

## Lab 6 Notes

Ehsan Karimi

Following are the screenshots of /etc/sysconf/iptables for all the machines:

Machine A:

```
File Edit View Search Terminal Tabs Help
ubuntu@bhp:~ x root@router:~ x root@carriage:~ x root@platen:~ x root@chase:~ x root@saddle:~ x root@roller:~ x ubuntu@bhp:~ x
# Generated by iptables-save v1.4.21 on Tue Dec  4 13:55:07 2018
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -o ens192 -j MASQUERADE
COMMIT
# Completed on Tue Dec  4 13:55:07 2018
# Generated by iptables-save v1.4.21 on Tue Dec  4 13:55:07 2018
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -n icmp --icmp-type 8 -j ACCEPT
-A INPUT -p icmp -n icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -n icmp --icmp-type 11 -j ACCEPT
-A INPUT -p icmp -n icmp --icmp-type 3 -j ACCEPT
-A INPUT -s 100.64.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 100.64.25.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 100.64.254.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 10.21.32.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 198.18.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j LOG --log-level 6
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
#ip specific drop rules
-A FORWARD -s 157.240.2.35/32 -j DROP
-A FORWARD -d 157.240.2.35/32 -j DROP
-A FORWARD -s 54.193.38.238/32 -j DROP
-A FORWARD -d 54.193.38.238/32 -j DROP
-A FORWARD -s 216.176.177.74/32 -j DROP
-A FORWARD -d 216.176.177.74/32 -j DROP
#icmp rules
-A FORWARD -p icmp -n icmp --icmp-type 8 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -n icmp --icmp-type 0 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -n icmp --icmp-type 11 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -n icmp --icmp-type 3 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
# ssh rules
-A FORWARD -d 100.64.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 100.64.25.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 100.64.254.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 10.21.32.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 198.18.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -s 100.64.0.0/16 -p tcp -m state --state NEW -m tcp --sport 22 -j ACCEPT
-A FORWARD -s 100.64.25.0/24 -p tcp -m state --state NEW -m tcp --sport 22 -j ACCEPT
-A FORWARD -s 100.64.254.0/24 -p tcp -m state --state NEW -m tcp --sport 22 -j ACCEPT
1,1 Top
```

```
File Edit View Search Terminal Tabs Help
ubuntu@hpc:~ x root@router:~ x root@carriage:~ x root@platen:~ x root@chase:~ x root@saddle:~ x root@roller:~ x ubuntu@hpc:~ x
-A FORWARD -d 216.176.177.74/32 -j DROP

#icmp rules
-A FORWARD -p icmp -m icmp --icmp-type 8 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 0 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 11 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 3 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT

# ssh rules
-A FORWARD -d 100.64.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 100.64.25.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 10.21.32.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 198.18.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -s 100.64.0.0/16 -p tcp -m state --state NEW -m tcp --sport 22 -j ACCEPT
-A FORWARD -s 100.64.25.0/24 -p tcp -m state --state NEW -m tcp --sport 22 -j ACCEPT
-A FORWARD -s 10.21.32.0/24 -p tcp -m state --state NEW -m tcp --sport 22 -j ACCEPT
-A FORWARD -s 198.18.0.0/16 -p tcp -m state --state NEW -m tcp --sport 22 -j ACCEPT

# Machine B and F
-A FORWARD -d 100.64.25.2/32 -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A FORWARD -d 100.64.25.2/32 -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A FORWARD -s 100.64.25.2/32 -p tcp -m state --state NEW -m tcp --sport 80 -j ACCEPT
-A FORWARD -s 100.64.25.2/32 -p tcp -m state --state NEW -m tcp --sport 443 -j ACCEPT
-A FORWARD -d 100.64.25.5/32 -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A FORWARD -d 100.64.25.5/32 -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A FORWARD -s 100.64.25.5/32 -p tcp -m state --state NEW -m tcp --sport 80 -j ACCEPT
-A FORWARD -s 100.64.25.5/32 -p tcp -m state --state NEW -m tcp --sport 443 -j ACCEPT

# Machine C
-A FORWARD -s 100.64.0.0/16 -d 100.64.25.3/32 -j ACCEPT
-A FORWARD -s 100.64.0.0/16 -d 100.64.25.3/32 -p tcp -m state --state NEW -m tcp --dport 20 -j ACCEPT
-A FORWARD -s 100.64.0.0/16 -d 100.64.25.3/32 -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
-A FORWARD -s 172.20.74.249 -d 100.64.25.3/32 -p tcp -m state --state NEW -m tcp --dport 20 -j ACCEPT
-A FORWARD -s 172.20.74.249 -d 100.64.25.3/32 -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
-A FORWARD -s 100.64.25.3/32 -p tcp --dport 20 -j ACCEPT
-A FORWARD -s 100.64.25.3/32 -p tcp --dport 21 -j ACCEPT
-A FORWARD -s 100.64.25.3/32 -p tcp --dport 80 -j ACCEPT
-A FORWARD -s 100.64.25.3/32 -p tcp --dport 443 -j ACCEPT
-A FORWARD -s 100.64.25.3/32 -p tcp --dport 22 -j ACCEPT

# Machine D
-A FORWARD -d 100.64.25.4/32 -p udp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -d 100.64.25.4/32 -p tcp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -s 100.64.25.4/32 -p tcp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -s 100.64.25.4/32 -p udp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT

-A OUTPUT -o lo -j ACCEPT
COMMIT
Completed on Tue Dec 4 13:55:07 2018

86,1 Bot
```

