Test Documentation

Ben Soer

A00843110

COMP 8006

BTECH Set 6D

Table of Contents

[Test Chart 3](#__RefHeading___Toc113_588438470)

[Inbound Tests 3](#__RefHeading___Toc2280_150870594)

[Outbound Tests 5](#__RefHeading___Toc2282_150870594)

[Results 6](#__RefHeading___Toc115_588438470)

[Inbound Tests 6](#__RefHeading___Toc2284_150870594)

[TOS\_T1 6](#__RefHeading___Toc2286_150870594)

[TOS\_T2 6](#__RefHeading___Toc2288_150870594)

[TOS\_T3 6](#__RefHeading___Toc2290_150870594)

[TOS\_T4 6](#__RefHeading___Toc2292_150870594)

[TOS\_T5 6](#__RefHeading___Toc2294_150870594)

[TOS\_T6 6](#__RefHeading___Toc2296_150870594)

[TOS\_T7 6](#__RefHeading___Toc2298_150870594)

[TOS\_T8 6](#__RefHeading___Toc2300_150870594)

[NAE\_T1 6](#__RefHeading___Toc2302_150870594)

[NAE\_T2 7](#__RefHeading___Toc2304_150870594)

[IE\_T1 7](#__RefHeading___Toc2306_150870594)

[IE\_T2 8](#__RefHeading___Toc2308_150870594)

[OI\_T1 8](#__RefHeading___Toc2310_150870594)

[OI\_T2 9](#__RefHeading___Toc2312_150870594)

[SYNFIN\_T1 9](#__RefHeading___Toc2314_150870594)

[TELNET\_T1 10](#__RefHeading___Toc2316_150870594)

[TELNET\_T2 10](#__RefHeading___Toc2318_150870594)

[TELNET\_T3 10](#__RefHeading___Toc2320_150870594)

[EXPDR\_T1 11](#__RefHeading___Toc2322_150870594)

[EXPDR\_T2 11](#__RefHeading___Toc2324_150870594)

[TCP\_T3 12](#__RefHeading___Toc2326_150870594)

[TCP\_T4 12](#__RefHeading___Toc2328_150870594)

[UDP\_T3 13](#__RefHeading___Toc2330_150870594)

[UDP\_T4 13](#__RefHeading___Toc2332_150870594)

[ICMP\_T1 13](#__RefHeading___Toc2334_150870594)

[Outbound Tests 14](#__RefHeading___Toc2336_150870594)

# Test Chart

## Inbound Tests

Below is a breakdown chart of all the tests executed and the appropriate tests. Note that the Rule/Test # correspond directly to the iptables rule in the fwall.sh file and the hping3 test in the hping-tests.sh file. Each rule is commented with these numbers in the source files if you would like to see how each rule corresponds.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rule/Test #** | **Test Description** | **Tool Used** | **Expected Result** | **Pass / Fail** |
| TOS\_T1 | SSH Traffic Should have Miminimse Delay TOS (4) | Wireshark | Packet Has TOS 4 | PASS – See Attached |
| TOS\_T2 | SSH Traffic Should have Miminimse Delay TOS (4) | Wireshark | Packet Has TOS 4 | PASS – See Attached |
| TOS\_T3 | SSH Traffic Should have Miminimse Delay TOS (4) | Wireshark | Packet Has TOS 4 | PASS – See Attached |
| TOS\_T4 | SSH Traffic Should have Miminimse Delay TOS (4) | Wireshark | Packet Has TOS 4 | PASS – See Attached |
| TOS\_T5 | FTP Traffic Should have Maximum Throughput TOS (2) | Wireshark | Packet Has TOS 2 | PASS – See Attached |
| TOS\_T6 | FTP Traffic Should have Maximum Throughput TOS (2) | Wireshark | Packet Has TOS 2 | PASS – See Attached |
| TOS\_T7 | FTP Traffic Should have Maximum Throughput TOS (2) | Wireshark | Packet Has TOS 2 | PASS – See Attached |
| TOS\_T8 | FTP Traffic Should have Maximum Throughput TOS (2) | Wireshark | Packet Has TOS 2 | PASS – See Attached |
| NAE\_T1 | New or Established TCP Connections Should Get Through | Hping3 | SYN Call Should Get Through | PASS – See Attached |
| NAE\_T2 | New or Established UDP Connections Should Get Through | Hping3 + Accounting Table | UDP Call Should Get Through | PASS – See Attached |
| IE\_T1 | Established TCP Connections Should Get Through | Google Chrome + Accounting Table | TCP Established Calls Should Get Through | PASS – See Attached |
| IE\_T2 | Established UDP Connections Should Get Through | Hping3 + Accounting Table | UDP Should Fail Due To No Established Connection | PASS – See Attached |
| OI\_T1 | Drop Incoming Packets with Source Matching Internal Host IP | Hping3 + Accounting Tables | Packet Is Dropped | PASS - Packet Dropped But Not Where Expected |
| OI\_T2 | Drop Incoming Packets with Source Matching Firewall Interal IP | Hping3 + Accounting Tables | Packet Is Dropped | PASS - Packet Dropped But Not Where Expected |
| SYNFIN\_T1 | Drop Incoming Packets with with SYN and FIN flags set | Hping3 | Packet Is Dropped | PASS – See Attached |
| TELNET\_T1 | Drop Telnet Connections | Hping3 | Packet Is Dropped | PASS – See Attached |
| TELNET\_T2 | Drop Telnet Connections | Hping3 | Packet Is Dropped | PASS – See Attached |
| TELNET\_T3 | Drop Telnet Connections | Hping3 | Packet Is Dropped | PASS – See Attached |
| EXPDR\_T1 | Drop Explicit TCP Ports | Hping3 | Packet Is Dropped | PASS – See Attached |
| EXPDR\_T2 | Drop Explicit UDP Ports | Hping3 + Accounting Tables | Packet Is Dropped | PASS – See Attached |
| TCP\_T3 | Allow NEW and Established Connections on Valid TCP Ports Through | Hping3 | Packets Get Through | PASS – See Attached |
| TCP\_T4 | Allow only ESTABLISHED Connections on valid Response ports Through | Hping3 | Packets Won't Get Through due to Hping3 unable to hold a session | PASS – See Attached |
| UDP\_T3 | Allow NEW and ESTABLISHED Connections on Valid UDP Ports Through | Hping 3 + Accounting Table | Packet Gets Through | PASS – See Attached |
| UDP\_T4 | Allow only ESTABLISHED Connections on valid Response ports Through | Hping3 + Accounting Table | Packet Will Go Through Since UDP Has No State and Hping3 does not hold a sessions | PASS – See Attached |
| ICMP\_T1 | ICMP Of The Appropriate Type Will Be Let Through | Hping3 | Valid ICMP Type Will Go Through | PASS – See Attached |

