

# Computer Network Security

Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

## Firewall Exploration Lab

### Task 1: Implementing a Simple Firewall

#### Task 1.A: Implement a Simple Kernel Module

```
#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");
```

C

```
$ make
$ sudo insmod hello.ko (inserting a module) $ lsmod | grep hello (list modules)
$ sudo rmmod hello
```

Bash

```

seed@Naman209: ~/.../kernel_module
File Actions Edit View Help
seed@Naman209: ~/.../kernel_module
seed@Naman209: ~/.../kernel_module
[10/27/22]seed@Naman209:~$ cd Desktop/Labsetup/volumes/
kernel_module/ packet_filter/
[10/27/22]seed@Naman209:~$ cd Desktop/Labsetup/volumes/kernel_module/
[10/27/22]seed@Naman209:~/.../kernel_module$ make
make -C /lib/modules/5.15.0-46-generic/build M=/home/seed/Desktop/Labsetup/volumes/kernel_mo
dule modules
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-46-generic'
  CC [M] /home/seed/Desktop/Labsetup/volumes/kernel_module/hello.o
  MODPOST /home/seed/Desktop/Labsetup/volumes/kernel_module/Module.symvers
  CC [M] /home/seed/Desktop/Labsetup/volumes/kernel_module/hello.mod.o
  LD [M] /home/seed/Desktop/Labsetup/volumes/kernel_module/hello.ko
  BTF [M] /home/seed/Desktop/Labsetup/volumes/kernel_module/hello.ko
Skipping BTF generation for /home/seed/Desktop/Labsetup/volumes/kernel_module/hello.ko due t
o unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-46-generic'
[10/27/22]seed@Naman209:~/.../kernel_module$ sudo insmod hello.ko
[10/27/22]seed@Naman209:~/.../kernel_module$ lsmod|grep hello.
hello.c      hello.ko      hello.mod      hello.mod.c      hello.mod.o      hello.o
[10/27/22]seed@Naman209:~/.../kernel_module$ lsmod|grep hello
hello          16384   0
[10/27/22]seed@Naman209:~/.../kernel_module$ sudo rmmod hello
[10/27/22]seed@Naman209:~/.../kernel_module$ 

```

Bash

```

sudo dmesg -k -w

```

```

seed@Naman209: ~/.../kernel_module
File Actions Edit View Help
seed@Naman209: ~/.../kernel_module
seed@Naman209: ~/.../kernel_module
[ 3393.021775] br-dfd45ec1074b: port 1(vetha548845) entered disabled state
[ 3393.034453] device vetha548845 left promiscuous mode
[ 3393.034453] br-dfd45ec1074b: port 1(vetha548845) entered disabled state
[ 3429.853103] br-0b38324955fd: port 1(veth4c0a90f) entered blocking state
[ 3429.854419] br-0b38324955fd: port 1(veth4c0a90f) entered disabled state
[ 3429.877663] device veth4c0a90f entered promiscuous mode
[ 3433.466264] eth0: renamed from veth498928e
[ 3433.492576] IPv6: ADDRCONF(NETDEV_CHANGE): veth4c0a90f: link becomes ready
[ 3433.493862] br-0b38324955fd: port 1(veth4c0a90f) entered blocking state
[ 3433.493945] br-0b38324955fd: port 1(veth4c0a90f) entered forwarding state
[ 3433.495473] IPv6: ADDRCONF(NETDEV_CHANGE): br-0b38324955fd: link becomes ready
[ 4835.964175] br-0b38324955fd: port 1(veth4c0a90f) entered disabled state
[ 4835.967812] veth498928e: renamed from eth0
[ 4836.053932] br-0b38324955fd: port 1(veth4c0a90f) entered disabled state
[ 4836.060491] device veth4c0a90f left promiscuous mode
[ 4836.060658] br-0b38324955fd: port 1(veth4c0a90f) entered disabled state
[ 6506.409468] hello: loading out-of-tree module taints kernel.
[ 6506.412215] hello: module verification failed: signature and/or required key missing - ta
inting kernel
[ 6506.419404] Hello World!
[ 6548.978142] Bye-bye World!.

```

### Task 1.B: Implement a Simple Firewall Using Netfilter

Bash

```

dig @8.8.8.8 www.example.com

```

```
seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
[11/20/22]seed@Naman209:~$ dig @8.8.8.8 example.com

; <>> DiG 9.16.1-Ubuntu <>> @8.8.8.8 example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21231
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
example.com.        19978    IN      A      93.184.216.34

;; Query time: 11 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Nov 20 17:30:18 IST 2022
;; MSG SIZE  rcvd: 56

[11/20/22]seed@Naman209:~$
```

```
Bash
sudo dmesg -k -w
```

The screenshot shows a Linux desktop environment with a terminal window open in a window manager. The terminal window title is "seed@Naman209: ~". It displays log output from the kernel module "seedFilter". The log includes messages about apparmor\_parser detecting capacity changes, audit events for profile\_replace, and seedFilter handling UDP traffic. The terminal window has a menu bar with File, Actions, Edit, View, Help. The desktop background features a blue and purple abstract design. A "Software Updater" window is visible at the bottom left.

```
unconfined" name="snap.snap-store.hook.configure" pid=2596 comm="apparmor_parser"
[ 177.026011] loop11: detected capacity change from 0 to 129520
[ 201.739156] loop7: detected capacity change from 0 to 484392
[ 204.058597] audit: type=1400 audit(1668942880.190:70): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="snap.code.code" pid=3128 comm="apparmor_parser"
[ 204.060344] audit: type=1400 audit(1668942880.190:71): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="snap.code.url-handler" pid=3129 comm="apparmor_parser"
[ 204.170366] audit: type=1400 audit(1668942880.302:72): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="snap-update-ns.code" pid=3131 comm="apparmor_parser"
[ 3306.001472] seedFilter: loading out-of-tree module taints kernel.
[ 3306.003482] seedFilter: module verification failed: signature and/or required key missing - tainting kernel
[ 3306.009581] Registering filters.  []
[ 3341.692225] *** LOCAL_OUT
[ 3341.692292]      127.0.0.1  --> 127.0.0.1 (UDP)
[ 3341.701228] *** LOCAL_OUT
[ 3341.701274]      192.168.64.6  --> 8.8.8.8 (UDP)
[ 3341.701373] *** Dropping 8.8.8.8 (UDP), port 53
[ 3346.692812] *** LOCAL_OUT
[ 3346.692995]      192.168.64.6  --> 8.8.8.8 (UDP)
[ 3346.693303] *** Dropping 8.8.8.8 (UDP), port 53
```

For seedFilter:

```
$ make
$ sudo insmod seedFilter.ko
$ lsmod | grep seedFilter
```

SEEDLabsRefer

```
seed@Naman209: ~/.../packet_filter
File Actions Edit View Help
nman209: ~          seed@Naman209: ~/.../packet_filter
[11/20/22]seed@Naman209:~/.../packet_filter$ nano Makefile
[11/20/22]seed@Naman209:~/.../packet_filter$ make
make -C /lib/modules/5.15.0-46-generic/build M=/home/seed/Desktop/Labsetup/Files/packet_filter modules
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-46-generic'
  CC [M]  /home/seed/Desktop/Labsetup/Files/packet_filter/seedFilter.o
  MODPOST /home/seed/Desktop/Labsetup/Files/packet_filter/Module.symvers
  CC [M]  /home/seed/Desktop/Labsetup/Files/packet_filter/seedFilter.mod.o
  LD [M]  /home/seed/Desktop/Labsetup/Files/packet_filter/seedFilter.ko
  BTF [M] /home/seed/Desktop/Labsetup/Files/packet_filter/seedFilter.ko
Skipping BTF generation for /home/seed/Desktop/Labsetup/Files/packet_filter/seedFilter.ko due to unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-46-generic'
[11/20/22]seed@Naman209:~/.../packet_filter$ sudo insmod seedFilter.ko
[11/20/22]seed@Naman209:~/.../packet_filter$ lsmod|grep seedFilter.
seedFilter           16384  0
[11/20/22]seed@Naman209:~/.../packet_filter$ lsmod|grep seedFilter
seedFilter           16384  0
[11/20/22]seed@Naman209:~/.../packet_filter$ dig @8.8.8.8 www.example.com
; <>> DiG 9.16.1-Ubuntu <>> @8.8.8.8 www.example.com
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached

[11/20/22]seed@Naman209:~/.../packet_filter$
```

Software Updater

seed@Naman209:~/.../packet\_filter

A screenshot of a terminal window titled "seed@Naman209: ~". The window contains a list of log entries from a networking application, likely a firewall or packet sniffer. The entries show various routing and filtering decisions for UDP traffic. The log includes entries for LOCAL\_OUT, POST\_ROUTING, PRE\_ROUTING, LOCAL\_IN, and LOCAL\_OUT rules, with specific source and destination addresses like 127.0.0.1, 8.8.8.8, and 192.168.64.1. The terminal has a dark theme and is running on a Linux system.

```
[ 3719.622369] Registering filters.  
[ 3740.027988] *** LOCAL_OUT  
[ 3740.028074] 127.0.0.1 --> 127.0.0.1 (UDP)  
[ 3740.028342] *** POST_ROUTING  
[ 3740.028350] 127.0.0.1 --> 127.0.0.1 (UDP)  
[ 3740.028489] *** PRE_ROUTING  
[ 3740.028497] 127.0.0.1 --> 127.0.0.1 (UDP)  
[ 3740.028511] *** LOCAL_IN  
[ 3740.028515] 127.0.0.1 --> 127.0.0.1 (UDP)  
[ 3740.037432] *** LOCAL_OUT  
[ 3740.037465] 192.168.64.6 --> 8.8.8.8 (UDP)  
[ 3740.037542] *** POST_ROUTING  
[ 3740.037549] 192.168.64.6 --> 8.8.8.8 (UDP)  
[ 3740.051130] *** PRE_ROUTING  
[ 3740.051359] 8.8.8.8 --> 192.168.64.6 (UDP) █  
[ 3740.051509] *** LOCAL_IN  
[ 3740.051528] 8.8.8.8 --> 192.168.64.6 (UDP)  
[ 3745.460639] *** PRE_ROUTING  
[ 3745.460949] 192.168.64.1 --> 192.168.64.255 (UDP)  
[ 3745.461099] *** LOCAL_IN  
[ 3745.461123] 192.168.64.1 --> 192.168.64.255 (UDP)  
[ 3745.461628] *** PRE_ROUTING  
[ 3745.461662] 192.168.64.1 --> 192.168.64.255 (UDP)  
[ 3745.461943] *** LOCAL_IN  
[ 3745.461989] 192.168.64.1 --> 192.168.64.255 (UDP)
```

