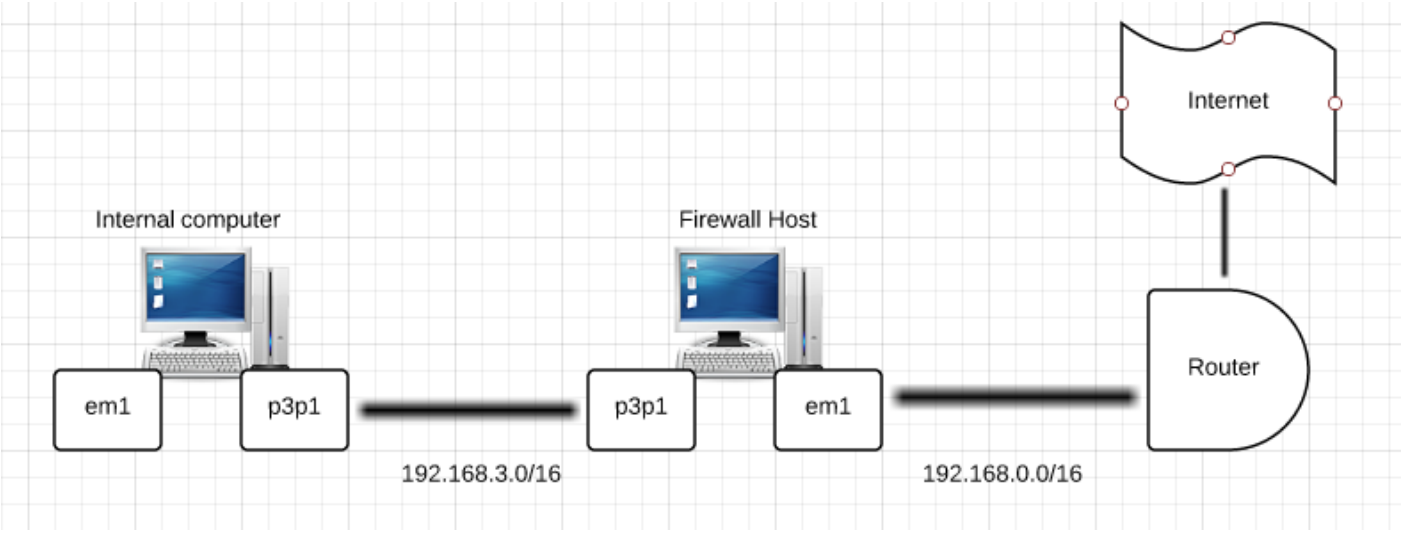
COMP 8008 Assignment 2

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

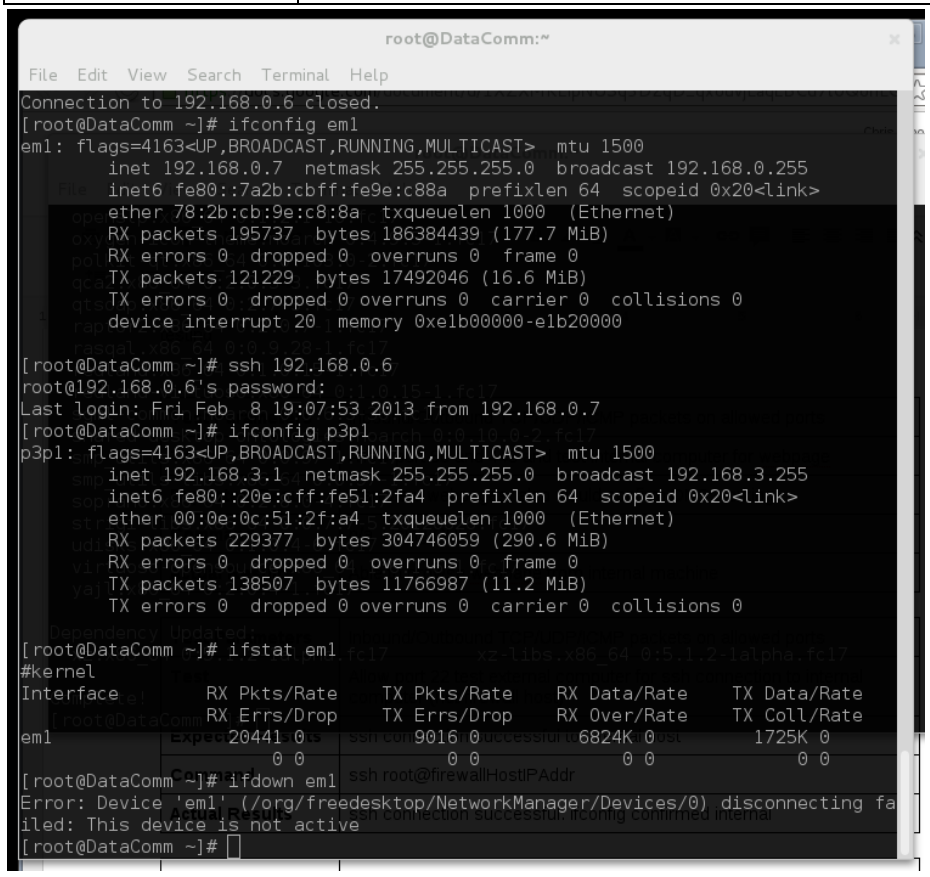
revert -- script to remove all rules, chains in default, nat and mangle tables

