Assignment #1

Simple Personal Linux Firewall

Steffen L. Norgren
A00683006

COMP 8006 - Network Administration & Security II • BCIT • January 28, 2010

Table of Contents

Overview 3

Design Work 3

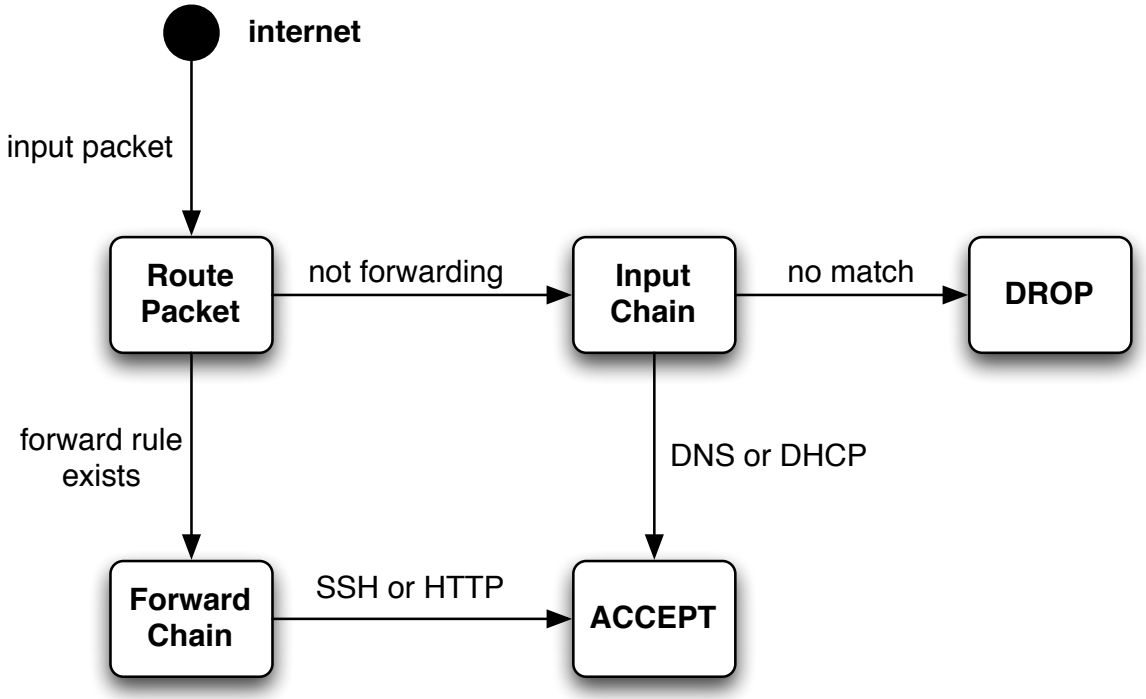
Testing 5

Overview

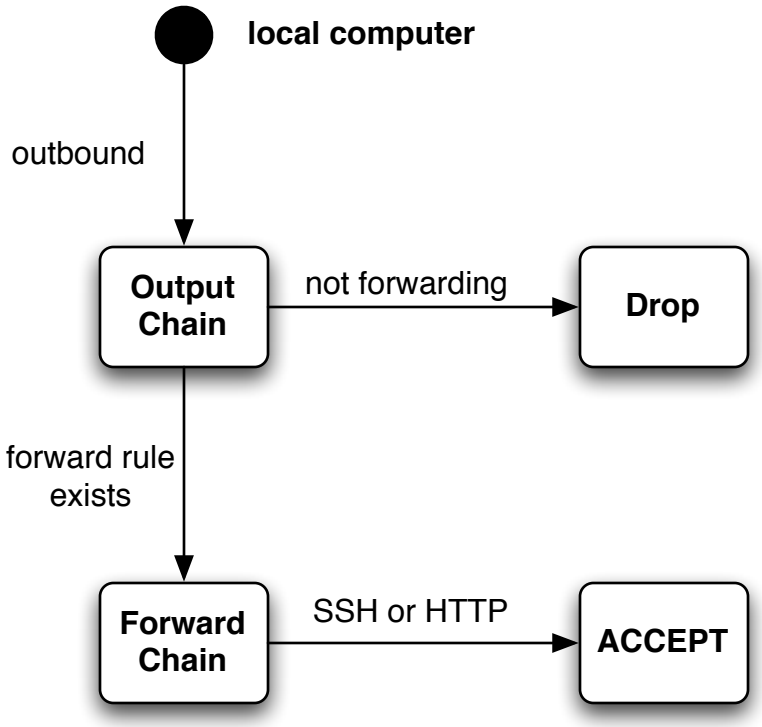
This assignment was for the purpose of creating a simple Linux firewall where everything would be blocked with the exception of SSH and HTTP traffic. To do this, I had to first create a default DROP policy and then selectively open the needed ports, which also included DHCP and DNS. Additionally, I needed make sure that the firewall allowed communication via established connections.

Design Work

Inbound Traffic



Outbound Traffic

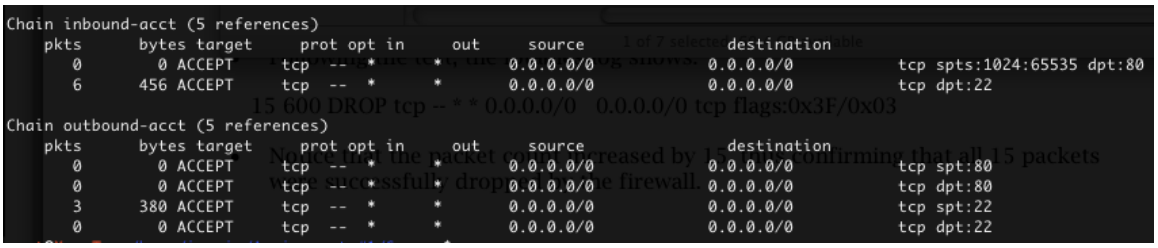


TESTING

Rule #	Test Description	Tool Used	Expected Results	Pass/Fail
1	Permit inbound/ outbound SSH packets.	Log on to the ssh server from and external ssh client	The iptables -L -n -v -x audit should show the traffic.	Pass. Detailed results are attached.
