Comp 8006 Assignment 2

Network Emulator

By:

John Warren

For: Aman Abdulla

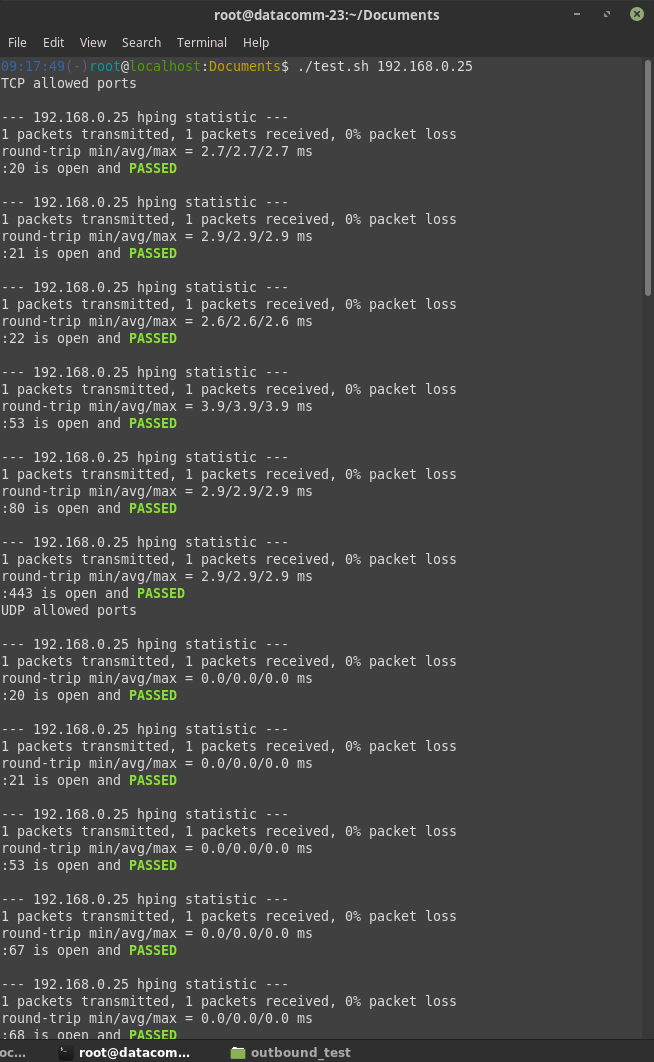
Due: Feb 7, 2019

Table of Contents

[**Design Work**](#_t6zt4uaxclk) **3**

[Objective](#_30j0zll) 3

[Usage](#_neyxjoifywnt) 3

[Specifications](#_1fob9te) 3

[Set up](#_3znysh7) 4

[State Machine](#_2et92p0) 4

[Pseudo Code](#_tyjcwt) 5

[**Test Plan & Results**](#_h8fukb4xbjcf) **5**

[Inbound](#_1t3h5sf) 5

[Outbound](#_uqd9q4b53ynb) 7

# Design Work

## Objective

To design, implement and test a standalone Linux firewall and packet filter

## Usage

Firewall

Run with root access ./fw0.sh

Client

Run with root access ./client\_setup.sh

## Specifications

1 - use netfilter

2 - load user configuration for all forwarded traffic

3 - set default policies for firewall

4 - dns, dhcp enabled

5 - in/out tcp/udp ports, icmp types

6 - default rule = drop

7 - reject wrong way (i.e. syn in on high ports)

8 - accept fragments

9 - drop tcp with SYN & FIN set

10 - no telnet packets allowed

11 - block external

111, 137-139, 515, 32768-32775

12 - ftp/ssh minimum delay,

13 - ftp max thruput

14 - first [en01] = outside, second [enp3s2] = inside

15 - test procedure; test rules, print results (log)

16 - need to know which rule passed/failed

17 - Allow user to define own rules

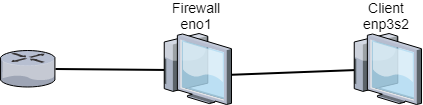
18 – separate file for config

19 – define network interfaces

20 – define allowed tcp, udp, icmp

21 – stateful filtering

## Set up



## State Machine



## Pseudo Code

User Variables

1 – Provide variables to allow user to define values for internal and external interfaces, subnets and IP addresses.