Testing

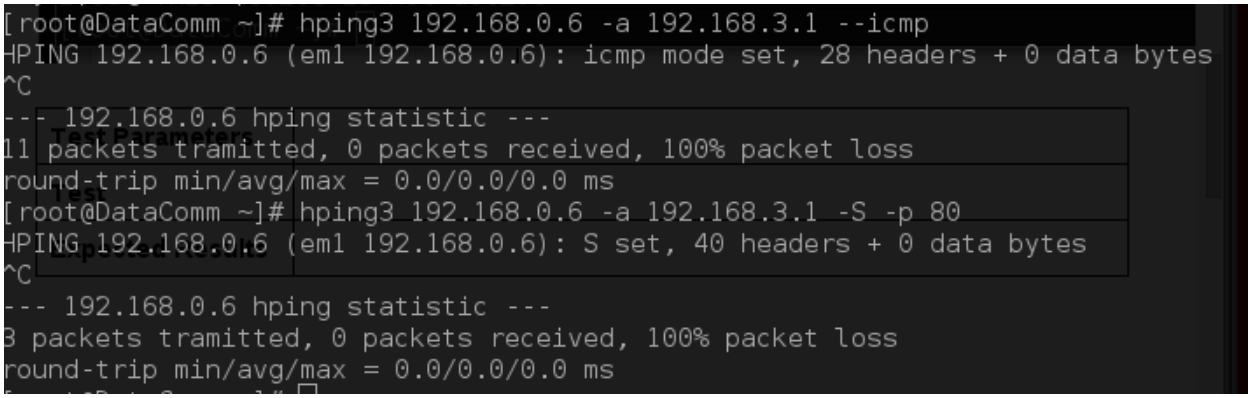
The following test cases were used to test the requirements parameters of the firewall.

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

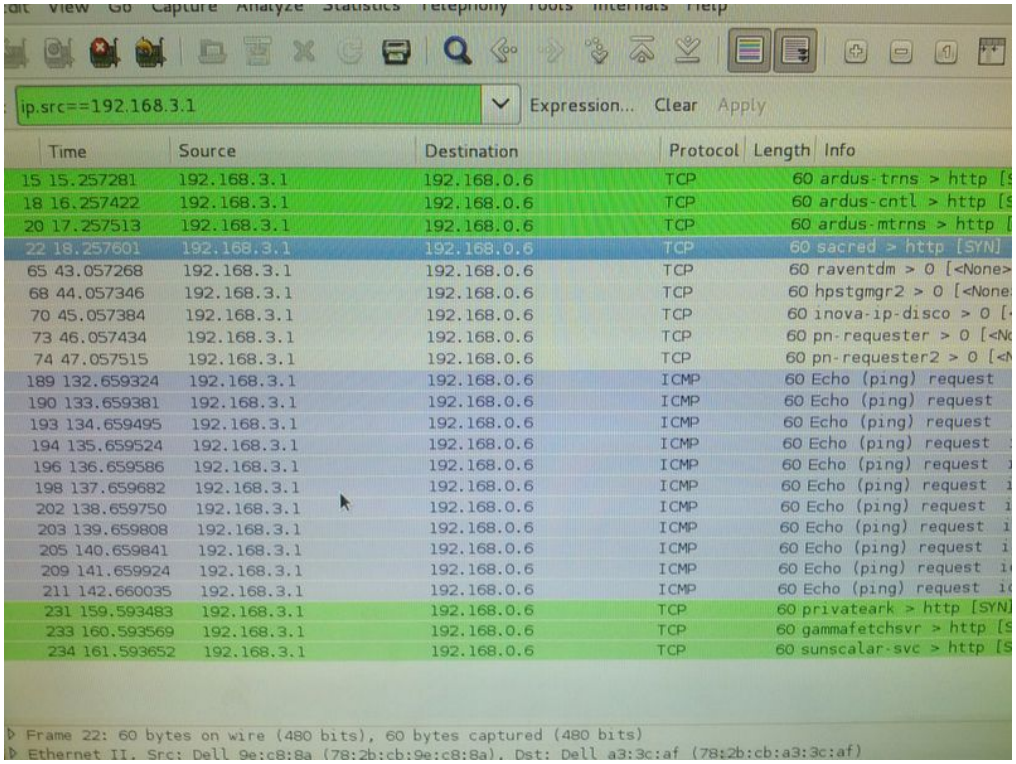
Test Parameters	Inbound/Outbound TCP/UDP/ICMP packets on allowed ports
Test	Allow port 22 test external computer for ssh connection to internal computer (not firewall host)
Expected Results	ssh connection successful to internal host
Command	ssh root@firewallHostIPAddr
Actual Results	ssh connection successful.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



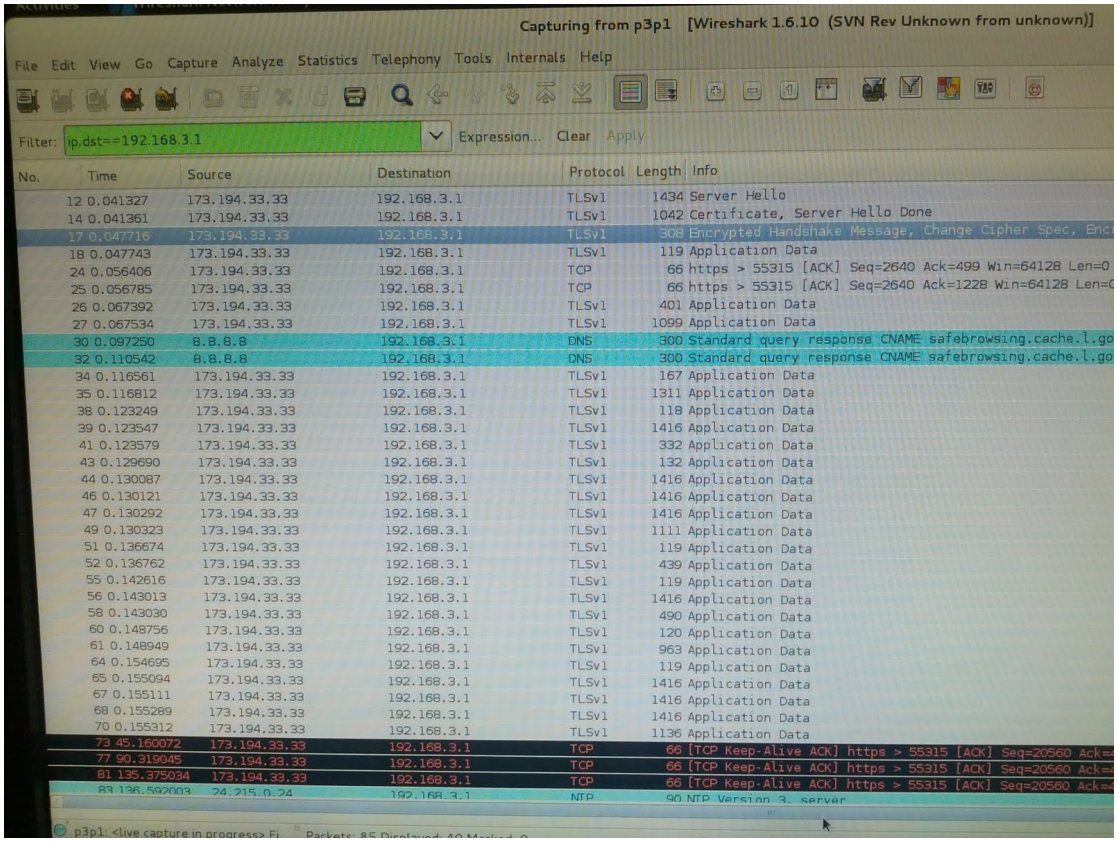
Test Parameters	Do not accept any packets with a source address from the outside matching your internal network
Test	Craft spoofed packets from Hping3
Expected Results	Packet
Command	hping3 192.168.0.6 -a 192.168.3.1 -S -p 80 hping3 192.168.0.6 -a 192.168.3.1 --icmp
Actual Results	Packets dropped by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



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.

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

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

Test Parameters	Block all external traffic directed to ports 32768 – 32775, 137 – 139, TCP ports 111 and 515.
Test	Crafted packets to ports within range
Expected Results	Packets dropped
Command	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
Actual Results	1 packets tramitted, 0 packets received, 100% packet loss 3 packets tramitted, 0 packets received, 100% packet loss 5 packets tramitted, 0 packets received, 100% packet loss 7 packets tramitted, 0 packets received, 100% packet loss

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

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

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