COMP 8006
Assignment 1
January 29 / 2015

Geoff Dabu
A00817395

INTRODUCTION

The purpose of this assignment is to write a 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: User Defined Chains

Three User Defined Chains were implemented:

- trafficSSH
- trafficWWW
- trafficALL

trafficSSH - tracks all inbound and outbound packets whose src or dst port equals 22
trafficWWW - tracks all inbound and outbound packets whose src or dst port equals 80
trafficALL - tracks all inbound and outbound packets

TESTING

The following table presents the tests for the requested constraints. For each test case the hping command used for testing is listed, along with the expected/actual results. To verify that the results were valid, screenshots were also supplied. Each test case consists of at least three screenshots; **Before Hping Packet Craft, Hping Packet Craft and After Hping Packet Craft.** The Before and After Hping Packet Craft screenshots present the rule which reacted to the packets crafted/sent by hping. eg. For test case 1a (Permit inbound ssh), I took a screenshot of the input chain rule before any packets were sent. Then I took a screenshot of the 5 packets that were sent by hping, and then finally I took a screenshot of the same chain rule but this time the rule listing showed that 5 packets were accepted.

In addition, for test cases which validated SSH and WWW connections I provided screenshots of SSH connections through terminal, and connections made to Apache.

Test Environment:

Host A (System with firewall): 192.168.0.118
Host B: 192.168.0.143

Both machines were running Fedora 20.

Test Case	Description	Hping Command	Expected Results	Actual Results
SSH				
1a	Permit **inbound** ssh (request)	hping3 192.168.0.118 -c 5 -S -s 8006 -p 22 (sent from Host B)	Accept 5 packets	
1b	Permit **outbound** ssh (response)	hping3 192.168.0.143 -c 1 -S -A -s 22 -p 8006 (sent from Host A)	Accept 1 packets	

Test Screenshots

1a

Before Hping Packet Craft (INBOUND CHAIN):

```
0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp dpt:22
```

Hping Packet Craft (from Host B):

```
[root@localhost hping-master]# hping3 192.168.0.118 -c 5 -S -s 8006 -p 22
HPING 192.168.0.118 (p2p1 192.168.0.118): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.118 ttl=64 DF id=64408 sport=22 flags=RA seq=0 win=0 rtt=0.4 ms
len=46 ip=192.168.0.118 ttl=64 DF id=65006 sport=22 flags=RA seq=1 win=0 rtt=0.6 ms
len=46 ip=192.168.0.118 ttl=64 DF id=65475 sport=22 flags=RA seq=2 win=0 rtt=0.5 ms
len=46 ip=192.168.0.118 ttl=64 DF id=578 sport=22 flags=RA seq=3 win=0 rtt=0.5 ms
len=46 ip=192.168.0.118 ttl=64 DF id=1480 sport=22 flags=RA seq=4 win=0 rtt=0.5 ms

--- 192.168.0.118 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.5/0.6 ms
```

After Hping Packet Craft (INBOUND CHAIN):

```
5      200 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp dpt:22
```

1b

Before Hping Packet Craft (OUTBOUND CHAIN):

```
0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp spt:22
```

Hping Packet Craft (from Host A):

```
[root@localhost 8006Assignment1]# hping3 192.168.0.143 -c 1 -S -A -s 22 -p 8006
HPING 192.168.0.143 (p2p1 192.168.0.143): SA set, 40 headers + 0 data bytes
len=46 ip=192.168.0.143 ttl=64 DF id=59265 sport=8006 flags=R seq=0 win=0 rtt=0.6 ms

--- 192.168.0.143 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.6/0.6/0.6 ms
```

After Hping Packet Craft (OUTBOUND CHAIN):

```
1       40 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp spt:22
```

An ssh connection initiated by host B to host A, would also verify both test case 1a and 1b. Shown below is a screenshot of a successful ssh login from host b to a.

```
[root@localhost hping-master]# ssh 192.168.0.118
root@192.168.0.118's password:
Last login: Mon Jan 26 23:32:35 2015 from 192.168.0.143
[root@localhost ~]#
```

