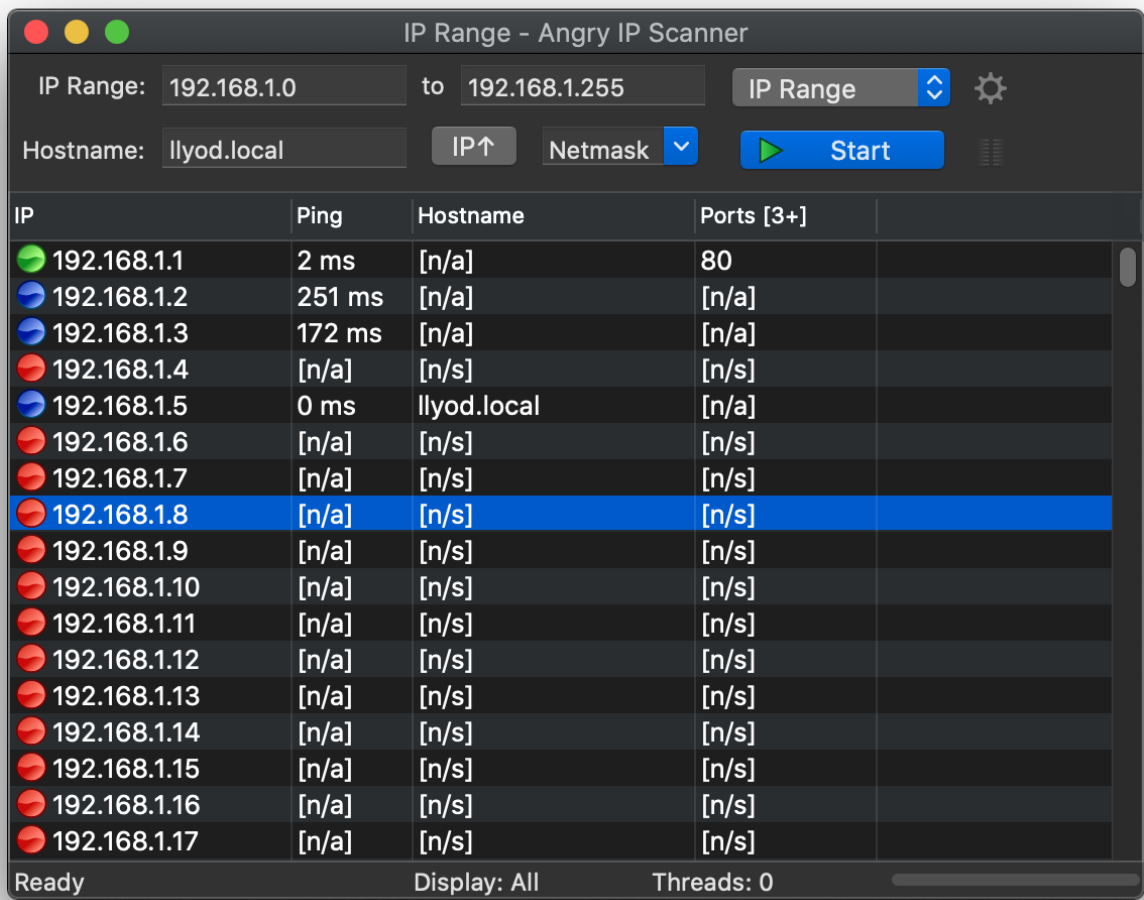


Lab Homework 4

Elijah Luckey

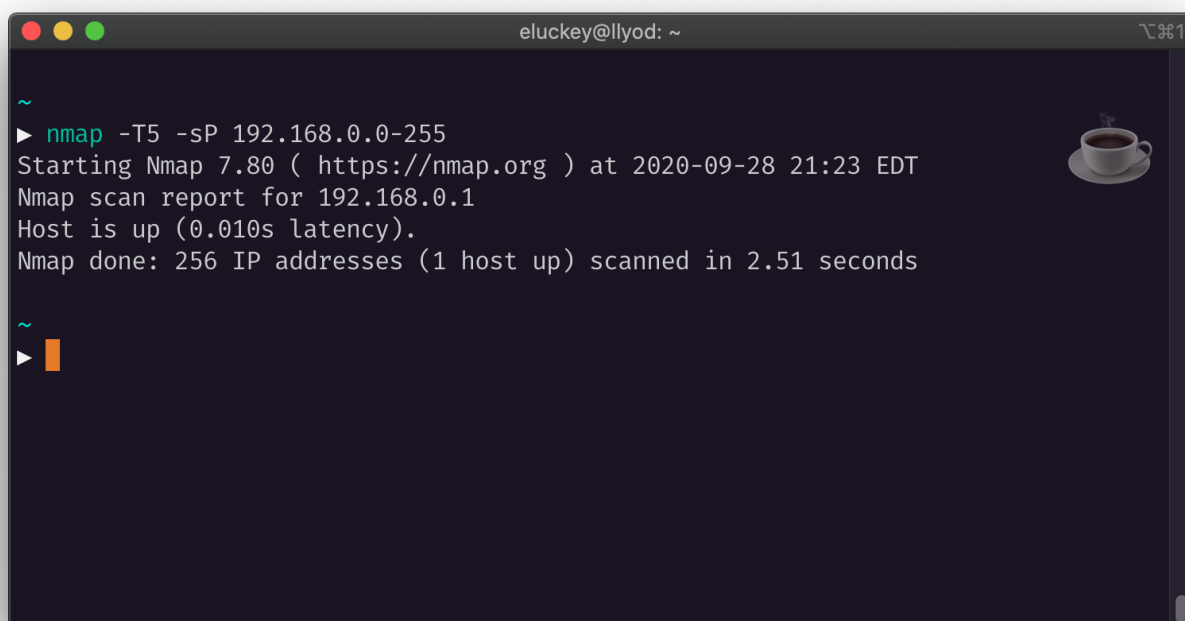
Sept. 28, 2020

A Ping Sweeping



Port Scanning

1.

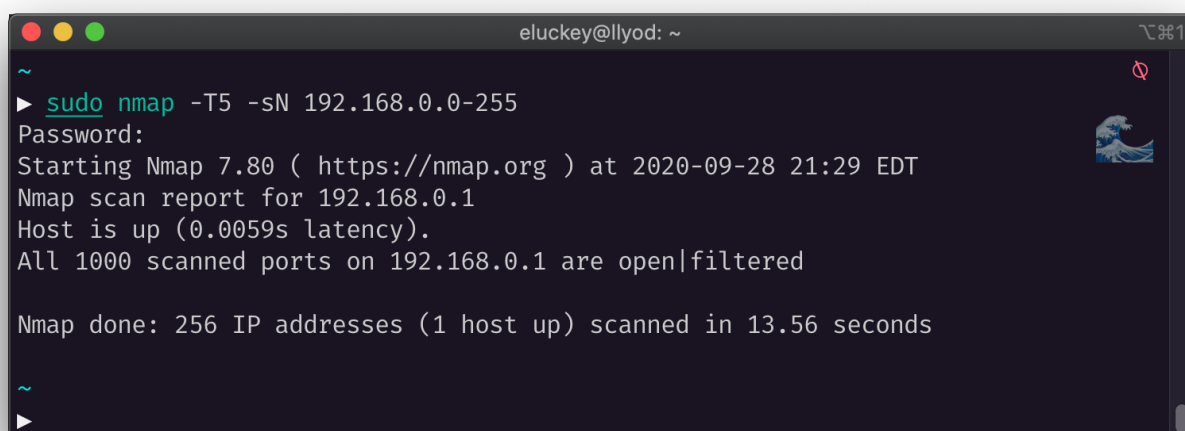


A terminal window titled 'eluckey@llyod: ~' with standard macOS window controls. The terminal shows the execution of 'nmap -T5 -sP 192.168.0.0-255'. The output indicates that Nmap 7.80 was started at 2020-09-28 21:23 EDT, scanned 192.168.0.1, and found it up with a latency of 0.010s. A total of 256 IP addresses were scanned in 2.51 seconds. A small coffee cup icon is visible in the top right corner of the terminal window.

```
~
▶ 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.



A terminal window titled 'eluckey@llyod: ~' with standard macOS window controls. The terminal shows the execution of 'sudo nmap -T5 -sN 192.168.0.0-255'. The output indicates that Nmap 7.80 was started at 2020-09-28 21:29 EDT, scanned 192.168.0.1, and found it up with a latency of 0.0059s. All 1000 scanned ports on 192.168.0.1 are open|filtered. A total of 256 IP addresses were scanned in 13.56 seconds. A small wave icon is visible in the top right corner of the terminal window.

```
~
▶ 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 min/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 the network to reveal more open and even vulnerable ports.