Intern Name: S. Sai Amrutha
Mail: 240160226211.sunkavalli@gdgu.org

Task 1 – SCANNING LOCAL NETWORK FOR OPEN PORTS

Tools used: Nmap, Google

Code: nmap -sS -Pn --top-ports 20 -T4 192.168.12.0/24 -oN nmap_quick_10.0.72.0-21.text

Dataset: Target subnet 192.168.12.0/24 and Nmap's top 20 TCP ports database.

INTRODUCTION:

This exercise performs controlled, ethical network reconnaissance on the local subnet using Nmap, with optional packet captures via Wireshark. The primary goal is to discover live hosts and enumerate open TCP services to assess the immediate attack surface and identify basic security exposures. By documenting discovered services, associated risks, and recommended mitigations, this task builds practical skills in network discovery, evidence collection, and initial vulnerability assessment.

PORT SCANNING:

Port scanning is a controlled network reconnaissance technique used to discover which communication endpoints (ports) on a host are open, closed, or filtered; each open port usually maps to a running service (for example, HTTP on 80, SSH on 22). Security teams use port scans to build an inventory of live services and validate firewall rules, while attackers use them to map the attack surface and identify potentially vulnerable services.

Typical scans send probes (SYN, connect, UDP) and interpret responses to classify port state; SYN scans are common because they're fast and avoid completing full TCP handshakes. Key risks from exposed ports include unauthorized access, data exfiltration, and remote code execution if services are unpatched or misconfigured; mitigations include patching, minimizing listening services, strict firewalling, and network segmentation.

TCP SYN SCAN:

Nmap is a powerful, freely available network scanning tool that can quickly profile the network by identifying which ports are open and which services are running. The TCP SYN scan (nmap sS) is a fast and stealthy method that sends SYN packets to the target ports and monitors responses to determine the port status without completing the full TCP handshake. This is the method used in the scan results shown in your images, where ports like 22 (SSH), 23 (Telnet), and 80 (HTTP) were discovered as open on one device, while all major ports were found closed on another

OPEN PORT:

An open port is a network port actively accepting connections. Each port corresponds to a service (e.g., port 80 → HTTP web server, port 22 → SSH). Open ports can be necessary for functionality, but also increase exposure; attackers target them to exploit weaknesses in the running services.

IP RANGES:

An IP range is the set of all possible addresses within a subnet, defined by an IP address and subnet mask (CIDR notation). For example, 192.168.1.0/24 covers addresses from 192.168.1.1 to 192.168.1.254. Understanding IP ranges helps identify the full scope of devices to scan in a network.

NETWORK RECONNAISSANCE:

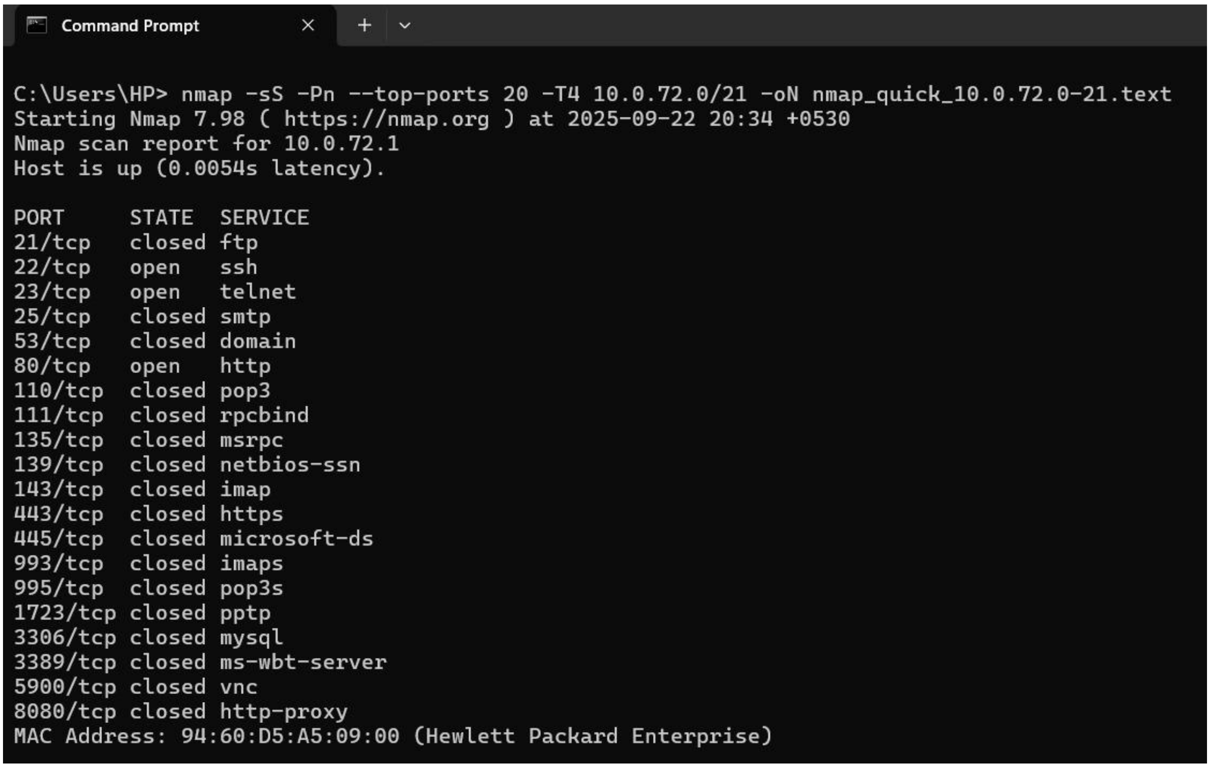
Network reconnaissance is the process of gathering information about devices, services, and vulnerabilities on a network. It is often the first step in both defensive assessments and malicious attacks. Tools like Nmap are used to discover live hosts, open ports, and service versions to map the attack surface.