2 – Allow user to define what ports to allow for udp and tcp and icmp types

Configure Firewall

1. Backup existing configuration
2. configure network cards
3. Flush existing configuration
4. apply default rule and drop all packets
5. define chains
6. apply user rules, assigning chains for each of tcp, udp, icmp
   1. for each port, apply rule, add to chain

Configure client

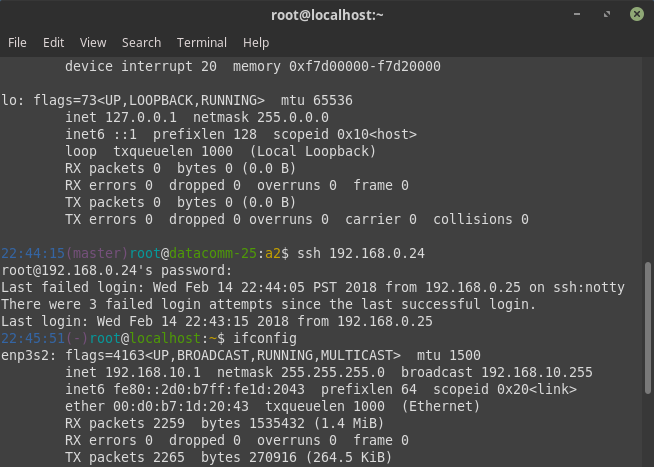
1. Backup current config
2. Disable primary network
3. Connect network cable
4. Configure internal network card

# Test Plan & Results

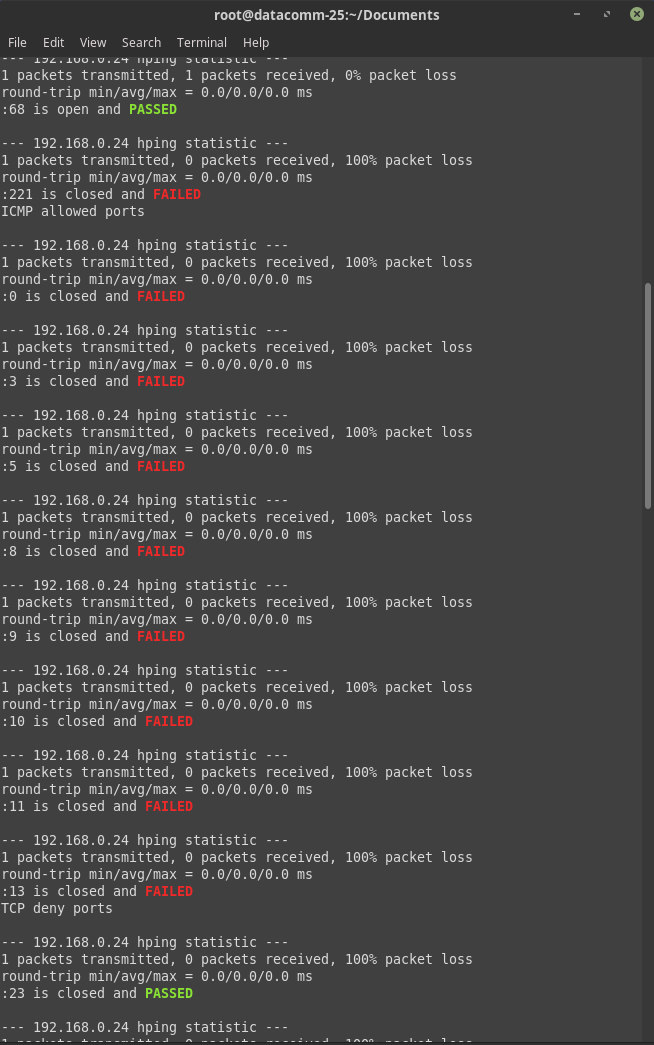
Usage ‘./test.sh <IP of target>’ on either client for outbound or another machine on the network for inbound

