TASK – 1

SCANNING LOCAL NETWORK FOR OPEN PORTS

Tools used: Nmap

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: Vijjada Prem Sai

Local Network Port Scanning Report

Introduction:

This report presents the findings from a network reconnaissance task aimed at identifying open and closed TCP ports on devices within my local network. The purpose of this exercise is to understand network exposure and assess potential security risks related to open ports.

Tools Used

- Nmap (Network Mapper): Used for scanning the network to detect open, closed, and filtered ports.
- Wireshark (optional): Can be used for packet capturing and deeper analysis (not performed in this task).

Methodology:

1. Identified the local subnet IP range: 192.168.12.0/24.
2. Executed a TCP SYN scan using the command: nmap -sS 192.168.12.0/24.
3. Noted the status of scanned ports on each active host.
4. Saved raw Nmap scan outputs as screenshots to document the scanning results.
5. Analysed the scan results to identify network services running on open ports and recognize any potential security exposure.

Results and Analysis

- A total of 256 IP addresses were scanned within the network subnet.
- Multiple hosts were up and responsive to the scan.

Host: 192.168.12.139 (Apple)

- All scanned ports for this device appeared as filtered, such as rsftp (26), hosts2-ns (81), news (144), smtps (465), postgresql (5432), X11 (6001), and others.
- The presence of exclusively filtered ports suggests strong firewall settings or active filtering, making this device well protected from network probing and external threats.

Host: 192.168.12.1 (Hewlett Packard Enterprise)

- This device had three open ports: SSH (22), Telnet (23), and HTTP (80).
- SSH enables secure remote command-line access, while Telnet allows unencrypted remote sessions and is considered a security risk if left active.
- The HTTP port is typically used for web server or device management interfaces.
- The exposure of both SSH and Telnet means security policies should favor disabling Telnet and relying on SSH for remote access.

Host: 192.168.12.52 (Unknown Vendor)

- Major ports were found closed, including SSH (22), Telnet (23), SMTP (25), HTTP (80), HTTPS (443), MySQL (3306), and Remote Desktop (3389).
- The lack of open services points to a secure, minimal-exposure configuration or an inactive system.

Overall Network Posture

- Most hosts either had filtered or closed ports, reflecting robust security controls and limited-service exposure.
- The only exceptions were the Apple device with filtered ports and the HP device exposing remote access and web services.

Security Insights

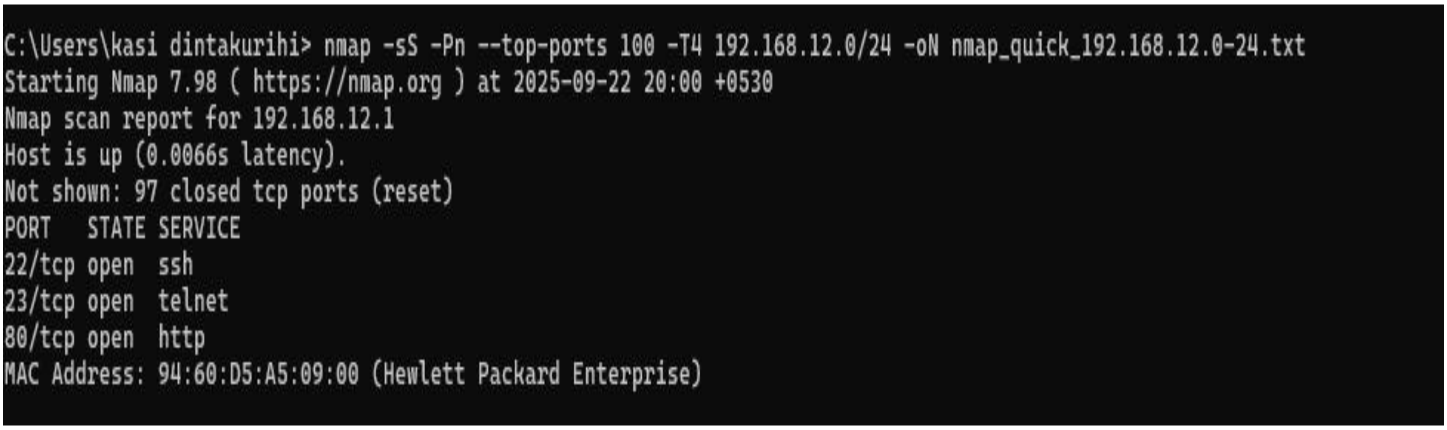
- Hosts with only filtered or closed ports are well defended against unauthorized access.
- Any open ports, such as SSH or HTTP, should be monitored and secured with strong authentication, updated software, and network access controls.
- Devices with filtered ports (like the Apple host) exemplify recommended security practice for minimizing attack surfaces.