NETWORK SECURITY BASICS:

At its core, network security is about minimizing unnecessary exposure and controlling traffic flow. Best practices include:

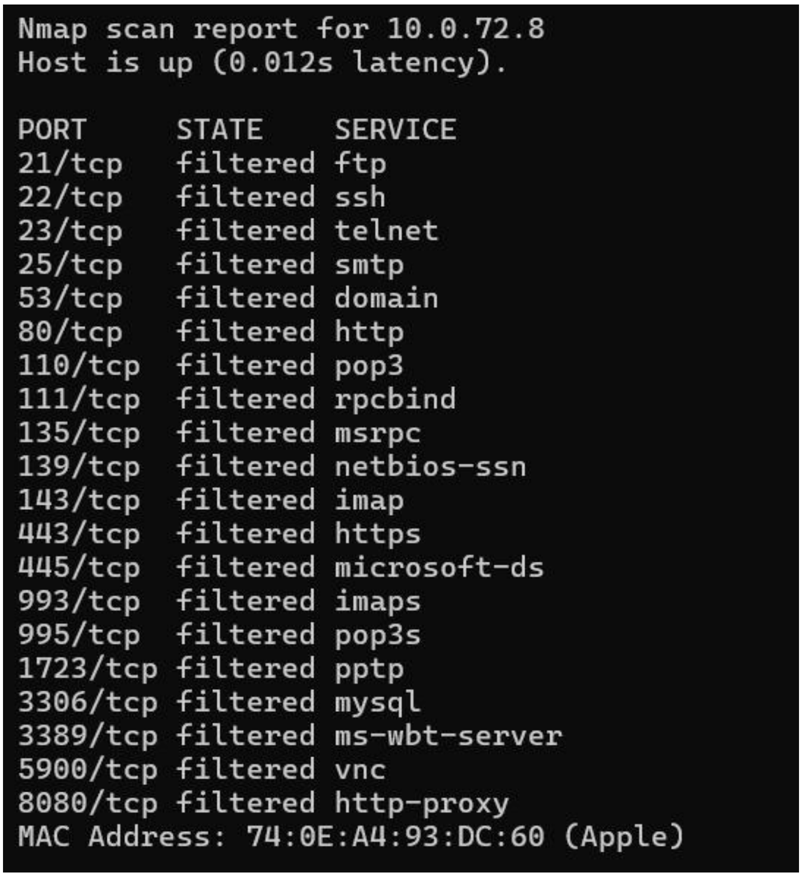
- Closing unused ports and services.
- Using firewalls to restrict access.
- Regular patching and updates to services.
- Monitoring with intrusion detection and logging.
- Segmenting networks to contain potential breaches.

HERE ARE SOME RAW OUTPUT IN FROM OF SCREENSHOTS:



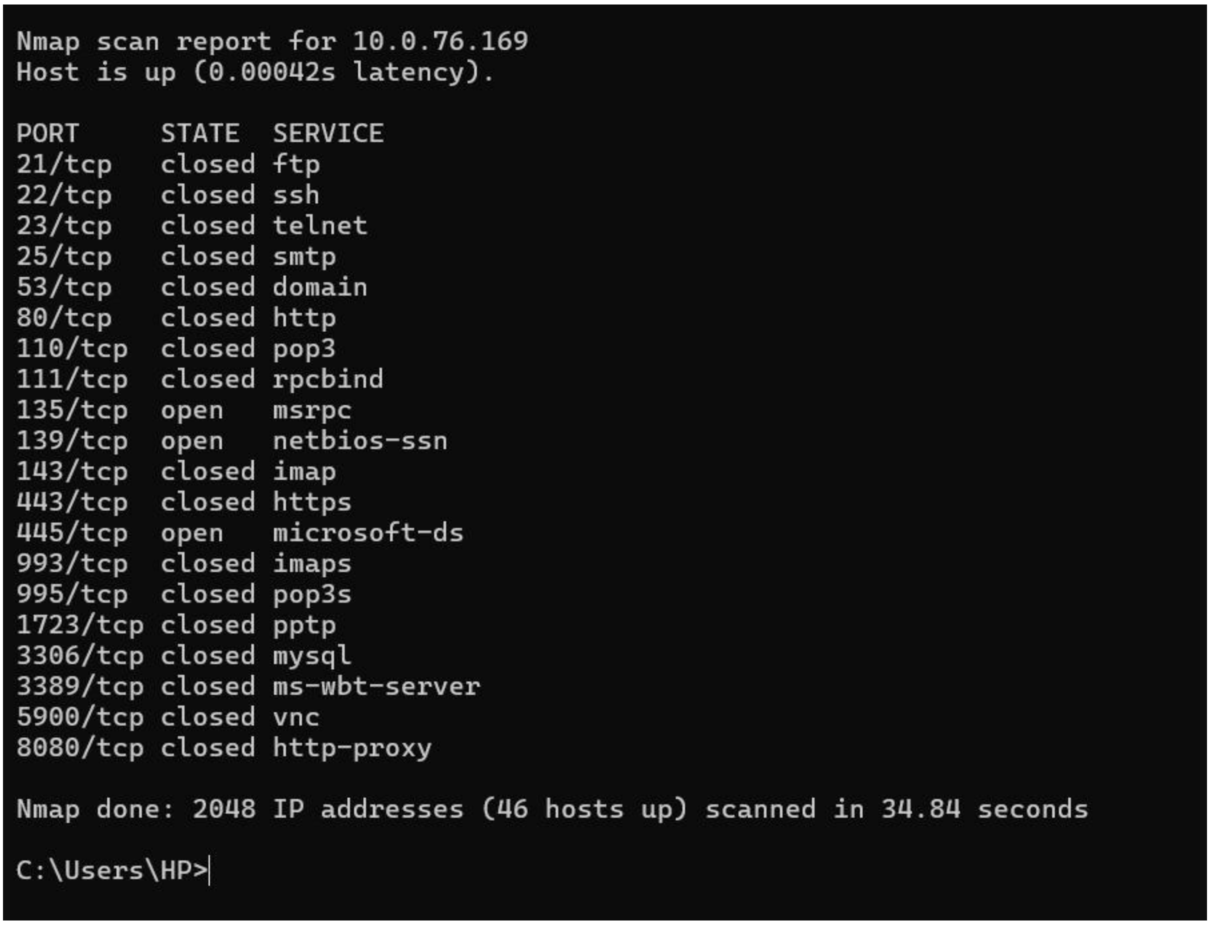
```
C:\Users\HP> nmap -sS -Pn --top-ports 20 -T4 10.0.72.0/21 -oN nmap_quick_10.0.72.0-21.text
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-22 20:34 +0530
Nmap scan report for 10.0.72.1
Host is up (0.0054s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   open   telnet
25/tcp   closed smtp
53/tcp   closed domain
80/tcp   open   http
110/tcp  closed pop3
111/tcp  closed rpcbind
135/tcp  closed msrpc
139/tcp  closed netbios-ssn
143/tcp  closed imap
443/tcp  closed https
445/tcp  closed microsoft-ds
993/tcp  closed imaps
995/tcp  closed pop3s
1723/tcp closed pptp
3306/tcp closed mysql
3389/tcp closed ms-wbt-server
5900/tcp closed vnc
8080/tcp closed http-proxy
MAC Address: 94:60:D5:A5:09:00 (Hewlett Packard Enterprise)
```



```
Nmap scan report for 10.0.72.8
Host is up (0.012s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   filtered http
110/tcp  filtered pop3
111/tcp  filtered rpcbind
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  filtered https
445/tcp  filtered microsoft-ds
993/tcp  filtered imaps
995/tcp  filtered pop3s
1723/tcp filtered pptp
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
5900/tcp filtered vnc
8080/tcp filtered http-proxy
MAC Address: 74:0E:A4:93:DC:60 (Apple)
```



```
Nmap scan report for 10.0.76.169
Host is up (0.00042s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   closed ssh
23/tcp   closed telnet
25/tcp   closed smtp
53/tcp   closed domain
80/tcp   closed http
110/tcp  closed pop3
111/tcp  closed rpcbind
135/tcp  open   msrpc
139/tcp  open   netbios-ssn
143/tcp  closed imap
443/tcp  closed https
445/tcp  open   microsoft-ds
993/tcp  closed imaps
995/tcp  closed pop3s
1723/tcp closed pptp
3306/tcp closed mysql
3389/tcp closed ms-wbt-server
5900/tcp closed vnc
8080/tcp closed http-proxy

Nmap done: 2048 IP addresses (46 hosts up) scanned in 34.84 seconds

C:\Users\HP>
```

CONCLUSION:

In this task, we scanned the local network to identify active devices and their open ports. The exercise helped in understanding how network hosts communicate and how services are exposed through ports. We learned the importance of open port detection for maintaining network security, as open ports can be potential entry points for attackers. This task provided practical experience in network reconnaissance, IP addressing, subnetting, and the basics of network security monitoring.

****