For seedPrint:

```
$ make  
$ sudo insmod seedPrint.ko  
$ lsmod | grep seedPrint
```

SEEDLabsRefer

```
seed@Naman209: ~/.../packet_filter
File Actions Edit View Help
seed@Naman209: ~/.../packet_filter
[11/20/22]seed@Naman209:~/.../packet_filter$ sudo insmod seedPrint.ko
[11/20/22]seed@Naman209:~/.../packet_filter$ lsmod|grep seedPrint
seedPrint           16384   0
[11/20/22]seed@Naman209:~/.../packet_filter$ dig @8.8.8.8 www.example.com

; <>> DiG 9.16.1-Ubuntu <>> @8.8.8.8 www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38010
;; 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.    21478    IN      A      93.184.216.34

;; Query time: 19 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Nov 20 19:03:54 IST 2022
;; MSG SIZE  rcvd: 60

[11/20/22]seed@Naman209:~/.../packet_filter$
```

Software Updater

seed@Naman209: ~/.../packet\_filter

```
seed@Naman209: ~
File Actions Edit View Help
: ~/.../packet_filter      seed@Naman209: ~
[ 5163.276928]      192.168.64.6  --> 185.125.190.49 (TCP)
[ 5163.280861] *** PRE_ROUTING
[ 5163.280896]      185.125.190.49  --> 192.168.64.6 (TCP)
[ 5163.281048] *** LOCAL_IN
[ 5163.281058]      185.125.190.49  --> 192.168.64.6 (TCP)
[ 5163.447346] *** PRE_ROUTING
[ 5163.447550]      185.125.190.49  --> 192.168.64.6 (TCP)
[ 5163.447685] *** LOCAL_IN
[ 5163.447702]      185.125.190.49  --> 192.168.64.6 (TCP)
[ 5163.448290] *** LOCAL_OUT
[ 5163.448367]      192.168.64.6  --> 185.125.190.49 (TCP)
[ 5163.448430] *** POST_ROUTING
[ 5163.448444]      192.168.64.6  --> 185.125.190.49 (TCP)
[ 5163.448646] *** PRE_ROUTING
[ 5163.448729]      185.125.190.49  --> 192.168.64.6 (TCP)
[ 5163.448799] *** LOCAL_IN
[ 5163.448815]      185.125.190.49  --> 192.168.64.6 (TCP)
[ 5163.453370] *** LOCAL_OUT
[ 5163.453407]      192.168.64.6  --> 185.125.190.49 (TCP)
[ 5163.453457] *** POST_ROUTING
[ 5163.453464]      192.168.64.6  --> 185.125.190.49 (TCP)
[ 5163.456683] *** PRE_ROUTING
[ 5163.456730]      185.125.190.49  --> 192.168.64.6 (TCP)
[ 5163.456847] *** LOCAL_IN
[ 5163.456857]      185.125.190.49  --> 192.168.64.6 (TCP)

Software Updater  seed@Naman209: ~
```

For seedBlock:

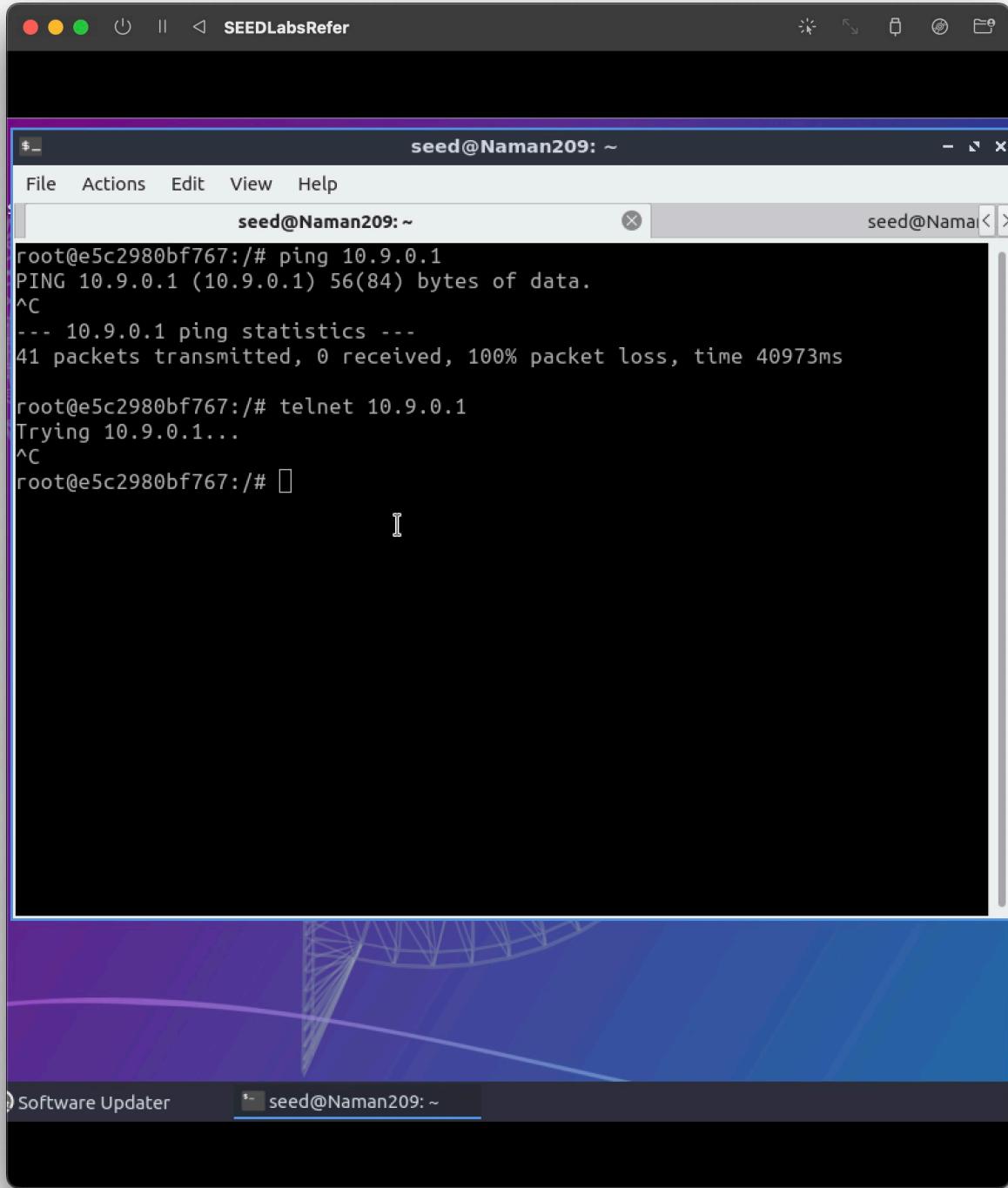
```
$ make
$ sudo insmod seedBlock.ko
$ lsmod | grep seedBlock
```

SEEDLabsRefer

```
seed@Naman209: ~
File Actions Edit View Help
naman209: ~                               seed@Naman209: ~
[ 4926.417128] *** Dropping 10.9.0.1 (ICMP)
[ 4927.439459] *** Dropping 10.9.0.1 (ICMP)
[ 4928.463242] *** Dropping 10.9.0.1 (ICMP)
[ 4929.487240] *** Dropping 10.9.0.1 (ICMP)
[ 4930.511417] *** Dropping 10.9.0.1 (ICMP)
[ 4931.536863] *** Dropping 10.9.0.1 (ICMP)
[ 4932.558719] *** Dropping 10.9.0.1 (ICMP)
[ 4933.583361] *** Dropping 10.9.0.1 (ICMP)
[ 4934.606310] *** Dropping 10.9.0.1 (ICMP)
[ 4935.631148] *** Dropping 10.9.0.1 (ICMP)
[ 4936.655682] *** Dropping 10.9.0.1 (ICMP)
[ 4937.678522] *** Dropping 10.9.0.1 (ICMP)
[ 4938.702417] *** Dropping 10.9.0.1 (ICMP)
[ 4939.727695] *** Dropping 10.9.0.1 (ICMP)
[ 4940.545895] *** LOCAL_OUT
[ 4940.545967] 127.0.0.1 --> 127.0.0.53 (UDP)
[ 4940.547108] *** LOCAL_OUT
[ 4940.547136] 127.0.0.1 --> 127.0.0.53 (UDP)
[ 4940.551423] *** LOCAL_OUT
[ 4940.551459] 127.0.0.53 --> 127.0.0.1 (UDP)
[ 4940.552751] *** LOCAL_OUT
[ 4940.552765] 127.0.0.53 --> 127.0.0.1 (UDP)
[ 4940.750319] *** Dropping 10.9.0.1 (ICMP)
[ 4941.777456] *** Dropping 10.9.0.1 (ICMP)
[ 4942.801069] *** Dropping 10.9.0.1 (ICMP)
```

