**01.What is Nmap? Install Nmap from Official Website?**

Nmap is a powerful and flexible open-source tool used for scanning and mapping networks. It helps identify hosts, open ports, running services, operating systems, and even vulnerabilities. It's widely used in cybersecurity assessments and ethical hacking.

Here are The some Features and Purpose

* Host Discovery used for the Find online devices
* Port Scanning used for the Check open/closed/filtered ports
* Service Version Detection used for the Find software version (e.g., Apache 2.4.29)
* Operating System used for the Detection Guess OS type (Linux, Windows, etc.)
* NSE Scripting Engine used for the Run custom or built-in scripts to find issues
* Stealth Mode used for the Evade detection by firewalls or IDS (e.g., -sS)

**Install Nmap from Official Website**

Install Nmap

Windows: Download from https://nmap.org/download.html → Choose the Windows installer.

Linux (e.g., Kali): Run

sudo apt update && sudo apt install Nmap

**02.Find your Ip range?**

Find Your Local IP Range

Open terminal and run:

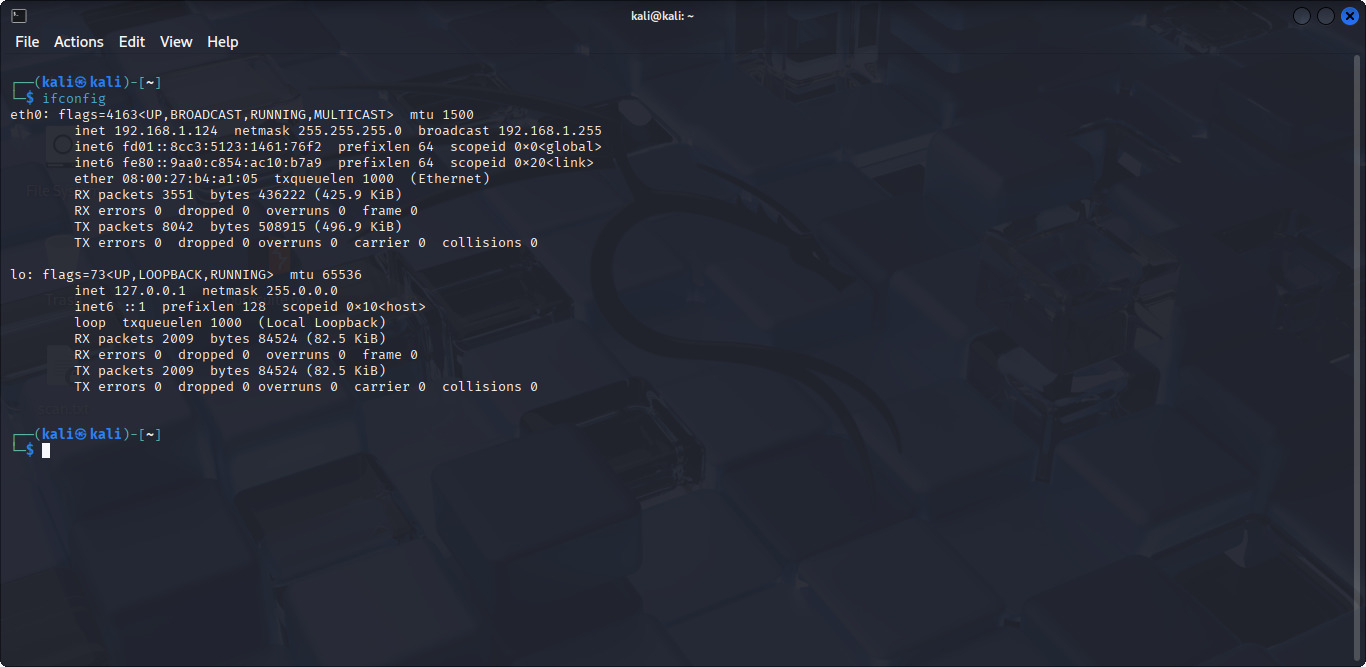
ip a # (Linux/Kali)

ipconfig # (Windows CMD)

Look for your IP, e.g., 192.168.1.12

Your network range will typically be 192.168.1.0/24, where:

192.168.1.0 is the network address

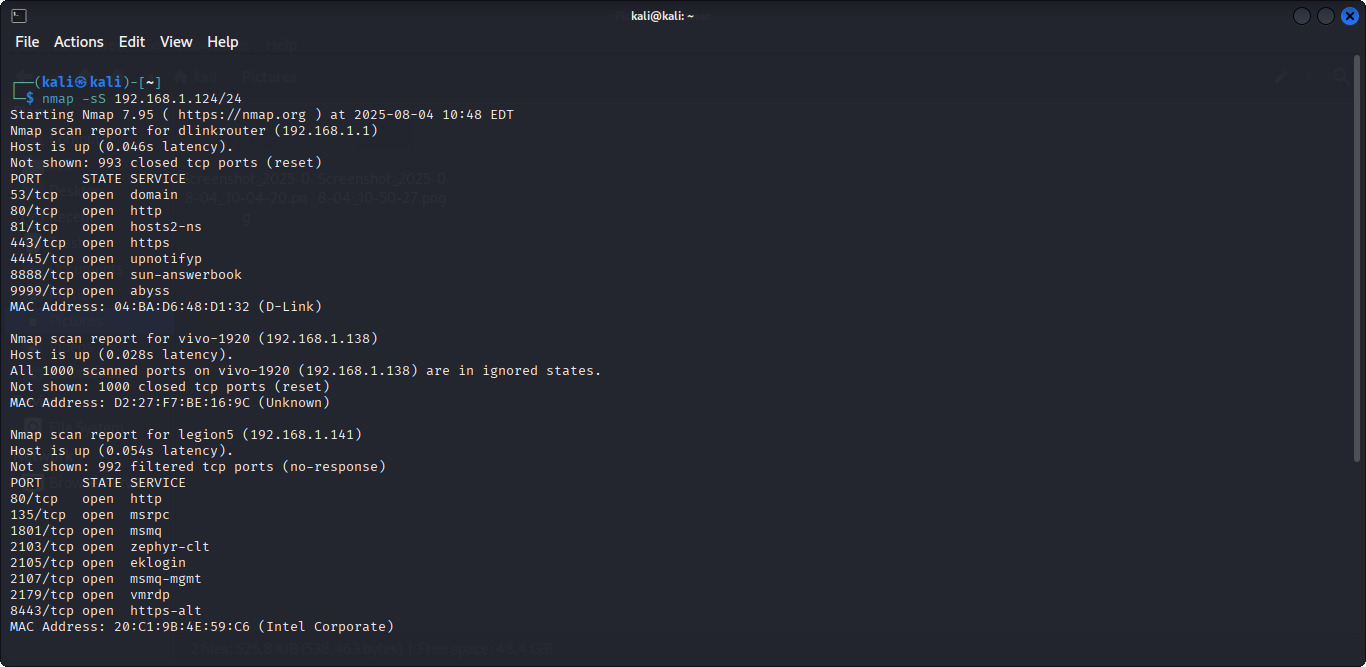


**03.RUN Nmap -sS IP address To perform TCP SYN Scan?**

**Command:- nmap -sS 192.168.1.124/24**

**sS = SYN scan (stealthy, faster)**

**This shows live devices and their open TCP ports**





**04.Optionally analyze packet capture with Wireshark?**

**Wireshark is a network protocol analyzer — a powerful tool used to capture, inspect, and analyze network traffic in real time.It lets you see everything happening on a network — like who is communicating with whom, what data is being sent, and which protocols are being used.**

**Open Wireshark and select your active network adapter.**

**ip.addr == 192.168.1.X**A screenshot of a computer

AI-generated content may be incorrect.

