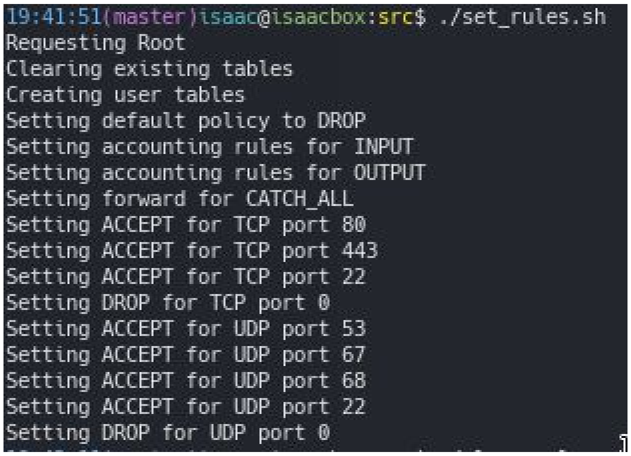
8006 Asn1 - Testing

Finite testing space, infinite user error

Isaac Morneau; A00958405

Running the Firewall

Simply enter the src folder and execute `./set_rules`
Which will give you and output like

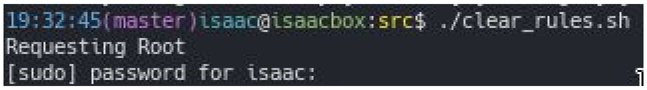


```
19:41:51(master)isaac@isaacbox:src$ ./set_rules.sh
Requesting Root
Clearing existing tables
Creating user tables
Setting default policy to DROP
Setting accounting rules for INPUT
Setting accounting rules for OUTPUT
Setting forward for CATCH_ALL
Setting ACCEPT for TCP port 80
Setting ACCEPT for TCP port 443
Setting ACCEPT for TCP port 22
Setting DROP for TCP port 0
Setting ACCEPT for UDP port 53
Setting ACCEPT for UDP port 67
Setting ACCEPT for UDP port 68
Setting ACCEPT for UDP port 22
Setting DROP for UDP port 0
```

Depending on what you entered into the config text files.
Should it be run without root it will prompt you

Clearing the Firewall

Simply enter the src folder and execute `./clear_rules`
This will remove all firewall configuration and return it to default.



```
19:32:45(master)isaac@isaacbox:src$ ./clear_rules.sh
Requesting Root
[sudo] password for isaac:
```

As you can see if not run with root both scripts will request it in order to continue.

Testing Table

Note: the spelling error `tramitted` was directly from the output of hping3 and as such has been left in.

Condition	Testing Method (Command)	Result
Permit Inbound SSH	sudo hping3 192.168.0.16 -c 1 -S -p 22	1 packets tramitted, 1 packets received, 0% packet loss
Permit Outbound SSH	sudo hping3 -p 22 -S -c 1 192.168.0.5	1 packets tramitted, 1 packets received, 0% packet loss
Permit Inbound WWW	sudo hping3 192.168.0.16 -c 1 -S -p 80	1 packets tramitted, 1 packets received, 0% packet loss
	sudo hping3 192.168.0.16 -c 1 -S	1 packets tramitted, 1 packets received,

	-p 443	0% packet loss
Permit Outbound WWW	curl vk-k.com	<html> <head><title>301 Moved Permanently</title></head> <body bgcolor="white"> <center><h1>301 Moved Permanently</h1></center> <hr><center>nginx</center> </body> </html>
Drop inbound to port 80 from source ports less than 1024	sudo hping3 -s 400 -p 80 -c 1 192.168.0.16	1 packets tramitted, 0 packets received, 100% packet loss
Drop all Inbound packets on port 0	sudo hping3 192.168.0.16 -c 1 -S -p 0	1 packets tramitted, 0 packets received, 100% packet loss
Drop all Outbound packets on port 0	sudo hping3 -s 0 -p 80 -S vk-k.com	HPING vk-k.com (wlp2s0 70.68.160.89): S set, 40 headers + 0 data bytes [send_ip] sendto: Operation not permitted

Testing TCP Raw Output

A full TCP port scan was run for completeness and the results are as expected from the listed test. While the http and https ports were closed this is as expected as there was no web server running on the machine but they were not filtered as the other denied ports were.

```
14:01:33(master)isaac@isaacbox:~$ sudo nmap -T4 -v -sS -p- 192.168.0.16

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-31 14:01 PST
Initiating ARP Ping Scan at 14:01
Scanning 192.168.0.16 [1 port]
Completed ARP Ping Scan at 14:01, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:01
Completed Parallel DNS resolution of 1 host. at 14:01, 0.00s elapsed
Initiating SYN Stealth Scan at 14:01
Scanning DESKTOP-A9IHJU9.hitronhub.home (192.168.0.16) [65535 ports]
Discovered open port 22/tcp on 192.168.0.16
SYN Stealth Scan Timing: About 17.59% done; ETC: 14:04 (0:02:25
remaining)
SYN Stealth Scan Timing: About 53.44% done; ETC: 14:03 (0:00:53
remaining)
Completed SYN Stealth Scan at 14:03, 91.49s elapsed (65535 total
ports)
```

```
Nmap scan report for DESKTOP-A9IHJU9.hitronhub.home (192.168.0.16)
Host is up (0.0071s latency).
Not shown: 65532 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  closed http
443/tcp closed https
MAC Address: 94:E9:79:53:56:C7 (Liteon Technology)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 91.75 seconds
           Raw packets sent: 131138 (5.770MB) | Rcvd: 74 (2.952KB)
```