CIS4204.01 **Brandon Thompson**
Dr. Ashokkumar Patel Due: 2/20/21

Lab Homework 3: Ping sweeping, Port scanning, and Packet crafting

A: Ping Sweeping

Ping sweep using angry IP of my home network.

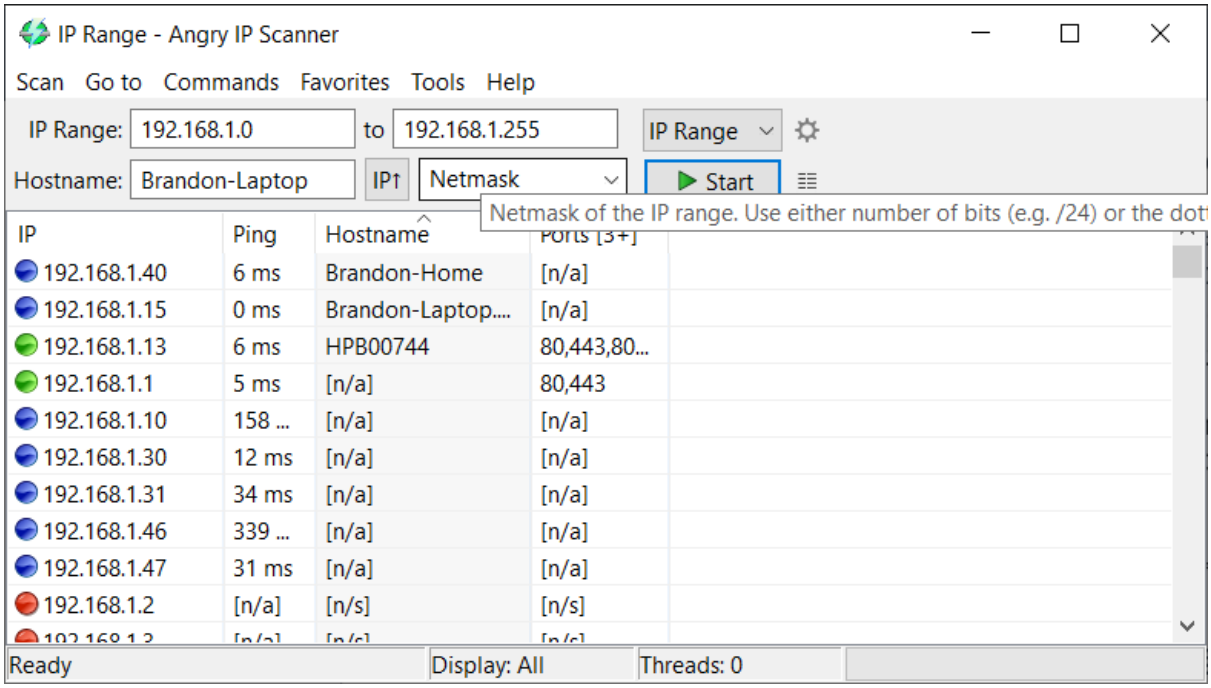

Figure 1: Angry IP output.

The output of Angry IP shows that the devices connected to the network that respond to pings and if some specified ports are opened.

B: Port Scanning

Using the Zenmap tool I scanned Florida Poly's IP address using `SYN` scan, `NULL` scan, `XMAS` scan and a Connection scan.

