Assignment #1

Clemens Lo

A00863045

COMP 8006   January 28, 2016

TABLE OF CONTENTS

Overview

This assignment was for the purpose of creating a simple Linux firewall using iptables, which followed the following constraints:

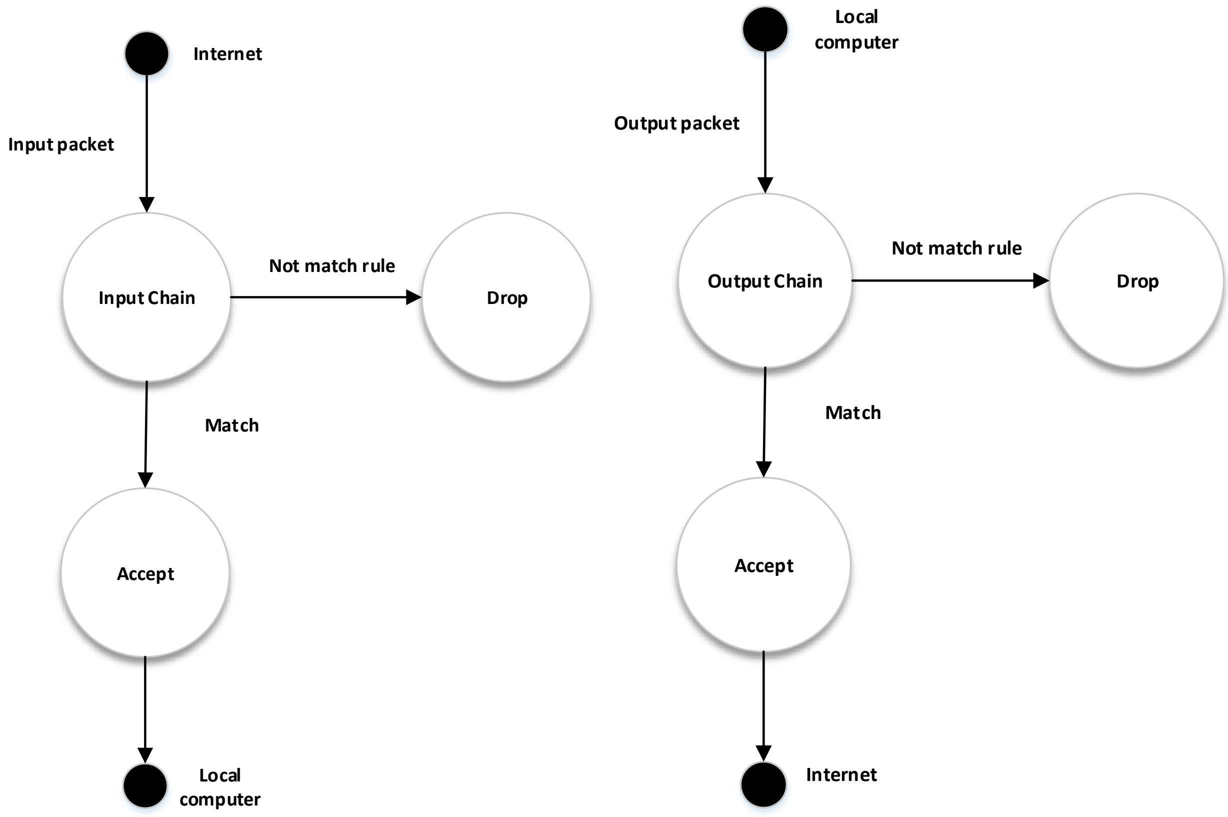
- Default policy to drop
- Permit inbound and outbound ssh packets
- Permit inbound and outbound www packets
- Drop packets destined to port 80 from ports less than 1024
- Drop all packets to and from port 0
- Keep track of all ssh and www traffic using custom chains
- Allow DNS and DHCP traffic through

Design Work

There are three User Defined Chains implemented:

- SSHTraffic – tracks all in/outbound packets witch src or sdt port equals 22
- WWWTraffic - tracks all in/outbound packets witch src or sdt port equals 80
- ALLTraffic - tracks all in/outbound packets

