Parth R Doshi

ECE 404 – HW09

#1 Flush and delete all previously defined rules and chains.

```
sudo iptables -t filter -F

sudo iptables -t filter -X

sudo iptables -t mangle -F

sudo iptables -t mangle -X

sudo iptables -t nat -F

sudo iptables -t nat -X

sudo iptables -t raw -F

sudo iptables -t raw -X
```

Description : These commands delete all previously defined rules and chains. Every rule begins with the words ‘sudo iptables’ followed by the flag for the table we want to operate on, in this case it is the ‘filter’ table. The ‘-F’ flag deletes any previous flag. In a similar manner this operation is carried out for all the different tables : filter, mangle, nat, and raw.

#2 Write a rule that only accepts packets that originate from f1.com.

```
sudo iptables -t filter -A INPUT -j DROP

sudo iptables -t filter -A INPUT -p tcp -s 67.199.248.12 -j ACCEPT
```

Description : The rule specifies from which IP address should the machine accept packets from using the ‘ACCEPT’ target. This IP address is the IP address of ‘f1.com.’ This was found using ‘ping f1.com’ in the terminal.

#3 For all outgoing packets, change their source IP address to your own machine’s IP address

# (Hint: Refer to the MASQUERADE target in the nat table).

```
sudo iptables -t nat -A POSTROUTING -o eth0 -p tcp -j MASQUERADE
```

Description : To reroute the packets from one IP address to another, we use the POSTROUTING flag which alters the packets as they are about to go out. This time we need to access the ‘nat’ tables and use the target ‘MASQUERADE.’

#4 Write a rule to protect yourself against indiscriminate and nonstop scanning of ports on your machine.

```
sudo iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST SYN -m limit --limit 1/s -j ACCEPT
```

Description : To protect my machine from nonstop port scanning we use the limit argument to limit any SYN, ACK, FIN or RST packets. These packets are required to establish connection as learned in lecture. The ‘—limit 1/s’ limits the number of incoming new connection requests to 1 per second.

#5 Write a rule to protect yourself from a SYN-flood Attack by limiting the number of incoming

# 'new connection' requests to 1 per second once your machine has reached 500 requests.

```
sudo iptables -A FORWARD -p tcp --syn -m limit --limit 1/s --limit-burst 500 -j ACCEPT
```

This limits the number of SYN packets or new connection requests to 1 per second once the machine reaches 500 requests. The '–limit-burst' allows us to specify the number of requests after which we want to apply the condition.

```
#6 Write a rule to allow full loopback access on your machine i.e. access using localhost

# (Hint: You will need two rules, one for the INPUT chain and one the OUTPUT chain on the

# FILTER table. The interface is 'lo'.)

sudo iptables -t filter -A INPUT -i lo -j ACCEPT

sudo iptables -t filter -A OUTPUT -i lo -j ACCEPT
```

Description : This allows you to access the localhost by specifying the 'lo' argument. Here we need two rules if we want full loop back access. This includes the INPUT and OUTPUT chain.

```
#7 Write a port forwarding rule that routes all traffic arriving on port 8888 to port 25565. Make

# sure you specify the correct table and chain. Subsequently, the target for the rule should be

# DNAT.

sudo iptables -t nat -A PREROUTING -p tcp --dport 8888 -j DNAT --to-destination :25565
```

Description : This rule allows for port forwarding. For this we must use the 'nat' tables. To redirect all the traffic arriving on a specific port. The –dport specifies the source port which is 8888 and the destination port is 25565. The protocol used is TCP which is also specified. PREROUTING signifies that the alters the packet as it comes in.

```
#8 Write a rule that only allows outgoing ssh connections to engineering.purdue.edu. You

# will need two rules, one for the INPUT chain and one for the OUTPUT chain on the FILTER

# table. Make sure to specify the correct options for the --state suboption for both rules.

sudo iptables -A OUTPUT -p tcp --dport 22 -d engineering.purdue.edu -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A INPUT -p tcp --sport 22 -s engineering.purdue.edu -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
```