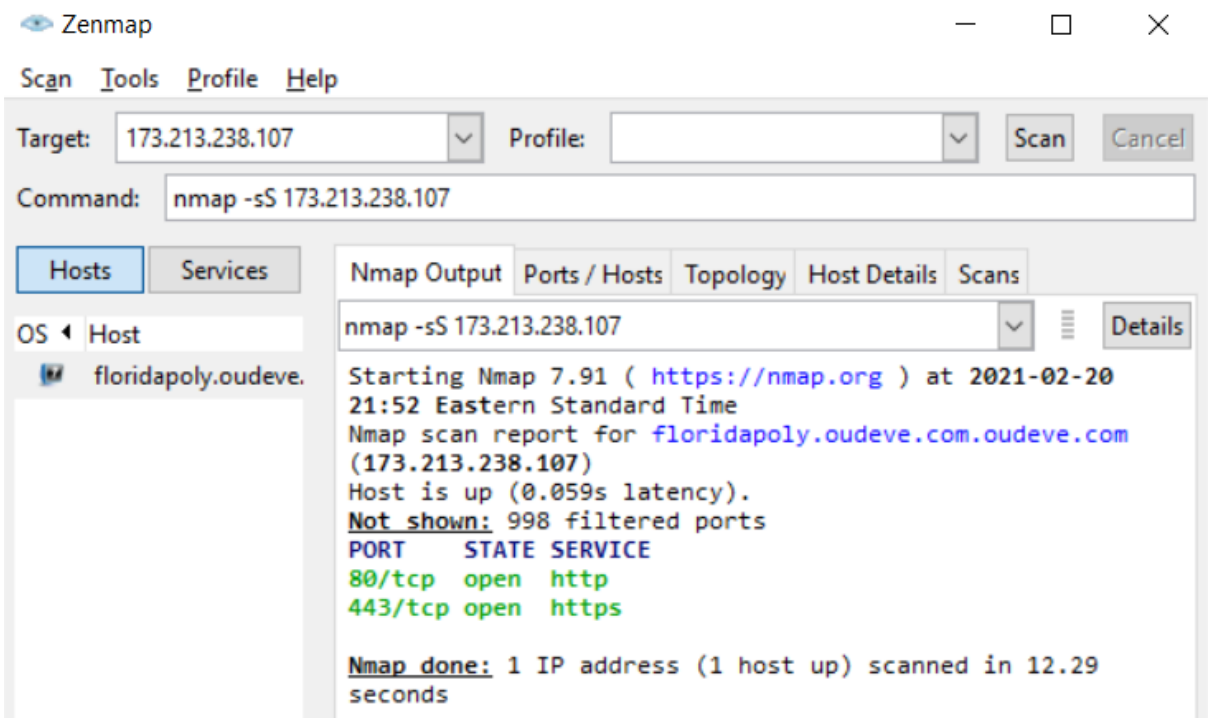

Figure 2: Zenmap output of SYN scan.

Half connect scan shows open ports via TCP but does not send the final ACK packet. This scan tends to be faster and is less likely to be logged than the full connection scan.

