COMP 8006 Assignment 2 Testing Doc

Alex Zielinski

02/15/2018

Table of Contents

Outbound Test Cases 3

Test Case 1 (Accept Outbound HTTP) 4

Test Case 2 (Accept Outbound HTTPS) 4

Test Case 3 (Accept Outbound DNS) 5

Test Case 4 (Drop Outbound Telnet) 5

Test Case 5 (Drop Outbound SYN FIN Packets) 6

Test Case 6 (Accept Outbound ICMP) 6

Inbound Test Cases 7

Test Case 1 (Accept Inbound HTTP) 8

Test Case 2 (Accept Inbound HTTPS) 8

Test Case 3 (Accept Inbound DNS) 9

Test Case 4 (Drop Inbound Telnet) 9

Test Case 5 (Drop Inbound SYN FIN Packets) 10

Test Case 6 (Accept Inbound ICMP) 10

Test Case 7 (Drop Inbound Port 111 Traffic) 11

Test Case 8 (Drop Inbound Port 515 Traffic) 11

Test Case 9 (Drop Inbound Port 137 Traffic) 12

Test Case 10 (Drop Inbound Port 32768 Traffic) 12

Outbound Test Cases

Test Case	Test Description	Tool Used	Expected Results	Pass/Fails
1	Forward outbound HTTP (port 80) traffic	hping3	Hping3 results should be 0% packet loss with iptables logs backing this up	Pass
2	Forward outbound HTTPS (port 443) traffic	hping3	Hping3 results should be 0% packet loss with iptables logs backing this up	Pass
3	Forward outbound DNS (port 53) traffic	hping3	Hping3 results should be 0% packet loss with iptables logs backing this	Pass
4	Drop outbound telnet traffic	hping3	Hping3 results should be 100% packet loss with iptables logs backing this	Pass
5	Drop outbound SYN FIN packets	hping3	Hping3 results should be 100% packet loss with iptables logs backing this	Pass
6	Forward outbound ICMP packets	hping3	Hping3 results should be 0% packet loss with iptables logs backing this	Pass

Note: Three lab computers were used for these tests. *The **Internal Computer*** (192.168.0.9, network card enp3s2 with IP 192.168.10.1) was used to simulate a computer that existed on an internal network that was hidden from the outside. This computer was connected by a cross-over cable to the **Firewall Computer** (192.168.0.8, network card enp3s2 with IP 192.168.10.1) who only forwarded packets into and out of the internal computer. The last computer was the **External Computer** which simulated an external machine communicating with the internal computer via the firewall machine. Packets were sent from the internal computer to the external computer for outbound tests and vice versa to inbound traffic. The following iptables command was used to view logs of chains: ***iptables -L -n -v -x***.

Please refer to the design doc located in the project folder's top directory for a detailed description of how the firewall script works.

Test Case 1 (Accept Outbound HTTP)

- Ensure that outbound HTTP (port 80) traffic is permitted. Hping3 was used to send 3 TCP packets from the internal computer to the external computer with a destination port of 80. Hping3 results state 0% packet loss with the 3 transmitted packets.

```
22:22:07(-)root@localhost:~$ hping3 192.168.0.3 -p 80 -c 3 -S
HPING 192.168.0.3 (enp3s2 192.168.0.3): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.3 ttl=63 DF id=30392 sport=80 flags=RA seq=0 win=0 rtt=1.8 ms
len=46 ip=192.168.0.3 ttl=63 DF id=30777 sport=80 flags=RA seq=1 win=0 rtt=2.7 ms
len=46 ip=192.168.0.3 ttl=63 DF id=31675 sport=80 flags=RA seq=2 win=0 rtt=2.5 ms

--- 192.168.0.3 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.8/2.3/2.7 ms
```

- After the command was run the iptables log shows:

FORWARD CHAIN

```
 3      120 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
 3      120 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
```

- 3 packets were accepted in the forward chain coming from the internal machine and 3 response packets were forwarded back.

