**Solution Guide: Testing Firewall Rules with Nmap**

The goal of this activity was to practice using Nmap to test your firewall's defenses. You used some of the scan types most commonly used by attackers to identify the strength and weaknesses of your firewalls.

**Note:** In these examples we will be using the IP address 172.17.18.72. However, the IP address of your UFW machine will be different. Make sure to substitute your machine's IP address whenever you see 172.17.18.72.

Log into your UFW VM and firewalld VM with the credentials provided. firewalld will serve as your attack machine for this activity, and UFW as the victim.

Set up your test environment. Type the following commands in your UFW VM:

* sudo ufw reset
* sudo ufw enable
* sudo ufw default deny incoming
* sudo ufw default deny outgoing
* sudo ufw allow 80
* sudo ufw allow 22
* sudo ufw allow 443

From your firewalld VM, perform a basic Nmap scan against the UFW machine to help you determine whether the system is alive or not:

* nmap 172.17.18.72
* Which ports are open and what are their associated protocols and service types?
  + port 22/tcp ssh, port 80/tcp http, port 443/tcp https

Run the command that returns results that include service and daemon type:

* sudo nmap -sV 172.17.18.72
* What versions are returned in the results if any?
* 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
* 80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

443/tcp closed http

* Why was Nmap able to enumerate these services?
  + Because the ports are open and active.

With the ufw firewall still enabled, type the command that performs OS detection and service detection using fast execution.

* $ sudo nmap -A -T4 172.17.18.72
* Was this nmap scan able to determine which distribution of Linux is running on the host and if so, which one?
  + Yes, Ubuntu
* Was this nmap scan able to return an exact match for the OS on the host?
  + No, the nmap scan returned "No exact OS matches for host (test conditions non-ideal)".

Run uname -a.

* Does the currently installed version of Linux match any of the version within the "Aggressive OS guesses" section of the nmap scan?
  + No.

Run the Nmap command that will determine whether or not a firewall is stateful:

* sudo nmap -sA 172.17.18.72
* What are the port states?
  + Unfiltered.
* What type of firewall is being used and at which layer of the OSI model does it operate?
  + The firewall is stateful, and operates at OSI Layers 3 and 4.

**Bonus**

* What is a SYN scan and what is its primary benefit, from a hacking perspective?
  + The TCP SYN scan, also known as “half-connect scan” sends a SYN packet to the victim. This scan is beneficial from a hacking perspective because of its stealth, since it does not complete the TCP three-way handshake.
* What are the three possible responses of a SYN Scan and what do they mean?
  + SYN/ACK: Port is open, meaning the attacker can use this port.
  + RST: The port is closed.
  + No response: The port is filtered, meaning there’s a firewall protecting it. The port is most likely open but is protected by the firewall.