## Machine B:

```
File Edit View Search Terminal Tabs Help
ubuntu@hpc:~ x root@router:~ x root@carriage:~ x root@platen:~ x root@chase:~ x root@saddle:~ x root@roller:~ x ubuntu@hpc:~ x
# Generated by iptables-save v1.4.21 on Thu Nov 29 15:01:48 2018
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [21:11176]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A INPUT -s 100.64.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 100.64.25.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 100.64.254.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 10.21.32.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 198.18.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -m state --state NEW -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -m state --state NEW -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
COMMIT
Completed on Thu Nov 29 15:01:48 2018

/etc/sysconfig/iptables" 21l, 1032C

21,1 All
```

## Machine C:

```
File Edit View Search Terminal Tabs Help
ubuntu@hp:~ x root@router:~ x root@carriage:~ x root@platen:~ x root@chase:~ x root@roller:~ x root@saddle:~ x ubuntu@hp:~ x
# Generated by iptables-save v1.4.21 on Tue Dec 4 13:04:33 2018
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s 100.64.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 100.64.25.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 100.64.254.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 10.21.32.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 198.18.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 100.64.0.0/16 -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
-A INPUT -s 100.64.0.0/16 -p tcp -m state --state NEW -m tcp --dport 20 -j ACCEPT
-A INPUT -s 172.20.74.249/32 -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
-A INPUT -s 172.20.74.249/32 -p tcp -m state --state NEW -m tcp --dport 20 -j ACCEPT
-A INPUT -s 100.64.0.0/16 -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -d 100.64.25.4/32 -p tcp -m tcp --dport 53 -j ACCEPT
-A OUTPUT -d 100.64.25.4/32 -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 22 -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 21 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 20 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
COMMIT
# Completed on Tue Dec 4 13:04:33 2018

```

21,1

ALL

## Machine D:

```
File Edit View Search Terminal Tabs Help
ubuntu@hp:~ x root@router:~ x root@carriage:~ x root@platen:~ x root@chase:~ x root@saddle:~ x root@roller:~ x ubuntu@hp:~ x
# Generated by iptables-save v1.4.21 on Fri Nov 30 18:15:19 2018
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [28:2576]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A INPUT -s 100.64.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 100.64.25.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 100.64.254.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 10.21.32.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 198.18.0.0/16 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p udp -m udp --sport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 53 -j ACCEPT
COMMIT
# Completed on Fri Nov 30 18:15:19 2018

```

23,1

ALL

## Machine E:

```
File Edit View Search Terminal Tabs Help
ubuntu@hp:~ * root@router:~ * root@carriage:~ * root@platen:~ * root@chase:~ * root@saddle:~ * root@roller:~ * ubuntu@hp:~
# Generated by iptables-save v1.4.21 on Sun Dec  2 15:38:26 2018
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:1032]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s 100.64.0.25/32 -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A INPUT -s 10.21.32.0/24 -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A INPUT -i ens256 -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A INPUT -p icmp -n icmp --icmp-type 8 -j ACCEPT
-A INPUT -p icmp -n icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -n icmp --icmp-type 11 -j ACCEPT
-A INPUT -p icmp -n icmp --icmp-type 3 -j ACCEPT
-A INPUT -s 10.21.32.0/24 -p tcp -m tcp --dport 445 -m state --state NEW -j ACCEPT
-A INPUT -s 10.21.32.0/24 -p tcp -m tcp --dport 135 -m state --state NEW -j ACCEPT
-A INPUT -s 10.21.32.0/24 -p udp -m udp --dport 137 -m state --state NEW -j ACCEPT
-A INPUT -s 10.21.32.0/24 -p udp -m udp --dport 138 -m state --state NEW -j ACCEPT
-A INPUT -s 10.21.32.0/24 -p udp -m udp --dport 139 -m state --state NEW -j ACCEPT
-A INPUT -s 10.21.32.0/24 -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A INPUT -s 100.64.0.25/32 -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
COMMIT
# Completed on Sun Dec  2 15:38:26 2018

/etc/sysconfig/iptables* 25L, 1307C

22,0-1 All
```

