I confirm that I will keep the content of this Lab confidential. I confirm that I have not received any unauthorized assistance in preparing for or writing this Lab. I acknowledge that a mark of 0 may be assigned for copied work.

Name: Siddharth Samber

Student number: 110124156

LAB 7

Master of Applied Computing

Networking & Data Security

COMP 8677

University of Windsor

Submitted By:

Siddharth Samber

110124156

Submission Date:

20 March 2024

PART 1

CHANGING DEFAULT POLICIES FOR FILTER TABLE

```
[03/17/24]seed@VM:~/lab 8$ docker ps
CONTAINER ID        IMAGE                                   COMMAND
 CREATED             STATUS              PORTS               NAMES
55b7b4bd766b        handsonsecurity/seed-ubuntu:large   "bash -c ' ip route …"
 3 days ago          Up About a minute                       host2-192.168.60.6
8f73256529ca        handsonsecurity/seed-ubuntu:large   "bash -c ' ip route …"
 3 days ago          Up About a minute                       hostA-10.9.0.5
11b7292cf7e0        handsonsecurity/seed-ubuntu:large   "bash -c ' ip route …"
 3 days ago          Up About a minute                       host1-192.168.60.5
348c3d6f45e2        seed-router-image                   "bash -c ' ip route …"
 3 days ago          Up About a minute                       host3-192.168.60.7
939216d2b65a        seed-router-image                   "bash -c ' ip route …"
 3 days ago          Up About a minute                       seed-router
[03/17/24]seed@VM:~/lab 8$ docksh 93
root@939216d2b65a:/# iptables -P INPUT ACCEPT
root@939216d2b65a:/# iptables -P OUTPUT ACCEPT
root@939216d2b65a:/# iptables -P FORWARD DROP
```

Observations / Explanation of Rule

FORWARD CHAIN : By default all passing Packets which are forwarded from router will be dropped.

OUTPUT AND INPUT CHAIN : By default all Packets which are received (incoming packet) and sent (outgoing packet) by router will be accepted .

PING 10.9.0.5 and Router (192.168.60.11) FROM 192.168.60.6

```
[03/17/24]seed@VM:~$ docksh 55
root@55b7b4bd766b:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
^C
--- 10.9.0.5 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4090ms

root@55b7b4bd766b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
64 bytes from 192.168.60.11: icmp_seq=1 ttl=64 time=0.303 ms
64 bytes from 192.168.60.11: icmp_seq=2 ttl=64 time=0.221 ms
64 bytes from 192.168.60.11: icmp_seq=3 ttl=64 time=0.125 ms
^C
--- 192.168.60.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2093ms
rtt min/avg/max/mdev = 0.125/0.216/0.303/0.072 ms
```

Observations / Explanation of Rule

1. No Packets were received by 10.9.0.5 as those packets need to be frowarded by router and according to rule forwarded packets should be dropped by default.

2. Packets were received by router 192.168.60.11 as these packets need to be sent to router and according to rule incoming packets (input chain) should be accepted by default.

CHANGING DEFAULT POLICY FOR FORWARD CHAIN

```
root@939216d2b65a:/# iptables -P INPUT ACCEPT
root@939216d2b65a:/# iptables -P OUTPUT ACCEPT
root@939216d2b65a:/# iptables -P FORWARD DROP
root@939216d2b65a:/# iptables -P FORWARD ACCEPT
```

FORWARD CHAIN : By default Packets which are forwarded from router will be accepted now

```
root@55b7b4bd766b:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=63 time=0.150 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.067 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.066 ms
^C
--- 10.9.0.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2050ms
rtt min/avg/max/mdev = 0.066/0.094/0.150/0.039 ms
root@55b7b4bd766b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
64 bytes from 192.168.60.11: icmp_seq=1 ttl=64 time=0.140 ms
64 bytes from 192.168.60.11: icmp_seq=2 ttl=64 time=0.055 ms
64 bytes from 192.168.60.11: icmp_seq=3 ttl=64 time=0.063 ms
^C
--- 192.168.60.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2055ms
rtt min/avg/max/mdev = 0.055/0.086/0.140/0.038 ms
```

Observations / Explanation of Rule

1. Packets were received by 10.9.0.5 as those packets need to be frowarded by router and according to changed rule forwarded packets should be accepted by default now.
2. Packets were received by router 192.168.60.11 as these packets need to be sent to router and according to rule packets at input chain should be accepted by default.

