# Task: Scan Your Local Network for Open Ports

Purpose: Learn basic network reconnaissance to discover open ports and understand service exposure on devices within your local network.

## Hints / Mini Guide

1. Install Nmap from the official website (https://nmap.org). Use a trusted source and verify checksums if available.

2. Find your local IP range (example: 192.168.1.0/24). On Windows run `ipconfig`; on Linux/macOS run `ip addr` or `ifconfig`.

3. Run: `nmap -sS 192.168.1.0/24` to perform a TCP SYN scan (requires appropriate permissions).

4. Note down IP addresses and open ports found. Example output lines: `192.168.1.5 open 22/tcp ssh`.

5. Optionally capture and analyze packets with Wireshark for deeper inspection (e.g., to view handshakes or application data).

6. Research common services running on those ports (e.g., 22 -> SSH, 80 -> HTTP, 443 -> HTTPS, 3389 -> RDP).

7. Identify potential security risks: outdated services, management interfaces exposed to the LAN, default credentials, unnecessary open ports.

8. Save scan results as a text or HTML file using Nmap options (for example `-oN output.txt` or `-oX output.xml`).

## Outcome

Basic network reconnaissance skills and a practical understanding of network service exposure.

## 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) — for scanning.

- Wireshark (optional) — for packet capture and analysis.

### Step-by-step Instructions

1. Ensure you have permission to scan the network. Only scan networks and devices you own or are explicitly allowed to test.

2. Install Nmap:  
 - Windows: download the installer from nmap.org and follow setup.  
 - Linux: use your package manager, e.g., `sudo apt install nmap` (Ubuntu/Debian) or `sudo dnf install nmap` (Fedora).  
 - macOS: use Homebrew `brew install nmap` or download a package.

3. Identify your local IP/subnet:  
 - Windows: open Command Prompt and run `ipconfig`.  
 - Linux/macOS: open Terminal and run `ip addr` or `ifconfig`.  
 - Look for the IPv4 address and subnet (e.g., 192.168.1.x/24).

4. Perform a basic TCP SYN scan:  
 - Example: `nmap -sS 192.168.1.0/24`  
 - Notes: -sS requires raw socket privileges (run as root/Administrator on many systems).

5. Save the scan results to a file:  
 - Simple text: `nmap -sS 192.168.1.0/24 -oN scan\_results.txt`  
 - Greppable: `-oG results.gnmap`  
 - XML (for tools/import): `-oX results.xml`

6. Review the results:  
 - For each host, note open ports and service names. Example line: `22/tcp open ssh`.  
 - Cross-check the service version using `-sV` (service detection): `nmap -sS -sV 192.168.1.0/24`.

7. (Optional) Capture traffic with Wireshark while scanning to inspect protocol behavior, TCP handshakes, or suspicious payloads.

8. Research and classify services:  
 - Look up common services for each open port.  
 - Identify which services are necessary and which are potential risks (e.g., outdated SSH, open SMB, unsecured database ports).

9. Identify risks and remediation ideas:  
 - Close unused ports or restrict access via firewall rules.  
 - Update or patch vulnerable services.  
 - Disable unnecessary services or move management interfaces off the general LAN.

10. Document and save your findings in a report or the saved Nmap output files for future reference.

### Safety & Legal Reminder

Only scan networks and devices you own or have explicit permission to test. Unauthorized scanning is illegal and may cause disruptions.

### Quick Reference Commands

- Find your IP (Windows): ipconfig

- Find your IP (Linux/macOS): ip addr or ifconfig

- Basic SYN scan: nmap -sS 192.168.1.0/24

- Service detection: nmap -sS -sV 192.168.1.0/24

- Save results (text): nmap -sS 192.168.1.0/24 -oN scan\_results.txt

- Save results (XML): nmap -sS 192.168.1.0/24 -oX scan\_results.xml

- Run a faster scan (fewer ports): nmap -F 192.168.1.0/24

- Aggressive scan (includes OS/version detection): nmap -A 192.168.1.0/24

### How to Explain This to Students

Demonstrate a small scan on a controlled device you own. Show the Nmap output, explain what 'open' means vs 'filtered', and map common ports to services (e.g., 22 -> SSH). Emphasize legal and safety considerations.