Software Updater

seed@Naman209: ~



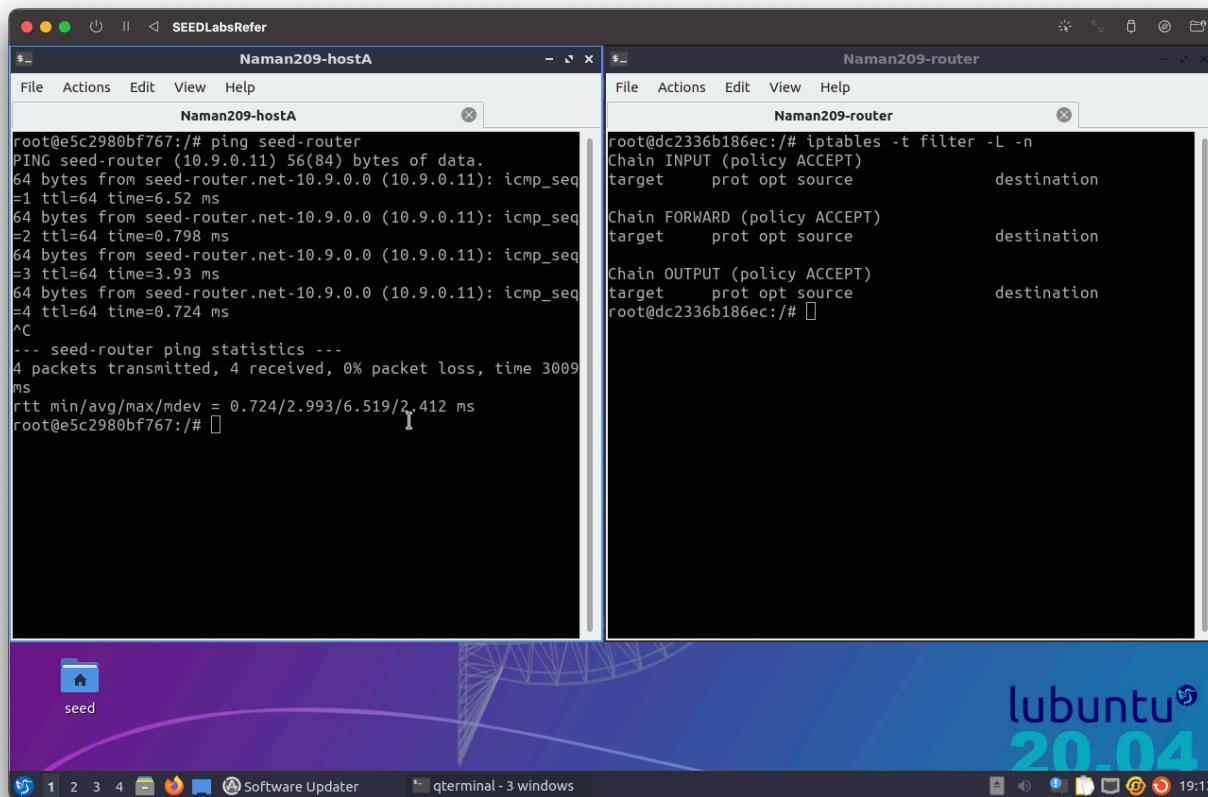
## Task 2: Experimenting with Stateless Firewall Rules

### Task 2.A: Protecting the Router

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
iptables -P OUTPUT DROP
iptables -P INPUT DROP
iptables -t filter -L -n
```

```
ping seed-router
```

Bash



```
telnet seed-router
```

Bash

```

root@e5c2980bf767:/# 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=1.14 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=2 ttl=64 time=1.80 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=3 ttl=64 time=2.26 ms
^C
--- seed-router ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 1.136/1.733/2.264/0.462 ms
root@e5c2980bf767:/# telnet seed-router
Trying 10.9.0.11...
^C
root@e5c2980bf767:/#

```

```

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@dc2336b186ec:/# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
root@dc2336b186ec:/# iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
root@dc2336b186ec:/# iptables -P INPUT DROP
root@dc2336b186ec:/# iptables -P OUTPUT DROP
root@dc2336b186ec:/# 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
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT    icmp -- 0.0.0.0/0              0.0.0.0/0
          icmp-type 0
root@dc2336b186ec:/#

```

Questions:

1 .Can you ping the router

-> Yes, Pinging the router is possible

2 .Can you telnet into the router

-> No, Cannot telnet into the server, as it's stuck at 'Trying'

### Task 2.B: Protecting the Internal Network

```

iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DROP
iptables -A FORWARD -i eth1 -p icmp --icmp-type echo-request -j ACCEPT # iptables -A FORWARD -i eth0
iptables -P FORWARD DROP
iptables -L -n -v

```

```

ping 192.168.60.5
ping seed-router

```

SEEDLabsRefer

```

root@e5c2980bf767:/# 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 ---
9 packets transmitted, 0 received, 100% packet loss, time 8199ms

root@e5c2980bf767:/# 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=0.849 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=2 ttl=64 time=0.838 ms
64 bytes from seed-router.net-10.9.0.0 (10.9.0.11): icmp_seq=3 ttl=64 time=1.91 ms
^C
--- seed-router ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2010 ms
rtt min/avg/max/mdev = 0.838/1.199/1.912/0.503 ms
root@e5c2980bf767:/# 
```

```

root@dc2336b186ec:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DROP
root@dc2336b186ec:/# iptables -A FORWARD -i eth1 -p icmp --icmp-type echo-request -j ACCEPT
root@dc2336b186ec:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-reply -j ACCEPT
root@dc2336b186ec:/# iptables -P FORWARD DROP
root@dc2336b186ec:/# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
      0      0          DROP   icmp --    eth0   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth1   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
      0      0          DROP   icmp --    eth0   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth1   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth1   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
root@dc2336b186ec:/# 
```

lubuntu 20.04

Bash

```

ping 10.9.0.5
telnet 10.9.0.5 
```

```

root@c0c8be59da37:/# 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=9.18 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.874 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=3.12 ms
^C
--- 10.9.0.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2016 ms
rtt min/avg/max/mdev = 0.874/4.391/9.178/3.506 ms
root@c0c8be59da37:/# telnet 10.9.0.5
bash: telnet: command not found
root@c0c8be59da37:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
root@c0c8be59da37:/# 
```