## Outbound Tests

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rule/Test #** | **Test Description** | **Tool Used** | **Expected Result** | **Pass / Fail** |
| DNS\_T1 | Standard DNS ping through port 53 | Hping3 | Packet Gets Through | PASS – See Attached |
| TCP\_T5 | TCP outbound connection on allowed port 80 | Hping3 | Packet Gets Through | PASS – See Attached |
| TCP\_T6 | TCP outbound connection on allowed port 21 | Hping3 | Packet Gets Through | PASS – See Attached |
| TCP\_T7 | TCP outbound connection on disallowed port 21 | Hping3 | Packet Will Not Through | PASS – See Attached |
| UDP\_T5 | UDP outbound packets on allowed port 53 | Hping3 | Packet Gets Through | PASS – See Attached |
| UDP\_T6 | UDP outbound packets on disallowed port 55 | Hping3 | Packet Will Not Through | PASS – See Attached |
| ICMP\_T2 | Outbound ICMP type 0 (echo response) | Hping3 | Packet Will Not Through | PASS – See Attached |
| ICMP\_T3 | Outbound invalid ICMP type 3 | Hping3 | Packet Will Not Through | PASS – See Attached |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| FRAG\_T1 | Outbound fragmented packet of 2k bytes | Hping3 | Packet Gets Through | PASS – See Attached |
| TCP\_T8 | Outbound TCP packet with FIN and SYN flag set | Hping3 | Packet Will Not Through | PASS – See Attached |
| TELNET\_T4 | Outbound telnet connection request | Hping3 | Packet Will Not Through | PASS – See Attached |
| LO\_T1 | Loopback packet sent | Hping3 | Packet Gets Through | PASS – See Attached |
| SSH\_T1 | Outbound SSH connection | Hping3 | Packet Gets Through | PASS – See Attached |
| FTP\_T1 | Outbound FTP connection | Hping3 | Packet Gets Through | PASS – See Attached |
| TCP\_T9 | Outbound TCP packets on ban ports | Hping3 | Packet Will Not Through | PASS – See Attached |

# Results

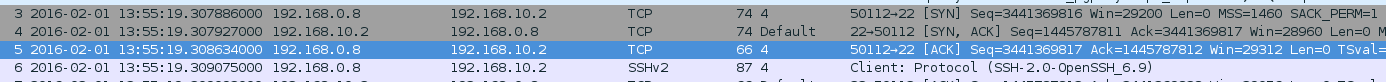
Below are the various screenshots of the test being run. The original images can be found in the /tests folder