<table>
<tr><th>Test Case</th><th>Description</th><th>Hping Command</th><th>Expected Results</th><th>Actual Results</th></tr>
<tr><td colspan="2">SSH</td><td></td><td colspan="2"></td></tr>
<tr><td>2a</td><td>Permit outbound ssh (request)</td><td>hping3 192.168.0.143 -c 5 -S -s 8006 -p 22 (sent from Host A)</td><td>Accept 5 packets</td><td></td></tr>
<tr><td>2b</td><td>Permit inbound ssh (response)</td><td>hping3 192.168.0.118 -c 5 -S -A -s 22 -p 8006 (sent from Host B)</td><td>Accept 1 packets</td><td></td></tr>
<tr><td colspan="5">Test Procedures/Documents/Screenshots</td></tr>
<tr><td>2a</td><td colspan="4">Before Hping Packet Craft (OUTBOUND CHAIN):
0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22
Hping Packet Craft (from Host A):
[root@localhost 8006Assignment1]# hping3 192.168.0.143 -c 5 -S -s 8006 -p 22
HPING 192.168.0.143 (p2p1 192.168.0.143): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.143 ttl=64 DF id=63898 sport=22 flags=RA seq=0 win=0 rtt=0.4 ms
len=46 ip=192.168.0.143 ttl=64 DF id=64935 sport=22 flags=RA seq=1 win=0 rtt=0.4 ms
len=46 ip=192.168.0.143 ttl=64 DF id=64998 sport=22 flags=RA seq=2 win=0 rtt=0.5 ms
len=46 ip=192.168.0.143 ttl=64 DF id=65129 sport=22 flags=RA seq=3 win=0 rtt=3.9 ms
len=46 ip=192.168.0.143 ttl=64 DF id=65175 sport=22 flags=RA seq=4 win=0 rtt=6.0 ms

--- 192.168.0.143 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/2.2/6.0 ms
After Hping Packet Craft (OUTBOUND CHAIN):
5 200 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22</td></tr>
<tr><td>2b</td><td colspan="4">Before Hping Packet Craft (INBOUND CHAIN):
0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:22

Hping Packet Craft (from Host B):
[root@localhost ~]# hping3 192.168.0.118 -S -A -c 1 -s 22 -p 8006
HPING 192.168.0.118 (p2p1 192.168.0.118): SA set, 40 headers + 0 data bytes

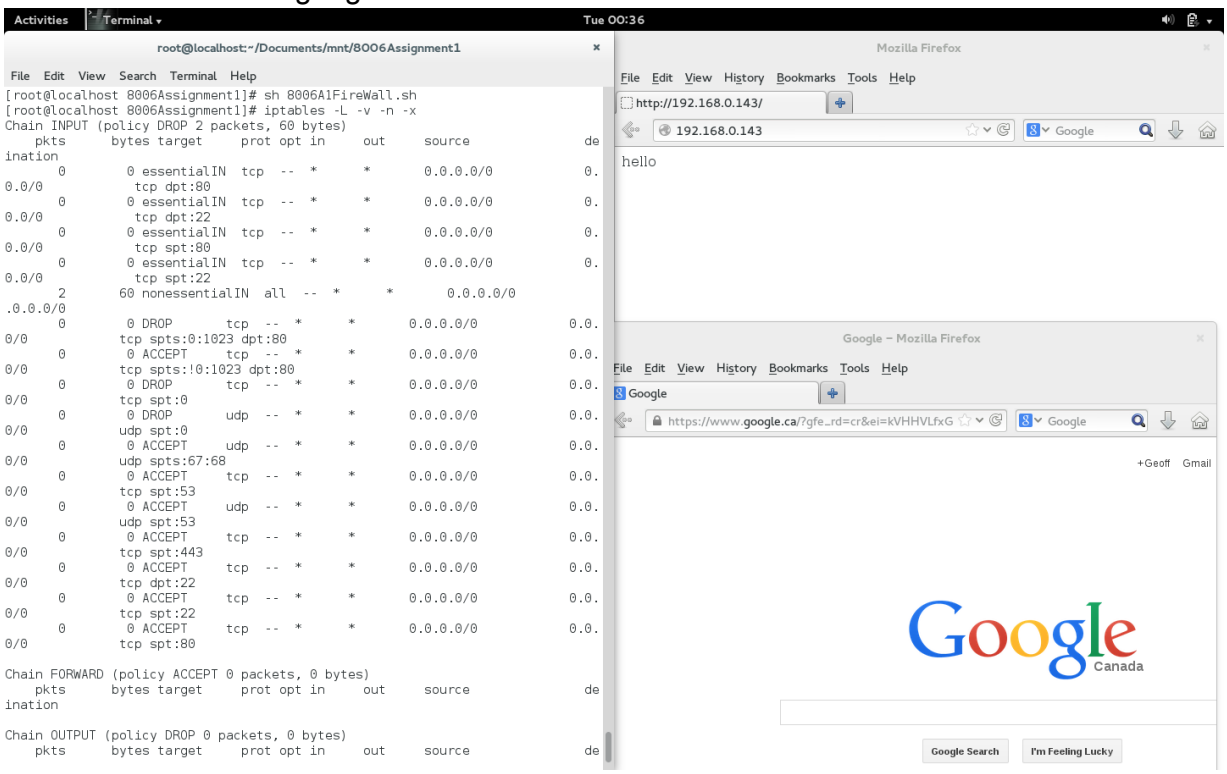
--- 192.168.0.118 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
After Hping Packet Craft (INBOUND CHAIN):
1 40 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:22</td></tr>
<tr><td colspan="5">An ssh connection initiated by host A to host B, would also verify both test case 2a and 2b. Shown below is a screenshot of a successful ssh login from host a to b.
[root@localhost 8006Assignment1]# ssh 192.168.0.143
root@192.168.0.143's password:
Last login: Tue Jan 27 00:06:09 2015 from 192.168.0.118
[root@localhost ~]#</td></tr>
</table>