```

root@dc2336b186ec:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DROP
root@dc2336b186ec:/# iptables -A FORWARD -i eth1 -p icmp --icmp-type echo-request -j ACCEPT
root@dc2336b186ec:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-reply -j ACCEPT
root@dc2336b186ec:/# iptables -P FORWARD DROP
root@dc2336b186ec:/# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
      0      0          DROP   icmp --    eth0   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth1   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
      0      0          DROP   icmp --    eth0   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth1   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth1   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
      0      0          ACCEPT  icmp --    eth0   *      0.0.0.0/0
root@dc2336b186ec:/# 
```

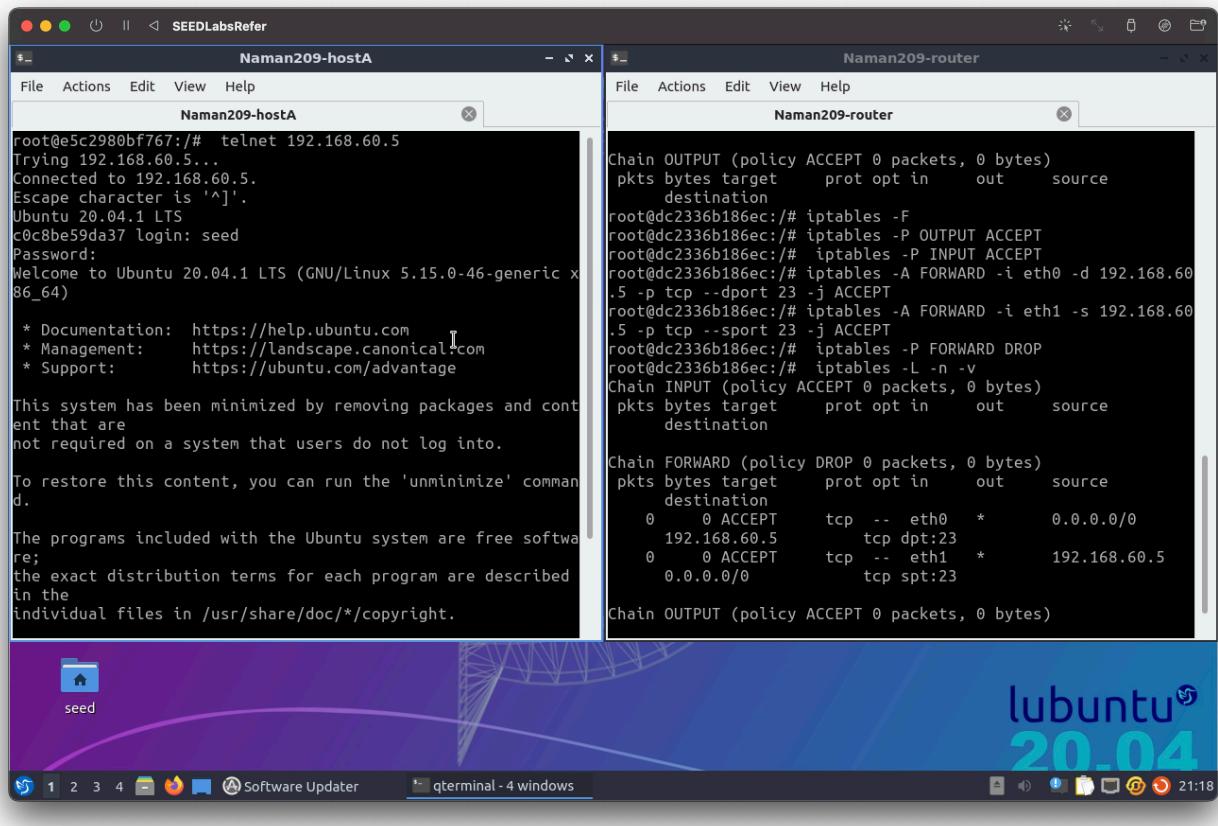
lubuntu 20.04

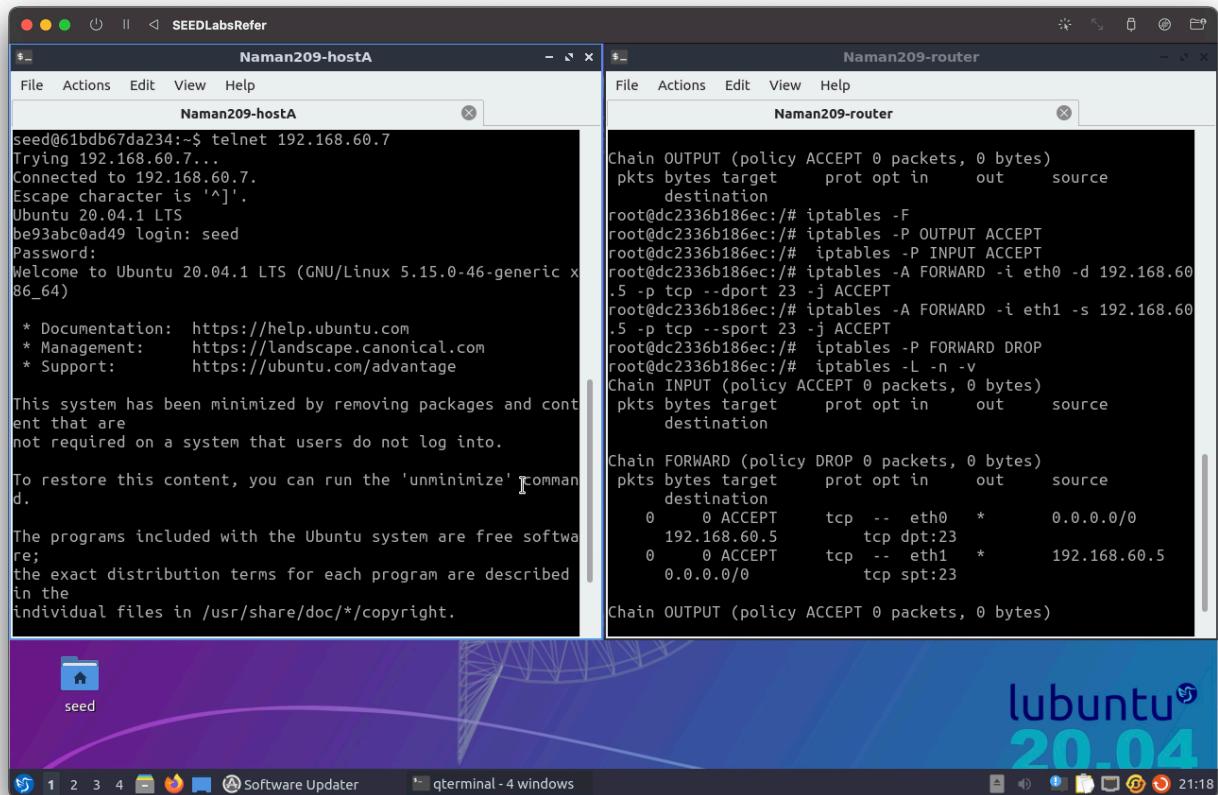
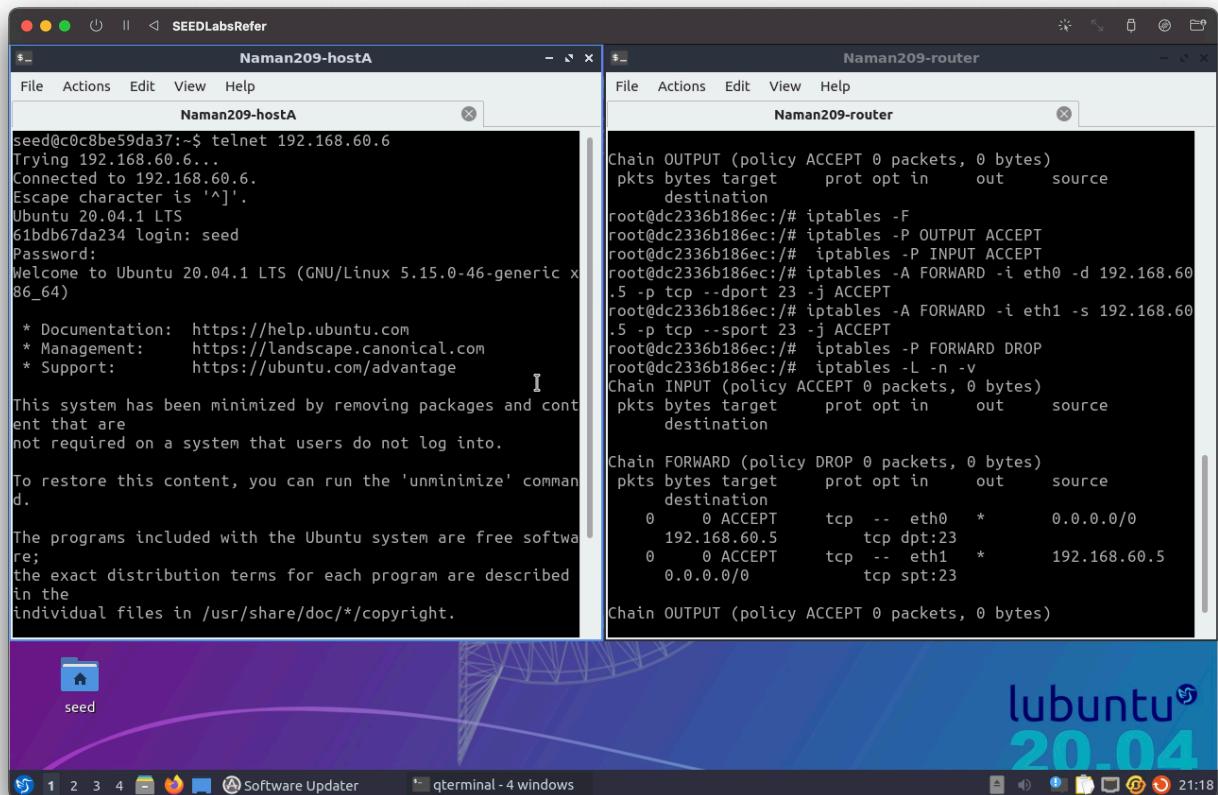
## Task 2.C: Protecting Internal Servers

```
iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 -j ACCEPT # iptables -A FORWARD -i eth1  
iptables -L -n -v
```

In host1:

```
telnet 192.168.60.5  
telnet 192.168.60.6  
telnet 192.168.60.7
```





In host2:

```
telnet 192.168.60.5
telnet 192.168.60.7
telnet 10.9.0.5
```

Bash

The screenshot shows a Lubuntu 20.04 desktop environment with two terminal windows open:

- Naman209-host2:** A terminal window showing a root shell on a host machine. The user runs `telnet 192.168.60.5` and successfully connects to the router's configuration port.
- Naman209-router:** A terminal window showing a root shell on a router machine. The user runs `iptables -L -n -v` to display the current iptables rules. The output shows the following chains:
  - Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)**  
pkts bytes target prot opt in out source destination  
root@dc2336b186ec:/# iptables -F
  - 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 \* 192.168.60.5  
0.0.0.0/0 0 0 ACCEPT tcp spt:23
  - Chain INPUT (policy ACCEPT 0 packets, 0 bytes)**  
pkts bytes target prot opt in out source destination

The desktop interface includes a dock with icons for seed, Software Updater, and qterminal, and a status bar at the bottom.

```
root@061bdb67da234:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^].
Ubuntu 20.04.1 LTS
c0c8be59da37 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-46-generic x86_64)

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

This system has been minimized by removing packages and content 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: Sun Nov 20 15:47:58 UTC 2022 from www.seed-server.com on pts/2
seed@c0c8be59da37:~$ 
```

```
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
root@dc2336b186ec:/# iptables -F
root@dc2336b186ec:/# iptables -P OUTPUT ACCEPT
root@dc2336b186ec:/# iptables -P INPUT ACCEPT
root@dc2336b186ec:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp -dport 23 -j ACCEPT
root@dc2336b186ec:/# iptables -A FORWARD -i eth1 -s 192.168.60.5 -p tcp -sport 23 -j ACCEPT
root@dc2336b186ec:/# iptables -P FORWARD DROP
root@dc2336b186ec:/# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
I
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 * 192.168.60.5
0.0.0.0/0 0 0 ACCEPT tcp spt:23
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
```

```

d.
Last login: Sun Nov 20 15:47:58 UTC 2022 from www.seed-server.com on pts/2
seed@dc0c8be59da37:~$ telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
be93abc0ad49 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-46-generic x86_64)

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

This system has been minimized by removing packages and content 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: Sun Nov 20 15:48:44 UTC 2022 from host2-192.168.60.6.net-192.168.60.0 on pts/1
seed@be93abc0ad49:~$ 
```

```

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination
root@dc2336b186ec:/# iptables -F
root@dc2336b186ec:/# iptables -P OUTPUT ACCEPT
root@dc2336b186ec:/# iptables -P INPUT ACCEPT
root@dc2336b186ec:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 -j ACCEPT
root@dc2336b186ec:/# iptables -A FORWARD -i eth1 -s 192.168.60.5 -p tcp --sport 23 -j ACCEPT
root@dc2336b186ec:/# iptables -P FORWARD DROP
root@dc2336b186ec:/# 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
  0    0 ACCEPT      tcp  --  eth0   *      0.0.0.0/0
  0    0 ACCEPT      tcp  dpt:23  *      192.168.60.5
  0    0 ACCEPT      tcp  --  eth1   *      192.168.60.5
  0    0.0.0.0/0      tcp  spt:23

