

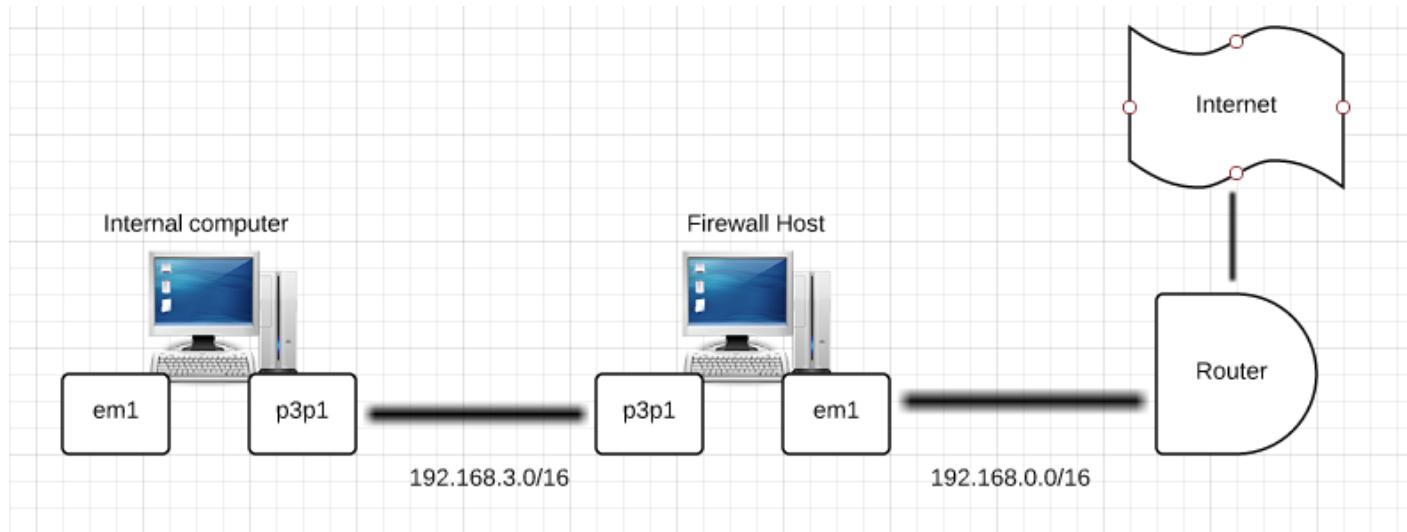
# COMP 8008 Assignment 2

Standalone Linux Firewall and Packet filter  
Chris Wood A00741285

## Firewall requirements

- Allow inbound and outbound user defined TCP ports
- Allow inbound and outbound user defined UDP ports
- Allow inbound and outbound user defined ICMP types
- Drop packets coming in to the firewall host from outside
- Drop packets with source address from internal machine coming from outside
- Drop connections coming the from way (inbound SYN to high ports)
- Accept fragments
- Allow all allowed TCP ports for existing connections
- Drop packets with SYN FIN bits set
- Drop telnet packets
- Drop external traffic to ports 32768:32775, 137:139, TCP ports 111 and 515
- Set FTP and SSH packets to Minimum Delay and Maximum Throughput
- Drop all other packets

## Configuration



## **Files**

fw -- file wall script, this can be configured for user defined variables for what is allowed and what is blocked

revert -- script to remove all rules, chains in default, nat and mangle tables

## **Testing**

The following test cases were used to test the requirements parameters of the firewall.

<b>Test Parameters</b>	Inbound/Outbound TCP/UDP/ICMP packets on allowed ports
<b>Test</b>	Allow port 80 and 443 and test internal computer for webpage
<b>Expected Results</b>	Can view webpages, also would confirm DNS working
<b>Command</b>	n/a. Using GUI
<b>Actual Results</b>	Able to browse webpage from internal machine

