Intern Name :- Anurag Malekar

anuragmalekarofficial@gmail.com

* Task 1

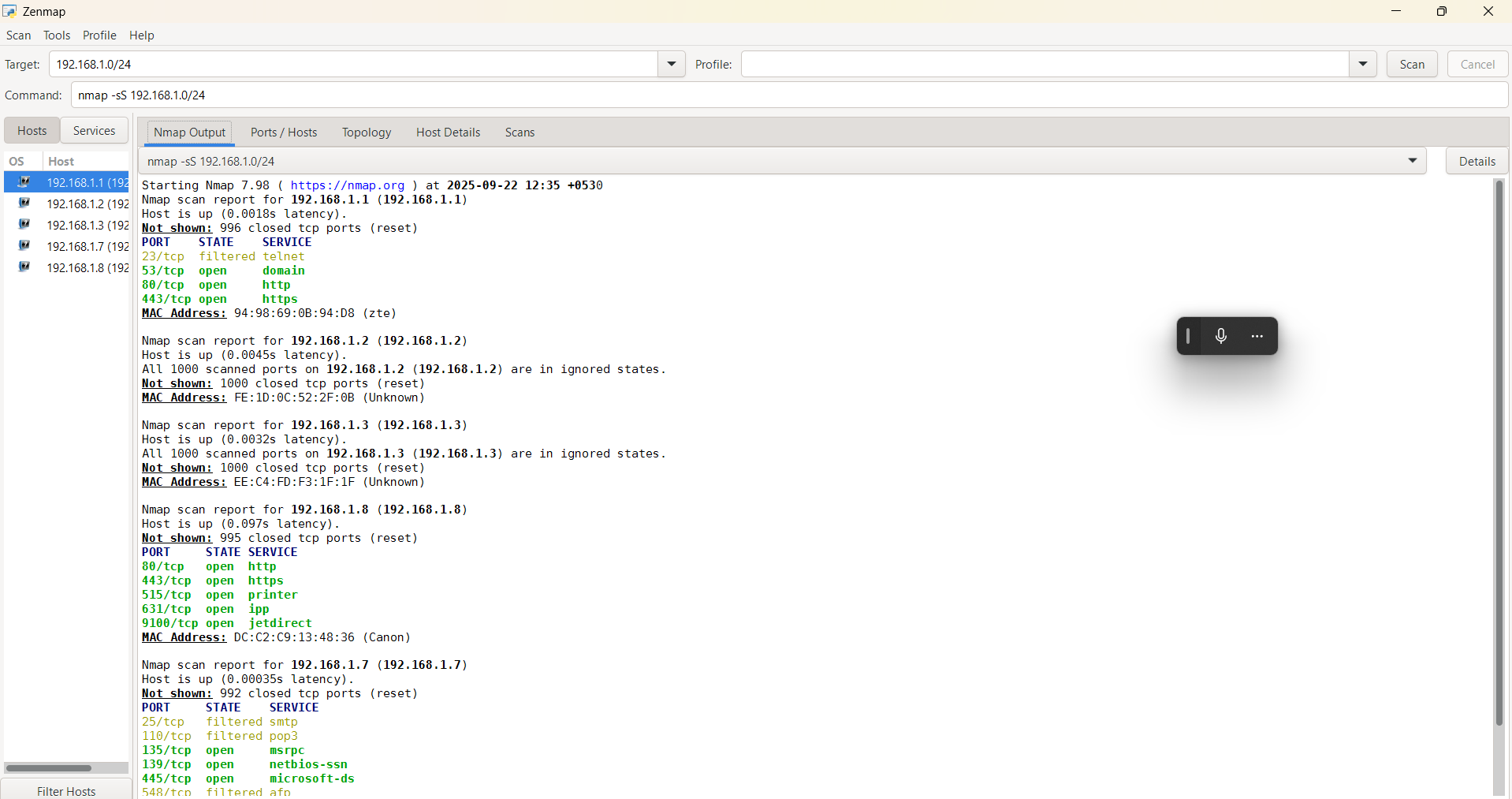
By Provided Information Like:-

Objective: Learn to discover open ports on devices in your local network to understand network exposure.

Tools: Nmap (free), Wireshark (optional)

* Steps Performed

1. Installed Nmap From Official Website.
2. Runned Command nmap -sS 192.168.1.0/24 to perform TCP SYN scan.



1. Found Open Ports And Common Services Running On It.

Like :- 80/tcp open http

443/tcp open https

515/tcp open printer

631/tcp open ipp

9100/tcp open jetdirect

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

548/tcp filtered afp

5357/tcp open wsdapi

7070/tcp open realserver

* Common Services Running On Them.

1.HTTP

2.HTTPS

3.MSRPC

* Identified Potential Security Risks From Open Ports.

**2.1 Unauthorized Access**

* Open ports (e.g., RDP – 3389, SSH – 22, FTP – 21) may allow direct remote connections.
* If weak or default credentials are used, attackers can gain unauthorized system access.

**2.2 Exploitation of Vulnerabilities**

* Services listening on open ports may have unpatched vulnerabilities.
* Exploits targeting these weaknesses can lead to remote code execution, privilege escalation, or full system compromise.
* Example: SMBv1 (port 445) exploited by the WannaCry ransomware attack.

**2.3 Malware Propagation**

* Worms and malware frequently use open ports to spread across systems.
* Example: SQL Slammer worm (port 1434) spread globally in minutes, disrupting financial and government systems.

**2.4 Information Disclosure**

* Certain open ports reveal sensitive system information (e.g., software version, operating system type).
* Attackers can use this intelligence to craft targeted exploits.

**2.5 Denial of Service (DoS/DDoS) Attacks**

* Attackers can flood services running on open ports with malicious traffic.
* This may result in resource exhaustion, service downtime, or complete system unavailability.

**2.6 Lateral Movement and Network Pivoting**

* A compromised device with open ports can serve as a **launchpad** for attackers to move laterally across the internal network.
* This increases the scope of compromise beyond the initial victim.

**2.7 Botnet Recruitment**

* Insecure open ports can allow attackers to compromise devices and integrate them into botnets.
* These botnets are often used for large-scale DDoS attacks, spam campaigns, or cryptocurrency mining.
* Used Sources While Working On It.

1.CHATGPT

2.Google

3.Gemini AI