Test Case 2 (Accept Outbound HTTPS)

- Ensure that outbound HTTPS (port 443) traffic is permitted. Hping3 was used to send 3 TCP packets from the internal computer to the external computer with a destination port of 443. Hping3 results state 0% packet loss with the 3 transmitted packets.

```
22:22:14(-)root@localhost:~$ hping3 192.168.0.3 -p 443 -c 3 -S
HPING 192.168.0.3 (enp3s2 192.168.0.3): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.3 ttl=63 DF id=2555 sport=443 flags=RA seq=0 win=0 rtt=1.7 ms
len=46 ip=192.168.0.3 ttl=63 DF id=2661 sport=443 flags=RA seq=1 win=0 rtt=1.7 ms
len=46 ip=192.168.0.3 ttl=63 DF id=2685 sport=443 flags=RA seq=2 win=0 rtt=1.5 ms

--- 192.168.0.3 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.5/1.6/1.7 ms
```

- After the command was run the iptables log shows:

FORWARD CHAIN

```
 3      120 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
 3      120 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
```

- 3 packets were accepted in the forward chain coming from the internal machine and 3 response packets were forwarded back.

Test Case 3 (Accept Outbound DNS)

- Ensure that outbound DNS (port 53) traffic is permitted. Hping3 was used to send UDP 3 packets from the internal computer to the external computer with a destination port of 53. Hping3 results state 0% packet loss with the 3 transmitted packets.

```
22:26:27(-)root@localhost:~$ hping3 192.168.0.3 -p 53 -c 3 -2
HPING 192.168.0.3 (enp3s2 192.168.0.3): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.0.3 name=UNKNOWN
ICMP Port Unreachable from ip=192.168.0.3 name=UNKNOWN
ICMP Port Unreachable from ip=192.168.0.3 name=UNKNOWN

--- 192.168.0.3 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

- After the command was run the iptables log shows:

FORWARD CHAIN

```
  3      168 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
  0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
  0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
  3       84 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0
```

- 3 packets were accepted in the forward chain coming from the internal machine and 3 response packets were forwarded back.

Test Case 4 (Drop Outbound Telnet)

- Ensure that outbound telnet (port 23) traffic is dropped. Hping3 was used to send 3 TCP packets from the internal computer to the external computer with a destination port of 23. Hping3 results state 100% packet loss with the 3 transmitted packets.

```
22:26:53(-)root@localhost:~$ hping3 192.168.0.3 -p 23 -c 3 -S
HPING 192.168.0.3 (enp3s2 192.168.0.3): S set, 40 headers + 0 data bytes

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

- After the command was run the iptables log shows:

FORWARD CHAIN

```
0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:23
3      120 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:23
```

- 3 packets were dropped in the forward chain coming from the internal machine.

Test Case 5 (Drop Outbound SYN FIN Packets)

- Ensure that outbound SYN FIN packets are dropped. Hping3 was used to send 3 TCP packets from the internal computer to the external computer with a destination port of 80. Hping3 results state 100% packet loss with the 3 transmitted packets.

```
22:30:50(-)root@localhost:~$ hping3 192.168.0.3 -p 80 -c 3 -SF
HPING 192.168.0.3 (enp3s2 192.168.0.3): SF set, 40 headers + 0 data bytes

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

- After the command was run the iptables log shows:

FORWARD CHAIN

```
 3      120 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
 0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
```

- 3 packets were dropped in the forward chain coming from the internal machine.

Test Case 6 (Accept Outbound ICMP)

- Ensure that outbound ICMP is permitted. Hping3 was used to send 3 ICMP packets from the internal computer to the external computer. Hping3 results state 0% packet loss with the 3 transmitted packets.

```
22:33:37(-)root@localhost:~$ hping3 192.168.0.3 -1 -c 3
HPING 192.168.0.3 (enp3s2 192.168.0.3): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.3 ttl=63 id=46674 icmp_seq=0 rtt=2.7 ms
len=46 ip=192.168.0.3 ttl=63 id=46838 icmp_seq=1 rtt=2.6 ms
len=46 ip=192.168.0.3 ttl=63 id=46865 icmp_seq=2 rtt=2.3 ms

--- 192.168.0.3 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.3/2.5/2.7 ms
```

- After the command was run the iptables log shows:

FORWARD CHAIN