## Inbound Tests

### TOS\_T1

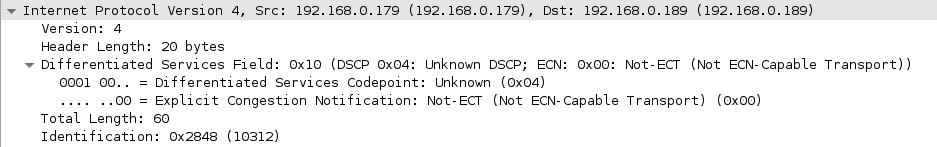
See in the 6th Column the 4. This is the TOS Column of 4 (Minimum Delay)

Wireshark



### TOS\_T2

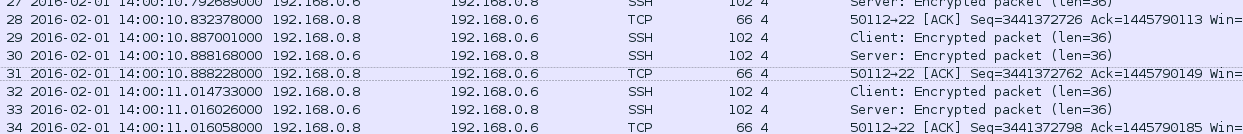
Wireshark



### TOS\_T3

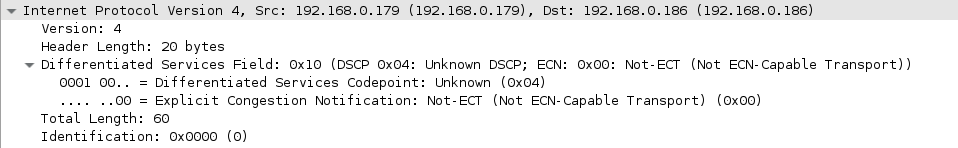
See in the 6th Column the 4. This is the TOS Column of 4 (Minimum Delay)