2	Permit inbound/ outbound HTTP packets.	hping3 & opening a browser session.	hping2 should show a response on port 80 and and the iptables -L -n -v -x audit should show the traffic.	Pass. Detailed results are attached.
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. Detailed results are attached.
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.	Fail. Detailed results are attached.
5	Drop all incoming packets that have both the SYN and FIN bits set together.	hping3	hping2 should not show any response and the iptables -L -n -v -x audit should show the dropped traffic.	Pass. Detailed results are attached.
6	Allow outbound DNS & DHCP packets	nslookup	Should return results for any particular domain and the iptables -L -n -v -x audit should show the traffic.	Pass. Detailed results are attached.

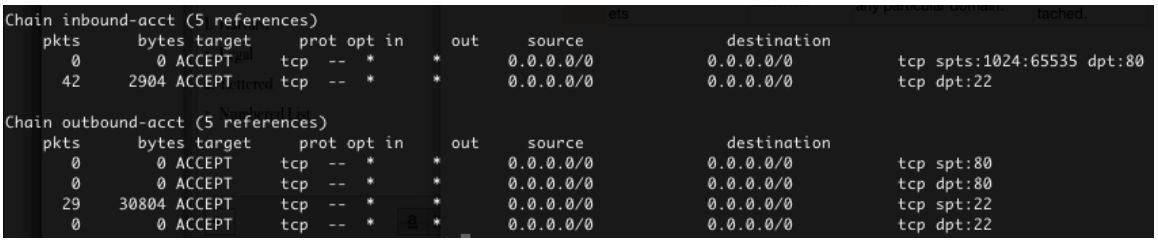
Test Case #1

Before the test:



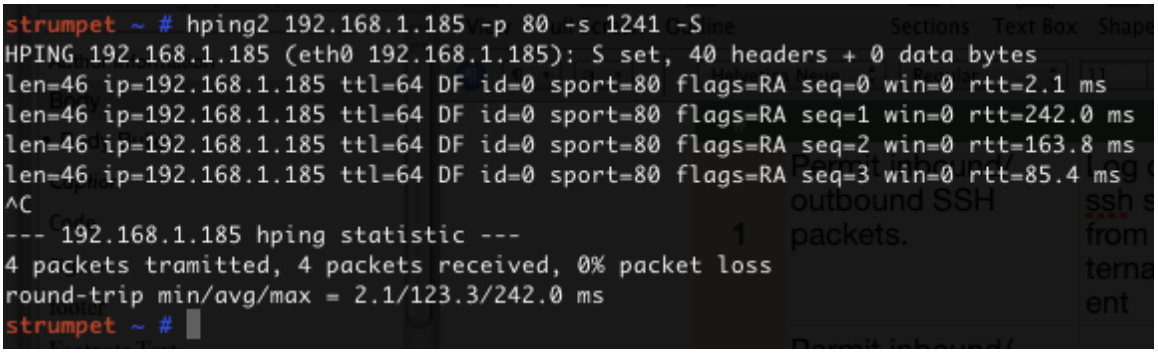
```
Chain inbound-acct (5 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1024:65535 dpt:80
       6      456 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22

Chain outbound-acct (5 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
       3      380 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
```

After the test:



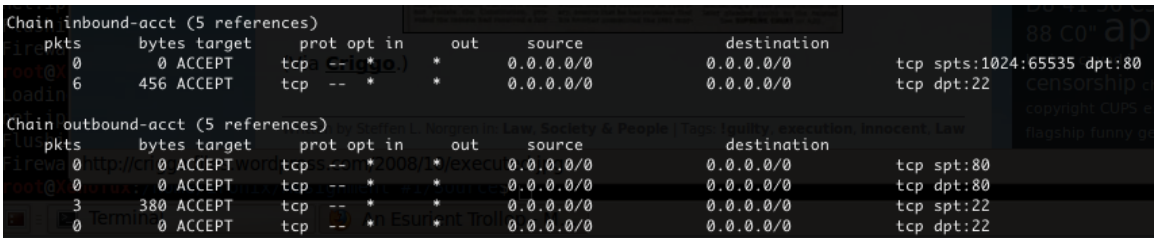
```
Chain inbound-acct (5 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1024:65535 dpt:80
      42     2904 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22

Chain outbound-acct (5 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
      29    30804 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
```

Test Case #2



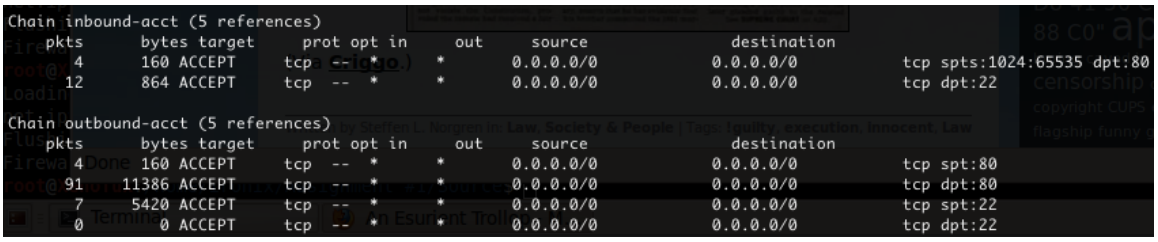
```
strumpet ~ # hping2 192.168.1.185 -p 80 -s 1241 -S
HPING 192.168.1.185 (eth0 192.168.1.185): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.185 ttl=64 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=2.1 ms
len=46 ip=192.168.1.185 ttl=64 DF id=0 sport=80 flags=RA seq=1 win=0 rtt=242.0 ms
len=46 ip=192.168.1.185 ttl=64 DF id=0 sport=80 flags=RA seq=2 win=0 rtt=163.8 ms
len=46 ip=192.168.1.185 ttl=64 DF id=0 sport=80 flags=RA seq=3 win=0 rtt=85.4 ms
^C
--- 192.168.1.185 hping statistic ---
4 packets tramitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.1/123.3/242.0 ms
strumpet ~ #
```

