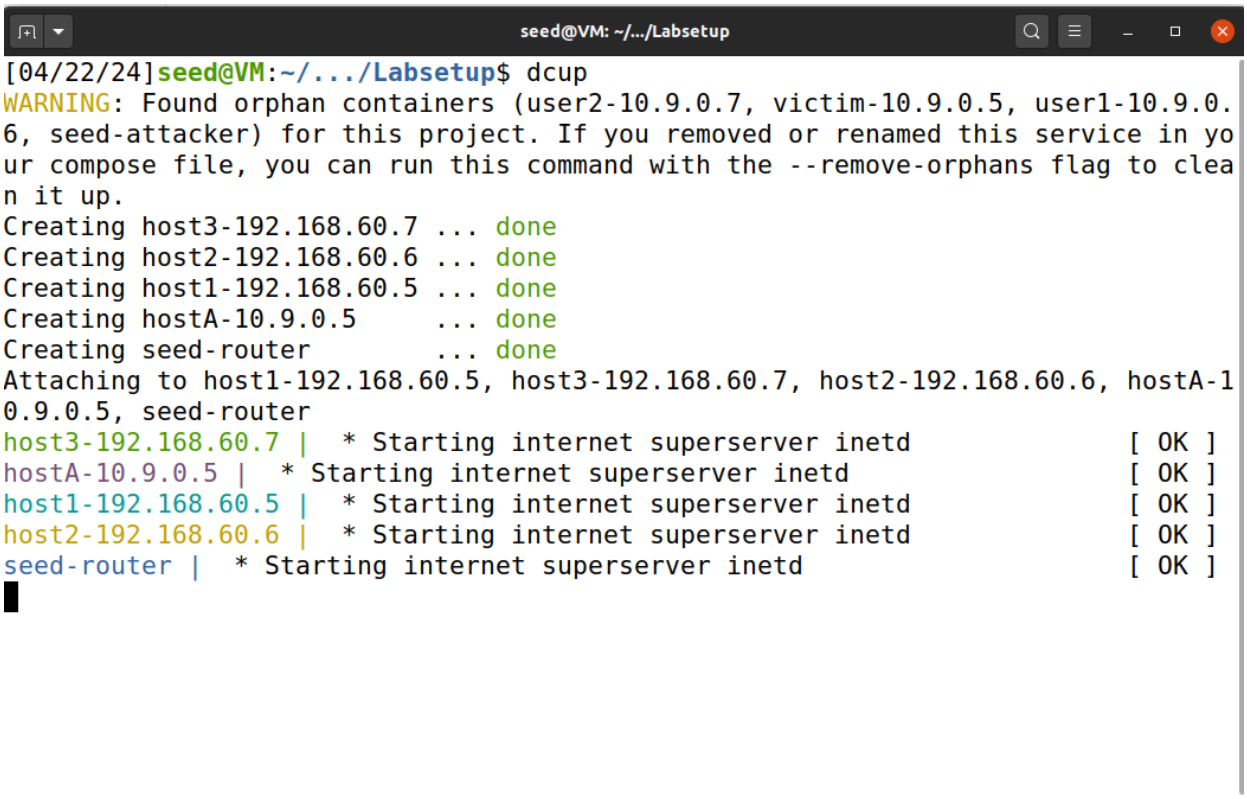
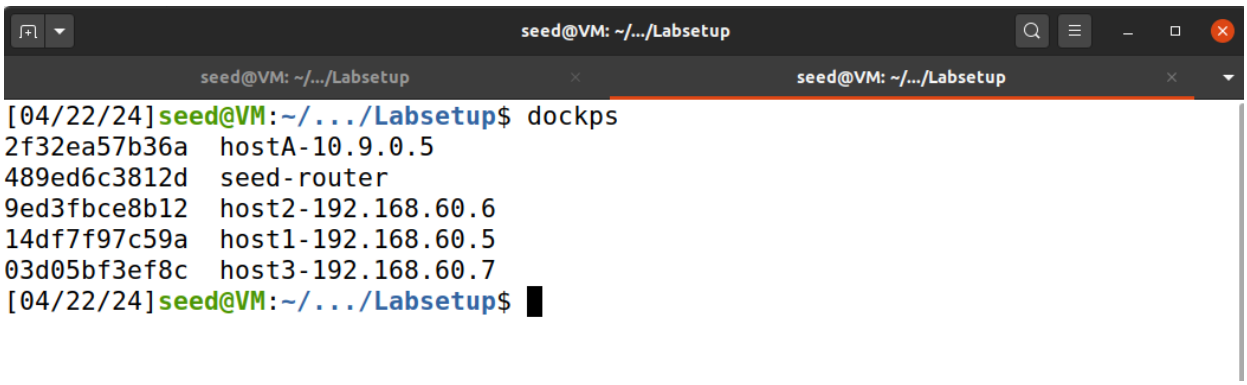
This lab exercise's main goals are to achieve two learning objectives: understanding firewall operation and setting up a basic network firewall. First, a stateless packet-filtering firewall will be created, which will assess packets and determine if they should be passed or discarded based on pre-established firewall rules. This will provide us with an overview of the fundamental operations of firewalls. It's crucial to remember that Linux comes with an integrated firewall called iptables that is based on Netfilter. Netfilter and firewall-related topics are the main topics of this lab.

