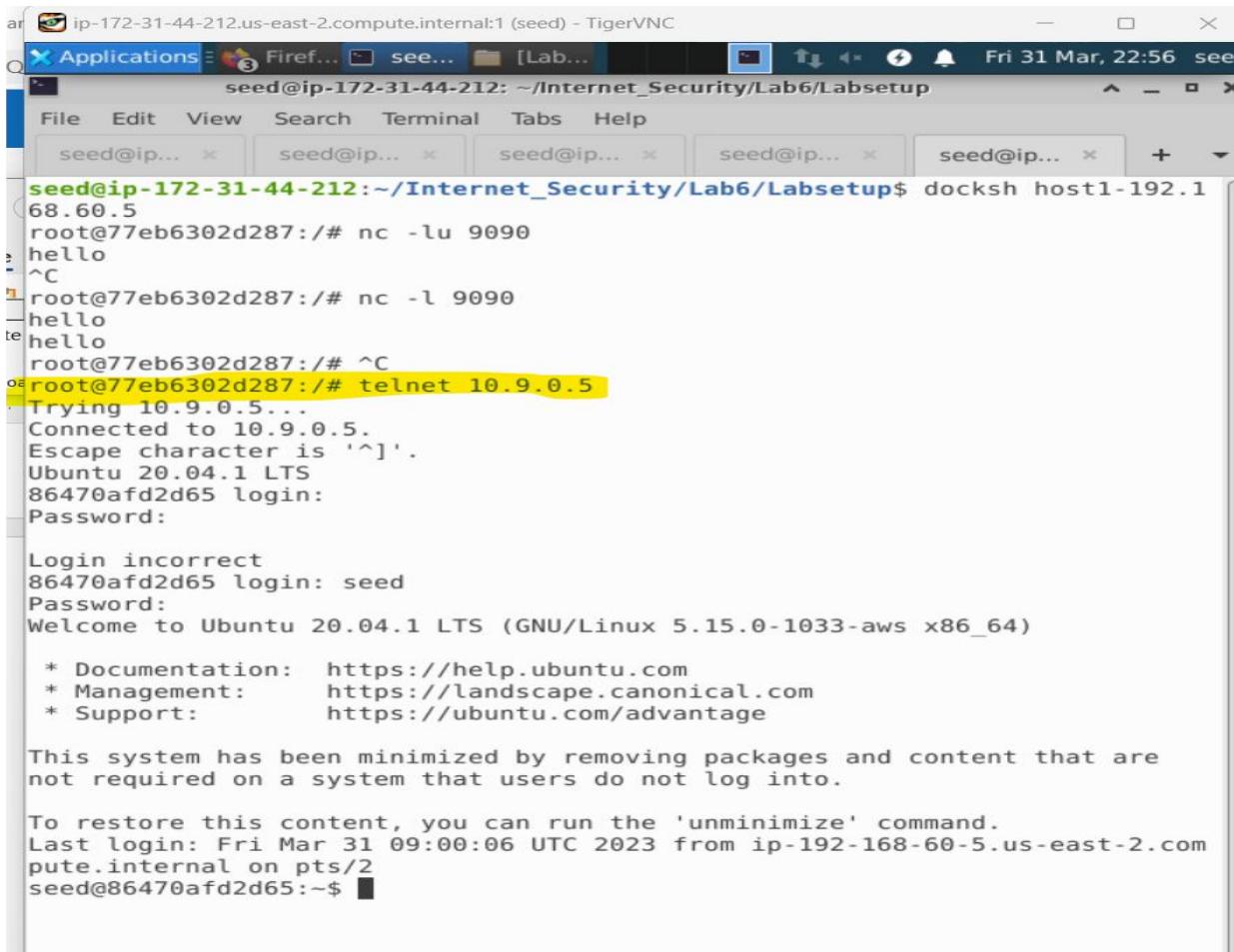
```
root@ad4423d4610e:/# iptables -A FORWARD -p tcp -j DROP  
root@ad4423d4610e:/# iptables -P FORWARD ACCEPT  
root@ad4423d4610e:/# iptables -L -n  
Chain INPUT (policy ACCEPT)  
target     prot opt source          destination  
  
Chain FORWARD (policy ACCEPT)  
target     prot opt source          destination  
ACCEPT    tcp  --  0.0.0.0/0        192.168.60.5      tcp dpt:23 fl  
ags:0x17/0x02 ctstate NEW  
ACCEPT    tcp  --  0.0.0.0/0        0.0.0.0/0        tcp flags:0x1  
7/0x02 ctstate NEW  
ACCEPT    tcp  --  0.0.0.0/0        0.0.0.0/0        ctstate RELAT  
ED,ESTABLISHED  
DROP     tcp  --  0.0.0.0/0        0.0.0.0/0  
  
Chain OUTPUT (policy ACCEPT)  
target     prot opt source          destination  
root@ad4423d4610e:/#
```

