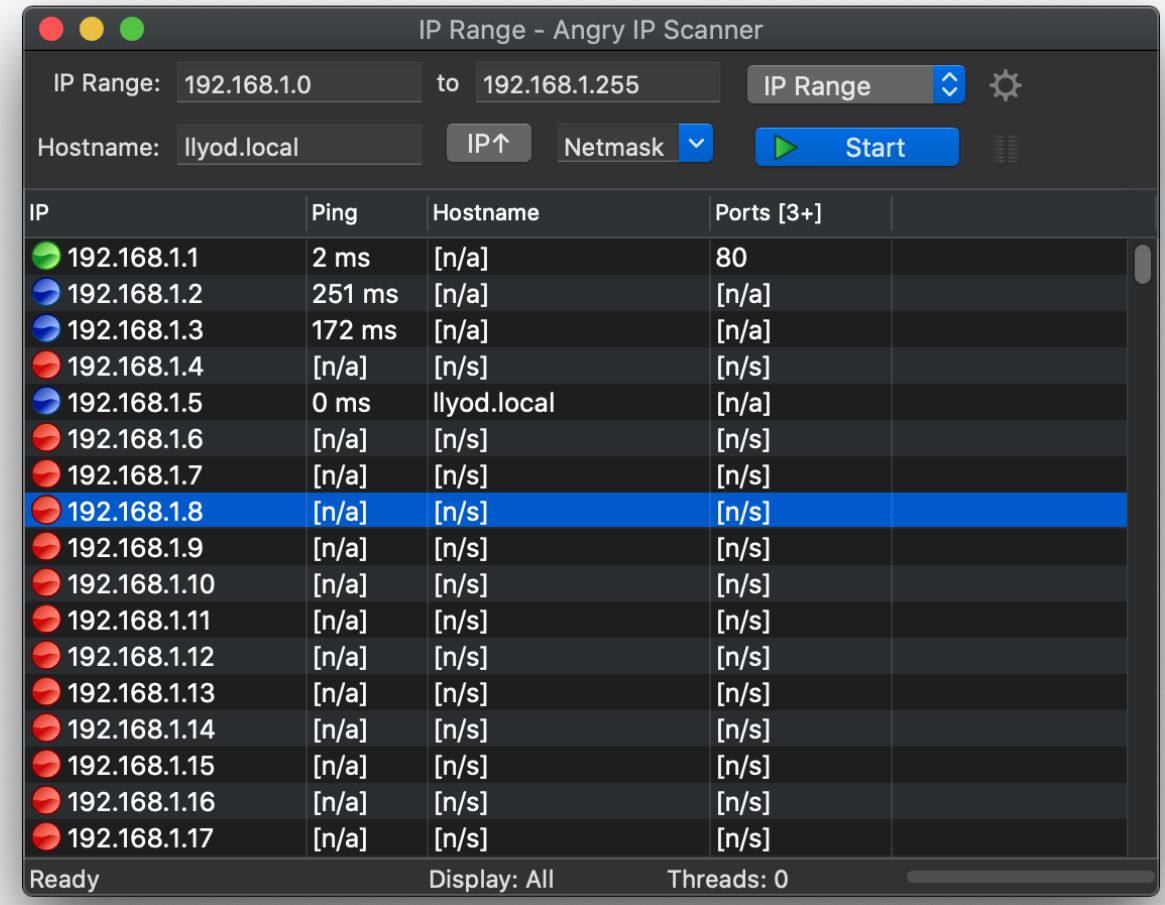
Lab Homework 4

Elijah Luckey

Sept. 28, 2020

A Ping Sweeping



Port Scanning

1.

```
eluckey@llyod: ~

~
▶ nmap -T5 -sP 192.168.0.0-255
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 21:23 EDT
Nmap scan report for 192.168.0.1
Host is up (0.010s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 2.51 seconds

~
▶
```

2.

```
eluckey@llyod: ~

~
▶ sudo nmap -T5 -sN 192.168.0.0-255
Password:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 21:29 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0059s latency).
All 1000 scanned ports on 192.168.0.1 are open|filtered

Nmap done: 256 IP addresses (1 host up) scanned in 13.56 seconds

~
▶
```

3.

```
eluckey@llyod: ~
~
▶ sudo nmap -T5 -sX 192.168.0.0-255
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 21:31 EDT
Nmap scan report for 192.168.0.1
Host is up (0.031s latency).
All 1000 scanned ports on 192.168.0.1 are open|filtered

Nmap done: 256 IP addresses (1 host up) scanned in 32.22 seconds

~
▶
```

4.

```
eluckey@llyod: ~
~
▶ sudo nmap -T5 -sT 192.168.0.0-255
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 21:34 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0099s latency).
Not shown: 998 filtered ports
PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap done: 256 IP addresses (1 host up) scanned in 14.33 seconds

~
▶
```

Packet Crafting

```
eluckey@kali:~$ sudo hping3 --spoof 192.168.1.1 -c 3 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): NO FLAGS are set, 40 headers, 0 data bytes

--- 192.168.1.1 hping statistic ---
3 packets transmitted,  packets received, 100% packet loss
round-trip man/avg/max = 0.0/0.0/0.0 ms
eluckey@kali:~$
```

Discussion

Using these tools (`nmap`, `Angry IP Scanner`, and `hping`) can prove useful for testing network insecurities for local systems. In this experiment, we didn't necessarily find any insecurities (since the connected devices

are limited in number on the local network) but can see where each instance of the tools can be useful. The *Angry IP Scanner* and `nmap` tools both showed `port 80` to be filtered/open in the experiment. Each of those tools can provide very wide scans on teh network to reveal more open and even vulnerable ports.