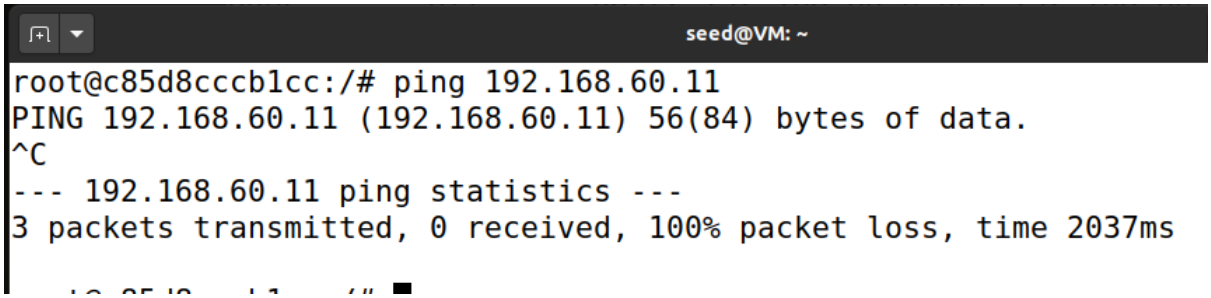
PART 2

BLOCKING INCOMING PACKETS

```
root@989f2398dd0a:/# iptables -A INPUT -s 192.168.60.6 -j DROP
root@989f2398dd0a:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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



Observations / Explanation of Rule

The appended rule drop the incoming packet from source ip 192.168.60.6

Answer

Ping router from 192.168.60.6 : It fails and no packets are received as incoming packet with source ip 192.168.60.6 will be dropped as per the appended rule.

BLOCKING OUTGOING PACKETS WITH

```
root@989f2398dd0a:/# iptables -A OUTPUT -d 192.168.60.6 -j DROP
root@989f2398dd0a:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             host2-192.168.60.6.net-192.168.60.0
root@989f2398dd0a:/# ping 192.168.60.6
PING 192.168.60.6 (192.168.60.6) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 192.168.60.6 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3213ms
```

Observations / Explanation of Rule

The appended rule drop the outgoing packet from source ip 192.168.60.6

Answer

Ping 192.168.60.6 from router : It fails and says sendmsg operation not permitted and no packet received therefore as outgoing packet with destination ip 192.168.60.6 will be dropped as per the appended rule.

PART 3

```
root@939216d2b65a:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere
root@939216d2b65a:/# iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere


Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere
```

Observations / Explanation of Rule

1. iptables -L displays all the rules in the filter table be default.
2. iptables -L –line-number also tell the index or sequence number of the rule. This is helpful to know how rules will be scaned and also for deleting rules.

PART 4

```
root@939216d2b65a:/# iptables -L INPUT --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere

root@939216d2b65a:/# iptables -D INPUT 1
root@939216d2b65a:/# iptables -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
root@939216d2b65a:/#
```

Observations / Explanation of Rule

1. First rules in INPUT chain of filter table are displayed with index numbers with iptables -L INPUT –line-number
2. Second with iptables -D INPUT 1 , index number 1 rule from INPUT Chain is deleted
3. Iptables -L INPUT is used to verify whether rule is delted or not, It is verified that it is deleted.

PART 5

```
root@939216d2b65a:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere
root@939216d2b65a:/# iptables -t filter -F
root@939216d2b65a:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

Observations / Explanation of Rule

With the help of iptables -t filter -F we flush that is we delete all the rules in all chains of filter table.

PART 6

APPENIDNG RULES

```
root@939216d2b65a:/# iptables -P INPUT DROP
root@939216d2b65a:/# iptables -A INPUT -p tcp --dport 23 -j ACCEPT
```

PING AND TELNET

```
root@55b7b4bd766b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
^C
--- 192.168.60.11 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6143ms

root@55b7b4bd766b:/# telnet 192.168.60.11
Trying 192.168.60.11...
Connected to 192.168.60.11.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
939216d2b65a login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Mar 17 05:12:26 UTC 2024 on pts/2
seed@939216d2b65a:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.11  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:0a:09:00:0b  txqueuelen 0  (Ethernet)
        RX packets 90  bytes 10411 (10.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5  bytes 378 (378.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Observations / Explanation of Rule

1. First we set default policy to drop all packets at INPUT chain
2. Second we append a rule for INPUT chain that for TCP protocol with destination port 23 packets will be accepted

Answer

1. Telenet succeeds because it uses destination port 23 and TCP protocl
2. Ping fails as by default packets are to be dropped at INPUT chain

PART 7

```
root@939216d2b65a:/# iptables -A OUTPUT -p udp --dport 53 -d 8.8.8.8 -j DROP
root@939216d2b65a:/# dig uwindsor.ca

; <<>> DiG 9.16.1-Ubuntu <<>> uwindsor.ca
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1947
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;uwindsor.ca.                   IN      A

;; ANSWER SECTION:
uwindsor.ca.            3600    IN      A       137.207.71.196