Here the rules are just set up. From the above screenshot we can see the conntrack module added some flag and related established and so the default policy in this forward accept

```
root@ad4423d4610e:/# conntrack -L
icmp      1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=19
2.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@ad4423d4610e:/#
```

Now we let the module track automatically with these rules.

Now lets try “telnet 10.9.0.5” from the inside host one to the external host



The screenshot shows a terminal window titled "seed@ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC". The terminal session is running under the user "seed" on the host "ip-172-31-44-212". The command "docksh host1-192.1.68.60.5" was run, followed by "nc -lu 9090". A connection attempt was made from "root@77eb6302d287" on port 9090. The terminal then shows a telnet session starting with "Trying 10.9.0.5...". The connection was successful, and the user was prompted for a password. The password was entered as "seed". The system responded with "Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)". It also provided documentation links for documentation, management, and support. At the end, it mentioned that the system has been minimized and provided instructions to restore content using the 'unminimize' command.

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host1-192.1.68.60.5
root@77eb6302d287:/# nc -lu 9090
hello
^C
root@77eb6302d287:/# nc -l 9090
hello
hello
root@77eb6302d287:/# ^C
root@77eb6302d287:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
86470af2d65 login:
Password:

Login incorrect
86470af2d65 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Mar 31 09:00:06 UTC 2023 from ip-192-168-60-5.us-east-2.compute.internal on pts/2
seed@86470af2d65:~$
```

And for the outside host it can only telnet into a host one inside host one

```
File Edit View Search Terminal Tabs Help
seed@ip... × seed@ip... × seed@ip... × seed@ip... × seed@ip... × +
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host A-10.9
.0.5
Error: No such container: host
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh hostA-10.9.
0.5
root@86470afd2d65:/# nc -u 192.168.60.5 9090
hello
^C
root@86470afd2d65:/# nc 192.168.60.5 9090
hello
hello
^C
root@86470afd2d65:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^].
Ubuntu 20.04.1 LTS
77eb6302d287 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Mar 31 08:56:04 UTC 2023 from ip-10-9-0-5.us-east-2.compute
.internal on pts/2
seed@77eb6302d287:~$ exit
logout
Connection closed by foreign host.
root@86470afd2d65:/# █
```

We can try other host inside the network

```
root@86470afd2d65:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
root@86470afd2d65:/#
```

We can see it's not allowed, which is enforced by the rule but the rule, destination with the telnet service is allowed.

For any other service this should also be disabled, but for the inner host to the outside host any service is allowed, so you can try tcp server, we can use netcat to set up tcp server udp server.

We are going to try tcp server on this host

```
seed@ip-172-31-44-212: ~/Internet_Security/Lab0/LabSetup
File Edit View Search Terminal Tabs Help
seed@ip... <--> seed@ip... <--> seed@ip... <--> seed@ip... <--> seed@ip... + -
root@77eb6302d287:/# nc -lu 9090
hello
^C
root@77eb6302d287:/# nc -l 9090
hello
hello
root@77eb6302d287:/# ^C
root@77eb6302d287:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5...
Escape character is '^]'.
Ubuntu 20.04.1 LTS
86470af2d65 login:
Password:
Login incorrect
86470af2d65 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Mar 31 09:00:06 UTC 2023 from ip-192-168-60-5.us-east-2.com
pute.internal on pts/2
seed@86470af2d65:~$ ls
seed@86470af2d65:~$ exit
logout
Connection closed by foreign host.
root@77eb6302d287:/# nc -l 9090
```

Then on the outside host try to connect