Design Diagrams



Testing

Rule #	Test Description	Tool Used	Expected Results	Pass/Fail
1	Permit inbound/ outbound SSH packets.	hping3 & SSH	The iptables -L -n -v -x audit should show the traffic.	pass
2	Permit inbound/ outbound HTTP packets.	hping3	hping2 should show a response on port 80 and and the iptables -L -n -v -x audit should show the traffic.	pass
3	Drop traffic to port 80 from source port < 1024	hping3	hping2 should not show any response and the iptables -L -n -v -x audit should NOT show the traffic.	pass
4	Drop all incoming packets from/to port 0.	hping3	hping2 should not show any response and the iptables -L -n -v -x audit should show the dropped traffic.	pass
5	Allow outbound DNS & DHCP packets	nslookup & dhclient	Should return results for any particular domain and the iptables -L -n -v -x audit should show the traffic.	pass
6	Drop all inbound traffic except for SSH and HTTP traffic.	zenmap	Should only show port 80 and 22 open	pass

Test Environment:

Host A (with firewall): 192.168.10.237

Host B: 192.168.10.97

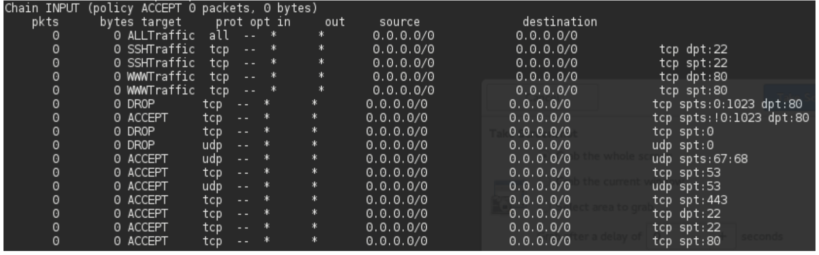
TEST CASE 1

Test Case	Description	hping Command	Expected Results	Actual Results
SSH				
1a	Permit inbound ssh (request)	hping3 192.168.10.237 -c 5 -S -s 8006 -p 22 (sent from Host B)	Accept 5 packets	10 packets accepted
1b	Permit outbound ssh (response)	hping3 192.168.10.97 -c 5 -S -s 8006 -p 22 (sent from Host A)	Accept 5 packet	1 packet accepted

Screenshots

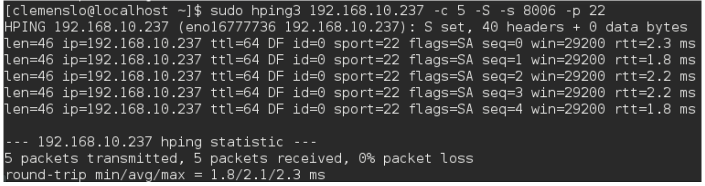
1a

Before hping (INBOUND CHAIN):



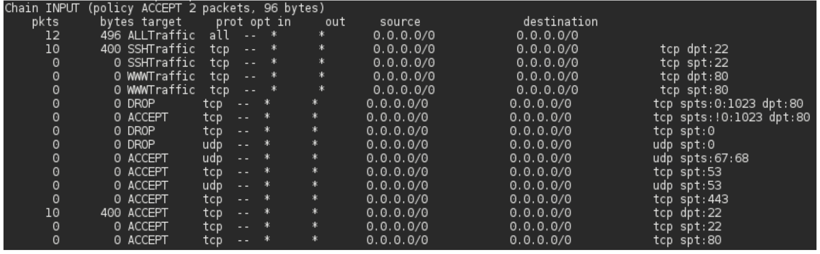
```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ALLTraffic  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spts:!0:1023 dpt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:0
       0        0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:0
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spts:67:68
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:53
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:53
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:443
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
```

hping (from Host B):



```
[clemenslo@localhost ~]$ sudo hping3 192.168.10.237 -c 5 -S -s 8006 -p 22
HPING 192.168.10.237 (eno16777736 192.168.10.237): S set, 40 headers + 0 data bytes
len=46 ip=192.168.10.237 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=2.3 ms
len=46 ip=192.168.10.237 ttl=64 DF id=0 sport=22 flags=SA seq=1 win=29200 rtt=1.8 ms
len=46 ip=192.168.10.237 ttl=64 DF id=0 sport=22 flags=SA seq=2 win=29200 rtt=2.2 ms
len=46 ip=192.168.10.237 ttl=64 DF id=0 sport=22 flags=SA seq=3 win=29200 rtt=2.2 ms
len=46 ip=192.168.10.237 ttl=64 DF id=0 sport=22 flags=SA seq=4 win=29200 rtt=1.8 ms

--- 192.168.10.237 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.8/2.1/2.3 ms
```

