Title- scanning local network for open ports

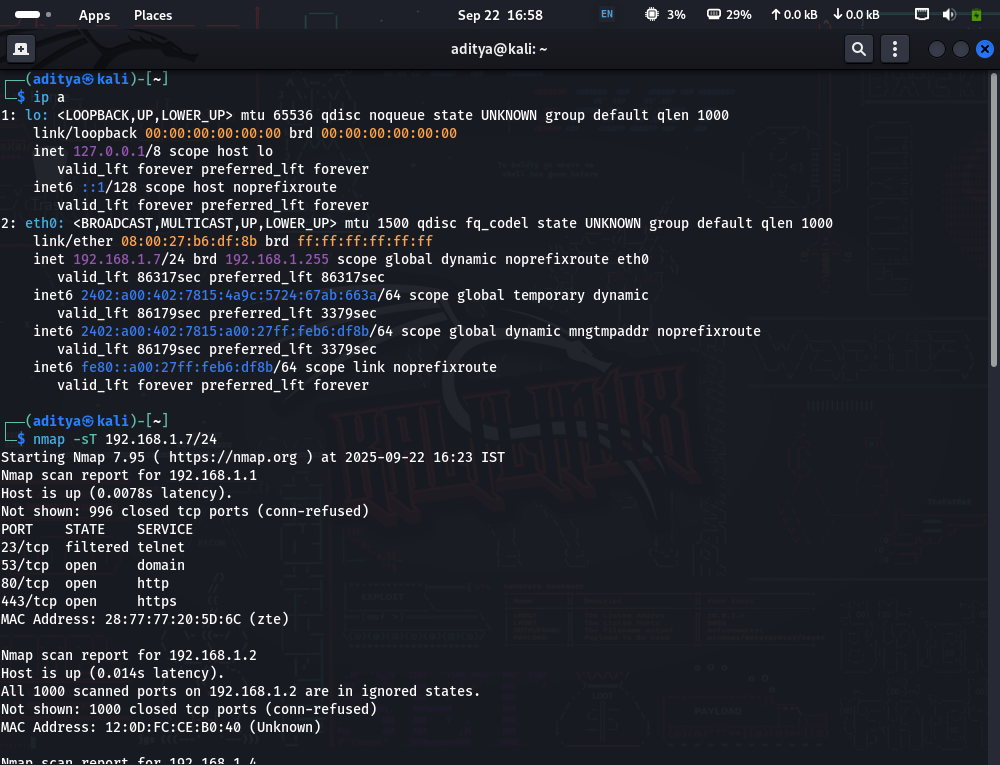
**1. Objective**  
Discover local IP range; perform TCP scan; note IP addresses and open ports; identify common services and security risks.

**2. Environment**

* Machine: Kali Linux VM
* Tools used: Nmap (version: nmap --version), (optional) Wireshark
* Local network range discovered: 192.168.1.1/24

