CYBER SECURITY INTERNSHIP

Task1 : Scan your Local Network For Open Ports:

C:\Users\Akash>nmap -sS [redacted]

Starting Nmap 7.98 (https://nmap.org) at 2025-09-22 18:43 +0530

Nmap scan report for [redacted]

Host is up (0.0033s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE

53/tcp open domain

MAC Address: [redacted] (Unknown)

Nmap scan report for [redacted]

Host is up (0.00034s latency).

Not shown: 997 closed tcp ports (reset)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

Nmap done: 256 IP addresses (2 hosts up) scanned in 5.99 seconds

Research analysis:

1) Port 135 (TCP) – MS RPC (Microsoft Remote Procedure Call) service is running.
2) Port 139 (TCP) – NetBIOS Session Service, used for Windows file and printer sharing.
3) Port 445 (TCP) – Microsoft-DS (Directory Services), runs SMB over TCP/IP for file and printer sharing.

Potential Security Risks: Ports 135, 139, and 445 (TCP) are potential security risks because attackers can exploit them for unauthorized access, spreading malware, or stealing data, especially if file/printer sharing or RPC services are exposed to the internet.