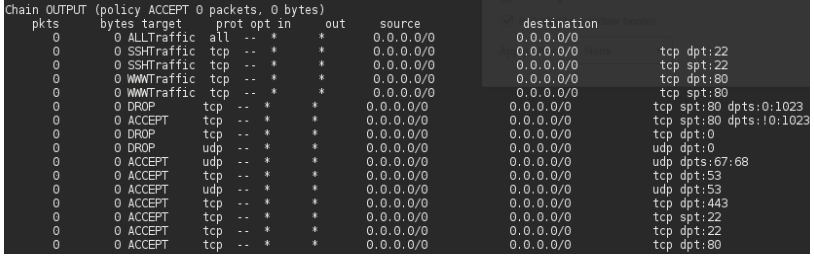
After hping (INBOUND CHAIN):



```
Chain INPUT (policy ACCEPT 2 packets, 96 bytes)
    pkts      bytes target     prot opt in     out     source               destination
      12      496 ALLTraffic  all  --  *      *       0.0.0.0/0            0.0.0.0/0
      10      400 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spts:!0:1023 dpt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:0
       0        0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:0
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spts:67:68
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:53
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:53
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:443
      10      400 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
```

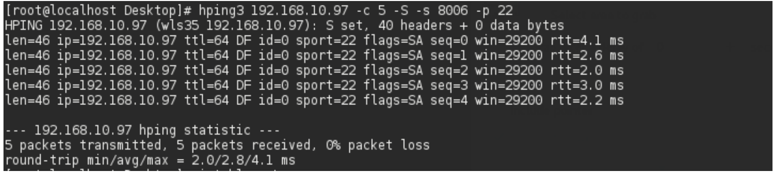
1b

Before hping (OUTBOUND CHAIN):



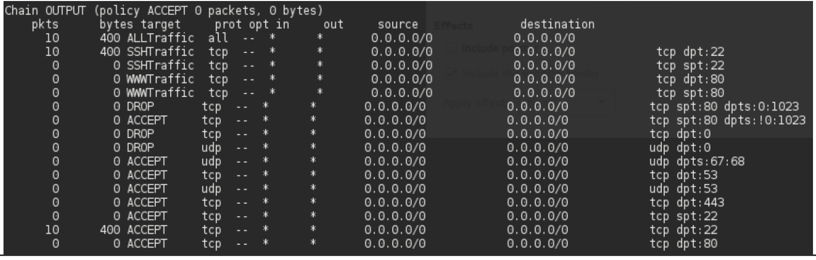
```
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ALLTraffic  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80 dpts:0:1023
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80 dpts:!0:1023
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:0
       0        0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:0
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpts:67:68
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
```

hping (from Host A)



```
[root@localhost Desktop]# hping3 192.168.10.97 -c 5 -S -s 8006 -p 22
HPING 192.168.10.97 (wls35 192.168.10.97): S set, 40 headers + 0 data bytes
len=46 ip=192.168.10.97 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=4.1 ms
len=46 ip=192.168.10.97 ttl=64 DF id=0 sport=22 flags=SA seq=1 win=29200 rtt=2.6 ms
len=46 ip=192.168.10.97 ttl=64 DF id=0 sport=22 flags=SA seq=2 win=29200 rtt=2.0 ms
len=46 ip=192.168.10.97 ttl=64 DF id=0 sport=22 flags=SA seq=3 win=29200 rtt=3.0 ms
len=46 ip=192.168.10.97 ttl=64 DF id=0 sport=22 flags=SA seq=4 win=29200 rtt=2.2 ms

--- 192.168.10.97 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.0/2.8/4.1 ms
```

