ITSY 1300 – Intro to Cybersecurity
Fundamentals of Information Security: Cybersecurity (88252)
Security Lab 2 – NMAP Port Scan
Exercise 1 – NMAP Introduction & Install

Ana Herrera Flores

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Nmap was named “Security Product of the Year” by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest. It was even featured in twelve movies, including The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, and The Bourne Ultimatum.

WEBSITE: https://nmap.org/

1. Review NMAP’s website and answer the following questions:
a. What is NMAP?
Nmap is a free and open-source tool used in networking and security. You can use it to find open ports for networking and vulnerabilities in security.

b. How can using NMAP help security staff?
Nmap scans the network for available hosts, services, operating systems, firewalls are in use, open ports and other characteristics that can help security staff to find vulnerabilities in the network and proceed to protect this one.

c. Describe some of the key features of NMAP.

Port Scanning: Nmap can identify open ports on target hosts to determine what services are running.
OS detection: Nmap can identify the OS running on the target host.
Vulnerability Detection: Nmap can help to detect known vulnerabilities in the system.
Service and Version Identification: Nmap can identify outdated software running on open ports, which is fundamental for security.

2. Download and install NMAP to your Desktop
a. https://nmap.org/download.html
3. Use the Latest Stable release and Latest Npcap.
Done

ITSY 1300 – Lab 2
Exercise 2 – Scanning with NMAP

In this exercise, we will Scan local computers.
Compile a report with the following information:

a. What is the O/S type & version?
Microsoft Window 10 1607 – 11 23H2

b. What does traceroute show?
It shows the route and the time taken to reach each hop.

i. What is traceroute?
A command that allows you to see communication from router to router until it reaches the final destination.

c. What is the webserver version?
I don't have a webserver. Window 11 (home) doesn't come with one by default and I have not installed one.

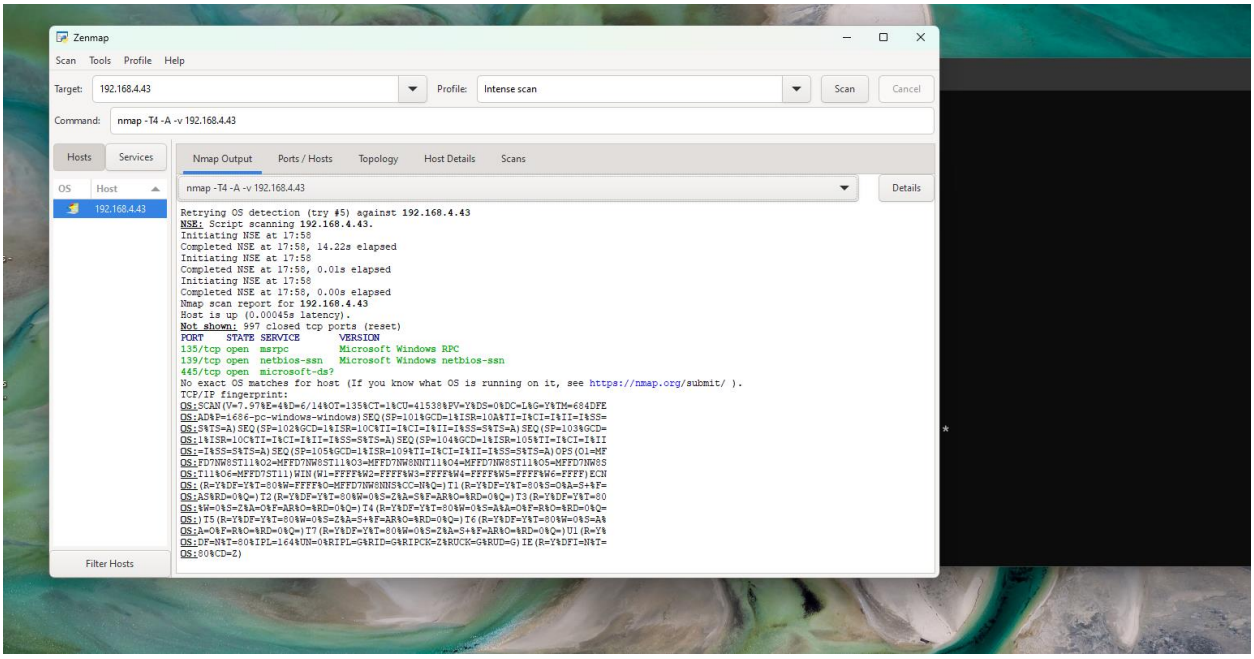
d. What ports are available?
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?

