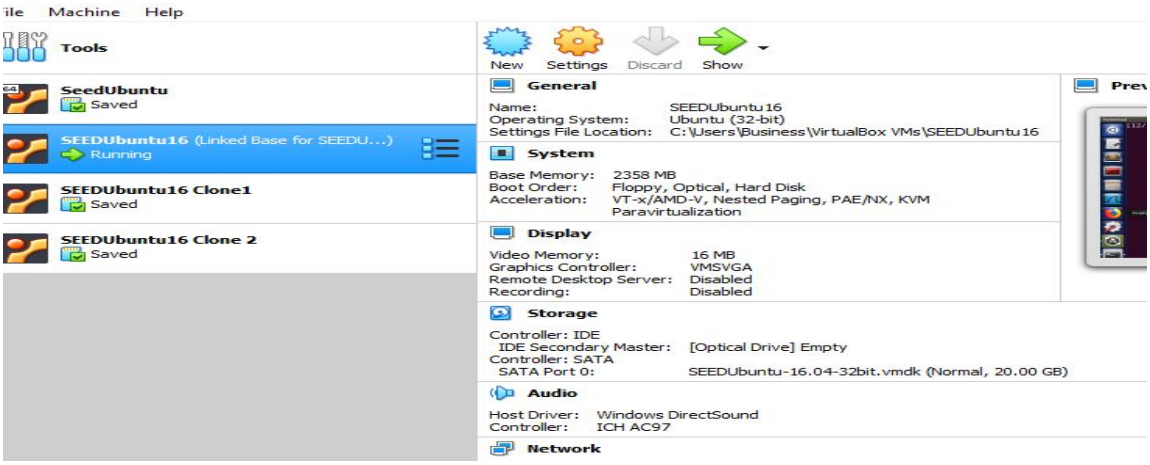
Internet and Enterprise Security: Lab9

December 14, 2019

(a) Clone your main virtual machine, creating two more virtual machines



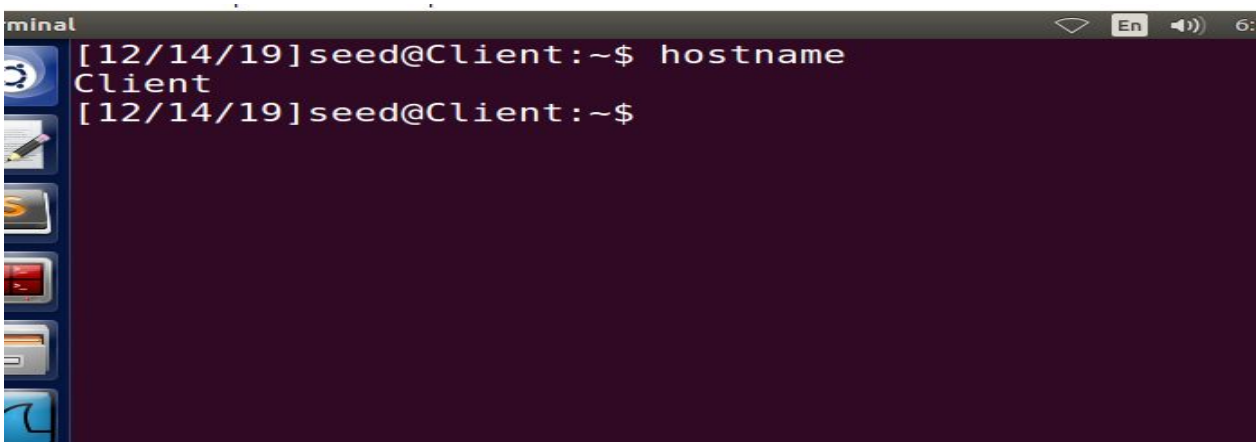
I cloned the SEEDUbuntu16 and replicated to two more Ubuntu machines named SEEDUbuntu16 Clone 1 and SEEDUbuntu16 Clone 2.

