Steve Cary

Firewalls: Linux Admin

4/5/2020

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

I chose the statements I have listed because they are simple and have been tested, so I know they work. Also, by doing them individually in this way instead of one full script, it helps me to learn the ports used by the different services or utilities included within the operating system. For the most part, my commands are all the same minus the port number. I simply state to accept or Drop/reject input/output from different ports.

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

First I make sure port 80 and 8080 are open to accept traffic:

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

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

To reroute the traffic from a specific interface (eth0), I can issue the following:

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

2. Deal with MySQL service (open needed ports)

I needed to perform a google search to find out what ports are used by MySQL service.

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)

To allow SSH traffic, I ensure the port is set correctly and open to accept traffic.

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

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

I also ensure that the "Port" variable is uncommented from /etc/ssh/ssh.config

To deny traffic, I can use the same syntax but change ACCEPT to DROP.

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

I also ensure that the "Port" variable is commented from /etc/ssh/ssh.config

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

Mail services use many ports, this command allows me to set the permissions on many ports at the same time.

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

To allow a specific host:

iptables -A INPUT -s "INSERT IP" -j ACCEPT

iptables -A OUTPUT -d "INSERT IP" -j ACCEPT

To block a specific host:

iptables -P INPUT -s "INSERT IP" -j DROP

iptables -P OUTPUT -s "INSERT IP" -j DROP

To allow a specific MAC address:

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

To block a specific host:

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

Block telnet:

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

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

6. Write a script to backup your Firewall/iptables

iptables-save > /class/iptables.backup

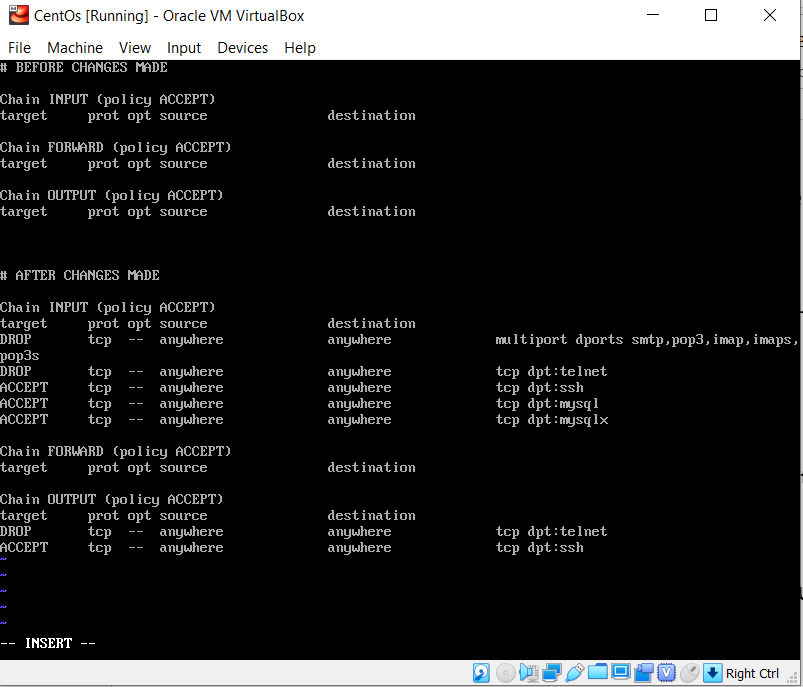
Use Wireshark to show that your statements/scripts are working properly.

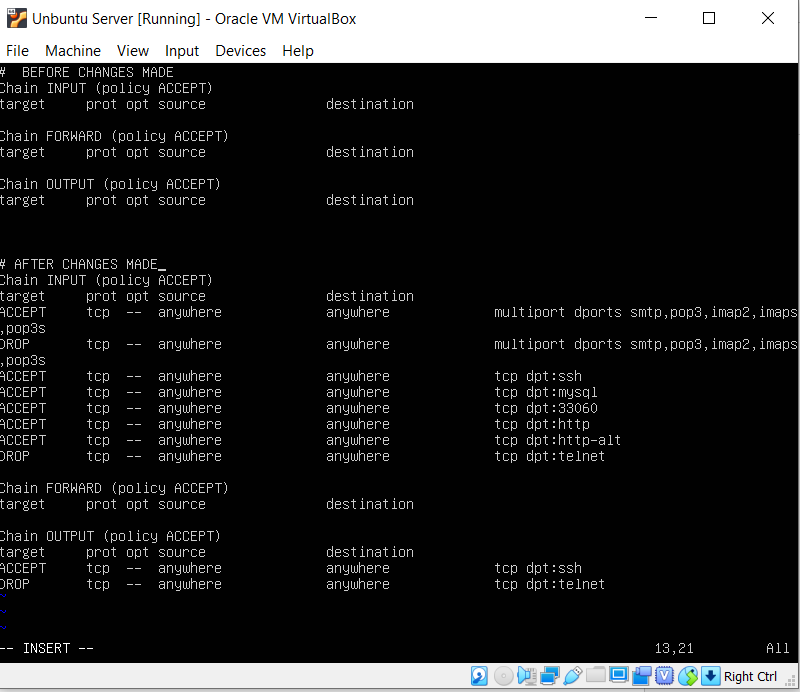
Due to using these VM's being on my work laptop I am unable to run wireshark, it just doesn't run properly and I am unable to see traffic on any of my interfaces, even those outside of my VM's. I've tried to troubleshoot this in class with Jay and others, but had no success.

For now, the firewalls are set up identically on my CentOS server and my Unbuntu server. I have allowed ssh traffic, and redirected the traffic to port 8080. I have opened the ports for the MySQL services. I have blocked telnet and disabled all mail related ports as I do not expect mail to be used on these virtual machines.

I did not block ping because I may need it going forward to test communication between my VM’s.

I plan to add the IP address and/or MAC address for each VM to ACCEPT both INPUT/OUTPUT.





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

To prevent a DDOS attack I would perform the following:

1. Block all incoming and outgoing traffic on all ports.

2. I would only open the ports I need.

3. Priority ports would have traffic redirected to other ports seldom used.

4. I would block all traffic from unknown IP addresses.

5. Monitor network traffic for suspicious activity using wireshark.

https://www.researchgate.net/publication/265181297\_Mitigating\_DoSDDoS\_attacks\_using\_iptables

https://www.researchgate.net/publication/265181297\_Mitigating\_DoSDDoS\_attacks\_using\_iptables