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
```

```

seed@be93abc0ad49:~$ telnet 10.9.0.5...
Trying 10.9.0.5...
^C
seed@be93abc0ad49:~$ 
```

```

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination
root@dc2336b186ec:/# iptables -F
root@dc2336b186ec:/# iptables -P OUTPUT ACCEPT
root@dc2336b186ec:/# iptables -P INPUT ACCEPT
root@dc2336b186ec:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 -j ACCEPT
root@dc2336b186ec:/# iptables -A FORWARD -i eth1 -s 192.168.60.5 -p tcp --sport 23 -j ACCEPT
root@dc2336b186ec:/# iptables -P FORWARD DROP
root@dc2336b186ec:/# 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
  0    0 ACCEPT      tcp  --  eth0   *      0.0.0.0/0
  0    0.0.0.0/0      tcp  dpt:23  *      192.168.60.5
  0    0 ACCEPT      tcp  --  eth1   *      192.168.60.5
  0    0.0.0.0/0      tcp  spt:23

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
```

Observation:

`iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 -j ACCEPT` It accepts any tcp connection on the interface eth0 where the destination port is 23 and ip is 192.168.60.5

```
iptables -A FORWARD -i eth1 -s 192.168.60.5 -p tcp --sport 23 -j ACCEPT
```

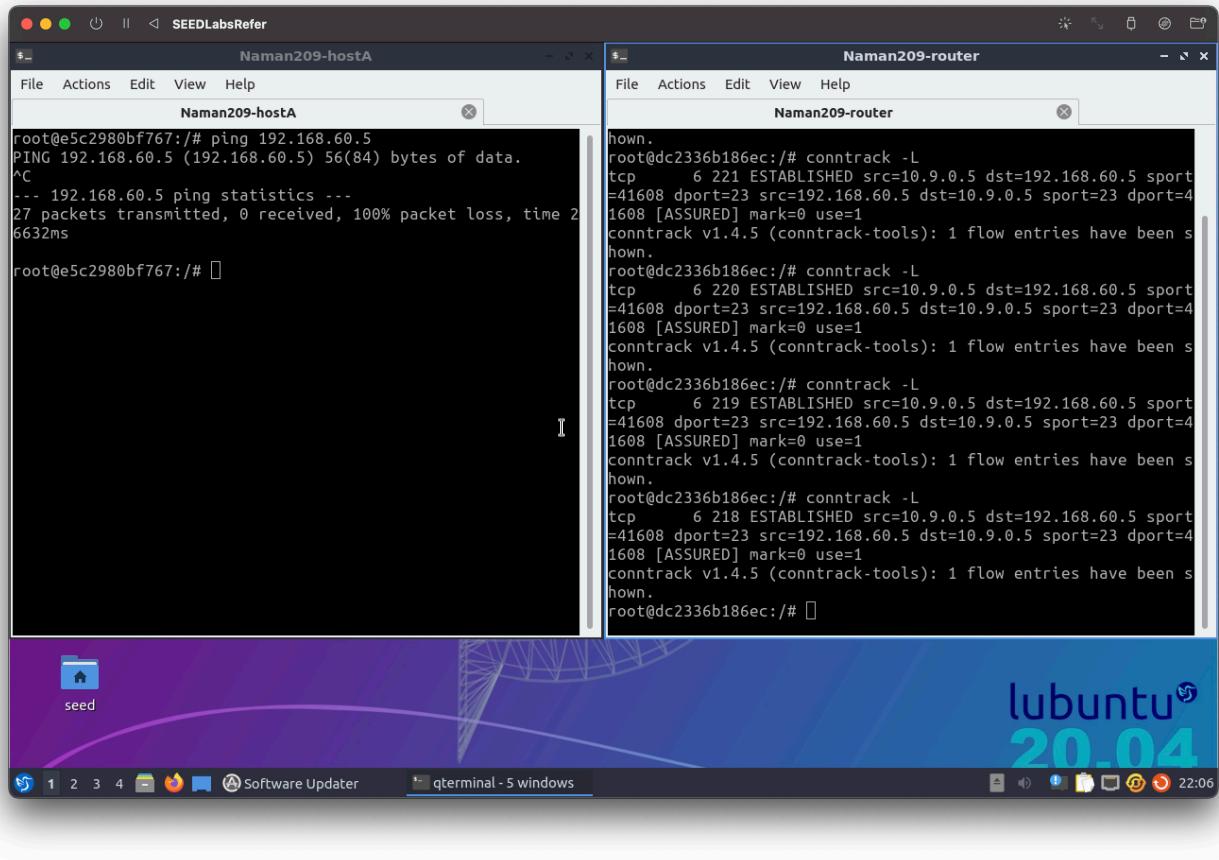
It accepts any tcp connection on the interface eth1 where the source port is 23 and ip is 192.168.60.5

## Task 3: Connection Tracking and Stateful Firewall

### Task 3.A: Experiment with the Connection Tracking

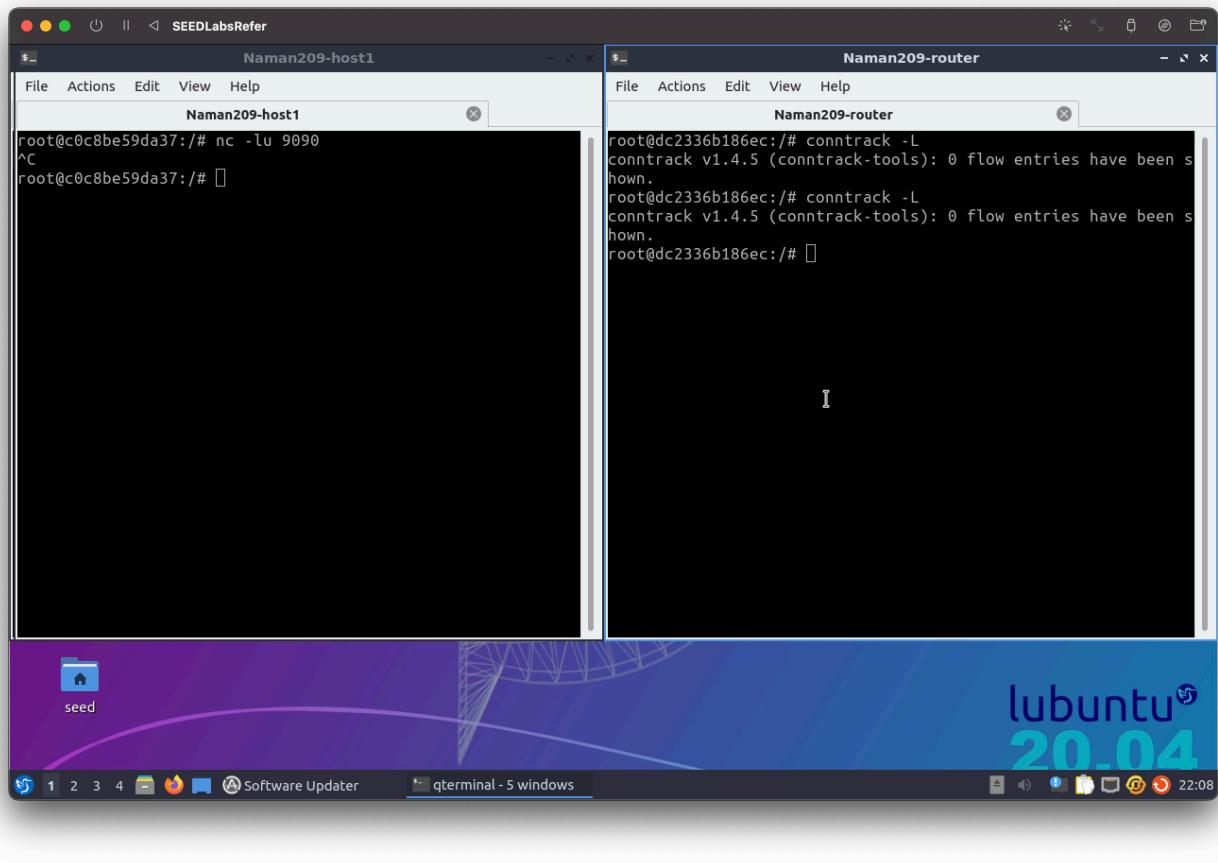
```
ping 192.168.60.5  
conntrack -L
```

Bash