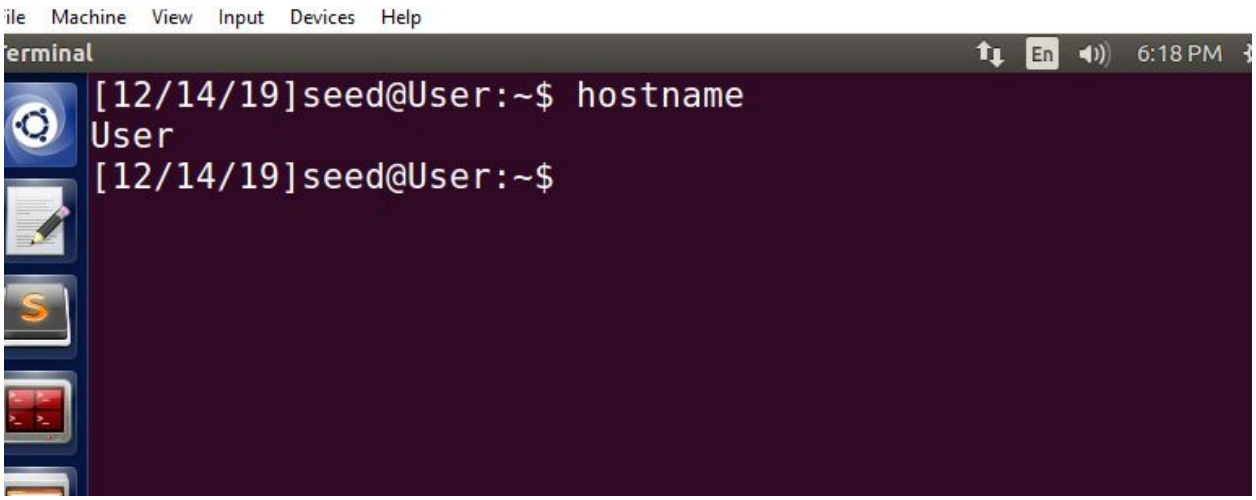
(b) The machines should have hostnames, which should appear on the command prompt instead of VM

I changed the hostnames of each Virtual Machine to Client, Savyata-Server and User and the local domain name for all remains as localhost @ 127.0.0.1

```
[12/14/19]seed@VM:~$
[12/14/19]seed@VM:~$ sudo hostnamectl set-hostname Clie
nt
[12/14/19]seed@VM:~$ hostname
Client
[12/14/19]seed@VM:~$ sudo vi /etc/hosts
```


Machine View Input Devices Help
6:00 PM
[12/14/19]seed@Savyata-server:~$
System Settings


[12/14/19]seed@Client:~$ hostname
Client
[12/14/19]seed@Client:~$


Machine View Input Devices Help
6:18 PM
[12/14/19]seed@User:~$ hostname
User
[12/14/19]seed@User:~$

Below figure shows the localhost and the FULLY Qualified Domain name for a machine.

```
[12/14/19]seed@User:~$ sudo cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       User

# The following lines are desirable for IPv6 capable
Sublime Text
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1       User
127.0.0.1       Attacker
127.0.0.1       Server
127.0.0.1       www.SeedLabSQLInjection.com
127.0.0.1       www.xsslabelgg.com
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
[12/14/19]seed@User:~$
```

Below figure shows the localhost and the FULLY Qualified Domain name for a machine.

```
[12/14/19]seed@Client:~$ sudo cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       Client

# The following lines are desirable for IPv6 capable ho
sts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1       User
127.0.0.1       Attacker
127.0.0.1       Server
127.0.0.1       www.SeedLabSQLInjection.com
127.0.0.1       www.xsslabelgg.com
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
[12/14/19]seed@Client:~$
```

Below figure shows the localhost and the FULLY Qualified Domain name for a machine.

```
tion.
[12/14/19]seed@Savyata-server:~$ sudo cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       Savyata-server

# The following lines are desirable for IPv6 capable ho
sts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1       User
127.0.0.1       Attacker
127.0.0.1       Server
127.0.0.1       www.SeedLabSQLInjection.com
127.0.0.1       www.xsslabelgg.com
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
[12/14/19]seed@Savyata-server:~$
```

(c) Follow the instructions on p.16 to convert your setup to a static IP environment, where your individual machines are configured to have static IP addresses

Below is the configuration for Static IP addresses for all virtual machines. After the configuration, the machines will be set in NAT connections.