```
5      140 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
1       28 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
```

- The ICMP packets coming from the internal computer were accepted as well as the ICMP responses.

Inbound Test Cases

Test Case	Test Description	Tool Used	Expected Results	Pass/Fails
1	Forward inbound HTTP (port 80) traffic	hping3	Hping3 results should be 0% packet loss with iptables logs backing this up	Pass
2	Forward inbound HTTPS (port 443) traffic	hping3	Hping3 results should be 0% packet loss with iptables logs backing this up	Pass
3	Forward inbound DNS (port 53) traffic	hping3	Hping3 results should be 0% packet loss with iptables logs backing this	Pass
4	Drop inbound telnet traffic	hping3	Hping3 results should be 100% packet loss with iptables logs backing this	Pass
5	Drop inbound SYN FIN packets	hping3	Hping3 results should be 100% packet loss with iptables logs backing this	Pass
6	Forward inbound ICMP packets	hping3	Hping3 results should be 0% packet loss with iptables logs backing this	Pass
7	Drop port 111 traffic	hping3	Hping3 results should be 100% packet loss with iptables logs backing this	Pass
8	Drop port 515 traffic	hping3	Hping3 results should be 100% packet loss with iptables logs backing this	Pass
9	Drop port 137 traffic	hping3	Hping3 results should be 100% packet loss with iptables logs backing this	Pass
10	Drop port 32768 traffic	hping3	Hping3 results should be 100% packet loss with iptables logs backing this	Pass

Test Case 1 (Accept Inbound HTTP)

- Ensure that inbound HTTP (port 80) traffic is permitted. Hping3 was used to send 3 TCP packets from the external computer to the internal computer with a destination port of 80. Hping3 results state 0% packet loss with the 3 transmitted packets.

```
22:37:57(-)root@datacomm-03:Documents$ hping3 192.168.0.8 -p 80 -c 3 -S
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.8 ttl=62 DF id=5815 sport=80 flags=RA seq=0 win=0 rtt=1.8 ms
len=46 ip=192.168.0.8 ttl=62 DF id=5869 sport=80 flags=RA seq=1 win=0 rtt=1.7 ms
len=46 ip=192.168.0.8 ttl=62 DF id=5937 sport=80 flags=RA seq=2 win=0 rtt=1.6 ms

--- 192.168.0.8 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.6/1.7/1.8 ms
```

- After the command was run the iptables log shows:

FORWARD CHAIN

```
3      120 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
3      120 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
```

- 3 packets were accepted in the forward chain coming from the external machine and 3 response packets were forwarded back.

Test Case 2 (Accept Inbound HTTPS)

- Ensure that inbound HTTPS (port 443) traffic is permitted. Hping3 was used to send 3 TCP packets from the external computer to the internal computer with a destination port of 443. Hping3 results state 0% packet loss with the 3 transmitted packets.

```
22:38:44(-)root@datacomm-03:Documents$ hping3 192.168.0.8 -p 443 -c 3 -S
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.8 ttl=62 DF id=47347 sport=443 flags=RA seq=0 win=0 rtt=1.7 ms
len=46 ip=192.168.0.8 ttl=62 DF id=47992 sport=443 flags=RA seq=1 win=0 rtt=1.6 ms
len=46 ip=192.168.0.8 ttl=62 DF id=48193 sport=443 flags=RA seq=2 win=0 rtt=2.4 ms

--- 192.168.0.8 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.6/1.9/2.4 ms
```

- After the command was run the iptables log shows:

FORWARD CHAIN

```
3      120 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
3      120 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
```

- 3 packets were accepted in the forward chain coming from the external machine and 3 response packets were forwarded back.

Test Case 3 (Accept Inbound DNS)

- Ensure that inbound DNS (port 53) traffic is permitted. Hping3 was used to send 3 UDP packets from the external computer to the internal computer with a destination port of 53. Hping3 results state 0% packet loss with the 3 transmitted packets.

```
22:39:51(-)root@datacomm-03:Documents$ hping3 192.168.0.8 -p 53 -c 3 -2
HPING 192.168.0.8 (eno1 192.168.0.8): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.0.8 name=UNKNOWN
ICMP Port Unreachable from ip=192.168.0.8 name=UNKNOWN
ICMP Port Unreachable from ip=192.168.0.8 name=UNKNOWN

--- 192.168.0.8 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

- After the command was run the iptables log shows:

FORWARD CHAIN

```
3      168 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
3       84 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0
```

- 3 packets were accepted in the forward chain coming from the external machine and 3 response packets were forwarded back.