Wireshark



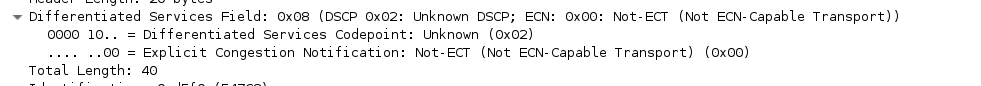
### TOS\_T4

Wireshark



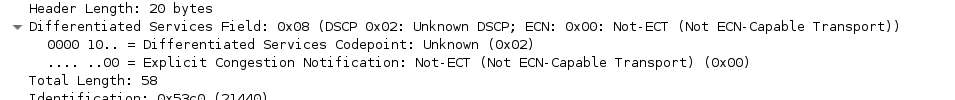
### TOS\_T5

Wireshark



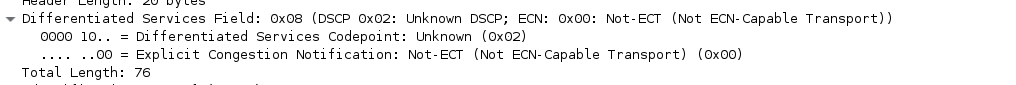
### TOS\_T6

Wireshark



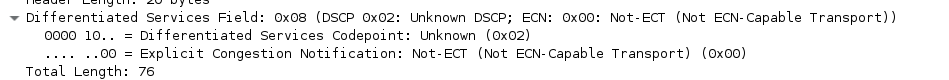
### TOS\_T7

Wireshark



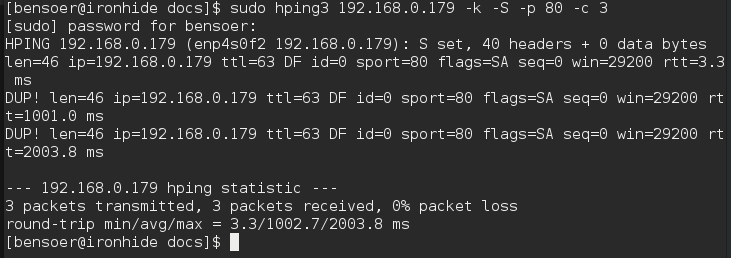
### TOS\_T8

Wireshark



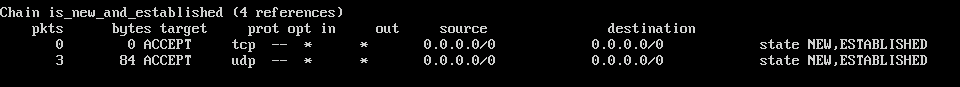
### NAE\_T1

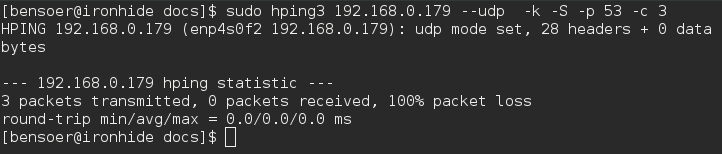
Hping3



### NAE\_T2

Accounting Table Before

Hping3

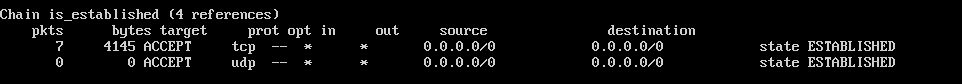
Accounting Table After

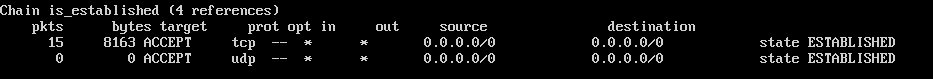
### 

### IE\_T1

Test was executed by loading a page hosted on the internal host in Google Chrome. After the initial SYN by the browser, the SYN ACK and ACK packets fall under the is\_established chain

Accounting Table Before

Accounting Table After



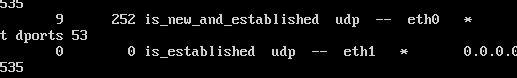
### IE\_T2

From this test we can see that UDP traffic being stateless does not easily fall under being established. We can see from before and after that is\_established packets do not change. Instead we can see them being redirect to the is\_new\_and\_established chain from the udp\_traffic chain

Accounting Table Before

Accounting Table After

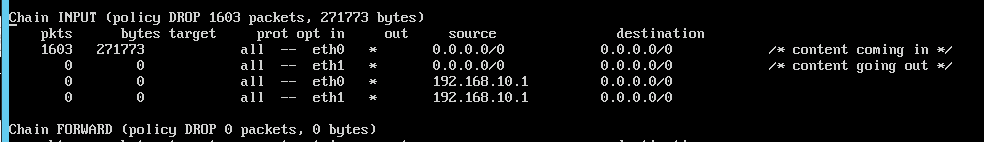
Where Traffic Actualy Went

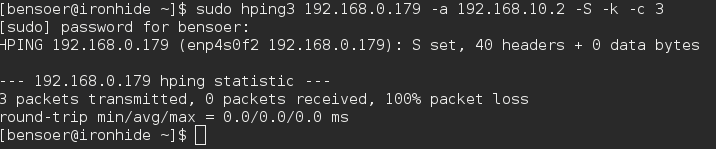


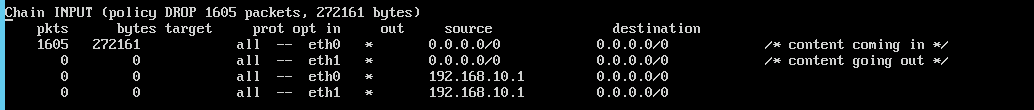
### OI\_T1

Results were successful in that the packets were blocked. But they were blocked by being dropped in the INPUT chain of the gateway. Rules put in the FORWARD chain are never used. The rules added in the INPUT chain are soley for accounting of this test.

Accounting Table Before

Hping3

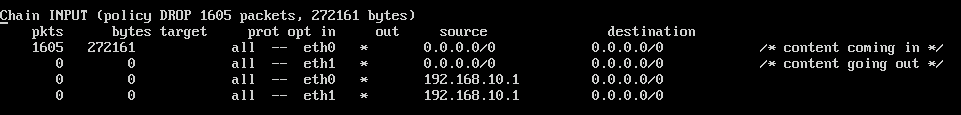
Accounting Table After

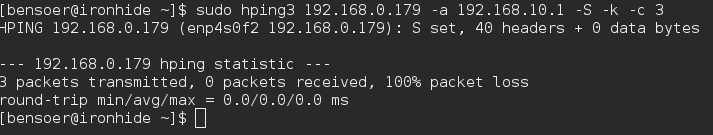


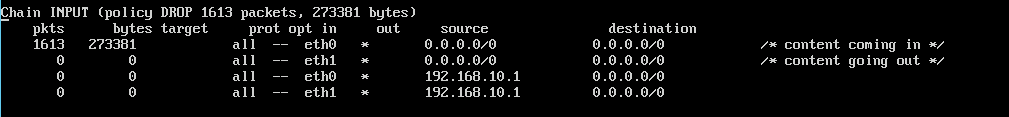
### OI\_T2

Results were successful in that the packets were blocked. But they were blocked by being dropped in the INPUT chain of the gateway. Rules put in the FORWARD chain are never used. The rules added in the INPUT chain are soley for accounting of this test.

