COMP 8006 Assignment 1

Table of Contents

[Usage 2](#_Toc505170157)

[Design 2](#_Toc505170158)

[Psudocode 2](#_Toc505170159)

[Testing 2](#_Toc505170160)

[Nmap 2](#_Toc505170161)

[DNS + WWW 3](#_Toc505170162)

[Hping - inbound traffic to port 80 (http) from source ports less than 1024 3](#_Toc505170163)

# Usage

> ./ez-firewall.sh

# Design

## Psudocode

Flush all chains  
Delete all user chains

Set default policies to DROP for all chains

Create user chain for ssh  
Create user chain for www

Drop all packets from port 0  
Drop all packets to port 0

Drop inbound traffic to port 80 from source ports 0 to 1023

Jump all packets to and from ports 80 and 443 to www chain  
Jump all packets to and from port 22 to ssh chain  
Accept all packets to and from port 53

Accept all packets to www chain  
Accept all packets to ssh chain

# Testing

Testing done with test.sh

Usage:  
> ./test.sh &> <filename>

## Nmap

Used for testing inbound packets to port 80,443,53,22,0 with both tcp and udp Protocol

# Nmap done at Mon Jan 29 13:43:50 2018 -- 1 IP address (1 host up) scanned in 1.51 seconds

# Nmap 7.60 scan initiated Mon Jan 29 13:46:09 2018 as: nmap -oA results --append-output -p 80,443,53,22,0 192.168.0.5

Nmap scan report for 192.168.0.5

Host is up (0.00028s latency).

PORT STATE SERVICE

**0/tcp filtered unknown**

**22/tcp filtered ssh**

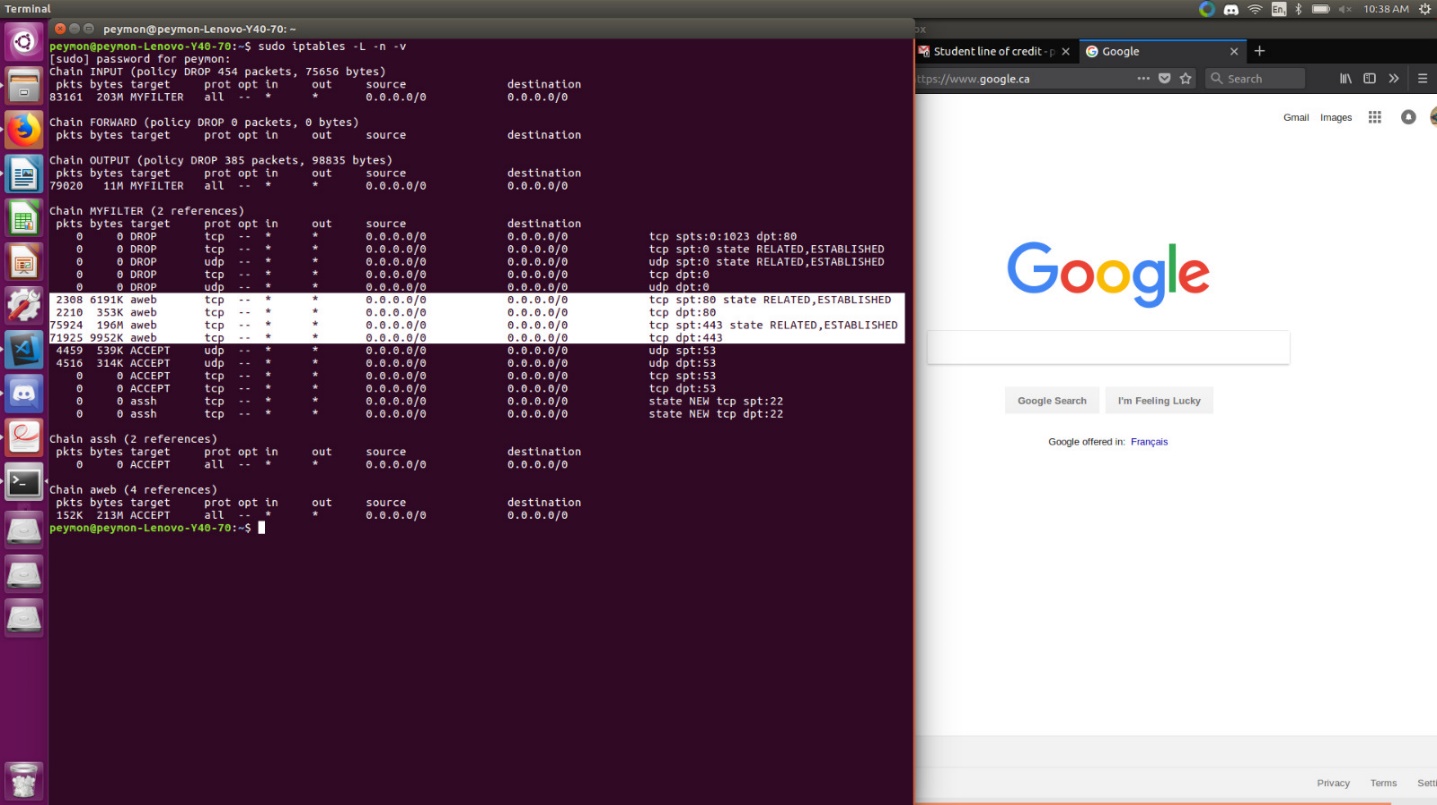
**53/tcp closed domain**

**80/tcp closed http**

**443/tcp closed https**

MAC Address: 98:90:96:DC:EB:26 (Dell)

## DNS + WWW



## Hping - inbound traffic to port 80 (http) from source ports less than 1024

--- 192.168.0.5 hping statistic ---

10 packets transmitted, 0 packets received, 100% packet loss

round-trip min/avg/max = 0.0/0.0/0.0 ms

HPING 192.168.0.5 (eno1 192.168.0.5): S set, 40 headers + 0 data bytes