## Lab setup

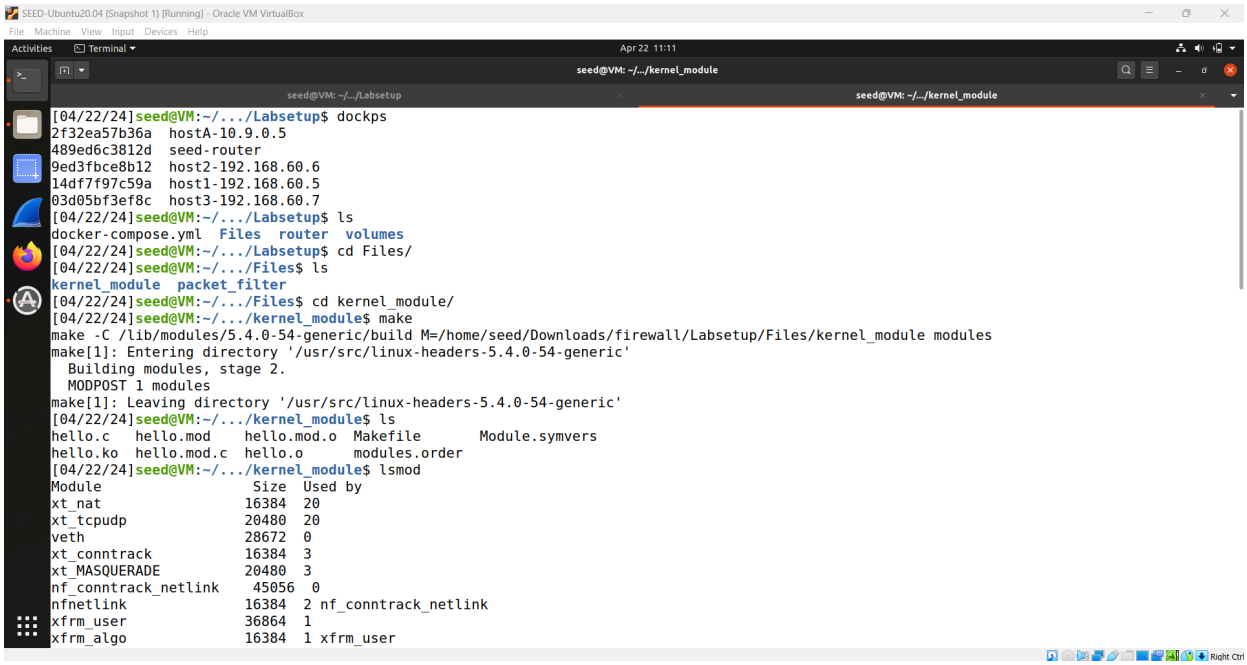


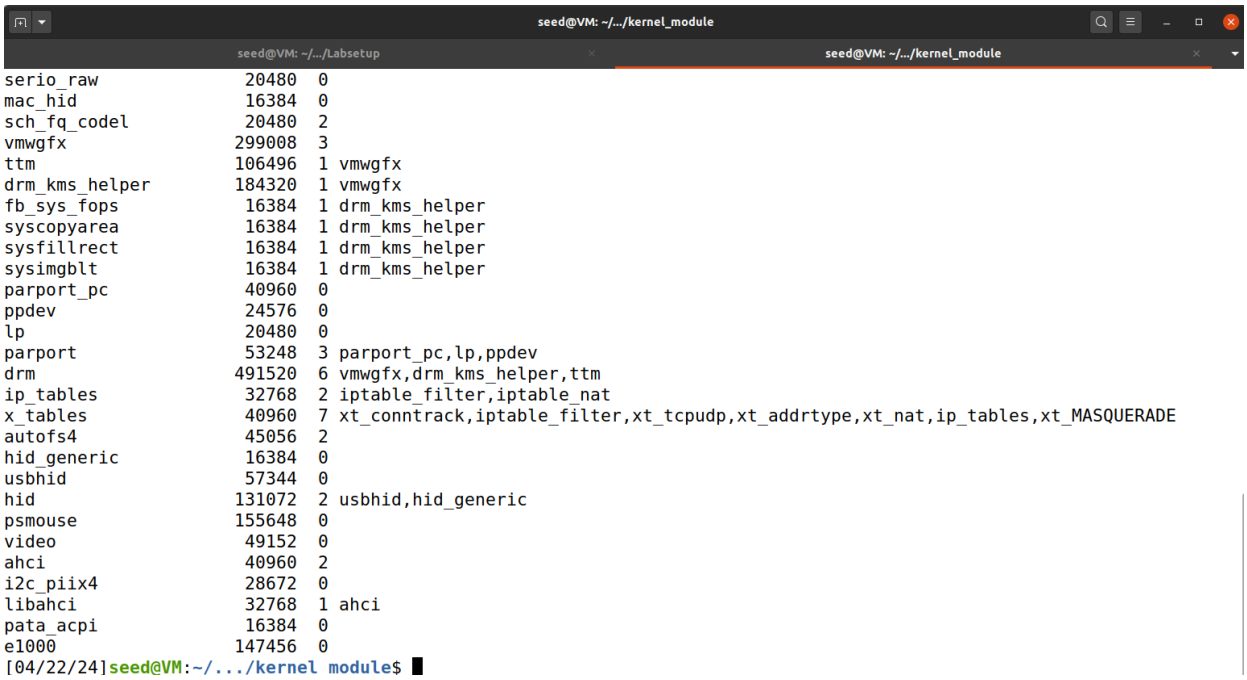




Task 1.a:

The 'Make' command, which automatically determines which parts of a complex programme require recompilation and issues the necessary commands, must be run before we can proceed. Run the 'ls' command first, then 'Make' to view the output of the Make command. A feature known as the Loadable Kernel Module (LKM) makes it possible to add new modules to the kernel while it is running without having to restart the machine or rebuild the kernel. An LKM can be used to implement packet filtering as part of the firewall capability. This exercise will aid in our familiarization with LKM.

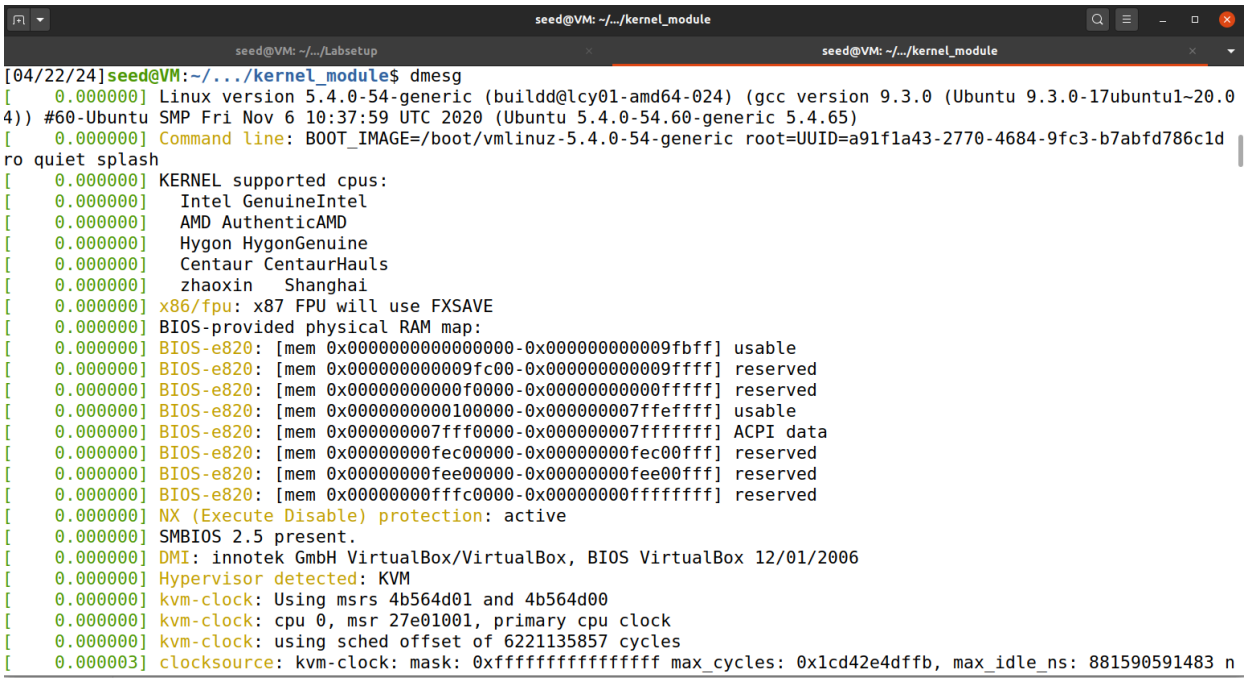
A basic loadable kernel module with the code provided prints "Hello World!" upon loading and "Bye-bye World!" upon removal from the kernel. These messages are printed into the /var/log/syslog file rather than appearing on the screen. We can use the "dmesg" command to view the messages.

