Write scripts or statements to modifying firewall rules (IPtables) for specific purposes:

**1. Deal with web server (open needed ports, and forward port 80 traffic to 8080)**

Ensure ports 80 and 8080 are open and then run these commands:

iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -i eth0 -p tcp --dport 8080 -j ACCEPT

Then route traffic from the specified interface using:

iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080

2. **Deal with MySQL service (open needed ports)**

After googling what ports are used with MySQL, I can use these commands to complete:

iptables -A INPUT -p tcp --dport 3306 -j ACCEPT

iptables -A INPUT -p tcp --dport 33060 -j ACCEPT

**3. Deal with SSH service (allow incoming and outgoing SSH, second script to deny SSH)**

First, I must make sure the port is accepting traffic:

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

iptables -A OUTPUT -p tcp --dport 22 -j ACCEPT

Then I need to deny SSH, to do this I must change its status from ACCEPT to drop:

iptables -A INPUT -p tcp --dport 22 -j DROP

**4. Deal with Email service (Such as allow or block incoming SMTP,POP3...)**

In order to edit email services we must work with multiple ports, so we need to use the command *multiport*:

iptables -A INPUT -p tcp -m multiport --dports 25,110,143,993,995 -j ACCEPT

iptables -A INPUT -p tcp -m multiport --dports 25,110,143,993,995 -j DROP

**5. Script to allow/block specific hosts, MAC addresses, block telnet, block ping**

ALLOW HOST:

iptables -A INPUT -s "**SPECIFIED IP ADDRESS**" -j ACCEPT

iptables -A OUTPUT -d "**SPECIFIED IP ADDRESS**" -j ACCEPT

BLOCK HOST:

iptables -P INPUT -s "**SPECIFED IP ADDRESS**" -j DROP

iptables -P OUTPUT -s "**SPECIFED IP ADDRESS**" -j DROP

BLOCK PING:

iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

iptables -A OUTPUT -p icmp --icmp-type echo request -j DROP

BLOCK TELNET:

iptables -A INPUT -p tcp --dport 23 -j DROP

iptables -A OUTPUT -p tcp --dport 23 -j DROP

ALLOW MAC ADDRESS:

iptables -I INPUT -m mac --mac-source "**INSERT MAC ADDRESS**" -j ACCEPT

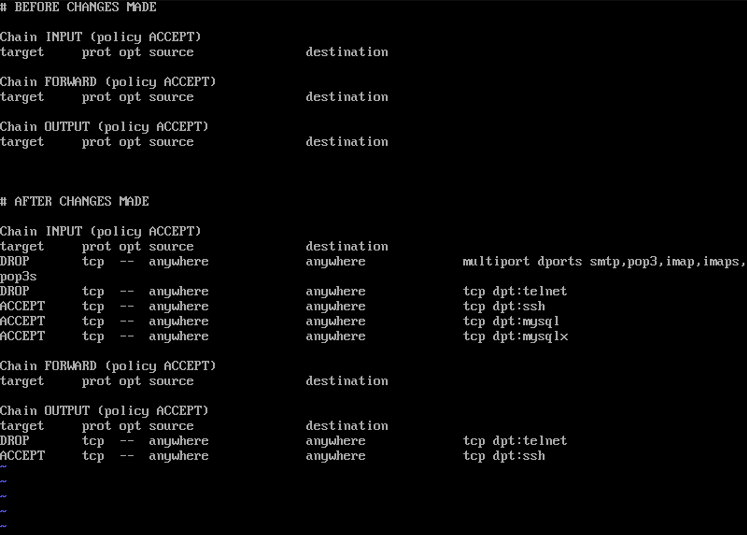
BLOCK MAC ADDRESS:

iptables -I INPUT -m mac --mac-source "**INSERT MAC ADDRESS**" -j REJECT

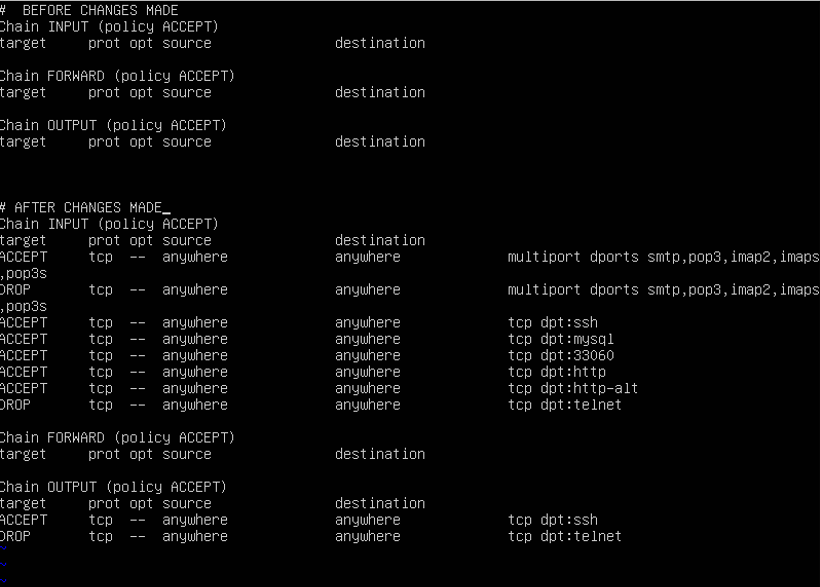
**6. Write a script to backup your Firewall/iptables**

iptables-save > /class/tables.backup

CENTOS:



UNBUNTU:



**Write the specs for how you think you could prevent a DDOS attack using IPtables.  Can you write a script for this?**

* Only having open ports that are being used
* Block traffic from IP addresses that are unknown
* Monitor traffic using Wireshark

<https://www.researchgate.net/publication/265181297_Mitigating_DoSDDoS_attacks_using_iptables>

<https://phoenixnap.com/blog/prevent-ddos-attacks>