```
root@86470af2d65:/# nc 192.168.60.5 9090
```

```
root@77eb6302d287:/# nc -l 9090
^C
root@77eb6302d287:/#
```

```
root@86470af2d65:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
root@86470af2d65:/# nc 192.168.60.5 9090
helloroot@86470af2d65:/# hello
```

And now on the host 1 we want to access netcat udp server.

Want to connect to this netcat UDP server

```
root@77eb6302d287:/# nc -u 10.9.0.5 9090
hello
root@77eb6302d287:/#
```

We type hello on host and we have received hello

```
root@77eb6302d287:/# nc -u 10.9.0.5 9090
hello
root@77eb6302d287:/#
```

Rule allows internal host to visit any external server and we are able to see it worked we received hello.

Here we use the contract as it explains the arrangement distribution of each approach. The disadvantage of contracts is that it consumes more resources because it need to keep the connection status, however the rules are not strict as the connection status

```
root@ad4423d4610e:/# conntrack -L
icmp      1 29 src=192.168.60.11 dst=192.168.60.5 type=8 code=0 id=34 src=19
2.168.60.5 dst=192.168.60.11 type=0 code=0 id=34 use=1
conntrack v1.4.5 (conntrack-tools): 1 flow entries have been shown.
root@ad4423d4610e:/# iptables -F
root@ad4423d4610e:/# 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@ad4423d4610e:/#
```

```
root@ad4423d4610e:/# ipatbles -P ACCEPT
bash: ipatbles: command not found
root@ad4423d4610e:/# iptables -p ACCEPT
iptables v1.8.4 (legacy): unknown protocol "accept" specified
Try `iptables -h' or 'iptables --help' for more information.
root@ad4423d4610e:/# iptables -P FORWARD ACCEPT
root@ad4423d4610e:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --d
port 23 --syn -j ACCEPT
root@ad4423d4610e:/# ■
root@ad4423d4610e:/# iptables -P FORWARD ACCEPT
root@ad4423d4610e:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --d
port 23 --syn -j ACCEPT
root@ad4423d4610e:/# iptables -A FORWARD -i eth0 -p tcp --syn -j DROP
root@ad4423d4610e:/# ■
```

How are the other packet will go in or go out or pass through the router

```
root@ad4423d4610e:/# iptables -A FORWARD -i eth0 -p tcp --syn -j DROP
root@ad4423d4610e:/# iptables -A FORWARD -p tcp -j ACEEPT
iptables v1.8.4 (legacy): Couldn't load target 'ACEEPT':No such file or d
ectory
```

```
Try `iptables -h' or 'iptables --help' for more information.
root@ad4423d4610e:/# iptables -A FORWARD -p tcp -j ACCEPT
root@ad4423d4610e:/# ■
```

```
root@ad4423d4610e:/# iptables -A FORWARD -p tcp -j ACCEPT
root@ad4423d4610e:/# iptables -P FORWARD ACCEPT
root@ad4423d4610e:/# 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 fl
ags:0x17/0x02
DROP     tcp  --  0.0.0.0/0            0.0.0.0/0          tcp flags:0x1
7/0x02
ACCEPT    tcp  --  0.0.0.0/0            0.0.0.0/0
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ad4423d4610e:/#
```

Now we can test the telnet

```
root@86470afd2d65:/# telnet 192.168.60.6
Trying 192.168.60.6...
^C
root@86470afd2d65:/#
```

```
root@86470afd2d65:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
77eb6302d287 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1033-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Mar 31 22:59:28 UTC 2023 from ip-10-9-0-5.us-east-2.compute
.internal on pts/2
seed@77eb6302d287:~$
```

The screenshot shows a terminal window with multiple tabs. The active tab displays the following command-line session:

```
root@ad4423d4610e:/# iptables -P ACCEPT
bash: iptables: command not found
root@ad4423d4610e:/# iptables -p ACCEPT
iptables v1.8.4 (legacy): unknown protocol "accept" specified
Try `iptables -h` or 'iptables --help' for more information.
root@ad4423d4610e:/# iptables -P FORWARD ACCEPT
root@ad4423d4610e:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 --syn -j ACCEPT
root@ad4423d4610e:/# iptables -A FORWARD -i eth0 -p tcp --syn -j DROP
root@ad4423d4610e:/# iptables -A FORWARD -p tcp -j ACCEPT
iptables v1.8.4 (legacy): Couldn't load target 'ACEEPT':No such file or directory
Try `iptables -h` or 'iptables --help' for more information.
root@ad4423d4610e:/# iptables -A FORWARD -p tcp -j ACCEPT
root@ad4423d4610e:/# iptables -P FORWARD ACCEPT
root@ad4423d4610e:/# iptables -L -n
Chain INPUT (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 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@ad4423d4610e:/# iptables -F
root@ad4423d4610e:/# 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@ad4423d4610e:/#
```

Task 4: Limiting Network Traffic

We can also limit the packets that can pass through the firewall and this time using limit method or module of the iptables

```
root@ad4423d4610e:/# 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]
      iptables -D chain rulenum [options]
      iptables -[LS] [chain [rulenum]] [options]
      iptables -[FZ] [chain] [options]
      iptables -[NX] chain
      iptables -E old-chain-name new-chain-name
      iptables -P chain target [options]
      iptables -h (print this help information)
```

Commands:

```
root@ad4423d4610e:/# iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/mi
nute --limit-burst 5 -j ACCEPT
root@ad4423d4610e:/#
```

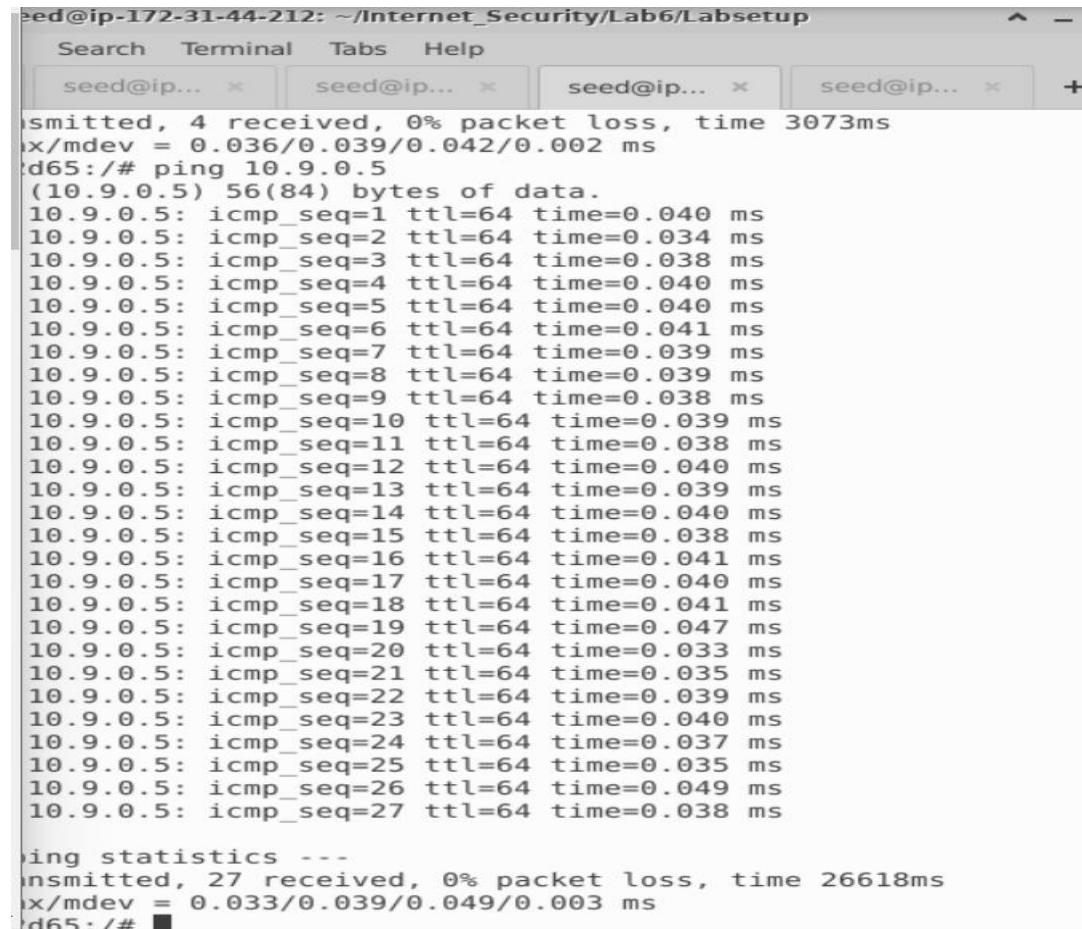
Now lets ping ping from inside host 1 to external host A