Recommendations

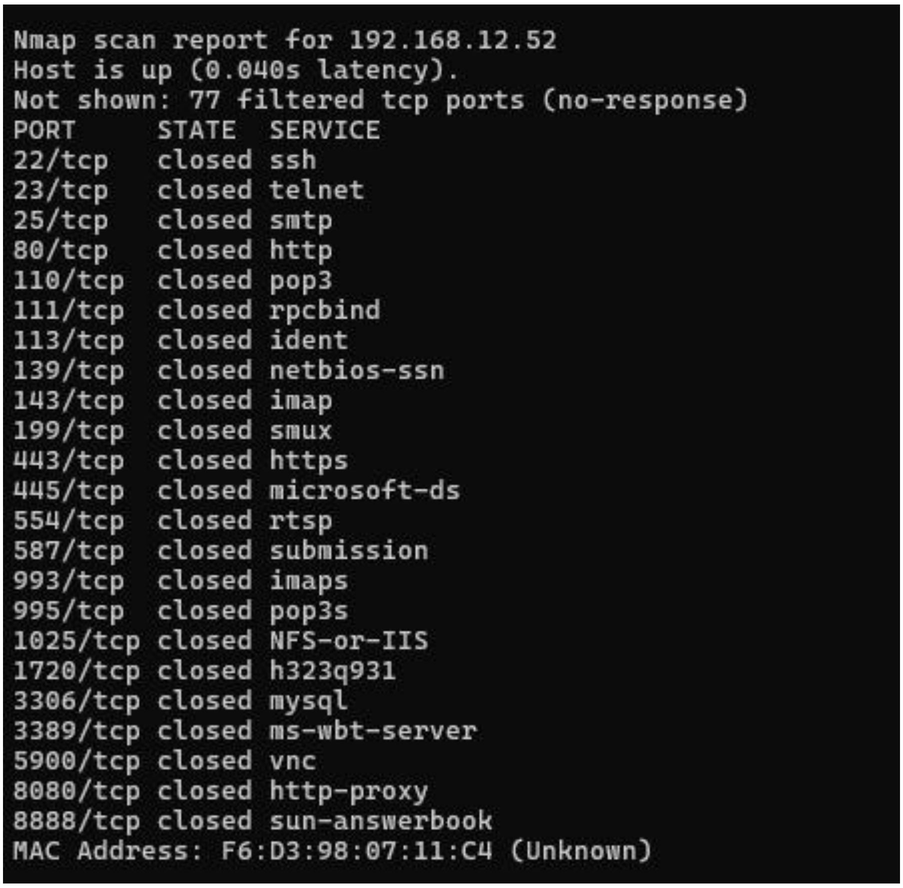
- Regularly scan for open ports to ensure new services are not inadvertently exposed.
- Disable legacy protocols like Telnet in favor of secure alternatives (SSH).

- Confirm firewall configurations are actively blocking unwanted traffic on all devices.