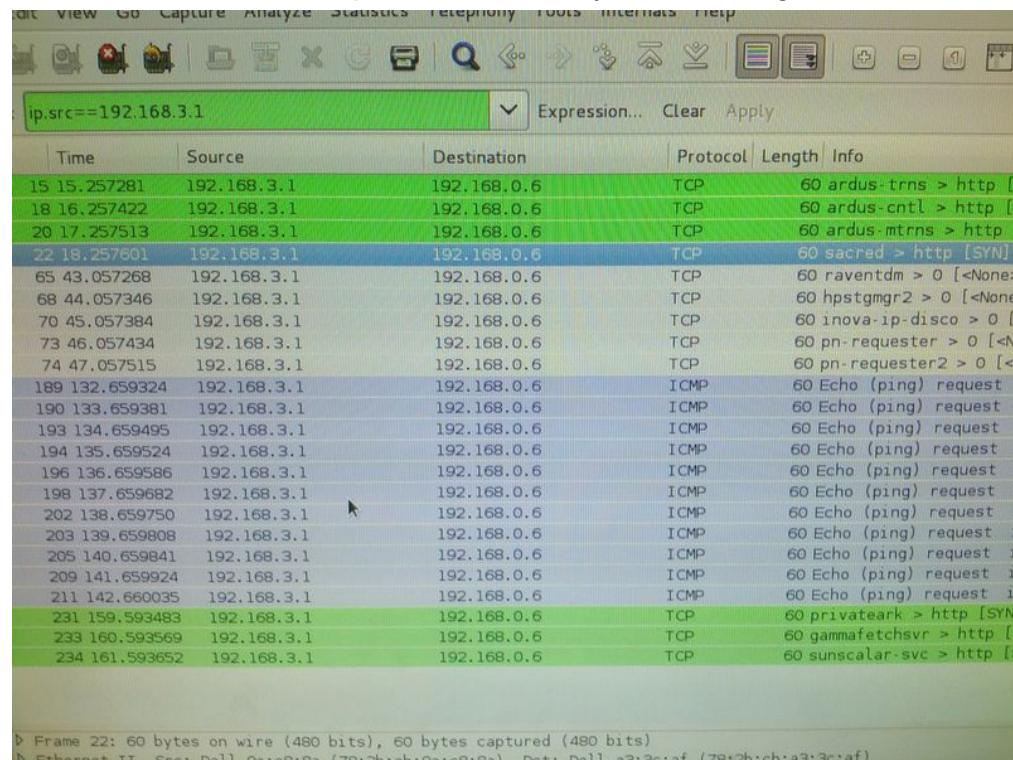
<b>Test Parameters</b>	Inbound/Outbound TCP/UDP/ICMP packets on allowed ports
<b>Test</b>	Allow port 22 test external computer for ssh connection to internal computer (not firewall host)
<b>Expected Results</b>	ssh connection successful to internal host
<b>Command</b>	ssh root@firewallHostIPAddr
<b>Actual Results</b>	ssh connection successful. ifconfig confirmed internal.

```
root@DataComm:~ 
File Edit View Search Terminal Help
Connection to 192.168.0.6 closed.
[root@DataComm ~]# ifconfig em1
em1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.0.7 netmask 255.255.255.0 broadcast 192.168.0.255
                inet6 fe80::7a2b:cbff:fe9e:c88a prefixlen 64 scopeid 0x20<link>
                      ether 78:2b:cb:9e:c8:8a txqueuelen 1000 (Ethernet)
                        RX packets 195737 bytes 186384439 (177.7 MiB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 121229 bytes 17492046 (16.6 MiB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
                        TX queueing discipline qdisc mq
                        device interrupt 20 memory 0xe1b00000-e1b20000
                        r�asal x86_64 0:0:9_28_1.fc17
[root@DataComm ~]# ssh 192.168.0.6
root@192.168.0.6's password: 
Last login: Fri Feb  8 19:07:53 2013 from 192.168.0.7
[root@DataComm ~]# ifconfig p3p1
p3p1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.3.1 netmask 255.255.255.0 broadcast 192.168.3.255
                inet6 fe80::20e:cff:fe51:2fa4 prefixlen 64 scopeid 0x20<link>
                      ether 00:0e:0c:51:2f:a4 txqueuelen 1000 (Ethernet)
                        RX packets 229377 bytes 304746059 (290.6 MiB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 138507 bytes 11766987 (11.2 MiB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
                        TX queueing discipline qdisc mq
                        device interrupt 19 memory 0xf000000-f0020000
                        Dependency Updated:
[root@DataComm ~]# ifstat em1
#kernel
Interface    RX Pkts/Rate    TX Pkts/Rate    RX Data/Rate    TX Data/Rate
#          RX Errs/Drop    TX Errs/Drop    RX Over/Rate    TX Coll/Rate
em1      Expected 20441 0ts    ssh.com9016 0 access 6824K 0ust    1725K 0
                    0 0           0 0           0 0           0 0
[root@DataComm ~]# ifdown em1 ssh root@firewallHostIPAddr
Error: Device 'em1' (/org/freedesktop/NetworkManager/Devices/0) disconnecting failed: This device is not active
[root@DataComm ~]#
```

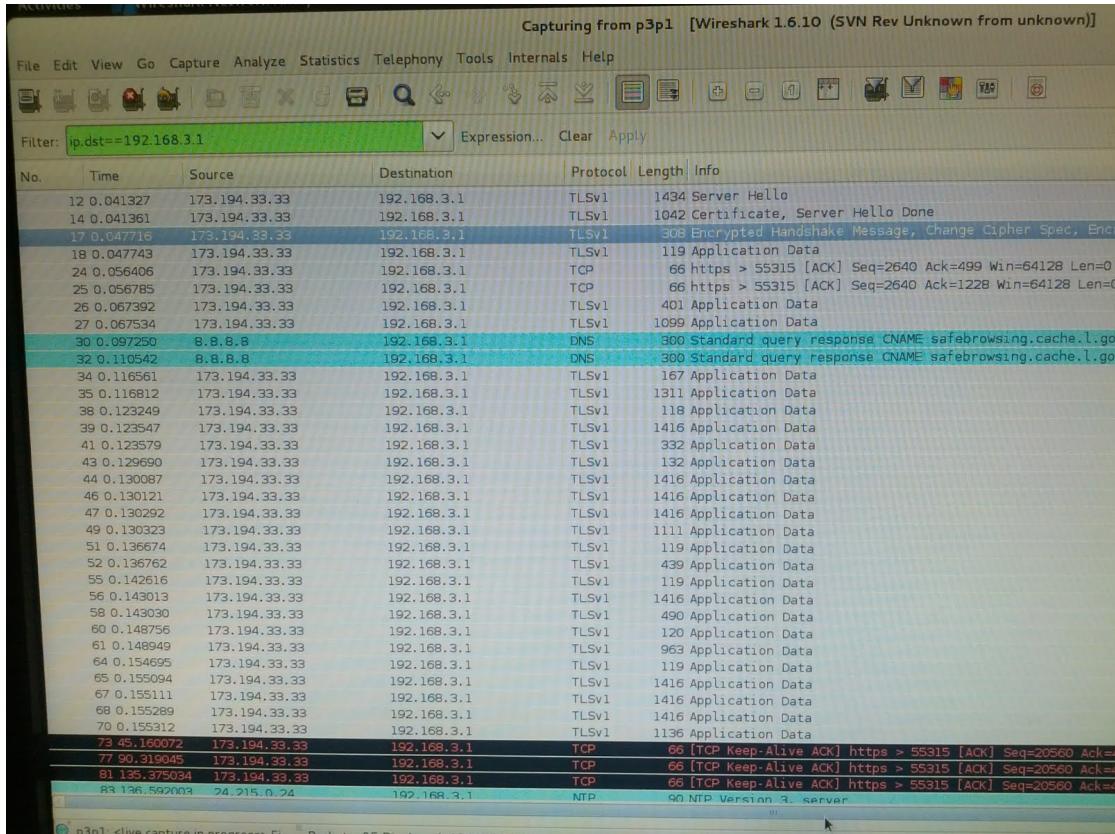
<b>Test Parameters</b>	Do not accept any packets with a source address from the outside matching your internal network
<b>Test</b>	Craft spoofed packets from Hping3
<b>Expected Results</b>	Packet
<b>Command</b>	hping3 192.168.0.6 -a 192.168.3.1 -S -p 80 hping3 192.168.0.6 -a 192.168.3.1 --icmp
<b>Actual Results</b>	Packets dropped by firewall and not received by internal host. See below.

```
[root@DataComm ~]# hping3 192.168.0.6 -a 192.168.3.1 --icmp
HPING 192.168.0.6 (em1 192.168.0.6): icmp mode set, 28 headers + 0 data bytes
^C
--- 192.168.0.6 hping statistic ---
11 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@DataComm ~]# hping3 192.168.0.6 -a 192.168.3.1 -S -p 80
HPING 192.168.0.6 (em1 192.168.0.6): S set, 40 headers + 0 data bytes
^C
--- 192.168.0.6 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Commands above; 100% packet loss as they are not being directed back to us.



Firewall wireshark above, receive packets at the interface level



Internal wireshark above. No packets from above are being received. Packets are being dropped at the firewall as expected.

<b>Test Parameters</b>	You must ensure the you reject those connections that are coming the “wrong” way (i.e., inbound SYN packets to high ports).
<b>Test</b>	Crafted SYN packets to high ports
<b>Expected Results</b>	Packets dropped
<b>Command</b>	hping3 192.168.0.6 -S -p 65555 hping3 192.168.0.6 -S -p 2065
<b>Actual Results</b>	3 packets transmitted, 0 packets received, 100% packet loss 5 packets transmitted, 0 packets received, 100% packet loss

<b>Test Parameters</b>	Drop all TCP packets with the SYN and FIN bit set.
<b>Test</b>	Crafted SYN FIN packets
<b>Expected Results</b>	Packets dropped
<b>Command</b>	<pre>hping3 192.168.0.6 -S -F -p 80 -c 3 hping3 192.168.0.6 -S -F -p 22 -c 5</pre>
<b>Actual Results</b>	<p>3 packets transmitted, 0 packets received, 100% packet loss        5 packets transmitted, 0 packets received, 100% packet loss</p>

<b>Test Parameters</b>	Block all external traffic directed to ports 32768 – 32775, 137 – 139, TCP ports 111 and 515.
<b>Test</b>	Crafted packets to ports within range
<b>Expected Results</b>	Packets dropped
<b>Command</b>	<pre>hping3 192.168.0.6 -S -p 32769 -c 1 hping3 192.168.0.6 -S -p 138 -c 3 hping3 192.168.0.6 -S -p 111 -c 5 hping3 192.168.0.6 -S -p 515 -c 7</pre>
<b>Actual Results</b>	<p>1 packets transmitted, 0 packets received, 100% packet loss        3 packets transmitted, 0 packets received, 100% packet loss        5 packets transmitted, 0 packets received, 100% packet loss        7 packets transmitted, 0 packets received, 100% packet loss</p>

<b>Test Parameters</b>	For FTP and SSH services, set control connections to "Minimum Delay" and FTP data to "Maximum Throughput".
<b>Test</b>	Use protocol that has been set to be mangled and view mangle table
<b>Expected Results</b>	Specific packets in mangle table
<b>Command</b>	Connected with SSH
<b>Actual Results</b>	Packets viewed in mangle table