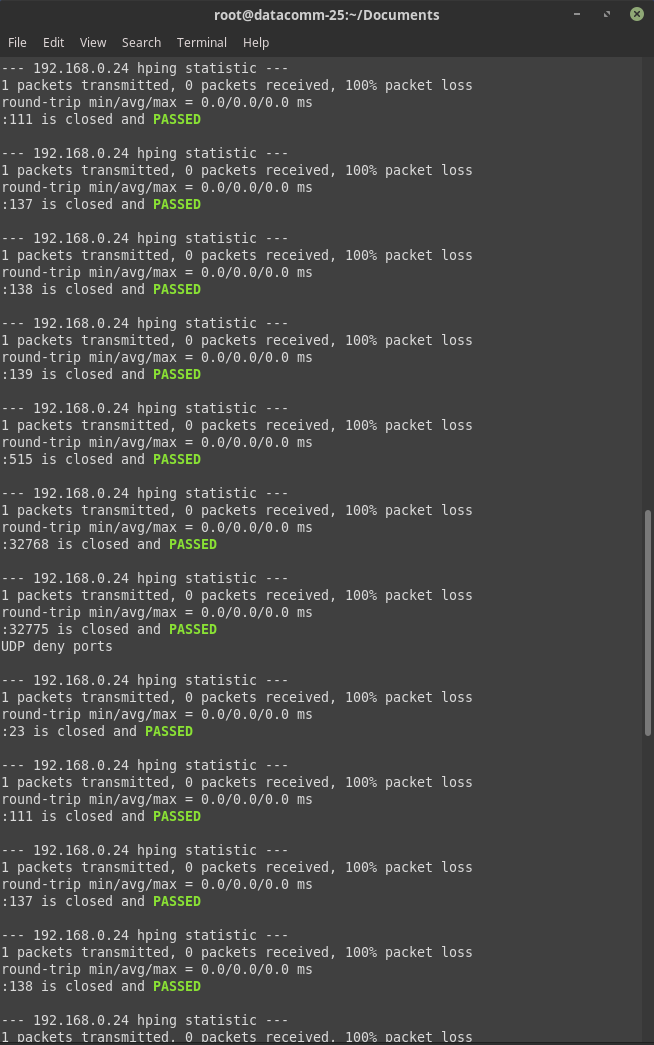
## Inbound

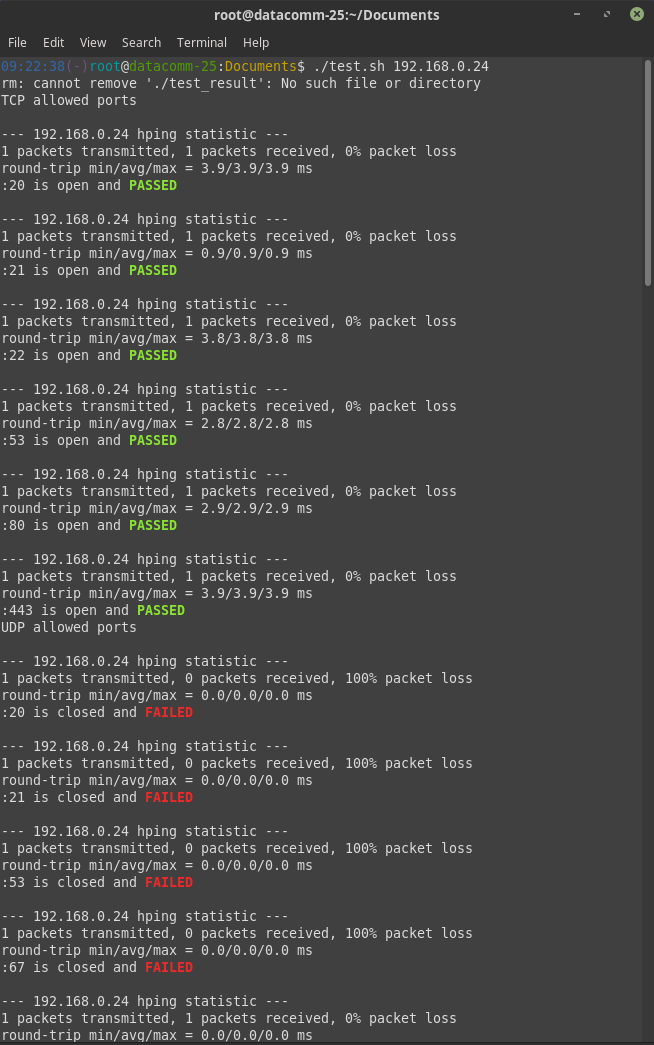
|  |  |  |  |
| --- | --- | --- | --- |
| Testing | Test method | expected | Result |
| TCP port 22 | hping3 ip -V -S -p 22 -c 1 | ALLOWED | PASS |
| TCP port 80 | hping3 ip -V -S -p 80 -c 1 | ALLOWED | PASS |
| TCP port 443 | hping3 ip -V -S -p 443 -c 1 | ALLOWED | PASS |
| UDP port 53 | hping3 ip -V –udp -S -p 53 -c 1 | ALLOWED | FAILED |
| UDP port 67 | hping3 ip -V –udp -S -p 67 -c 1 | ALLOWED | FAILED |
| UDP port 68 | hping3 ip -V –udp -S -p 68 -c 1 | ALLOWED | FAILED |
| ICMP port 0 | hping3 ip -V -1 -S -p 0 -c 1 | ALLOWED | FAILED |
| ICMP port 8 | hping3 ip -V -1 -S -p 8 -c 1 | ALLOWED | FAILED |
| TCP port 23 | hping3 ip -V -S -p 23 -c 1 | DROPPED | PASS |
| TCP port 111 | hping3 ip -V -S -p 111 -c 1 | DROPPED | PASS |
| TCP port 137 | hping3 ip -V -S -p 137 -c 1 | DROPPED | PASS |
| TCP port 138 | hping3 ip -V -S -p 138 -c 1 | DROPPED | PASS |
| TCP port 139 | hping3 ip -V -S -p 139 -c 1 | DROPPED | PASS |