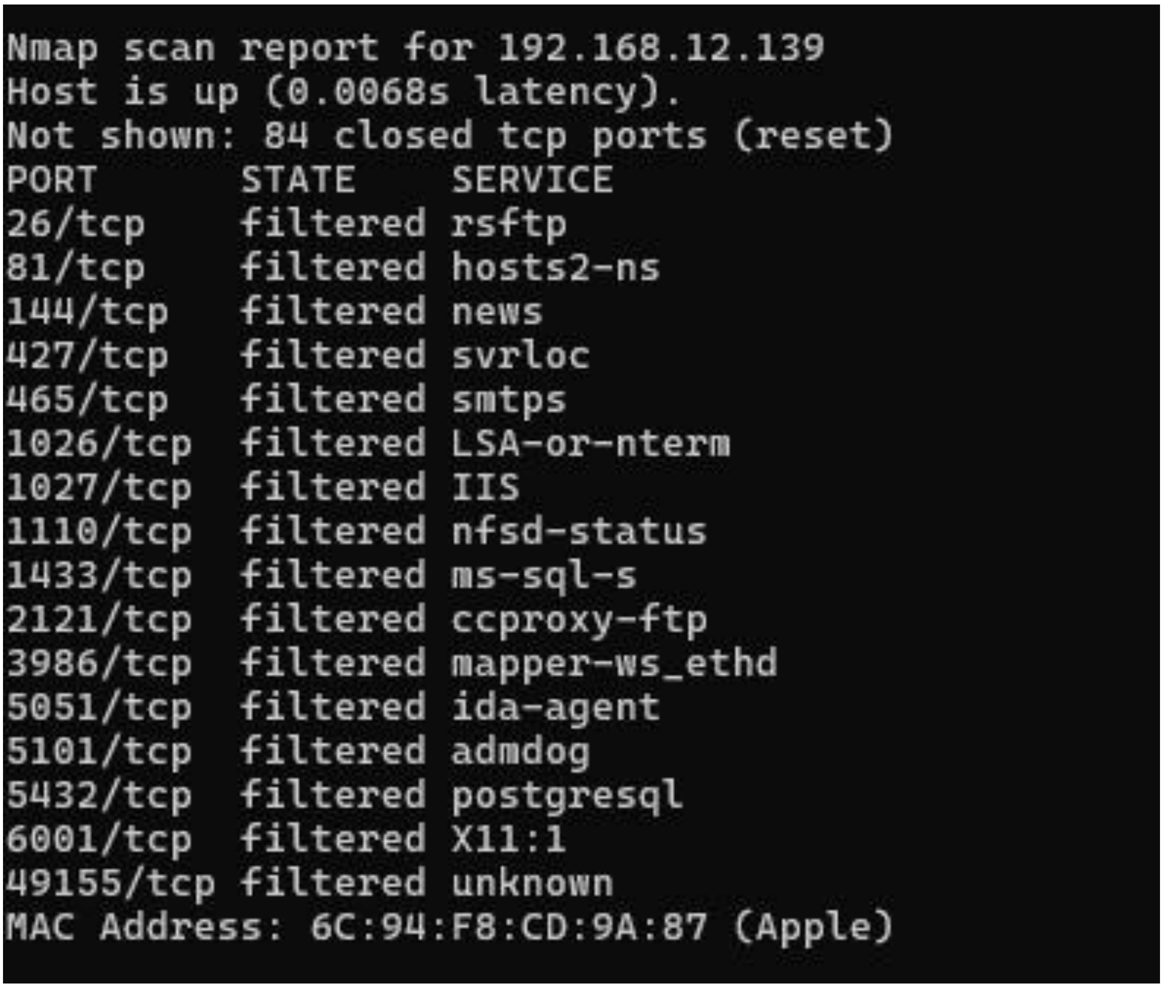
Raw Outputs :



```
C:\Users\kasi dintakurihi> nmap -sS -Pn --top-ports 100 -T4 192.168.12.0/24 -oN nmap_quick_192.168.12.0-24.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-22 20:00 +0530
Nmap scan report for 192.168.12.1
Host is up (0.0066s latency).
Not shown: 97 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http
MAC Address: 94:60:D5:A5:09:00 (Hewlett Packard Enterprise)
```



```
Nmap scan report for 192.168.12.52
Host is up (0.040s latency).
Not shown: 77 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    closed ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    closed http
110/tcp   closed pop3
111/tcp   closed rpcbind
113/tcp   closed ident
139/tcp   closed netbios-ssn
143/tcp   closed imap
199/tcp   closed smux
443/tcp   closed https
445/tcp   closed microsoft-ds
554/tcp   closed rtsp
587/tcp   closed submission
993/tcp   closed imaps
995/tcp   closed pop3s
1025/tcp  closed NFS-or-IIS
1720/tcp  closed h323q931
3306/tcp  closed mysql
3389/tcp  closed ms-wbt-server
5900/tcp  closed vnc
8080/tcp  closed http-proxy
8888/tcp  closed sun-answerbook
MAC Address: F6:D3:98:07:11:C4 (Unknown)
```



```
Nmap scan report for 192.168.12.139
Host is up (0.0068s latency).
Not shown: 84 closed tcp ports (reset)
PORT      STATE    SERVICE
26/tcp    filtered rsftp
81/tcp    filtered hosts2-ns
144/tcp   filtered news
427/tcp   filtered svrloc
465/tcp   filtered smtps
1026/tcp  filtered LSA-or-nterm
1027/tcp  filtered IIS
1110/tcp  filtered nfsd-status
1433/tcp  filtered ms-sql-s
2121/tcp  filtered ccproxy-ftp
3986/tcp  filtered mapper-ws_ethd
5051/tcp  filtered ida-agent
5101/tcp  filtered admdog
5432/tcp  filtered postgresql
6001/tcp  filtered X11:1
49155/tcp filtered unknown
MAC Address: 6C:94:F8:CD:9A:87 (Apple)
```

Identifying potential security risk from open ports:

Open ports are like open doors on a computer or network. If these doors are not properly protected, bad actors can use them to enter the system and cause problems. For example:

Open remote access ports like SSH allow control over the device, but if passwords are weak, attackers can break in.

Ports like Telnet send information in plain text, making it easy for attackers to steal data.

Web ports (HTTP) can have software vulnerabilities that hackers may exploit.

Important Windows ports used for file sharing (SMB) have been targets of big attacks like ransomware.

Oports make it easier for attackers to scan and find weak spots on your network.

If services running on these ports aren't updated or configured correctly, attackers can take advantage and cause damage.

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.