Test Case	Description	Hping Command	Expected Results	Actual Results
WWW				
3a	Permit **outbound** www (request)	hping3 192.168.0.143 -c 5 -S -s 8006 -p 80 (from host A)	Accept 5 packets	
3b	Permit **inbound** www (response)	hping3 192.168.0.118 -c 1 -S -A -s 80 -p 8006 (from host B)	Accept 1 packets	
4	Drop **inbound** traffic to port 80 (http requests) from source ports less than 1024	hping3 192.168.0.118 -c 5 -S -s 1 -p 80 (from host B)	Drop 5 packets	
Test Procedures/Documents/Screenshots				

3a	**Before Hping Packet Craft (OUTBOUND CHAIN):**
	`0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80`
	Hping Packet Craft (from Host A):
	`[root@localhost 8006Assignment1]# hping3 192.168.0.143 -c 5 -S -s 8006 -p 80`
	`HPING 192.168.0.143 (p2p1 192.168.0.143): S set, 40 headers + 0 data bytes`
	`len=46 ip=192.168.0.143 ttl=64 DF id=63678 sport=80 flags=RA seq=0 win=0 rtt=0.8 ms`
	`len=46 ip=192.168.0.143 ttl=64 DF id=64434 sport=80 flags=RA seq=1 win=0 rtt=0.4 ms`
	`len=46 ip=192.168.0.143 ttl=64 DF id=65291 sport=80 flags=RA seq=2 win=0 rtt=0.7 ms`
	`len=46 ip=192.168.0.143 ttl=64 DF id=230 sport=80 flags=RA seq=3 win=0 rtt=0.5 ms`
	`len=46 ip=192.168.0.143 ttl=64 DF id=320 sport=80 flags=RA seq=4 win=0 rtt=0.6 ms`
	`--- 192.168.0.143 hping statistic ---`
	`5 packets transmitted, 5 packets received, 0% packet loss`
	`round-trip min/avg/max = 0.4/0.6/0.8 ms`
	After Hping Packet Craft (OUTBOUND CHAIN):
	`5 200 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80`			

3b	**Before Hping Packet Craft (INBOUND CHAIN):**
	`0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:80`
	Hping Packet Craft (from Host B):
	`[root@localhost hping-master]# hping3 192.168.0.118 -S -A -c 1 -s 80 -p 8006`
	`HPING 192.168.0.118 (p2p1 192.168.0.118): SA set, 40 headers + 0 data bytes`
	`len=46 ip=192.168.0.118 ttl=64 DF id=51234 sport=8006 flags=R seq=0 win=0 rtt=0.7 ms`
	`--- 192.168.0.118 hping statistic ---`
	`1 packets transmitted, 1 packets received, 0% packet loss`
	`round-trip min/avg/max = 0.7/0.7/0.7 ms`
	After Hping Packet Craft (INBOUND CHAIN):
	`1 40 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:80`			

A connection request by host a to apache web server running on host b verifies both 3a and 3b. Shown below is host a connecting to apache running on host b as well as an opened browser connected to google.com.



