

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
```

```
(base) julian@bonaire:~/projects/exploits/network-security$ sudo nmap -sS -A -T4 -p0-65535 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-29 08:08 PDT
Warning: 45.33.32.156 giving up on port because retransmission cap hit (6).
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0059s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 65426 closed ports, 107 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
| 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
| 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
OS fingerprint not ideal because: Host distance (10 network hops) is greater than five
No OS matches for host
Network Distance: 10 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 111/tcp)
HOP RTT ADDRESS
1 3.42 ms 10.31.128.2
2 3.28 ms xb-nw-rtr-vlan11.SUNet (171.64.0.193)
3 15.20 ms dc-sf-rtr-vl3.SUNet (171.66.255.146)
4 4.90 ms dc-sfo-agg4--stanford-100g.cenic.net (137.164.23.178)
5 7.27 ms dc-svl-agg8--sfo-agg4-100gbe.cenic.net (137.164.11.92)
6 5.68 ms dc-svl-agg10--svl-agg8-300g.cenic.net (137.164.11.80)
7 6.21 ms eqix-sv1.linode.com (206.223.116.196)
8 17.90 ms if-0-0-2-997.gw2.fnc1.us.linode.com (213.52.131.188)
9 6.97 ms if-2-6.csw6-fnc1.linode.com (173.230.159.69)
10 7.87 ms scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 676.07 seconds
(base) julian@bonaire:~/projects/exploits/network-security$
```

Figure 1: nmap console output

Working notes:

- Flags used: `sS` = TCP SYN scan; `-A` = OS detection (`-O`), version detection (`-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.

JULIAN COOPER

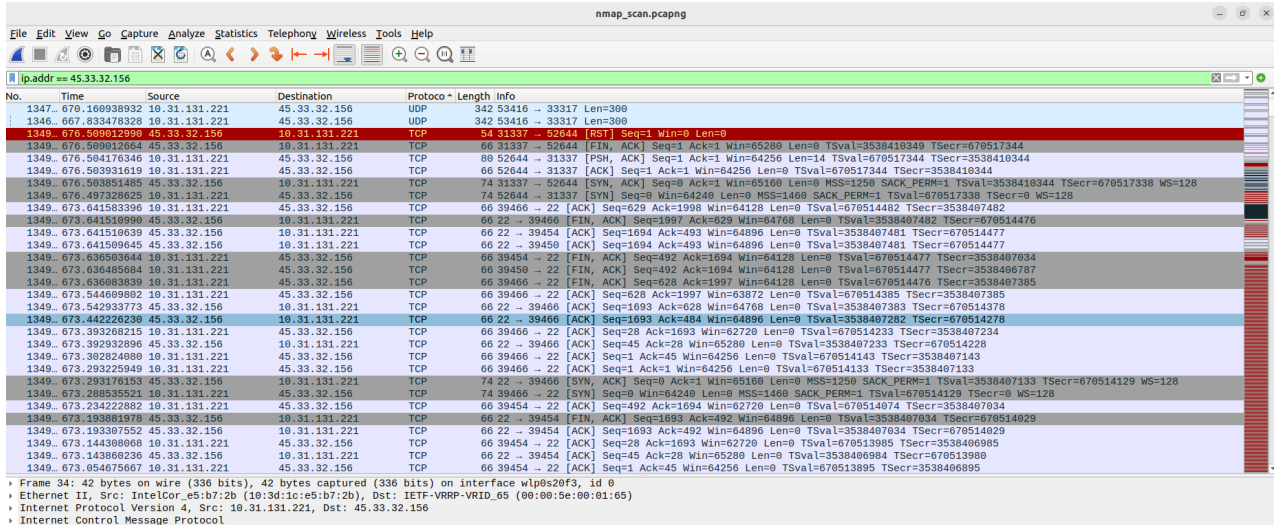


Figure 2: wireshark gui output

Working notes:

- XX
- XX