| TCP port 515 | hping3 ip -V -S -p 515 -c 1 | DROPPED | PASS |
| TCP port 32768 | hping3 ip -V -S -p 32768 -c 1 | DROPPED | PASS |
| TCP port 32775 | hping3 ip -V -S -p 32775 -c 1 | DROPPED | PASS |
| UDP port 23 | hping3 ip -V –udp -1 -S -p 0 -c 1 | DROPPED | PASS |
| UDP port 111 | hping3 ip -V –udp -1 -S -p 8 -c 1 | DROPPED | PASS |
| UDP port 137 | hping3 ip -V –udp -S -p 23 -c 1 | DROPPED | PASS |
| UDP port 138 | hping3 ip -V –udp -S -p 111 -c 1 | DROPPED | PASS |
| UDP port 139 | hping3 ip -V –udp -S -p 137 -c 1 | DROPPED | PASS |
| UDP port 515 | hping3 ip -V –udp -S -p 138 -c 1 | DROPPED | PASS |
| UDP port 32768 | hping3 ip -V –udp -S -p 139 -c 1 | DROPPED | PASS |
| UDP port 32775 | hping3 ip -V –udp -S -p 515 -c 1 | DROPPED | PASS |
| ICMP port 200 | hping3 ip -V -1 -S -p 200 -c 1 | DROPPED | PASS |
| TCP SPOOF | hping3 ip -V -c 1 -S -s 80 -p 80 --spoof 192.168.10.5 | DROPPED | PASS |
| TCP SYN FIN | hping3 ip -V -c 1 -s 1000 -p 80 -SF | DROPPED | PASS |
| UDP fragment | hping3 ip -V -S -p 22 -c 1 -f | DROPPED |  |

