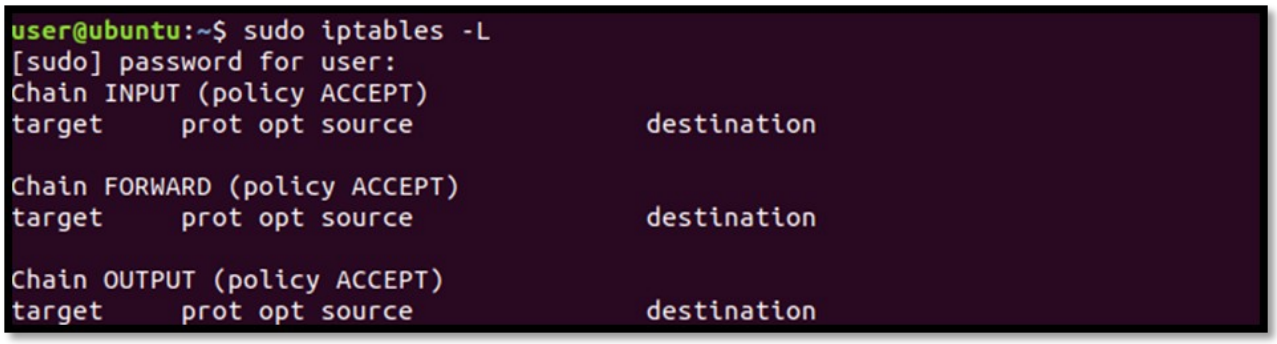
3.8 Guided Exercise: Configuring iptables Rules

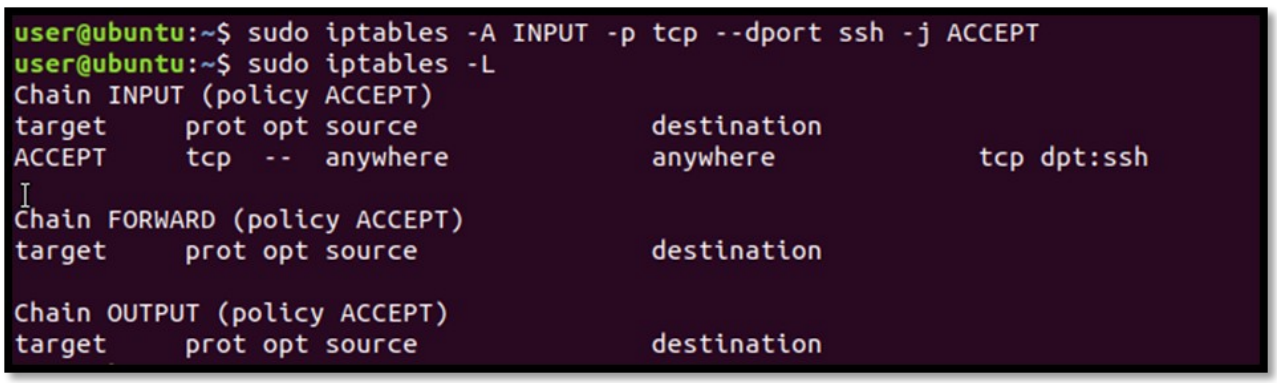
Resources	
Files	None
Machines	Ubuntu Server

In this exercise, you are required to write custom iptables rules.

Login to Ubuntu Server and then run the command “sudo iptables -L”. It will ask for the user password. Enter the user password which is “Pa$$w0rd”, press enter and then it will show the current iptables rules.



Write the command “sudo iptables –A INPUT –p tcp --dport ssh –j ACCEPT” and if sudo asks for the user password enter “Pa$$w0rd”. Then run the command sudo iptables –L to list the iptables rules.



Write the command “sudo iptables –A INPUT –p tcp --dport 80 –j ACCEPT” and if sudo asks for the user password enter “Pa$$w0rd”. Then run the command sudo iptables –L to list the iptables rules.

```
user@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
user@ubuntu:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

To save the iptables rules run the command “sudo iptables-save”.

```
user@ubuntu:~$ sudo iptables-save
# Generated by iptables-save v1.6.1 on Fri Jul 12 09:47:24 2019
*filter
:INPUT ACCEPT [90:7472]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [148:10952]
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
COMMIT
# Completed on Fri Jul 12 09:47:24 2019
```