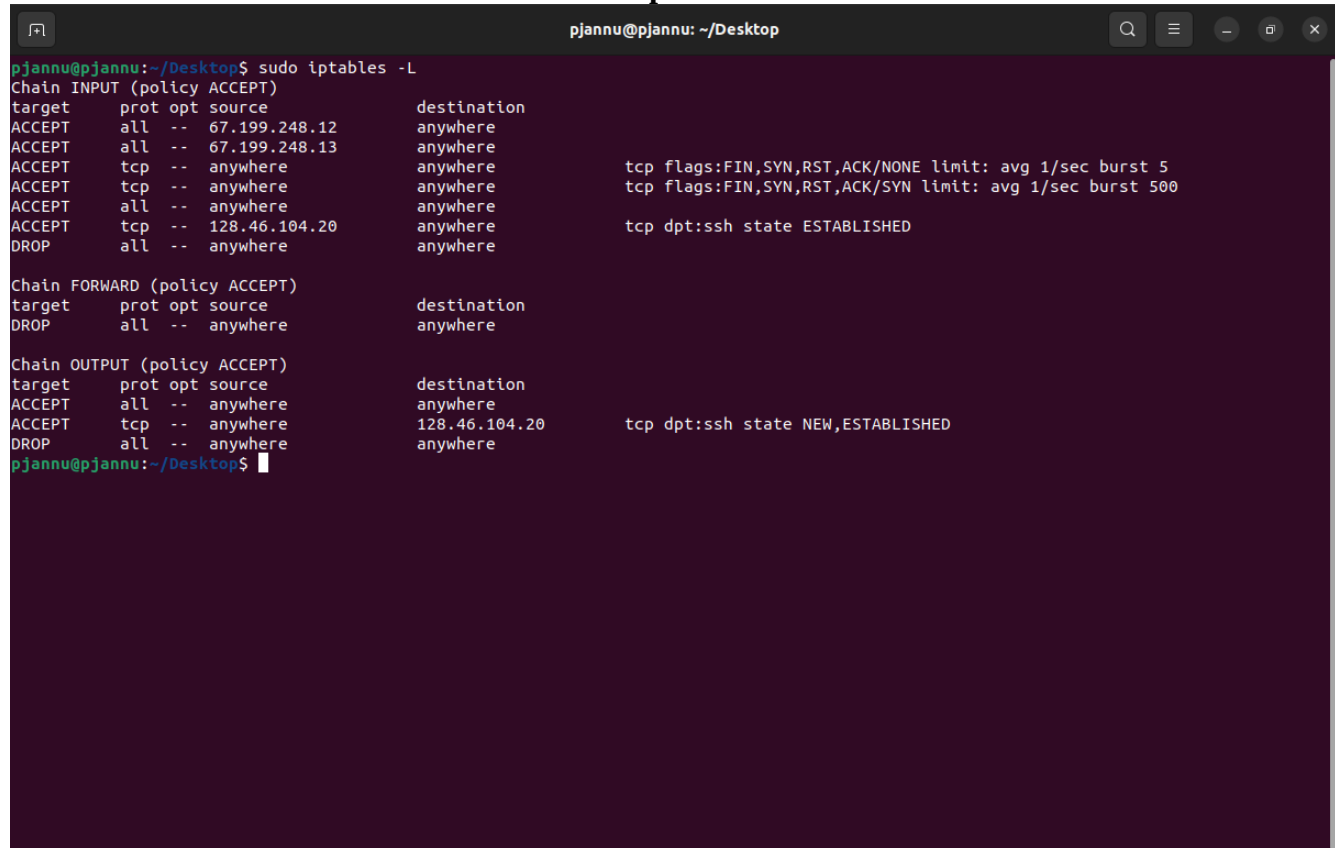


ECE404 HW09
Prateek Jannu
pjannu@purdue.edu

Sudo iptables -L



```
pjannu@pjannu:~/Desktop$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- 67.199.248.12 anywhere
ACCEPT all -- 67.199.248.13 anywhere
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
ACCEPT all -- anywhere anywhere
ACCEPT tcp -- 128.46.104.20 anywhere tcp dpt:ssh state ESTABLISHED
DROP all -- anywhere anywhere

Chain FORWARD (policy ACCEPT)
target prot opt source destination
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
pjannu@pjannu:~/Desktop$
```