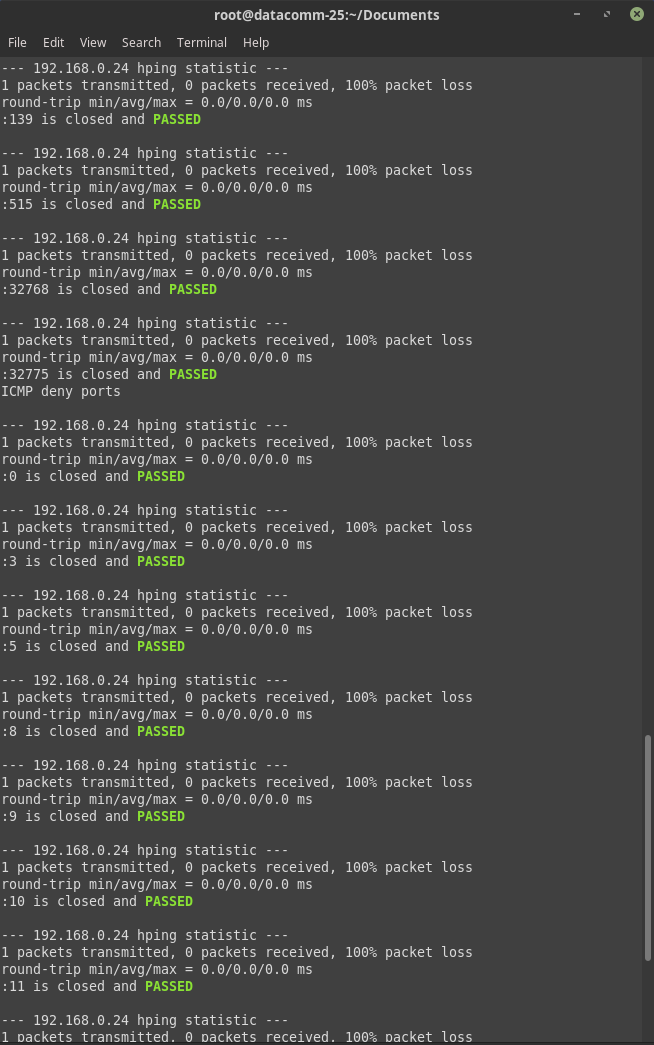
SSH in - Connected

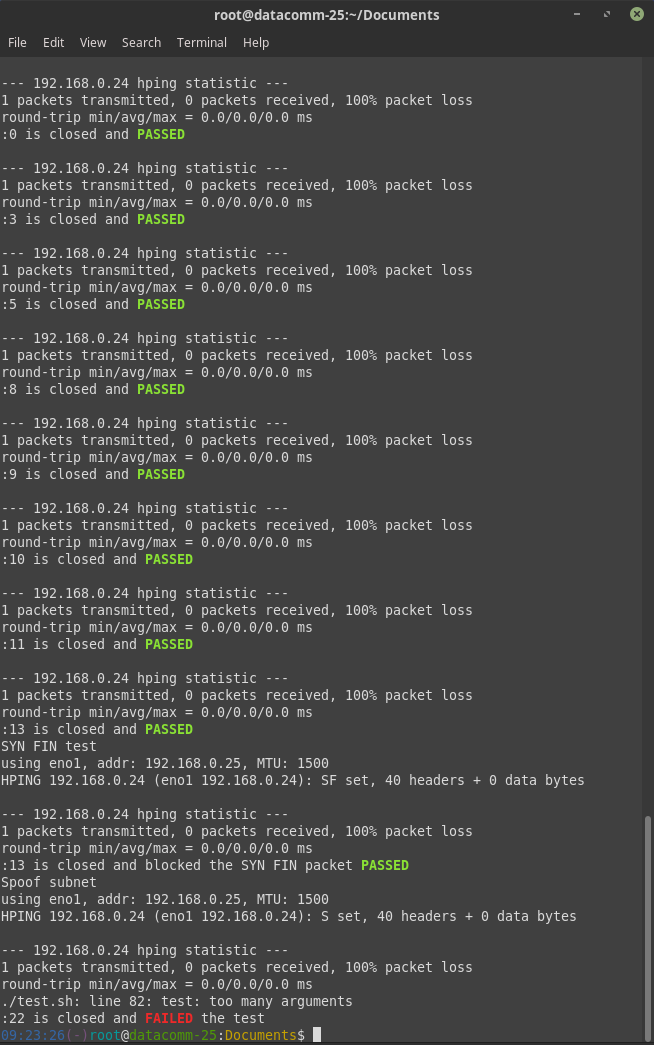
## 











## Outbound

|  |  |  |  |
| --- | --- | --- | --- |
| Testing | Test method | expected | Result |
| TCP port 22 | hping3 ip -V -S -p 22 -c 1 | ALLOWED | PASS |
| TCP port 80 | hping3 ip -V -S -p 80 -c 1 | ALLOWED | PASS |
| TCP port 443 | hping3 ip -V -S -p 443 -c 1 | ALLOWED | PASS |
| UDP port 53 | hping3 ip -V –udp -S -p 53 -c 1 | ALLOWED | PASS |
| UDP port 67 | hping3 ip -V –udp -S -p 67 -c 1 | ALLOWED | PASS |
| UDP port 68 | hping3 ip -V –udp -S -p 68 -c 1 | ALLOWED | PASS |
| ICMP port 0 | hping3 ip -V -1 -S -p 0 -c 1 | ALLOWED | PASS |
| ICMP port 8 | hping3 ip -V -1 -S -p 8 -c 1 | ALLOWED | PASS |
| TCP port 23 | hping3 ip -V -S -p 23 -c 1 | DROPED | PASS |
| TCP port 111 | hping3 ip -V -S -p 111 -c 1 | DROPED | PASS |
| TCP port 137 | hping3 ip -V -S -p 137 -c 1 | DROPED | PASS |
| TCP port 138 | hping3 ip -V -S -p 138 -c 1 | DROPED | PASS |
| TCP port 139 | hping3 ip -V -S -p 139 -c 1 | DROPED | PASS |
