Nathan Christensen-Padilla

Adrianna Holden-Gouveia

Linux Administration

12/12/2021

Firewalls CentOS

I installed nmap so I could check my open ports but ended up using other methods.

Command: sudo yum install nmap

Text

Description automatically generated

Also I needed to install iptables services to get my iptables to work correctly.

Text

Description automatically generated

Lastly, I needed to install httpd:

Text

Description automatically generated

Then I started it and checked the status to make sure it is running.

Text

Description automatically generated

1. Deal with web server

Commands:

Ports 80 and 443 opened:

Port 80: sudo iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT

Port 443: sudo iptables -A INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT

Text

Description automatically generated

Port 80 redirected to port 8080:

sudo iptables -t nat -I PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080

sudo iptables -I INPUT -p tcp --dport 8080 -j ACCEPT

Text

Description automatically generated

Allow traffic for local interface and allow established connections:

sudo iptables -A INPUT -i lo -j ACCEPT

sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Text

Description automatically generated

Save Iptables (I do this after every question):

sudo service iptables save



Tried connecting to the ports:

:80

Application

Description automatically generated with medium confidence

:443Graphical user interface, application

Description automatically generated

I chose to use these commands because they allow me to use these ports when needed and it’s a relativly simple set of rules so it’s easy to keep track of. This deals with web server because it allows me to use both of the needed ports 443 and 80 to use in my server.

1. Deal with MySQL service

Commands:

Open port 3306:

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



Tried connecting to port 3306:

Graphical user interface, application

Description automatically generated

I choose to use this command because it opens up the port and allows access and because of it being lower down in the list it has to go through the other checks, so I think it’s fine. Also, this deals with MySQL service because it opened up the needed port for me to be able to use it.

1. Deal with SSH service

Command:

Allow incoming SSH connections:



Allow outgoing SSH connection response only if they are established:



Allow outgoing SSH connection requests:



Allow outgoing SSH connection responses if they are ESTABLISHED:



Connected to the server using SSH port 22 with the WinSCP app:

A screenshot of a computer

Description automatically generated

I chose to use these commands because it only allows me to connect to my server on the local network and I considered this dealing with SSH because it allows me to access my server and allows me to add or take files from the server as I please.

1. Deal with Email service

Command:



Tried connecting to each Email Service port list above:

Graphical user interface, application

Description automatically generated

My way of dealing with the Email service is to block all email ports because for my server I’m not going to be using it for email.

1. Script to allow/block specific hosts, MAC addresses

Command:

Allow my computer access using my MAC address:



Block my computers MAC address instead:



I chose to use these commands because I can use them to allow certain connections to go through and if I want to, I can block other ones. Also, I wasn’t too sure how to use Wireshark to show this, but I was still able to join my server with the first command enabled and then second one blocked me.

A computer screen capture

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

1. A script/command to block telnet, block ping

Block Telnet:



The reason I went with this command is because it blocks all traffic on port 23 which is what telnet uses.

Block ping:



I went with this script because it blocks icmp which is used for ping and it worked really well because as show in the picture below the ping worked at first but then I added the rule and then all my requests failed.

Graphical user interface, text, application

Description automatically generated

Original Iptables:

Graphical user interface, text, application

Description automatically generatedText

Description automatically generated

Iptables after:Text

Description automatically generatedA picture containing table

Description automatically generated

Sources:

[iptables: The Default Linux Firewall (opensourceforu.com)](https://www.opensourceforu.com/2015/04/iptables-the-default-linux-firewall/)

[Linux firewalls: What you need to know about iptables and firewalld | Opensource.com](https://opensource.com/article/18/9/linux-iptables-firewalld)

[Installing Telnet In CentOS/RHEL/Scientific Linux 6 & 7 | Unixmen](https://www.unixmen.com/installing-telnet-centosrhelscientific-linux-6-7/)

[❤ 💻 Linux - iptables redirect port 80 to 8080 - Dirask](https://dirask.com/posts/Linux-iptables-redirect-port-80-to-8080-pO7kwp)

<https://danielmiessler.com/blog/professional-firewall-iptables/>

[How To Install the Apache Web Server on CentOS 7 | DigitalOcean](https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-centos-7)

[How to Start/Stop and Enable/Disable FirewallD and Iptables Firewall in Linux (tecmint.com)](https://www.tecmint.com/start-stop-disable-enable-firewalld-iptables-firewall/)

<https://www.tecmint.com/linux-iptables-firewall-rules-examples-commands/>

[Linux IPTables: Incoming and Outgoing Rule Examples (SSH and HTTP) (thegeekstuff.com)](https://www.thegeekstuff.com/2011/03/iptables-inbound-and-outbound-rules/)

[Configure MAC based Filtering using Iptables in Linux (tecadmin.net)](https://tecadmin.net/mac-address-filtering-using-iptables/)

[How to Block Ping ICMP Requests to Linux Systems (tecmint.com)](https://www.tecmint.com/block-ping-icmp-requests-to-linux/)