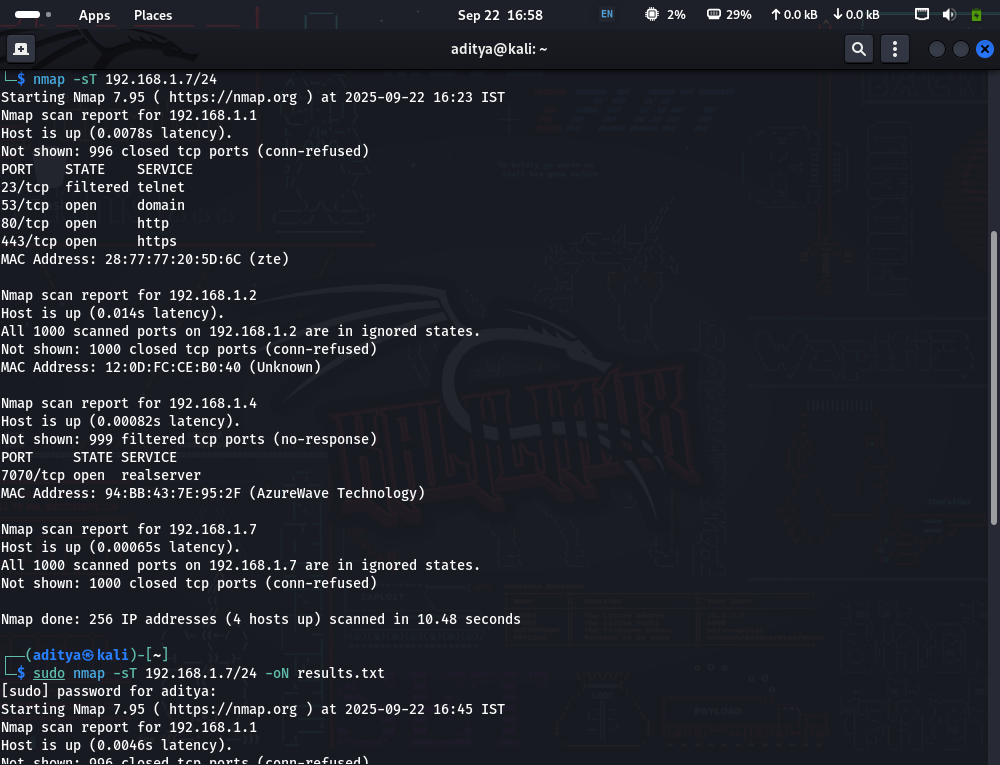
**3. tools used- Nmap(CLI)**

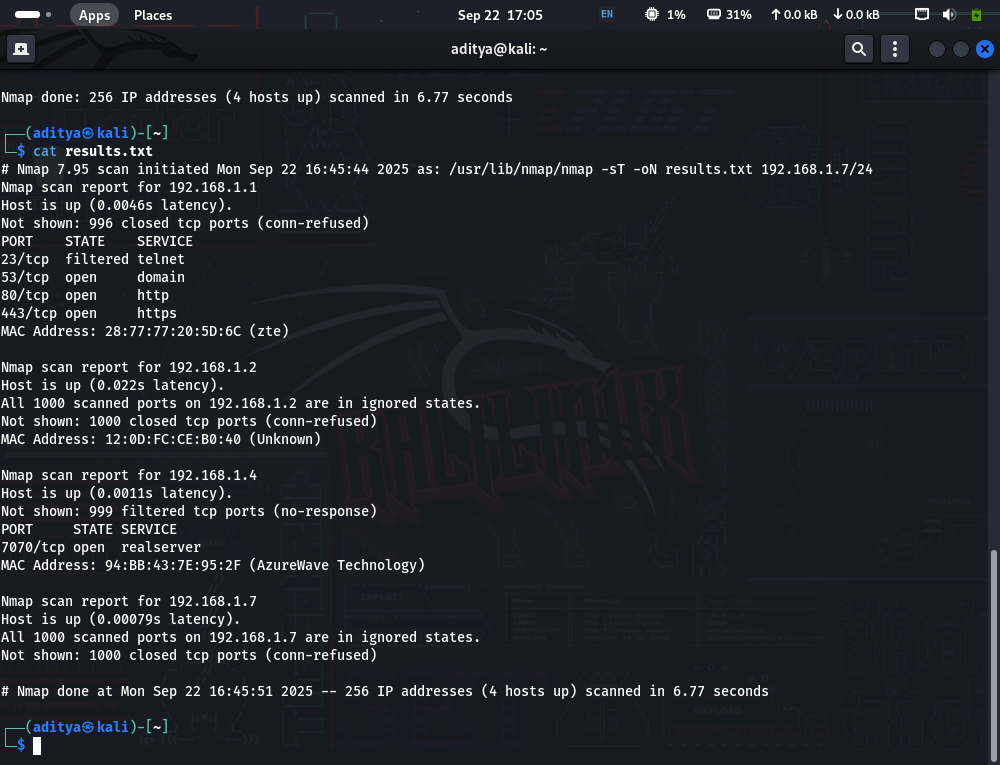
**4. Commands executed**

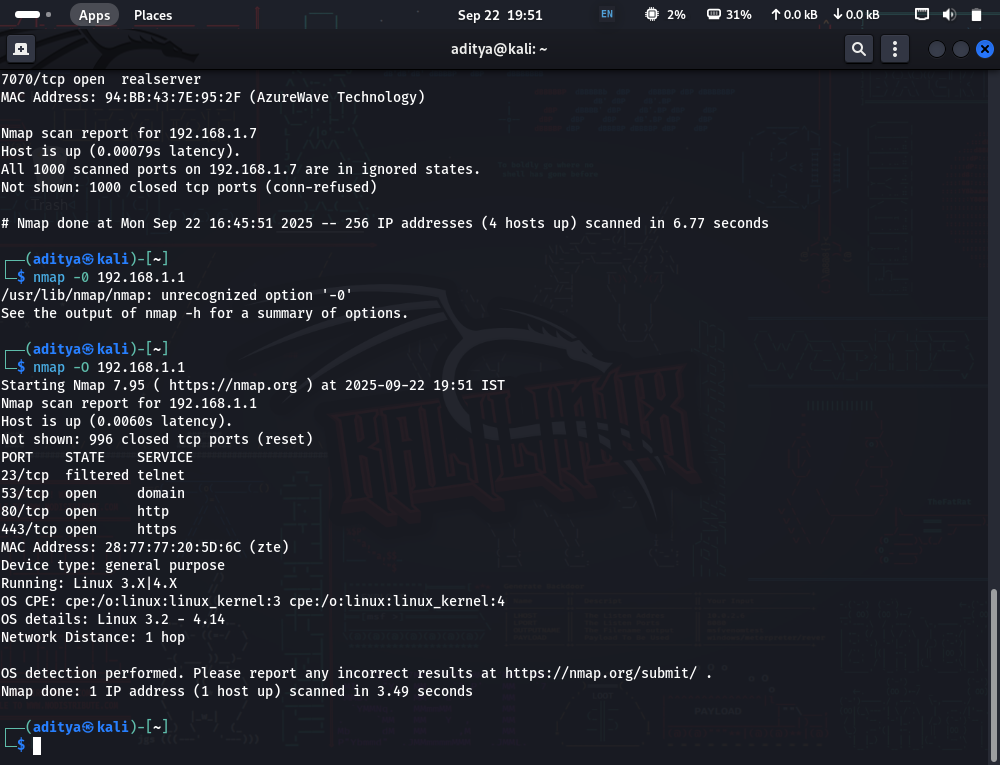


The command ip a is used to find the local IP address, in this case when the command was run, it showed the ip 192.168.1.7/24

