TASK 1

SCANNING LOCAL NETWORK FOR OPEN PORTS

TOOLS USED : Nmap

Code:nmap -sS -Pn -TOP-PORTS 20 -T4 -On nmap_scan_10.0.8.0-21.txt 10.0.8.0/21

Dataset:Target subnet 10.0.8.0/21 and Nmap’s top 20 TCP ports database

NAME : Abhishek.S

LOCAL NETWORK PORT SCANNING REPORT

PORTS

A port in computer networking is like a virtual “door” that allows data to enter or leave a device (such as a computer or server).

- Each device connected to the internet (or a network) has an IP address (like its house address).
- A port number works like an apartment or room number inside that house — it helps identify which application or service the data should go to.

Port Range

Port numbers are 16-bit unsigned integers, so they go from 0 to 65,535.

They are divided into 3 categories:

1. Well-Known Ports (0 – 1023)
    - Reserved for core services and protocols.
    - Examples:
        - 20/21 → FTP
        - 22 → SSH
        - 25 → SMTP
        - 53 → DNS
        - 80 → HTTP
        - 443 → HTTPS
2. Registered Ports (1024 – 49,151)
    - Assigned to user applications or third-party services.
    - Examples:
        - 1433 → Microsoft SQL Server
        - 3306 → MySQL
        - 3389 → Remote Desktop Protocol (RDP)
3. Dynamic / Private / Ephemeral Ports (49,152 – 65,535)
    - Used temporarily by client devices when connecting to servers.

- Example: When you open a website, your computer may use port 51,234 (random ephemeral port) to connect to the server's port 443.

OPEN PORT

- A port that is listening for incoming connections.
- Means some application/service is running and ready to communicate.
- Example:
  - If a web server is running on your computer, Port 80 (HTTP) will be open.
  - When someone types your IP in a browser, their request enters through Port 80.

CLOSED PORTS

- A port that is not listening for connections.
- No application is using it.
- If someone tries to connect, the system responds with "connection refused" or just ignores it.

  Example:

  If no FTP server is running , port 21 will be closed

WIRESHARK

Wireshark is a **free and open-source network protocol analyzer** (also called a packet sniffer).

It lets you **capture and examine the data ("packets")** traveling over a network in real time.

◈ What It Does

- **Captures packets** moving between devices.
- **Shows details** of each packet (IP address, port, protocol, contents, etc.).
- Helps in **network troubleshooting, monitoring, and security analysis**.

Example

If you open Wireshark and start capturing:

- You browse a website → Wireshark shows packets on **Port 443 (HTTPS)**.
- You send an email → It shows packets on **Port 25 (SMTP)**.

- Local Network Port Scanning Report

  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. 2. Identified the local subnet IP range: 192.168.12.0/24. Executed a TCP SYN scan using the command: nmap -sS 192.168.12.0/24. 3. 4. Noted the status of scanned ports on each active host. 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.

  • A total of 256 IP addresses were scanned within thenetwork 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 f irewall 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

TASK 1

```
Nmap scan report for 10.0.8.58
Host is up (0.022s 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  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: 6A:49:27:18:8A:64 (Unknown)
```

```
Nmap scan report for 10.0.8.201
Host is up.

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: AC:19:8E:0D:23:93 (Intel Corporate)
```

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.