

Academic Year: 2025-26

Semester: V

Class / Branch: TE IT Subject: Security Lab

Name of Instructor: Prof. Vishal Badgujar

Name of Student: Suyash Y Mane

Student ID: 24204008

Date of Performance: 30/07/2025 Date of Submission: 30/07/2025

Experiment No. 3

Aim: To study installation and configuration of Linux Kernel firewall iptables.

Code Screen Shots:

To list the current rules that are configured for iptables:

```
t@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -L
[sudo] password for apsit:
Chain INPUT (policy ACCEPT)
target prot opt source
                                                       destination
Chain FORWARD (policy DROP)
target prot opt source dest
DOCKER-USER all -- anywhere ar
DOCKER-ISOLATION-STAGE-1 all -- anywhere
                                                       destination
                                                         anywhere
                                                                           anywhere
             all -- anywhere
all -- anywhere
all -- anywhere
                                                      anywhere
                                                                                   ctstate RELATED, ESTABLISHED
                                                      anywhere
anywhere
DOCKER
 CCEPT
 CCEPT
                    -- anywhere
                                                       anywhere
 Chain OUTPUT (policy ACCEPT)
                                                      destination
target
              prot opt source
Chain DOCKER (1 references)
target prot opt source
                                                       destination
target
Chain DOCKER-ISOLATION-STAGE-1 (1 references)
                                                      destination
target prot opt source de:
DOCKER-ISOLATION-STAGE-2 all -- anywhere
                                                                           anywhere
              all -- anywhere
                                                       anywhere
Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target prot opt source
DROP all -- anywhere
RETURN all -- anywhere
                                                       destination
                                                       anywhere
Chain DOCKER-USER (1 references)
              prot opt source
all -- anywhere
                                                       destination
                                                       anywhere
```



A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

The command allows incoming traffic for established and related connections by using the conntrack module to track connection states.