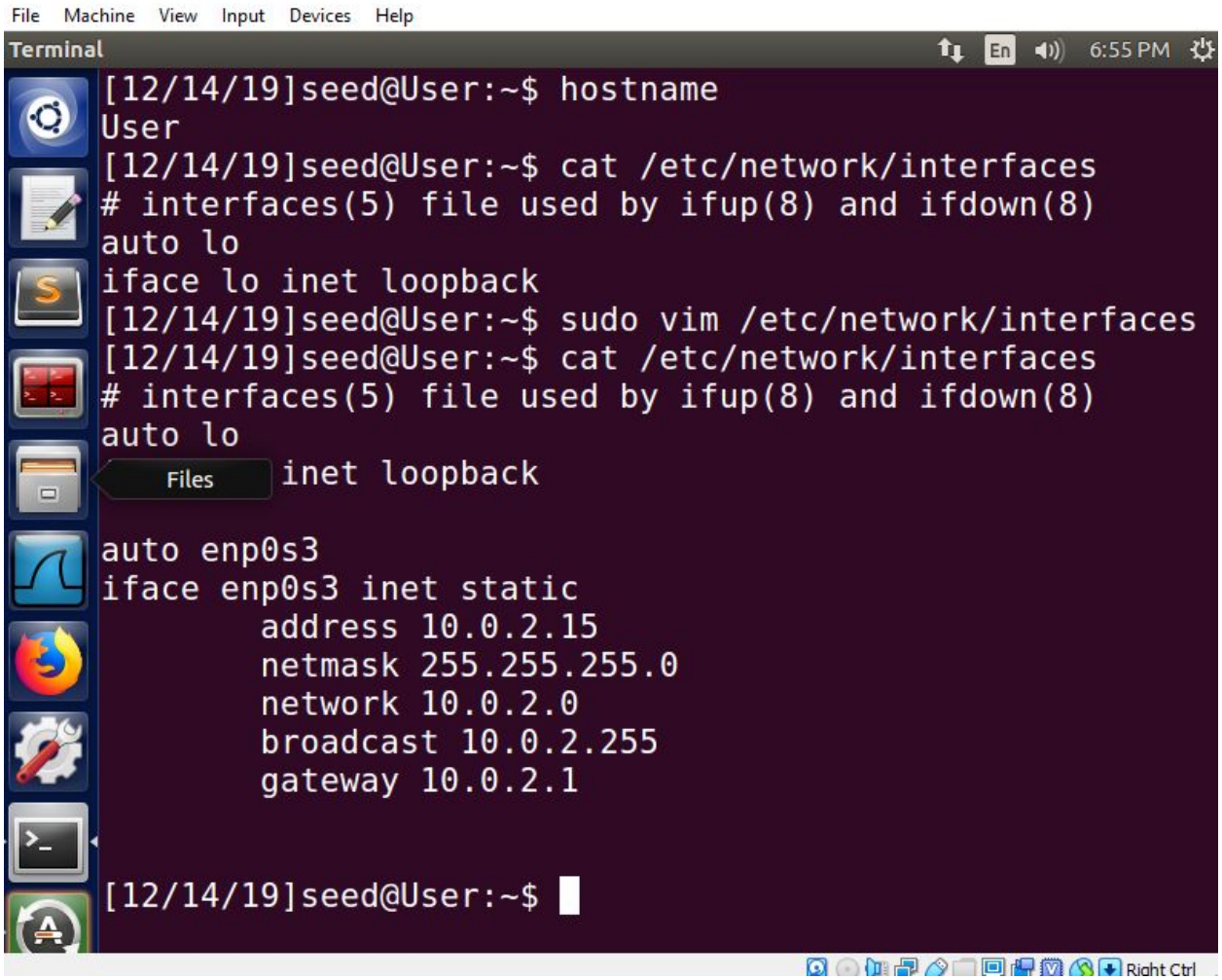
```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
face lo inet loopback

auto enp0s3
iface enp0s3 inet static
address 10.0.2.15
netmask 255.255.255.0
network 10.0.2.0
broadcast 10.0.2.255
gateway 10.0.2.1
~
~
~
~
~
~
~
~
~
                                        11,16          All
```

```
sudo: vim/etc/network/interfaces: command not found
[12/14/19]seed@Savyata-server:~$ sudo vim /etc/network/
interfaces
[12/14/19]seed@Savyata-server:~$ sudo reboot
```