1. Clearing and Deleting Rules:

- sudo iptables -t raw -F and sudo iptables -t raw -X: These commands clear (-F) and delete (-X) all rules within the raw table.
- Similarly, sudo iptables -t nat -F and sudo iptables -t nat -X clear and delete rules within the nat table, which is responsible for Network Address Translation.
- sudo iptables -t mangle -F and sudo iptables -t mangle -X do the same for the mangle table, which is used for specialized packet alterations.
- sudo iptables -t filter -F and sudo iptables -t filter -X clear and delete rules within the filter table, which is the default table and is used for packet filtering.

2. Accepting Incoming Traffic from Source f1.com:

- `sudo iptables -t filter -A INPUT -s f1.com -j ACCEPT`: This rule allows incoming traffic from the source f1.com by appending (-A) a rule to the INPUT chain in the filter table. If a packet matches this rule (source IP is f1.com), it will be accepted (-j ACCEPT).

3. Applying NAT to Outgoing Packets:

- `sudo iptables -t nat -A POSTROUTING -j MASQUERADE`: This rule is added to the POSTROUTING chain in the nat table. It masquerades (MASQUERADE) outgoing packets, meaning it replaces the source IP address with the IP address of the outgoing interface.

4. Limiting Incoming TCP Traffic:

- `sudo iptables -t filter -A INPUT -p tcp --tcp-flags SYN,ACK,FIN,RST NONE -m limit --limit 1/s -j ACCEPT`: This rule limits incoming TCP traffic by setting conditions on the TCP flags. It allows TCP packets with no flags set. The -m limit option is used to limit the matching rate, allowing only 1 packet per second (--limit 1/s).

5. Limiting Incoming SYN Packets:

- `sudo iptables -t filter -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 500 -j ACCEPT`: This rule limits incoming SYN packets. It allows TCP packets with the SYN flag set (--syn). The --limit 1/s option limits the matching rate to 1 packet per second, while --limit-burst 500 allows bursts of up to 500 packets.

6. Accepting Loopback Traffic:

- `sudo iptables -t filter -A INPUT -i lo -j ACCEPT` and `sudo iptables -t filter -A OUTPUT -o lo -j ACCEPT`: These rules accept all loopback (lo) traffic for both incoming and outgoing packets. Loopback interface is used for communication within the same machine.

7. Port Redirection:

- `sudo iptables -t nat -A PREROUTING -p tcp --dport 8888 -j REDIRECT --to-ports 25565`: This rule redirects incoming TCP traffic on port 8888 to port 25565 using destination NAT (REDIRECT).

8. Accepting SSH Connections from engineering.purdue.edu :

- sudo iptables -t filter -A INPUT -p tcp --dport 22 -s 128.46.104.20 -m state --state ESTABLISHED -j ACCEPT: This rule allows SSH connections from IP 128.46.104.20 only if they are in an established state.

- sudo iptables -t filter -A OUTPUT -p tcp --dport 22 -d 128.46.104.20 -m state --state NEW,ESTABLISHED -j ACCEPT: This rule allows outgoing SSH connections to IP 128.46.104.20 only if they are in a new or established state.

9. Dropping Other Traffic:

- sudo iptables -t filter -A INPUT -j DROP, sudo iptables -t filter -A OUTPUT -j DROP, sudo iptables -t filter -A FORWARD -j DROP: These rules drop all incoming, outgoing, and forwarded traffic respectively, which doesn't match any of the previous rules.