4	**Before Hping Packet Craft (INBOUND CHAIN):** 0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spts:0:1023 dpt:80 **Hping Packet Craft (from host b):** [root@localhost hping-master]# hping3 192.168.0.118 -S -c 5 -s 1 -p 80 HPING 192.168.0.118 (p2p1 192.168.0.118): S set, 40 headers + 0 data bytes --- 192.168.0.118 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 Packet Craft (INBOUND CHAIN):** 5 200 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spts:0:1023 dpt:80

Test Case	Description	Hping Command	Expected Results	Actual Results
Reserved Port 0				
6	Drop all **inbound** packets from reserved port 0	hping3 192.168.0.118 -s 0 -c 1 (from host B)	drop 1 packet	drop 1 packet
7	Drop all **outbound** traffic to reserved port 0	hping3 192.168.0.143 -p 0 -s 8006 -c 10 (from host A)	drop 10 packet	1 packet was dropped, then hping rejected the the next and output "Operation not permited"
Test Procedures/Documents/Screenshots				

6	**Before Hping Packet Craft (INBOUND CHAIN):**
	`0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:0`
	Hping Packet Craft (from Host B):
	`[root@localhost html]# hping3 192.168.0.118 -s 0 -c 1`
	`HPING 192.168.0.118 (p2p1 192.168.0.118): NO FLAGS are set, 40 headers + 0 data bytes`
	`--- 192.168.0.118 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 Packet Craft (INBOUND CHAIN):
	`1 40 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:0`			

7	**Before Hping Packet Craft (OUTBOUND CHAIN):**
	`0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:0`
	Hping Packet Craft (from host A):
	`[root@localhost 8006Assignment1]# hping3 192.168.0.143 -p 0 -s 8006 -c 10`
	`HPING 192.168.0.143 (p2p1 192.168.0.143): NO FLAGS are set, 40 headers + 0 data bytes`
	`[send ip] sendto: Operation not permitted`
	After Hping Packet Craft (OUTBOUND CHAIN):
	`1 40 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:0`			

Test Case	Description	Hping Command	Expected Results	Actual Results
User Defined Accounting				
8	Track all ssh traffic	hping 192.168.0.143 -s 8006 -p 22 -c 20 (from host A)	count 20 packets	count 20 packets
9	Track all www traffic	hping 192.168.0.143 -s 8006 -p 80 -c 20 (from host A)	count 20 packets	count 20 packets
Test Procedures/Documents/Screenshots				

8	**User Defined Chain before hping:**
	`Chain trafficSSH (4 references)`
	`pkts bytes target prot opt in out source destination`
	`0 0 all -- * * 0.0.0.0/0 0.0.0.0/0`
	Hping Packet Craft (from host A):
	`[root@localhost 8006Assignment1]# hping 192.168.0.143 -s 8006 -p 22 -c 20`
	`HPING 192.168.0.143 (p2p1 192.168.0.143): NO FLAGS are set, 40 headers + 0 data bytes`
	`--- 192.168.0.143 hping statistic ---`
	`20 packets transmitted, 0 packets received, 100% packet loss`
	`round-trip min/avg/max = 0.0/0.0/0.0 ms`
	After Hping Packet Craft (USER DEFINED CHAIN):
	`Chain trafficSSH (4 references)`
	`pkts bytes target prot opt in out source destination`
	`20 800 all -- * * 0.0.0.0/0 0.0.0.0/0`			

9	**User Defined Chain before hping:**
	`Chain trafficWWW (4 references)`
	`pkts bytes target prot opt in out source destination`
	`0 0 all -- * * 0.0.0.0/0 0.0.0.0/0`
	Hping Packet Craft (from host A):
	`[root@localhost 8006Assignment1]# hping 192.168.0.143 -s 8006 -p 80 -c 20`
	`HPING 192.168.0.143 (p2p1 192.168.0.143): NO FLAGS are set, 40 headers + 0 data bytes`
	`--- 192.168.0.143 hping statistic ---`
	`20 packets transmitted, 0 packets received, 100% packet loss`
	`round-trip min/avg/max = 0.0/0.0/0.0 ms`
	After Hping Packet Craft (USER CHAIN):
	`Chain trafficWWW (4 references)`
	`pkts bytes target prot opt in out source destination`
	`20 800 all -- * * 0.0.0.0/0 0.0.0.0/0`			