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:-$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT apsit@apsit-HP-280-Pro-G6-Microtower-PC:-$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source
target
ACCEPT
                                                       destination
                                                                                   ctstate RELATED, ESTABLISHED
              all -- anywhere
                                                       anywhere
Chain FORWARD (policy DROP)
target prot opt source desi
DOCKER-USER all -- anywhere ar
DOCKER-ISOLATION-STAGE-1 all -- anywhere
                                                      destination
                                                         anywhere
                                                                           anvwhere
             all -- anywhere
all -- anywhere
all -- anywhere
all -- anywhere
                                                      anywhere
                                                                                   ctstate RELATED, ESTABLISHED
ACCEPT
DOCKER
                                                       anywhere
ACCEPT
                                                       anywhere
ACCEPT
                                                       anywhere
Chain OUTPUT (policy ACCEPT)
target
             prot opt source
                                                       destination
Chain DOCKER (1 references)
target prot opt source
target
                                                       destination
Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target prot opt source de:
DOCKER-ISOLATION-STAGE-2 all -- anywhere
RETURN all -- anywhere any
                                                       destination
                                                                           anvwhere
                                                       anvwhere
Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target
              prot opt source
                                                       destination
              all -- anywhere
all -- anywhere
DROP
                                                       anywhere
                                                       anywhere
RETURN
Chain DOCKER-USER (1 references)
target
RETURN
             prot opt source
all -- anywhere
                                                       destination
                                                       anvwhere
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:-$ sudo iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
apsit@apsit-HP-280-Pro-G6-Microtower-PC:-$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED
Chain FORWARD (policy DROP)
target prot opt source
DOCKER-USER all -- anywhere
                                                                          destination
                                                                            anywhere
DOCKER-ISOLATION-STAGE-1 all --
ACCEPT all -- anywhere
DOCKER all -- anywhere
ACCEPT all -- anywhere
                                                              anywhere
                                                                                                     anywhere
                                                                                                                ctstate RELATED,ESTABLISHED
                                                                          anywhere
                                                                          anywhere
anywhere
                   all -- anywhere
all -- anywhere
ACCEPT
                                                                          anywhere
Chain OUTPUT (policy ACCEPT)
target prot opt source
ACCEPT all -- anywhere
                                                                          destination
                                                                                                               ctstate RELATED.ESTABLISHED
                                                                          anywhere
Chain DOCKER (1 references)
target prot opt source
                                                                          destination
Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target prot opt source destination
target protopt source des
DOCKER-ISOLATION-STAGE-2 all -- anywhere
RETURN all -- anywhere any
                                                                                                     anywhere
                                                                          anywhere
 Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target
DROP
                 prot opt source
all -- anywhere
all -- anywhere
                                                                          destination
anywhere
RETURN
                                                                           anvwhere
Chain DOCKER-USER (1 references)
target prot opt source
RETURN all -- anywhere
                                                                           destination
                                                                          anywhere
```

PARSHVANATH CHARITABLE TRUST'S A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

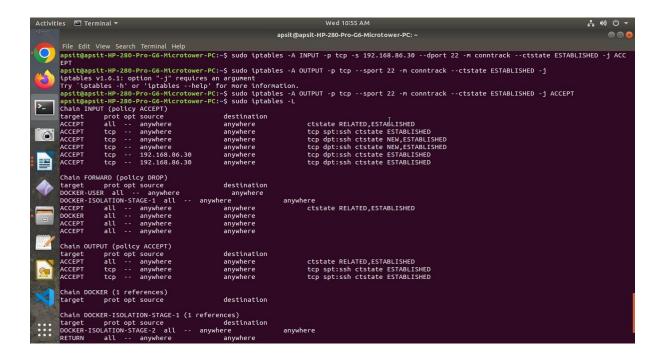
The first command allows incoming SSH (TCP port 22) traffic for new and established connections, while the second allows outgoing traffic for established SSH connections.

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACC
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -A OUTPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source
ACCEPT all -- anywhere
ACCEPT tcp -- anywhere
ACCEPT tcp -- anywhere
                                                                             destination
                                                                             anywhere
anywhere
                                                                                                                     ctstate RELATED, ESTABLISHED
                                                                                                                    tcp spt:ssh ctstate ESTABLISHED
tcp dpt:ssh ctstate NEW,ESTABLISHED
tcp dpt:ssh ctstate NEW,ESTABLISHED
                                                                              anywhere
ACCEPT
                    tcp
                                                                              anywhere
Chain FORWARD (policy DROP)
target prot opt source
DOCKER-USER all -- anywhere
DOCKER-ISOLATION-STAGE-1 all
                                                                anywhere
anywhere
                                                                              destination
                                                                                                          anywhere
                all -- anywhere
all -- anywhere
all -- anywhere
all -- anywhere
all -- anywhere
                                                                            anywhere
                                                                                                                      ctstate RELATED, ESTABLISHED
ACCEPT
DOCKER
                                                                             anywhere
ACCEPT
                                                                             anywhere
anywhere
ACCEPT
Chain OUTPUT (policy ACCEPT)
target prot opt source
ACCEPT all -- anywhere
ACCEPT tcp -- anywhere
                                                                                                                     ctstate RELATED,ESTABLISHED tcp spt:ssh ctstate ESTABLISHED
                                                                             anywhere
anywhere
Chain DOCKER (1 references)
                   prot opt source
                                                                             destination
Chain DOCKER-ISOLATION-STAGE-1 (1 references)
                                                                             destination
target protopt source des
DOCKER-ISOLATION-STAGE-2 all -- anywhere
RETURN all -- anywhere any
                                                                                                          anywhere
                                                                             anywhere
Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target prot opt source destination
                   prot opt source
all -- anywhere
all -- anywhere
target
DROP
                                                                             anywhere
anywhere
 RETURN
Chain DOCKER-USER (1 references)
```



(NBA Accredited)

The first command allows incoming SSH (TCP port 22) traffic from the IP range 192.168.86.30 for new and established connections, while the second allows outgoing traffic for established SSH connections.