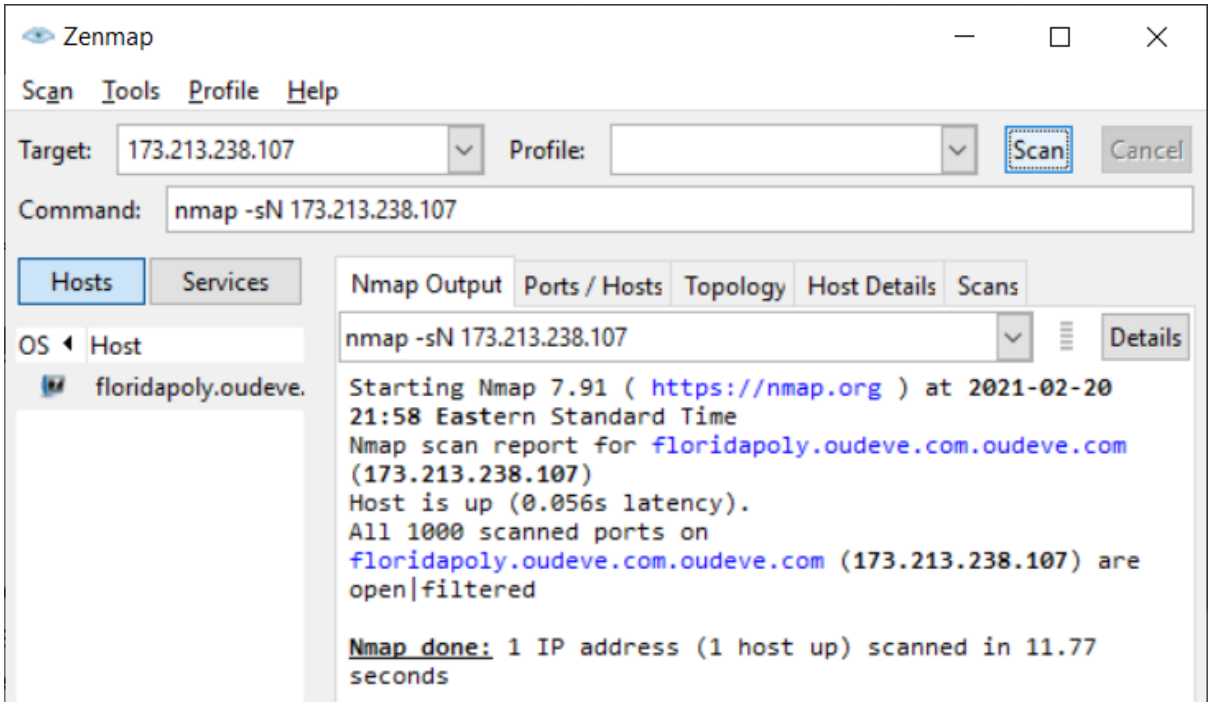

Figure 3: Zenmap output of NULL scan.

This scan sends packets with no flags enabled. Very clearly defines if ports are opened or closed.

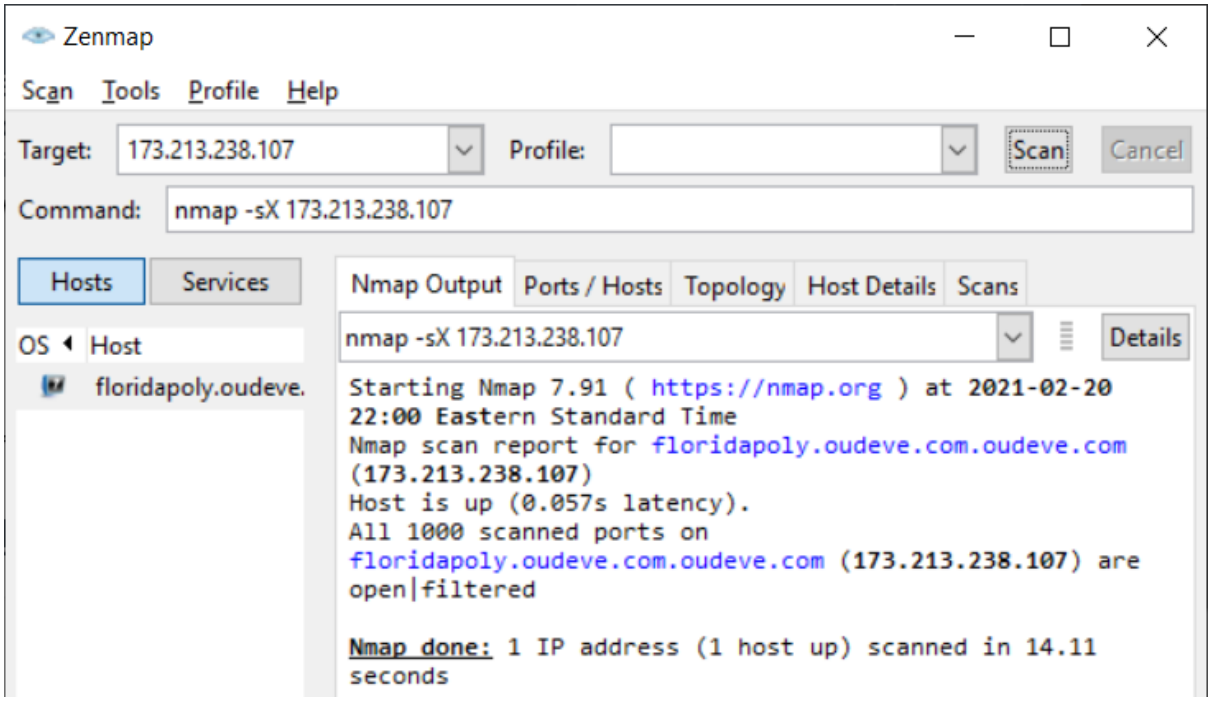

Figure 4: Zenmap output of XMAS scan.

