

8006 Asn2 - Testing

So you want to pass the firewall eh?

Isaac Morneau; A00958405

John Agapeyev; A00928238

8006 Asn2 - Testing	1
Setup of client	3
Step 1	3
Setup of firewall	3
Step 1	3
Step 2	3
Expected result	3
Cleanup	4
Step 1	4
Test inbound traffic	4
Step 1	4
Step 2	4
Expected result	4
Test outbound traffic	5
Step 1	5
Expected result	5

Setup of client

Step 1

On the client machine run `./client.sh`

Setup of firewall

Step 1

On the firewall machine run `./firewall.sh`

Step 2

On the firewall machine run `./run.sh`

Expected result

```
15:49:42(master)root@datacomm-15:scripts$ ./firewall.sh && ./run.sh
Enabling interface enp3s2
Setting IP 192.168.1.1/255.255.255.0
SIOCADDRT: File exists
Clearing existing tables
Creating user tables
Setting default policy to DROP
Setting accounting rules
Setting NAT forwarding rules
Drop all telnet
Block outgoing tcp traffic to listed ports
Drop SYN-FIN packets
Drop incoming packets coming from outside with source of the inside
Allowing fragments
Set TOS for ftp and ssh
Loading the configs
Setting ACCEPT for TCP port 20
Setting ACCEPT for TCP port 21
Setting ACCEPT for TCP port 22
Setting ACCEPT for TCP port 80
Setting ACCEPT for TCP port 443
Setting ACCEPT for UDP port 20
Setting ACCEPT for UDP port 21
Setting ACCEPT for UDP port 22
Setting ACCEPT for UDP port 53
15:49:48(master)root@datacomm-15:scripts$
```

Cleanup

Step 1

To disable the rules on either machine run `./cleanup.sh`

Test inbound traffic

Step 1

On a machine outside the network the client machine run `./inbound_test.sh`

Step 2

Follow the prompts and enter the IPs as directed

Expected result

```
16:26:57(master)root@datacomm-16:tests$ ./inbound_test.sh
Enter firewall IP: 192.168.0.15
Enter host IP: 192.168.1.5
Blocked Ports 32768-32775,137-139,111,515 test
Test passed
Allowed TCP test
Test passed
Blocked UDP test
Test passed
Allowed UDP test
Test passed
Blocked SynFin test
Test passed
Blocked Telnet test
Test passed
Blocked Internal Destination test
Test passed
Blocked Internal Source test
Test passed
16:27:33(master)root@datacomm-16:tests$
```

Test outbound traffic

Step 1

On the client machine run `./outbound_test.sh`

Expected result

On the client

```
16:02:19(master)root@datacomm-14:8006-asn2$ ./tests/outbound_test.sh
Fragment test
Test passed
DNS test
Test passed
SYN/FIN test
Test passed
Telnet test
Test passed
Ports 32768-32775 test
Test passed
Port 137-139 test
Test passed
Port 111 test
Test passed
Port 515 test
Test passed
Orphan SYN/ACK test
Test passed
Christmas test
Test passed
```

On the firewall

```
16:04:24(master)root@datacomm-15:scripts$ iptables -L -nxv
Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts      bytes target     prot opt in     out     source            destination
Chain FORWARD (policy DROP 17 packets, 664 bytes)
  pkts      bytes target     prot opt in     out     source            destination
  146      33911 XxKr0n05Xx420blazeit all  --  enp3s2 eno1    0.0.0.0/0        0.0.0.0/0
   80      44412 XxKr0n05Xx420blazeit all  --  eno1    enp3s2  0.0.0.0/0        0.0.0.0/0
Chain OUTPUT (policy DROP 10 packets, 778 bytes)
Chain XxKr0n05Xx420blazeit (2 references)
  pkts      bytes target     prot opt in     out     source            destination
   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
  16       704 DROP      tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp dpts:32768:32775
   6       264 DROP      tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp dpts:137:139
   3       120 DROP      tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp dpt:111
   3       120 DROP      tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp dpt:515
   6       240 DROP      tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp flags:0x03/0x03
   0         0 DROP      all  --  eno1    *      192.168.1.0/24   0.0.0.0/0
   0         0 ACCEPT    all  -f  *      *      0.0.0.0/0        0.0.0.0/0
   0         0 ACCEPT    tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp spt:20 state NEW,ESTABLISHED
   0         0 ACCEPT    tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp dpt:20 state NEW,ESTABLISHED
   0         0 ACCEPT    tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp spt:21 state NEW,ESTABLISHED
   0         0 ACCEPT    tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp dpt:21 state NEW,ESTABLISHED
   0         0 ACCEPT    tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp spt:22 state NEW,ESTABLISHED
   0         0 ACCEPT    tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp dpt:22 state NEW,ESTABLISHED
   6       683 ACCEPT    tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp spt:80 state NEW,ESTABLISHED
   9       776 ACCEPT    tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp dpt:80 state NEW,ESTABLISHED
  64     42971 ACCEPT    tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp spt:443 state NEW,ESTABLISHED
  79     30601 ACCEPT    tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp dpt:443 state NEW,ESTABLISHED
   0         0 ACCEPT    tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp spt:53 state NEW,ESTABLISHED
   0         0 ACCEPT    tcp  --  *      *      0.0.0.0/0        0.0.0.0/0        tcp dpt:53 state NEW,ESTABLISHED
   0         0 ACCEPT    udp  --  *      *      0.0.0.0/0        0.0.0.0/0        udp spt:20 state NEW,ESTABLISHED
   0         0 ACCEPT    udp  --  *      *      0.0.0.0/0        0.0.0.0/0        udp dpt:20 state NEW,ESTABLISHED
   0         0 ACCEPT    udp  --  *      *      0.0.0.0/0        0.0.0.0/0        udp spt:21 state NEW,ESTABLISHED
   0         0 ACCEPT    udp  --  *      *      0.0.0.0/0        0.0.0.0/0        udp dpt:21 state NEW,ESTABLISHED
   0         0 ACCEPT    udp  --  *      *      0.0.0.0/0        0.0.0.0/0        udp spt:22 state NEW,ESTABLISHED
   2        56 ACCEPT    udp  --  *      *      0.0.0.0/0        0.0.0.0/0        udp dpt:22 state NEW,ESTABLISHED
   6       646 ACCEPT    udp  --  *      *      0.0.0.0/0        0.0.0.0/0        udp spt:53 state NEW,ESTABLISHED
   6       358 ACCEPT    udp  --  *      *      0.0.0.0/0        0.0.0.0/0        udp dpt:53 state NEW,ESTABLISHED
```