After hping (OUTBOUND CHAIN):



```
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
      10      400 ALLTraffic  all  --  *      *       0.0.0.0/0            0.0.0.0/0
      10      400 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80 dpts:0:1023
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80 dpts:!0:1023
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:0
       0        0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:0
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpts:67:68
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
      10      400 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
```

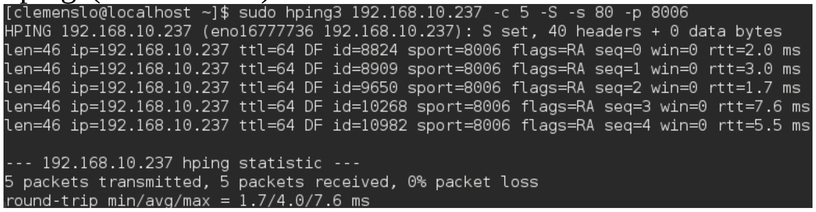
TEST CASE 2

Test Case	Description	hping Command	Expected Results	Actual Results
WWW				
1a	Permit inbound www (request)	hping3 192.168.10.237 -c 5 -S -s 80 -p 8006 (sent from Host B)	Accept 5 packets	5 packets accepted
1b	Permit outbound www (response)	hping3 192.168.10.97 -c 5 -S -s 8006 -p 80 (sent from Host A)	Accept 5 packet	5 packets accepted

Screenshots

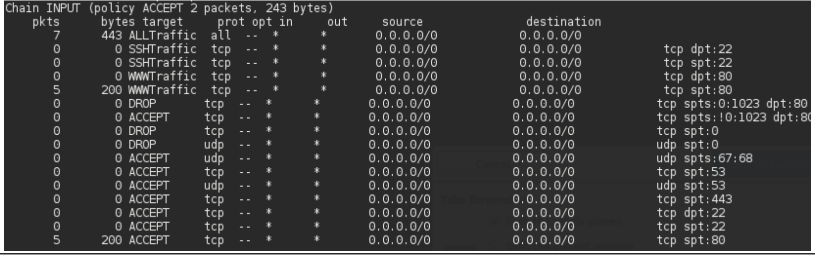
1a

hping (from Host B):



```
[clemenslo@localhost ~]$ sudo hping3 192.168.10.237 -c 5 -S -s 80 -p 8006
HPING 192.168.10.237 (eno16777736 192.168.10.237): S set, 40 headers + 0 data bytes
len=46 ip=192.168.10.237 ttl=64 DF id=8824 sport=8006 flags=RA seq=0 win=0 rtt=2.0 ms
len=46 ip=192.168.10.237 ttl=64 DF id=8909 sport=8006 flags=RA seq=1 win=0 rtt=3.0 ms
len=46 ip=192.168.10.237 ttl=64 DF id=9650 sport=8006 flags=RA seq=2 win=0 rtt=1.7 ms
len=46 ip=192.168.10.237 ttl=64 DF id=10268 sport=8006 flags=RA seq=3 win=0 rtt=7.6 ms
len=46 ip=192.168.10.237 ttl=64 DF id=10982 sport=8006 flags=RA seq=4 win=0 rtt=5.5 ms

--- 192.168.10.237 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.7/4.0/7.6 ms
```

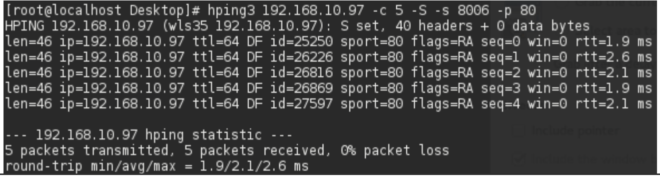
After hping (INBOUND CHAIN):



```
Chain INPUT (policy ACCEPT 2 packets, 243 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       7      443 ALLTraffic  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
       5      200 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spts:!0:1023 dpt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:0
       0        0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:0
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spts:67:68
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:53
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:53
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:443
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       5      200 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
```

