Project 3: Network Attacks & Defenses

1. Nmap Port Scanning

Idea: Want to probe which ports are open on our target machine (victim server). Ran the nmap command below on the target machine `scanme.nmap.org`. The scan took 11 minutes over throttled stanford network. The output is shown in Figure 1.

```
sudo nmap -sS -A -T4 -p0-65535 scanme.nmap.org
```

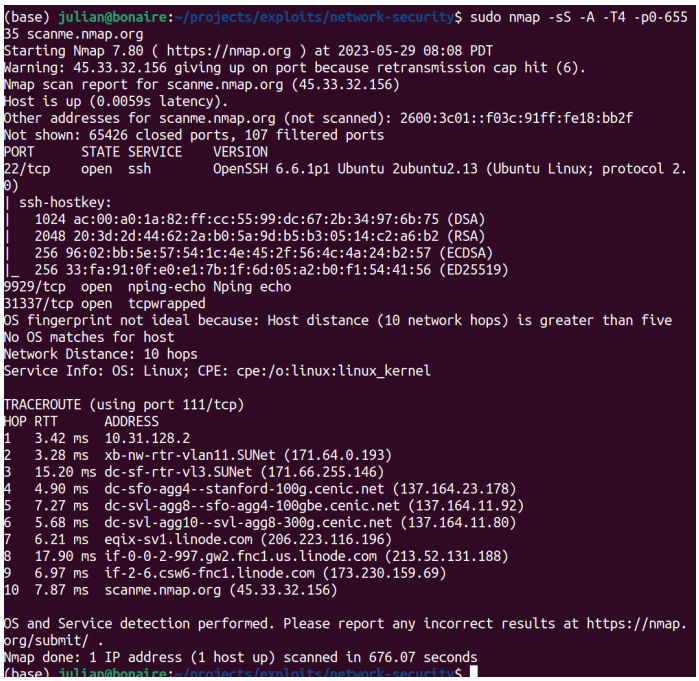

Figure 1: nmap console output

Working notes:

- Flags used: sS = TCP SYN scan; -A = OS detection (-O), version detetction (-sV), script scanning (-sC), traceroute (–traceroute); T4 = quick scan; -p0-65535 = expand scan from top 1000 to all ports
- Relevant websites: `https://nmap.org/book/man-version-detection.html` and `https://nmap.org/book/man-port-scanning-techniques.html`

2. Wireshark Packet Sniffing

Idea: Wireshark is a tool to monitor local network traffic.

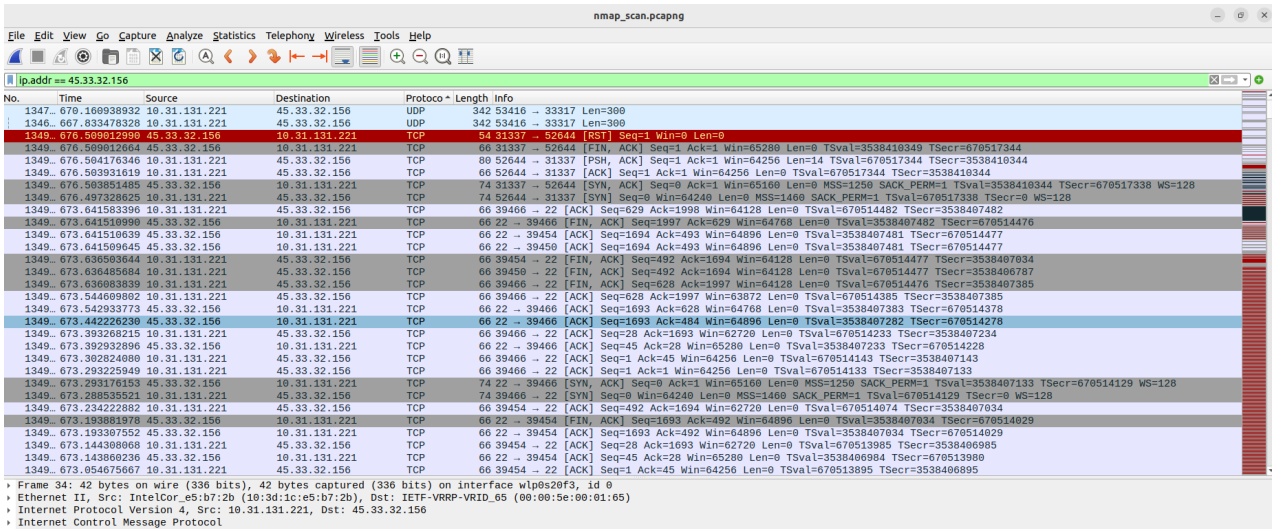

Figure 2: wireshark gui output

Working notes:

- xx
- xx