PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)

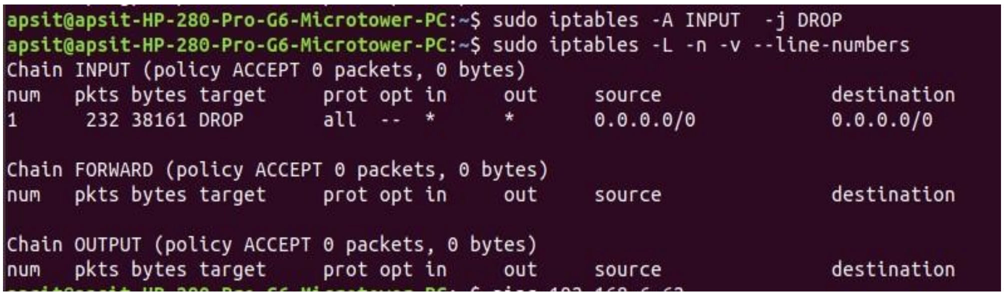
Department of Information Technology

Semester: V **Name of Student: Vis**
Academic Year: 2022-23 **Student ID: 20104084**
Class / Branch: TE IT
Subject: Security Lab (SL)
Name of Instructor: Prof. Apeksha Mohite

EXPERIMENT NO. 3A

Aim: To Study use of Iptables to configure stateful Software firewall on Linux H

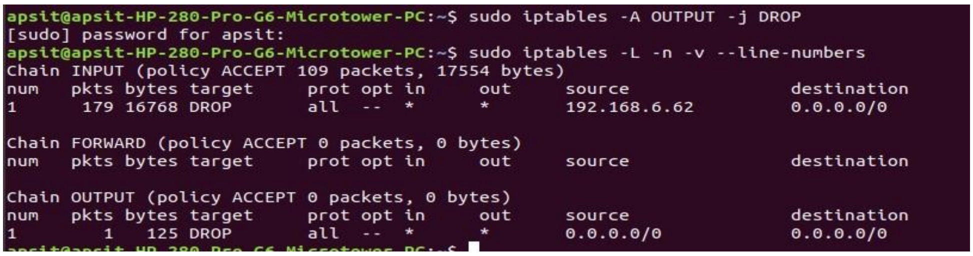
Making default policy of INPUT and OUTPUT Chain as DROP :



```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -A INPUT  -j DROP
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      232 38161 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ ping 192.168.6.62
```

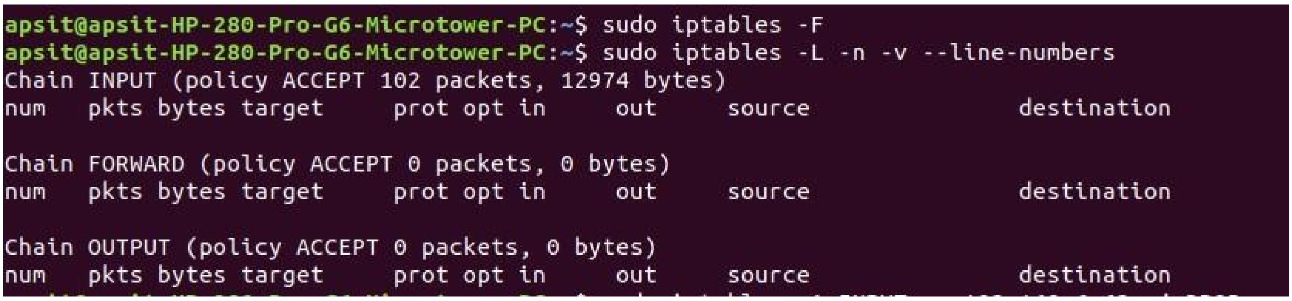


```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -A OUTPUT -j DROP
[sudo] password for apsit:
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 109 packets, 17554 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      179 16768 DROP       all  --  *      *       192.168.6.62         0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        1   125 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$
```

Flushing out all the rules:

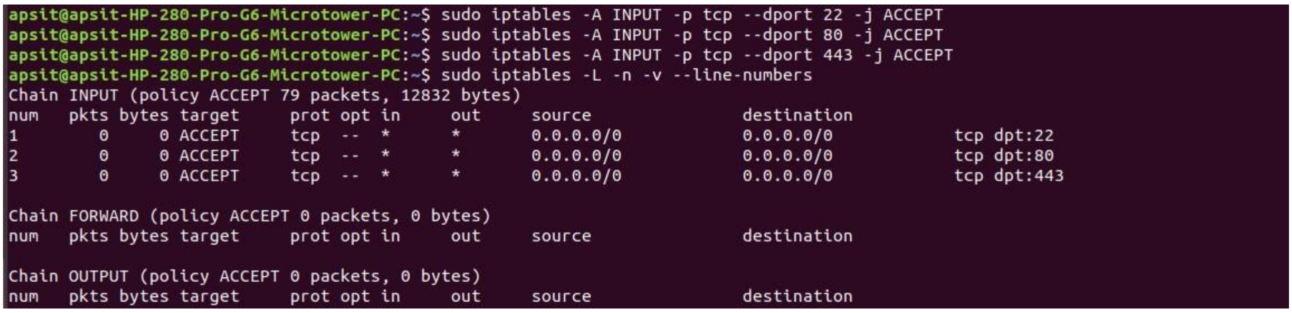


```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -F
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 102 packets, 12974 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
```

Allowing the ports:

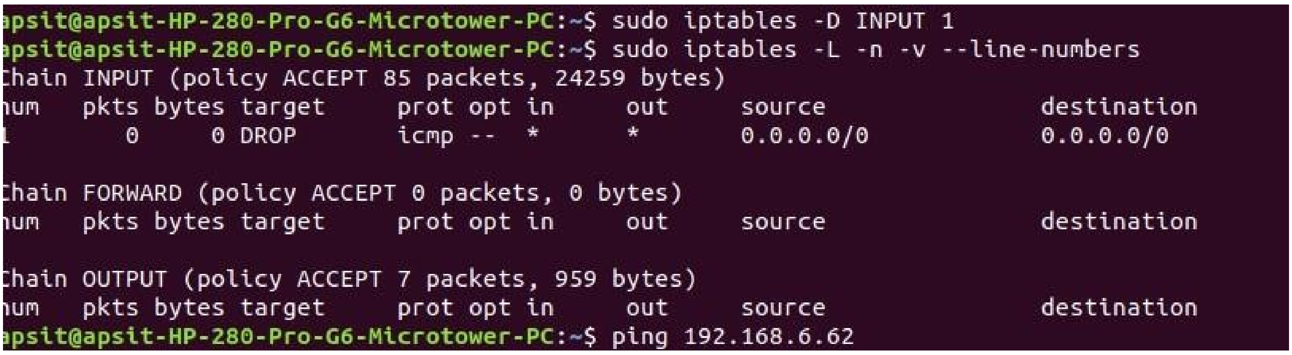


```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 79 packets, 12832 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
2        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
3        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
```

Deleting the rule:



```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -D INPUT 1
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 85 packets, 24259 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 7 packets, 959 bytes)
num   pkts bytes target     prot opt in     out     source               destination
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ ping 192.168.6.62
```

Conclusion: Thus we have successfully studied use of Iptables to configure stateful Software firewall on Linux Host.