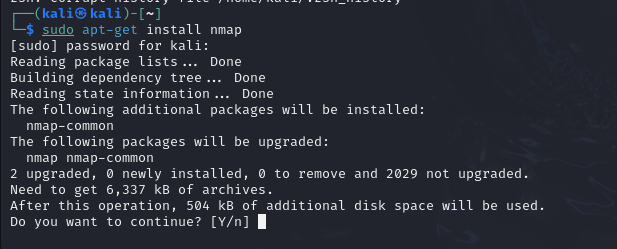
**Port scanning, TCP SYN scan, IP ranges, network reconnaissance, open ports, network security**

**Task 1: Scan Your Local Network for Open Ports**

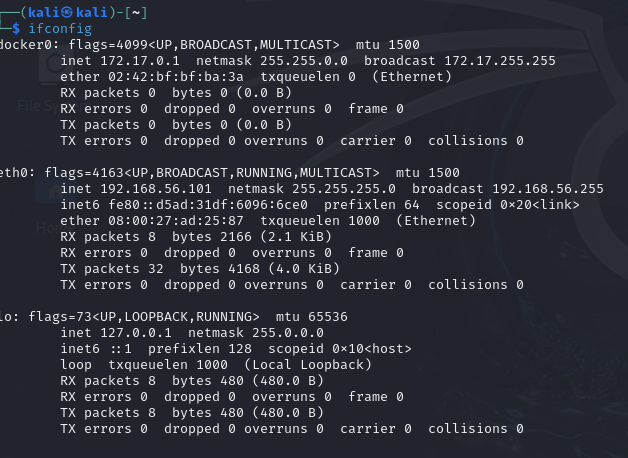
* **Objective**: Learn to discover open ports on devices in your local network to understand network exposure.
* **Tools:** Nmap , Wireshark.

1. **Install Nmap from official website**

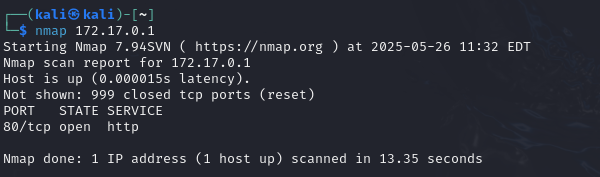
**Install Nmap in kali linux : sudo apt-get install nmap**

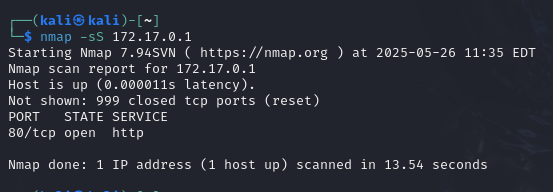


**2. Find your local IP range: ifconfig**

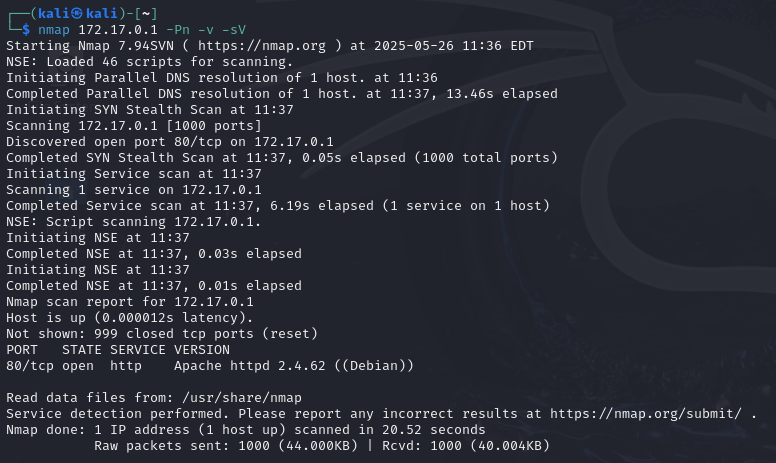


**3. Run: nmap scan**





**Nmap Portscan: nmap 172.17.0.1 –Pn –v –sV**



**4.Note down IP addresses and open ports found.**

#### Target IP Address: 172.17.0.1

#### Open Port Found:

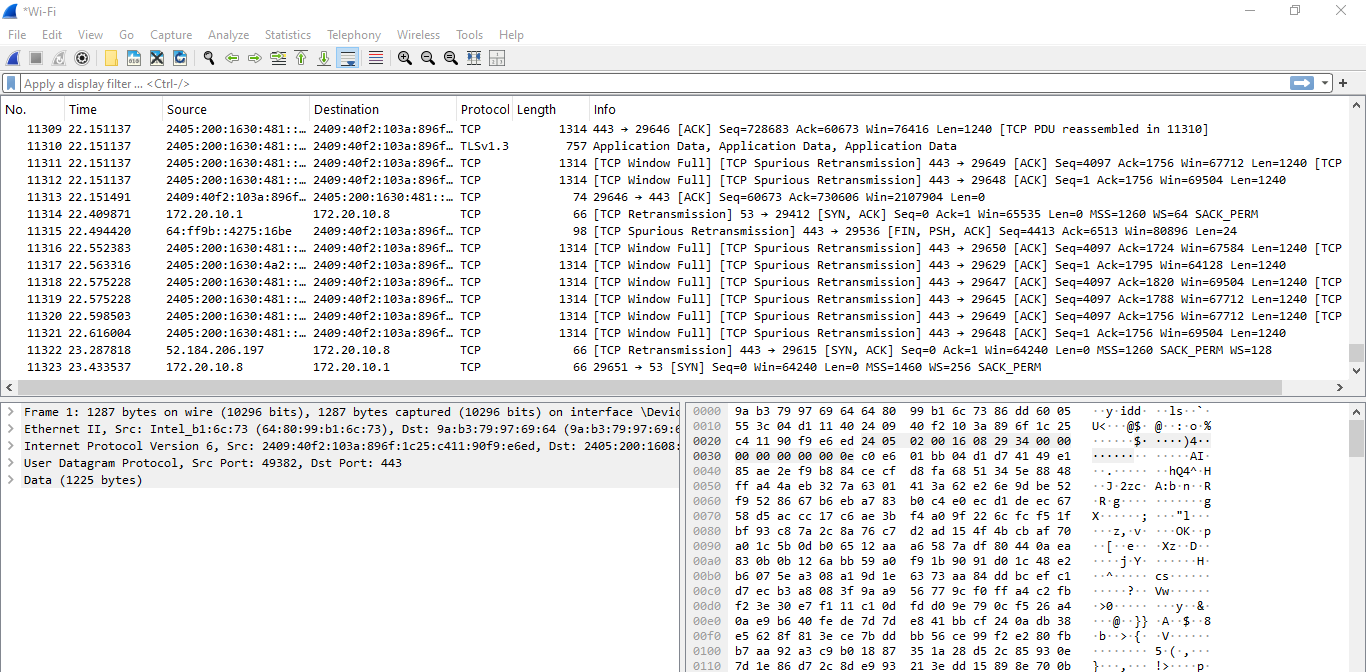
#### Port 80/tcp

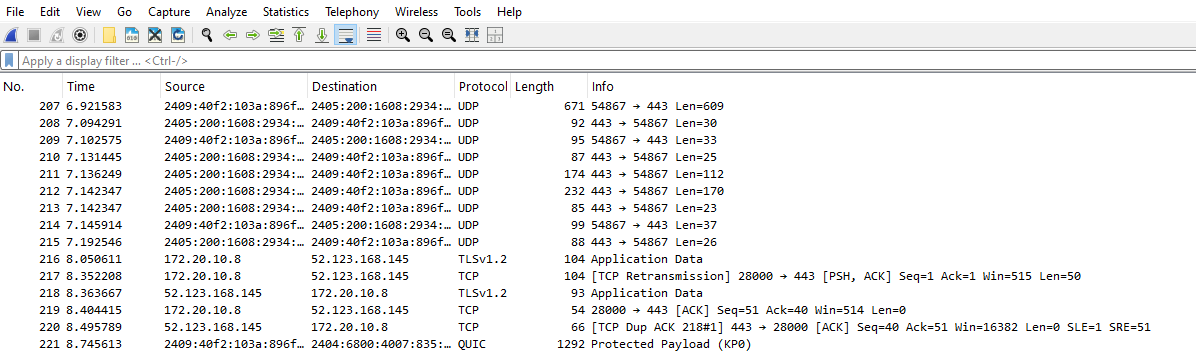
#### State: Open

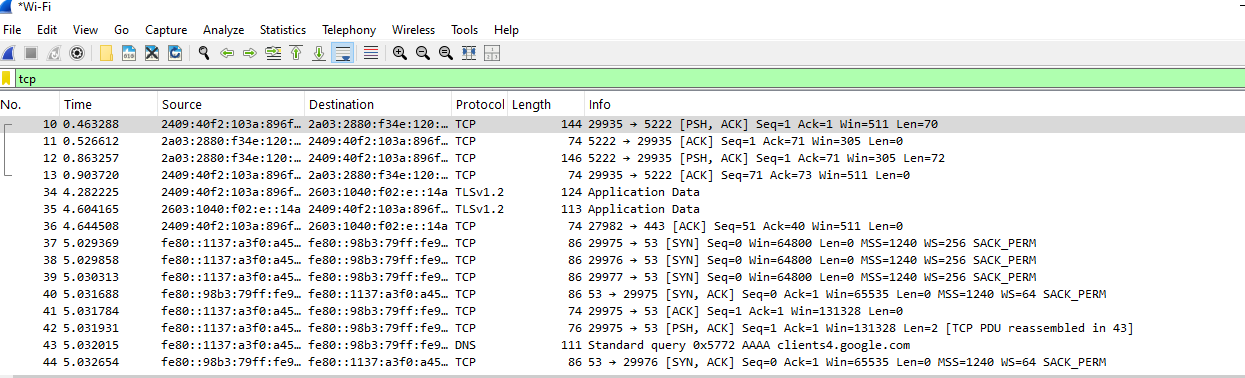
#### Service: HTTP

#### Version: Apache httpd 2.4.62 (Debian)

**5. Analyze packet capture with Wireshark.**







**Research: Common Service on Port 80:**

Port 80 (HTTP):

Port 80 is used for HTTP, the standard protocol for unencrypted web traffic.

Commonly hosted by Apache, Nginx, or IIS servers.

It is widely used for web servers but does not provide encryption, meaning data is sent in plain text.

**Potential Security Risks of Open Port 80**

| **Risk** | **Description** |
| --- | --- |
| **Lack of Encryption** | All data transferred is in plain text. Can be intercepted (man-in-the-middle attacks). |
| **Outdated Software** | Apache 2.4.62 may have known vulnerabilities |
| **Exposure to Recon Tools** | Easily detectable via tools like Nmap, Shodan, etc. |
| **Misconfigurations** | Default files or directories might expose sensitive data. |
| **Exploit Vectors** | Vulnerabilities in HTTP headers, directory traversal, or server misconfigurations can be exploited. |

**Packet Analysis Using Wireshark:**

Key Observations:

* **TCP Handshakes** were clearly captured (SYN, SYN-ACK, ACK).
* Communication on **port 80** and **443** (HTTPS) was also visible.
* **TLSv1.2** suggests some secure connections were happening on other services (likely web browsing or background app connections).
* Multiple packets show [PSH, ACK], which are used in data transfer after handshakes.

**Recommendations:**

 **Redirect Port 80 to 443** using HTTPS with SSL/TLS.

 **Harden Apache**:

* Disable directory listing
* Remove default pages
* Keep the server software updated

 **Apply Firewall Rules**:

* Only allow port 80 if absolutely necessary.
* Restrict access using IP filtering or firewall rules.

 **Perform Vulnerability Scanning**:

* Use tools like Nikto, OWASP ZAP, or Nessus to assess weaknesses.

 **Monitor Logs**:

* Enable detailed Apache logging and analyze for suspicious patterns.