Lab 24 – Using ARP command for network reconnaissance

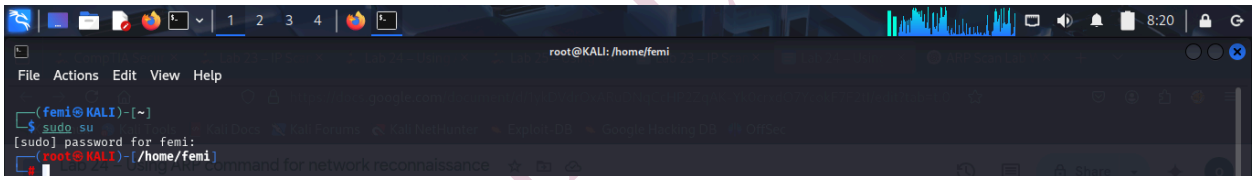
✅ Lab Objective:

You're learning to use the arp-scan tool to map IP addresses to MAC addresses on your local network. This is important for network reconnaissance—the process of discovering devices connected to a network.

🔧 Lab Preparation

1. Log in as Root

sudo su -

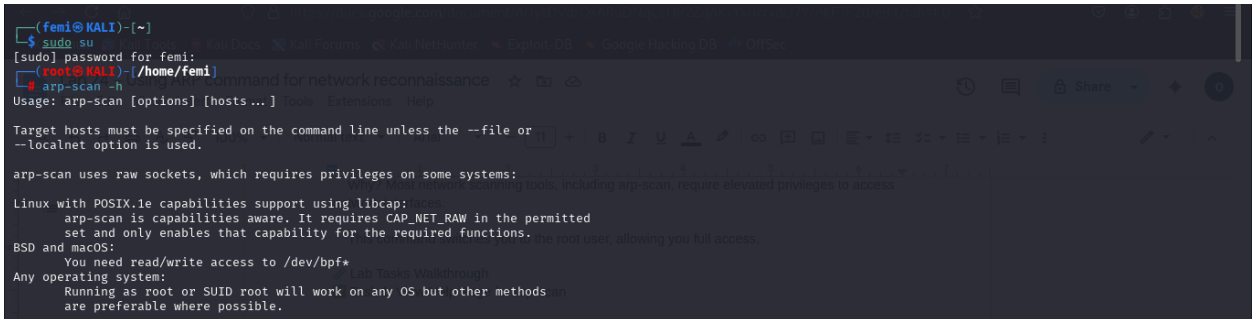


Why? Most network scanning tools, including arp-scan, require elevated privileges to access network interfaces.

This command switches you to the root user, allowing you full access.

🧪 Lab Tasks Walkthrough

✅ Task 1: View Help Page for arp-scan



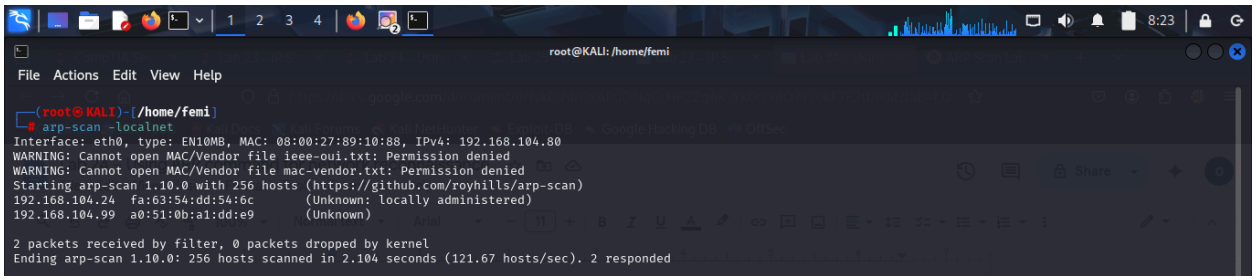
arp-scan -h

Why? This command shows the help menu. It provides available options, flags, and syntax for using arp-scan.

Example flags: -I for interface, --localnet for scanning local subnet, etc.

✅ Task 2: Scan the Local Network

arp-scan --localnet



What it does: Scans all IPs in your current subnet (e.g., 192.168.1.0/24) using ARP requests.

Why ARP? ARP works at Layer 2 (Data Link layer). It cannot be blocked by host firewalls, making it very effective for local discovery.

Output Explanation:

IP Address — The address of the detected device.