Accounting Table Before

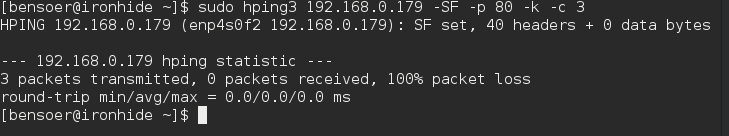
Hping3

Accounting Table After



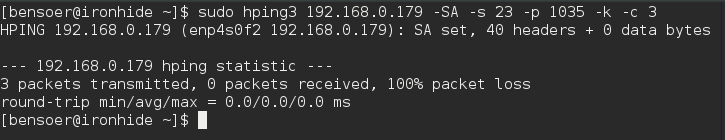
### SYNFIN\_T1

Hping3



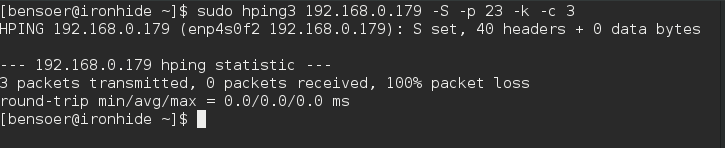
### TELNET\_T1

Hping3



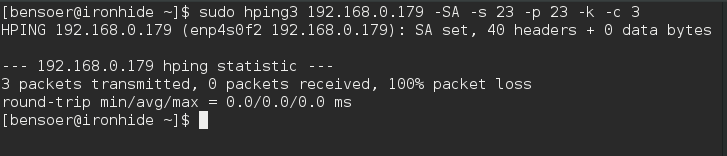
### TELNET\_T2

Hping3



### TELNET\_T3

Hping3



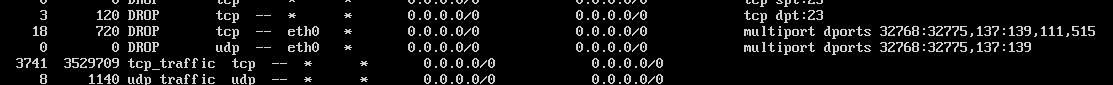
### EXPDR\_T1

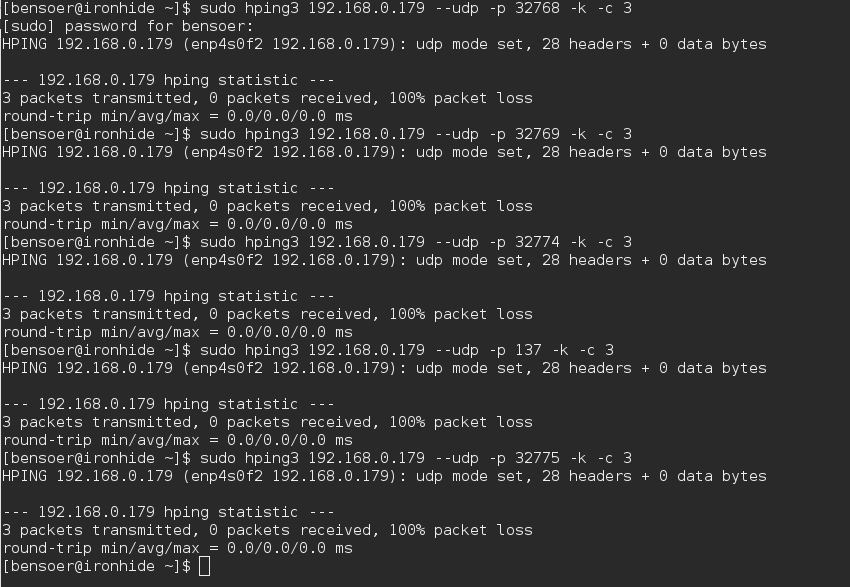
Hping3

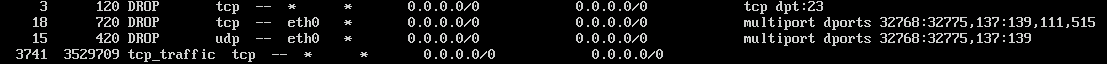
### 

### EXPDR\_T2

Accounting Table Before

Hping3

Accounting Table After



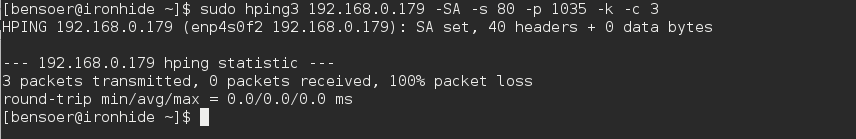
### TCP\_T3

Hping3

### 

### TCP\_T4

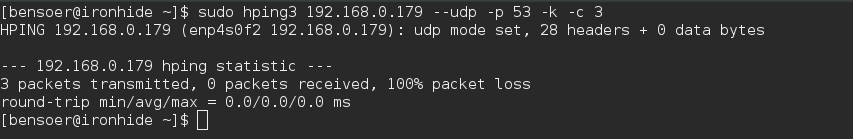
Hping3



### UDP\_T3

Accounting Table Before

Hping3

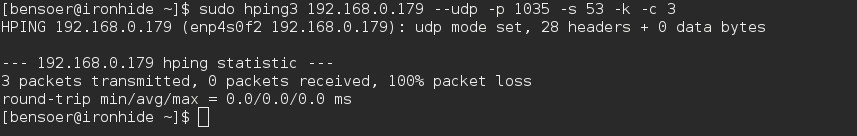
Accounting Table After



### UDP\_T4

Accounting Table Before

Hping3

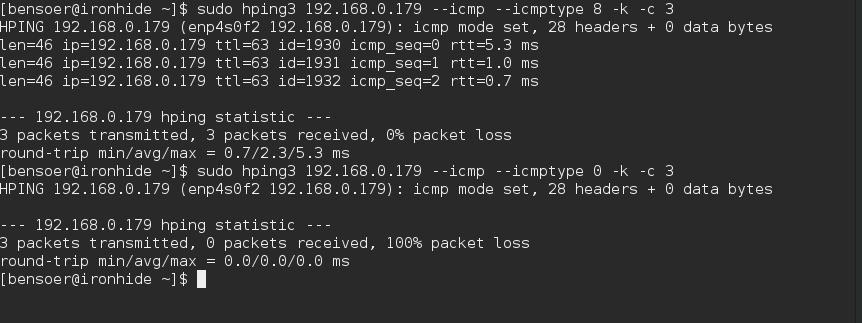
Accounting Table After



### ICMP\_T1

Below shows a valid ICMP and an invalid ICMP being sent through. These can be set in the firewall script. For this test ICMP type 8 (echo) are allowed through, but ICMP type 0 (echo response) is not allowed through. This being because echo response is what comes back, not what goes through

