**Network Scanning Experiment: Scan Your Home Network Using Nmap**

**Objective:**  
To perform a basic scan of your home network using **Nmap** (Network Mapper) to identify active devices and open ports.

**Steps to Perform the Experiment:**

**Step 1: Install Nmap (If Not Installed)**

Nmap is available for Windows, Linux, and macOS.

**For Windows:**

1. Download the Nmap installer from: <https://nmap.org/download.html>
2. Install it, including **Zenmap** (GUI version, optional).
3. Open **Command Prompt (cmd)** or **PowerShell**.

**For Linux/macOS:**

* Install Nmap using the terminal:
* sudo apt install nmap # Debian/Ubuntu
* sudo yum install nmap # RHEL/CentOS
* brew install nmap # macOS (Homebrew)
* Check if Nmap is installed:
* nmap --version

**Step 2: Identify Your Home Network IP Range**

* Find your local **IP address**:
  + **Windows:** Run in Command Prompt:
  + ipconfig
  + **Linux/macOS:** Run in Terminal:
  + ifconfig
  + Look for an address like **192.168.X.X** or **10.X.X.X** under **Wi-Fi or Ethernet Adapter**.
* Find your **network subnet** (common ones are 192.168.1.0/24 or 10.0.0.0/24).

**Step 3: Perform Basic Network Scan**

* Open a terminal or command prompt and run:
* nmap -sn 192.168.1.0/24
  + This scans all devices on the network without probing ports.
  + It lists active devices (your router, phone, laptop, smart devices, etc.).

**Step 4: Perform a Port Scan on a Device**

To check open ports on a specific device (e.g., your router with IP 192.168.1.1):

nmap -p- 192.168.1.1

* This scans **all** (0-65535) ports of the device.
* You can also scan common ports only:
* nmap -F 192.168.1.1
  + This scans the **top 100** most common ports.

**Step 5: Detect Services and OS**

To get detailed information about a device, run:

nmap -A 192.168.1.1

* This detects services (HTTP, SSH, etc.), operating system, and uptime.

**Step 6: Scan for Vulnerabilities (Optional & Ethical Use Only)**

To check for common vulnerabilities on a device:

nmap --script vuln 192.168.1.1

* **Only use this for ethical testing on your own devices.**

**Precautions & Ethical Considerations**

✅ **Use Nmap only on networks you own or have permission to scan.**  
✅ **Scanning unknown networks without authorization is illegal.**  
✅ **Avoid aggressive scanning on shared networks (e.g., school, work).**  
✅ **Ensure your firewall or security software allows scanning if needed.**

Would you like me to help analyze your scan results or refine your approach? 🚀