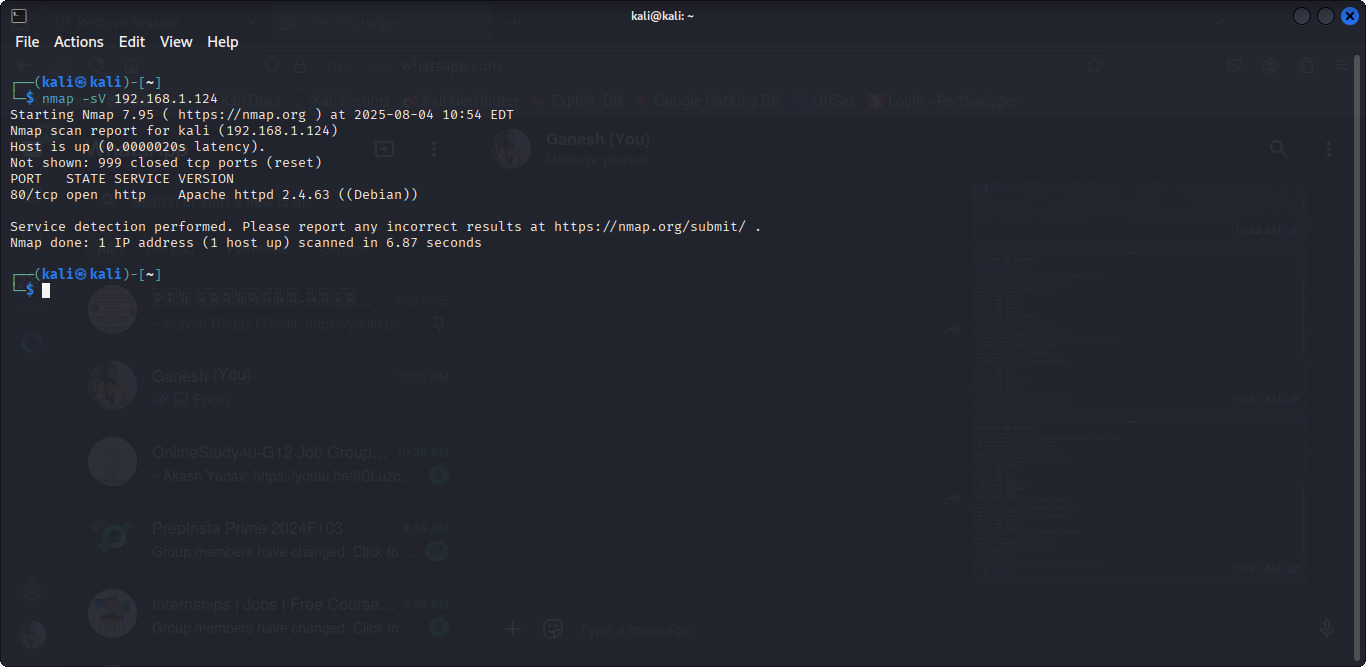
**You can see the live packets while Nmap is scanning.**

**06.** **6.Research common services running on those ports.**

**Look up ports and services:**

* **Port 22 → SSH**
* **Port 80 → HTTP (Web)**
* **Port 443 → HTTPS**
* **Port 445 → SMB (Windows File Sharing)**
* **Port 3306 → MySQL**

**Command:- nmap -sV 192.168.1.124**

* 

**07.Identifying potential security risks from open ports?**

**When you scan a system with tools like \*Nmap, open ports can reveal \*\*vulnerable services\* or \*entry points\* for attackers.**

|  |  |  |
| --- | --- | --- |
| **Port** | **Port** | **Potential Risk** |
| **21** | **FTP** | **Unencrypted login; susceptible to brute-force or anonymous access** |
| **22** | **SSH** | **Brute-force attack, weak passwords, outdated SSH version** |
| **23** | **Telnet** | **Unencrypted communication; attacker can sniff login credentials** |
| **25** | **SMTP** | **Open relays used to send spam; vulnerable to spoofing** |
| **53** | **DNS** | **Can be used for DNS poisoning or amplification DDoS attacks** |
| **80** | **HTTP** | **If web server has vulnerabilities (e.g., outdated WordPress, Apache)** |
| **443** | **HTTPS** | **Misconfigured SSL/TLS can expose to MITM attacks** |
| **110** | **POP3** | **Credentials sent in plain text if not secured** |
| **139/445** | **SMB** | **Used in WannaCry ransomware attack; vulnerable to remote code execution** |
| **3306** | **MySQL** | **Can expose databases if misconfigured or default passwords used** |
| **3389** | **RDP** | **Targeted in brute-force and remote desktop attacks** |

**How Open Ports Become a Risk:**

**Outdated Software– Unpatched services listening on open ports.**

**Default Credentials – Especially common in routers, FTP, or DB services.**

**No Access Control – Services like MySQL or MongoDB exposed to the internet.**

**Port Forwarding Misuse – From NAT/router misconfigurations.**

**No Firewall or IDS/IPS – System is directly exposed.**