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.

Name: S. Sai Amrutha

Network Scanning and Open Ports:

Network scanning is a fundamental cybersecurity process used to identify active devices and open ports within a local or remote network. Open ports are specific network ports on a device that accept incoming network connections, often corresponding to running services such as SSH (port 22), Telnet (port 23), or HTTP (port 80). Attackers frequently target open ports because they can offer entry points for exploitation if those services are insecure or outdated

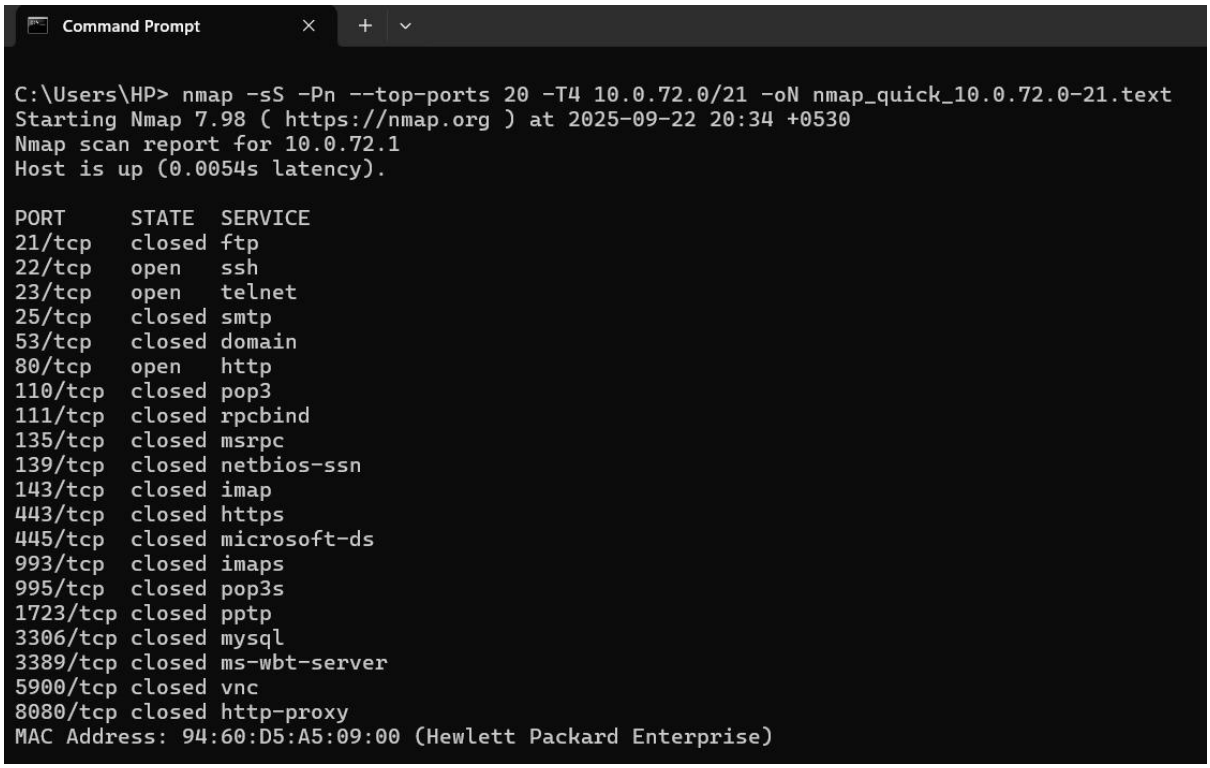
Nmap and TCP SYN Scans:

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

Security Implications

Open ports represent potential vulnerabilities, especially if the service is unnecessary or not properly secured. For example, Telnet (port 23) transmits data in plaintext and should be avoided or protected with strong access controls. Firewalls and proper configuration restrict unnecessary port exposure and help mitigate risks. Regular scanning with tools like Nmap, combined with traffic analysis (using tools like Wireshark), allows network administrators to assess both active services and overall exposure, providing an essential layer of defense for networked systems.

RAW OUTPUTS:


Command Prompt
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

The network scan revealed limited open ports, demonstrating good default host protections in most cases. However, the presence of SMB-related ports open on a host warrants further security checks to ensure no vulnerabilities are present. This exercise helped in understanding network port scanning, service identification, and the importance of minimizing unnecessary open ports to reduce attack surfaces.

****