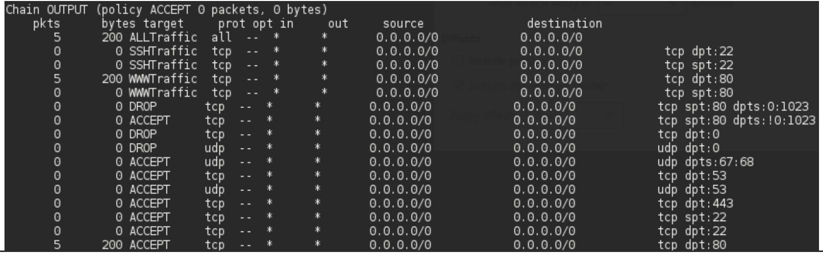
1b

hping (from Host A)



```
[root@localhost Desktop]# hping3 192.168.10.97 -c 5 -S -s 8006 -p 80
HPING 192.168.10.97 (wls35 192.168.10.97): S set, 40 headers + 0 data bytes
len=46 ip=192.168.10.97 ttl=64 DF id=25250 sport=80 flags=RA seq=0 win=0 rtt=1.9 ms
len=46 ip=192.168.10.97 ttl=64 DF id=26226 sport=80 flags=RA seq=1 win=0 rtt=2.6 ms
len=46 ip=192.168.10.97 ttl=64 DF id=26816 sport=80 flags=RA seq=2 win=0 rtt=2.1 ms
len=46 ip=192.168.10.97 ttl=64 DF id=26869 sport=80 flags=RA seq=3 win=0 rtt=1.9 ms
len=46 ip=192.168.10.97 ttl=64 DF id=27597 sport=80 flags=RA seq=4 win=0 rtt=2.1 ms

--- 192.168.10.97 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.9/2.1/2.6 ms
```

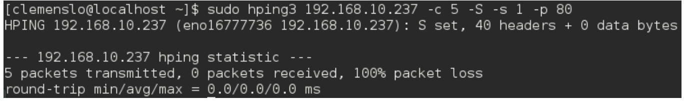
	After hping (OUTBOUND CHAIN):



```
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       5      200 ALLTraffic  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       5      200 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80 dpts:0:1023
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80 dpts:!0:1023
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:0
       0        0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:0
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpts:67:68
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       5      200 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
```

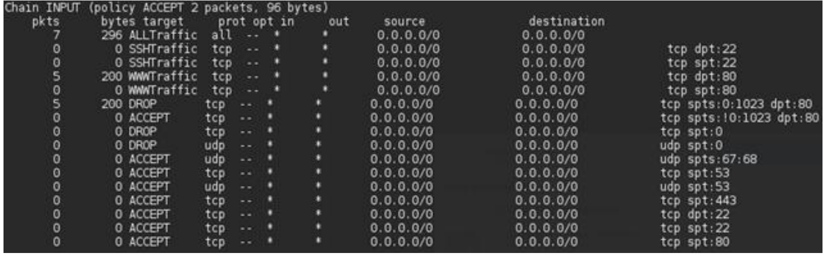
TEST CASE 3

Test Case	Description	hping Command	Expected Results	Actual Results
WWW				
3	Drop inbound traffic to port 80 from source ports less than 1024	hping3 192.168.10.237 -c 5 -S -s 1 -p 80 (sent from Host B)	Drop 5 packet	5 packets dropped
Screenshots				
3	hping (from Host B):			



```
[clemenslo@localhost ~]$ sudo hping3 192.168.10.237 -c 5 -S -s 1 -p 80
HPING 192.168.10.237 (eno16777736 192.168.10.237): S set, 40 headers + 0 data bytes

--- 192.168.10.237 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

After hping (INBOUND CHAIN):



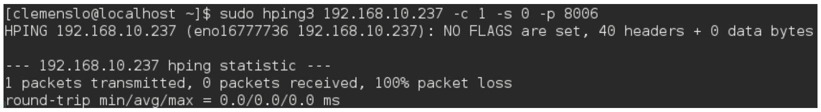
```
Chain INPUT (policy ACCEPT 2 packets, 96 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       7      296 ALLTraffic  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       5      200 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
       5      200 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spts:!0:1023 dpt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:0
       0        0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:0
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spts:67:68
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:53
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:53
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:443
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
```

TEST CASE 4

Test Case	Description	hping Command	Expected Results	Actual Results
Reserved Port 0				
1a	Drop all inbound packets from reserved port 0	hping3 192.168.10.237 -c 1 -s 0 -p 8006	Drop 1 packet	1 packet dropped
1b	Drop all outbound traffic to reserved port 0	hping3 192.168.10.97 -c 1 -p 0 -s 8006	Drop 1 packet	1 packet dropped
Screenshots				

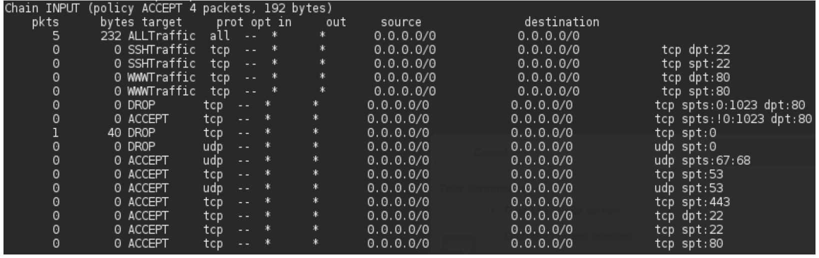
1a

hping (from Host B):



