**Task 1: Scan Your Local Network for Open Ports**

**Objective**: *Learn to discover open ports on devices in your local network to understand network exposure*.

**Tools:** *Nmap (free), Wireshark (optional)*

**Key Concepts*:*** *Port scanning, TCP SYN scan, IP ranges, network reconnaissance, open ports, network security basics*

So, my local Area Network consists of 192.168.1.1/24 IP subnet.

Firstly, I installed Nmap on my Windows 11 machine. You can either use Windows or Linux OS for scanning the port using Nmap, but using Linux is more reliable in the cybersecurity field.

Using- ***nmap -sS 192.168.1.1/24***

A screenshot of a computer

AI-generated content may be incorrect.

I found two active IP addresses,192.168.1.1 and 192.168.1.121

Open Ports are for 192.168.1.1:

53/tcp open domain

Open Ports for 192.168.1.121:

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

2869/tcp open icslap

3306/tcp open mysql

3389/tcp open ms-wbt-server

5357/tcp open wsdapi

1.**135/tcp — msrpc (Microsoft RPC / DCE-RPC)**

**What it is:** Windows RPC (Remote Procedure Call) endpoint mapper used by many Windows services (DCOM, service control, administration).  
**Why it matters:** Common target for info gathering and exploitation (exposes many RPC interfaces).  
**Check/remediate:** If the host is Windows and RPC is needed for normal operation, restrict access to trusted hosts via firewall. Otherwise, block from the LAN or disable unused RPC-based services and apply Windows updates.

2.**139/tcp — netbios-ssn (NetBIOS Session Service)**

**What it is:** Old Windows/NetBIOS session service used for legacy file/print sharing and NetBIOS name resolution.  
**Why it matters:** Can leak hostnames/shares and be abused to enumerate accounts/shares or pass-the-hash style attacks.  
**Check/remediate:** Disable NetBIOS over TCP/IP if not required. Use SMB over TCP (port 445) with proper authentication, or restrict port 139 at the firewall.

3.**445/tcp — microsoft-ds (SMB / Microsoft-DS)**

**What it is:** Modern Windows file/print sharing (SMB/CIFS) and many Windows network services.  
**Why it matters:** High-risk if exposed — historical critical vulnerabilities (e.g., EternalBlue) target SMB. can also expose shares and credential attacks.  
**Check/remediate:** Ensure SMBv1 is disabled, apply OS updates/patches, audit/limit shared folders, require strong authentication, and firewall the port if not needed.

4.**2869/tcp — icslap (Windows Web Services / UPnP/ICS-related)**

**What it is:** Often associated with Windows Web Services / UPnP/Internet Connection Sharing related services (service name shown as icslap in some service lists). Device discovery/management services use it on Windows.  
**Why it matters:** Can expose device/service information; UPnP-related services can be abused if misconfigured.  
**Check / remediate:** If not intentionally using device discovery or UPnP on that machine, disable the corresponding Windows services (UPnP, SSDP, etc.) and block the port. Run netstat -ano or services.msc to find the owning process.

5.**3306/tcp — mysql (MySQL/MariaDB)**

**What it is:** MySQL database server port.  
**Why it matters:** If bound to 0.0.0.0 or accessible across the LAN, attackers can attempt brute force, SQL injection via misconfigured apps, or data exfiltration.  
**Check/remediate:** Confirm whether MySQL is intended to be reachable remotely. If not, bind it to 127.0.0.1 (or internal IP only), enforce strong DB accounts/passwords, disable remote root login, and use firewall rules. Keep DB patched.

6.**3389/tcp — ms-wbt-server (Microsoft RDP)**

**What it is:** Remote Desktop Protocol (Windows remote GUI).  
**Why it matters:** High-value target — weak credentials or unpatched RDP has been exploited widely. Exposing RDP increases the risk of brute-force, credential theft, and remote compromise.  
**Check/remediate:** Do **not** expose RDP unless required. Use Network Level Authentication (NLA), strong passwords, two-factor authentication where possible, change the default port only as a minor hurdle, and restrict access with a firewall or VPN.

7.**5357/tcp — wsdapi (Web Services for Devices / WSD)**

**What it is:** Windows Web Services for Devices API — used for network device discovery/configuration (e.g., printers, scanners).  
**Why it matters:** It can leak device info and be abused to enumerate or interact with network devices.  
**Check/remediate:** If you don’t use networked printers/scanners via WSD, disable the WSD or related services and block the port from untrusted hosts.

8.**53/tcp — domain (DNS — Domain Name System)**

**What it is:** DNS listens on port 53 (UDP for queries, TCP for zone transfers and large responses). It resolves hostnames to IPs and vice-versa and can act as an authoritative name server or a recursive resolver for clients.  
**Why it matters:** A misconfigured DNS server can be abused as an *open resolver* (used for reflection/amplification DDoS), expose internal DNS zone data via zone transfers, leak infrastructure details, or reveal software versions (which may have vulnerabilities). DNS is critical for network functionality — disrupting it impacts many services.