```
nc -l 9090
```

Bash

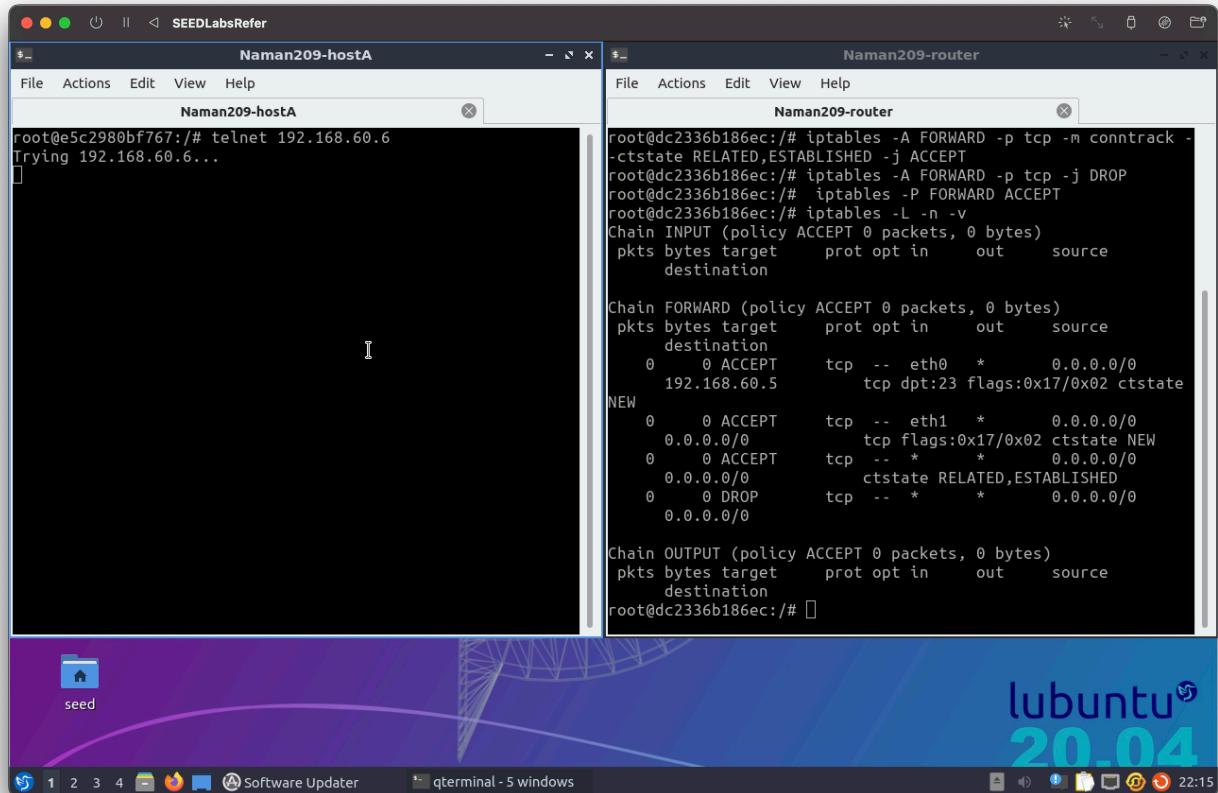
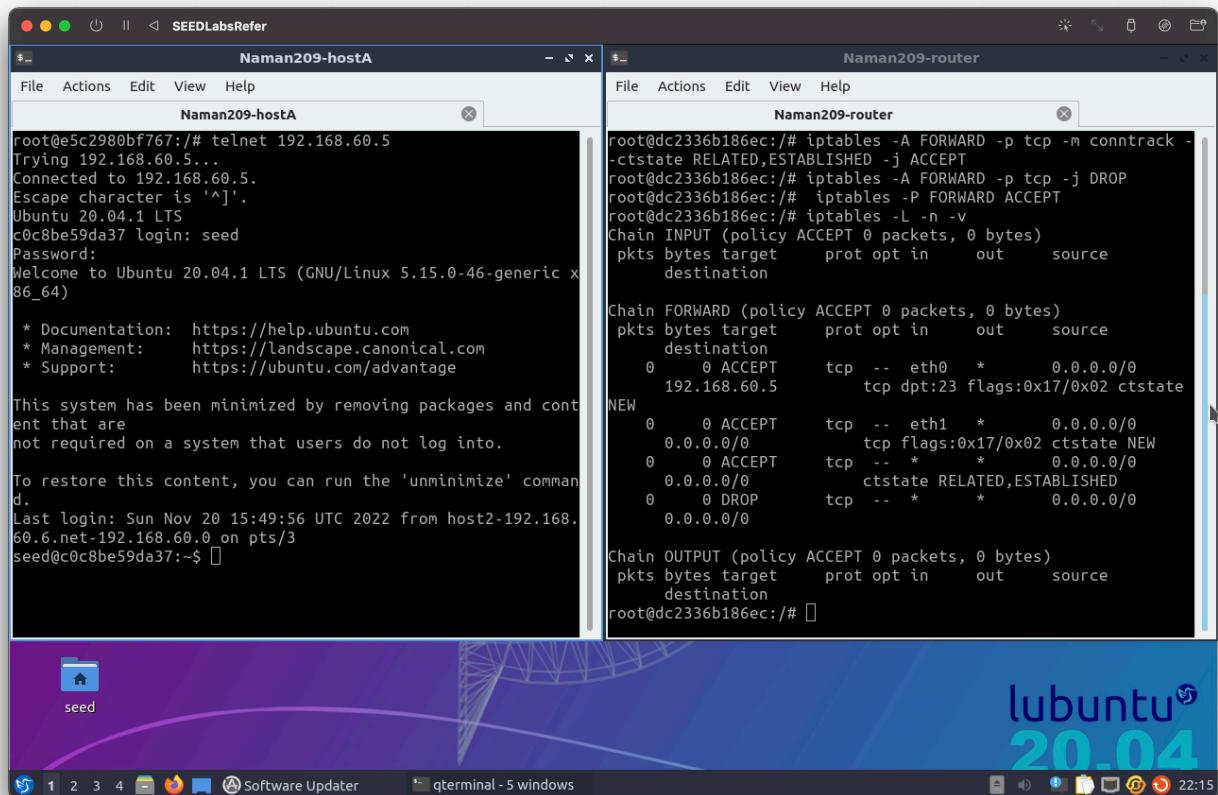


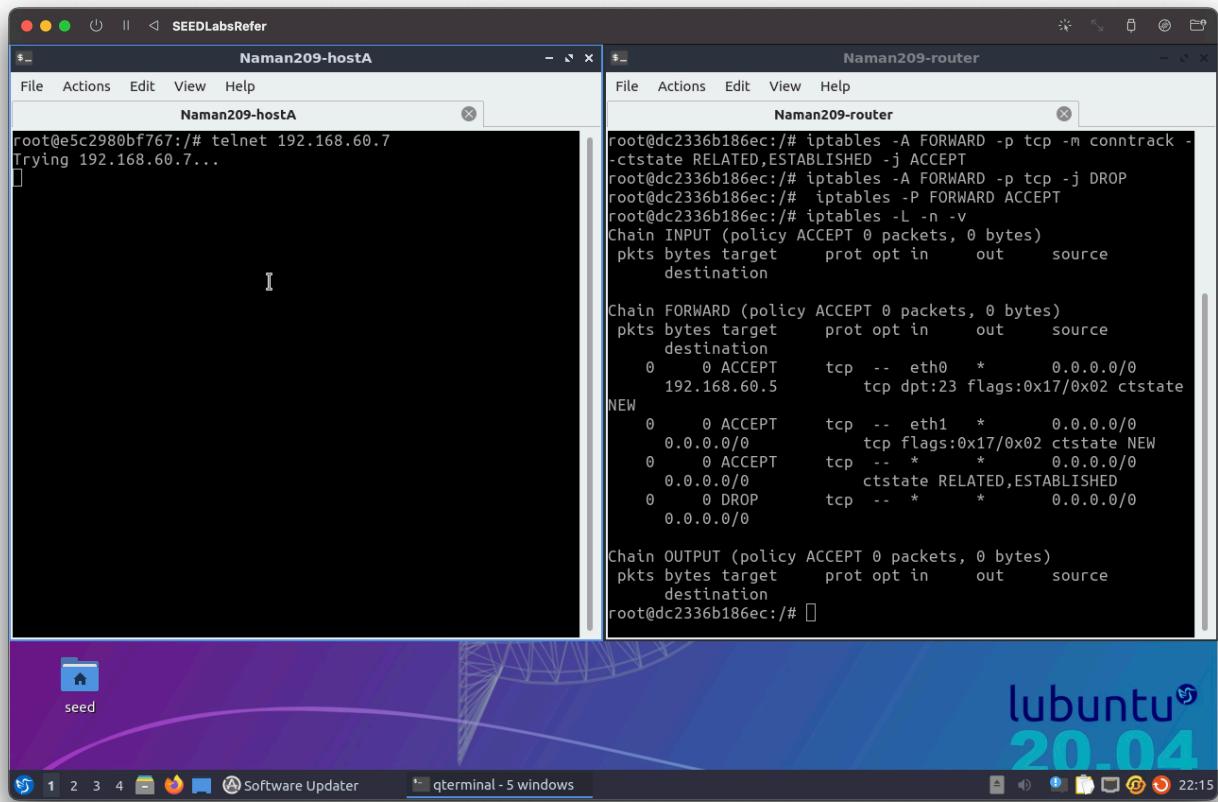
### Task 3.B: Setting Up a Stateful Firewall

```
iptables -A FORWARD -p tcp -i eth0 -d 192.168.60.5 --dport 23 --syn -m conntrack --ctstate NEW -j ACCEPT
iptables -A FORWARD -i eth1 -p tcp --syn -m conntrack --ctstate NEW -j ACCEPT
iptables -A FORWARD -p tcp -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -p tcp -j DROP # iptables -P FORWARD ACCEPT
iptables -L -n -v
```

On host A:

```
telnet 192.168.60.5
telnet 192.168.60.6
telnet 192.168.60.7
```





On host 2:

```
telnet 192.168.60.5
telnet 192.168.60.7
telnet 10.9.0.5
```

SEEDLabsRefer

Naman209-host2

```
root@61bdb67da234:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c0c8be59da37 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-46-generic x86_64)

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

This system has been minimized by removing packages and content 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: Sun Nov 20 16:45:47 UTC 2022 from host3-192.168.60.7.net-192.168.60.0 on pts/4
seed@c0c8be59da37:~$ 
```

Naman209-router

