**1. Install Nmap**

**🔸 On Linux (Kali/Ubuntu):**

bash

CopyEdit

sudo apt update

sudo apt install nmap

**🔸 On Windows:**

Download from:  
🔗 https://nmap.org/download.html

🖼️ Screenshot Tip: Take a screenshot of Nmap installation confirmation.

**2. Find Your Local IP Range**

Run:

bash

CopyEdit

ip a

Look for your IP (e.g., 192.168.1.7 → subnet is likely 192.168.1.0/24)

Or:

bash

CopyEdit

ip route

🖼️ Screenshot Tip: Highlight your IP and subnet range.

**3. Run Nmap TCP SYN Scan**

Command:

bash

CopyEdit

nmap -sS 192.168.1.0/24

Explanation:

* -sS: TCP SYN (Stealth) scan
* 192.168.1.0/24: Scans all 256 IPs in that subnet

📌 Sample Output:

pgsql

CopyEdit

Nmap scan report for 192.168.1.1

Host is up (0.0021s latency).

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

443/tcp closed https

Nmap scan report for 192.168.1.5

Host is up (0.0019s latency).

PORT STATE SERVICE

3389/tcp open ms-wbt-server

🖼️ Screenshot Tip: Copy full terminal output and save it.

**4. Note IPs and Open Ports**

| **IP Address** | **Open Ports** | **Services** |
| --- | --- | --- |
| 192.168.1.1 | 22, 80 | SSH, HTTP |
| 192.168.1.5 | 3389 | Remote Desktop (RDP) |

Save these in a table or a .txt/.csv file.

**5. Optional: Packet Capture in Wireshark**

Start Wireshark **before running Nmap**:

* Select your network interface
* Use capture filter: host 192.168.1.x
* Run Nmap scan
* Analyze packets: TCP SYN, SYN-ACK

🖼️ Screenshot Tip: Mark SYN packets from your scan.

**6. Research Common Services on Found Ports**

Common ports/services:

* 22 → SSH
* 80 → HTTP
* 443 → HTTPS
* 3389 → RDP
* 445 → SMB

Use:

* https://www.speedguide.net/port.php?port=22
* https://nmap.org/nsedoc/

**7. Identify Potential Security Risks**

Examples:

* **SSH open to all** → Risk of brute-force
* **HTTP instead of HTTPS** → Data unencrypted
* **RDP open** → Vulnerable to exploits like BlueKeep

🧠 Tip: Recommend disabling unused ports or setting up firewalls.

**8. Save Scan Results**

To .txt:

bash

CopyEdit

nmap -sS 192.168.1.0/24 -oN scan\_results.txt

To .html (with xsltproc):

bash

CopyEdit

nmap -sS -oX scan\_results.xml 192.168.1.0/24

xsltproc scan\_results.xml -o scan\_report.html

