Task 1: Using Firewall

a.Prevent A(10.0.2.4) from doing telnet to Machine B(10.0.2.5).

```
sudo ufw enable => sudo ufw deny out 23/tcp //Doing this on machine A
```

b.Prevent B from doing telnet to Machine A.

```
sudo ufw enable => sudo ufw deny in 23/tcp
```

c.Prevent A from visiting an external web site. You can choose any website that you like to block, but keep in mind, some web servers have multiple IP addresses.

```
ping facebook.com => sudo ufw deny out to 157.240.22.19
```

//Firewall rules are only modified under root privilege.

Task 2: How Firewall Works(Host on VM2-10.0.2.4)

//rules.o

```
ip_header = (struct iphdr *)skb_network_header(sock_buff); //Grabbing IP header
```

a.Drop icmp request packet from VM3(10.0.2.5).

```
if(IP_header->protocol==1)&if(icmp_header->type == 8 && icmp_header->code == 0 && ((ip_header->saddr & 0xff000000) >> 24) == 5) => return NF_DROP;
```

b.Drop all telnet packets.

```
if(ip_header->protocol == 6)&if(dst_port==23) => return NF_DROP;
```

c.Drop all packets from VM1(10.0.2.15)

```
if(((ip_header->saddr & 0xff000000) >> 24) == 15); => return NF_DROP;
```

//Makefile.txt

```
Obj-m +=rules.o
All: make -C /lib/modules/$(shell uname -r)/build/ M=/home/seed/firewall_prog/ modules
```

//Need to modify /lib/modules/$(shell uname -r)/build/Makefile

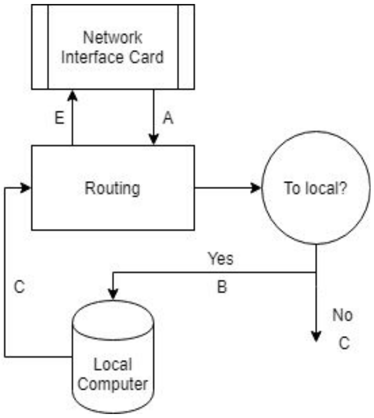
Disable #enforce correct pointer usage incompatible-pointer-types

//Then use command “sudo make” to generate rules.ko => insert rules with “insmod rules.ko”

To view all active modules/rules, use “lsmod”, to remove one, use “rmmod rules”

Question 1: What types of hooks does Netfilter support, and what can you do with these hooks? Please draw a diagram to show how packets flow through these hooks.

A.NF_INET_PRE_ROUTING: Hook placed before incoming packets coming to the routing code.
B.NF_INET_LOCAL_IN: When incoming packets pass through routing and comes to local.
C.NF_INET_FORWARD: When incoming packets pass through routing but towards to others.
D.NP_INET_LOCAL_OUT: Any packets were just sent out from local.
E.NF_INET_POST_ROUTING: Before packets leave the network where the local is located.



Question 2: Where should you place a hook for ingress filtering, and where should you place a hook for egress filtering?

Since we want to deal with the packets earlier. I chose A&C.

Question 3: Can you modify packets using Netfilter?

Yes we can modify received packets’ dst port, ip and checksum with Loadable Kernel Module, an object file(.ko) that contains code to extend the running kernel.

Hedao Tian 1256221
SEED Labs – Linux Firewall Exploration Lab

Task 3: Evading Egress Filtering

a: Telnet to VM3(10.0.2.5) through the firewall.(Through VM1(10.0.2.15))

ssh -L 8000:10.0.2.5:23 10.0.2.15 //Use SSH(port 22) connect to VM1=> port 23

b: Connecting to Facebook using SSH Tunnel.

ssh -D 9000 -C 10.0.2.15 //Since VM2 talks with VM1 in ethernet, ip information is not transmitted in their SSH packets. Cach cleaning is required. Dynamic port forwarding.

socks Host 127.0.0.1 Port 9000 //When you're hosting a SOCKS proxy on your local PC, you'll need to enter 127.0.0.1 and the port the SOCKS proxy is listening on. For example, you'll need to do this if you create an SSH tunnel using dynamic port forwarding and want to send your browsing traffic through it.

Question 4: If ufw blocks the TCP port 22, which is the port used by SSH, can you still set up an SSH tunnel to evade egress filtering?

Yes. The SSH used port number can be changed in file /etc/ssh/sshd.conf.

Task 4: Web Proxy (Application Firewall)

a: Setup.

IP 10.0.2.15 Port 3128 //Define proxy server IP with its default listening port.

sudo gedit /etc/squid/squid.conf //Open proxy setting file on proxy machine.

acl one_site dstdomain www.google.ca

http_access allow one_site & http_access deny all //Allow only one_site

b: Using Web Proxy to evade Firewall.

sudo ufw deny out to *IP of www.google.com // It's allowed by squid, so we can bypass.

Question 5: If ufw blocks the TCP port 3128, can you still use web proxy to evade the firewall?

Yes. The listening port number can be changed into different one in squid.conf.

c: URL Rewriting/Redirection.

url_rewrite_program /etc/squid/myprog.pl

url_rewrite_children 5 //Insert the program for running. I also inserted one_site2 as www.hedaotian.com and allowed it to be accessed in order to achieve the test.