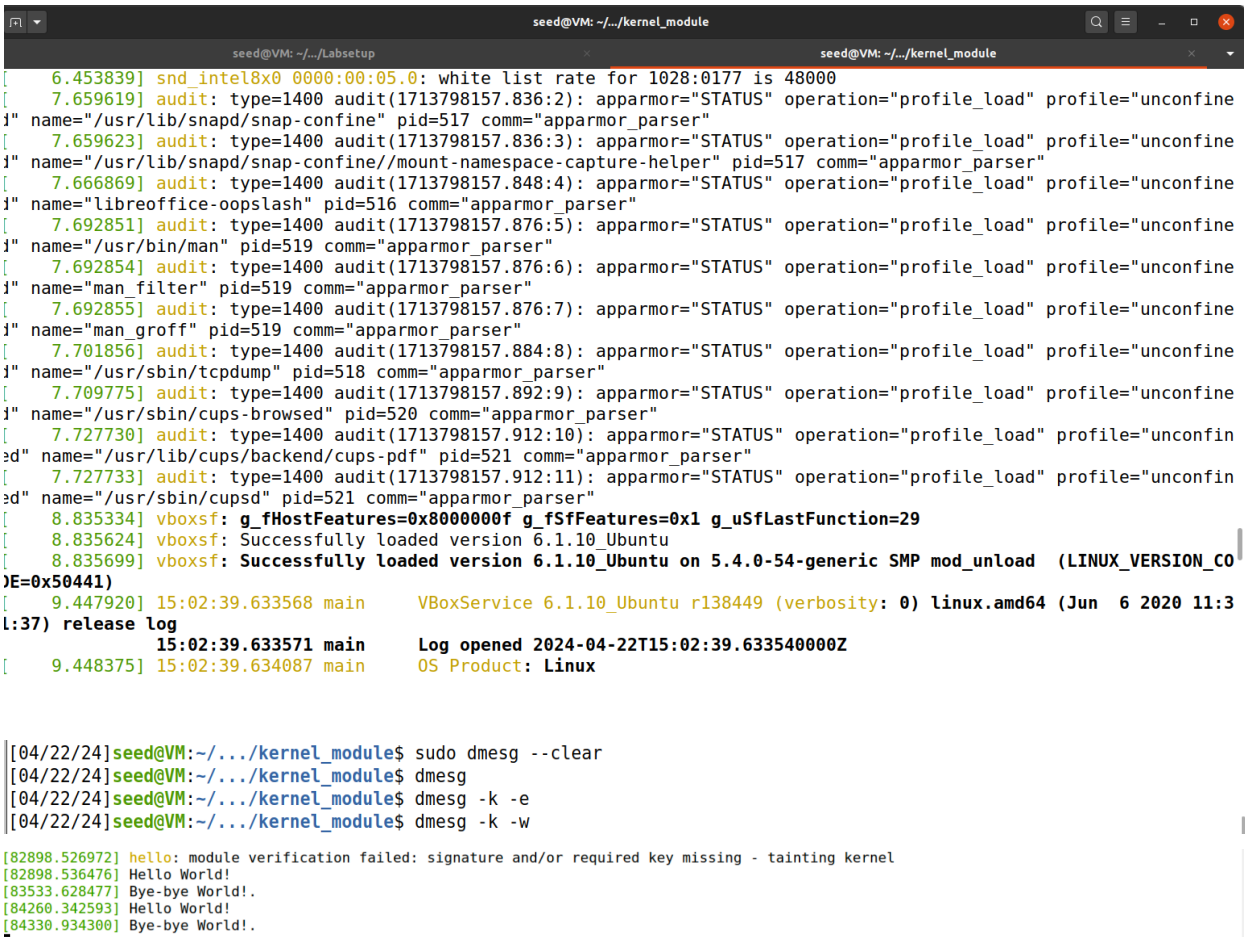





We insert the module hello.ko


We use the command dmesg to view the packet information in the terminal


seed@VM: ~/.../kernel_module
seed@VM: ~/.../Labsetup
seed@VM: ~/.../kernel_module
[04/22/24]seed@VM:~/.../kernel_module$ dmesg
[ 0.000000] Linux version 5.4.0-54-generic (buildd@lcy01-amd64-024) (gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1~20.04)) #60-Ubuntu SMP Fri Nov 6 10:37:59 UTC 2020 (Ubuntu 5.4.0-54.60-generic 5.4.65)
[ 0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.4.0-54-generic root=UUID=a91f1a43-2770-4684-9fc3-b7abfd786c1d ro quiet splash
[ 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: x87 FPU will use FXSAVE
[ 0.000000] BIOS-provided physical RAM map:
[ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
[ 0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
[ 0.000000] BIOS-e820: [mem 0x0000000000100000-0x00000007ffefffff] usable
[ 0.000000] BIOS-e820: [mem 0x00000007fff0000-0x00000007ffffffff] ACPI data
[ 0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[ 0.000000] NX (Execute Disable) protection: active
[ 0.000000] SMBIOS 2.5 present.
[ 0.000000] DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[ 0.000000] Hypervisor detected: KVM
[ 0.000000] kvm-clock: Using msrs 4b564d01 and 4b564d00
[ 0.000000] kvm-clock: cpu 0, msr 27e01001, primary cpu clock
[ 0.000000] kvm-clock: using sched offset of 6221135857 cycles
[ 0.000003] clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 881590591483 n


seed@VM: ~/.../kernel_module
seed@VM: ~/.../Labsetup
seed@VM: ~/.../kernel_module
[ 6.453839] snd_intel8x0 0000:00:05.0: white list rate for 1028:0177 is 48000
[ 7.659619] audit: type=1400 audit(1713798157.836:2): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/snapd/snap-confine" pid=517 comm="apparmor_parser"
[ 7.659623] audit: type=1400 audit(1713798157.836:3): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/snapd/snap-confine//mount-namespace-capture-helper" pid=517 comm="apparmor_parser"
[ 7.666869] audit: type=1400 audit(1713798157.848:4): apparmor="STATUS" operation="profile_load" profile="unconfined" name="libreoffice-oopslash" pid=516 comm="apparmor_parser"
[ 7.692851] audit: type=1400 audit(1713798157.876:5): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/bin/man" pid=519 comm="apparmor_parser"
[ 7.692854] audit: type=1400 audit(1713798157.876:6): apparmor="STATUS" operation="profile_load" profile="unconfined" name="man_filter" pid=519 comm="apparmor_parser"
[ 7.692855] audit: type=1400 audit(1713798157.876:7): apparmor="STATUS" operation="profile_load" profile="unconfined" name="man_groff" pid=519 comm="apparmor_parser"
[ 7.701856] audit: type=1400 audit(1713798157.884:8): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/tcpdump" pid=518 comm="apparmor_parser"
[ 7.709775] audit: type=1400 audit(1713798157.892:9): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/cups-browsed" pid=520 comm="apparmor_parser"
[ 7.727730] audit: type=1400 audit(1713798157.912:10): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/cups/backend/cups-pdf" pid=521 comm="apparmor_parser"
[ 7.727733] audit: type=1400 audit(1713798157.912:11): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/cupsd" pid=521 comm="apparmor_parser"
[ 8.835334] vboxsf: g_fHostFeatures=0x8000000f g_fSfFeatures=0x1 g_uSfLastFunction=29
[ 8.835624] vboxsf: Successfully loaded version 6.1.10_Ubuntu
[ 8.835699] vboxsf: Successfully loaded version 6.1.10_Ubuntu on 5.4.0-54-generic SMP mod_unload (LINUX_VERSION_CODE=0x50441)
[ 9.447920] 15:02:39.633568 main VBoxService 6.1.10_Ubuntu r138449 (verbosity: 0) linux.amd64 (Jun 6 2020 11:31:37) release log
15:02:39.633571 main Log opened 2024-04-22T15:02:39.633540000Z
[ 9.448375] 15:02:39.634087 main OS Product: Linux
[04/22/24]seed@VM:~/.../kernel_module$ sudo dmesg --clear
[04/22/24]seed@VM:~/.../kernel_module$ dmesg
[04/22/24]seed@VM:~/.../kernel_module$ dmesg -k -e
[04/22/24]seed@VM:~/.../kernel_module$ dmesg -k -w
[82898.526972] hello: module verification failed: signature and/or required key missing - tainting kernel
[82898.536476] Hello World!
[83533.628477] Bye-bye World!.
[84260.342593] Hello World!
[84330.934300] Bye-bye World!.

