🛡️ 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 and improve security awareness.

Tools Required:

* Nmap (network scanning tool)
* Wireshark (optional for packet analysis)

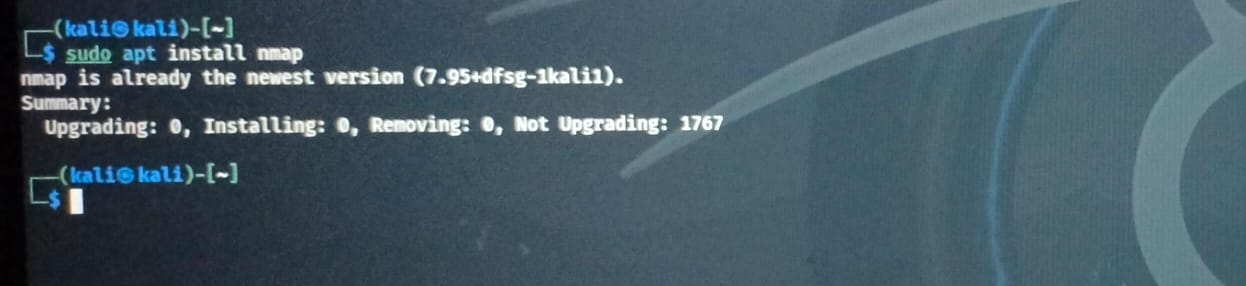
Step 1: Install Nmap (if not already installed)

Kali Linux typically comes with Nmap pre-installed. To check:

Bash: sudo apt update

sudo apt install nmap

Output:



Step 2: Identify Your Local Network IP Range

You need the IP address and subnet to scan your network.

Run:

Bash: ip a

Or

Ifconfig

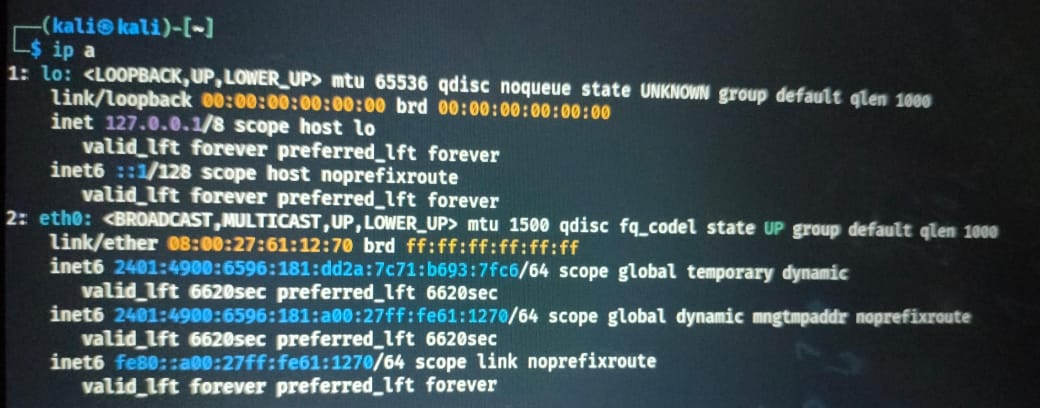
Or

Ip addr show

Sample Output:

inet 192.168.1.5/24

Output:



Here, 127.0.0.1/8 is your subnet (255.255.255.0).

Step 3: Perform a Basic Network Scan

Run a ping sweep to find live hosts:

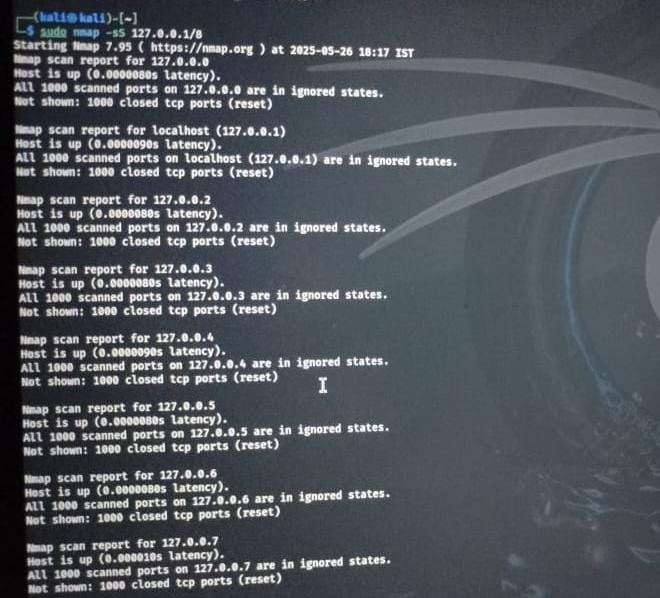
Bash: nmap -sn 127.0.0.1/8

Now perform a TCP SYN scan:

Bash: sudo nmap -sS 127.0.0.1/8

* -sS = SYN scan (stealthy and fast)
* Use sudo for best results (to allow raw packet sending)

Output:



Step 4: Analyze the Output

Nmap will show a list of live IP addresses and open ports, such as:

Sample Output:

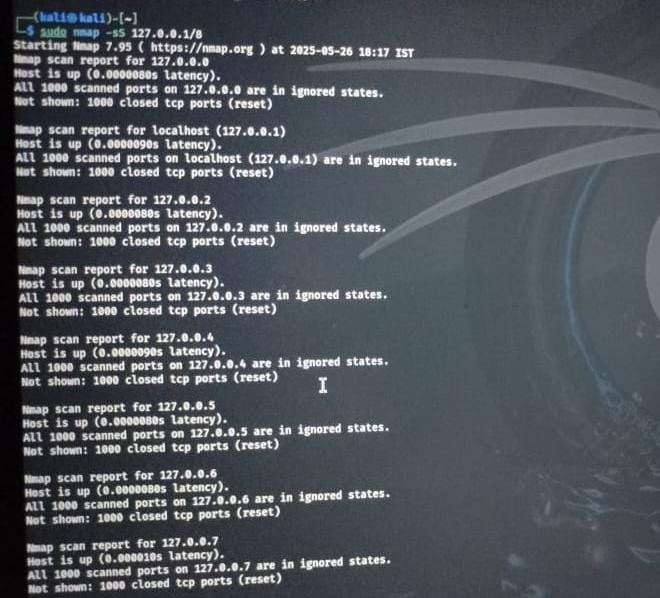
Nmap scan report for 127.0.0.1/8

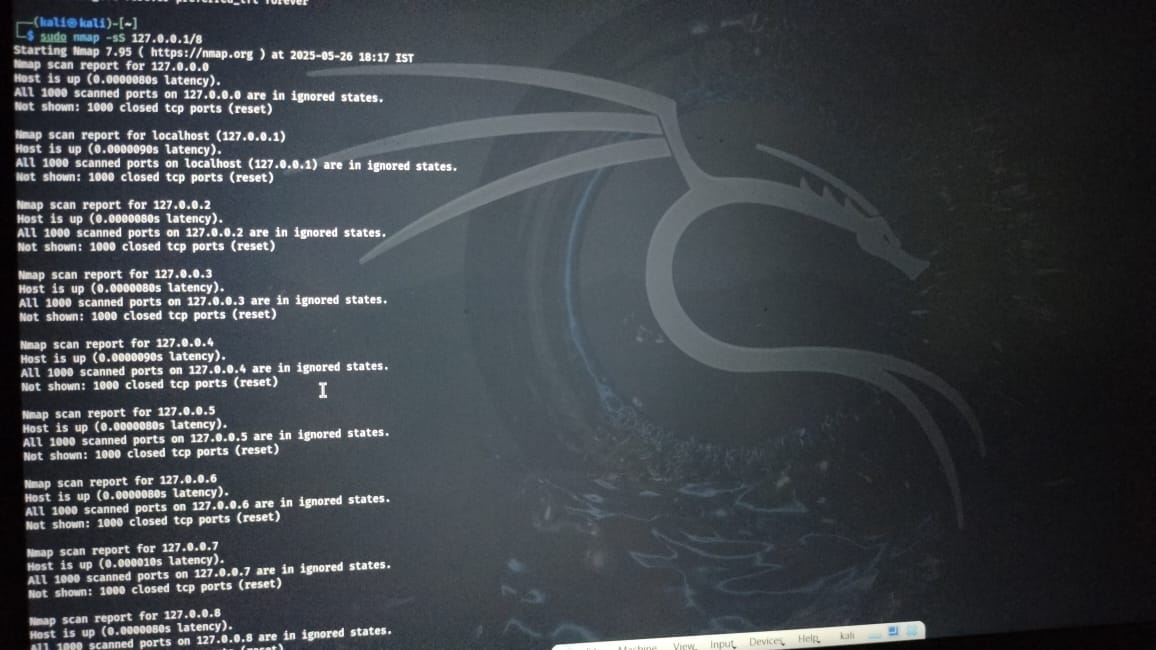