```
root@86470af2d65:/# 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=64 time=0.040 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=0.040 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=64 time=0.038 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=64 time=0.036 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=64 time=0.035 ms
64 bytes from 10.9.0.5: icmp_seq=6 ttl=64 time=0.035 ms
64 bytes from 10.9.0.5: icmp_seq=7 ttl=64 time=0.033 ms
64 bytes from 10.9.0.5: icmp_seq=8 ttl=64 time=0.046 ms
64 bytes from 10.9.0.5: icmp_seq=9 ttl=64 time=0.040 ms
64 bytes from 10.9.0.5: icmp_seq=10 ttl=64 time=0.045 ms
64 bytes from 10.9.0.5: icmp_seq=11 ttl=64 time=0.043 ms
64 bytes from 10.9.0.5: icmp_seq=12 ttl=64 time=0.038 ms
64 bytes from 10.9.0.5: icmp_seq=13 ttl=64 time=0.039 ms
64 bytes from 10.9.0.5: icmp_seq=14 ttl=64 time=0.039 ms
64 bytes from 10.9.0.5: icmp_seq=15 ttl=64 time=0.039 ms
64 bytes from 10.9.0.5: icmp_seq=16 ttl=64 time=0.043 ms
64 bytes from 10.9.0.5: icmp_seq=17 ttl=64 time=0.040 ms
64 bytes from 10.9.0.5: icmp_seq=18 ttl=64 time=0.040 ms
^C
--- 10.9.0.5 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17384ms
rtt min/avg/max/mdev = 0.033/0.039/0.046/0.003 ms
root@86470af2d65:/#
```

We are getting the response from the host A

Those packets not in the first rule will be dropped by the 2nd rule. Finally these packets our passed where we see continuously get this response of dropping packets

```
root@ad4423d4610e:/# iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/mi  
nute --limit-burst 5 -j ACCEPT  
root@ad4423d4610e:/# iptables -A FORWARD -s 10.9.0.5 -j DROP
```



The screenshot shows a terminal window with four tabs labeled 'seed@ip...', each showing a different session. The main window displays the output of a ping command to 10.9.0.5. The output shows 27 ICMP packets sent, 0% packet loss, and a total time of 26618ms. The 'rx/mdev' value is 0.033/0.039/0.049/0.003 ms. The 'tx/mdev' value is 0.036/0.039/0.042/0.002 ms.

