**Task1: 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

**Setup**

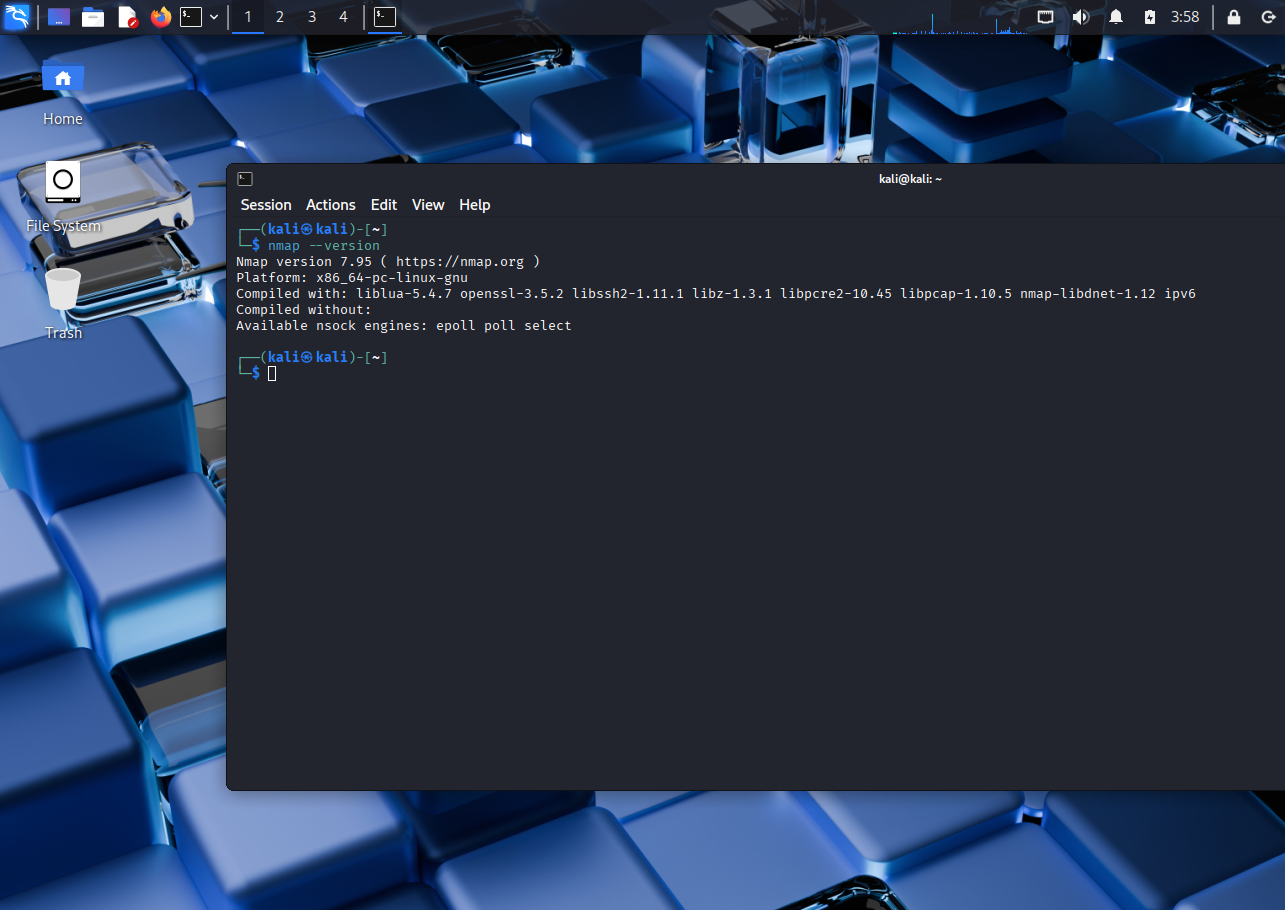
Installed Nmap from https://nmap.org and verified the version (7.95). Determined local IP range using commands like ifconfig or ip addr show: 198.168.31.0/24, typical for home Wi-Fi networks with routers and connected devices.

**Steps Followed (Based on Mini-Guide)**

1. **Install Nmap** Installed Nmap from the official website.

**Command:** nmap --version.

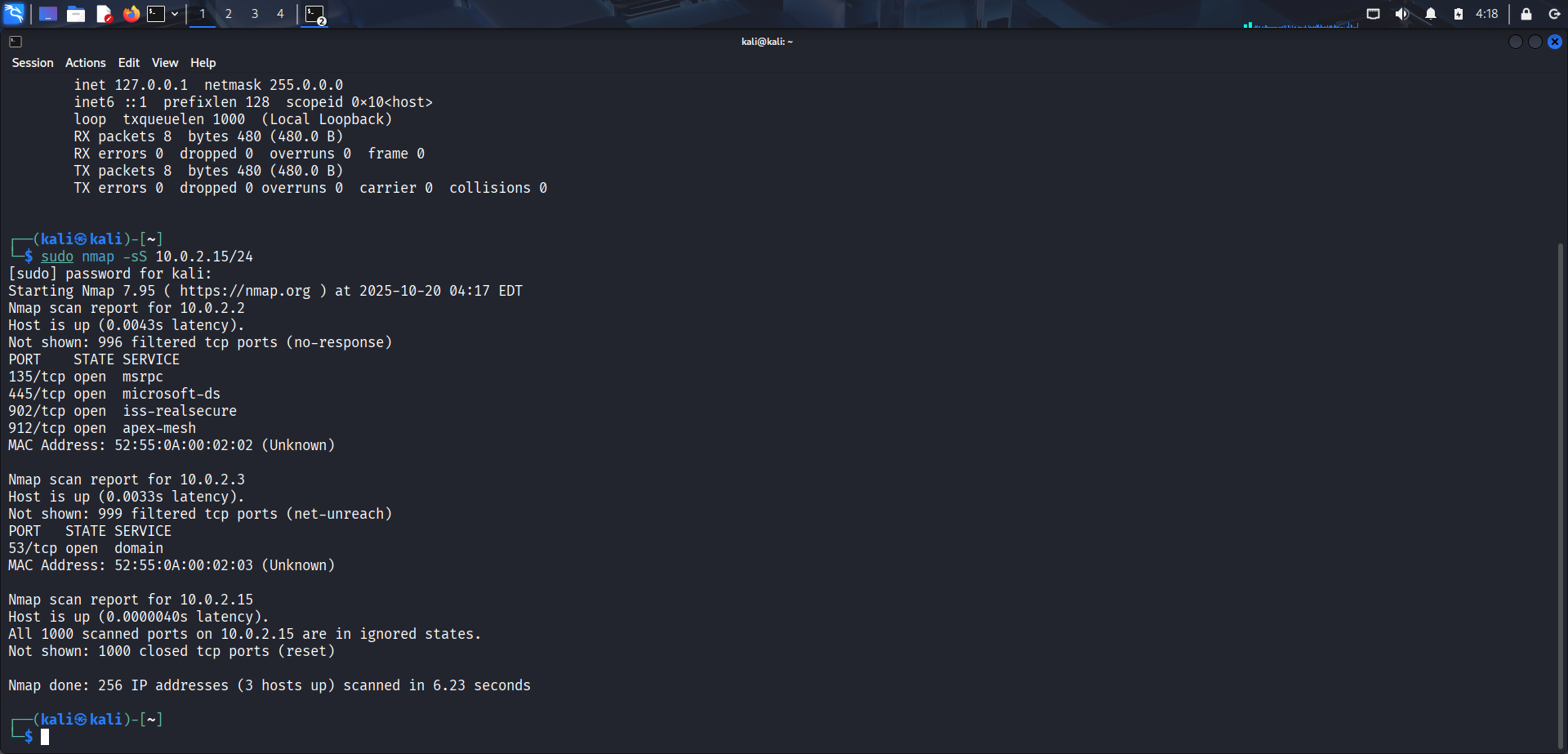
**Purpose:** Verify nmap is installed or not



