HW 9 ECE 404

Nimal Padmanabhan
March 28, 2023

For this programming assignment, we were assigned to write firewall rules in Linux using **iptables**. To start things off, we begin by flushing out previously defined rules and chains in the **filter, mangle, nat, and raw** tables in order to start writing new firewall rules. Next, we begin by writing a rule that only accepts packets originating from the **f1.com** domain by using the **ACCEPT** flag, which is applied to the **INPUT** chain. Then, we want to change the source IP address to match the IP address of the local machine. We do so by using the **nat** and **POSTROUTING** flags. We are supposed to specify the host name ID, which we can get by doing an **ifconfig** command (mine was wlp59s0). We add a **MASQUERADE** flag at the end of command to do the translation of the source IP address to the local IP address. To prevent indiscriminate port scanning and SYN-flood attacks, we do the following commands:

sudo iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST NONE -m limit --limit 1/s -j ACCEPT
sudo iptables -A FORWARD -p tcp --syn -m limit --limit 1/s --limit-burst 500 -j ACCEPT

The –**limit and –limit-burst** commands enforce restrictions on how frequently the packets are sent and how many packets can be sent. In this case, the number of incoming connections is limited to 1 per second, and it caps out at 500 requests. These limit rules are applied to the **FORWARD** chain. Next, we allow full loopback access on the local machine by using the **lo** flag, and we apply this rule to the **INPUT** and **OUTPUT** chains. We then perform port forwarding to route all traffic from port 8888 to port 25655. To do this, we modify the **nat** table and use the **PREROUTING** flag to perform the port forwarding. We also write rules for the **INPUT** and **OUTPUT** chains to only allow outgoing ssh connections to the **engineering.purdue.edu** domain using the **tcp** protocol. We do this by doing the following:

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

**sudo iptables -A INPUT -p tcp --sport 22 -s engineering.purdue.edu -m **
state --state ESTABLISHED -j ACCEPT

For the **OUTPUT** chain, we use the states **NEW** and **ESTABLISHED**. **NEW** means the packet started a new connection while **ESTABLISHED** has seen a packet that is associated with a connection and has packets in both directions. Finally, we drop any other packets that are not caught by the above rules by using the **DROP** flag for the **INPUT**, **FORWARD**, and **OUTPUT** chains.

```
nimal@nimal-XPS-15-7590:~/ECE404/HW9$ bash firewall404.sh
[sudo] password for nimal:
nimal@nimal-XPS-15-7590:~/ECE404/HW9$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  67.199.248.13        anywhere             tcp dpt:http
ACCEPT     tcp  --  67.199.248.12        anywhere             tcp dpt:http
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/NONE limit: avg 1/sec burst 5
ACCEPT     tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/SYN limit: avg 1/sec burst 500
DROP       all  --  anywhere             anywhere

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
nimal@nimal-XPS-15-7590:~/ECE404/HW9$
```

Figure 1: Output of running **sudo iptables -L**

```
nimal@nimal-XPS-15-7590:~/ECE404/HW9$ cat MyFirewall.bk
# Generated by iptables-save v1.8.7 on Mon Mar 27 14:37:29 2023
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -s 67.199.248.12/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -s 67.199.248.13/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -s 128.46.104.20/32 -p tcp -m tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
-A INPUT -j DROP
-A FORWARD -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK NONE -m limit --limit 1/sec -j ACCEPT
-A FORWARD -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m limit --limit 1/sec -j ACCEPT
-A FORWARD -j DROP
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -d 128.46.104.20/32 -p tcp -m tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -j DROP
COMMIT
# Completed on Mon Mar 27 14:37:29 2023
# Generated by iptables-save v1.8.7 on Mon Mar 27 14:37:29 2023
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -p tcp -m tcp --dport 8888 -j DNAT --to-destination :25565
-A POSTROUTING -o wlp59s0 -j MASQUERADE
COMMIT
# Completed on Mon Mar 27 14:37:29 2023
nimal@nimal-XPS-15-7590:~/ECE404/HW9$
```

Figure 2: Current firewall configuration saved in **MyFirewall.bk**

The second part of the assignment required us to do initial setup of the spam filter. For this, we used our ece404f4 email and subscribed to various newsletters to populate the inbox. The figure below shows a snippet of the many emails sent to the ece404f4 account, which is stored in the file **logfile**.

```
47
From 1axbt3z0fbms3tb2md3ri9ztt6dw3fwekk9msq-ece404f4=ecn.purdue.edu@241939m.brookings.edu  Mon Mar 27 07:03:45 2023
 Subject: Starting School Later, Why Young People are Driving Less, and More
  Folder: spamFolder                                                  71131



New message log:
48
From delivery_20230327093016.30951208.19452@bounce.buzzfeed.com  Mon Mar 27 09:30:38 2023
 Subject: Spring is in the air!
  Folder: spamFolder                                                  36748



New message log:
49
From foxnews_EB09D294D8E72AB5B5752412A0C4341B4C7F77AF4A1D50C2@response.wc07.net  Mon Mar 27 11:52:17 2023
 Subject: Car flips on Los Angeles freeway after tire pops off pickup truck:
  Folder: spamFolder                                                   7184



New message log:
50
From foxnews_EB09D294D8E72AB5661C6DFC3D09D9CA4C7F77AF4A1D50C2@response.wc07.net  Mon Mar 27 12:32:26 2023
 Subject: Nashville school shooting: Multiple people injured, shooter dead
  Folder: spamFolder                                                   7155



New message log:
51
From 1axb8xles4dgqpgbvhfxqgolh43yr53k07nds6-ece404f4=ecn.purdue.edu@241939m.brookings.edu  Mon Mar 27 12:42:54 2023
 Subject: See more ways to connect with us
  Folder: spamFolder                                                  38201
[ece404f4@ececomp3 ~/Mail]$
```

Figure 3: Screenshot of **cat logfile**, which contains the emails in the ece404f4 email account