## Machine F:

```
File Edit View Search Terminal Tabs Help
ubuntu@hp:~ * root@router:~ * root@carriage:~ * root@platen:~ * root@chase:~ * root@roller:~ * root@saddle:~ * ubuntu@hp:~
# Generated by iptables-save v1.4.21 on Thu Nov 29 15:17:47 2018
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [147:15092]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -n icmp --icmp-type 8 -j ACCEPT
-A INPUT -p icmp -n icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -n icmp --icmp-type 11 -j ACCEPT
-A INPUT -p icmp -n icmp --icmp-type 3 -j ACCEPT
-A INPUT -s 100.64.0.0/16 -p tcp -m state --state NEW -n tcp --dport 22 -j ACCEPT
-A INPUT -s 100.64.254.0/24 -p tcp -m state --state NEW -n tcp --dport 22 -j ACCEPT
-A INPUT -s 100.64.254.0/24 -p tcp -m state --state NEW -n tcp --dport 22 -j ACCEPT
-A INPUT -s 10.21.32.0/24 -p tcp -m state --state NEW -n tcp --dport 22 -j ACCEPT
-A INPUT -s 198.18.0.0/16 -p tcp -m state --state NEW -n tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -n state --state NEW -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -n state --state NEW -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
COMMIT
# Completed on Thu Nov 29 15:17:47 2018

/etc/sysconfig/iptables* 21L, 1033C

21,1 All
```

Following are screenshots demonstrating samples of the key functioning requirements:

Blocking Facebook :

```
[root@carriage ~]# ping 157.240.2.35
PING 157.240.2.35 (157.240.2.35) 56(84) bytes of data.
```

```
26 2184 DROP all -- * * 0.0.0.0/0 157.240.2.35
```

allow Inbound Ssh connections:

```
[root@carriage ~]# ssh root@100.64.25.3
root@100.64.25.3's password:
```

```
0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0
tcp spt:22 ctstate RELATED,ESTABLISHED
6 360 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0
```

Sending Http request from external network to machine B:

```
ubuntu@hp:~$ wget http://100.64.25.2:80/index.html
--2018-12-05 15:57:41-- http://100.64.25.2/index.html
Connecting to 100.64.25.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13888 (14K)
Saving to: 'index.html.6'

index.html.6      100%[=====>] 13.56K  5.40KB/s   in 2.5s
2018-12-05 15:57:44 (5.40 KB/s) - 'index.html.6' saved [13888/13888]
```

router:

```
state NEW tcp spt:22
1 60 ACCEPT tcp -- * * 0.0.0.0/0 100.64.25.2
state NEW tcp dpt:80
0 0 ACCEPT tcp -- * * 0.0.0.0/0 100.64.25.2
```

MachineB:

```
state NEW tcp dpt:22
3 180 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0
tcp dpt:80 state NEW
0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0
```

Allow NEW inbound ftp traffic only from 100.64.0.0/16 and 172.20.74.249:

MachineB:

```
[root@carriage ~]# wget ftp://100.64.25.3/
--2018-12-05 16:01:42--  ftp://100.64.25.3/
      => '.listing'
Connecting to 100.64.25.3:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.      ==> PWD ... done.
==> TYPE I ... done.    ==> CWD not needed.
==> PASV ... done.      ==> LIST ... done.

[ <=>                                     ] 0

2018-12-05 16:01:42 (0.00 B/s) - '.listing' saved [0]

Removed '.listing'.
Wrote HTML-ized index to 'index.html.11' [196].
[root@carriage ~]#
```

MachineC:

```
state NEW tcp dpt:22
 1    60 ACCEPT      tcp  --  *    *           100.64.0.0/16       0.0.0.0/0
state NEW tcp dpt:21
 0     0 ACCEPT      tcp  --  *    *           100.64.0.0/16       0.0.0.0/0
```

DNS query from machine E:

MachineE:

```
[root@roller ~]# nslookup www.google.com
Server:          100.64.25.4
Address:         100.64.25.4#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.3.4
```

MachineA:

```
tcp dpt:22
 1    60 ACCEPT      udp  --  *    *           0.0.0.0/0           100.64.25.4
udp dpt:53 state NEW,ESTABLISHED
 0     0 ACCEPT      tcp  --  *    *           0.0.0.0/0           100.64.25.4
tcp dpt:53 state NEW,ESTABLISHED
```

MachineD:

```
state NEW tcp dpt:22
 1    60 ACCEPT      udp  --  *    *    0.0.0.0/0      0.0.0.0/0
udp dpt:53
```