This scan sends packets with multiple flags enabled. If there is no response from the target it typically means that the port is open.

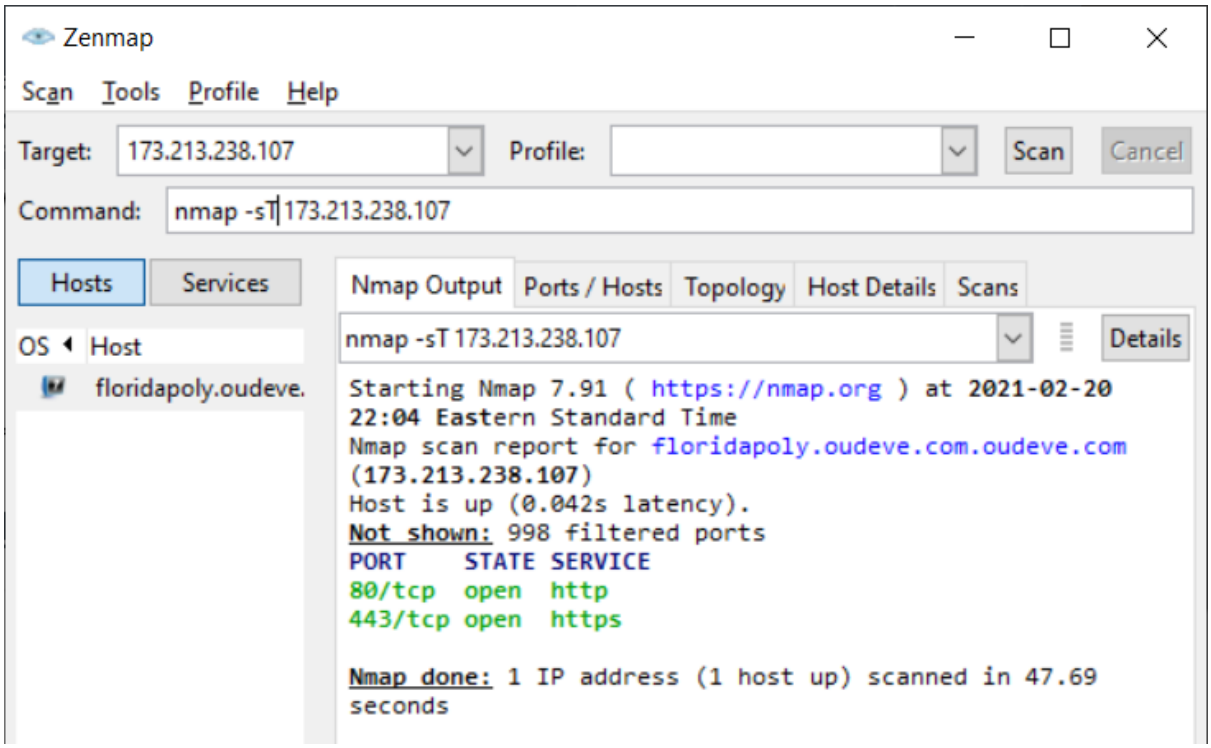

Figure 5: Zenmap output of full connect scan

The Full connect scan identifies open ports via a completed TCP handshake. This scan is more likely to be logged.

C: Packet Crafting

Kali Linux's `hping3` tool is used to craft a packet and receive a response from the target.