Using the command dmesg -k -w, the message included in the packets is shown on the terminal.
We made the module print "Hello world" when we first presented it.
The module we introduced can be successfully expelled by typing sudo rmmod hello, which prints "Bye bye World," indicating that the module has been removed.

Task 1.b

Subtask 1: The purpose of Netfilter is to enable packet manipulation by authorised users. It accomplishes this by introducing hooks into the Linux kernel that are positioned at different locations, such as the paths for incoming and outgoing packets. We can modify arriving packets by attaching our own programmes to the appropriate hooks within the Loadable Kernel Module (LKM). Within our programme, we are able to choose which packets to block or alter. In this job, we will create a packet filtering module using LKM and Netfilter.
The firewall policies that the module retrieves from a data structure will be used to determine whether or not to block packets. Students are permitted to hardcode firewall policies in the programme because filtering is the main focus.

We must visit the seed virtual machine and execute the make command in order to compile the seedFilter kernel module.
The creation of the seedFilter.ko file is the process's output. We may use the "dig @8.8.8.8 www.example.com" command to see if our kernel module is blocking '8.8.8.8'. This command will not produce any output when it is executed. We can view the command's output after uninstalling the module.

```
[04/22/24]seed@VM:~/.../packet_filter$ ls
Makefile  seedFilter.c
[04/22/24]seed@VM:~/.../packet_filter$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Downloads/firewall/Labsetup/Files/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CC [M]  /home/seed/Downloads/firewall/Labsetup/Files/packet_filter/seedFilter.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/Downloads/firewall/Labsetup/Files/packet_filter/seedFilter.mod.o
  LD [M]  /home/seed/Downloads/firewall/Labsetup/Files/packet_filter/seedFilter.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[04/22/24]seed@VM:~/.../packet_filter$ ls
Makefile       Module.symvers  seedFilter.ko   seedFilter.mod.c  seedFilter.o
modules.order  seedFilter.c    seedFilter.mod  seedFilter.mod.o
[04/22/24]seed@VM:~/.../packet_filter$ sudo insmod seedFilter.ko
[04/22/24]seed@VM:~/.../packet_filter$ lsmod | grep sed
Module                  Size  Used by
[04/22/24]seed@VM:~/.../packet_filter$ lsmod | grep seed
seedFilter             16384  0
```

```
[04/22/24]seed@VM:~/.../packet_filter$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=35.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=23.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=57 time=29.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=57 time=21.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=57 time=18.1 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=57 time=23.7 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=57 time=18.8 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=57 time=23.4 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=57 time=23.5 ms
^C
--- 8.8.8.8 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8024ms
rtt min/avg/max/mdev = 18.065/24.229/35.385/5.083 ms
[04/22/24]seed@VM:~/.../packet_filter$
```

```
[04/22/24]seed@VM:~/.../packet_filter$ ping 8.8.4.4
PING 8.8.4.4 (8.8.4.4) 56(84) bytes of data.
64 bytes from 8.8.4.4: icmp_seq=1 ttl=57 time=28.6 ms
64 bytes from 8.8.4.4: icmp_seq=2 ttl=57 time=27.4 ms
64 bytes from 8.8.4.4: icmp_seq=3 ttl=57 time=71.3 ms
64 bytes from 8.8.4.4: icmp_seq=4 ttl=57 time=30.3 ms
64 bytes from 8.8.4.4: icmp_seq=5 ttl=57 time=24.2 ms
^C
--- 8.8.4.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4011ms
rtt min/avg/max/mdev = 24.240/36.364/71.273/17.566 ms
[04/22/24]seed@VM:~/.../packet filter$
```

```
[04/22/24]seed@VM:~/.../packet_filter$ dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48123
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.com.        3600    IN      A       93.184.215.14

;; Query time: 80 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Apr 22 11:28:27 EDT 2024
;; MSG SIZE  rcvd: 60

[04/22/24]seed@VM:~/.../packet filter$
```

