ASSIGNMENT 4: CMDS

# Get a root prompt

```
sudo -i
```

# Get the IP information

```
ifconfig -a
```

# Start SSH server

```
service ssh start
```

# What network ports are open?

```
netstat -tulpn
```

# Get host info on facebook

```
host -t a www.facebook.com
```

# Get the entire network for that single host

```
whois 69.171.228.40 | grep CIDR
```

# Drop everything to that network

```
iptables -A OUTPUT -p tcp -d 69.171.224.0/19 -j DROP
```

# Drop or Accept Traffic from a secific mac address

```
iptables -A INPUT -m mac --mac-source 00:0F:EA:91:04:08 -j DROP
```

# Change your own mac address at will

```
macchanger eth0
```

# host fake Facebook.com using python
# Be in the folder with the html files first

```
python -m SimpleHTTPServer 8080
```

# Redirect all incoming port 80 requests to 8080

```
iptables -t nat -I PREROUTING --src 0/0 --dst 192.168.1.5 -p tcp --dport 80 -j
REDIRECT --to-ports 8080
```

######################################
## Standard IPTABLES STUFF
# Check the deault policy chain behavior

```
sudo iptables -L | grep policy
```

# Check all existing rules

```
sudo iptables -L -n -v
```

# Check the current rules

```
sudo iptables -L
```

# Reset your iptables rules

```
sudo iptables -F
```

# Block all incoming requests

```
sudo iptables INPUT -j DROP
```

# Block a specific IP Address

```
sudo iptables -A INPUT -s [ip address] -j DROP
```

# Block all TCP requests from an IP

```
sudo iptables -A INPUT -p tcp -s [ip address] -j DROP
```

# Unblock an IP

```
sudo iptables -D INPUT -s [ip address] -j DROP
```

# Block IP Address Ranges

```
sudo iptables -A INPUT -s [ip address.0/24] -j DROP
```

# Unblck IP Address Ranges

```
sudo iptables -D INPUT -s [ip address.0/24] -j DROP
```

# Block all TCP requests for given IP Range

```
sudo iptables -A INPUT -p tcp -s [ip address.0/24] -j DROP
```

# Unblock all TCP requests for iven IP Range

```
sudo iptables -D INPUT -p tcp -s [ip address.0/24] -j DROP
```

# Replace ACCEPT with DROP to block port
## open port ssh tcp port 22 ##

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -s 192.168.1.0/24 -m state --states NEW -p tcp --dport 22 -j ACCEPT
```

## open cups (printing serive) udp/tcp port 631 for LAN users ##

```
iptables -A INPUT -s 192.168.1.0/24 -p udp -m udp --dport 631 -j ACCEPT
iptables -A INPUT -s 192.168.1.0/24 -p tcp -m tcp --dport 631 -j ACCEPT
```

# allow time sync via NTP for lan users (open udp port 123) #

```
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p udp --dport 123 -j ACCEPT
```

## open tcp port 25 (smtp) for all

```
iptables -A INPUT -m state --state NEW -p tcp --dport 25 -j ACCEPT
```

# open dns server ports for all

```
iptables -A INPUT -m state --state NEW -p udp --dport 53 -j ACCEPT
iptables -A INPUT -m state --state NEW -p tcp --dport 53 -j ACCEPT
```

# open http/https (Apache) server port to all

```
iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT
```

## open tcp port 110 (pop3) for all

```
iptables -A INPUT -m state --state NEW -p tcp --dport 110 -j ACCEPT
```

## open tcp port 143 (imap) for all

```
iptables -A INPUT -m state --state NEW -p tcp --dport 143 -j ACCEPT
```

## open access to Samba file server for lan users only

```
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 137 -j ACCEPT
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 138 -j ACCEPT
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 139 -j ACCEPT
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 445 -j ACCEPT
```

# open access to proxy server for lan usres only

```
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 3128 -j ACCEPT
```

# open access to mysql server for lan users only

```
iptables -I INPUT -p tcp --dport 3306 -j ACCEPT
```