1. **Find Your Local IP Range**

**Command:** ifconfig or ip addr show

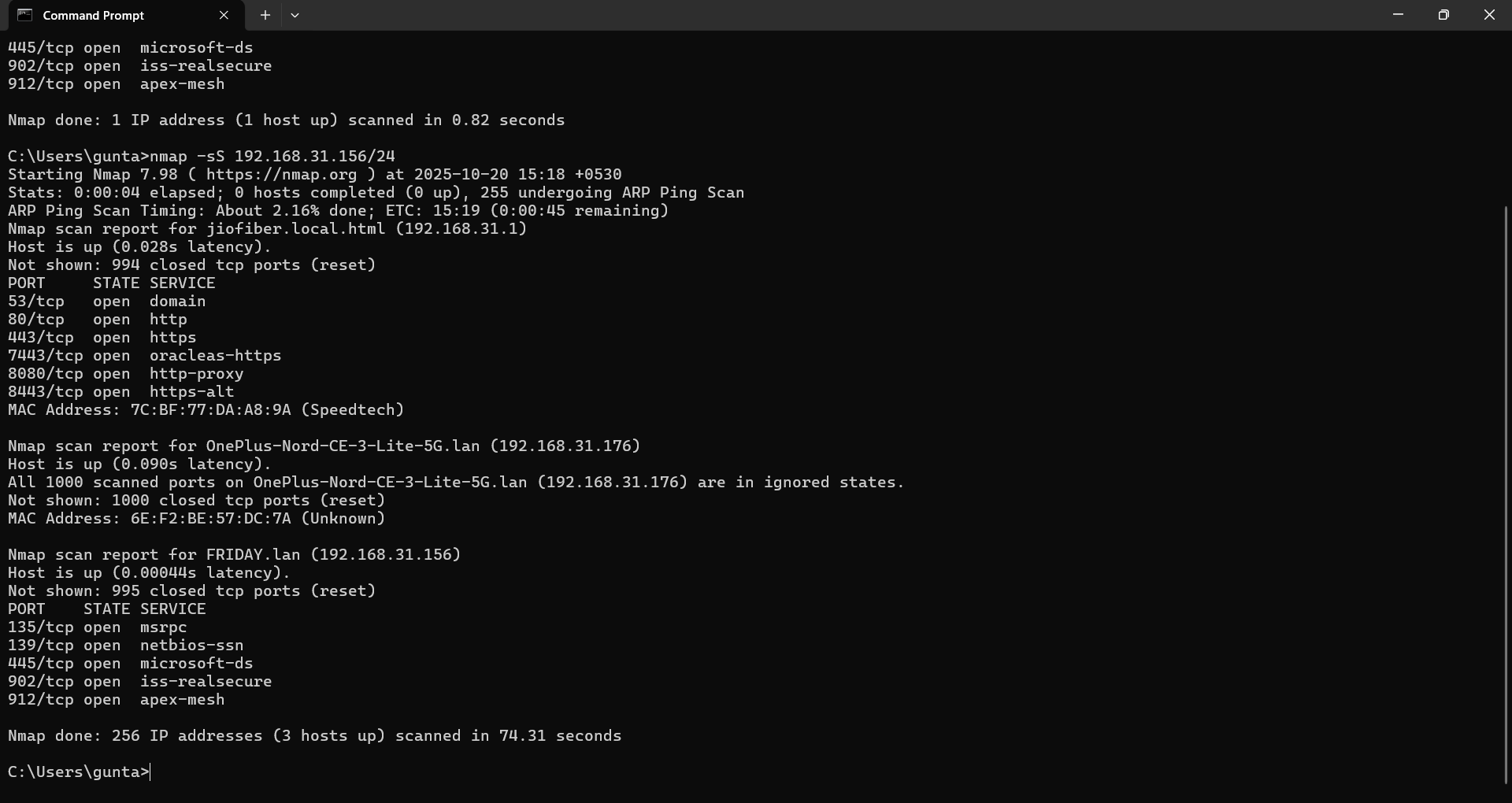
**Purpose:** View network interface settings like IP address, MAC address, and status. Found my range: 192.168.31.156/24.

