Jayden Rios

00325523

Firewalls Lab

UBUNTU SERVER

To create the script file, enter touch Firewalls.sh

Give the script permissions with the command chmod +rwx Firewalls.sh

Use vi editor to write the script. vi Firewalls.sh

Single script file to complete tasks 1-5. All tasks descriptions have been commented before code.

A screenshot of a computer program

Description automatically generated

Run the script under sudo to allow permissions ./Firewalls.sh -ports have been changed as script depicts

A screenshot of a computer

Description automatically generated

To see default open ports, you could use command netstat -tuln

A screen shot of a computer

Description automatically generated

CENTOS SERVER

To create the script file, enter touch Firewalls.sh

Give the script permissions with the command chmod +rwx Firewalls.sh

Use vi editor to write the script. vi Firewalls.sh

Single script file to complete tasks 1-5. All tasks descriptions have been commented before code.

A screenshot of a computer

Description automatically generated

Run the script ./Firewalls.sh -Ports have been changed as scripts depicts.

A screenshot of a computer

Description automatically generated

To show iptables rule sets you would enter sudo iptables -S

Rules after the script is ran.(Table Changes)

A screenshot of a computer program

Description automatically generated

Rules before script is run. (Default)A screenshot of a computer

Description automatically generated

To see default open ports, you could use command netstat -tuln

A screen shot of a computer

Description automatically generated

WIRESHARK RESULTS – Script Works

Wireshark is a network protocol analyzer application that captures packets of data on a network connection, like a virtual machine, computer, or any device connected to your internet network. It can packet capture, filter data and visualize entire network conversations.

Ping results shown on Wireshark for Ubuntu machine before script ran.

A screenshot of a computer

Description automatically generated

Ping results shown on Wireshark for Ubuntu machine postscript being ran.

A screenshot of a computer

Description automatically generated

SSH Port opened Ubuntu (port 22)



Allowed Mac-Address Ubuntu



Denied Mac-Address Ubuntu



Blocked Address result (request timed out)

A black screen with white text

Description automatically generated

Ports 80 and 8080 opened for rerouting Ubuntu





A screenshot of a computer

Description automatically generated

Denied telnet connection Ubuntu



Ping results shown on Wireshark for CentOS machine before script ran.

A screenshot of a computer

Description automatically generated

Ping results shown on Wireshark for CentOS machine postscript being run.

A black screen with white text

Description automatically generated



SSH Port opened CentOS (port 22)



Allowed Mac-Address CentOS



Denied Mac-Address CentOS



Blocked Mac-Address (request timed out)

A black screen with white text

Description automatically generated

Ports 80 and 8080 opened for rerouting CentOS





A screenshot of a computer

Description automatically generated

Denied Telnet connection CentOS



To find your Virtual Machine on the Wireshark application you would need to find the Ip Address of your machine. To do this enter the ip addr command. You would then look under the section that says “inet”.

A screenshot of a computer program

Description automatically generated

“inet 192.168.159.132”

You would then look up the list of devices on your home network shown on the Wireshark home screen.

A screenshot of a computer

Description automatically generated

You would then find the corresponding VMWare device that has the correct Ip Address.



As you can see when pinging the destination of the networks both appear.

Iptables are a useful tool that can give ways to mitigate the effects of a DDOS attack. A DDOS attack is an illegal cybersecurity attack in which the attacker floods a server with internet traffic to prevent accessing services online. These attacks can last up to a day or more and cause harm to those in need of internet access. The host of a server can write a script giving rule sets that not only block certain ports off, they can also add a limit to certain types of traffic by blocking invalid packets or packets that aren’t syn (sent to create new tcp packets). They can also set a limit to tcp / icmp requests. By slowing down a numerous amount of requests by an attacker, and preventing traffic, the host can help mitigate the effects of a DDOS attack on a server.

Some commands in a script you can use to mitigate DDOS effects are:

Iptables -A INPUT -p tcp –syn -m limit –limit 2/s –limit-burst 30 -j ACCEPT

This sets a new rule to limit the rate of incoming TCP SYN packets to only 2 per second with a bursting limit of 30 to reduce traffic. Anything that exceeds this set limit will be dropped due to the new rule.

Iptables -t mangle -A PREROUTING -p tcp ! –syn -m conntrack –ctstate NEW -j DROP

This can be used to block any new incoming tcp packets that aren’t SYN. This rule can be used to mitigate TCP ddos attacks.

Using sets of rules such as the ones below can help hosts to set limits or deny connection. This can help stop DDOS attacks on a server.

To show iptables rule sets you would enter sudo iptables -S

Rules after the script is ran.(Table Changes)

A screenshot of a computer program

Description automatically generated

Rules before script is run. (Default)A screenshot of a computer

Description automatically generated

As seen in the scripts all changes made have been updated as of



Sources:

*Ip Tables*, www.aholdengouveia.name/LinuxAdmin/iptables.html. Accessed 4 Dec. 2023.

Tucakov, Dejan. “Iptables Tutorial: Ultimate Guide to Linux Firewall.” *Knowledge Base by phoenixNAP*, 12 Jan. 2023, phoenixnap.com/kb/iptables-tutorial-linux-firewall.

*What Is a Distributed Denial-of-Service (Ddos) Attack? - Cloudflare*, www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. Accessed 4 Dec. 2023.

GitHub link to script: <https://github.com/JaydenRios/JaydenRios/blob/main/firewalls.sh>