| TCP port 515 | hping3 ip -V -S -p 515 -c 1 | DROPED | PASS |
| TCP port 32768 | hping3 ip -V -S -p 32768 -c 1 | DROPED | PASS |
| TCP port 32775 | hping3 ip -V -S -p 32775 -c 1 | DROPED | PASS |
| UDP port 23 | hping3 ip -V –udp -1 -S -p 0 -c 1 | DROPED | PASS |
| UDP port 111 | hping3 ip -V –udp -1 -S -p 8 -c 1 | DROPED | PASS |
| UDP port 137 | hping3 ip -V –udp -S -p 23 -c 1 | DROPED | PASS |
| UDP port 138 | hping3 ip -V –udp -S -p 111 -c 1 | DROPED | PASS |
| UDP port 139 | hping3 ip -V –udp -S -p 137 -c 1 | DROPED | PASS |
| UDP port 515 | hping3 ip -V –udp -S -p 138 -c 1 | DROPED | PASS |
| UDP port 32768 | hping3 ip -V –udp -S -p 139 -c 1 | DROPED | PASS |
| UDP port 32775 | hping3 ip -V –udp -S -p 515 -c 1 | DROPED | PASS |
| ICMP port 200 | hping3 ip -V -1 -S -p 200 -c 1 | DROPED | PASS |
| TCP SPOOF | hping3 ip -V -c 1 -S -s 80 -p 80 --spoof 192.168.10.5 | DROPPED | PASS |
| TCP SYN FIN | hping3 ip -V -c 1 -s 1000 -p 80 -SF | DROPPED | PASS |
| UDP fragment | hping3 ip -V -S -p 22 -c 1 -f | DROPPED |  |

SSH out test