PORT STATE SERVICE

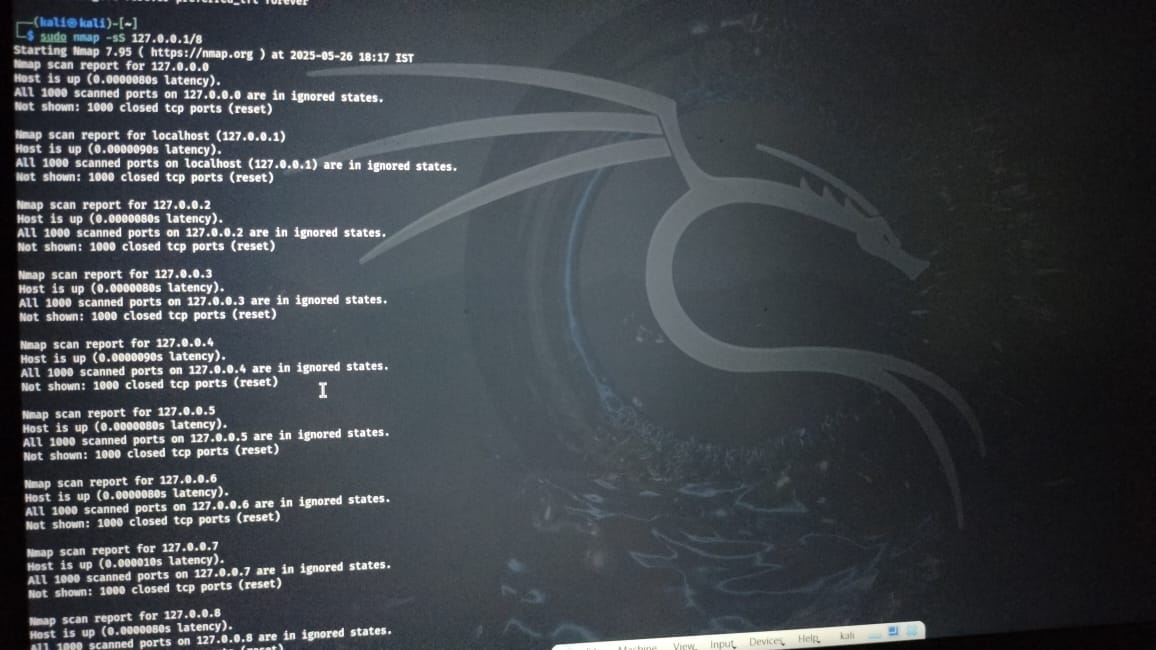
22/tcp open ssh

80/tcp open http

Output:







Step 5 (Optional): Capture and Analyze with Wireshark

1. Open Wireshark:

**Bash:** sudo wireshark

Output:

ip.addr == 127.0.0.1/8

tcp.port == 22

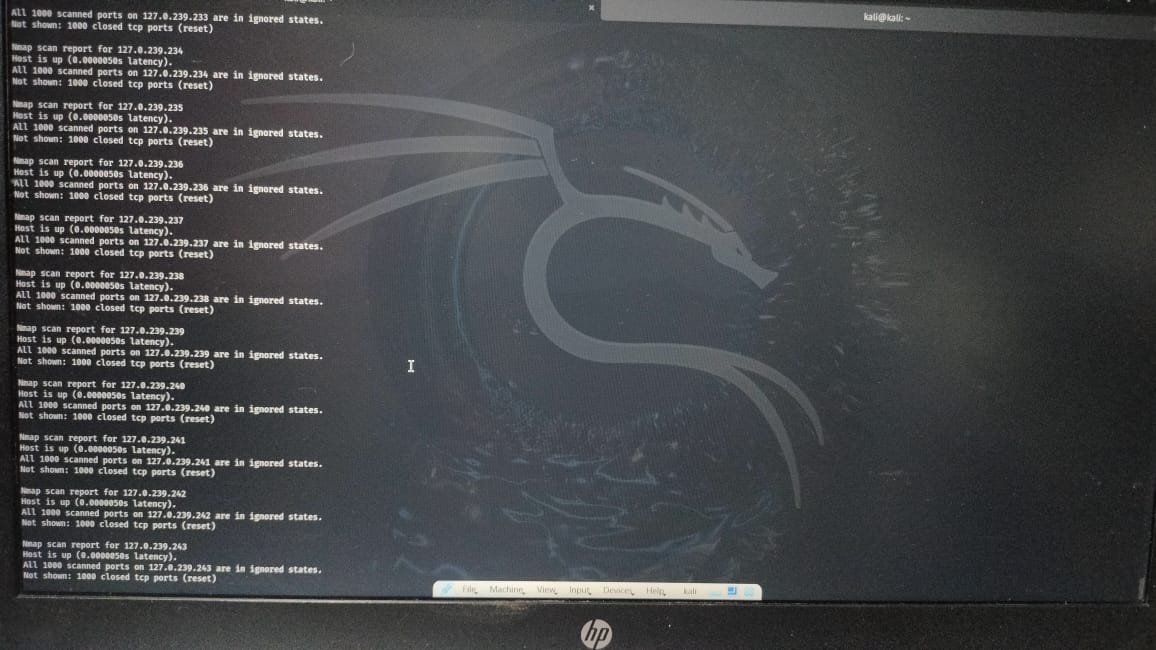
1. Stop capture and analyze traffic, especially SYN, SYN-ACK, and RST packets.

