**CYBER SECURITY INTERNSHIP DAY-1**

submitted by

**Radhika**

[**Rradhika0011@gmail.com**](mailto:Rradhika0011@gmail.com)

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

**Tools**: Nmap, Wireshark

**Outcome**: Basic network reconnaissance skills; understanding network service exposure.

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

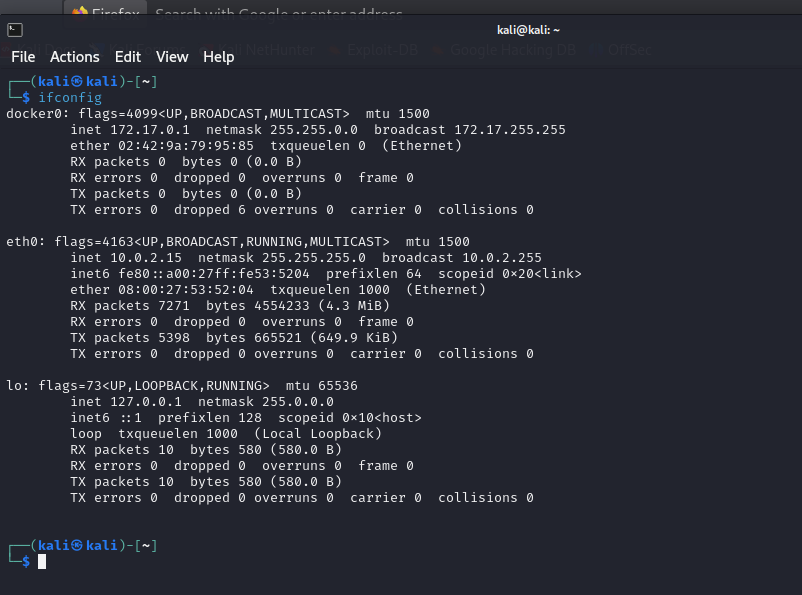
***Task 1 - Identify Live Hosts on a Network***

**Step 1: Open your Kali Linux**

**Step 2: Open Terminal**

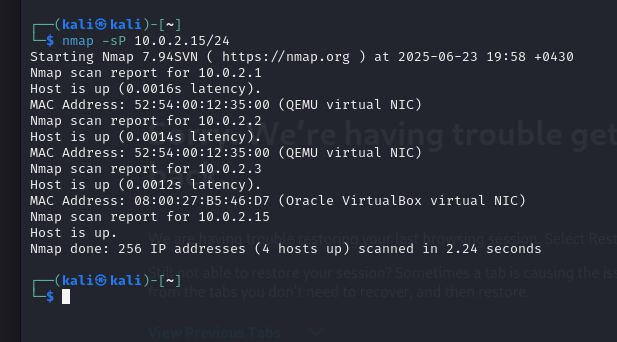
****

**The ifconfig (interface configuration) command is used in Unix-based systems to configure and display network interface information. It helps in managing IP addresses, network interfaces, and network connections.**

****

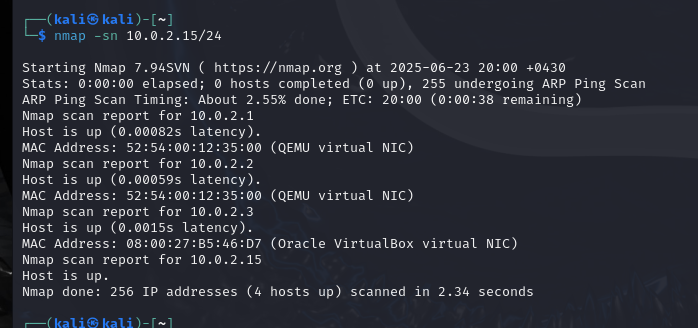
**I got the IP 10.0.2.15**

**Step 3: The terminal window is displayed. Performing a ping scan to discover the live hosts in a network.**

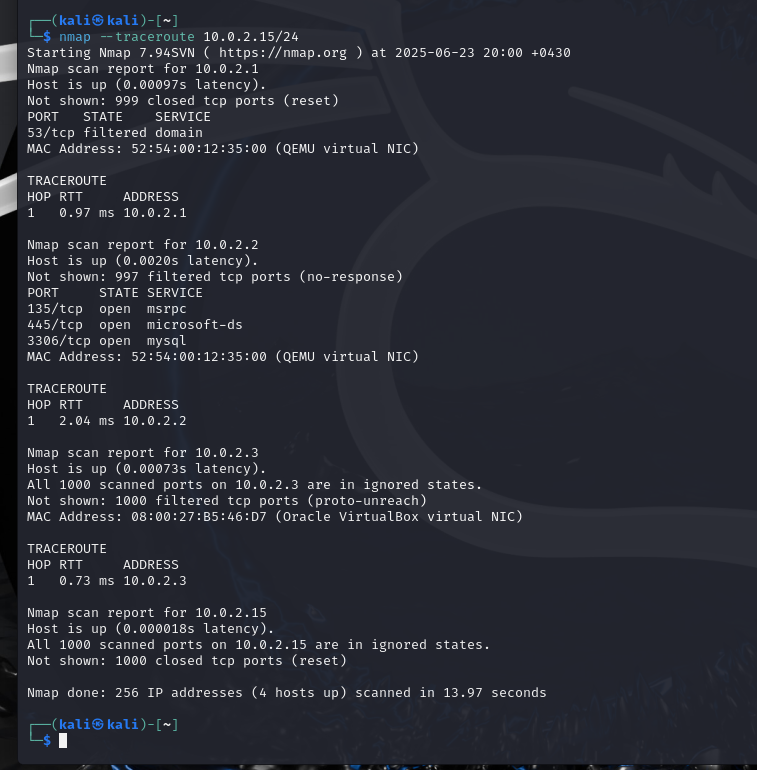
****

**4 hosts up**

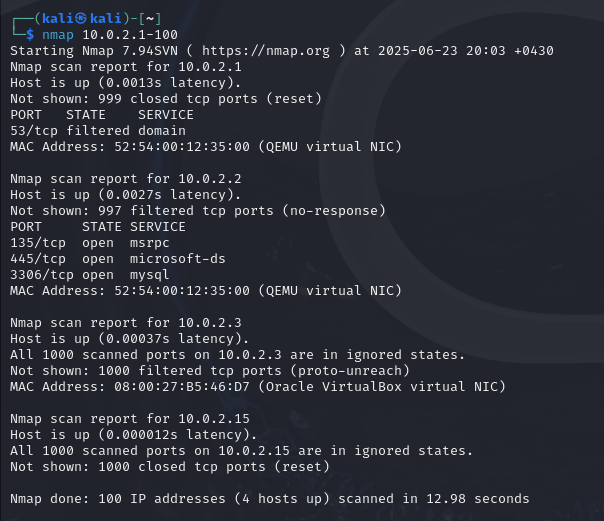
**Step 4: Performing a scan without ping. Performs a ping sweep to detect live hosts in the given network range. Useful for discovering active devices on a network.**

****

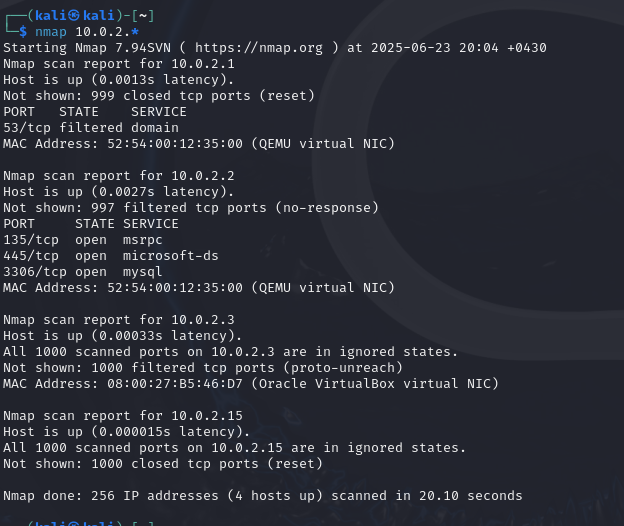
**Step 5: You can also trace the path between your system and each of the hosts that is live on the network. It is used to trace the network path (hops) between your machine and the target.**

****

**Step 6: You can also scan for live hosts on a network using an IP address range.**

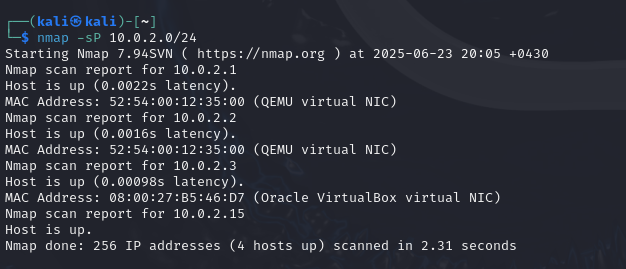
****

**Step 7: You can also use a wildcard to scan an IP range. It has searched for all live systems in the subnet of 256 IP addresses.**



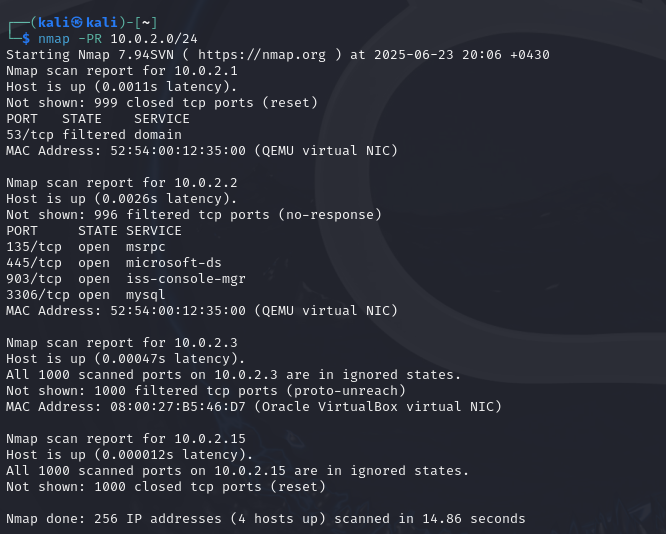
***Task 2: Perform Discovery Scans***

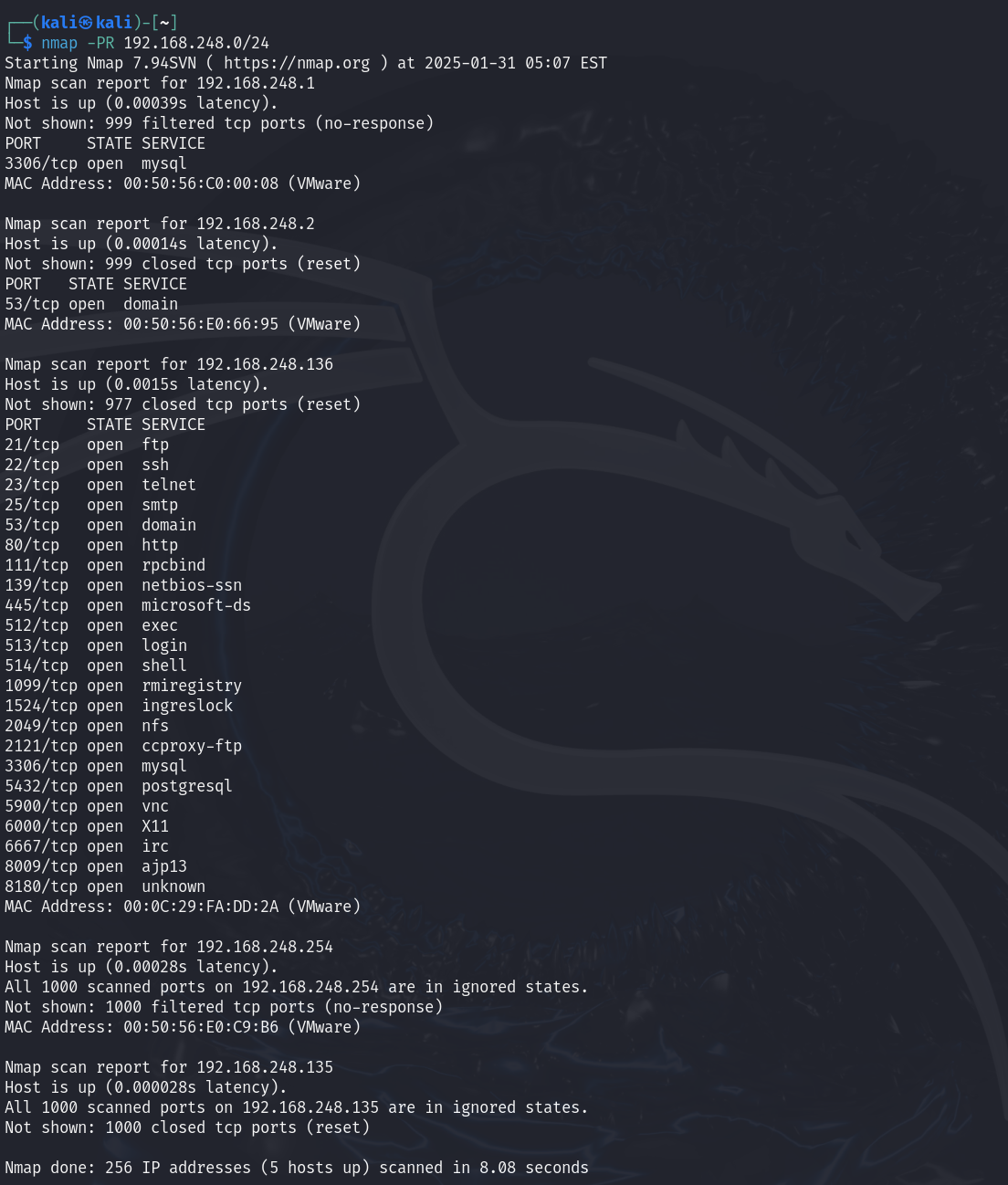
**Ping for discovering a host. When you execute this command, it sends an ICMP REQUEST message to every IP address. The hosts that respond to the ICMP REQUEST message are considered alive.**

******

**Sending ARP (Address Resolution Protocol) requests to the hosts on a given subnet, and if the target system responds to these requests, then it means that it is alive. This method, unlike the Ping scan method, is not usually blocked by the firewall. Therefore, you are likely to get a better outcome.**

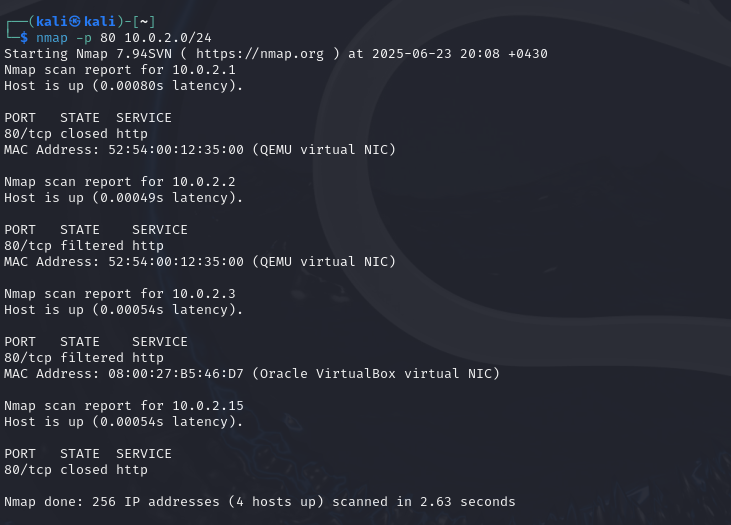
**-Best for LAN scans (faster & more reliable than ICMP pings).  
-Bypasses firewall restrictions blocking normal ping scans.  
-Efficient in Wi-Fi network enumeration for ethical hacking.**

****

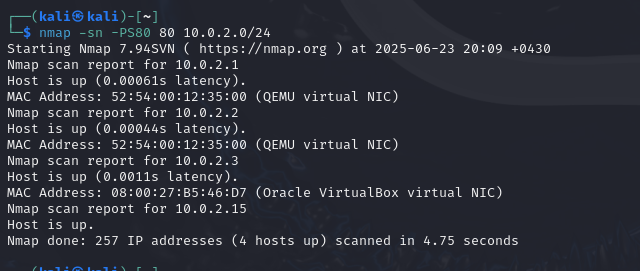
****

**Scanning for open ports to detect the system status. This could be useful when the systems have firewalls enabled, or the systems are in another subnet or network. When you attempt to detect the ports, the systems will respond to the request.**

**-Focus on specific ports instead of scanning all 1,000 default ports.  
-Helps in stealth scanning (narrowing targets for efficiency).  
-Useful for checking open/closed/filtered ports on a network.**

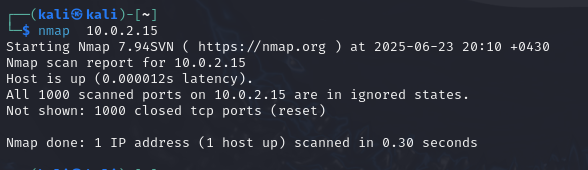
****

**Sending the SYN message to a specific port on a subnet to detect live systems.**

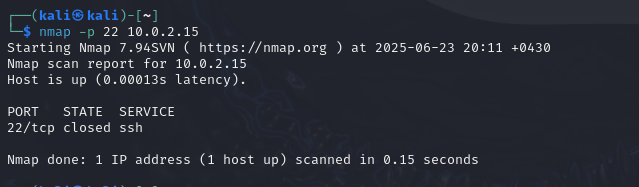


***Task 3: Perform Port Scanning***

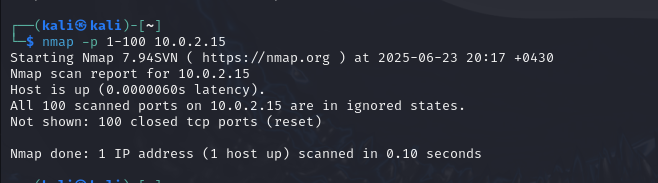
**One of the simplest methods is to target a system with the nmap command without using any parameters.**

****

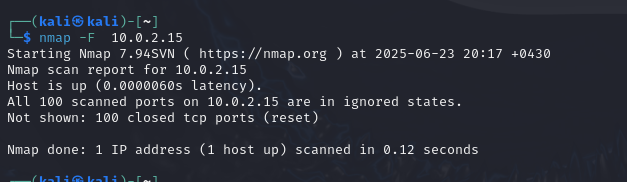
**Scanning for a single port on a host.**

****

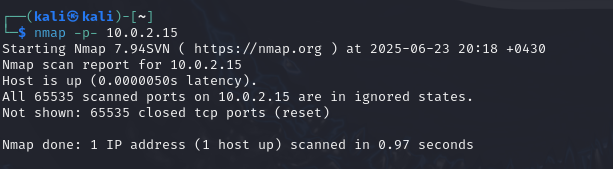
**Scan the range of ports.**

****

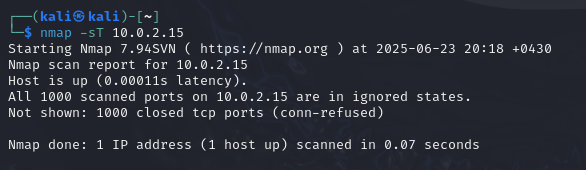
**Fast scan will scan for the 100 common ports on a given system.**

****

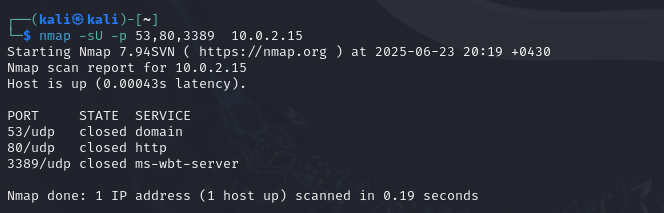
**Scanning for all 65535 ports on a system.**

****

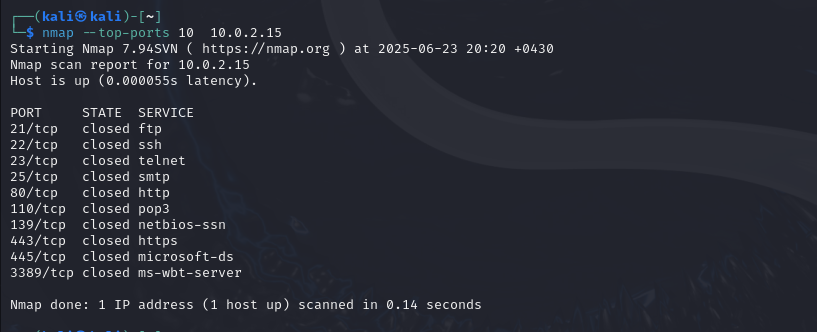
**Performing port scanning using TCP connect.**

****

**Perform port for the selective UDP ports.**

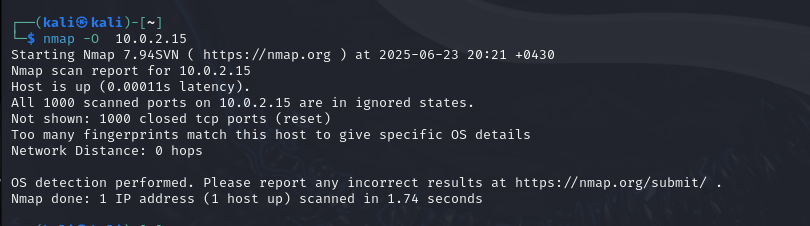
****

**Using the --top-ports parameter with a specified number to find ports.**



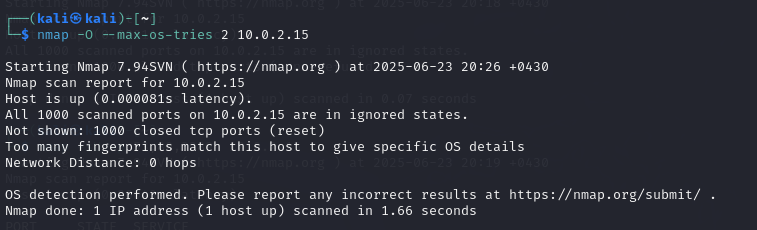
***Task 4: Fingerprint an Operating System***

**The -O parameter provides more options for operating system detection.**

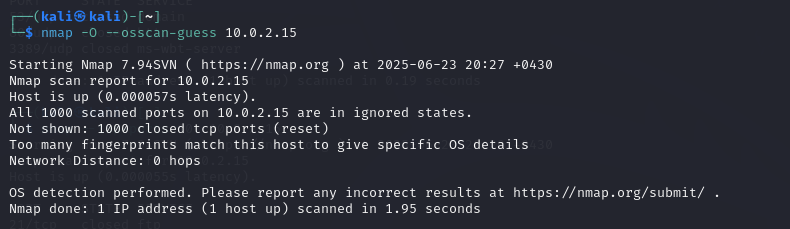
******

**Running and scan for the operating system only on the live hosts.**

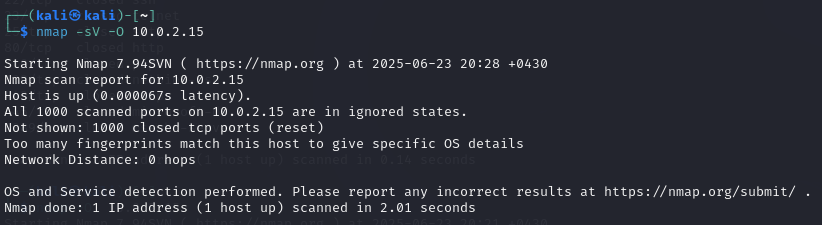
**Performing an operating system scan, Nmap, by default, attempts five times to detect the name and version. However, to speed up the process, can limit the number of attempts.**

****

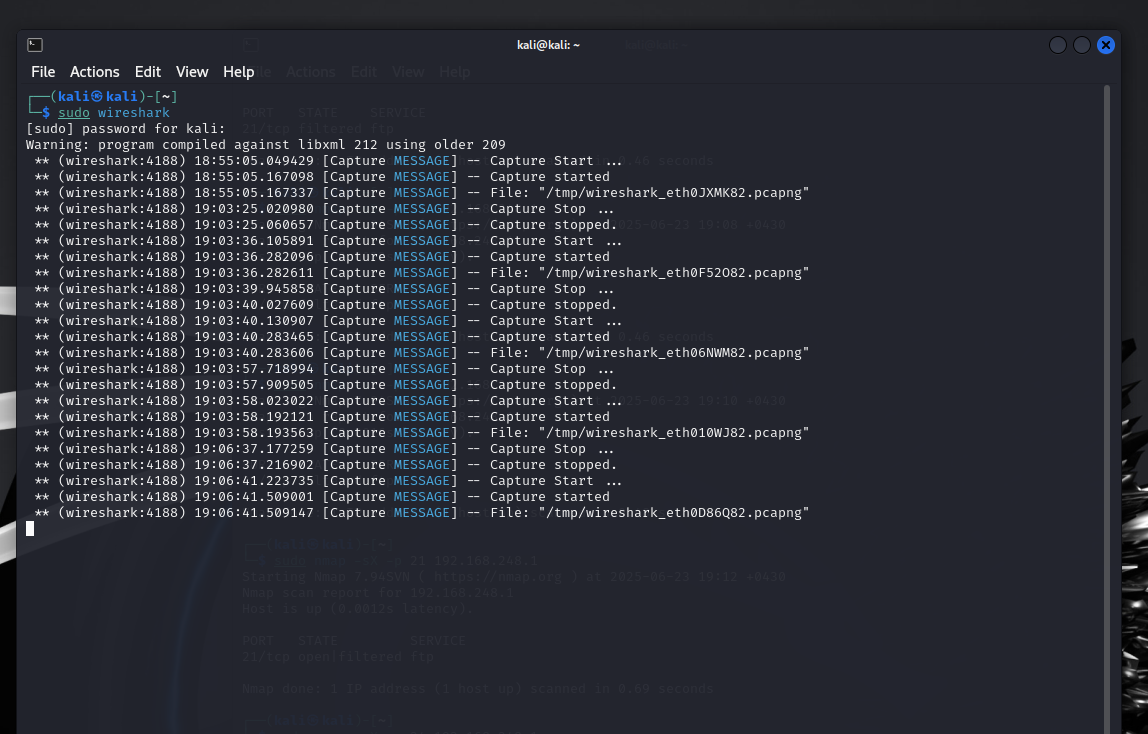
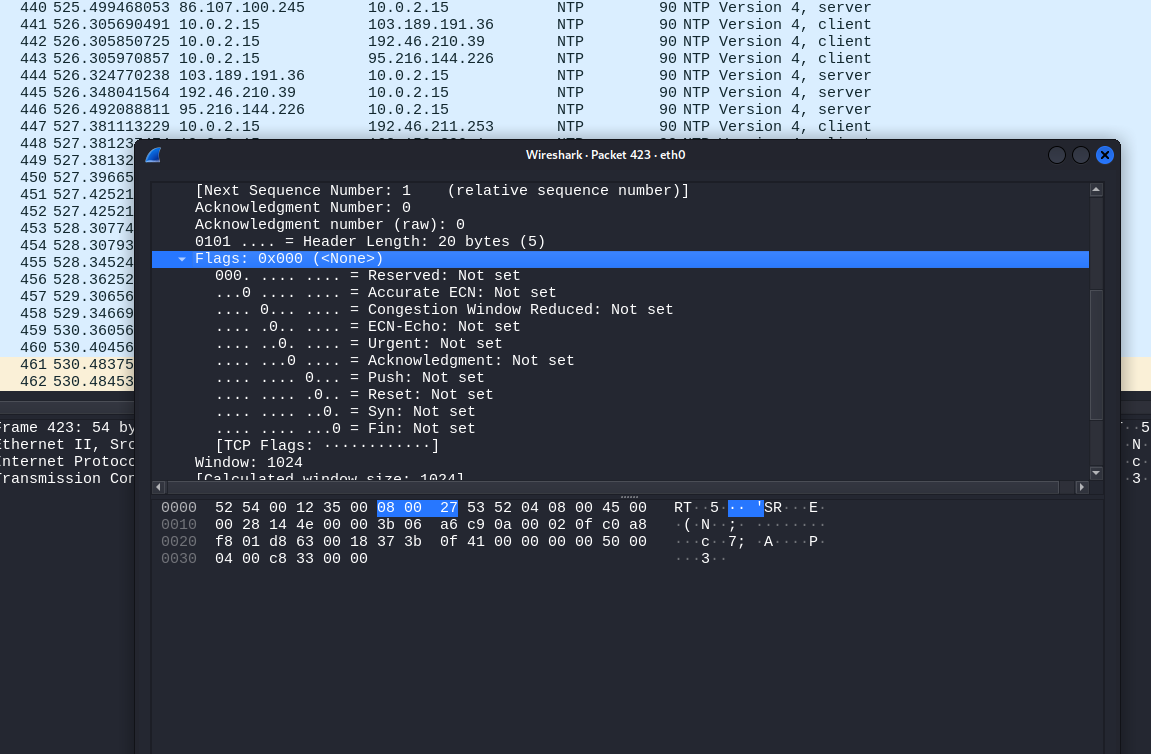
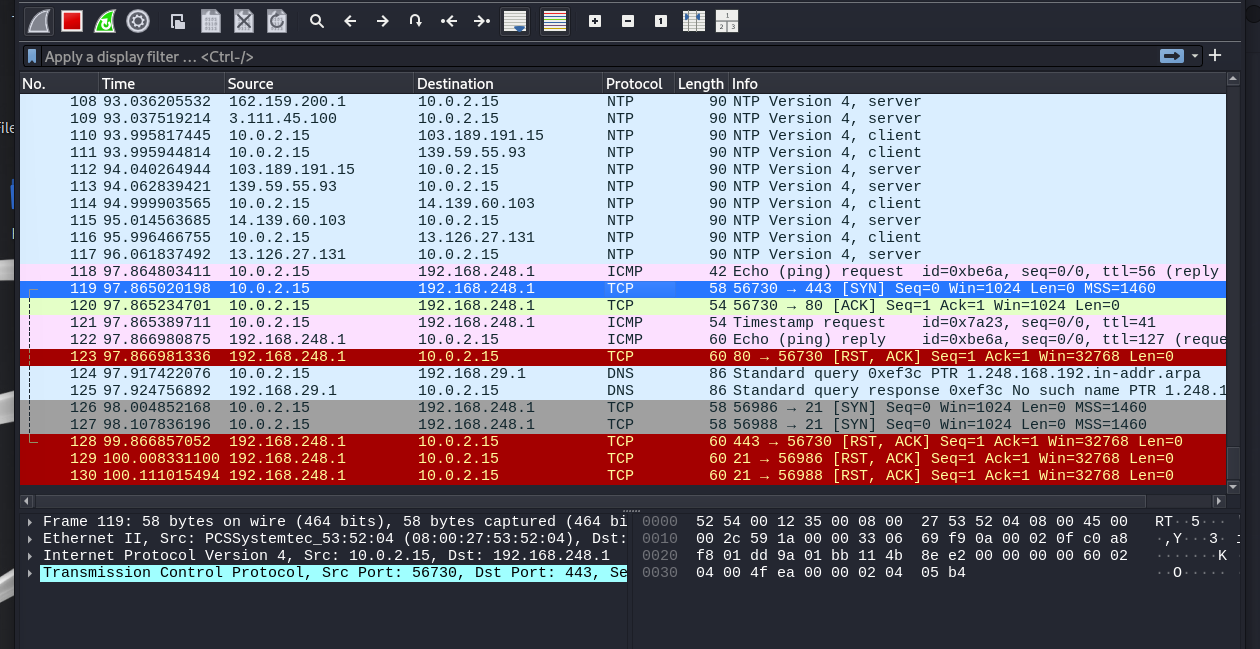
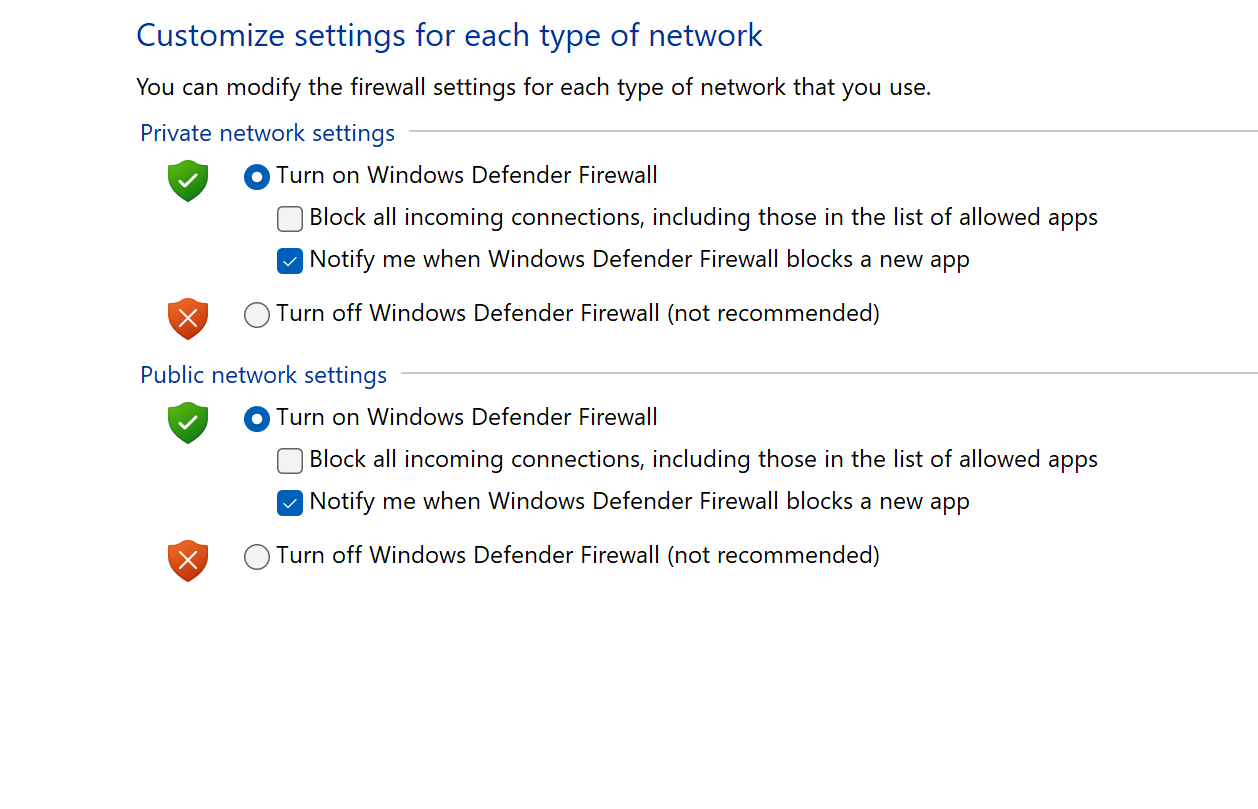
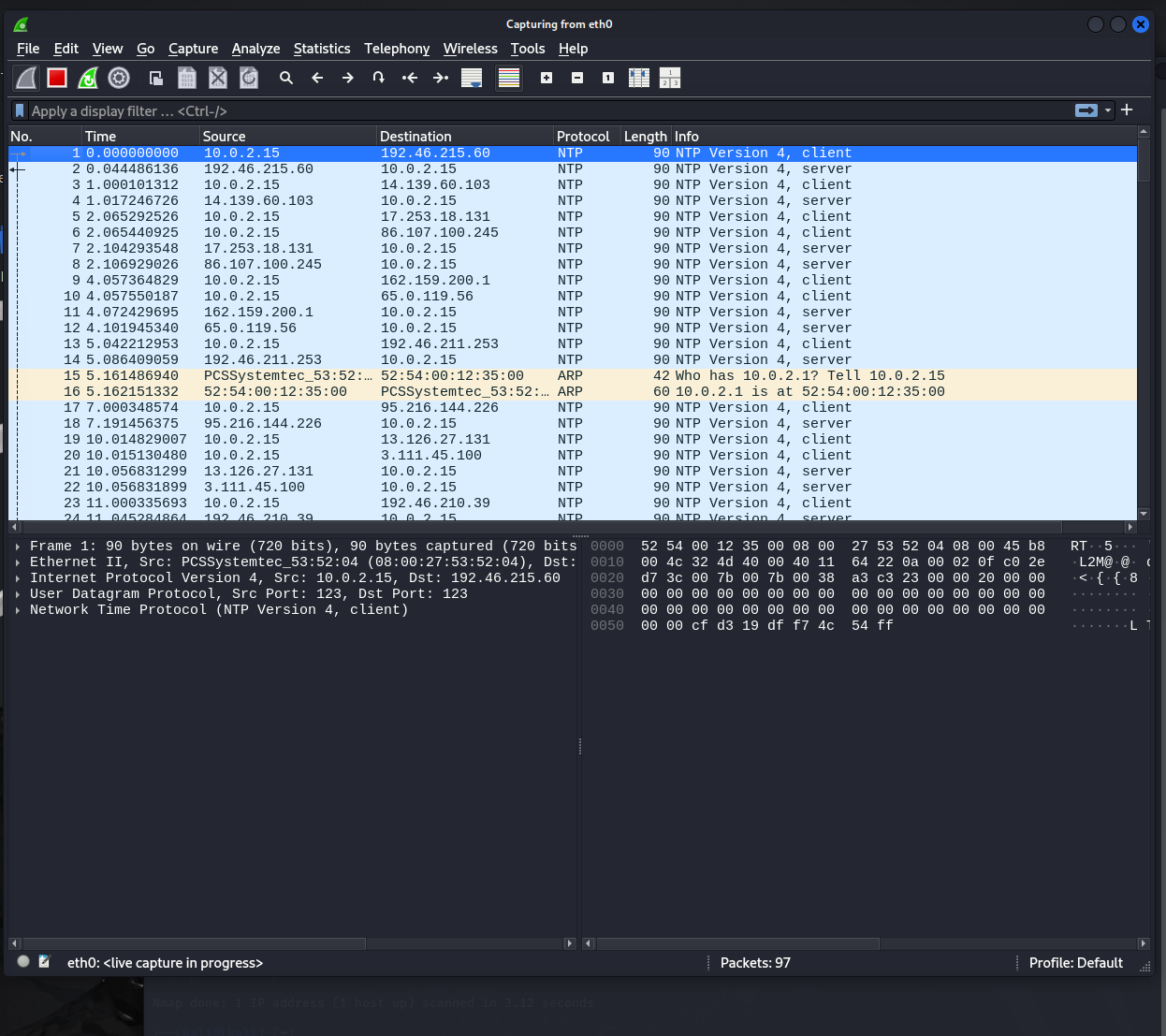
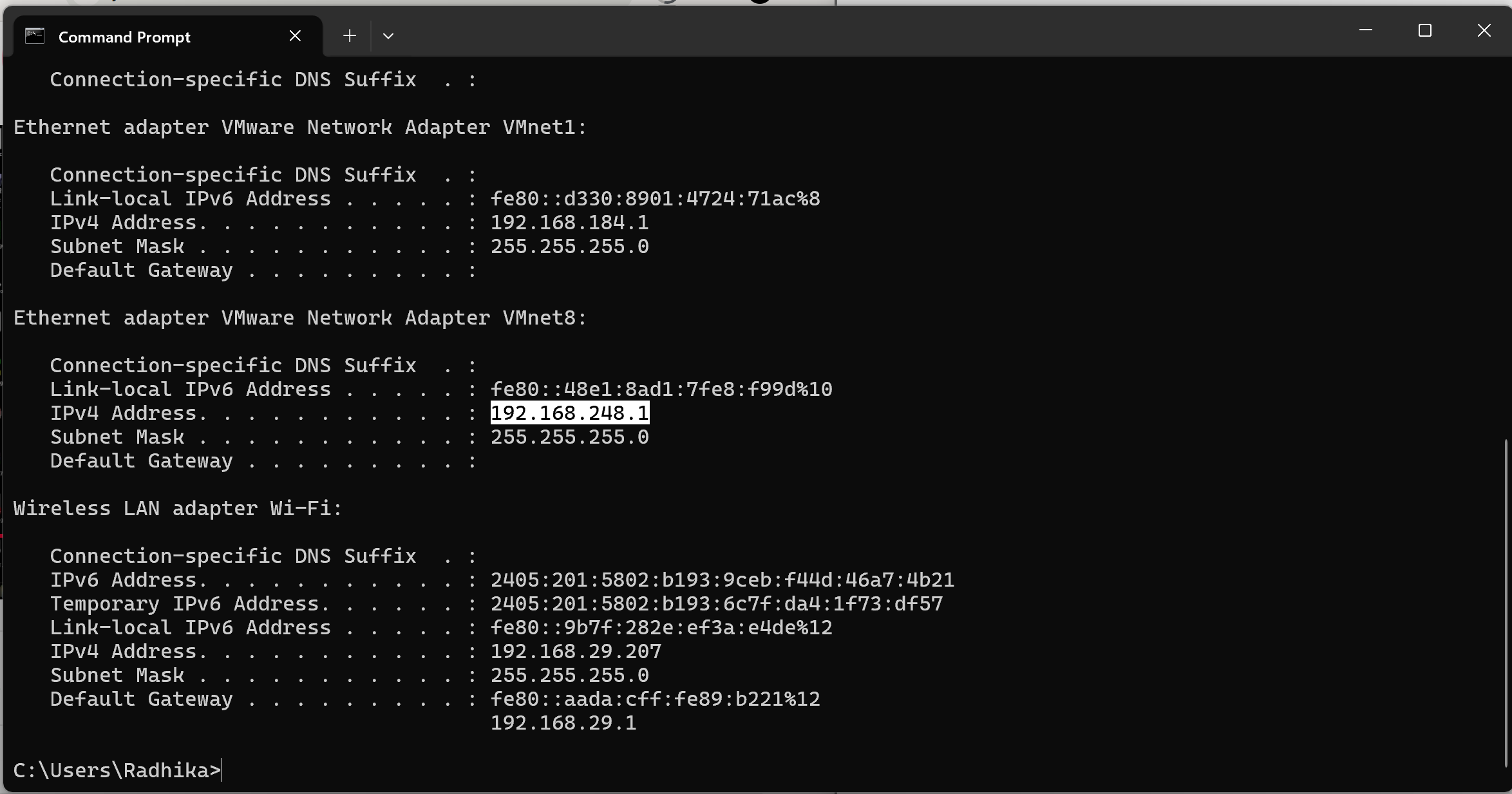
**Using --osscan-guess option with the -O parameter. It will attempt to detect the operating system. If it is not able to do so, then it will provide the closest signature possible. It performs an aggressive detection of the operating system.**

****

**Checking the version of the services on the open ports.**



**Wireshark**

****