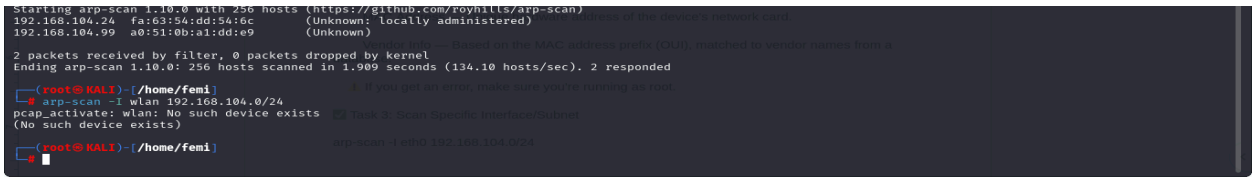
MAC Address — Unique hardware address of the device's network card.

Vendor Info — Based on the MAC address prefix (OUI), matched to vendor names from a database.

⚠️ If you get an error, make sure you're running as root.

✅ Task 3: Scan Specific Interface/Subnet

arp-scan -I eth0 192.168.104.0/24



-I eth0: Specifies which network interface to use (e.g., eth0, wlan0).

192.168.104.0/24: Explicitly states the subnet to scan.

Why? Useful if:

You're connected to multiple networks.

Your interface doesn't have an IP but is physically connected.

You want to scan a subnet different from the one you're in.

✅ Task 4: Scan a VLAN (Trunk Port)

(Command not explicitly shown, but implied logic follows the same pattern.)

arp-scan -I eth0.10 192.168.10.0/24

eth0.10: Denotes VLAN 10 on the eth0 interface (802.1q tagged).

Why? On trunk ports, you might want to scan specific VLANs. VLAN tagging allows you to do this using subinterfaces.

✅ Task 5: Identifying Unknown Devices & Updating Vendor DB
1. Sometimes, arp-scan might show:

Unknown

in the vendor column.

Why? The MAC address prefix isn’t in the tool's local vendor database.

What to do?

Use an online MAC lookup tool (e.g., https://macvendors.com).

Update the database with:

cd /usr/share/arp-scan
get-iab -v -u http://standards.ieee.org/develop/regauth/iab/iab.txt

get-oui -v -u http://standards.ieee.org/develop/regauth/oui/oui.txt

Why update? MAC address vendor databases evolve over time. Keeping them up to date increases accuracy.

2. Manually Add Known Spoofed MACs

echo "060027 SPOOFED-NIC TECHNOLOGIES LLC" >> /usr/share/arp-scan/mac-vendor.txt

Why? If you have custom or spoofed devices, you can add entries manually to keep track of them.

✅ Task 6: Save Scan Results for Later Analysis

arp-scan --localnet -W results.pcap

What it does: Saves scan results to a .pcap file for later analysis.

-W flag = Write to file in pcap format (used by tools like Wireshark or tcpdump).

tcpdump -nr results.pcap

What it does: Reads the .pcap file using tcpdump.

-n: Don't resolve names.

-r: Read from file instead of capturing live traffic.

Why? Great for:

Auditing

Offline analysis

Keeping records

🎯 What You Can Learn from ARP Scan Results

All active IPv4 devices on a local network.

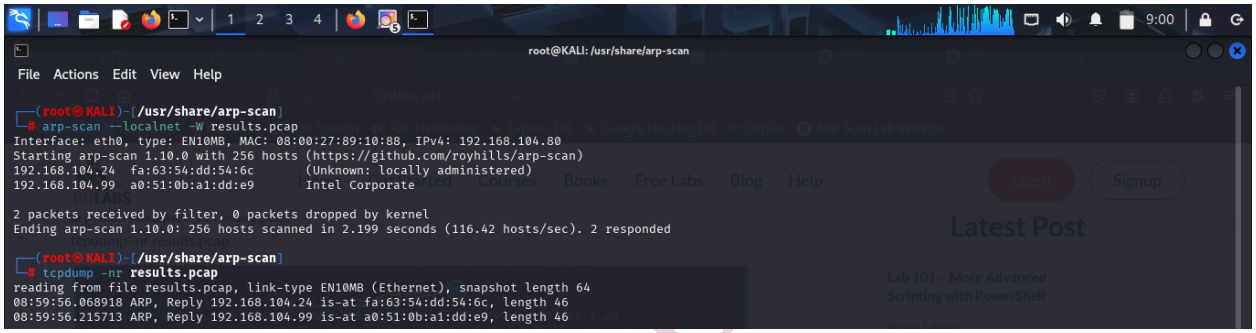
Map IP addresses to MAC addresses.

Identify vendor information.

Find IP conflicts (duplicate IPs).

Spot spoofed or unauthorized devices.

Validate VLAN segmentation and trunk configurations.



🔚 Conclusion

Using arp-scan is a fast, efficient way to conduct network reconnaissance on local IPv4 networks. It leverages the Address Resolution Protocol to map out who is connected, on what IP/MAC, and what vendor they're using.