🔍 Local Network Port Scanning & Packet Analysis

📌 Objective

To discover open ports and identify active hosts on the local network using Nmap, and optionally analyze the network traffic generated by the scan using Wireshark.

🛠️ Tools Used

- Nmap: For scanning the local IP range with TCP SYN scan.

- Wireshark: For analyzing network packets generated during the scan.

- Linux VM (VirtualBox) with NAT networking.

⏰ Task Steps Followed

1. Installed Nmap

sudo apt update
sudo apt install nmap

2. Found Local IP Range

Command used: ip a
Output: IP was 10.0.2.5
Scanned Range: 10.0.2.0/24

3. Ran TCP SYN Scan

nmap -sS -v -oN vm_scan_results.txt 10.0.2.0/24

4. Noted IPs and Open Ports

IP Address	Status	Open Ports	Notes
10.0.2.5	Up	None	All 1000 ports closed
10.0.2.3	Up	Filtered	Likely VirtualBox NAT Gateway
Others	Down	–	Not reachable via NAT network

5. Analyzed with Wireshark

Started Wireshark on interface (e.g., eth0) before scan. Used the filter:
tcp.flags.syn == 1 && tcp.flags.ack == 0
Observed outgoing SYN packets from 10.0.2.5 probing other hosts — matching Nmap's SYN scan behavior.

6. Researched Common Services (Examples)

PORT	SERVICE	USAGE
22	SSH	Secure shell for remote login
80	HTTP	Web traffic
443	HTTPS	Secure web traffic
3389	RDP	Remote Desktop Protocol
PORT	Service	Usage

7. Identified Security Risks

- Open ports can expose vulnerable services (e.g., outdated SSH/HTTP).
- Filtered ports indicate firewall presence, which is good for protection.
- NAT network limits visibility, which also reduces exposure to external threats.

8. Saved Outputs

- vm_scan_results.txt – Nmap scan result (plain text)
- nmap_scan.txt – Wireshark packet dump (in hex format)
- README.md – Task summary and documentation