Firewall Testing

This exercise:

Scans a host for open ports

Configures host-based firewall rules using iptables

Open listening ports using python3 simple http server

Initial Scan.

We'll do a few things here. First, open two ssh sessions to your JagCloud instance. One session will be to run the simple http server and the other to administer your instancec. Next, scan your instance for a closed port, then open that port and scan it again. We will use TCP 1194 for this exercise. TCP 1194 was selected for two reasons. First, TCP 1194 is a default port for OpenVPN, and second that port has been permitted through the network VPN. As a result, you will be able to scan TCP 1194 from the Internet.

Determine the default policy for the iptables INPUT chain: sudo iptables -L INPUT

Port closed: Scan your JagCloud instance for TCP 1194: nmap -p 1194 jagcloud-public-IP

Start the python3 simple http server on TCP 1194: python3 -m http.server 1194

Port open: Scan your JagCloud instance for TCP 1194.

Explain the default policy for the INPUT chain and compare results from the two scans.

Block Traffic to One Port from all Sources.

Next, block inbound traffic to TCP 1194 from all sources, but with a twist. Use a script to craft your firewall rules. Using a script gives us better control over the order of rules, and order matters.

#!/bin/bash

IPT='/usr/bin/sudo /sbin/iptables'

# Show detailed info. -L / list -v / verbose -n / use numbers instead of common names

# $IPT -L -v -n --line-numbers

# Flush/reset INPUT

printf "\nFlushing INPUT chain ($IPT -F INPUT)...\n"

$IPT -F INPUT

printf "\nAdding rules to INPUT chain...\n"

# The following command insert (-I) a rule in line 1 of the INPUT chain that DROPs packets with destination port TCP 1194

$IPT -I INPUT 1 -p tcp --destination-port 1194 -j DROP

# List the rules in the INPUT chain

$IPT -L INPUT -n -v --line-numbers

Create the above script in your JagCloud instance and run the script.

Scan TCP 1194 again and observe the results.

Allow Traffic from LAN (local subnet).

Modify the script from the previous step to allow packets to TCP 1194 from your internal IP address range and update your iptables firewall.

Scan TCP 1194 from the internet.

Create a second GCP instance and install nmap, create a GCP firewall rule to allow all protocols within your VPC. Scan your original instance from the new instance (your scanner).

Stop the scanner GCP instance when you have completed the scans.

Submission:

Identify the default policy for the INPUT chain and explain what that default policy does. Describe the results from the two initial scans.

Describe the results from the scan after TCP 1194 was blocked from all sources.

Describe the results from the final scan after iptables has been modified to allow traffic from your internal IP address range but block traffic to that port from all other sources.

Submit your final script to configure iptables.