Step 6: Research Common Services

Check what services are typically associated with the open ports found:

* 22/tcp → SSH
* 80/tcp → HTTP
* 443/tcp → HTTPS
* 21/tcp → FTP
* 23/tcp → Telnet

Step 7: Identify Potential Security Risks



| **Port** | **Protocol** | **Common Service** | **Notes** |
| --- | --- | --- | --- |
| 22 | TCP | SSH | Secure remote login |
| 23 | TCP | Telnet | Insecure, should be avoided |
| 80 | TCP | HTTP | Unencrypted web traffic |
| 443 | TCP | HTTPS | Encrypted web traffic |
| 3389 | TCP | RDP | Remote Desktop Protocol (Windows) |
| 21 | TCP | FTP | Insecure file transfer |
| 445 | TCP | SMB | Windows file sharing |
| 53 | UDP/TCP | DNS | Domain resolution |
| 3306 | TCP | MySQL | Database server |
| 5900 | TCP | VNC | Remote desktop sharing |

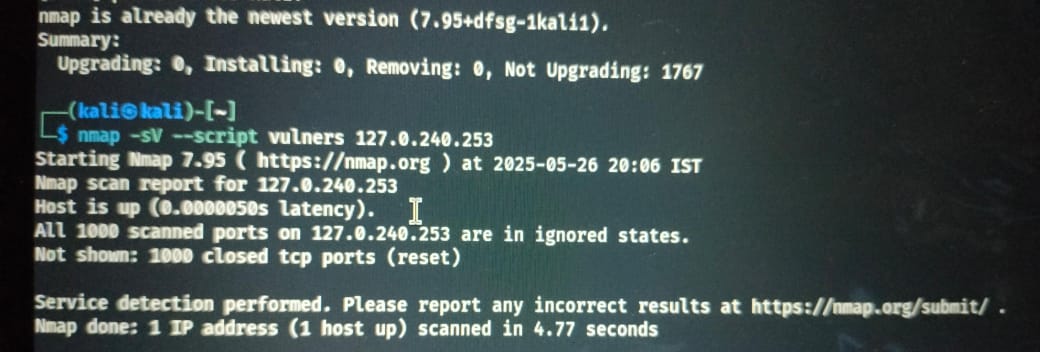
> Use search tools like CVE databases or:

Bash: nmap -sV --script vulners <target\_ip>

Or try:

nmap --script vuln <target\_ip>

Output:



Step 8: Save the Scan Results

Text output:

Bash:

sudo nmap -sS 127.0.0.1/8 -oN scan\_result.xml

CONCLUSION:

By this task we will understand how attackers or network administrators identify vulnerable systems. Learning to scan and assess a network is a first step toward:

* Penetration testing
* Vulnerability assessment
* Network hardening
* Ethical hacking

🧠 2. Practical Knowledge of Networking

By working with tools like Nmap and Wireshark, you’ll gain hands-on experience with:

* IP addressing and subnetting (e.g., 192.168.1.0/24)
* Network protocols (TCP, UDP, ICMP)
* Common ports and services (SSH, HTTP, FTP, etc.)
* Live host detection and enumeration

🧰 3. Tool Proficiency (Nmap, Wireshark)

You’ll get comfortable using industry-standard tools:

* 🔍 **Nmap** – for scanning and reconnaissance
* 📡 **Wireshark** (optional) – for packet-level analysis

These are among the most used tools in cybersecurity, network engineering, and digital forensics.

🧾 4. Analytical Thinking & Risk Assessment

You’ll learn how to:

* Interpret scan results
* Understand what each open port means
* Identify misconfigured or exposed services
* Recommend mitigation steps (e.g., firewall rules, disabling services)

This helps build your ability to think like a security analyst or attacker.

🧪 5. Hands-On Experience (Real-World Simulated Task)

This task mimics what professionals do in the field when auditing networks. You're not just learning theory—you’re doing actual recon on a live network (your local LAN).

🔁 7. Awareness of Your Own Network's Security

You’ll get insights into:

* What devices are on your network
* Which ports are open and potentially vulnerable
* Whether any unnecessary or dangerous services are running

This increases your personal or organizational cyber hygiene.