i. Describe the Ports. (Ie….what port numbers and what do they do)

Port 135: when labeled “msrpc” indicates the presence of RPC on a Window system. RCP allows applications on different computers to communicate and execute procedures on each other.
Port 139: indicates that the system is running NetBIOS Session Service; this is used for file and printer sharing.
Port 445: primally used for Server Message Block protocol (SMB), enabling file and printer sharing on Windows networks. It also plays a role in Microsoft Active Directory in network resources management. Leaving this port open to the public Internet is not recommended because it exposes your network to various attacks.

e. Describe what additional information is provided by NMAP.
OS Detection and Information
NSE Script Scanning
Host information
Ports
Vulnerability Detection

f. Provide a screenshot of the scan.



2. Scan your Home Network, including your own computer.
a. This works better if you have more than one device on your network.
Done

3. Compile a report on one of your devices with the following information:
a. What is the O/S type & version?

Apple macOS 11 (Big Sur) - 13 (Ventura)

b. What ports are available?
5000 tcp open rtsp
7000 tcp open rtsp

i. Describe the Ports. (Ie….what port numbers and what do they do)
Port 5000 and Port 7000: are both used in RTSP (Real-Time Streaming Protocol) used to control multimedia streaming sessions over IP networks. The default port is 554 and 5000/7000 are customed setting.

c. What is the hostname?
Mauras – MacBook Air
(192.168.4.69)

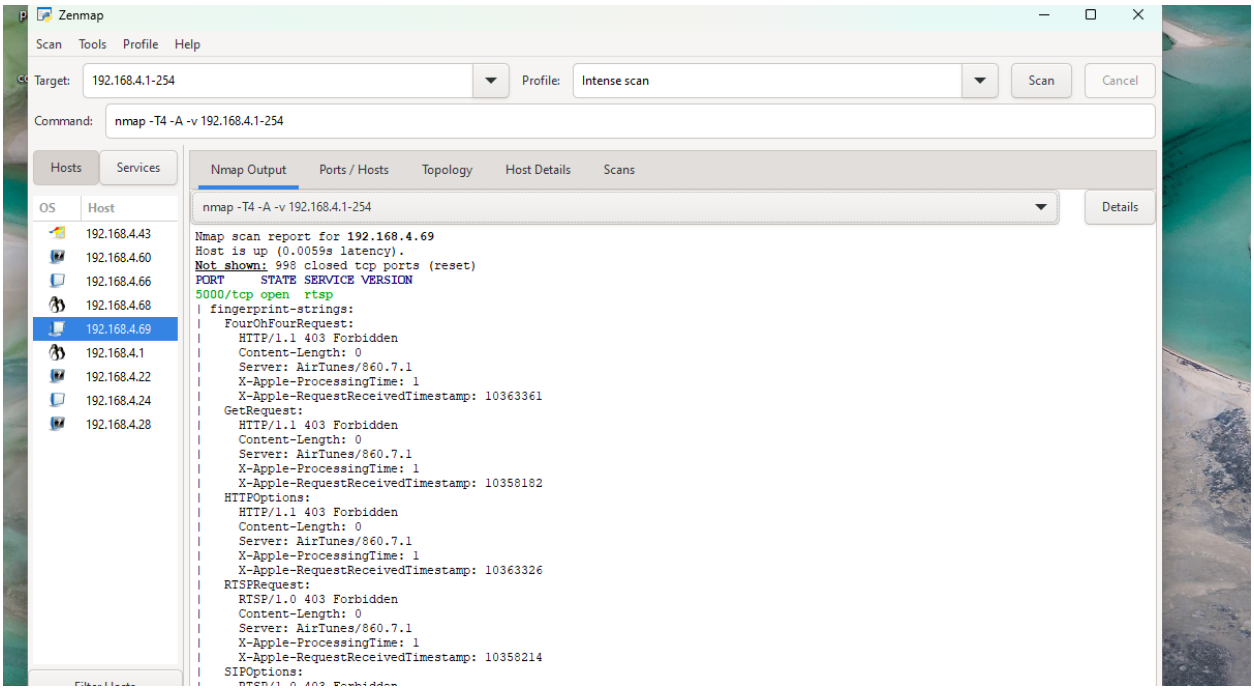
d. What is the MAC Address?
EA:07:BC:FC:90:B9