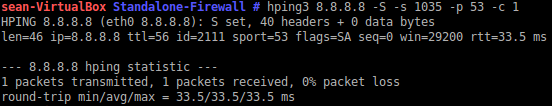
Hping3



## Outbound Tests

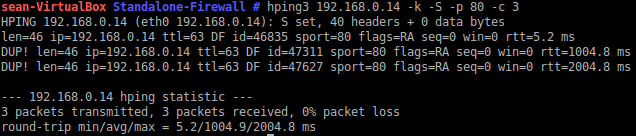
**DNS\_T1**

Testing the google DNS server form inside the firewall showing that it replied



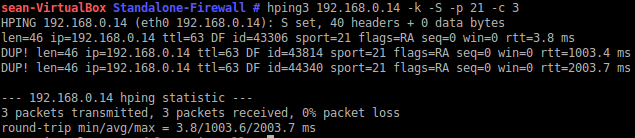
**TCP\_T5**

Successful TCP connection through firewall on allowed port 80



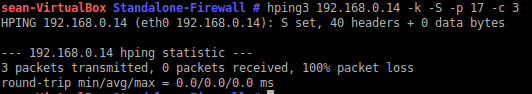
**TCP\_T6**

Successful TCP connection through firewall on allowed port 21



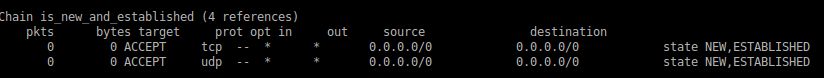
**TCP\_T7**

Unsuccessful TCP connection through firewall on disallowed port 17

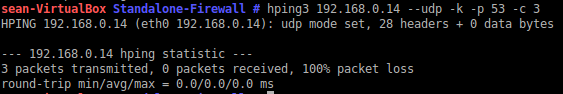


**UDP\_T5**

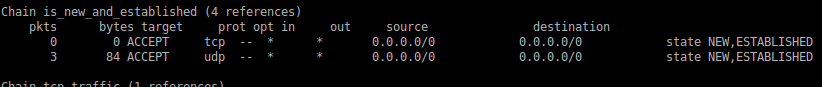
Before UDP request



UDP request on valid port 53

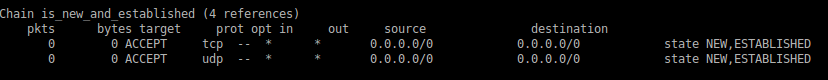


After UDP request



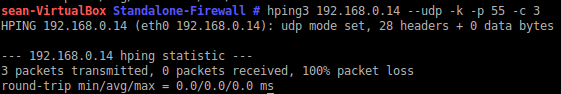
**UDP\_T6**

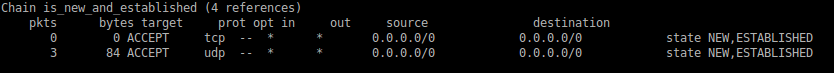
UDP request for on invalid port 55



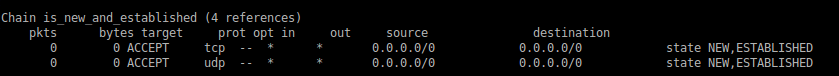
No traffic for UDP so farC:\Users\Root\AppData\Local\Microsoft\Windows\INetCache\Content.Word\UDP_T6_before2.png

