HW09: Firewalls with iptables
Name: Jack Gardner
ECN Login: gardne97
Due Date: 3/28/23

Code Description:

```
# 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
# -F Flushes all chains, -X deletes all custom chains
# Repeat this process for all tables

# 3.Only accept packets from f1.com
iptables -A INPUT -s f1.com -j ACCEPT
# -A INPUT specifies that the rule applies to the input chain
# -s f1.com -j ACCEPT accepts all packets originating from f1.com

# 4.Change source IP to my own machines IP address
iptables -t nat -A POSTROUTING -o any -j MASQUERADE
# -t nat -A POSTROUTING specifies that the rule applies to the postrouting chain of the nat
table
# -o specifies that any network interface is masqueraded
# -j MASQUERADE target is specified, meaning that the source of all output packets is the
device ip address

# 5.Protect against nonstop port scanning
iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST NONE -m limit --limit 1/s -j ACCEPT
# -A FORWARD -p tcp specifies the FORWARD chain for the tcp protocol
# --tcp-flags SYN, ACK... Specifies the type of tcp packets the rule applies to
# -m limit --limit 1/s only allows one of these packets per second
# -j ACCEPT accept the packet if it obeys all of the above rules

# 6.Protect against syn flooding
iptables -A FORWARD -p tcp --syn -m limit --limit 1/s --limit-burst 500 -j ACCEPT
# -A FORWARD -p tcp specifies the FORWARD chain for the tcp protocol
# --syn specifies that the rule applies to syn packets
# -m limit --limit 1/s only allows one of these packets per second
# --limit-burst 500 -j ACCEPT The packet is only accepted if the total request is less than 500

# 7.Allow full loopback access on your machine
```