Before the test:



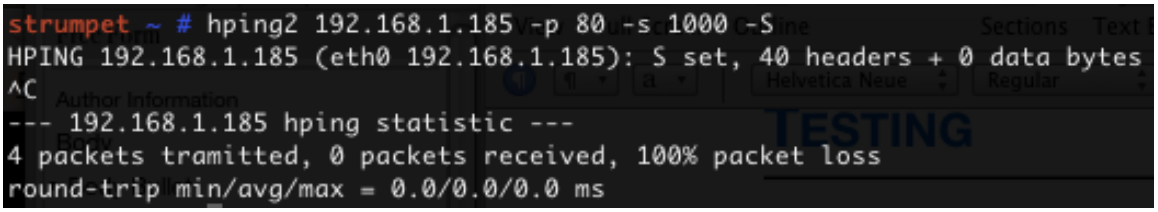
```
Chain inbound-acct (5 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1024:65535 dpt:80
       6      456 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22

Chain outbound-acct (5 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
       3      380 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
```

After the test:



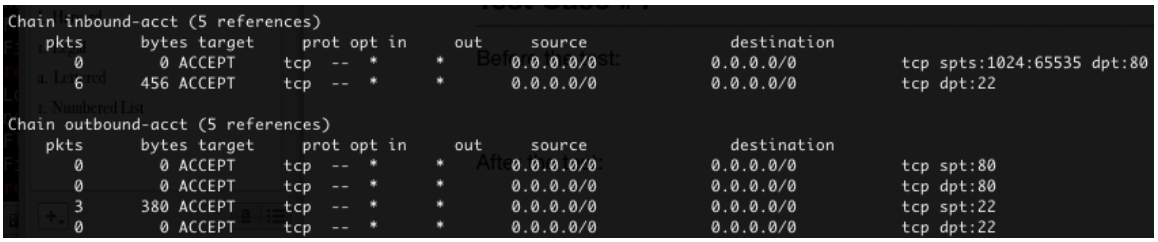
```
Chain inbound-acct (5 references)
    pkts      bytes target     prot opt in     out     source               destination
       4      160 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1024:65535 dpt:80
      12      864 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22

Chain outbound-acct (5 references)
    pkts      bytes target     prot opt in     out     source               destination
       4      160 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
      91    11386 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
       7     5420 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
```

Test Case #3



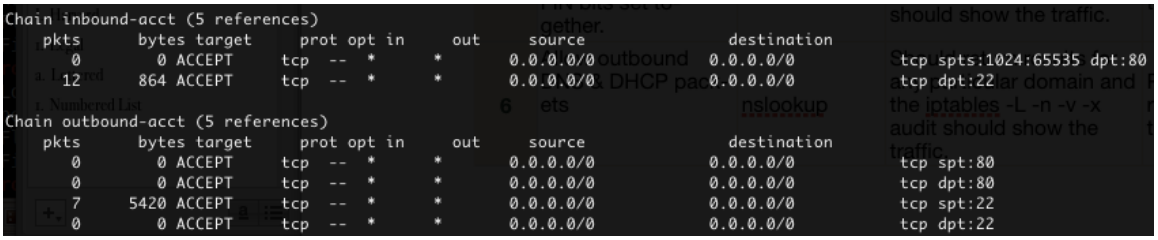
```
strumpet ~ # hping2 192.168.1.185 -p 80 -s 1000 -S
HPING 192.168.1.185 (eth0 192.168.1.185): S set, 40 headers + 0 data bytes
^C
--- 192.168.1.185 hping statistic ---
4 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Before the test:



```
Chain inbound-acct (5 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1024:65535 dpt:80
       6      456 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22

Chain outbound-acct (5 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
       3      380 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
```

After the test:



```
Chain inbound-acct (5 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1024:65535 dpt:80
      12      864 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22

Chain outbound-acct (5 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
       7     5420 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
```

Test Case #4

For some reason the first packet would be dropped, but all subsequent packets would go through. Haven't figured this one out yet.

```
strumpet ~ # hping2 192.168.1.185 -p 22 -s 0 -S
HPING 192.168.1.185 (eth0 192.168.1.185): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.185 ttl=64 DF id=0 sport=22 flags=SA seq=1 win=5840 rtt=234.2 ms
len=46 ip=192.168.1.185 ttl=64 DF id=0 sport=22 flags=SA seq=2 win=5840 rtt=155.7 ms
len=46 ip=192.168.1.185 ttl=64 DF id=0 sport=22 flags=A seq=3 win=5840 rtt=77.2 ms
^C
--- 192.168.1.185 hping statistic ---
5 packets tramitted, 3 packets received, 40% packet loss
round-trip min/avg/max = 77.2/155.7/234.2 ms
```

Before the test:

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
       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 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 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:!0x17/0x02 state NEW
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x3F
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x29
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x37
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x06/0x06
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x03/0x03
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:67 dpt:68
       0        0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           PKTTYPE = broadcast
       6      456 inbound-acct  tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0
       0        0 ACCEPT     all  --  eth0   *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
```

After the test:

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
       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 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 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:!0x17/0x02 state NEW
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x3F
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x29
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x37
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x06/0x06
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x03/0x03
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:67 dpt:68
       3      434 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           PKTTYPE = broadcast
      18     1080 inbound-acct  tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0
       0        0 ACCEPT     all  --  eth0   *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
```

Test Case #5

```
strumpet ~ # hping2 192.168.1.185 -p 22 -s 1274 -S -F
HPING 192.168.1.185 (eth0 192.168.1.185): SF set, 40 headers + 0 data bytes
^C
--- 192.168.1.185 hping statistic ---
4 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Before the test:

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
       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 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 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:!0x17/0x02 state NEW
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x3F
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x29
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x37
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x06/0x06
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x03/0x03
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:67 dpt:68
       0        0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           PKTTYPE = broadcast
       6      456 inbound-acct  tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0
       0        0 ACCEPT     all  --  eth0   *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
```

After the test:

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
       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 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
       7      280 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:!0x17/0x02 state NEW
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x3F
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x29
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x37
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x06/0x06
       0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x03/0x03
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:67 dpt:68
       5      823 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           PKTTYPE = broadcast
      11      812 inbound-acct  tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0
       0        0 ACCEPT     all  --  eth0   *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
```

Test Case #6

```
root@XenoTux:/home/ironix/Assignment #1/Source$ nslookup yahoo.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   yahoo.com
Address: 209.191.93.53
Name:   yahoo.com
Address: 69.147.114.224
Name:   yahoo.com
Address: 209.131.36.159
```

Before the test:

```
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     all  --  *      *       127.0.0.1            0.0.0.0/0
       0        0 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:68 state NEW
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53 state NEW
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53 state NEW
      18     1880 outbound-acct  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
```

After the test:

```
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     all  --  *      *       127.0.0.1            0.0.0.0/0
       0        0 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
       0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:68 state NEW
       0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53 state NEW
       1       55 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53 state NEW
      27     4028 outbound-acct  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
```