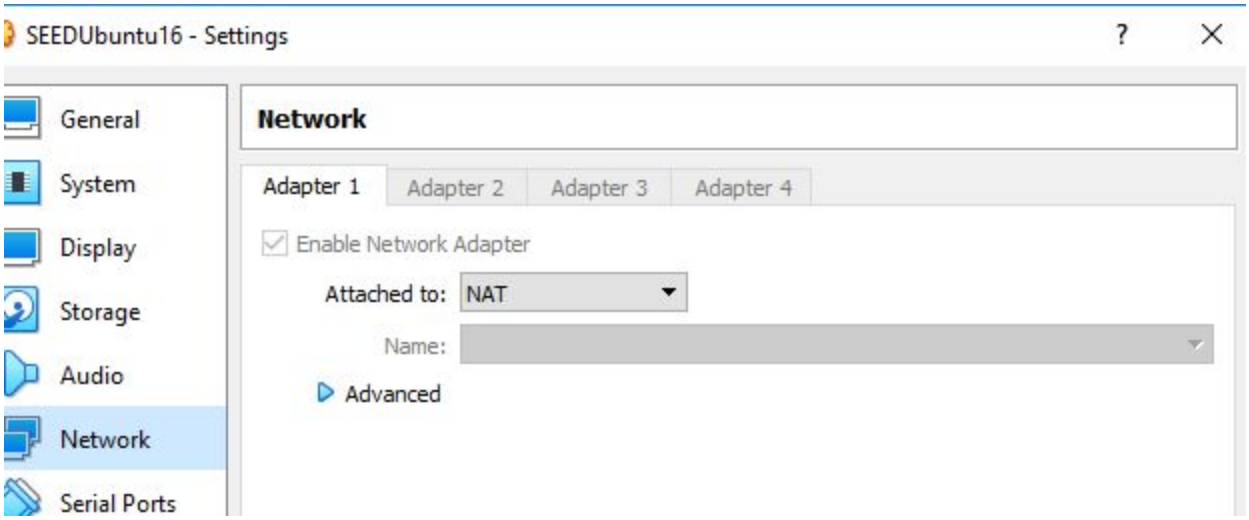
```
[12/14/19]seed@Savyata-server:~$ cat /etc/network/inter
faces
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto enp0s3
iface enp0s3 inet static
address 10.0.2.15
netmask 255.255.255.0
broadcast 10.0.2.255
gateway 10.0.2.1
[12/14/19]seed@Savyata-server:~$
```