```
[clemenslo@localhost ~]$ sudo hping3 192.168.10.237 -c 1 -s 0 -p 8006
HPING 192.168.10.237 (eno16777736 192.168.10.237): NO FLAGS are set, 40 headers + 0 data bytes

--- 192.168.10.237 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

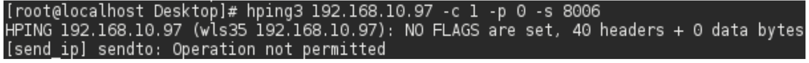
After hping (INBOUND CHAIN):



```
Chain INPUT (policy ACCEPT 4 packets, 192 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       5      232 ALLTraffic  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:0:1023 dpt:80
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:!0:1023 dpt:80
       1       40 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
       0        0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spts:67:68
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
```

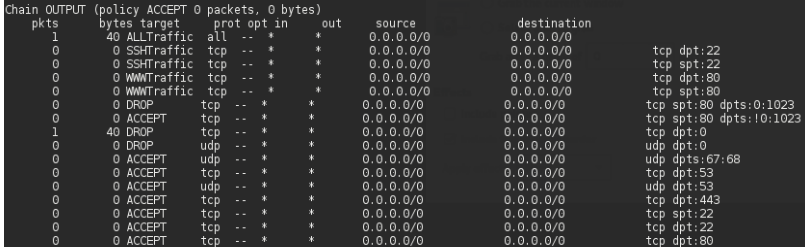
1b

hping (from Host A)



```
[root@localhost Desktop]# hping3 192.168.10.97 -c 1 -p 0 -s 8006
HPING 192.168.10.97 (wls35 192.168.10.97): NO FLAGS are set, 40 headers + 0 data bytes
[send_ip] sendto: Operation not permitted
```

After hping (OUTBOUND CHAIN):



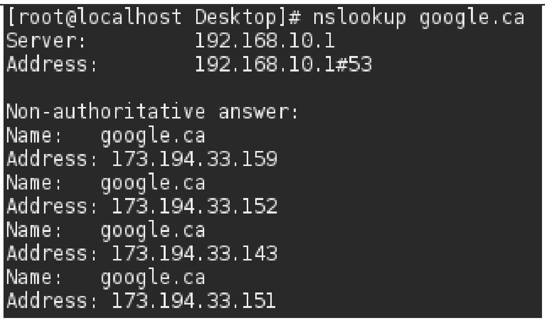
```
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       1       40 ALLTraffic  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80 dpts:0:1023
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80 dpts:!0:1023
       1       40 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
       0        0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpts:67:68
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
```

TEST CASE 5

Test Case	Description	Command	Expected Results	Actual Results
	DNS & DHCP			
5a	Permit all in/out bound DNS packets	nslookup google.ca	Packet accept from both in/out bound	Packet accepted from both in/out bound
5b	Permit outbound DHCP packets	dhclient -r	Accept 1 packet	1 packet accepted