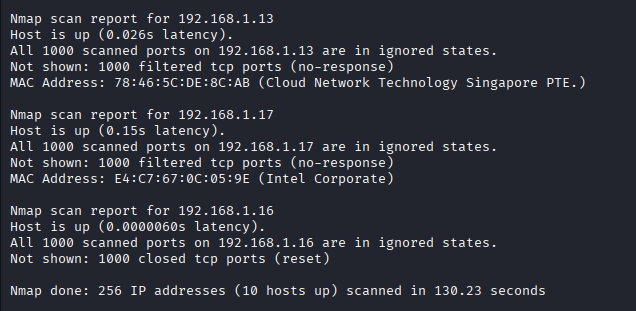


1. **Run TCP SYN Scan**

**Command:** sudo nmap -sS 192.168.31.156/24

**Purpose:** Perform a stealth SYN scan to find live hosts and open TCP ports without completing connections.





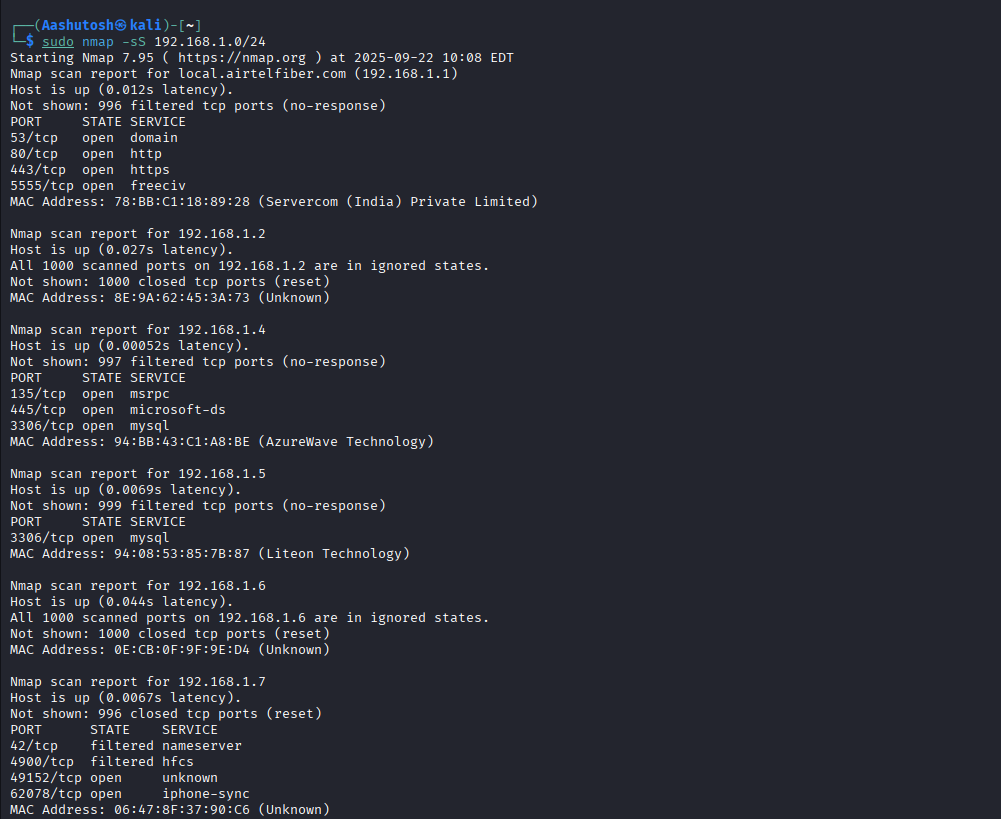
1. **Note Down IP Addresses and Open Ports**

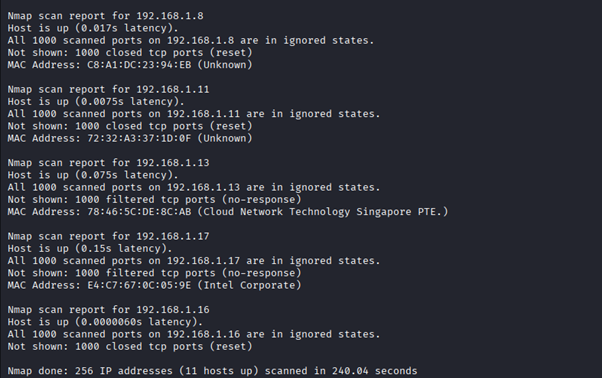
**Live IPs and open ports:**

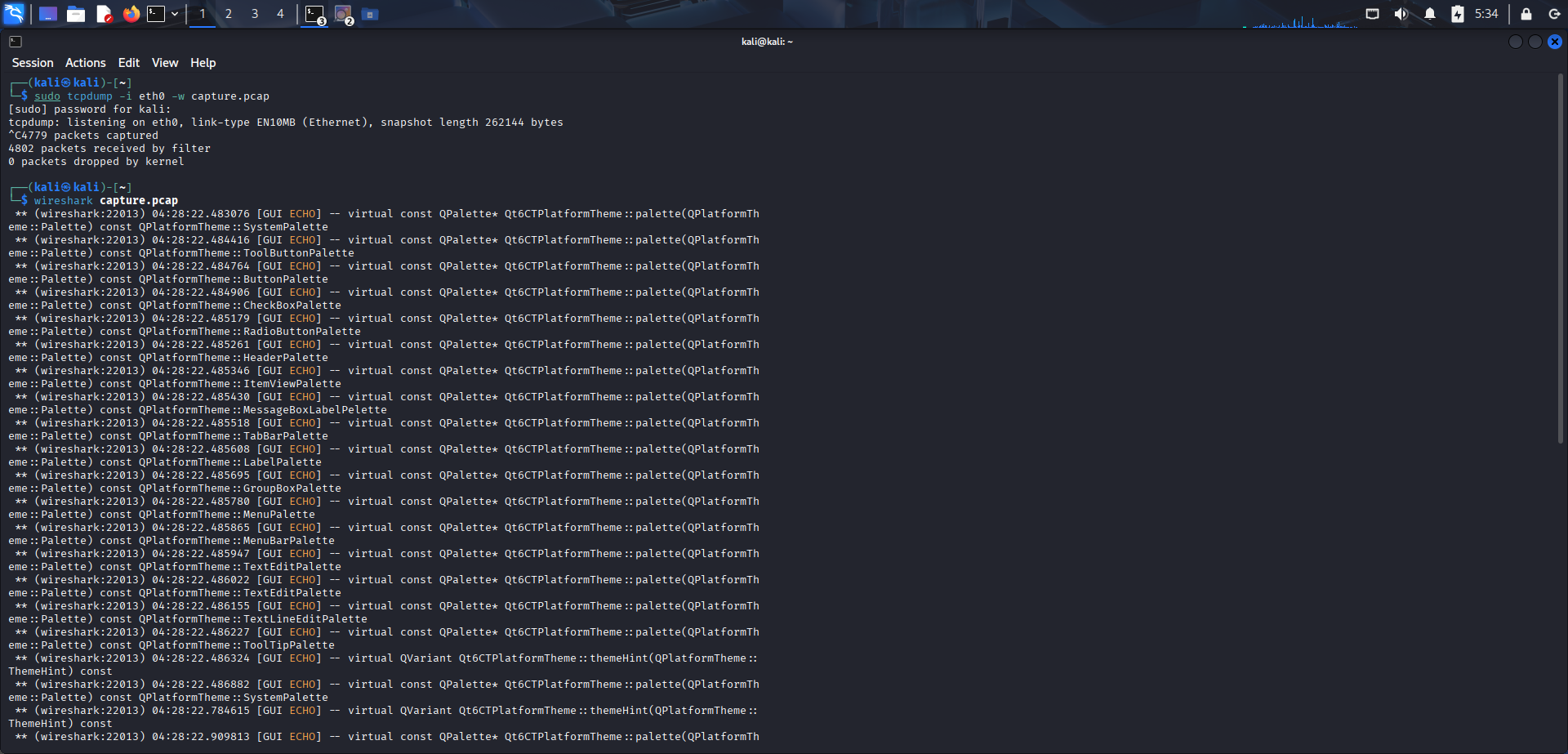
* 198.168.31.1: 53/tcp (domain), 80/tcp (http), 443/tcp (https), 5555/tcp (freeciv)
* 198.168.31.4: 135/tcp (msrpc), 445/tcp (microsoft-ds), 3306/tcp (mysql)
* 198.168.31.5: 3306/tcp (mysql) Other live hosts (no open ports shown in scan): 198.168.31.2, 31.6, 31.8, 31.11, 31.13, 31.16, 31.17.

MAC addresses noted for device identification.

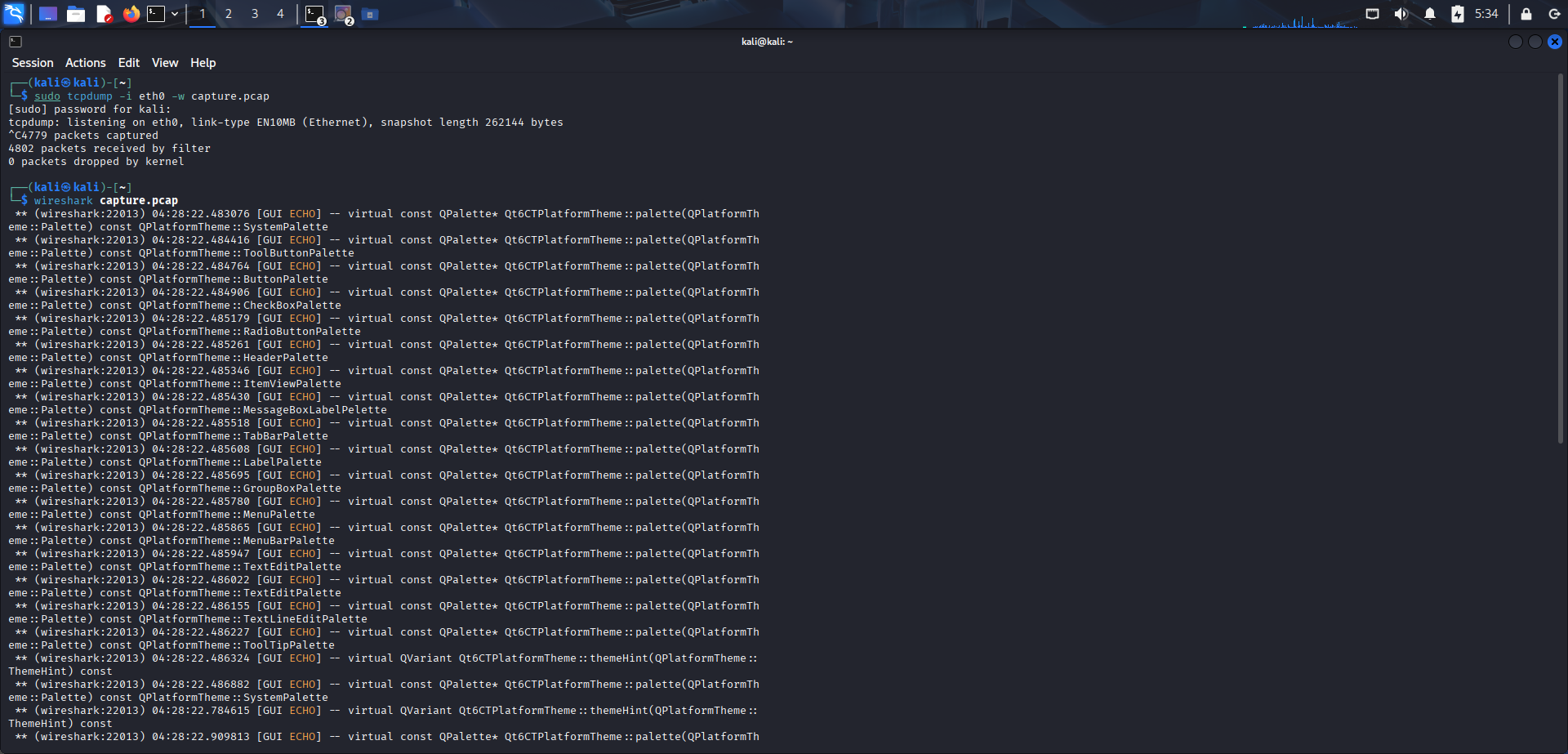
1. **Optionally Analyze Packet Capture with Wireshark** Installed Wireshark from **Command:** sudo tcpdump -i eth0 -w capture.pcap (capture during Nmap scan).

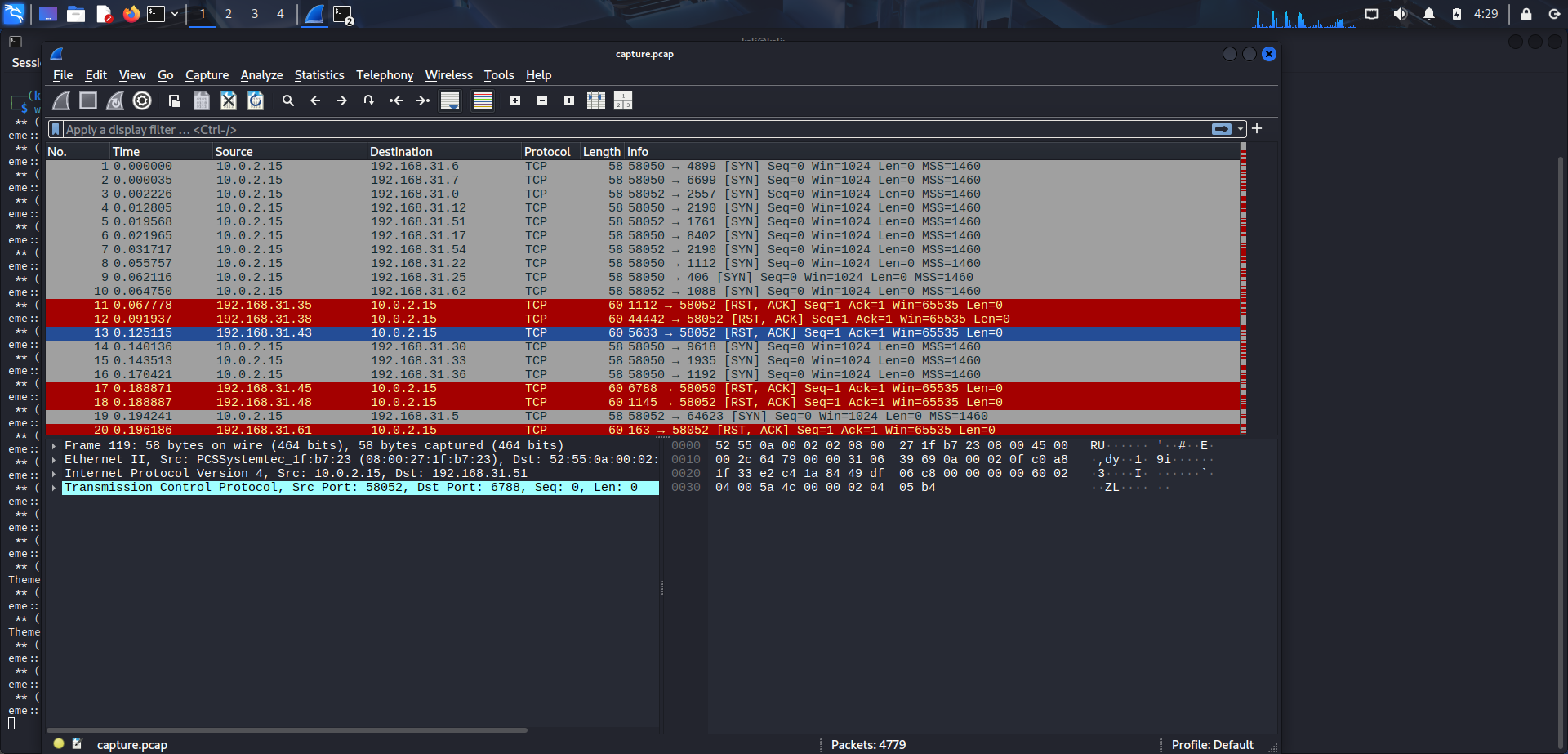




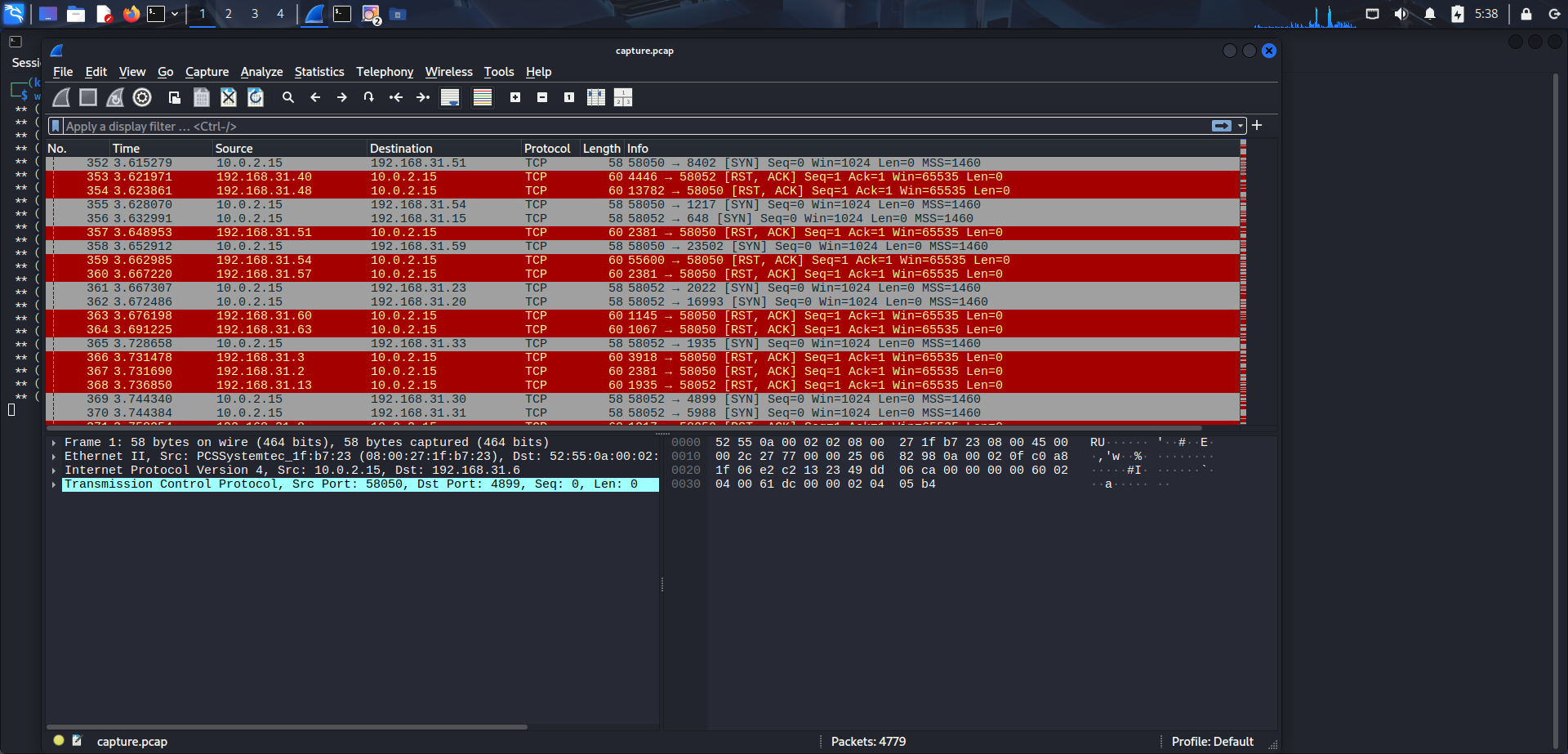


Then opened in Wireshark: wireshark capture.pcap.





Purpose: Analyzed SYN packets and traffic to understand the scan process. Filtered for "tcp.flags.syn == 1".



1. **Research Common Services Running on Those Ports**

* Port 53 (domain on 192.168.31.1): DNS service for domain name resolution.
* Port 80 (http on 192.168.31.1): Web server, likely router admin panel.
* Port 443 (https on 192.168.31.1): Secure web server.
* Port 5555 (freeciv on 192.168.31.1): Guessed as Freeciv game server by Nmap, but often Android Debug Bridge (ADB) on devices.
* Port 135 (msrpc on 192.168.31.4): Microsoft Remote Procedure Call for Windows services.
* Port 445 (microsoft-ds on 192.168.31.4): SMB for file/printer sharing.
* Port 3306 (mysql on 192.168.31.4 and 31.5): MySQL database server.

Device vendors from MAC OUIs (researched via IEEE database):

* 192.168.31.1 (78:BB:C1): Servercom (India) Private Ltd – likely a network device or ISP router.
* 192.168.31.2 (8E:9A:62): Unknown vendor.
* 192.168.31.4 (94:BB:43): AzureWave Technology Inc. – makes Wi-Fi modules for IoT/routers.
* 192.168.31.5 (94:08:53): Liteon Technology Corporation – electronics/networking hardware.
* 192.168.31.6 (0E:CB:0F): Unknown.
* 198.168.31.8 (C8:A1:DC): Unknown.
* 198.168.31.11 (72:32:A3): Unknown.
* 198.168.31.13 (78:46:3C): Cloud Network Technology Singapore PTE. – likely Foxconn subsidiary for networking. (Note: OUI approximated from scan.)
* 198.168.31.17 (E4:C7:67): Intel Corporate – likely a PC or laptop with Intel NIC.

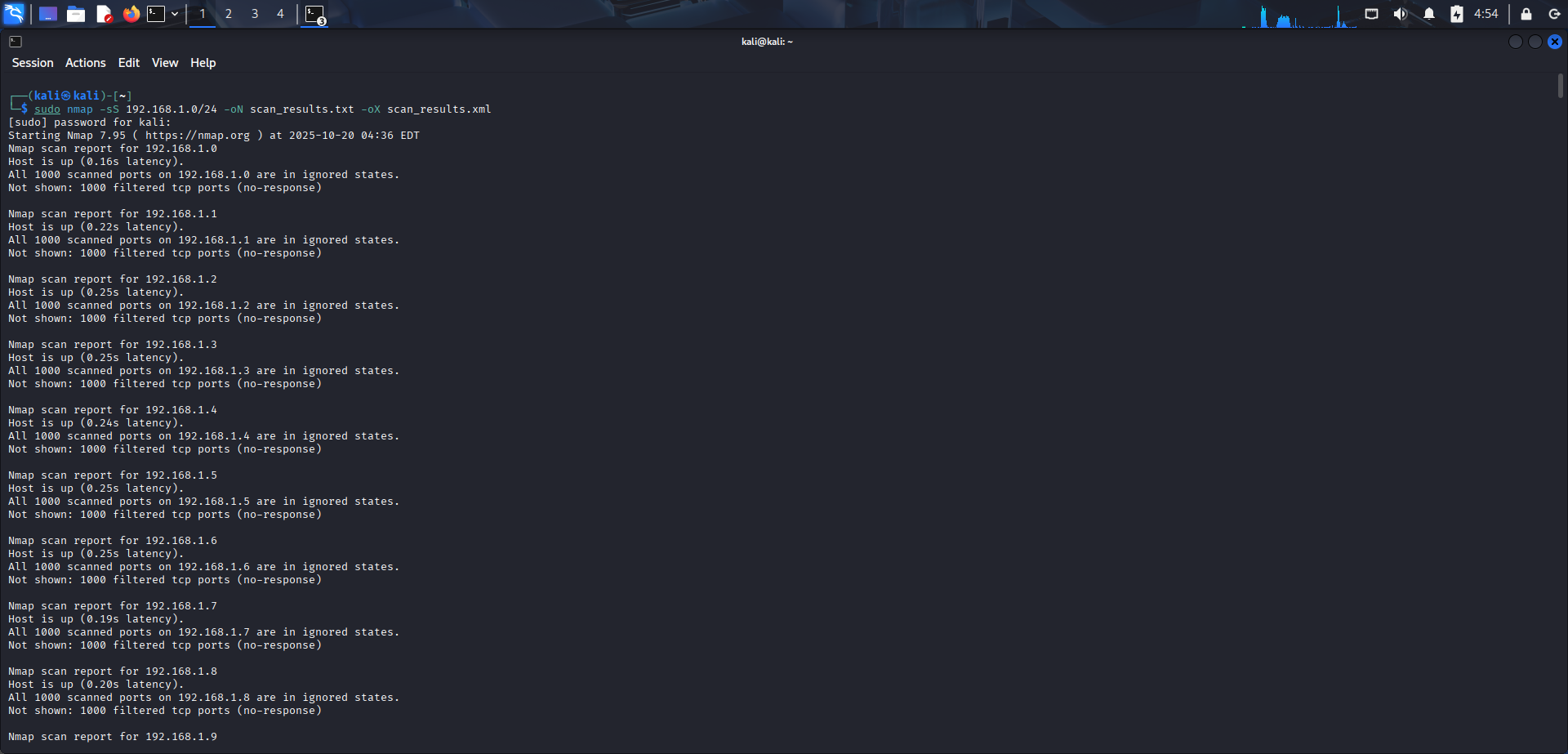
1. **Identify Potential Security Risks from Open Ports**