A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

This iptables command adds a rule to reject outgoing TCP traffic from IP 192.168.86.30 to destination port 873 (typically used by rsync) if the connection is already ESTABLISHED. It uses conntrack module to match existing connections and applies the REJECT action instead of just dropping the packet.

```
psit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo iptables -A OUTPUT -p tcp -s 192.168.86.30 --dport 873 -m conntrack --ctstate ESTABLISHED
EJECT

apsit@apsit=HP-280-Pro-G6-Microtower-PC:-$ sudo tptables -L
Chain INPUT (policy ACCEPT)

target prot opt source destination
ACCEPT all -- anywhere anywhere
ACCEPT tcp -- 192.168.86.30 anywhere
ACCEPT tcp -- 192.168.86.30 anywhere
REJECT tcp -- 192.168.86.30 anywhere
                                                                                                                               ctstate RELATED,ESTABLISHED
tcp spt:ssh ctstate ESTABLISHED
tcp dpt:ssh ctstate NEW,ESTABLISHED
tcp dpt:ssh ctstate NEW,ESTABLISHED
tcp dpt:ssh ctstate ESTABLISHED
tcp dpt:ssh ctstate ESTABLISHED
                                                                                                                                tcp dpt:rsvnc ctstate ESTABLISHED reject-with icmp-port-unreachable
 Chain FORWARD (policy DROP)
LAGENT FORWARD (POLICY DROP)
target prot opt source
DOCKER-USER all -- anywhere
DOCKER all -- anywhere
DOCKER all -- anywhere
ACCEPT all -- anywhere
ACCEPT all -- anywhere
                                                                       anywhere
anywhere
                                                                                    destination
                                                                                                                   anywhere
ctstate RELATED,ESTABLISHED
                                                                                    anywhere
anywhere
anywhere
                                                                                     anvwhere
 Chain OUTPUT (policy ACCEPT)
                     prot opt source
all -- anywhere
tcp -- anywhere
tcp -- anywhere
tcp -- anywhere
tcp -- 192.168.86.30
target
ACCEPT
ACCEPT
                                                                                    destination
                                                                                                                               ctstate RELATED,ESTABLISHED
tcp spt:ssh ctstate ESTABLISHED
tcp spt:ssh ctstate ESTABLISHED
                                                                                     anvwhere
                                                                                                                                tcp dpt:rsvnc ctstate ESTABLISHED reject-with icmp-port-unreachable
Chain DOCKER (1 references)
target prot opt source
                                                                                    destination
Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target prot opt source destinat
DOCKER-ISOLATION-STAGE-2 all -- anywhere
RETURN all -- anywhere anywhere
                                                                                                                   anywhere
 Chain DOCKER-ISOLATION-STAGE-2 (1 references
```



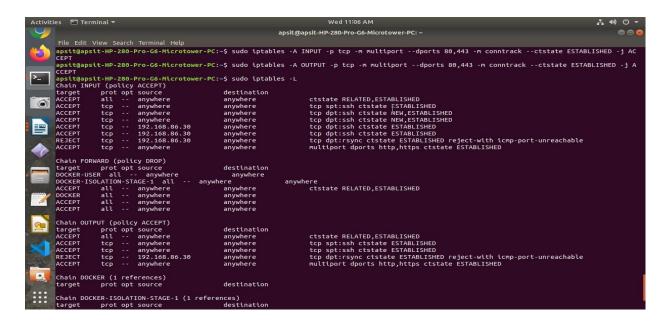
A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

These iptables rules allow incoming and outgoing HTTP (port 80) and HTTPS (port 443) traffic only if the connection is already established, ensuring secure web communication continuity.

It uses multiport to specify multiple destination ports and conntrack to match connections in the ESTABLISHED state.





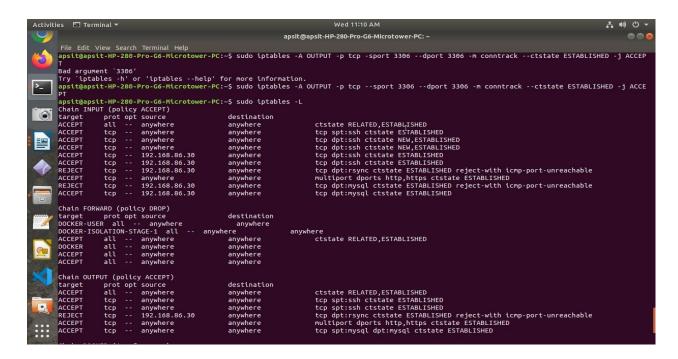
A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

This iptables rule allows outgoing MySQL traffic (port 3306) if the connection is already ESTABLISHED, ensuring database response packets are allowed.

It uses --sport and --dport to filter traffic on MySQL port and tracks connections using conntrack.



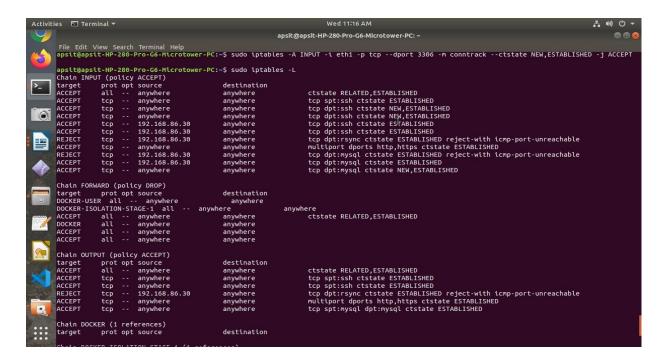


A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

The rule sudo iptables -A INPUT -i eth1 -p tcp --dport 3306 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT allows incoming MySQL traffic on port 3306 from interface eth1 for new and established connections.





Conclusion:

In this experiment, we learnt and understood how To study installation and configuration of Linux Kernel firewall iptables.





Department of Information Technology

(NBA Accredited)