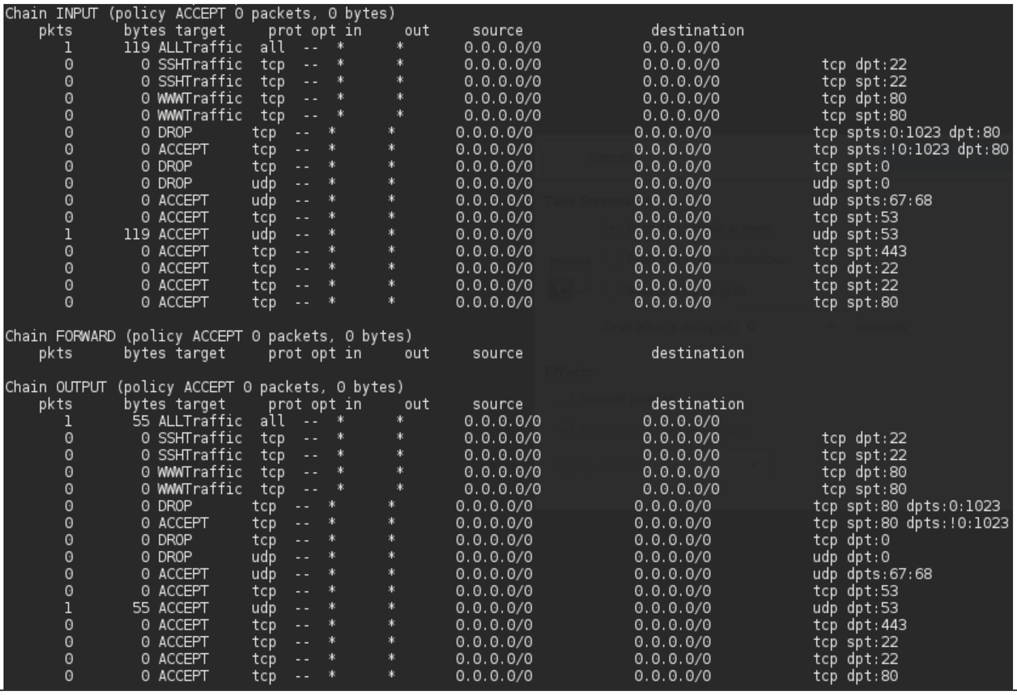
Screenshots

5a



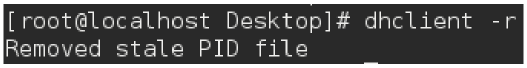
```
[root@localhost Desktop]# nslookup google.ca
Server:         192.168.10.1
Address:        192.168.10.1#53

Non-authoritative answer:
Name:   google.ca
Address: 173.194.33.159
Name:   google.ca
Address: 173.194.33.152
Name:   google.ca
Address: 173.194.33.143
Name:   google.ca
Address: 173.194.33.151
```

(INBOUND CHAIN):



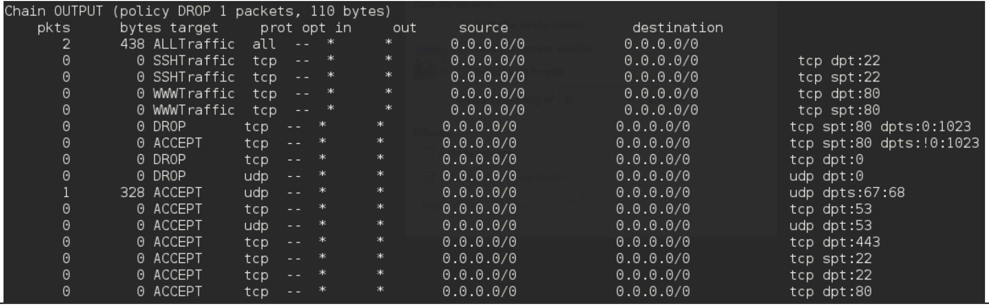
```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       1      119 ALLTraffic  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spts:!0:1023 dpt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:0
       0        0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:0
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spts:67:68
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:53
       1      119 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:53
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:443
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       1       55 ALLTraffic  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80 dpts:0:1023
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80 dpts:!0:1023
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:0
       0        0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:0
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpts:67:68
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
       1       55 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
```

5b



```
[root@localhost Desktop]# dhclient -r
Removed stale PID file
```

(OUTBOUND CHAIN):