UDP request to firewalled port 55



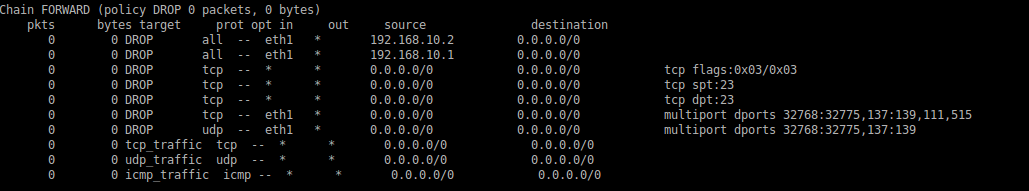
3 new packets for UDP logged in firewall

No new accepted traffic for UDP

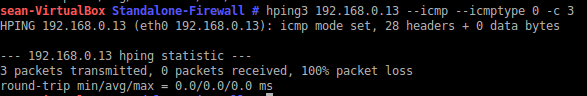


**ICMP\_T2**

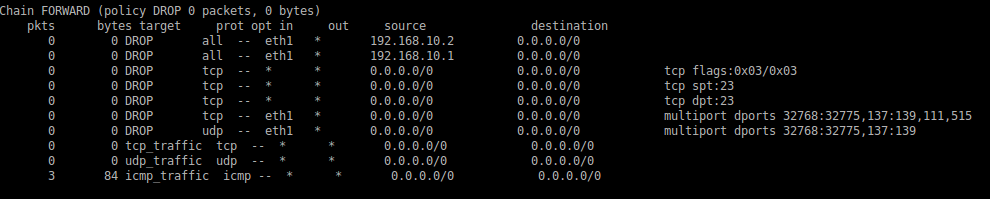
Valid ICMP type 0 (echo response) with not traffic so far



3 ICMP request outbound with type 0

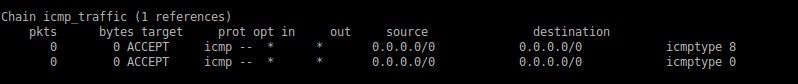
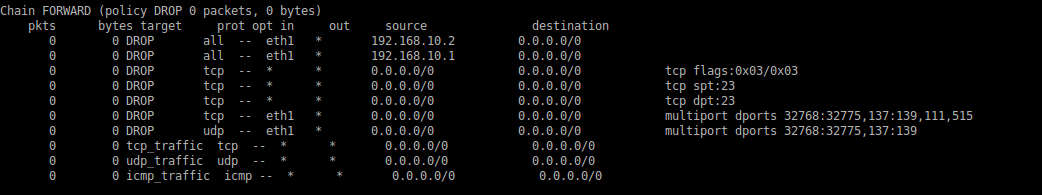


3 accepted ICMP type 0 request

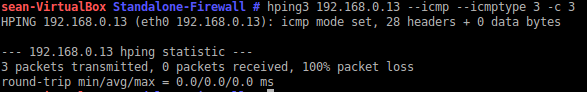


**ICMP\_T3**

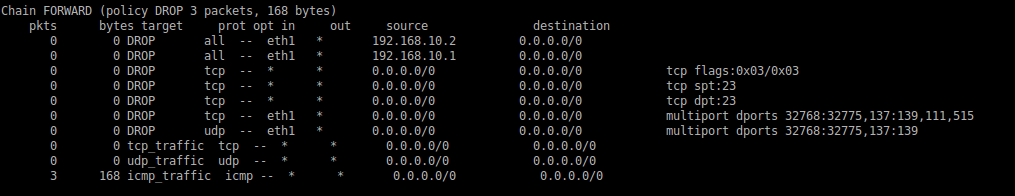
Invalid ICMP traffic of type 3. None so far