```
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup
Search Terminal Tabs Help
seed@ip... × seed@ip... × seed@ip... × seed@ip... × +
transmitted, 4 received, 0% packet loss, time 3073ms
rx/mdev = 0.036/0.039/0.042/0.002 ms
d65:/# ping 10.9.0.5
(10.9.0.5) 56(84) bytes of data.
10.9.0.5: icmp_seq=1 ttl=64 time=0.040 ms
10.9.0.5: icmp_seq=2 ttl=64 time=0.034 ms
10.9.0.5: icmp_seq=3 ttl=64 time=0.038 ms
10.9.0.5: icmp_seq=4 ttl=64 time=0.040 ms
10.9.0.5: icmp_seq=5 ttl=64 time=0.040 ms
10.9.0.5: icmp_seq=6 ttl=64 time=0.041 ms
10.9.0.5: icmp_seq=7 ttl=64 time=0.039 ms
10.9.0.5: icmp_seq=8 ttl=64 time=0.039 ms
10.9.0.5: icmp_seq=9 ttl=64 time=0.038 ms
10.9.0.5: icmp_seq=10 ttl=64 time=0.039 ms
10.9.0.5: icmp_seq=11 ttl=64 time=0.038 ms
10.9.0.5: icmp_seq=12 ttl=64 time=0.040 ms
10.9.0.5: icmp_seq=13 ttl=64 time=0.039 ms
10.9.0.5: icmp_seq=14 ttl=64 time=0.040 ms
10.9.0.5: icmp_seq=15 ttl=64 time=0.038 ms
10.9.0.5: icmp_seq=16 ttl=64 time=0.041 ms
10.9.0.5: icmp_seq=17 ttl=64 time=0.040 ms
10.9.0.5: icmp_seq=18 ttl=64 time=0.041 ms
10.9.0.5: icmp_seq=19 ttl=64 time=0.047 ms
10.9.0.5: icmp_seq=20 ttl=64 time=0.033 ms
10.9.0.5: icmp_seq=21 ttl=64 time=0.035 ms
10.9.0.5: icmp_seq=22 ttl=64 time=0.039 ms
10.9.0.5: icmp_seq=23 ttl=64 time=0.040 ms
10.9.0.5: icmp_seq=24 ttl=64 time=0.037 ms
10.9.0.5: icmp_seq=25 ttl=64 time=0.035 ms
10.9.0.5: icmp_seq=26 ttl=64 time=0.049 ms
10.9.0.5: icmp_seq=27 ttl=64 time=0.038 ms

ping statistics ---
transmitted, 27 received, 0% packet loss, time 26618ms
rx/mdev = 0.033/0.039/0.049/0.003 ms
d65:/#
```

We can see it does not work as expected.

Which means this limit takes effect after we add the second rule without the signal. It does not work why is that?

Reason: Those packets does not match this first rule without this second rule somehow they went through this router because they were not stopped for those packets not satisfied in this rule that is why we kept getting those packet just like no limit

```
root@86470afd2d65:/# iptables -F
root@86470afd2d65:/# 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@86470afd2d65:/# █
```

Task 5: Load Balancing

a) Using the nth mode (round-robin)

We need to add one rule before that we need to run the three servers host1, host2, host3

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup
File Edit View Search Terminal Tabs Help
S... X +
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host1-192.1
68.60.5
root@77eb6302d287:/# nc -luk 8080
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup
File Edit View Search Terminal Tabs Help
S... X +
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host2-192.1
68.60.6
root@b11c982b0c89:/# host1-192.168.60.5
bash: host1-192.168.60.5: command not found
root@b11c982b0c89:/# nc -luk 8080
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup
File Edit View Search Terminal Tabs Help
S... X +
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host3-192.1
68.60.7
root@5ee4fbca3e25:/# nc -luk 8080
```

```

root@ad4423d4610e:/# iptables -t nat -A PREROUTING -p --dport 8080 -m statis
tic --mode nth --every 3 --packet 0 -j DNAT --to-destination 192.168.60.5:
8080
iptables v1.8.4 (legacy): unknown protocol "--dport" specified
Try `iptables -h' or 'iptables --help' for more information.
root@ad4423d4610e:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m s
tatistic --mode nth --every 3 --packet 0 -j DNAT --to-destination 192.168.6
0.5:8080
root@ad4423d4610e:/# ■

```

```

root@86470afd2d65:/# echo hello | nc -u 10.9.0.11 8080^C
root@86470afd2d65:/# nc -luk 8080
hello

```

```

root@86470afd2d65:/# nc -luk 8080
hello

```

Every three packet pixel first packet, here those packets do not match the rule will continue on their journey so it looks like this packets do not match and they will not be modifies or blocked and they will come to this host.

We need to add two more rules, here if every three packet the first packet is send to a host one the we left only two so we need to change it to every two we pick the first one

```

root@ip-172-31-44-212.us-east-2.compute.internal:~ (seed) - TigerVNC
Applications Firefox seed@ip-172-31-44-212... [Labsetup - File Manager]
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup
File Edit View Search Terminal Tabs Help
seed@ip-172-31... seed@ip-172-31... seed@ip-172-31... seed@ip-172-31... seed@ip-172-31... seed@ip-172-31... seed@ip-172-31...
limit match options:
--limit avg
--limit-burst number
--limit-burst default
--limit-burst number /second
--limit-burst /second /day postfixed
--limit-burst number /second /day postfixed
root@ad4423d4610e:/# iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/minute --limit-burst 5 -j ACCEPT
root@ad4423d4610e:/# iptables -A FORWARD -s 10.9.0.5 -j DROP
root@ad4423d4610e:/# iptables -F
root@ad4423d4610e:/# 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@ad4423d4610e:/# iptables -t nat -A PREROUTING -p udp --dport 8080  \^C
root@ad4423d4610e:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --packet 0 -j DNAT --to-destination 192.168.60.5:8080
iptables v1.8.4 (legacy): unknown protocol "--dport" specified
Try `iptables -h' or 'iptables --help' for more information.
root@ad4423d4610e:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --packet 0 -j DNAT --to-destination 192.168.60.5:8080
root@ad4423d4610e:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --packet 0 -j DNAT --to-destination 192.168.60.6:8080
iptables v1.8.4 (legacy): unknown option "--to-destination"
Try `iptables -h' or 'iptables --help' for more information.
root@ad4423d4610e:/# 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@ad4423d4610e:/# 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
root@ad4423d4610e:/# 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@ad4423d4610e:/# ■

```

The table is inside the NAT table

```

root@ad4423d4610e:/# 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:127.0.0.11:35949
DNAT      udp  --  0.0.0.0/0      127.0.0.11      udp dpt:53 to:127.0.0.11:53054

Chain DOCKER_POSTROUTING (1 references)
target    prot opt source          destination
SNAT      tcp  --  127.0.0.11     0.0.0.0/0      tcp spt:35949 to::53
SNAT      udp  --  127.0.0.11     0.0.0.0/0      udp spt:53054 to::53
root@ad4423d4610e:/#

```

```

root@86470afd2d65:/# echo hello | nc -u 10.9.0.11 8080
^C
root@86470afd2d65:/# 

```

```

root@86470afd2d65:/# nc -luk 8080
hello
hello

```

Here we have a Single udp packet u can find the maximum payload for udp packet

```

root@ad4423d4610e:/# echo "hello hello hello" | nc -u 10.9.0.11 8080
root@ad4423d4610e:/# 

```

```

ip-172-31-44-212.us-east-2.compute.internal1 (seed) - TigerVNC
Applications Firefox seed@ip-172-31-44-212... [Labsetup - File Manager]
File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212... seed@ip-172-31-44-212... seed@ip-172-31-44-212... seed@ip-172-31-44-212... seed@ip-172-31-44-212...
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host2-192.168.60.6
root@b11c982b0c89:/# host1-192.168.60.5
bash: host1-192.168.60.5: command not found
root@b11c982b0c89:/# nc -luk 8080
^C
root@b11c982b0c89:/# nc -luk 8080
hello
hello hello

root@ad4423d4610e:/# echo "hello hello hello" | nc -u 10.9.0.11 8080
root@ad4423d4610e:/# echo "hello1" | nc -u 10.9.0.11 8080
root@ad4423d4610e:/# echo "hello2" | nc -u 10.9.0.11 8080
root@ad4423d4610e:/#

```

Everytime we run the code above the source port number is chosen randomly, so we can use random source of port we can use also wireshark

```
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup
File Edit View Search Terminal Help
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host2-192.168.60
.6
root@b11c982b0c89:/# nc -luk 8080
^C
root@b11c982b0c89:/# nc -luk 8080
hello hello hello
hello2
```

```
root@ad4423d4610e:/# echo " hello3" | nc -u 10.9.0.11 8080
root@ad4423d4610e:/#
```

```
seed@ip-172-31-44-212: ~/Internet_Security/Lab6/Labsetup
File Edit View Search Terminal Help
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host2-192.168.60
.6
root@b11c982b0c89:/# nc -luk 8080
hello hello hello
hello3
```

```
root@ad4423d4610e:/# nc -u 10.9.0.11 8080
hi1
hi2
hi3
```

Every three packet pixel first packet, here those packets do not match the rule will continue on their journey so it looks like this packets do not match and they will not be modified or blocked and they will come to this host.

We need to add two more rules, here if every three packet the first packet is send to a host one the we left only two so we need to change it to every two we pick the first one

```
root@b11c982b0c89:/# nc -luk 8080
hello
hello
hello1
hi1
hi2
hi3
```

b) Using Random mode

We used the following command

```
1)iptables -t nat -A PREROUTING
-p udp --dport 8080 -m statistic --mode random --probability
0.33333 -j DNAT --to-destination 192.168.60.5:8080
2)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
3) /# iptables -t nat -A PREROUTING
-p udp --dport 8080 -m statistic --mode random --probability
0.33333 -j DNAT --to-destination 192.168.60.5:8080
root@ad4423d4610e:/# iptables -t nat -L -n --line-numbers
```

In the pre routing chain we are able to see three rules

```

root@ad4423d4610e:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 0.33333 -j DNAT --to-destination 192.168.60.5:8080
root@ad4423d4610e:/# 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@ad4423d4610e:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 1 -j DNAT --to-destination 192.168.60.7:8080
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
4   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
5   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
6   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:127.0.0.11:35949
2   DNAT        udp  --  0.0.0.0/0      127.0.0.11      udp dpt:53 to:127.0.0.11:53054

Chain DOCKER_POSTROUTING (1 references)
num  target     prot opt source          destination
1   SNAT        tcp  --  127.0.0.11    0.0.0.0/0          tcp spt:35949 to::53
2   SNAT        udp  --  127.0.0.11    0.0.0.0/0          udp spt:53054 to::53
root@ad4423d4610e:#

```

```

seed@ip-172-31-... ✘ seed@ip-172-31-... ✘ seed@ip-172-31-... ✘ seed@ip-172-31-... ✘ seed@ip-172-31-...
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host2-192.168.60.6
root@b11c982b0c89:/# host1-192.168.60.5
bash: host1-192.168.60.5: command not found
root@b11c982b0c89:/# nc -luk 8080
^C
root@b11c982b0c89:/# nc -luk 8080
hello hello hello

File Edit View Search Terminal Tabs Help
seed@ip-172-31-... ✘ seed@ip-172-31-... ✘ seed@ip-172-31-... ✘ seed@ip-172-31-... ✘ seed@ip-172-31-...
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host1-192.168.60.5
root@77eb6302d287:/# nc -luk 8080
hello

```

```

root@ad4423d4610e:/# nc -u 10.9.0.11 8080
hi1
hi2
hi3

```

```

root@ad4423d4610e:/# nc -u 10.9.0.11 8080
hi1
hi2
hi3
hi4
hi5
hi6

```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host2-192.168.60.6
root@b11c982b0c89:/# host1-192.168.60.5
bash: host1-192.168.60.5: command not found
root@b11c982b0c89:/# nc -luk 8080
^C
root@b11c982b0c89:/# nc -luk 8080
hello hello hello
```

```
File Edit View Search Terminal Apps Help
seed@ip-172-31-44-212:~/Internet_Security/Lab6/Labsetup$ docksh host3-192.168.60.7
root@5ee4fbca3e25:/# nc -luk 8080
```