UNIX Course Module 10

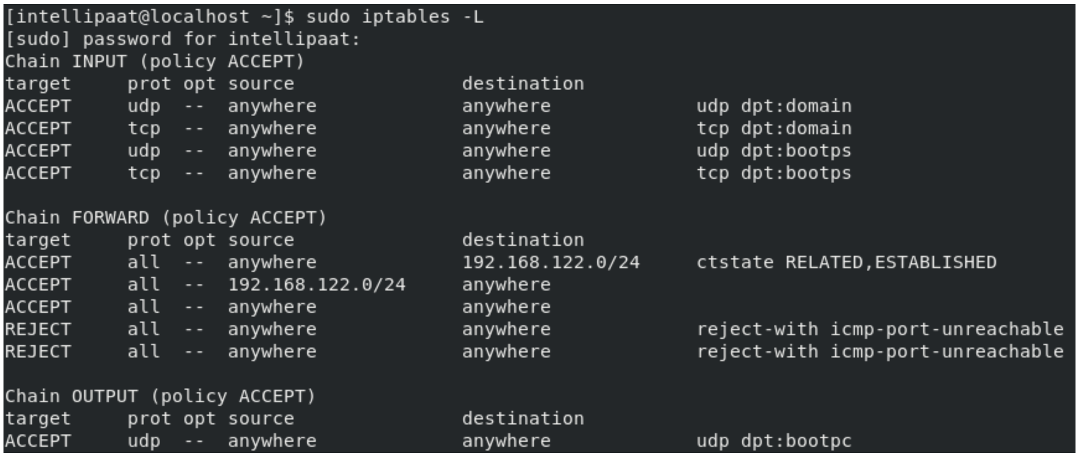
Hands-on: 2

support@intellipaat.com
+91-7022374614
US: 1-800-216-8930(Toll Free)

Use of IPTABLES Command

Operation 1: It is an application which can be used to configure firewall security tables.

```
$ sudo iptables -L
```



```
[intellipaat@localhost ~]$ sudo iptables -L
[sudo] password for intellipaat:
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:bootps
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:bootps

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             192.168.122.0/24     ctstate RELATED,ESTABLISHED
ACCEPT     all  --  192.168.122.0/24     anywhere
ACCEPT     all  --  anywhere             anywhere
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-unreachable
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:bootpc
```

Allowing a port

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

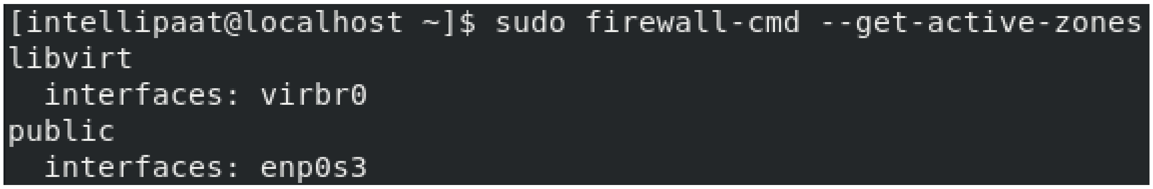
Blocking a port

```
sudo iptables -A INPUT -p tcp --dport 80 -j DROP
```

Use of FIREWALLD Command

Operation 1: Use host command to access the dynamically managed firewall application. To get the active zones which are basically allowed ports

```
$ sudo firewall-cmd –get-active-zones
```



```
[intellipaat@localhost ~]$ sudo firewall-cmd --get-active-zones
libvirt
  interfaces: virbr0
public
  interfaces: enp0s3
```

Allow port

```
sudo firewall-cmd --permanent --zone=public --add-port=80/tcp
```

Remove port

```
sudo firewall-cmd --zone=public --remove-port=80/tcp
```