We'll use the same window that was used to run the dmesg command to install the kernel module. The "sudo insmod seedFilter.ko" command can be used to install the kernel module. The "sudo lsmod | grep -i seed" command can be used to display all loaded kernel modules and filter out those with "seedFilter" in their names. This allows us to determine whether the module is installed. We'll use the command "sudo rmmod seedFilter" to remove the module. When the command is executed, "Registering filters" will appear first, followed by "The filters are being removed" to show that the filters are being removed.

```
[88381.290189] Registering filters.
[88422.183686] *** LOCAL_OUT
[88422.183748]     127.0.0.1  --> 127.0.0.53 (UDP)
[88422.184285] *** LOCAL_OUT
[88422.184287]     10.0.2.15  --> 192.168.1.1 (UDP)
[88422.269332] *** LOCAL_OUT
[88422.269335]     127.0.0.53  --> 127.0.0.1 (UDP)
[88422.470261] *** LOCAL_OUT
[88422.470264]     127.0.0.1  --> 127.0.0.53 (UDP)
[88422.470898] *** LOCAL_OUT
[88422.470900]     127.0.0.53  --> 127.0.0.1 (UDP)
[88436.648103] *** LOCAL_OUT
[88436.648106]     10.0.2.15  --> 192.168.1.1 (UDP)
[88483.416838] *** LOCAL_OUT
[88483.416841]     127.0.0.1  --> 127.0.0.1 (UDP)
[88483.418666] *** LOCAL_OUT
[88483.418668]     10.0.2.15  --> 8.8.4.4 (UDP)
[88483.418677] *** Dropping 8.8.4.4 (UDP), port 53
[88488.455349] *** LOCAL_OUT
[88488.455352]     10.0.2.15  --> 8.8.4.4 (UDP)
[88488.455379] *** Dropping 8.8.4.4 (UDP), port 53
[88493.459034] *** LOCAL_OUT
[88493.459038]     10.0.2.15  --> 8.8.4.4 (UDP)
[88493.459059] *** Dropping 8.8.4.4 (UDP), port 53
[88554.257033] *** LOCAL_OUT
[88554.257036]     10.0.2.15  --> 192.168.1.1 (UDP)
[88554.310799] *** LOCAL_OUT
[88554.310806]     10.0.2.15  --> 34.122.121.32 (TCP)
[88555.316916] *** LOCAL_OUT
[88555.317469]     10.0.2.15  --> 34.122.121.32 (TCP)
[88557.339234] *** LOCAL_OUT
[88557.339237]     10.0.2.15  --> 34.122.121.32 (TCP)
[88561.401382] *** LOCAL_OUT

[88574.252007]     10.0.2.15  --> 91.189.91.48 (TCP)
[88574.565261] *** LOCAL_OUT
[88574.565945]     10.0.2.15  --> 91.189.91.48 (TCP)
[88574.566418] *** LOCAL_OUT
[88574.566421]     10.0.2.15  --> 91.189.91.48 (TCP)
[88574.915537] *** LOCAL_OUT
[88574.916287]     10.0.2.15  --> 91.189.91.48 (TCP)
[88574.918545] *** LOCAL_OUT
[88574.918548]     10.0.2.15  --> 91.189.91.48 (TCP)
[88688.201731] *** LOCAL_OUT
[88688.201736]     192.168.60.1  --> 224.0.0.251 (UDP)
[88688.201897] *** LOCAL_OUT
[88688.201898]     10.9.0.1  --> 224.0.0.251 (UDP)
[88688.201951] *** LOCAL_OUT
[88688.201952]     172.17.0.1  --> 224.0.0.251 (UDP)
[88688.202398] *** LOCAL_OUT
[88688.202400]     10.0.2.15  --> 224.0.0.251 (UDP)
[88688.202675] *** LOCAL_OUT
[88688.202677]     127.0.0.1  --> 224.0.0.251 (UDP)
[88722.191162] *** LOCAL_OUT
[88722.191166]     127.0.0.1  --> 127.0.0.53 (UDP)
[88722.193291] *** LOCAL_OUT
[88722.193294]     10.0.2.15  --> 192.168.1.1 (UDP)
[88722.223766] *** LOCAL_OUT
[88722.223770]     127.0.0.53  --> 127.0.0.1 (UDP)
[88722.487769] *** LOCAL_OUT
[88722.487772]     127.0.0.1  --> 127.0.0.53 (UDP)
[88722.490228] *** LOCAL_OUT
[88722.490231]     127.0.0.53  --> 127.0.0.1 (UDP)
[88770.835372] The filters are being removed.
```

```
[04/22/24]seed@VM:~/.../packet_filter$ ping www.example.com
PING www.example.com (93.184.215.14) 56(84) bytes of data.
64 bytes from 93.184.215.14 (93.184.215.14): icmp_seq=1 ttl=54 time=27.0 ms
64 bytes from 93.184.215.14 (93.184.215.14): icmp_seq=2 ttl=54 time=26.5 ms
64 bytes from 93.184.215.14 (93.184.215.14): icmp_seq=3 ttl=54 time=51.3 ms
64 bytes from 93.184.215.14 (93.184.215.14): icmp_seq=4 ttl=54 time=21.0 ms
64 bytes from 93.184.215.14 (93.184.215.14): icmp_seq=5 ttl=54 time=18.8 ms
^C
--- www.example.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4024ms
rtt min/avg/max/mdev = 18.812/28.907/51.287/11.618 ms
[04/22/24]seed@VM:~/.../packet_filter$
```

```
seed@VM: ~/.../Labsetup   seed@VM: ~/.../packet_filter   seed@VM: ~/.../packet_filter
[04/22/24]seed@VM:~/.../packet_filter$ dig @8.8.4.4 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.4.4 www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59033
;; 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.        2944    IN      A       93.184.215.14

;; Query time: 35 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Mon Apr 22 11:35:23 EDT 2024
;; MSG SIZE  rcvd: 60
```

Using the "dig @8.8.8.8<www.example.com" command, we can see if the Google DNS server (8.8.8.8) is being blocked by the kernel module. The "sudo rmmod seedFilter" command can be used to remove the kernel module once the testing is finished. By doing this, the kernel module will be removed from memory and the system will be able to operate properly without the need for filtering rules.

## Subtask 2 :

*seedPrint.c  ×  seedBlock.c

```
75 int registerFilter(void) {
76    printk(KERN_INFO "seedPrint:Registering filters.\n");
77         //NF_INET_FORWARD
78    hook1.hook = printInfo;
79    hook1.hooknum = NF_INET_FORWARD;
80    hook1.pf = PF_INET;
81    hook1.priority = NF_IP_PRI_FIRST;
82    nf_register_net_hook(&init_net, &hook1);
83         //NF_INET_POST_ROUTING
84    hook2.hook = printInfo;
85    hook2.hooknum = NF_INET_POST_ROUTING;
86    hook2.pf = PF_INET;
87    hook2.priority = NF_IP_PRI_FIRST;
88    nf_register_net_hook(&init_net, &hook2);
89    //NF_INET_PRE_ROUTING
90    hook3.hook = printInfo;
91    hook3.hooknum = NF_INET_PRE_ROUTING;
92    hook3.pf = PF_INET;
93    hook3.priority = NF_IP_PRI_FIRST;
94    nf_register_net_hook(&init_net, &hook3);
95         //NF_INET_LOCAL_IN
96    hook4.hook = printInfo;
97    hook4.hooknum = NF_INET_LOCAL_IN;
98    hook4.pf = PF_INET;
99    hook4.priority = NF_IP_PRI_FIRST;
100   nf_register_net_hook(&init_net, &hook4;
101        //NF_INET_LOCAL_OUT
102   hook5.hook = printInfo;
103   hook5.hooknum = NF_INET_LOCAL_OUT;
104   hook5.pf = PF_INET;
105   hook5.priority = NF_IP_PRI_FIRST;
106   nf_register_net_hook(&init_net, &hook5);
```

