Caleb Javier

Professor Holden-Gouveia

CIS-245

27 October 2024

Assignment 7: Firewalls and IP Tables

This documentation will prepare learners to engage with IPTables in their servers (red hat or ubuntu), ensuring that they are able to change chains, write scripts to enable firewall setups after reboot, and allow/block specific hosts or MAC addresses. Sudo permissions are needed for this task.

1. **Managing IPTables for an Ubuntu Server**
   1. **Deal with web server**

Firstly ensure that port 80 has allowed traffic.



Next, allow port 8080 to receive traffic by using the same command:



Then, forward all traffic from port 80 to 8080 by using a NAT rule:



Because the rules are not saved after a reboot, they can be saved in a new file for reuse.

creates the file, where

 will save the newly created rules to that file. A script will be made later in order to reapply the rules.

When removing rules, the user can use -D INPUT instead of -A to delete them.

* 1. **Deal with MySQL service**

To access the MySQL service, port 3306 must be opened. This can be done similarly to above by opening the port and then ensuring that it is able to receive traffic, like so:



And then:



Should no errors occur, this has been properly dealt with.

* 1. **Deal with SSH service**

The port for SSH traffic is 22, so again, rules will be created for that port. This time for both input and output.



The script is as follows:

#!/bin/bash

#Deny al incoming packets

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

#Deny all outgoing packets

sudo iptables -A OUTPUT -p tcp --dport 22 -j DROP

#Review settings changes

sudo iptables-save

* 1. **Script to allow/block specific hosts**
  2. **Scripts/commands to block telnet and ping**