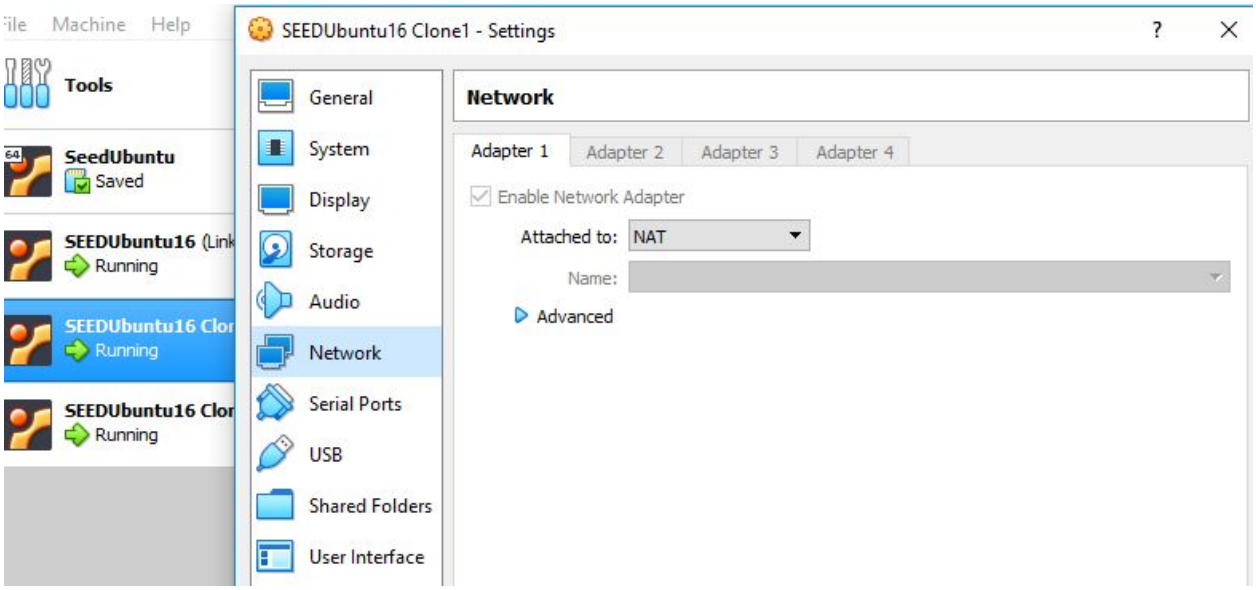
Right Ctrl

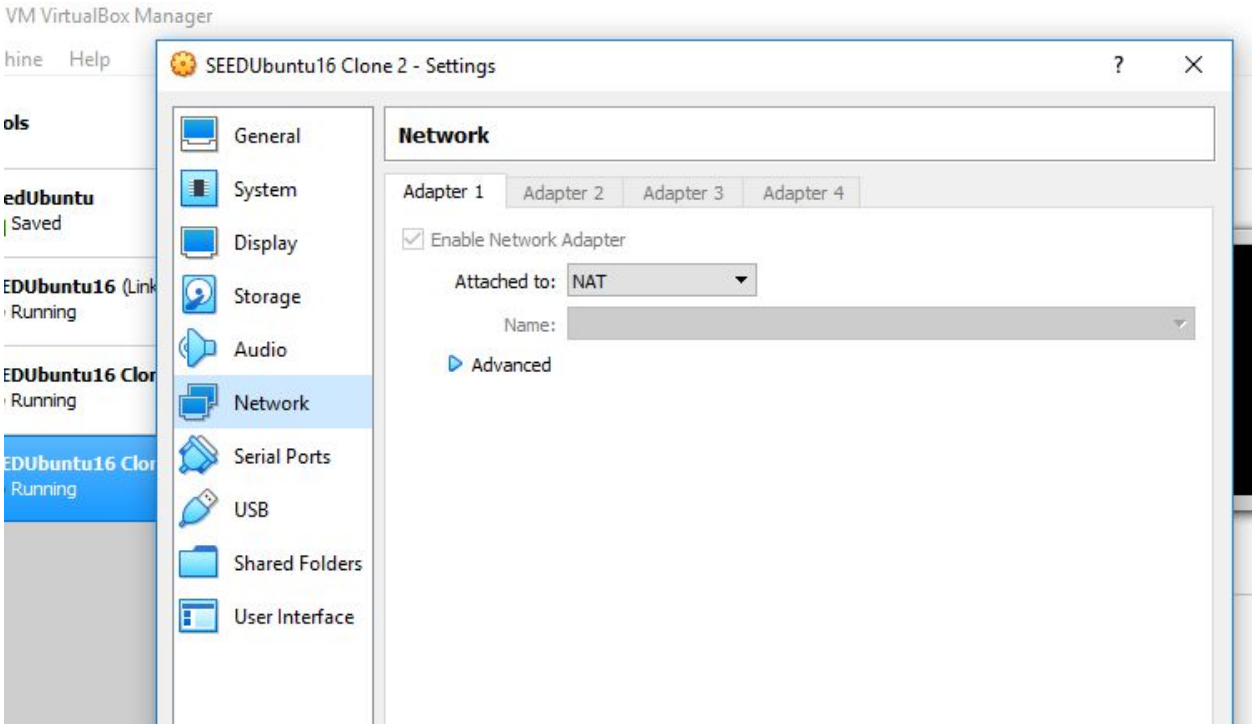
```
[12/14/19]seed@Client:~$ cat /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
face lo inet loopback

auto enp0s3
iface enp0s3 inet static
address 10.0.2.15
netmask 255.255.255.0
network 10.0.2.0
broadcast 10.0.2.255
gateway 10.0.2.1
[12/14/19]seed@Client:~$
```