We make changes in the code seedFilter.c (subtask1) and make seedPrint.c

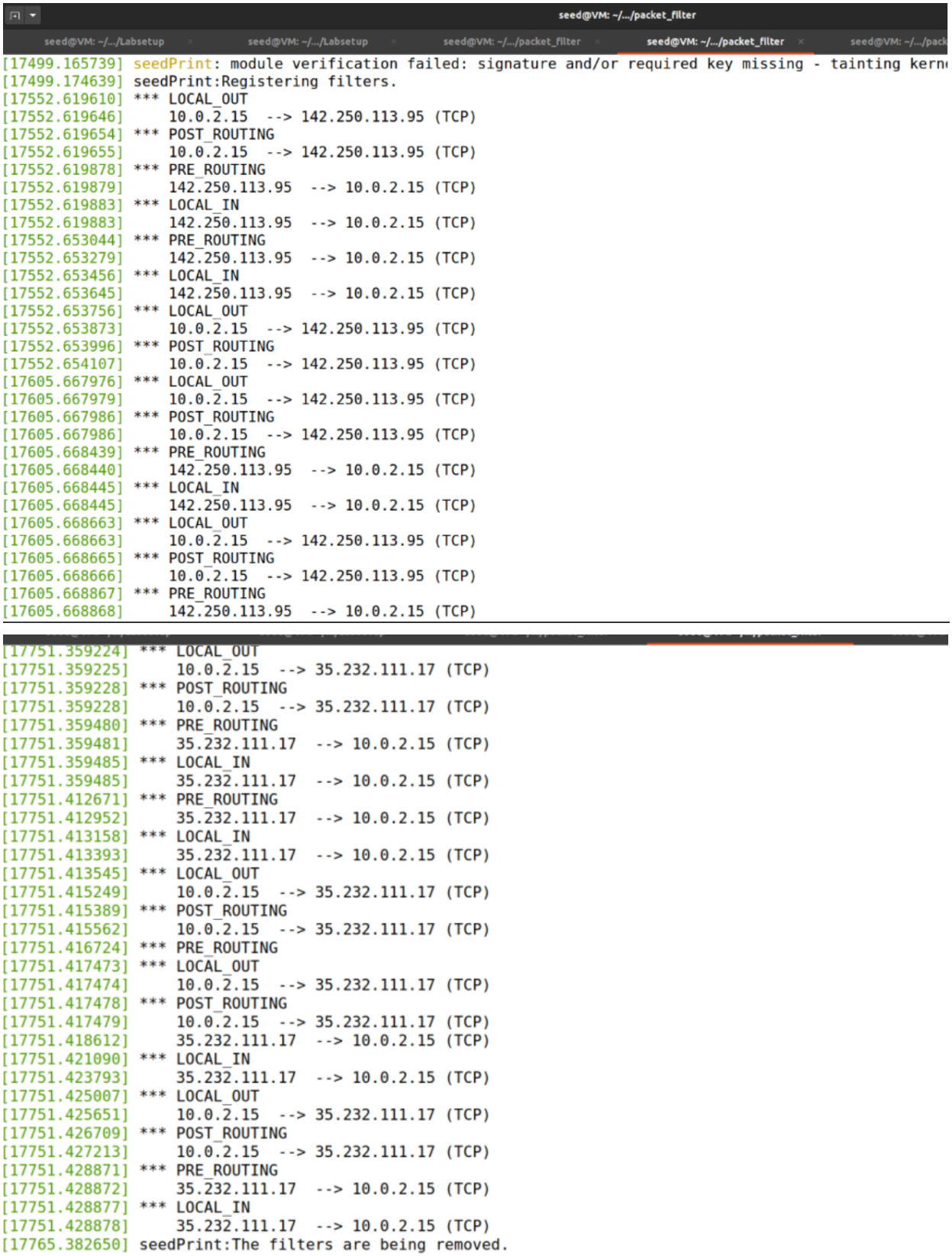
```
[04/22/24]seed@VM:~/.../Files$ cd packet_filter/
[04/22/24]seed@VM:~/.../packet_filter$ make clean
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Downloads/firewall/Labsetup/Files/packet_filter clean
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CLEAN   /home/seed/Downloads/firewall/Labsetup/Files/packet_filter/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[04/22/24]seed@VM:~/.../packet_filter$ ls
Makefile  seedFilter.c
[04/22/24]seed@VM:~/.../packet_filter$ cp seedFilter.c  seedPrint.c
[04/22/24]seed@VM:~/.../packet_filter$ gedit seed
```

The make command must be used to compile the kernel module for this task. Upon completion of the compilation process, multiple kernel modules will be produced within the same directory. To finish this operation, we will use the seedPrint.ko module, as indicated in the screenshot below.

```
[04/22/24]seed@VM:~/.../packet_filter$ ls
Makefile  seedFilter.c
[04/22/24]seed@VM:~/.../packet_filter$ cp seedFilter.c  seedPrint.c
[04/22/24]seed@VM:~/.../packet_filter$ gedit seed
^C
[04/22/24]seed@VM:~/.../packet_filter$ gedit seedPrint.c  &
[3] 6042
[04/22/24]seed@VM:~/.../packet_filter$ gedit Makefile &
[4] 6051
[04/22/24]seed@VM:~/.../packet_filter$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Downloads/firewall/Labsetup/Files/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  CC [M]  /home/seed/Downloads/firewall/Labsetup/Files/packet_filter/seedFilter.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /home/seed/Downloads/firewall/Labsetup/Files/packet_filter/seedFilter.mod.o
  LD [M]  /home/seed/Downloads/firewall/Labsetup/Files/packet_filter/seedFilter.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'
[4]   Done                    gedit Makefile
[04/22/24]seed@VM:~/.../packet_filter$ ls
Makefile       Module.symvers  seedFilter.ko   seedFilter.mod.c  seedFilter.o
modules.order  seedFilter.c    seedFilter.mod  seedFilter.mod.o  seedPrint.c
[04/22/24]seed@VM:~/.../packet_filter$ make
make -C /lib/modules/5.4.0-54-generic/build M=/home/seed/Downloads/firewall/Labsetup/Files/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-54-generic'
  Building modules, stage 2.
  MODPOST 1 modules
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-54-generic'

seed@VM:~/.../packet_filter$ sudo insmod seedPrint.ko
seed@VM:~/.../packet_filter$ sudo rmmod seedPrint.ko
seed@VM:~/.../packet_filter$
```

```
seed@VM: ~/.../Labsetup | seed@VM: ~/.../packet_filter | seed@VM: ~/.../packet_filter
[04/22/24]seed@VM:~/.../packet_filter$ dig @8.8.4.4 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.4.4 www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59033
;; 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.        2944    IN      A       93.184.215.14

;; Query time: 35 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Mon Apr 22 11:35:23 EDT 2024
;; MSG SIZE  rcvd: 60
```

During this incident, the host with the IP address 10.0.2.15 tried to initiate a connection with 142.250.113.95, leading to the generation of logs for the LOCAL_OUT and POST_ROUTING hooks. The LOCAL_OUT hook manages outgoing traffic, while the POST_ROUTING hook is the last step in processing outbound packets. The response from 142.250.113.95 activated the PRE_ROUTING hook as it was an incoming packet, and after moving through the PRE_ROUTING hook, it was directed to the LOCAL_IN hook. The POST_ROUTING hook has the capability to alter the destinations set by the LOCAL_OUT hook. The PRE_ROUTING hook handles incoming packets in their original state. For packets whose destination is not the host itself, the FORWARD hook comes into play, allowing packets to be routed to any of the machine's interfaces.


seed@VM: ~/.../packet_filter
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../packet_filter
seed@VM: ~/.../packet_filter
[17499.165739] seedPrint: module verification failed: signature and/or required key missing - tainting kern
[17499.174639] seedPrint:Registering filters.
[17552.619610] *** LOCAL_OUT
[17552.619646] 10.0.2.15 --> 142.250.113.95 (TCP)
[17552.619654] *** POST_ROUTING
[17552.619655] 10.0.2.15 --> 142.250.113.95 (TCP)
[17552.619878] *** PRE_ROUTING
[17552.619879] 142.250.113.95 --> 10.0.2.15 (TCP)
[17552.619883] *** LOCAL_IN
[17552.619883] 142.250.113.95 --> 10.0.2.15 (TCP)
[17552.653044] *** PRE_ROUTING
[17552.653279] 142.250.113.95 --> 10.0.2.15 (TCP)
[17552.653456] *** LOCAL_IN
[17552.653645] 142.250.113.95 --> 10.0.2.15 (TCP)
[17552.653756] *** LOCAL_OUT
[17552.653873] 10.0.2.15 --> 142.250.113.95 (TCP)
[17552.653996] *** POST_ROUTING
[17552.654107] 10.0.2.15 --> 142.250.113.95 (TCP)
[17605.667976] *** LOCAL_OUT
[17605.667979] 10.0.2.15 --> 142.250.113.95 (TCP)
[17605.667986] *** POST_ROUTING
[17605.667986] 10.0.2.15 --> 142.250.113.95 (TCP)
[17605.668439] *** PRE_ROUTING
[17605.668440] 142.250.113.95 --> 10.0.2.15 (TCP)
[17605.668445] *** LOCAL_IN
[17605.668445] 142.250.113.95 --> 10.0.2.15 (TCP)
[17605.668663] *** LOCAL_OUT
[17605.668663] 10.0.2.15 --> 142.250.113.95 (TCP)
[17605.668665] *** POST_ROUTING
[17605.668666] 10.0.2.15 --> 142.250.113.95 (TCP)
[17605.668867] *** PRE_ROUTING
[17605.668868] 142.250.113.95 --> 10.0.2.15 (TCP)
[17751.359224] *** LOCAL_OUT
[17751.359225] 10.0.2.15 --> 35.232.111.17 (TCP)
[17751.359228] *** POST_ROUTING
[17751.359228] 10.0.2.15 --> 35.232.111.17 (TCP)
[17751.359480] *** PRE_ROUTING
[17751.359481] 35.232.111.17 --> 10.0.2.15 (TCP)
[17751.359485] *** LOCAL_IN
[17751.359485] 35.232.111.17 --> 10.0.2.15 (TCP)
[17751.412671] *** PRE_ROUTING
[17751.412952] 35.232.111.17 --> 10.0.2.15 (TCP)
[17751.413158] *** LOCAL_IN
[17751.413393] 35.232.111.17 --> 10.0.2.15 (TCP)
[17751.413545] *** LOCAL_OUT
[17751.415249] 10.0.2.15 --> 35.232.111.17 (TCP)
[17751.415389] *** POST_ROUTING
[17751.415562] 10.0.2.15 --> 35.232.111.17 (TCP)
[17751.416724] *** PRE_ROUTING
[17751.417473] *** LOCAL_OUT
[17751.417474] 10.0.2.15 --> 35.232.111.17 (TCP)
[17751.417478] *** POST_ROUTING
[17751.417479] 10.0.2.15 --> 35.232.111.17 (TCP)
[17751.418612] 35.232.111.17 --> 10.0.2.15 (TCP)
[17751.421090] *** LOCAL_IN
[17751.423793] 35.232.111.17 --> 10.0.2.15 (TCP)
[17751.425007] *** LOCAL_OUT
[17751.425651] 10.0.2.15 --> 35.232.111.17 (TCP)
[17751.426709] *** POST_ROUTING
[17751.427213] 10.0.2.15 --> 35.232.111.17 (TCP)
[17751.428871] *** PRE_ROUTING
[17751.428872] 35.232.111.17 --> 10.0.2.15 (TCP)
[17751.428877] *** LOCAL_IN
[17751.428878] 35.232.111.17 --> 10.0.2.15 (TCP)
[17765.382650] seedPrint:The filters are being removed.

Subtask 3:

*seedPrint.c | seedBlock.c | Makefile

```
#obj-m += seedFilter.o
#obj-m += seedPrint.o
obj-m += seedBlock.o
all:
	make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules

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

ins:
	sudo dmesg -C
	sudo insmod seedFilter.ko

rm:
	sudo rmmod seedFilter

```

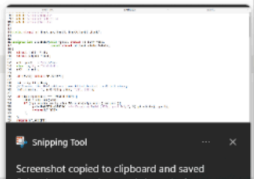
The seedBlock.c file, which is a duplicate of seedFilter.c with the modifications in the code as indicated below, inherits the makefile.

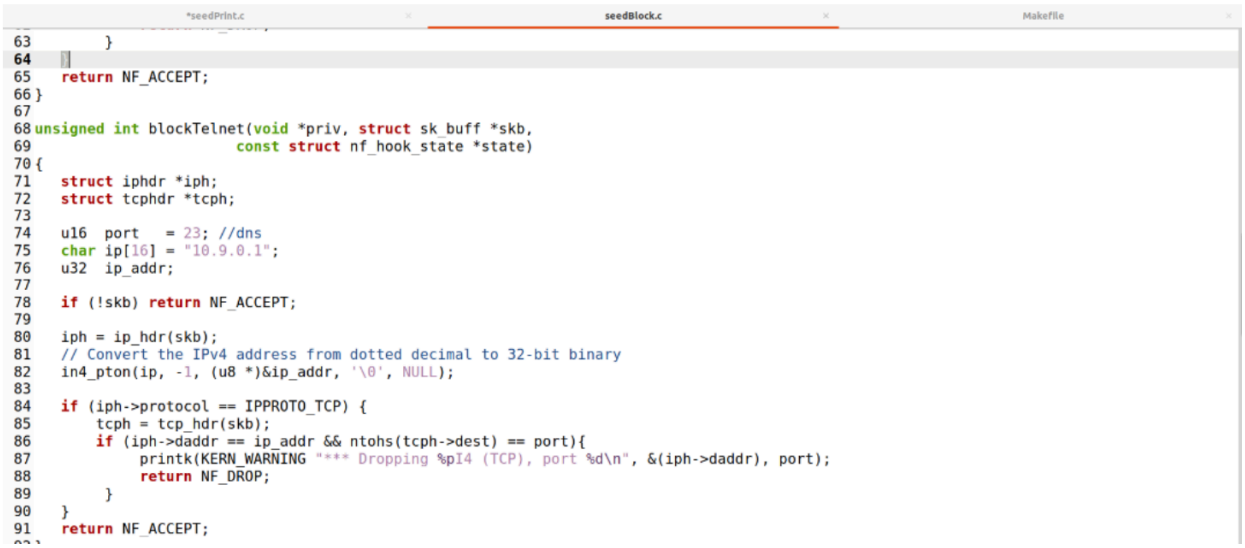
*seedPrint.c | seedBlock.c | Makefile

```c
#include <linux/icmp.h>
#include <linux/if_ether.h>
#include <linux/inet.h>


static struct nf_hook_ops hook1, hook2,hook3 ,hook4;


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

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

   if (!skb) return NF_ACCEPT;

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

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

*seedPrint.c | seedBlock.c | Makefile

```c
   return NF_ACCEPT;
}

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

   //u16  port   = 53; //dns
   char ip[16] = "10.9.0.1";
   u32  ip_addr;

   if (!skb) return NF_ACCEPT;

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

   if (iph->protocol == IPPROTO_ICMP) {
       icmph = icmp_hdr(skb);
       if (iph->daddr == ip_addr && icmph->type == ICMP_ECHO){
           printk(KERN_WARNING "*** Dropping %pI4 (ICMP)\n", &(iph->daddr));
           return NF_DROP;
        }
   }
   return NF_ACCEPT;
}

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






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

Using build, we compile the files to obtain the seedBlock.ko modules. This module is inserted, and the packets are looked for.If the firewall was effectively set up, the packets ought to be dropping from port 23.