```
[root@DataComm comp8006-assign2]# iptables -t mangle -L -v
Chain PREROUTING (policy ACCEPT 66 packets, 5778 bytes)
pkts bytes target     prot opt in     out     source               destination
      8  560 TOS          tcp  --  any    any    anywhere             anywhere
multiport dports ssh,ftp,ftp-data TOS setMinimize-Delay
      5  868 TOS          tcp  --  any    any    anywhere             anywhere
multiport sports ssh,ftp,ftp-data TOS setMinimize-Delay
      8  560 TOS          tcp  --  any    any    anywhere             anywhere
multiport dports ssh,ftp,ftp-data TOS setMaximize-Throughput
      5  868 TOS          tcp  --  any    any    anywhere             anywhere
multiport sports ssh,ftp,ftp-data TOS setMaximize-Throughput
```

<b>Test Parameters</b>	Do not allow Telnet packets at all.
<b>Test</b>	Crafted packets to port 23
<b>Expected Results</b>	Packets dropped
<b>Command</b>	hping3 192.168.0.6 -S -p 23 -c 3
<b>Actual Results</b>	3 packets transmitted, 0 packets received, 100% packet loss

<b>Test Parameters</b>	Accept fragments.
<b>Test</b>	Crafted fragmented packets to accepted port
<b>Expected Results</b>	0% packet loss
<b>Command</b>	hping3 192.168.0.6 -S -f -p 22 -c 5
<b>Actual Results</b>	5 packets transmitted, 5 packets received, 0% packet loss