Task 1 : Network Scanning and Traffic Capture

🎯 Objective

To scan the local network for open TCP ports using **Nmap** and analyze potential security risks based on the findings from both **Kali Linux** (VirtualBox) and **Windows 10**.

🛠️ Tools Used

- **Nmap** v7.95
- **Operating Systems**:
    - Windows 10 (Host)
    - Kali Linux (Guest – VirtualBox)
- **Terminals**: Windows Command Prompt, Kali Linux Terminal

🔄 Steps Performed

1. Verified Nmap installation on both Windows and Kali Linux using:

bash

CopyEdit

nmap --version

2. Identified the local IP address and subnet range:
    - **Kali Linux**: 10.241.85.177/24 (via ip a)
    - **Windows**: 10.241.85.124 (via ipconfig)
3. Ran TCP SYN scan on the subnet using:

bash

CopyEdit

nmap -sS <IP-address> or <IP-range>

4. Recorded the scan results in text format.
5. Took screenshots of scan commands and outputs.
6. Analyzed each open port for possible security implications.

📊 Scan Results Summary

🖥️ Windows Host – 10.241.85.124

Port	Service	Description	Risk Level
135	MSRPC	Windows RPC – used for DCOM services	⚠️ Medium – Can be targeted for Windows exploits
139	NetBIOS-SSN	File/Printer sharing (legacy)	❌ High – Exploitable legacy protocol
445	Microsoft-DS	SMB over TCP (file sharing)	❌ High – Exploited by ransomware like WannaCry
902	ISS RealSecure	VMware ESXi remote management port	⚠️ Medium – Disable if VMware not in use
912	Apex Mesh	Used by VMware/other internal services	⚠️ Medium – Uncommon port, review necessity

---

🐧 Kali Linux Host – 10.241.85.177 & Network Devices

IP Address	Port	Service	Description	Risk Level
10.241.85.236	53	DNS	Domain Name System	⚠️ Medium – Needs secure configuration
10.241.85.124	(As above in Windows scan)	—	See Windows scan table	—
10.241.85.177	—	—	No open TCP ports detected	✅ Low Risk

🖼️ Screenshots

- Windows Nmap scan
- Kali Linux Nmap scan
- IP detection commands (ip a & ipconfig)
- Nmap installation check on both systems

(Folders: **Screenshot for Windows** & **Screenshot for Linux**)

📁 Files Included

- Windows scan.txt – Full Nmap output (Windows)
- Linux scan.txt – Full Nmap output (Kali Linux)
- Screenshot for Windows scan.pdf
- Screenshot for Linux scan.pdf

✅ Conclusion

This scan identified several open ports across hosts in the network. Ports such as **445, 135, and 139** are high-risk and should be monitored, restricted, or closed if not needed.
The DNS service (port 53) found on **10.241.85.236** should be configured securely to prevent DNS-based attacks.
Regular scanning with Nmap can help detect newly opened ports and potential vulnerabilities before attackers exploit them.