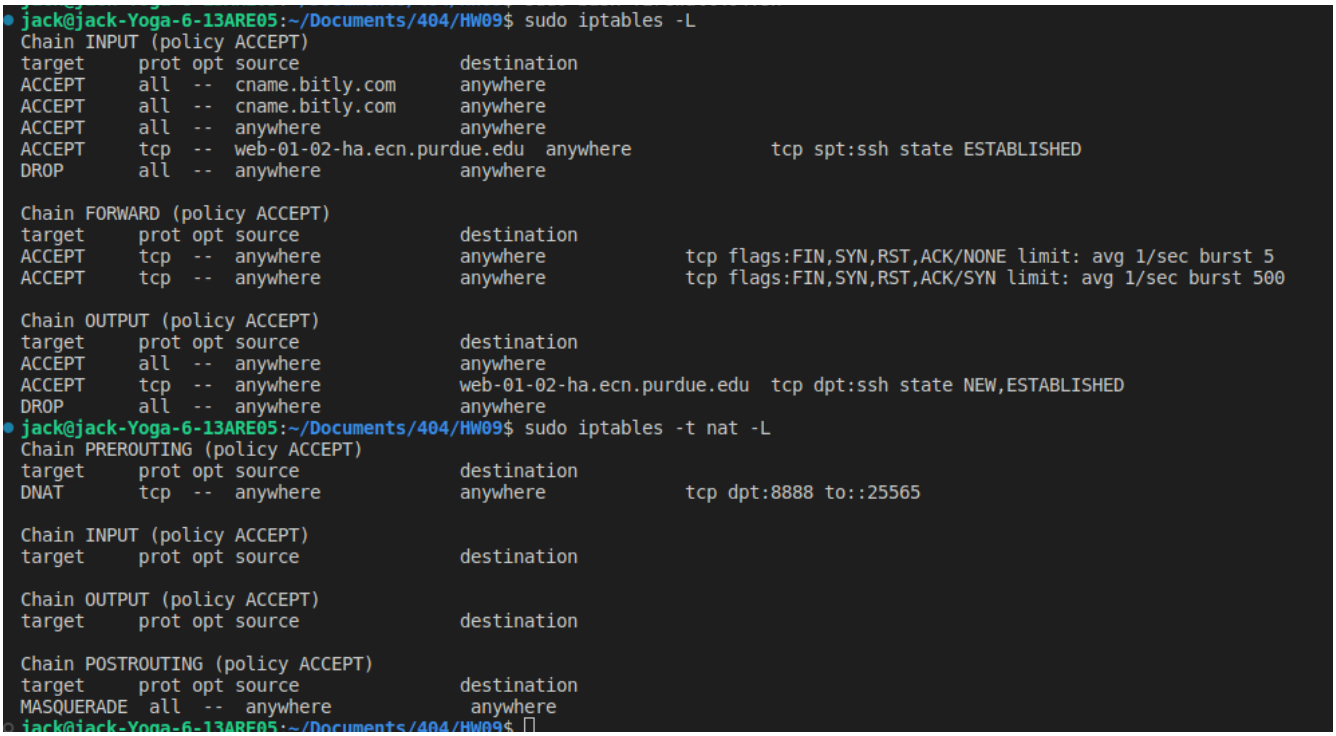
```
iptables -t filter -A INPUT -i lo -j ACCEPT
iptables -t filter -A OUTPUT -o lo -j ACCEPT
# -t filter -A INPUT / OUTPUT the rule applies to the input and output chain of the filter table respectively
# -i lo -j ACCEPT accepts input packets originating from localhost
# -o lo -j ACCEPT accepts output packets originating from localhost

# 8.Redirect all traffict on port 8888 to port 25565
iptables -t nat -A PREROUTING -p tcp --dport 8888 -j DNAT --to-destination :25565
# -t nat -A PREROUTING the rule applies to the PREROUTING chain in the nat table
# -p tcp --dport 8888 specifies that the incoming port must be 8888
# -j DNAT --to-destination :25565 reroutes the packet to the local port 25565

# 9.Only allow ssh connections to engineering.purdue.edu
iptables -A OUTPUT -p tcp --dport 22 -d engineering.purdue.edu -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 22 -s engineering.purdue.edu -m state --state ESTABLISHED -j ACCEPT
# -A OUTPUT/INPUT -p tcp specifies tcp packets in the output chain or input chain respectively
# --dport 22 -d/s engineering.purdue.edu specifies that the connection has to be related to the 22nd port (ssh port) of the destination or source hostname
# -m state --state NEW,ESTABLISHED / --state ESTABLISHED Allows you to create a new connection if you are sshing into a computer but does not allow a new computer to ssh into your device
# -j ACCEPT accepts the packet if it adheres to the above rules


# 10.Drop all other packets not accepted already
iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
# -A INPUT -j DROP drops all input packets that do not adhere to the above rules
# -A OUTPUT -j DROP drops all output packets that do not adhere to the above rules
```

IPTables Screenshot:



Mail Logfile:

New message log:
1
procmail: Couldn't determine implicit lockfile from "/usr/sbin/sendmail"
From gardne97@purdue.edu Tue Mar 28 15:09:59 2023
Subject: This is my subject
Folder: /usr/sbin/sendmail -oi gardne97@purdue.edu 6020
New message log:
2
From bounce+v2+904dd7.93cc8be.1680032864.BAABAQWtRUPTZ4H200pDro74iMG6pWzGZA==~ece404d2=ecn.purdue.edu@us.gigya-raas.com Tue Mar 28 15:48:06 2023
Subject: Welcome from Food Network!
Folder: spamFolder 36469
New message log:
3
From 0100018729c6373f-59f89f9d-2bb8-4f74-8f97-de33ae34db28-000000@email.washingtonpost.com Tue Mar 28 15:51:30 2023
Subject: Verify your email address
Folder: spamFolder 21116
New message log:
4
From security@facebookmail.com Tue Mar 28 15:53:26 2023
Subject: 145559 is your Facebook account recovery code
Folder: spamFolder 13325