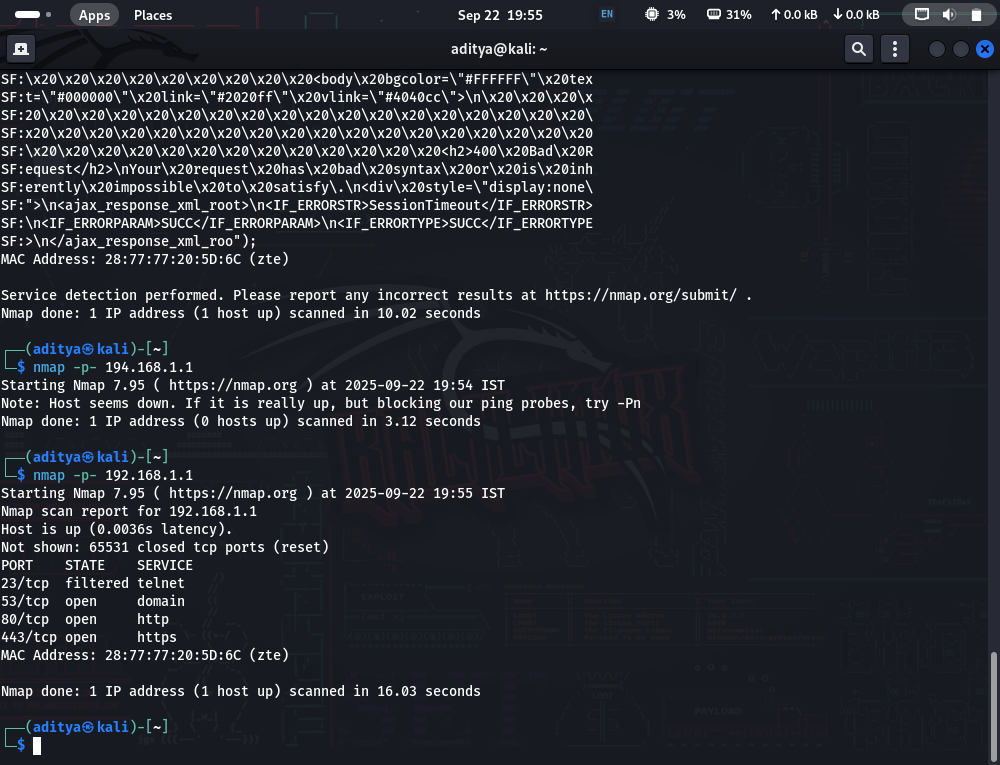
To perform a TCP scan we used nmap -ST that showed the open tcp ports







Nmap -O enables os detection in the open ports



The command nmap -p- scans all 1000 common ports

**🔹 Ports & Services Found**

* **23/tcp — Telnet**
  + *What it is:* Insecure remote login service (old, plaintext).
  + *Risk:* **High** — sends credentials in clear text, easy target for brute force. Should be disabled or replaced with SSH.
* **53/tcp — DNS**
  + *What it is:* Domain Name System service.
  + *Risk:* **Medium** — normally safe if it’s a DNS server, but can be abused for zone transfers or amplification attacks if misconfigured. Should not be exposed unless it’s a real DNS server.
* **88/tcp — Kerberos**
  + *What it is:* Authentication service used in Active Directory / Kerberos environments.
  + *Risk:* **High (if exposed to whole LAN/Internet)** — attackers may attempt ticket-granting abuse, brute force, or replay attacks. Should only be accessible to trusted clients in a domain.
* **443/tcp — HTTPS**
  + *What it is:* Secure web service (encrypted HTTP).
  + *Risk:* **Low–Medium** — depends on the web application and SSL/TLS configuration. Risk increases if the service is outdated or misconfigured.

**Conclusion**

**In this task, a TCP scan was performed across the local network to identify active devices, open ports, and the services running on them. The scan revealed open ports 23 (Telnet), 53 (DNS), 88 (Kerberos), and 443 (HTTPS) on the target devices. Analysis of these services indicates that Telnet and Kerberos are high-risk due to insecure plaintext authentication and sensitive authentication handling, respectively. DNS, while essential, could pose risks if misconfigured, and HTTPS depends on proper TLS configuration to ensure secure communication.**

**This exercise demonstrated how Nmap can be effectively used to discover devices and map network exposure. It highlighted the importance of monitoring open ports and services as part of basic network security practices. Overall, the task provided hands-on experience in network reconnaissance, port scanning, service identification, and initial security risk assessment, reinforcing the understanding of potential vulnerabilities in a local network environment.**