**NMAP Lab**

991451344

Professor: Sebastian Maniak

Timothy Pang

**Introduction**

In this lab, we are tasked with using nmap to identify target machines by sweeping through a network range, to specify port ranges in nmap and analyze the nmap-services file to determine more popular ports as well as to conduct TCP port scanning and analyze the difference between the two.

**Initial Scan**

**What does -n do? :**

According to the options summary, -n means never do DNS resolution.

**What does -sP do? :**

Looking at the output without -sP, -sP is for condensing the packet trace information to each ip from 1 – 255, as well as it shows the host information for the networks that are up.

**How many hosts do you see online? :**

**Text

Description automatically generated**

Figure 1.

There are a total of 5 hosts online.

**Scanning Linux (Vulnerable host)**

**How long did the scan take? :**

The scan took 0.08 seconds.

**What ports did you discover? :**

Discovered ports 21,22,23,80,111,2049 and 8080.

Text

Description automatically generated

Figure 2.

**What ports/services have you discovered? :**

Running sudo nmap -n -sT 10.200.2.59 -p 1-65535

Text

Description automatically generated

Figure 3.

Ports discovered and their services were:

* Port 21 / ftp
* Port 22 / ssh
* Port 23 / telnet
* Port 80 / http
* Port 111 / rpcbind
* Port 2049 / nfs
* Port 8080 / http-proxy
* Port 20048 / unknown
* Port 32799 / unknown
* Port 44595 / unknown

**Output Formats**

Text

Description automatically generated

Figure 4.

**Using Vi :**

Text

Description automatically generated

Figure 5.

**Execute grep :**

Text

Description automatically generated

Figure 6.

**Port Scans**

**Port Zero tcpdump and the packets :**

A screenshot of a computer

Description automatically generated with medium confidence

Figure 7.

On the tcpdump there are no changes however because port 0 is closed and you can’t connect to it, it is considered invalid.

**Command that scans ports :**

Text

Description automatically generated

Figure 8.

**AWS Environment**

Text

Description automatically generated

Figure 9.