Test Case 4 (Drop Inbound Telnet)

- Ensure that inbound telnet (port 23) traffic is dropped. Hping3 was used to send 3 TCP packets from the external computer to the internal computer with a destination port of 23. Hping3 results state 100% packet loss with the 3 transmitted packets.

```
22:41:41(-)root@datacomm-03:Documents$ hping3 192.168.0.8 -p 23 -c 3 -S
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes

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

- After the command was run the iptables log shows:

FORWARD CHAIN

```
3      120 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
```

- 3 packets were dropped in the forward chain coming from the external machine.

Test Case 5 (Drop Inbound SYN FIN Packets)

- Ensure that inbound SYN FIN packets are dropped. Hping3 was used to send 3 TCP packets from the external computer to the internal computer with a destination port of 80. Hping3 results state 100% packet loss with the 3 transmitted packets.

```
22:43:03(-)root@datacomm-03:Documents$ hping3 192.168.0.8 -p 80 -c 3 -SF
HPING 192.168.0.8 (eno1 192.168.0.8): SF set, 40 headers + 0 data bytes

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

- After the command was run the iptables log shows:

FORWARD CHAIN

```
 3      120 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
 0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
```

- 3 packets were dropped in the forward chain coming from the external machine.

Test Case 6 (Accept Inbound ICMP)

- Ensure that inbound ICMP is permitted. Hping3 was used to send 3 ICMP packets from the external computer to the internal computer. Hping3 results state 0% packet loss with the 3 transmitted packets.

```
22:43:20(-)root@datacomm-03:Documents$ hping3 192.168.0.8 -1 -c 3
HPING 192.168.0.8 (eno1 192.168.0.8): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.8 ttl=62 id=63656 icmp_seq=0 rtt=1.8 ms
len=46 ip=192.168.0.8 ttl=62 id=64010 icmp_seq=1 rtt=1.7 ms
len=46 ip=192.168.0.8 ttl=62 id=64129 icmp_seq=2 rtt=1.5 ms

--- 192.168.0.8 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.5/1.7/1.8 ms
```

- After the command was run the iptables log shows:

FORWARD CHAIN

```
3       84 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
0        0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
1       28 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
```

- The ICMP packets coming from the external computer were accepted as well as the ICMP responses.

Test Case 7 (Drop Inbound Port 111 Traffic)

- Ensure that inbound packets to port 111 are dropped. Hping3 was used to send 3 TCP packets from the external computer to the internal computer with a destination port of 111. Hping3 results state 100% packet loss with the 3 transmitted packets.

```
22:46:14(-)root@datacomm-03:Documents$ hping3 192.168.0.8 -p 111 -c 3 -S
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes

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

- After the command was run the iptables log shows:

FORWARD CHAIN

```
3      120 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport dports 111,515
```

- 3 packets were dropped in the forward chain coming from the external machine.

Test Case 8 (Drop Inbound Port 515 Traffic)

- Ensure that inbound packets to port 515 are dropped. Hping3 was used to send 3 TCP packets from the external computer to the internal computer with a destination port of 515. Hping3 results state 100% packet loss with the 3 transmitted packets.

```
22:47:06(-)root@datacomm-03:Documents$ hping3 192.168.0.8 -p 515 -c 3 -S
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes

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

- After the command was run the iptables log shows:

FORWARD CHAIN

```
3      120 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport dports 111,515
```

- 3 packets were dropped in the forward chain coming from the external machine.

Test Case 9 (Drop Inbound Port 137 Traffic)

- Ensure that inbound packets to port 137 are dropped. Hping3 was used to send 3 TCP packets from the external computer to the internal computer with a destination port of 137. Hping3 results state 100% packet loss with the 3 transmitted packets.

```
22:47:57(-)root@datacomm-03:Documents$ hping3 192.168.0.8 -p 137 -c 3 -S
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes

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

- After the command was run the iptables log shows:

FORWARD CHAIN

```
    3      120 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpts:137:139
```

- 3 packets were dropped in the forward chain coming from the external machine.

Test Case 10 (Drop Inbound Port 32768 Traffic)

- Ensure that inbound packets to port 32768 are dropped. Hping3 was used to send 3 TCP packets from the external computer to the internal computer with a destination port of 32768. Hping3 results state 100% packet loss with the 3 transmitted packets.

```
22:48:45(-)root@datacomm-03:Documents$ hping3 192.168.0.8 -p 32768 -c 3 -S
HPING 192.168.0.8 (eno1 192.168.0.8): S set, 40 headers + 0 data bytes

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

- After the command was run the iptables log shows:

FORWARD CHAIN

```
3      120 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpts:32768:32775
```

- 3 packets were dropped in the forward chain coming from the external machine.