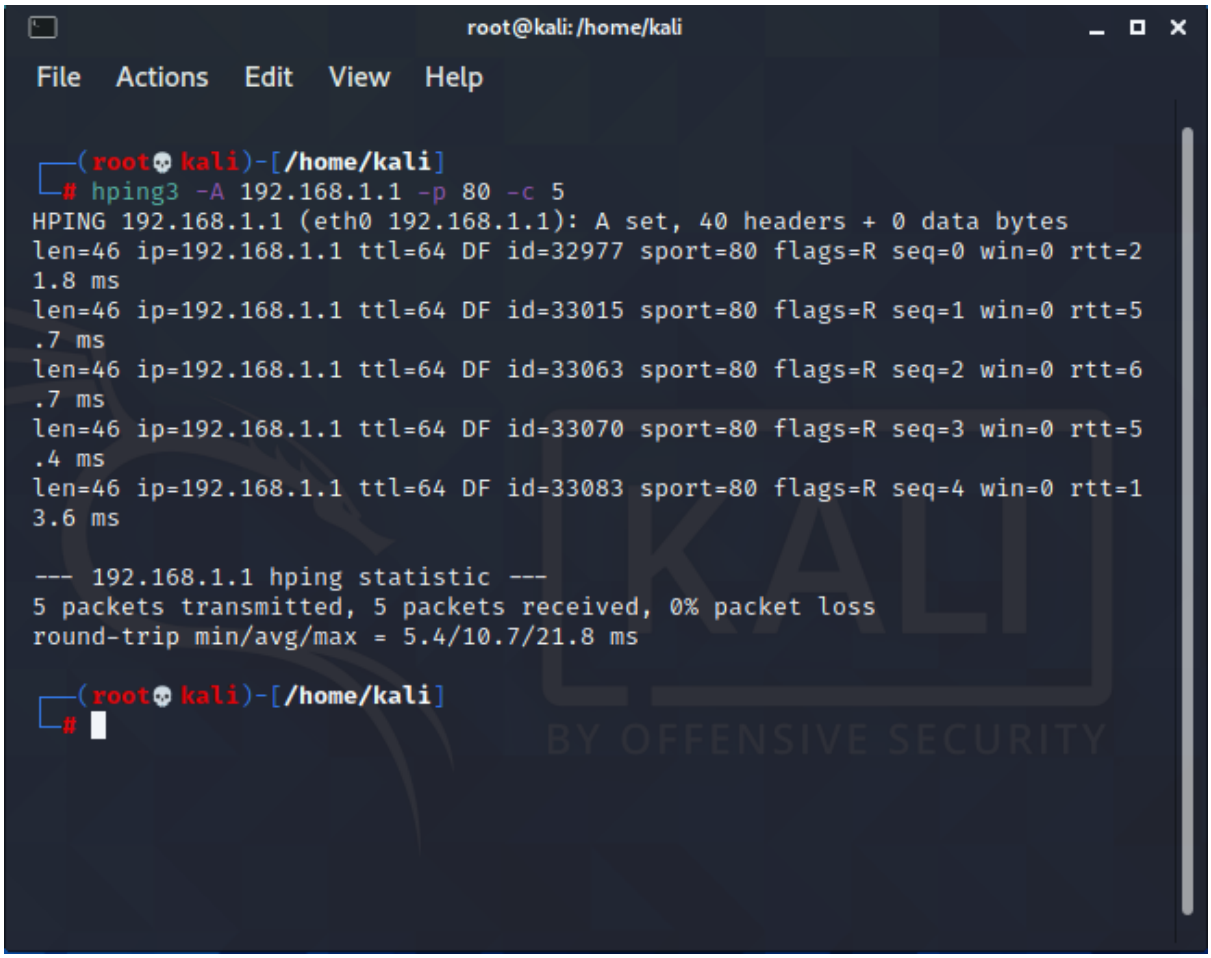

Figure 6: Hping3 with ACK scan on port 80.

In this lab we used network scanning tools to show devices on the network, ports that are open on devices and crafting packets. This is the process of scanning a network to discover the structure of the network and connected hosts. The Angry IP scan shows devices on the network that are available and online. Zenmap scans a specific IP for open ports using a variety of different scanning types meant to trick the system into giving a response despite a firewall or other countermeasure. Lastly, Kali Linux's Hping3 tool crafts a packet to send to an IP with the ability to specify flags.