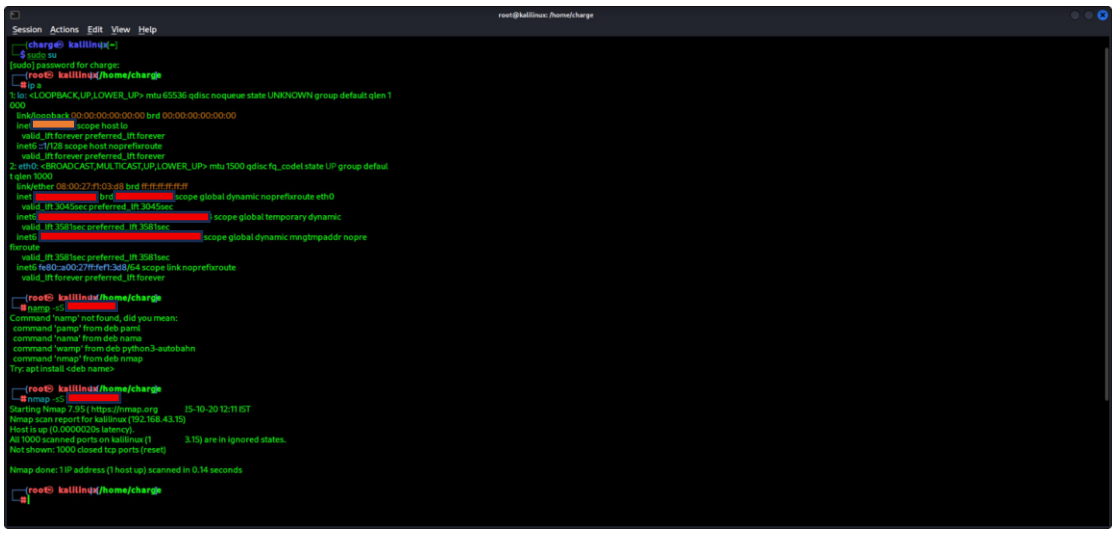
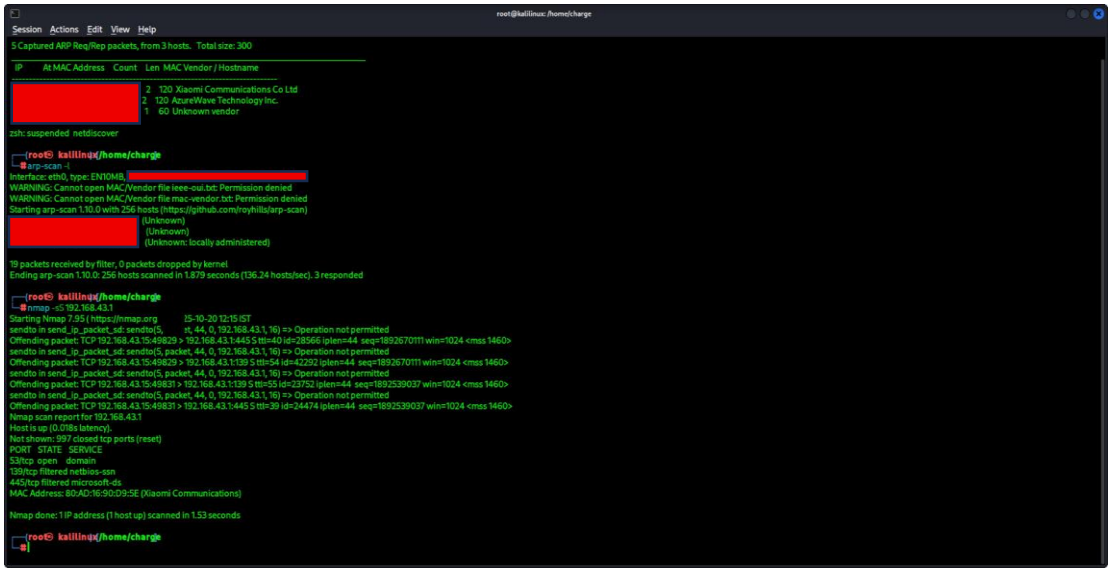
Task 1: Scan Your Local Network for Open Ports

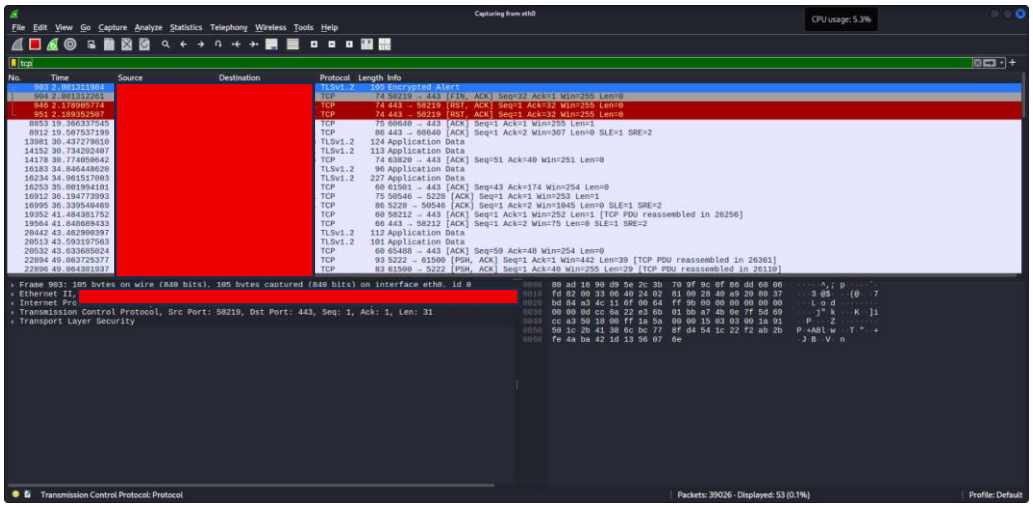
➢ **Find your local IP range (e.g., 192.168.1.0/24):**



➢ **Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan and note down IP addresses and open ports found:**



➢ Optionally analyze packet capture with Wireshark:



➢ Research common services running on those ports:

- **Zone transfer:** TCP is required for full zone transfers between authoritative servers or from a master to a slave.
- **Authoritative DNS server**: answers queries for zones it is authoritative
- **Recursive Queries**: Resolve names reliably for clients

⇨ These are the some of services that runs on 53/tcp port.

➢ Identify potential security risks from open ports:

⇨ TCP/UDP 53 (DNS) - Zone transfer leak:

- attacker can retrieve full DNS zone, like all hostnames/IPs.
- Version/feature disclosure: reveals vulnerable software/version (helps exploit).
- Cache poisoning / DNS spoofing: redirect users to malicious sites.

⇨ TCP 139:

- Null sessions - unauthenticated info disclosure (users, shares).
- Authentication bypass or relay attacks.

⇨ TCP 445 (SMB over TCP):

- Remote code execution / worm propagation.
- Unauthorized file/share access.
- Ransomware/malware spread.