e. Is the system part of a workgroup?
No

f. Is there any potential security flaw? hint: guest (smb) – Describe
i. Open up Windows Explorer:
1. \\studentsHostIP\c$
Replace studentsHostIP with real IP Address.
No

g. Describe what additional information is provided by NMAP.
Host
Open Ports
Device type
OS details
IP ID Sequence Generation
TCP Sequence Prediction

h. Provide a screenshot of the scan.



4. Compile another report on another device.

a. Use two other SCAN Types.

b. Provide a report and screenshot.

First Device using an Intense scan plus UDP

OS: Linux 4.15 - 5.19

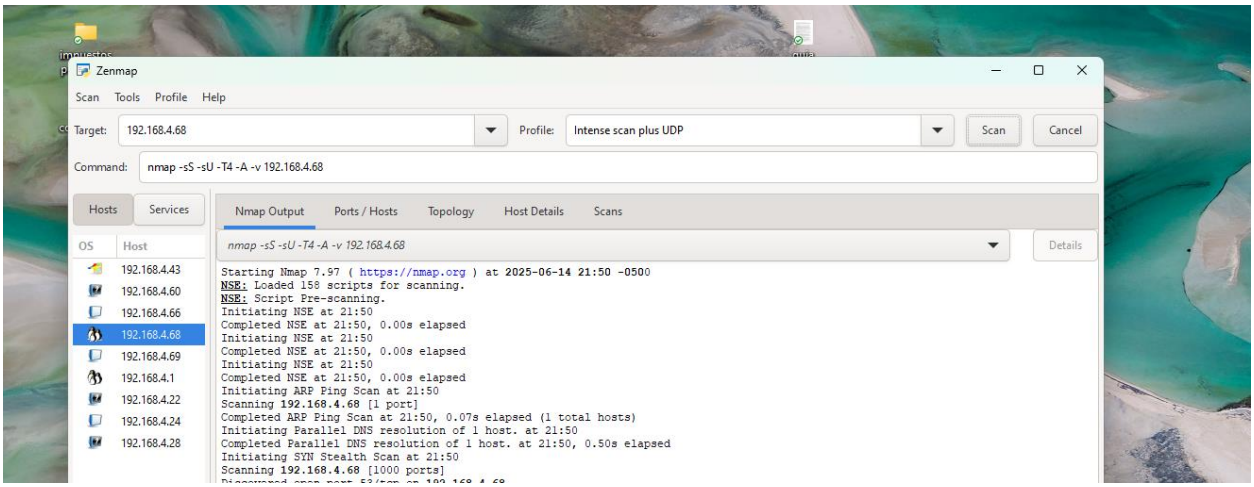
IPv4: 192.168.4.68

MAC: 30:57:8E:D3:36:8B

53 tcp open domain: primarily associated with DNS services

3001 tcp open Nessus: usually indicates the presence of a Nessus daemon on the target machine

Additional Information: Service scan timing, NSE, UDP scan timing, OS detection, ports.



Second Device using a Regular scan

OS: Apple iOS 15.0 - 15.6

IPv4: 192.168.4.24

MAC: AA:B6:E4:6E:28:AB

62078 tcp open tcpwrapped: indicates that a TCP handshake was completed but the connection then was lost by the remote host because this host was not on the list.