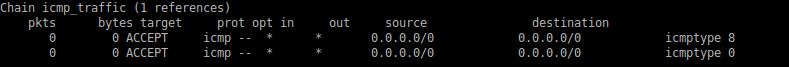
3 ICMP type 3 request



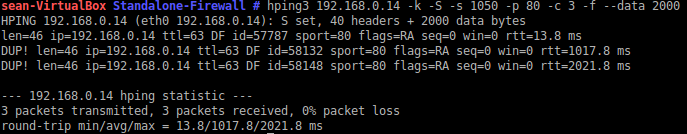
3 ICMP type 3 request logged

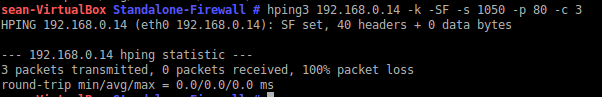


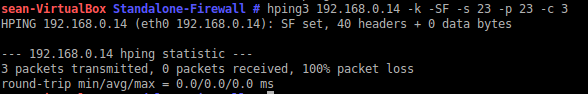
0 ICMP requests accepted



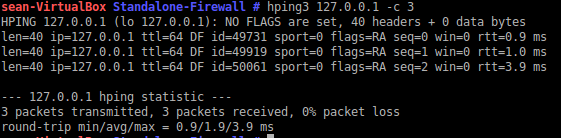
FRAM\_T1



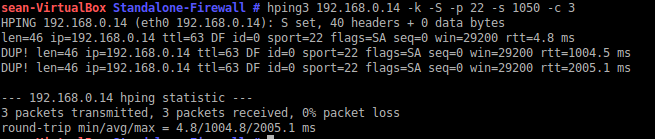
**TCP\_T8**

**TELNET\_T4**

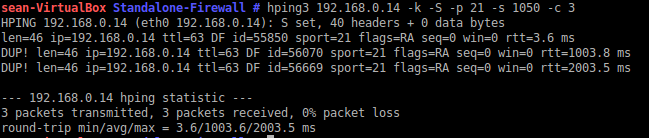
**LO\_T1**



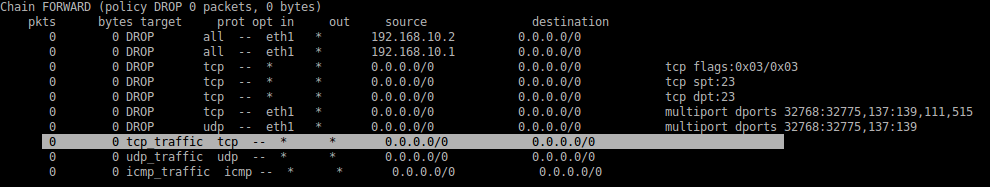
**SSH\_T1**

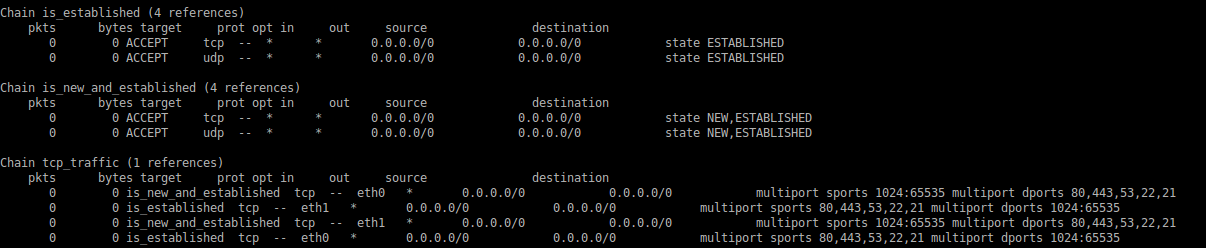


**FTP\_T1**

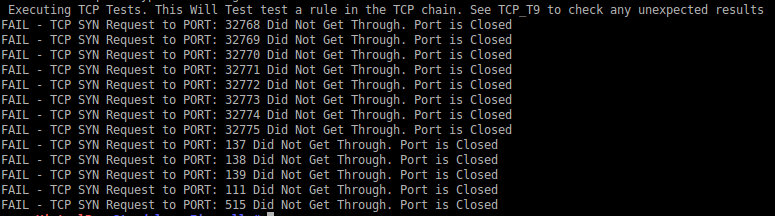


**TCP\_T9**

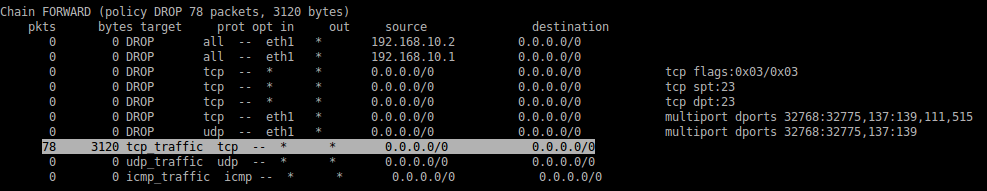
No traffic on TCP filter yet



Test TCP\_T9 running in testfrominternal.sh (each port is tested 3 times)



78 new packets on TCP filer (13 ban ports \* 3 tries for each port \* 2 counts per try)



No packets accepted in tcp\_traffic chain

