Comp 8006 Assignment 2

Mat Siwoski

Shane Spoor

# Notes:

### Running the application:

To run the application, navigate to the folder that the script was installed to and type:

**sudo ./config.sh**

In the event that the scrip does not run:

**chmod +x config.sh**

**chmod +x fw.sh**

to ensure that the script can be executed.

### Requirements:

The firewall had to follow the following requirements:

* Set the initial default policies.
* Design a test procedure that will test all your firewall rules and print the results of the test to a file. Make sure that someone reading the file contents will know exactly which rule worked and which rule failed.

# Firewall Rules:

These are the following rules that are followed by the Firewall:

* Get user specified parameters (see constraints) and create a set of rules that will implement the firewall requirements. Specifically the firewall will control:
  + Inbound/Outbound TCP packets on allowed ports.
  + Inbound/Outbound UDP packets on allowed ports.
  + Inbound/Outbound ICMP packets based on type numbers.
  + All packets that fall through to the default rule will be dropped.
  + Drop all packets destined for the firewall host from the outside.
  + Do not accept any packets with a source address from the outside matching your internal network.
  + You must ensure the you reject those connections that are coming the “wrong” way (i.e., inbound SYN packets to high ports).
  + Accept fragments.
  + Accept all TCP packets that belong to an existing connection (on allowed ports).
  + Drop all TCP packets with the SYN and FIN bit set.
  + Do not allow Telnet packets at all.
  + Block all external traffic directed to ports 32768 – 32775, 137 – 139, TCP ports 111 and 515.
  + For FTP and SSH services, set control connections to "Minimum Delay" and FTP data to "Maximum Throughput".

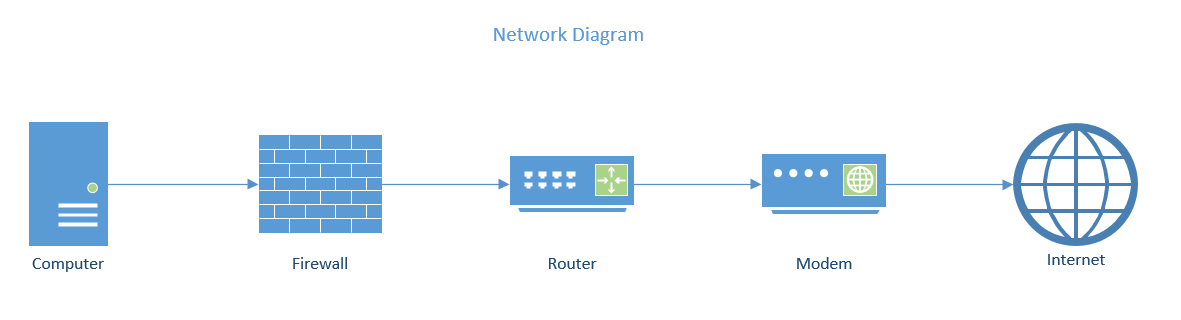
### Common Incoming packets

Common incoming malformed packets should also be set to DROP.

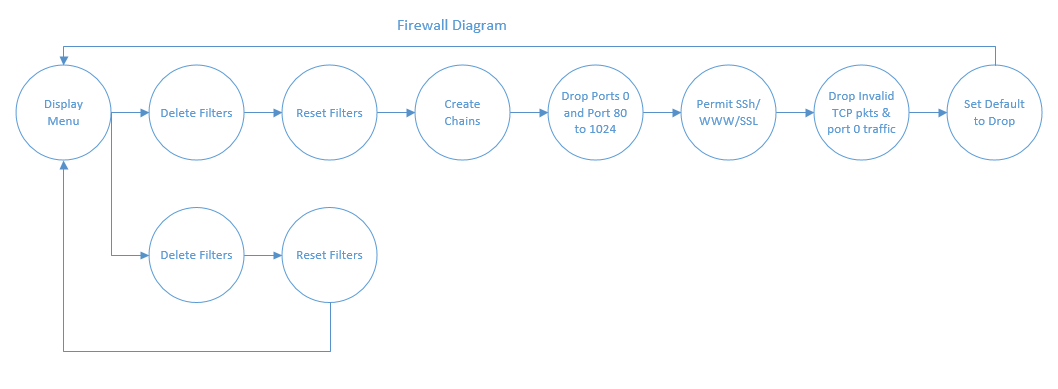
* All flags set
* No flags set
* Only URG flag set
* SYN FIN flags set
* SYN RST flags set
* SYN FIN PSH flags set
* SYN FIN RST PSH flags set
* Only FIN flag set
* FIN URG PSH flags set
* Incoming SYN packets