(d) the machines should remain on the NAT network


SEEDUbuntu16 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
NAT
Name:
Advanced


File
Machine
Help
Tools
SeedUbuntu
Saved
SEEDUbuntu16 (Link
Running
SEEDUbuntu16 Clon
Running
SEEDUbuntu16 Clon
Running
SEEDUbuntu16 Clone1 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
NAT
Name:
Advanced



(e) the machines should remain reachable from one another, and should maintain Internet access

Before creating a new firewall configuration, two things must be in place:

• all pre-existing rules should be flushed, in order to avoid conflicts with the new rules or unpredictable results

• the start-up default policies should all be set to ACCEPT before flushing old rules when configuring a remote firewall, in order to avoid the policies to be reset to BLOCK and deny remote access

I did the following processes in each Machines to create a new firewall configuration.

setting all policies to ACCEPT

flushing old iptables policies

allow incoming packets with destination port=22 (SSH)

allow incoming packets with destination port=80 (HTTP)

allow outgoing packets using TCP as transport

create an exception for the loopback interface to not disrupt same host programs

allow DNS (port=53) queries

change the default policies to DROP, as the rules to ACCEPT are now carved out

```
[12/14/19]seed@User:~$ sudo iptables -P INPUT ACCEPT
[12/14/19]seed@User:~$ sudo iptables -P OUTPUT ACCEPT
[12/14/19]seed@User:~$ sudo iptables -P FORWARD ACCEPT
[12/14/19]seed@User:~$ sudo iptables -F
[12/14/19]seed@User:~$ sudo iptables -A INPUT -p tcp --
dport 22 -j ACCEPT
[12/14/19]seed@User:~$ sudo iptables -A INPUT -p tcp --
dport 80 -j ACCEPT
[12/14/19]seed@User:~$ sudo iptables -A NPUT -p tcp --d
port 22 -j ACCEPT
iptables: No chain/target/match by that name.
[12/14/19]seed@User:~$ sudo iptables -A OUTPUT -p tcp -
m tcp -j  ACCEPT
[12/14/19]seed@User:~$ sudo iptables -I INPUT 1 -i lo -
j ACCEPT
[12/14/19]seed@User:~$ sudo iptables -A OUTPUT -p udp -
-dport 53 -j ACCEPT
[12/14/19]seed@User:~$ sudo iptables -A INPUT -p udp --
sport 53 -j ACCEPT
[12/14/19]seed@User:~$ sudo iptables -L
```

view the final firewall configuration

```
[12/14/19]seed@User:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

ACCEPT     all  --  anywhere             anywhere

ACCEPT     tcp  --  anywhere             anywhere
       tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere
       tcp dpt:http
ACCEPT     udp  --  anywhere             anywhere
       udp spt:domain

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination


Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

ACCEPT     tcp  --  anywhere             anywhere
```

```
       udp dpt:domain
[12/14/19]seed@User:~$ sudo iptables -P INPUT DROP
[12/14/19]seed@User:~$ sudo iptables -P OUTPUT DROP
[12/14/19]seed@User:~$ sudo iptables -P FORWARD DROP
[12/14/19]seed@User:~$ sudo iptables -A OUTPUT -p tcp -
m conntrack --cstate ESTABLISHED, RELATED -j ACCEPT
iptables v1.6.0: unknown option "--cstate"
Try `iptables -h' or 'iptables --help' for more informa
tion.
[12/14/19]seed@User:~$ sudo iptables -A OUTPUT -p tcp -
m conntrack --ctstate ESTABLISHED, RELATED -j ACCEPT
```

```
rtt min/avg/max/mdev = 0.019/0.049/0.065/0.022 ms
[12/14/19]seed@Savyata-server:~$ sudo iptables -P INPUT
 ACCEPT
[12/14/19]seed@Savyata-server:~$ sudo iptables -P OUTPU
T ACCEPT
[12/14/19]seed@Savyata-server:~$ sudo iptables -P FORWA
RD  ACCEPT
[12/14/19]seed@Savyata-server:~$ sudo iptables -F
[12/14/19]seed@Savyata-server:~$ sudo iptables -A INPUT
 -p tcp --dport 22 -j ACCEPT
[12/14/19]seed@Savyata-server:~$ sudo iptables -A INPUT
 -p tcp --dport 80 -j ACCEPT
[12/14/19]seed@Savyata-server:~$ sudo iptables -A OUTPU
T -p tcp -m tcp -j ACCEPT
[12/14/19]seed@Savyata-server:~$ sudo iptables -I INPUT
 1 -i lo -j ACCEPT
[12/14/19]seed@Savyata-server:~$ sudo iptables -A OUTPU
Trash --dport 53 -j ACCEPT
```

view the final firewall configuration

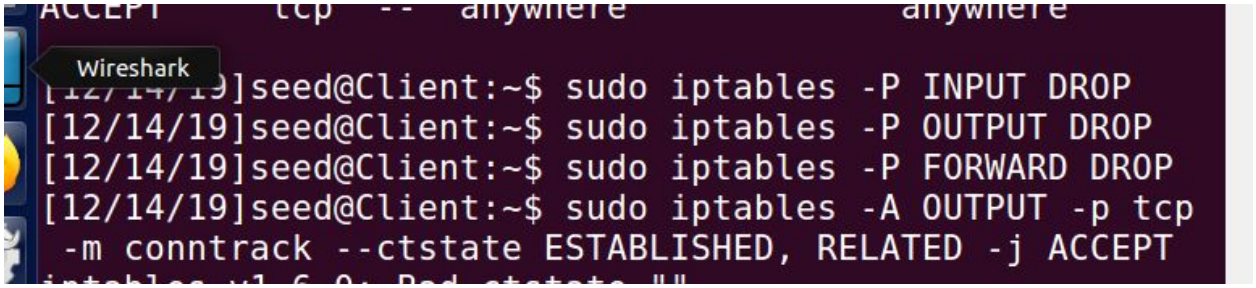
```
[12/14/19]seed@Savyata-server:~$ sudo iptables -A INPUT
-p udp --sport 53 -j ACCEPT
Bad argument `udp'
Try `iptables -h' or 'iptables --help' for more informa
tion.
[12/14/19]seed@Savyata-server:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

ACCEPT     all  --  anywhere             anywhere

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
```

```
       udp dpt:domain
[12/14/19]seed@Savyata-server:~$ sudo iptables -P INPUT
 DROP
[12/14/19]seed@Savyata-server:~$ sudo iptables -P OUTPU
T DROP
[12/14/19]seed@Savyata-server:~$ sudo iptables -P FORWA
RD  DROP
[12/14/19]seed@Savyata-server:~$ sudo iptables -A OUTPU
T -p tcp -m conntrack --ctstate ESTABLISHED, RELATED -j
ACCEPT
```

```
Search your computer
[12/14/19]seed@Client:~$ sudo iptables -P INPUT ACCEPT
[12/14/19]seed@Client:~$ sudo iptables -P OUTPUT ACCEPT
[12/14/19]seed@Client:~$ sudo iptables -P FORWARD ACCEP
T
[12/14/19]seed@Client:~$ sudo iptables -F
[12/14/19]seed@Client:~$ sudo iptables -A INPUT -p tcp
--dport 22 -j ACCEPT
[12/14/19]seed@Client:~$ sudo iptables -A INPUT -p tcp
--dport 80 -j ACCEPT
[12/14/19]seed@Client:~$ sudo iptables -A OUTPUT -p tcp
 -j ACCEPT
[12/14/19]seed@Client:~$ sudo iptables -I INPUT 1 -i lo
 -j ACCEPT
```

view the final firewall configuration

```
 -j ACCEPT
[12/14/19]seed@Client:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

ACCEPT     all  --  anywhere             anywhere

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

ACCEPT     tcp  --  anywhere             anywhere

[12/14/19]seed@Client:~$
```


ACCEPT tcp -- anywhere anywhere
Wireshark
[12/14/19]seed@Client:~$ sudo iptables -P INPUT DROP
[12/14/19]seed@Client:~$ sudo iptables -P OUTPUT DROP
[12/14/19]seed@Client:~$ sudo iptables -P FORWARD DROP
[12/14/19]seed@Client:~$ sudo iptables -A OUTPUT -p tcp
-m conntrack --ctstate ESTABLISHED, RELATED -j ACCEPT