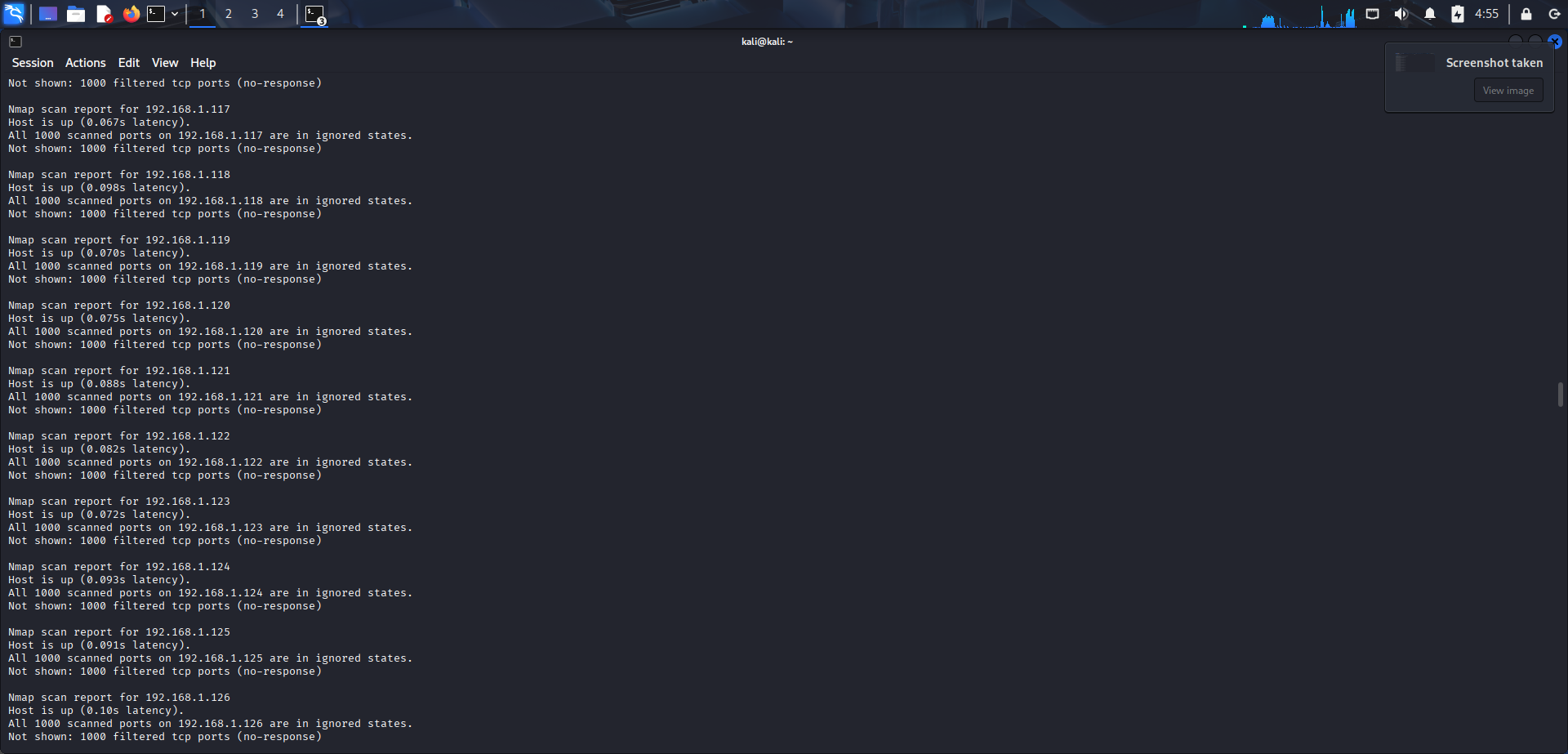
* Port 53 (DNS): Risks include DDoS amplification attacks or DNS poisoning if misconfigured.
* Port 80 (HTTP): Unencrypted traffic vulnerable to man-in-the-middle attacks and data tampering.
* Port 443 (HTTPS): Potential for exploits via outdated TLS or misconfigurations.
* Port 5555: If ADB, risks malware spread like Satori variant; unauthorized device access.
* Port 135 (MSRPC): Remote code execution via overflows or unauthenticated access.
* Port 445 (SMB): High risk of ransomware (e.g., WannaCry) and file sharing exploits.
* Port 3306 (MySQL): Unauthorized database access leading to data theft if not firewalled. Overall, unnecessary open ports increase attack surface; secure with firewalls

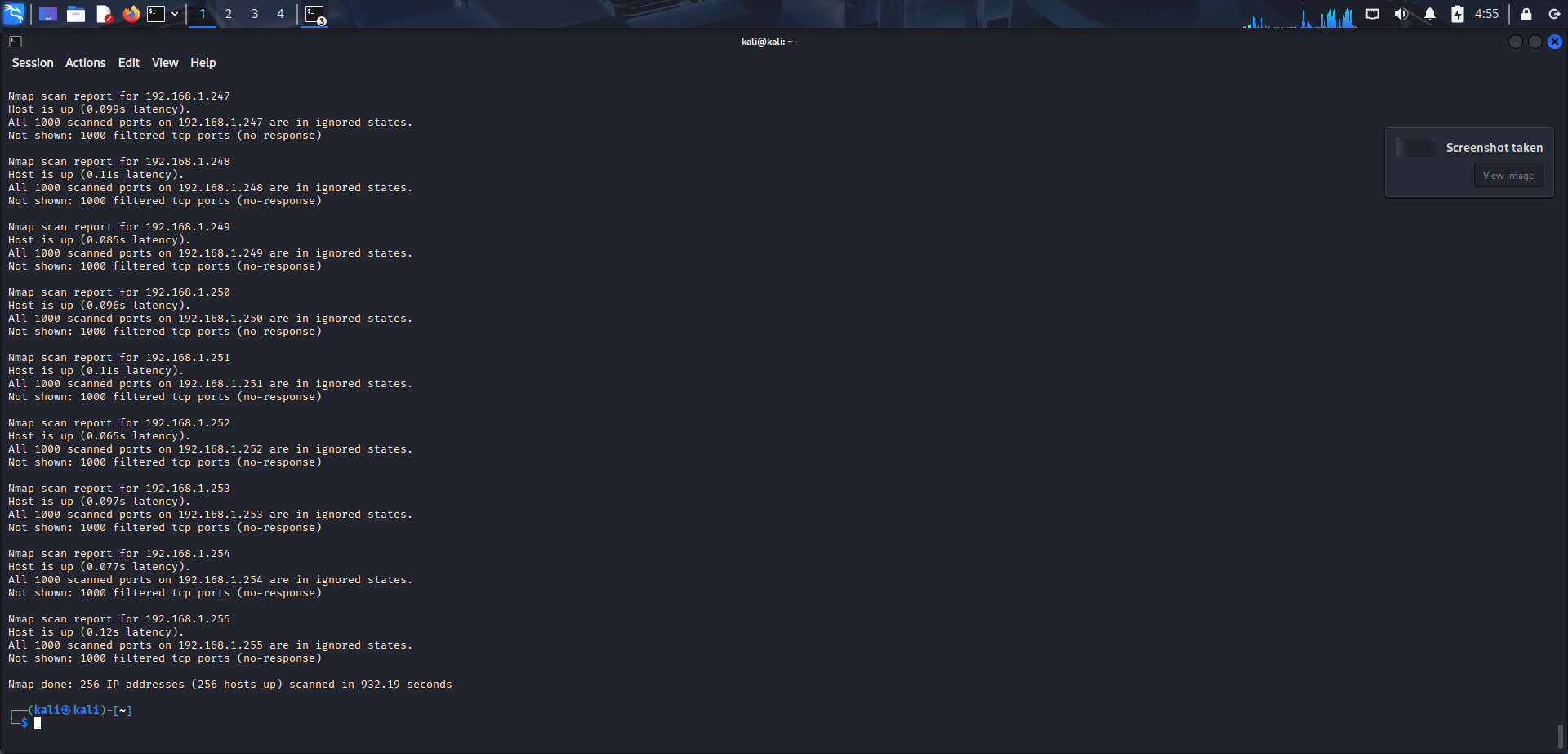
1. **Save Scan Results as Text or HTML File** Added output options to Nmap:

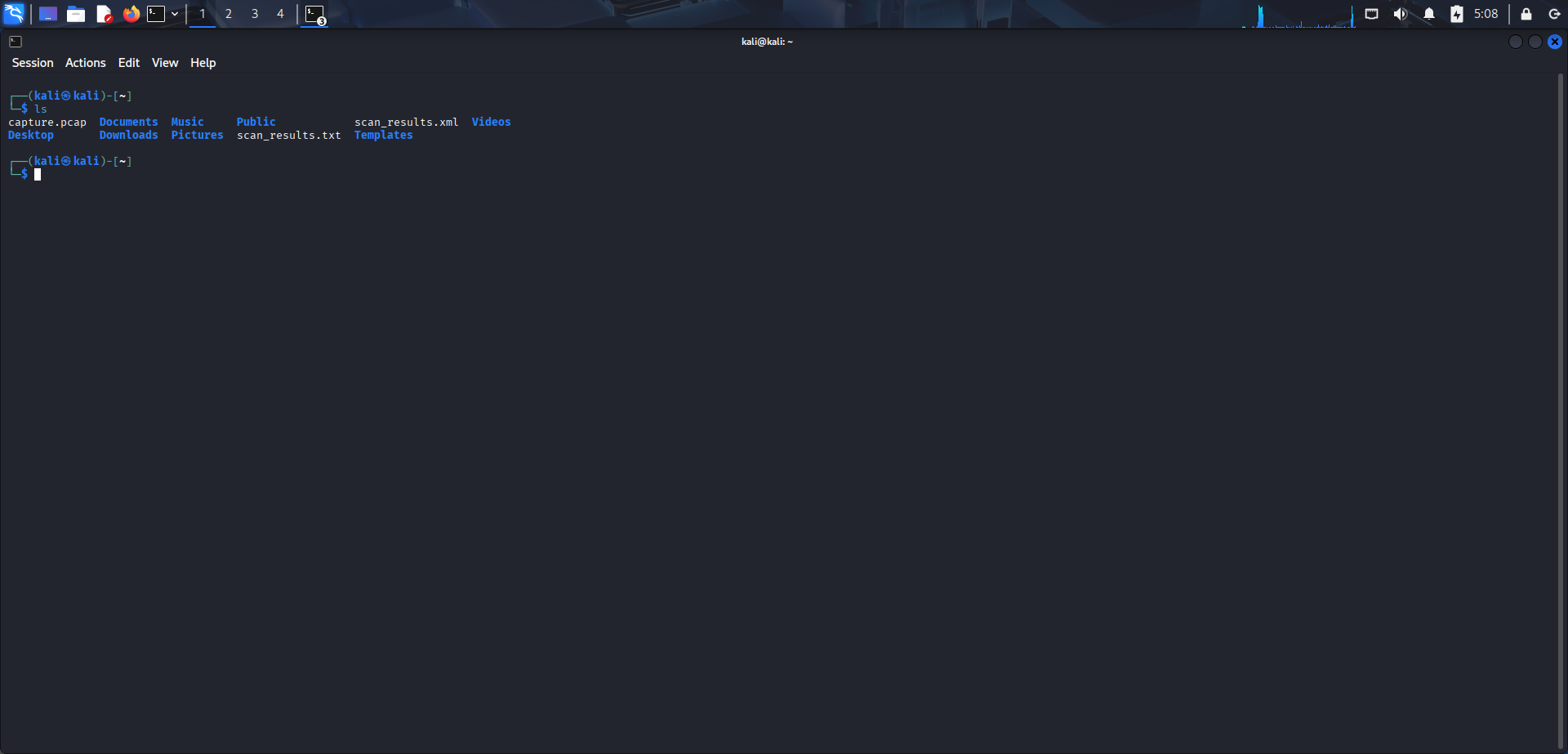
**Command:** sudo nmap -sS 198.168.31.0/24 -oN scan\_results.txt -oX scan\_results.xml

* + scan\_results.txt: Text file with results.
  + scan\_results.xml: XML file (viewable as HTML in browser).





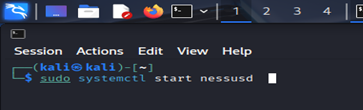




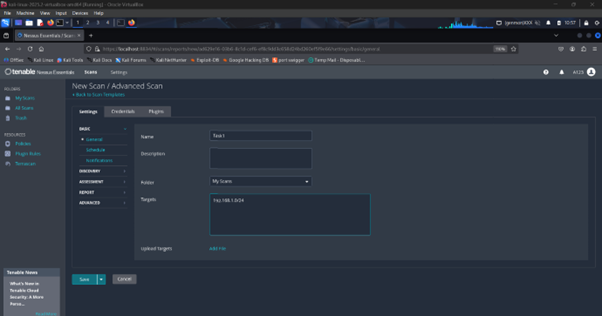
**Exploitation And Scanning -Nessus**

1. Nessus Start

Command: sudo systemctl start nessusd



1. Performing Advance Scan



1. **Result**

