Peyman Tehrani Parsa
A00922386

COMP 8006 Assignment 1

Table of Contents

Usage..2

Design...2

Psudocode..2

Testing...2

Nmap...2

DNS + WWW 3

Hping - inbound traffic to port 80 (http) from source ports less than 1024...3

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

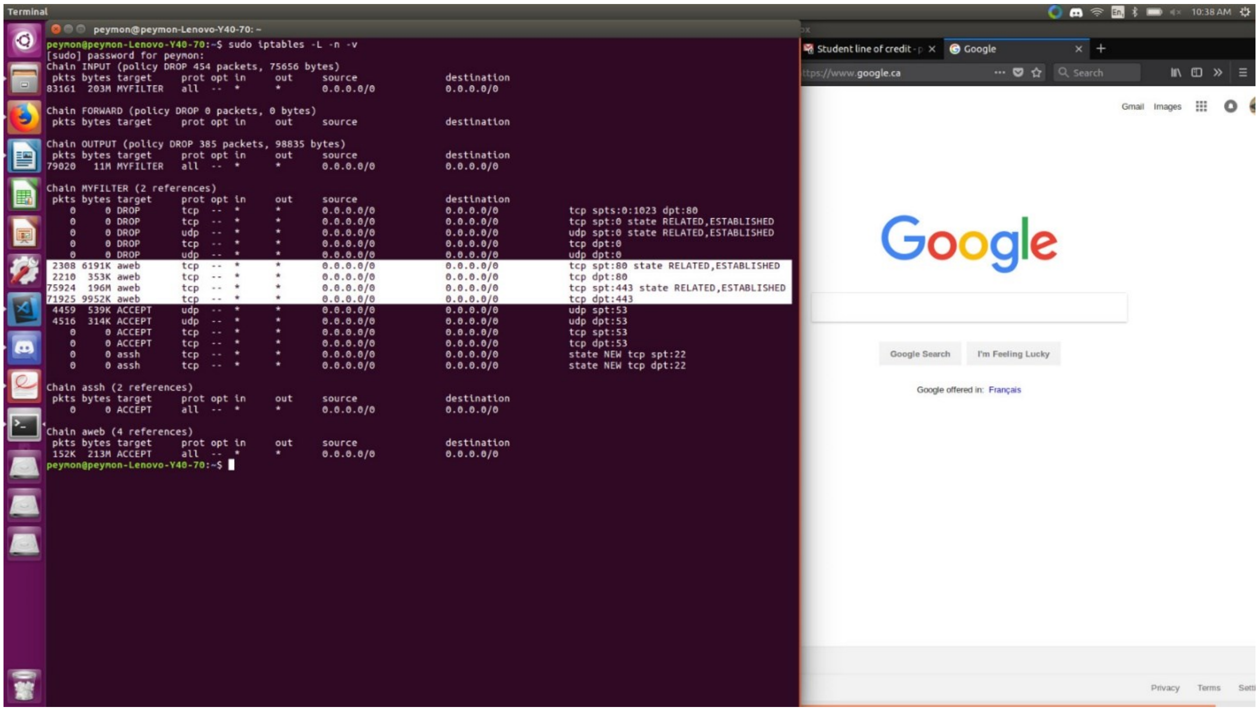
```
# Nmap done at Mon Jan 29 13:43:50 2018 -- 1 IP address (1 host up) scanned
in 1.51 seconds
# Nmap 7.60 scan initiated Mon Jan 29 13:46:09 2018 as: nmap -oA results --
append-output -p 80,443,53,22,0 192.168.0.5
Nmap scan report for 192.168.0.5
Host is up (0.00028s latency).

PORT    STATE    SERVICE
0/tcp   filtered unknown
22/tcp  filtered ssh
53/tcp  closed   domain
80/tcp  closed   http
443/tcp closed   https
```

Peyman Tehrani Parsa
A00922386

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

DNS + WWW



```
peymon@peymon-Lenovo-Y40-70:~$ sudo iptables -L -n -v
[sudo] password for peymon:
Chain INPUT (policy DROP 454 packets, 75656 bytes)
 pkts bytes target     prot opt in     out     source               destination
83161  203M MYFILTER   all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 385 packets, 98835 bytes)
 pkts bytes target     prot opt in     out     source               destination
79020   11M MYFILTER   all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain MYFILTER (2 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:0 state RELATED,ESTABLISHED
    0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:0 state RELATED,ESTABLISHED
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:0
    0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:0
 2308 6191K aweb       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:80 state RELATED,ESTABLISHED
 2210  353K aweb       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
75924  196M aweb       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:443 state RELATED,ESTABLISHED
71925 9952K aweb       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443
 4459  539K ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:53
 4516  314K ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp spt:53
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
    0     0 assh       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            state NEW tcp spt:22
    0     0 assh       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:22

Chain assh (2 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain aweb (4 references)
 pkts bytes target     prot opt in     out     source               destination
 152K  213M ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
peymon@peymon-Lenovo-Y40-70:~$ 
```

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