

Week 9 - IP Tables

Challenge:

Configure iptables on **Cybersec-server** to **permit HTTP and HTTPS request, drop all other traffic.**

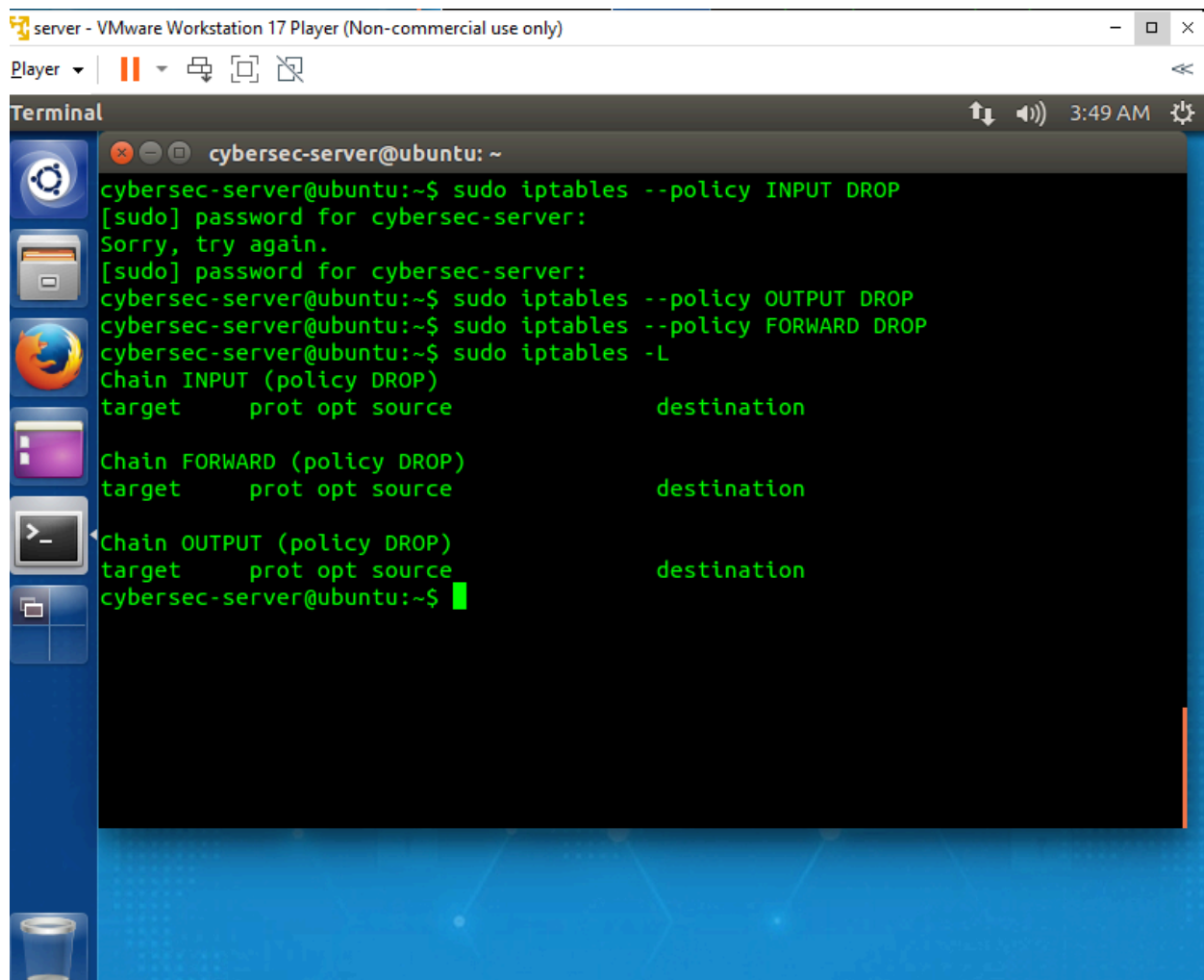
Hints:

1. HTTP and HTTPS use TCP.
2. The rules do not require mention of source or destination address.
3. Connection state: NEW, ESTABLISHED
4. Port Number of HTTP: 80
5. Port Number of HTTPS: 443

Screenshot Required:

1. Commands used to configure Iptables on Cybersec-Server to permit HTTP, HTTPS and drop other traffic.
2. Iptables chain after adding the rules. (`sudo iptables -L`)

Commands used to block all Traffic



```
server - VMware Workstation 17 Player (Non-commercial use only)
Player
Terminal
cybersec-server@ubuntu: ~
cybersec-server@ubuntu:~$ sudo iptables --policy INPUT DROP
[sudo] password for cybersec-server:
Sorry, try again.
[sudo] password for cybersec-server:
cybersec-server@ubuntu:~$ sudo iptables --policy OUTPUT DROP
cybersec-server@ubuntu:~$ sudo iptables --policy FORWARD DROP
cybersec-server@ubuntu:~$ sudo iptables -L
Chain INPUT (policy DROP)
target    prot opt source                destination

Chain FORWARD (policy DROP)
target    prot opt source                destination

Chain OUTPUT (policy DROP)
target    prot opt source                destination
cybersec-server@ubuntu:~$
```