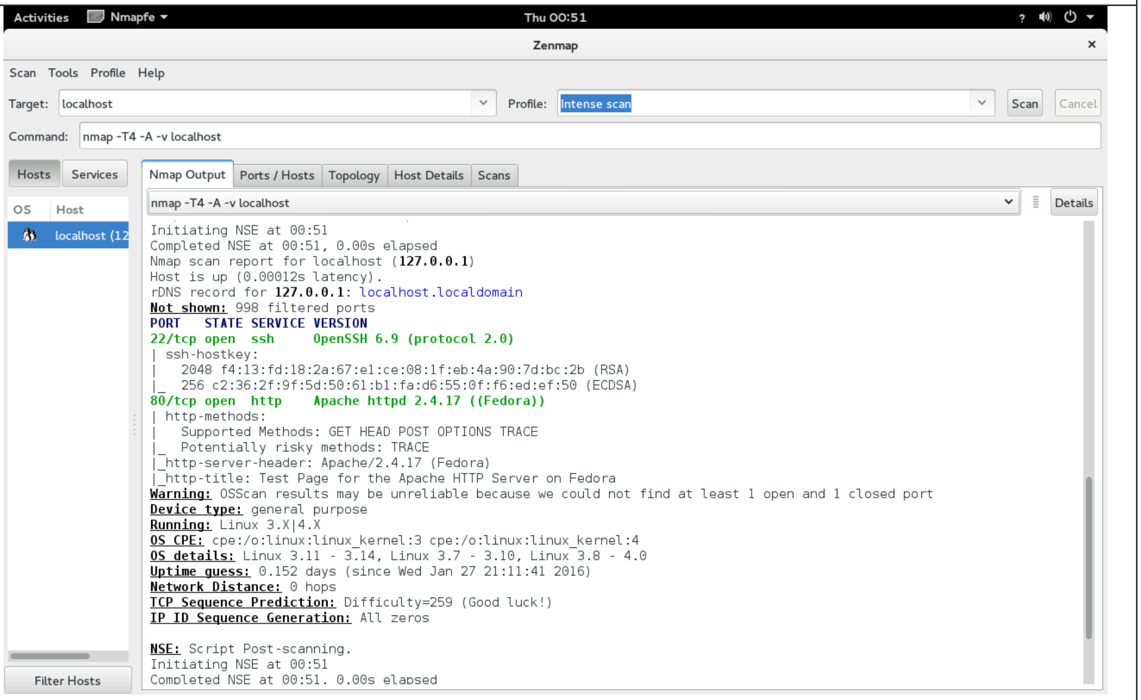
```
Chain OUTPUT (policy DROP 1 packets, 110 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       2      438 ALLTraffic  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 SSHTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
       0        0 WWWTraffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80 dpts:0:1023
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80 dpts:!0:1023
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:0
       0        0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:0
       1      328 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpts:67:68
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
```

TEST CASE 6

Test Case	Description	Command	Expected Results	Actual Results
	Port scanning			
6	Scanning all open port	nmapfe	Only port 22 and 80 open	Only port 80 and 22 open

Screenshots

6



Target: localhost

Profile: Intense scan

Command: nmap -T4 -A -v localhost

nmap -T4 -A -v localhost

```
Initiating NSE at 00:51
Completed NSE at 00:51, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00012s latency).
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.9 (protocol 2.0)
| ssh-hostkey:
|   2048 f4:13:fd:18:2a:67:e1:ce:08:1f:eb:4a:90:7d:bc:2b (RSA)
|_  256 c2:36:2f:9f:5d:50:61:b1:fa:d6:55:0f:f6:ed:ef:50 (ECDSA)
80/tcp open  http    Apache httpd 2.4.17 ((Fedora))
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.17 (Fedora)
|_http-title: Test Page for the Apache HTTP Server on Fedora
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 3.14, Linux 3.7 - 3.10, Linux 3.8 - 4.0
Uptime guess: 0.152 days (since Wed Jan 27 21:11:41 2016)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros

NSE: Script Post-scanning.
Initiating NSE at 00:51
Completed NSE at 00:51, 0.00s elapsed
```