```
root@dc2336b186ec:/# iptables -A FORWARD -p tcp -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
root@dc2336b186ec:/# iptables -A FORWARD -p tcp -j DROP
root@dc2336b186ec:/# iptables -P FORWARD ACCEPT
root@dc2336b186ec:/# 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
          0     0 ACCEPT    tcp  --  192.168.60.5  dpt:23 flags:0x17/0x02 ctstate NEW
          0     0 ACCEPT    tcp  --  eth1   *      0.0.0.0/0
          0     0 ACCEPT    tcp  --  *      *      0.0.0.0/0
          0     0 ACCEPT    tcp  --  0.0.0.0/0 ctstate RELATED,ESTABLISHED
          0     0 DROP      tcp  --  *      *      0.0.0.0/0
          0     0 ACCEPT    tcp  --  eth1   *      0.0.0.0/0
          0     0 ACCEPT    tcp  --  flags:0x17/0x02 ctstate NEW
          0     0 ACCEPT    tcp  --  *      *      0.0.0.0/0
          0     0 DROP      tcp  --  *      *      0.0.0.0/0
Chain FORWARD (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
          0     0 ACCEPT    tcp  --  192.168.60.5  dpt:23 flags:0x17/0x02 ctstate NEW
          0     0 ACCEPT    tcp  --  eth1   *      0.0.0.0/0
          0     0 ACCEPT    tcp  --  *      *      0.0.0.0/0
          0     0 ACCEPT    tcp  --  0.0.0.0/0 ctstate RELATED,ESTABLISHED
          0     0 DROP      tcp  --  *      *      0.0.0.0/0
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in      out      source destination
root@dc2336b186ec:/# 
```

lubuntu 20.04

SEEDLabsRefer

Naman209-host2

```
root@61bdb67da234:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
be93abc0ad49 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-46-generic x86_64)

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

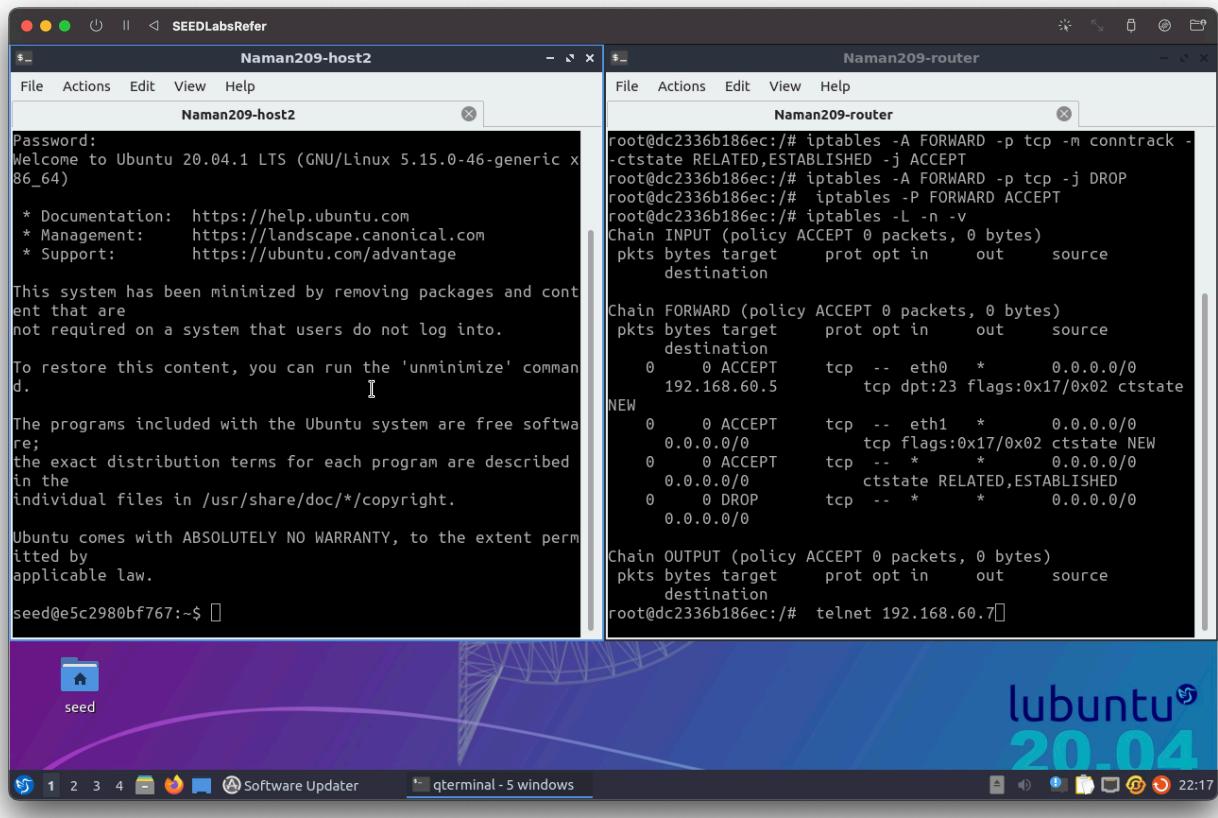
This system has been minimized by removing packages and content that are not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Nov 20 15:50:11 UTC 2022 from host1-192.168.60.5.net-192.168.60.0 on pts/2
seed@be93abc0ad49:~$ 
```

Naman209-router

```
root@dc2336b186ec:/# iptables -A FORWARD -p tcp -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
root@dc2336b186ec:/# iptables -A FORWARD -p tcp -j DROP
root@dc2336b186ec:/# iptables -P FORWARD ACCEPT
root@dc2336b186ec:/# 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
          0     0 ACCEPT    tcp  --  192.168.60.5  dpt:23 flags:0x17/0x02 ctstate NEW
          0     0 ACCEPT    tcp  --  eth1   *      0.0.0.0/0
          0     0 ACCEPT    tcp  --  *      *      0.0.0.0/0
          0     0 ACCEPT    tcp  --  0.0.0.0/0 ctstate RELATED,ESTABLISHED
          0     0 DROP      tcp  --  *      *      0.0.0.0/0
          0     0 ACCEPT    tcp  --  eth1   *      0.0.0.0/0
          0     0 ACCEPT    tcp  --  flags:0x17/0x02 ctstate NEW
          0     0 ACCEPT    tcp  --  *      *      0.0.0.0/0
          0     0 DROP      tcp  --  *      *      0.0.0.0/0
Chain FORWARD (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
          0     0 ACCEPT    tcp  --  192.168.60.5  dpt:23 flags:0x17/0x02 ctstate NEW
          0     0 ACCEPT    tcp  --  eth1   *      0.0.0.0/0
          0     0 ACCEPT    tcp  --  *      *      0.0.0.0/0
          0     0 ACCEPT    tcp  --  0.0.0.0/0 ctstate RELATED,ESTABLISHED
          0     0 DROP      tcp  --  *      *      0.0.0.0/0
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in      out      source destination
root@dc2336b186ec:/# telnet 192.168.60.7
```

lubuntu 20.04



Observation:

```
iptables -A FORWARD -p tcp -i eth0 -d 192.168.60.5 --dport 23 --syn -m conntrack --ctstate NEW -j ACCEPT
```

It accepts any tcp connection on the interface eth0 where the destination port is 23 and ip is 192.168.60.5 using the conntrack module

```
iptables -A FORWARD -i eth1 -p tcp --syn -m conntrack --ctstate NEW -j ACCEPT
```

It accepts connections on eth1 interface using the conntrack module

#### Task 4: Limiting Network Traffic

```
iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/minute --limit-burst 5 -j ACCEPT
iptables -A FORWARD -s 10.9.0.5 -j DROP
iptables -L -n -v
```

```
ping 192.168.60.5
```

```
root@e5c2980bf767:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=3.23 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=1.93 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=1.97 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=1.60 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=2.13 ms
^C
--- 192.168.60.5 ping statistics ---
6 packets transmitted, 5 received, 16.6667% packet loss, time 5010ms
rtt min/avg/max/mdev = 1.601/2.174/3.234/0.557 ms
root@e5c2980bf767:/# 
```

```
root@dc2336b186ec:/# iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/minute --limit-burst 5 -j ACCEPT
root@dc2336b186ec:/# iptables -A FORWARD -s 10.9.0.5 -j DROP
root@dc2336b186ec:/# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination
          0      0 ACCEPT    all  --  *      *      10.9.0.5
          0      0 0.0.0.0/0  limit: avg 10/min burst 5
          0      0 DROP      all  --  *      *      10.9.0.5
          0      0 0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination
          0      0 ACCEPT    all  --  *      *      10.9.0.5
          0      0 0.0.0.0/0  limit: avg 10/min burst 5
          0      0 DROP      all  --  *      *      10.9.0.5
          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@dc2336b186ec:/# 
```

```
iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/minute --limit-burst 5 -j ACCEPT
iptables -L -n -v
```

```
ping 192.168.60.5
```

```

root@e5c2980bf767:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=1.01 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=3.39 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=3.93 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=2.20 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=2.51 ms
^C
--- 192.168.60.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4022 ms
rtt min/avg/max/mdev = 1.014/2.609/3.933/1.007 ms
root@e5c2980bf767:/# 

root@dc2336b186ec:/# iptables -F
root@dc2336b186ec:/# iptables -P OUTPUT ACCEPT
root@dc2336b186ec:/# iptables -P INPUT ACCEPT
root@dc2336b186ec:/# iptables -A FORWARD -s 10.9.0.5 -m limit --limit 10/minute --limit-burst 5 -j ACCEPT
root@dc2336b186ec:/# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source
destination
      0      0 ACCEPT    all  --  *      *      10.9.0.5
      0      0.0.0/0      limit: avg 10/min burst 5
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source
destination
      0      0 ACCEPT    all  --  *      *      10.9.0.5
      0      0.0.0/0      limit: avg 10/min burst 5
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source
destination
root@dc2336b186ec:/# 

```

## Task 5: Load Balancing

```

iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --packet 0 -j DNAT
iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 2 --packet 0 -j DNAT
iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 1 --packet 0 -j DNAT
iptables -L -n -v

```

On Host 1,2,3