# Design:

### Network:



### Firewall:



# Test Results:

### Test #1: TCP

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing TCP Packets on Allowed Port 22 | hping3 $EXTERNAL\_IP -c 5 -S -p 22 | Received 5 packets | 5 packets received, 0% packet loss |

Screenshot:

### Test #2: TCP

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing TCP Packets on Allowed Port 80 | hping3 $EXTERNAL\_IP -c 5 -S -p 80 | Received 5 packets | 5 packets received, 0% packet loss |

Screenshot:

### Test #3: TCP

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing TCP Packets on Allowed Port 443 | hping3 $EXTERNAL\_IP -c 5 -S -p 443 | Received 5 packets | 5 packets received, 0% packet loss |

Screenshot:

### Test #4: TCP

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing TCP Packets on Unallowed Port 111 | hping3 $EXTERNAL\_IP -c 5 -S -p 111 | Dropped. No reply | 0 packets received, 100% packet loss |

Screenshot:

### Test #5: UDP

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing UDP Packets on Allowed Port 22 | hping3 $EXTERNAL\_IP --udp -c 5 -p 22 | Received 5 packets | 5 packets received, 0% packet loss |

Screenshot:

### Test #6: UDP

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing UDP Packets on Allowed Port 137 | hping3 $EXTERNAL\_IP --udp -c 5 -p 137 | Received 5 packets | 5 packets received, 0% packet loss |

Screenshot:

### Test #7: ICMP

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing ICMP packets, should be 0% loss | ping $EXTERNAL\_IP -c 5 | Received 5 packets | 5 packets received, 0% packet loss |

Screenshot:

### Test #8: ICMP

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Spoofing ICMP network address outside internal network | hping3 $EXTERNAL\_IP -c 5 --spoof $OUTSIDE\_NETWORK\_IP | Dropped. No reply | 0 packets received, 100% packet loss |

Screenshot:

### Test #9: Accept Fragments

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing ACCEPT fragments | hping3 $EXTERNAL\_IP -c 5 -f -p 443 -d 200 -S | Received 5 packets | 5 packets received, 0% packet loss |

Screenshot:

### Test #10: Testing SYN Packets coming the wrong way

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Spoofing ICMP network address outside internal network | hping3 $EXTERNAL\_IP -c 5 -p 1025 -S | Dropped. No reply | 0 packets received, 100% packet loss |

Screenshot:

### Test #11: Testing ACCEPT on all TCP connections that belong to an existing connection

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing ACCEPT on all TCP connections that belong to an existing connection | hping3 $EXTERNAL\_IP -A -c 5 -p 80 | Dropped. No reply | 0 packets received, 100% packet loss |

Screenshot:

### Test #12: Testing DROP on all TCP connections that send SYN, FIN

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing DROP on all TCP connections that send SYN-FIN | hping3 $EXTERNAL\_IP -S -F -c 5 -p 80 | Dropped. No reply | 0 packets received, 100% packet loss |

Screenshot:

### Test #13: Testing TELNET packets

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing TELNET packets | hping3 $EXTERNAL\_IP -c 5 -p 23 -S | Dropped. No reply | 0 packets received, 100% packet loss |

Screenshot:

### Test #14: Testing UDP drop on 32768-32775

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing UDP drop on 32768-32775 | hping3 $EXTERNAL\_IP --udp -c 5 -p 32769 | Dropped. No reply | 0 packets received, 100% packet loss |

Screenshot:

### Test #15: Testing UDP drop on 137-139

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing UDP drop on 137-139 | hping3 $EXTERNAL\_IP --udp -c 5 -p 138 | Dropped. No reply | 0 packets received, 100% packet loss |

Screenshot:

### Test #16: Testing TCP drop on 32768-32775

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing TCP drop on 32768-32775 | hping3 $EXTERNAL\_IP -S -c 5 -p 32770 | Dropped. No reply | 0 packets received, 100% packet loss |

Screenshot:

### Test #17: Testing TCP drop on 137-139

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing TCP drop on 137-139 | hping3 $EXTERNAL\_IP -S -c 5 -p 138 | Dropped. No reply | 0 packets received, 100% packet loss |

Screenshot:

### Test #18: Testing TCP drop on 111

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing TCP drop on 111 | hping3 $EXTERNAL\_IP -S -c 5 -p 111 | Dropped. No reply | 0 packets received, 100% packet loss |

Screenshot:

### Test #19: Testing TCP drop on 515

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Command | Expected Result | Actual Result |
| Testing TCP drop on 515 | hping3 $EXTERNAL\_IP -S -c 5 -p 138 | Dropped. No reply | 0 packets received, 100% packet loss |

Screenshot: