Task 1

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

**Tools:**  Nmap, Wireshark, Kali Linux (OS).

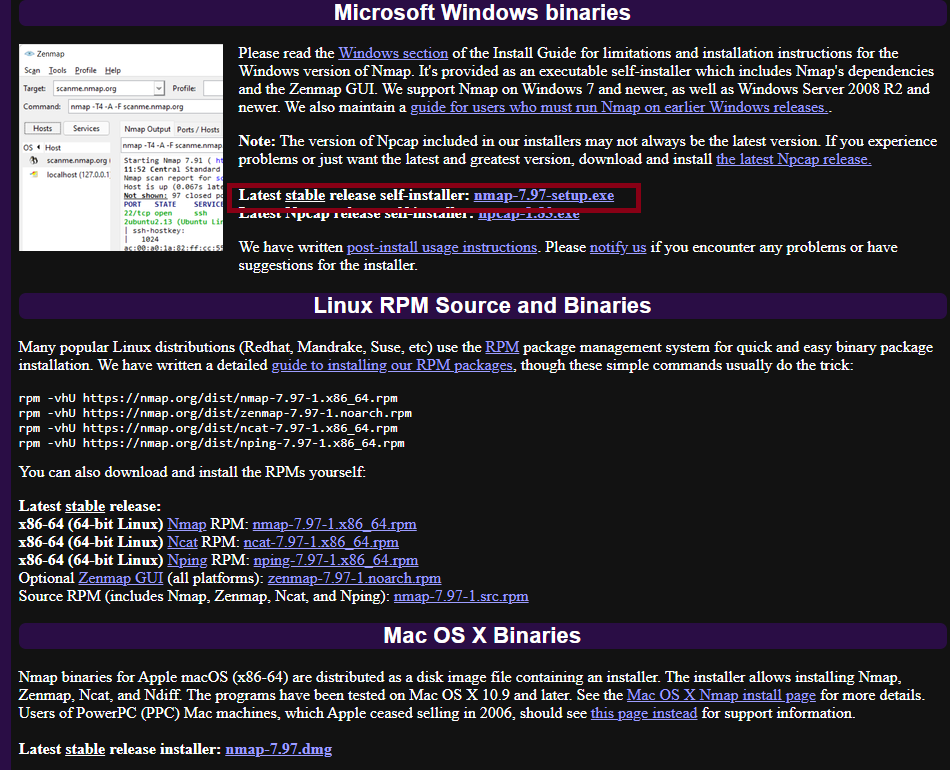
**Key Concepts:** Port scanning, TCP SYN scan, IP ranges, network reconnaissance, open ports, network security basics

**Execution:**

**Note:** I completed the task in kali linux (Debian based OS, installed in windows through virtual box)

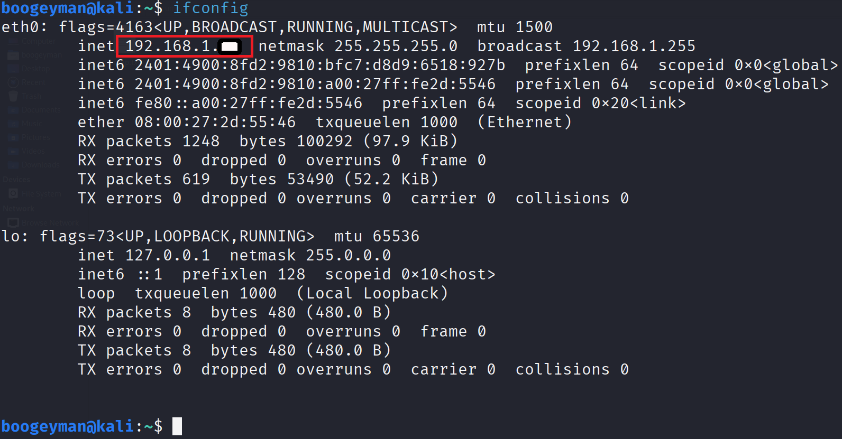
**Step-1:** Installing Nmap from official website. For windows, we have to install it from the official site. But in Kali Linux

Nmap is already registered. Make sure it is update to latest level.



(*Fig. 1*)

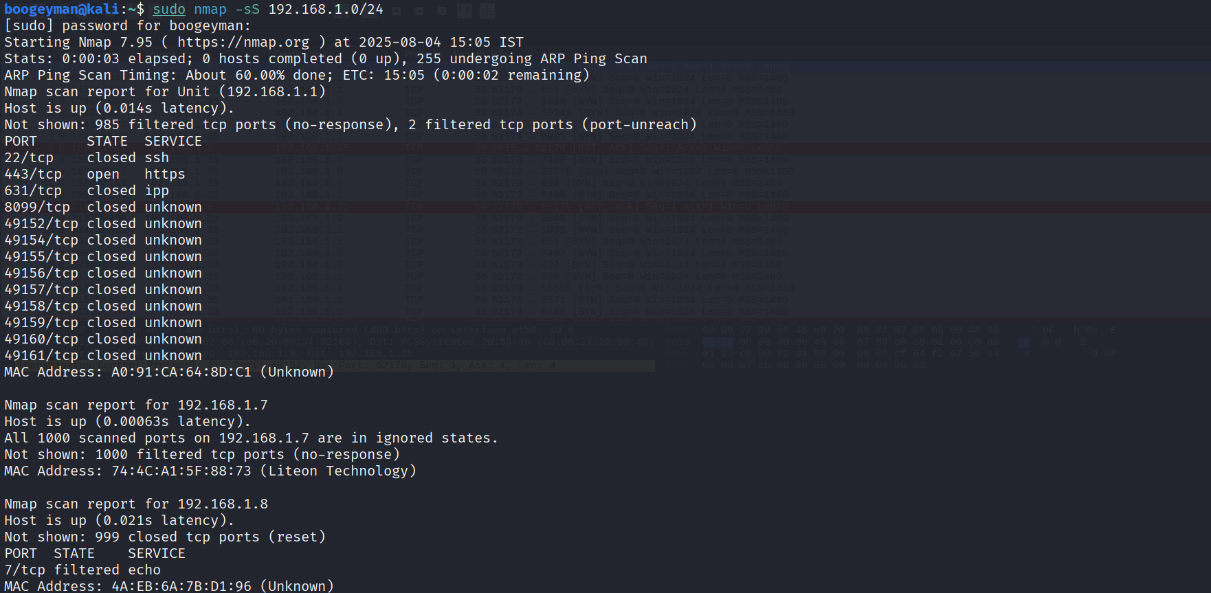
**Step-2:** Once updated, we can find our local IP range. Use *ifconfig* command to get the IP range.



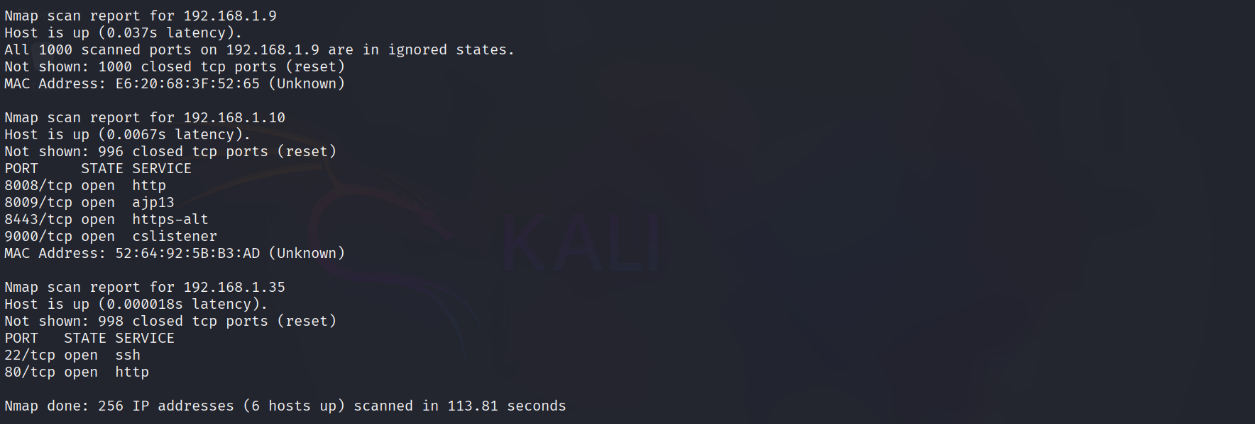
(*Fig. 2*)

**Step-3:** Now for the perform TCP Syn scan. Use *sudo nmap -sS 192.168.1.0/24*. The command “sudo” is required

to execute commands that requires administrator level permission.



(*Fig.3*)

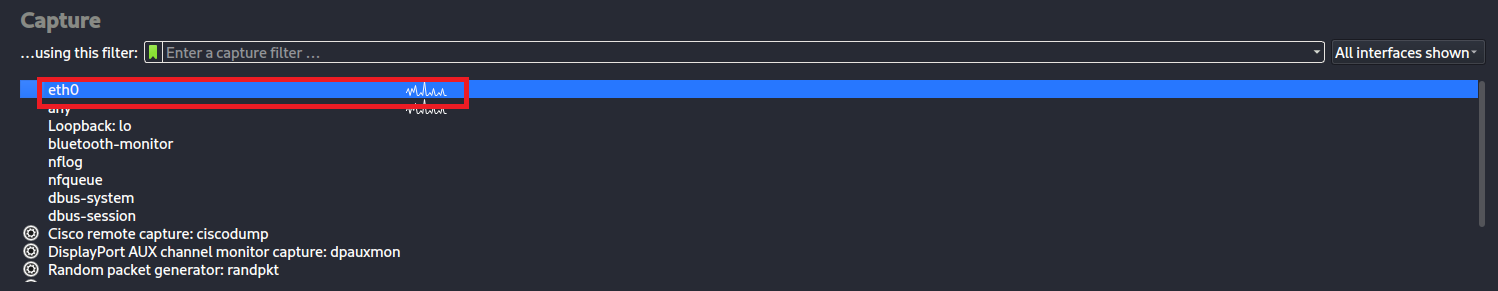


(*Fig. 4*)

**Step-4:**  Now for packet analysis, we need to sue **wireshark**. We can install wireshark from official website for

windows. For Kali linux, it is preinstalled. Make sure it is update to latest level.

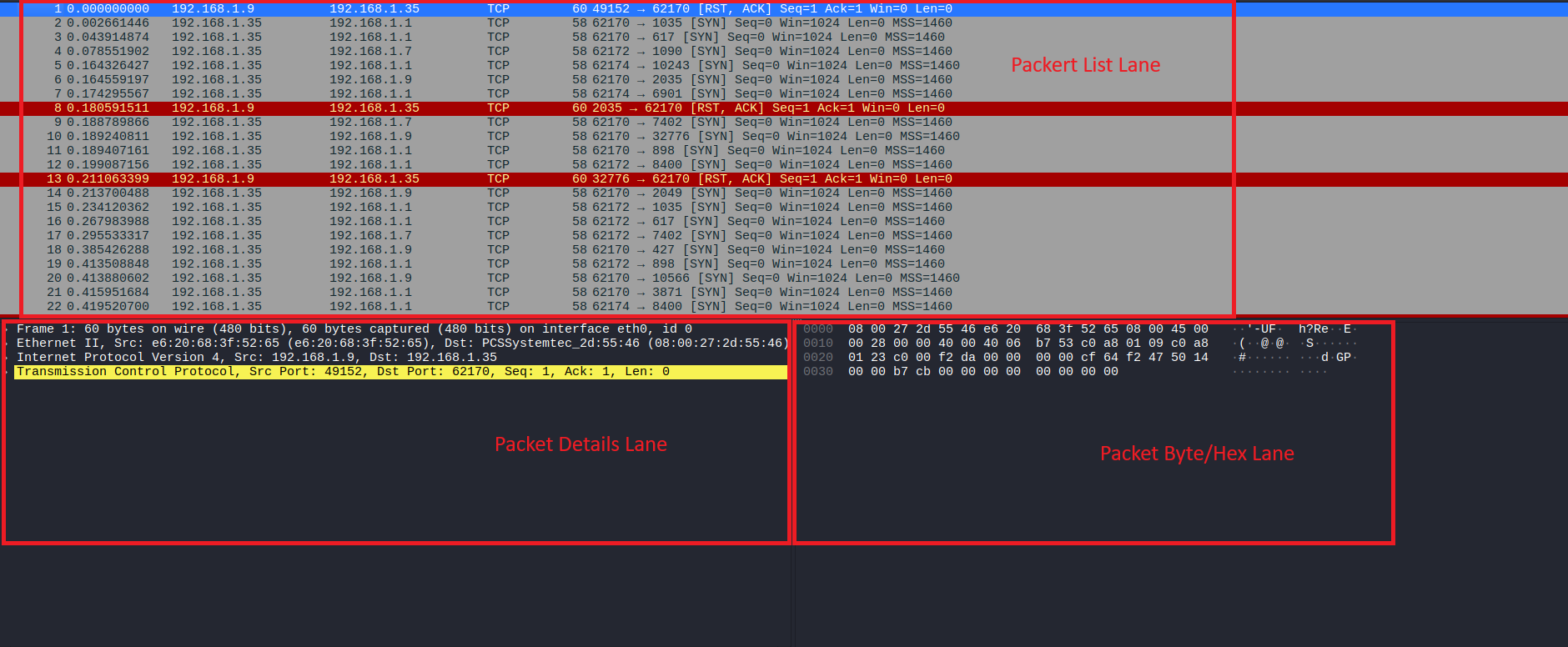
Step-5: We can start wireshark from terminal or we can start it from start option.



(*Fig. 5*)

*Note:* The eth0 is the interface for our localhost to capture packets.

**Step-7:** After selecting the *eth0*  interface, the packet capturing starts.



(*Fig. 6)*

**Note:** The highlighted region in the wireshark interface described in the image. The packets coloured in red at the *rst* flag/request.

**Step-6:** Some common services running on those ports. The open ports are Ssh (Secure Shell) on port 22 and

Apache2 on port 80.

* The SSH (Secure Shell) is a cryptographic network protocol primarily used for securely

accessing and managing devices and servers over an unsecured network. It is widely used by

system administrators and developers for several purposes.

* Apache2 (Apache HTTP Server), which operates on port 80, is a crucial component of web hosting.

Port 80 is the standard port for HTTP (Hypertext Transfer Protocol) traffic on the web. When one

enters a web address (e.g., http://example.com) in your web browser, your web browser is connected

to the web server on port 80 by default.

**Step-7:** Identification of potential security risks from open ports

1. Port 22 (SSH) –
   1. Brute-Force Attacks: Attackers might try guessing passwords and usernames through automated brute-force scripts.
   2. Taking advantage of Vulnerabilities: If SSH server software is outdated, known vulnerabilities can be exploited to obtain unauthorized access.
   3. Weak Authentication: Utilizing weak passwords or password-based authentication (rather than key-based) poses threat.
2. Port 80 (HTTP) –
   1. **Threats Unencrypted Traffic:** All, such as credentials or sensitive data, is sent in plaintext and can be intercepted and therefore insecure against man-in-the-middle or sniffing attacks.
   2. **Web Application Vulnerabilities:** Open port 80 usually refers to a web server (i.e., Apache). If the web site or server software is vulnerable (e.g., XSS, SQL injection, code execution vulnerabilities), these can be exploited by attackers.
   3. Reconnaissance involves attackers probing the web server to obtain version information and known vulnerabilities, thereby preparing for targeted attacks.

**Step-8:**  Save scan results as a text or HTML file.

The scan results are saved in a file named nmap\_res.txt