In the same window where the "dmesg" command was run, we can use the command "sudo insmod seedBlock.ko" to install the kernel module. The command "sudo lsmod | grep -i seed" can be used to confirm whether the module has been installed. The command "sudo rmmod seedBlock" can be used to eliminate the module from memory. When the module is registered

or uninstalled, the messages "seedBlock: Registering filters" and "seedBlock: The filters are being removed" will be shown, accordingly.

```
seed@VM:~/.../packet_filter$ sudo rmmod seedPrint.ko
seed@VM:~/.../packet_filter$ ls
     Module.symvers  seedPrint.c   seedPrint.mod    seedPrint.mod.o
der  seedFilter.c    seedPrint.ko  seedPrint.mod.c  seedPrint.o
seed@VM:~/.../packet_filter$ make clean
ib/modules/5.4.0-54-generic/build M=/home/seed/Downloads/firewall_exploration/Labsetup/Files/packet_filter clean
ntering directory '/usr/src/linux-headers-5.4.0-54-generic'
/home/seed/Downloads/firewall_exploration/Labsetup/Files/packet_filter/Module.symvers
eaving directory '/usr/src/linux-headers-5.4.0-54-generic'
seed@VM:~/.../packet_filter$ ls
seedFilter.c  seedPrint.c
seed@VM:~/.../packet_filter$ cp seedFilter.c  seedBlock.c
seed@VM:~/.../packet_filter$ gedit seedBlock.c
seed@VM:~/.../packet_filter$ make
ib/modules/5.4.0-54-generic/build M=/home/seed/Downloads/firewall_exploration/Labsetup/Files/packet_filter modules
ntering directory '/usr/src/linux-headers-5.4.0-54-generic'
/home/seed/Downloads/firewall_exploration/Labsetup/Files/packet_filter/seedBlock.o
 modules, stage 2.
1 modules
/home/seed/Downloads/firewall_exploration/Labsetup/Files/packet_filter/seedBlock.mod.o
/home/seed/Downloads/firewall_exploration/Labsetup/Files/packet_filter/seedBlock.ko
eaving directory '/usr/src/linux-headers-5.4.0-54-generic'
seed@VM:~/.../packet_filter$ ls
     Module.symvers  seedBlock.ko   seedBlock.mod.c  seedBlock.o   seedPrint.c
der  seedBlock.c     seedBlock.mod  seedBlock.mod.o  seedFilter.c
seed@VM:~/.../packet_filter$ sudo insmod seedBlock.ko
seed@VM:~/.../packet_filter$ sudo rmmod seedBlock.ko
```

Before the attack occurred, I created a container called "HOST" and used it to check connectivity by
running the commands "ping 10.9.0.1" and "telnet 10.9.0.1". Both tests were successful, and a connection
was established.

```
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data.
^C
--- 10.9.0.1 ping statistics ---
25 packets transmitted, 0 received, 100% packet loss, time 24583ms
```

And after entering telnet 10.9.0.1

```
Trying 10.9.0.1...
^C
```

```
seed@VM: ~/.../Labsetup   seed@VM: ~/.../Labsetup   seed@VM: ~/.../packet_filter   seed@VM: ~/.../packet_filter   seed@VM: ~   seed@VM: ~/.../packet_filter
[21865.019143] usb 2-1: Manufacturer: VirtualBox
[21865.246579] input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/usb2/2-1/2-1:1.0/0003:80EE:0021.0003/input/input9
[21865.310607] hid-generic 0003:80EE:0021.0003: input,hidraw0: USB HID v1.10 Mouse [VirtualBox USB Tablet] on usb-0000:00:06.0-1/input0
[21869.722266] e1000: enp0s3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
[22560.939384] Registering filters.
[22595.705743] *** LOCAL_OUT
[22595.705875]     10.0.2.15  --> 35.241.9.150 (TCP)
[22595.858207] *** LOCAL_OUT
[22595.858581]     10.0.2.15  --> 35.241.9.150 (TCP)
[22648.720495] *** LOCAL_OUT
[22648.720497]     10.0.2.15  --> 35.241.9.150 (TCP)
[22648.722950] *** LOCAL_OUT
[22648.722952]     10.0.2.15  --> 35.241.9.150 (TCP)
[22648.723152] *** LOCAL_OUT
[22648.723154]     10.0.2.15  --> 35.241.9.150 (TCP)
[22648.748030] *** LOCAL_OUT
[22648.748359]     10.0.2.15  --> 35.241.9.150 (TCP)
[22651.371847] *** Dropping 10.9.0.1 (UDP)
[22652.404959] *** Dropping 10.9.0.1 (UDP)
[22653.426151] *** Dropping 10.9.0.1 (UDP)
[22654.450206] *** Dropping 10.9.0.1 (UDP)
[22655.474308] *** Dropping 10.9.0.1 (UDP)
[22656.499196] *** Dropping 10.9.0.1 (UDP)
[22657.521928] *** Dropping 10.9.0.1 (UDP)
[22658.546152] *** Dropping 10.9.0.1 (UDP)
[22659.572244] *** Dropping 10.9.0.1 (UDP)
[22660.594616] *** Dropping 10.9.0.1 (UDP)
[22661.619194] *** Dropping 10.9.0.1 (UDP)
[22662.641998] *** Dropping 10.9.0.1 (UDP)
[22663.665496] *** Dropping 10.9.0.1 (UDP)
[22664.689256] *** Dropping 10.9.0.1 (UDP)
[22665.713276] *** Dropping 10.9.0.1 (UDP)
[22666.737212] *** Dropping 10.9.0.1 (UDP)
```

```
seed@VM: ~/.../Labsetup   seed@VM: ~/.../Labsetup   seed@VM: ~/.../packet_filter   seed@VM: ~/.../packet_filter
[22771.116019] *** LOCAL_OUT
[22771.116022]     10.0.2.15  --> 130.127.255.250 (UDP)
[22771.134976] *** LOCAL_OUT
[22771.134980]     10.0.2.15  --> 185.125.190.18 (TCP)
[22771.227621] *** LOCAL_OUT
[22771.228023]     10.0.2.15  --> 185.125.190.18 (TCP)
[22771.236637] *** LOCAL_OUT
[22771.236638]     10.0.2.15  --> 185.125.190.18 (TCP)
[22771.344190] *** LOCAL_OUT
[22771.344195]     10.0.2.15  --> 185.125.190.18 (TCP)
[22771.344801] *** LOCAL_OUT
[22771.344803]     10.0.2.15  --> 185.125.190.18 (TCP)
[22777.543761] *** LOCAL_OUT
[22777.544065]     10.0.2.15  --> 34.117.65.55 (TCP)
[22777.544459] *** LOCAL_OUT
[22777.544461]     10.0.2.15  --> 34.117.65.55 (TCP)
[22795.532071] *** LOCAL_OUT
[22795.532075]     10.0.2.15  --> 185.125.190.57 (UDP)
[22826.127340] *** Dropping 10.9.0.1 (UDP), port 23
[22827.147015] *** Dropping 10.9.0.1 (UDP), port 23
[22829.164243] *** Dropping 10.9.0.1 (UDP), port 23
[22833.258789] *** Dropping 10.9.0.1 (UDP), port 23
[22841.450579] *** Dropping 10.9.0.1 (UDP), port 23
[22857.592572] *** Dropping 10.9.0.1 (UDP), port 23
[22866.697855] *** LOCAL_OUT
[22866.697857]     127.0.0.1  --> 127.0.0.53 (UDP)
[22866.705085] *** LOCAL_OUT
[22866.705087]     127.0.0.1  --> 127.0.0.53 (UDP)
[22866.705928] *** LOCAL_OUT
[22866.705930]     10.0.2.15  --> 130.127.255.250 (UDP)
[22866.713084] *** LOCAL_OUT
[22866.713086]     127.0.0.1  --> 127.0.0.53 (UDP)
```

As we can see in the above, it is dropping the 10.9.0.1 when we attempt to connect; this means that a firewall has been successfully constructed, hence fulfilling the goal.