;; Query time: 159 msec
;; SERVER: 127.0.0.11#53(127.0.0.11)
;; WHEN: Sun Mar 17 05:24:27 UTC 2024
;; MSG SIZE  rcvd: 56

root@939216d2b65a:/# dig @8.8.8.8 uwindsor.ca

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8 uwindsor.ca
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached

root@939216d2b65a:/#
```

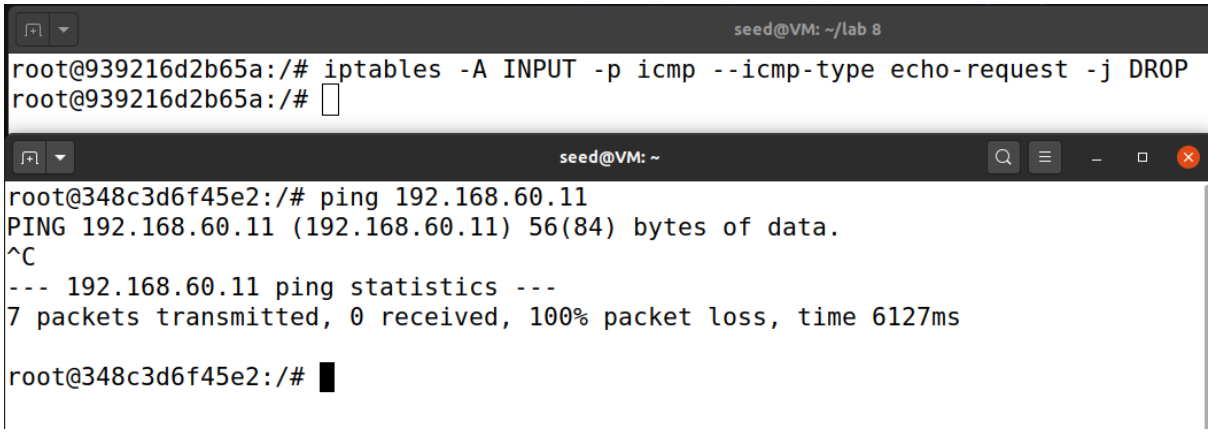
Observations / Explanation of Rule

1. We append rule that will drop all DNS packets where domain name server ip is 8.8.8.8 . DNS because protocol used is UDP and destination port is 53 and destination specified is 8.8.8.8
2. Result : Hence DNS request made by router to DNS server 8.8.8.8 will fail as packet is dropped.

Answer

1. dig www.uwindsor.ca succeeds because destination IP of DNS does not necessarily goes to 8.8.8.8 , even if it fails at 8.8.8.8 , it will try other DNS servers to resolve domain name.
2. dig @8.8.8.8 www.uwindsor.ca fails , because of the appended rule which says DNS server 8.8.8.8 is blocked for OUTPUT chain . It shows connection time out , no servers reached .

PART 8



Observations / Explanation of Rule

It drops incoming packet of router which are of type echo-request in ICMP protocl.

Answer

No reply was received by VM when ping was made to router

Explaination : As any packets with protocl icmp and –icmp-type echo-request will dropped at router's INPUT chain. Hence router never received those packets hence Router did not reply icmp echo reply message.

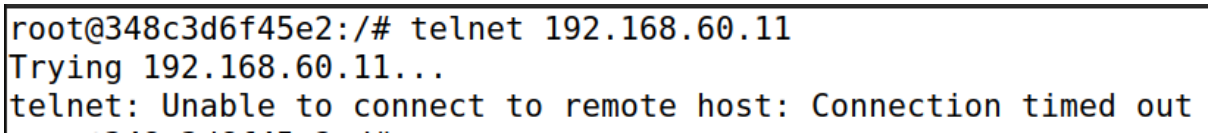
PART 9

```
root@939216d2b65a:/# iptables -P INPUT DROP
root@939216d2b65a:/# iptables -A INPUT -p tcp -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
root@939216d2b65a:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
348c3d6f45e2 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Mar 17 06:31:32 UTC 2024 from seed-router.net-192.168.60.0 on pts/2
seed@348c3d6f45e2:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.60.7  netmask 255.255.255.0  broadcast 192.168.60.255
        ether 02:42:c0:a8:3c:07  txqueuelen 0  (Ethernet)
        RX packets 314  bytes 23602 (23.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 194  bytes 15226 (15.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



Observations / Explanation of Rule

1. First we set default policy for INPUT chain to drop all incoming packets of router.
2. Second we append rule to INPUT chain specifying those TCP incoming packets which are in established or related state should be accepted. This means TCP rsponses to outgoing TCP requests will be accepted.

Answer

First telnet session (Router To VM) succeeds whereas latter one (VM to Router) was unable to connect to remote host

Explanation:

Router to VM : This Telnet connection succeeds because response packet from VM to Router are in response to TCP connection initiated by Router . Hence this packet is in related/established state .

VM to Router : This Telent connection fails because by default packets received by router will be dropped. So VM cannot establish Telnet Connection

PART 10

```
root@939216d2b65a:/# iptables -P INPUT DROP
root@939216d2b65a:/# iptables -A INPUT -p tcp -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
root@939216d2b65a:/# iptables-save  >myiptables.rules
root@939216d2b65a:/# iptables -F
root@939216d2b65a:/# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@939216d2b65a:/# iptables-restore < myiptables.rules
root@939216d2b65a:/# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@939216d2b65a:/#
```

Observations / Explanation of Rule

1. Rules can be saved using iptables-save > file_name.rules
2. Rules can be retrived from saved files using iptables-restore < file_name.rules

s