```

nc -luk 8080
nc -luk 8080
nc -luk 8080

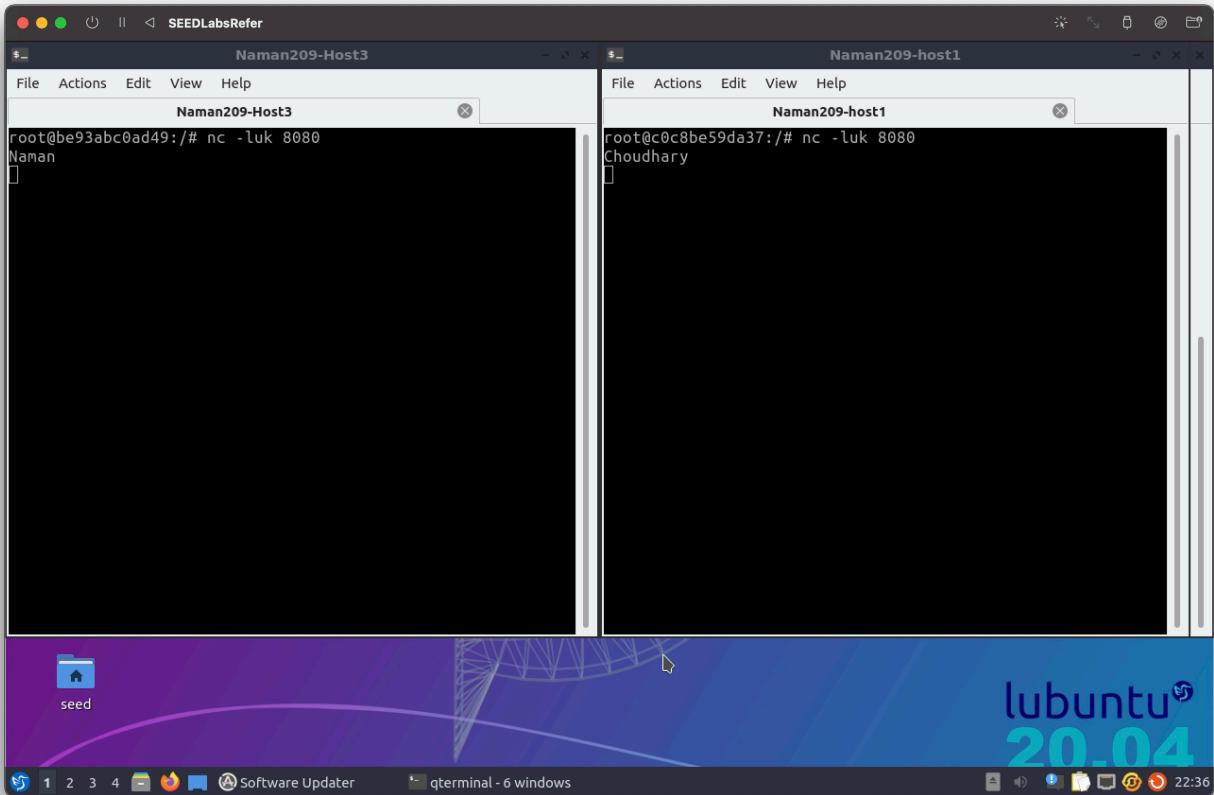
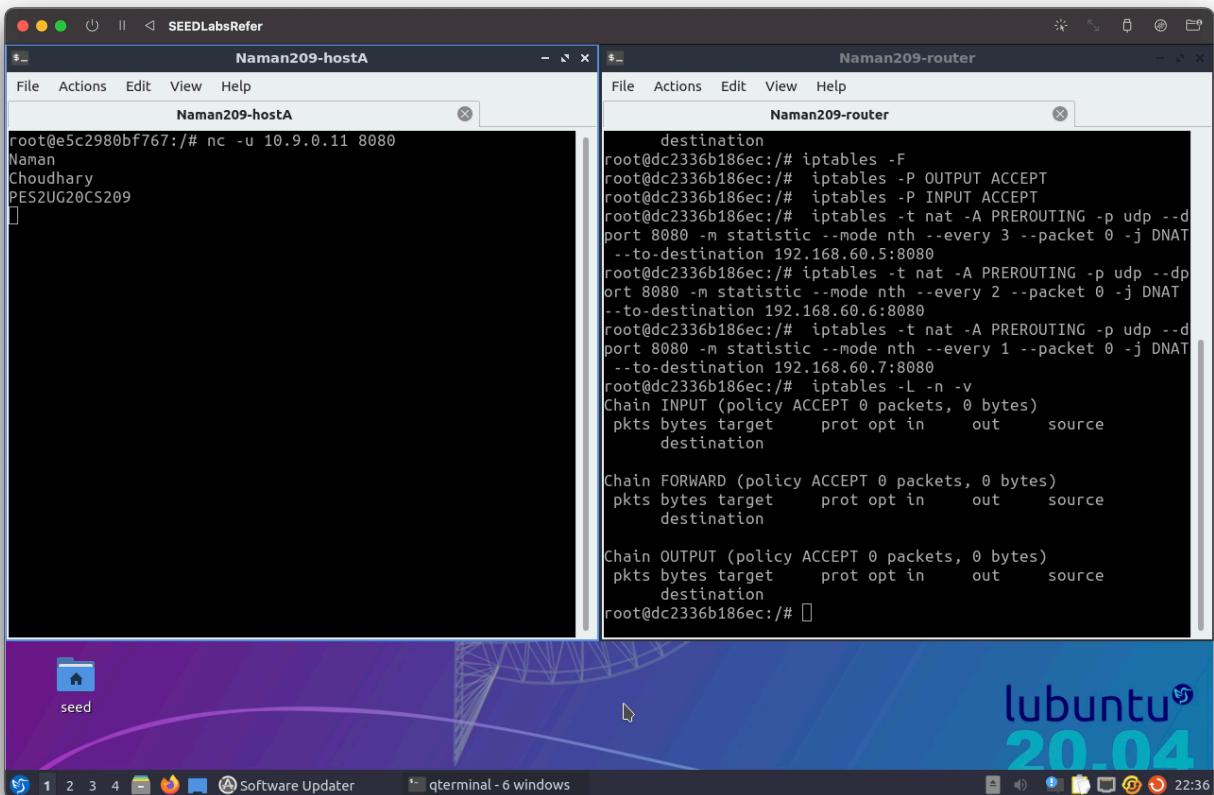
```

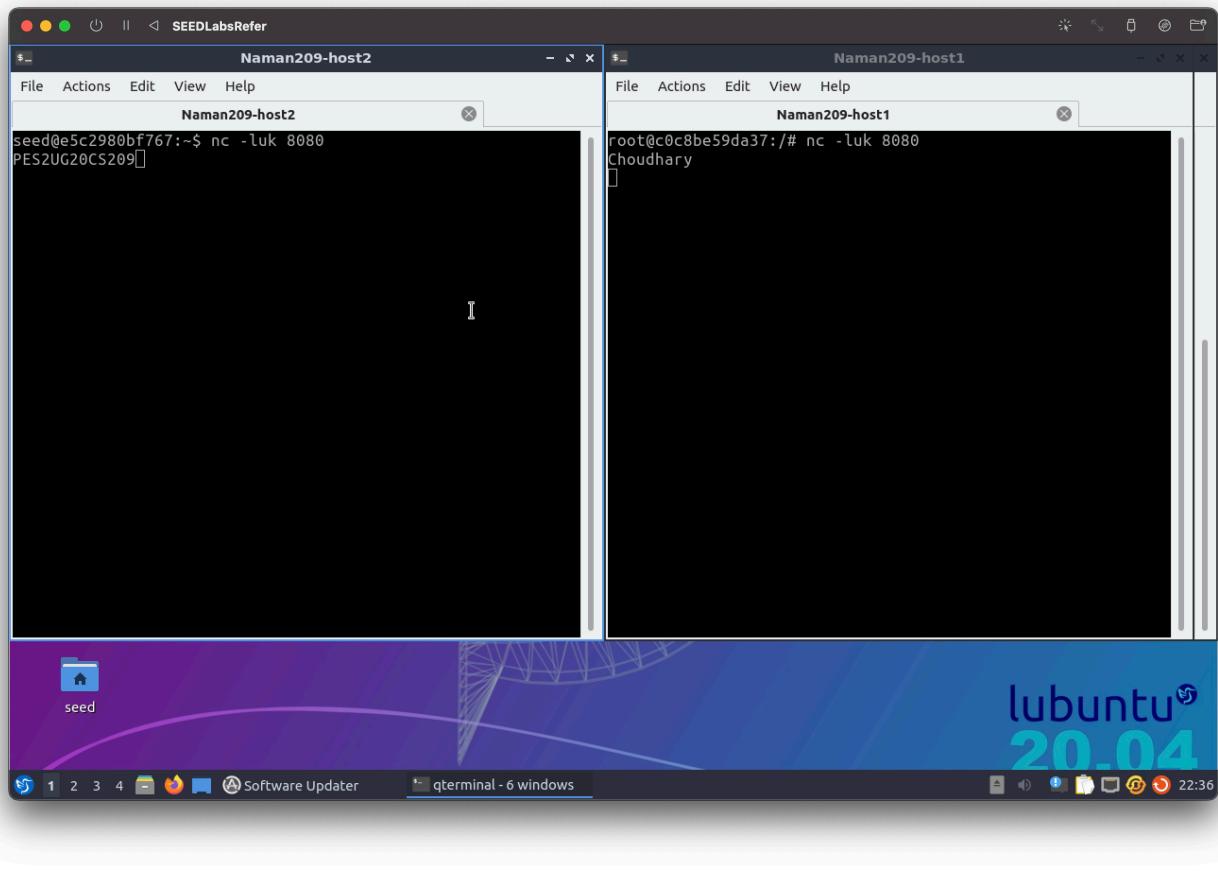
On Host A

```

nc -u 10.9.0.11 8080
< enter 3 words, wait 30 seconds before entering the next word>

```





### random mode

```
Bash
iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 0.3333 -j DNAT
iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 0.5 -j DNAT
iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 1 -j DNAT
iptables -L -n -v
```

On Host 1,2,3

```
Bash
nc -luk 8080
nc -luk 8080
nc -luk 8080
```

On Host A

```
Bash
nc -u 10.9.0.11 8080
< enter 3 words, wait 30 seconds before entering the next word>
```