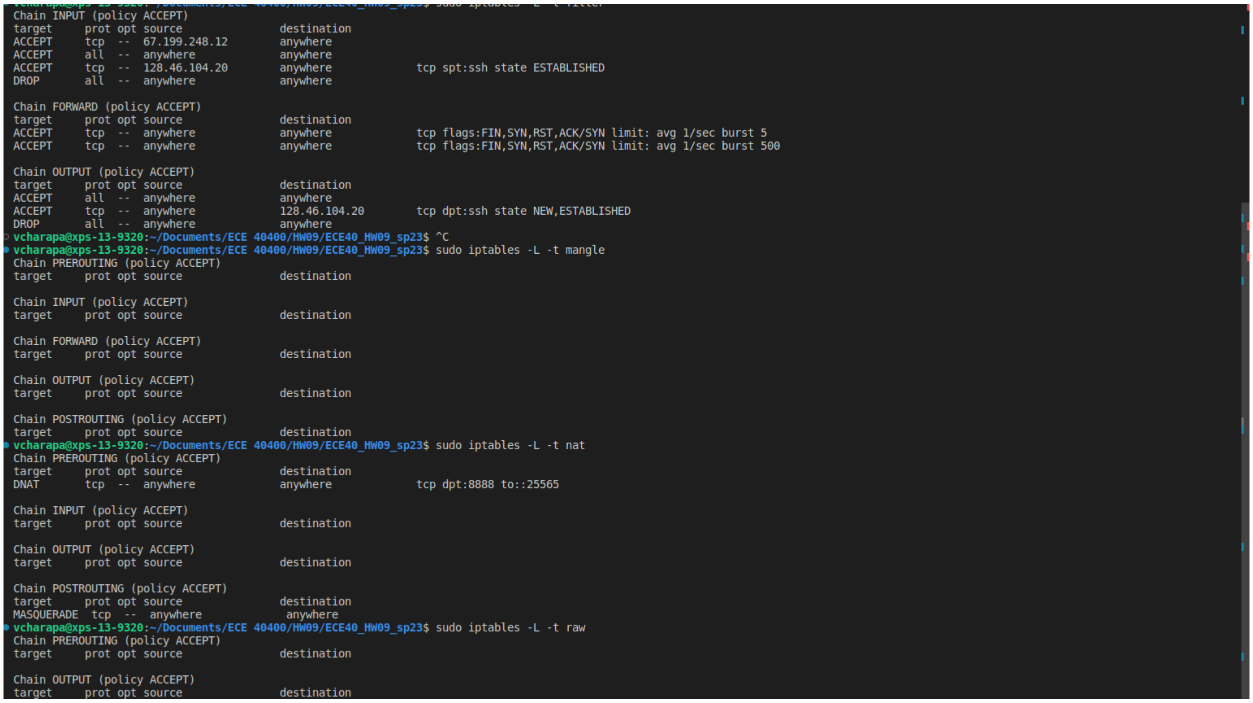
Description : port is 22 – purdue server, state is NEW, ESTABLISHED for the OUTPUT chain

Port is 22 – purdue server, state state is ESTABLISHED for the INPUT chain

```
#9 Drop any other packets if they are not caught by the above rules.

sudo iptables -A OUTPUT -j DROP

sudo iptables -A INPUT -j DROP
```

Description : Drops all the packets if the rules are not caught.

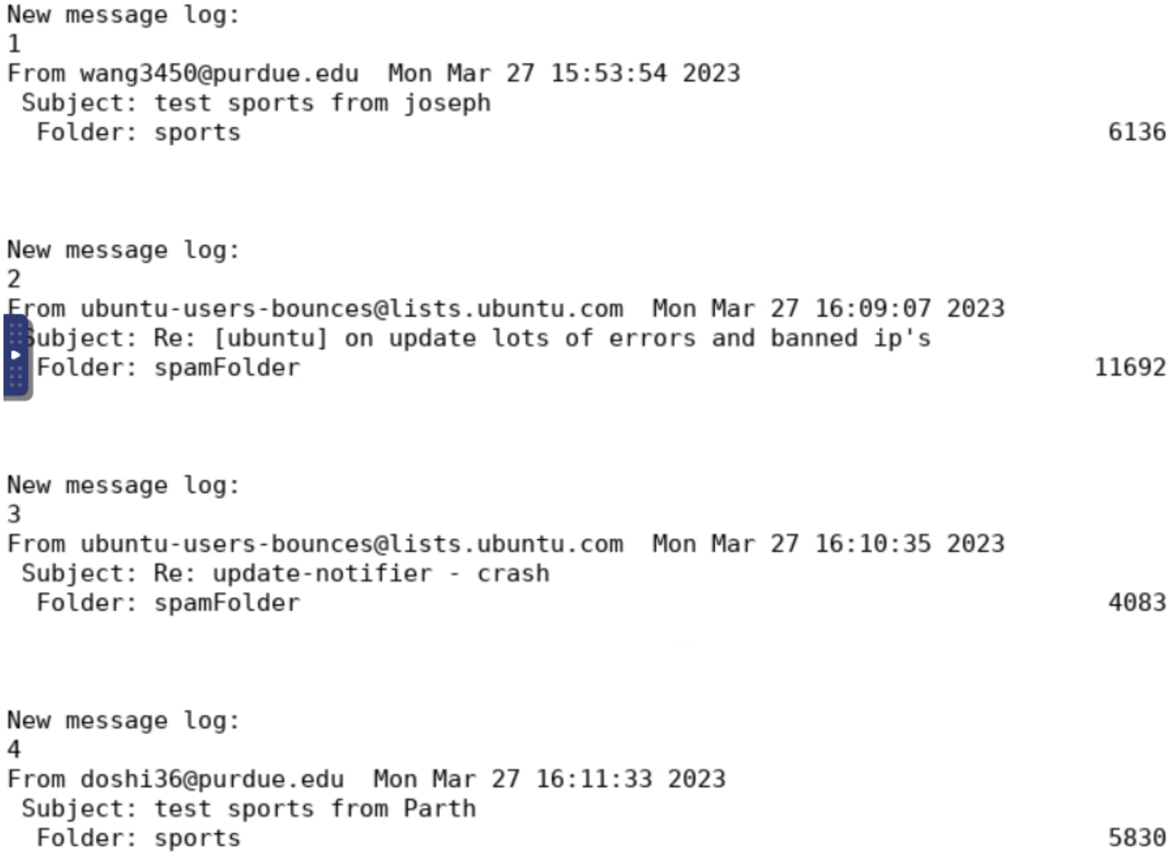
Output of uploaded firewall after running fire404.sh



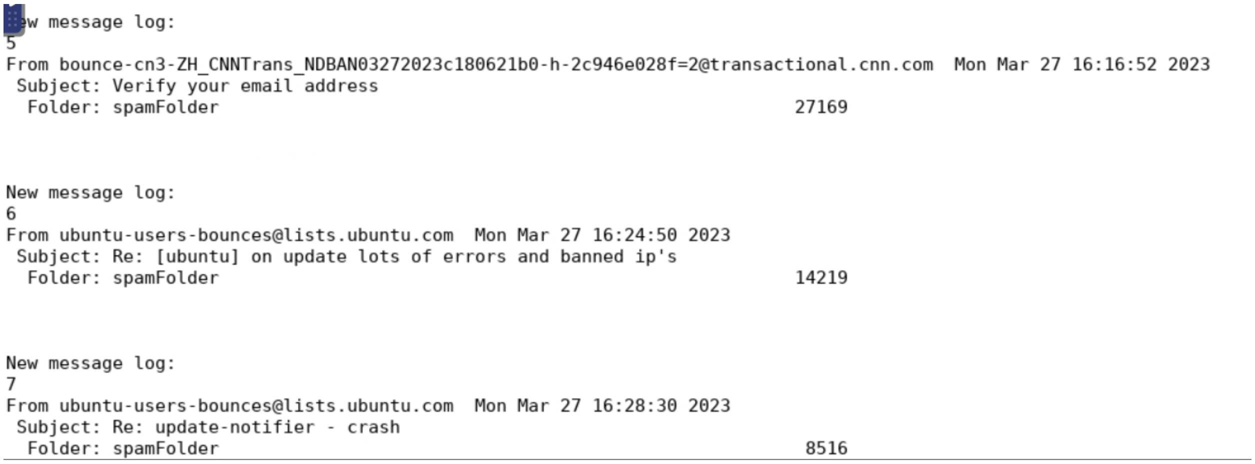
```
vcharapa@xps-13-9320:~/Documents/ECE 40400/HW09/ECE40_HW09_sp23$ sudo iptables -L -t filter
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  67.199.248.12        anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  128.46.104.20        anywhere             tcp spt:ssh state ESTABLISHED
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/SYN limit: avg 1/sec burst 5
ACCEPT     tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/SYN limit: avg 1/sec burst 500

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             128.46.104.20        tcp dpt:ssh state NEW,ESTABLISHED
DROP       all  --  anywhere             anywhere
vcharapa@xps-13-9320:~/Documents/ECE 40400/HW09/ECE40_HW09_sp23$ ^C
vcharapa@xps-13-9320:~/Documents/ECE 40400/HW09/ECE40_HW09_sp23$ sudo iptables -L -t mangle
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

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

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
vcharapa@xps-13-9320:~/Documents/ECE 40400/HW09/ECE40_HW09_sp23$ sudo iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             anywhere             tcp dpt:8888 to::25565

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  tcp  --  anywhere             anywhere
vcharapa@xps-13-9320:~/Documents/ECE 40400/HW09/ECE40_HW09_sp23$ sudo iptables -L -t raw
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

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

Note : This is printed from another friend’s machine since it is a Linux system.

Logfile Contents



```
New message log:
1
From wang3450@purdue.edu  Mon Mar 27 15:53:54 2023
 Subject: test sports from joseph
  Folder: sports                                                           6136



New message log:
2
From ubuntu-users-bounces@lists.ubuntu.com  Mon Mar 27 16:09:07 2023
 Subject: Re: [ubuntu] on update lots of errors and banned ip's
  Folder: spamFolder                                                      11692



New message log:
3
From ubuntu-users-bounces@lists.ubuntu.com  Mon Mar 27 16:10:35 2023
 Subject: Re: update-notifier - crash
  Folder: spamFolder                                                       4083



New message log:
4
From doshi36@purdue.edu  Mon Mar 27 16:11:33 2023
 Subject: test sports from Parth
  Folder: sports                                                           5830
```



```
New message log:
5
From bounce-cn3-ZH_CNNTrans_NDBAN03272023c180621b0-h-2c946e028f=2@transactional.cnn.com  Mon Mar 27 16:16:52 2023
 Subject: Verify your email address
  Folder: spamFolder                                                      27169



New message log:
6
From ubuntu-users-bounces@lists.ubuntu.com  Mon Mar 27 16:24:50 2023
 Subject: Re: [ubuntu] on update lots of errors and banned ip's
  Folder: spamFolder                                                      14219



New message log:
7
From ubuntu-users-bounces@lists.ubuntu.com  Mon Mar 27 16:28:30 2023
 Subject: Re: update-notifier - crash
  Folder: spamFolder                                                       8516
```