Lab 25 – Using the route command to display network information on Linux

🧭 Lab Objective:

Learn how to view, modify, and manage the IP/kernel routing table using the route command and the more modern ip command on a Kali Linux machine.
🛠️ Lab Requirements:

OS: Kali Linux (VM or physical)

Root access (some commands need elevated privileges)

Terminal access

⚙️ Step 0: Become Root User

sudo su -

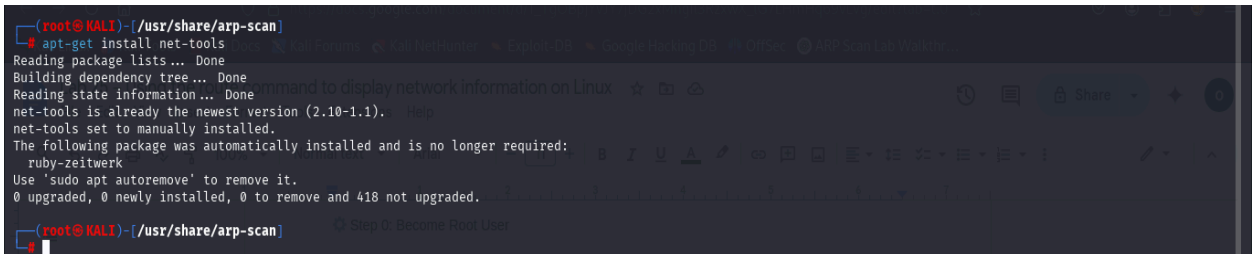
👈 Why?

Managing routing tables involves making changes at the network level.

Root access is required to add, remove, or reject routes.

🔹 Task 1: Install net-tools and View the Help Screen
✅ Step 1.1: Install net-tools

apt-get install net-tools



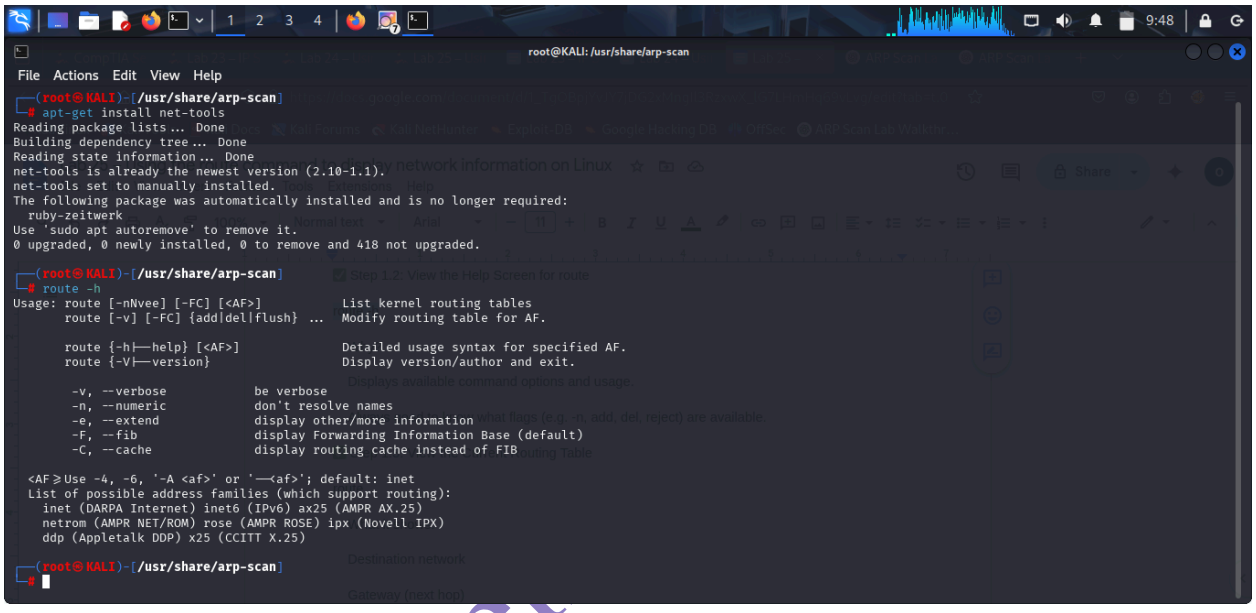
Why?

The legacy route command is part of the net-tools package.

Many modern distros use ip route instead, so you might need to install net-tools manually.

✅ Step 1.2: View the Help Screen for route

route -h



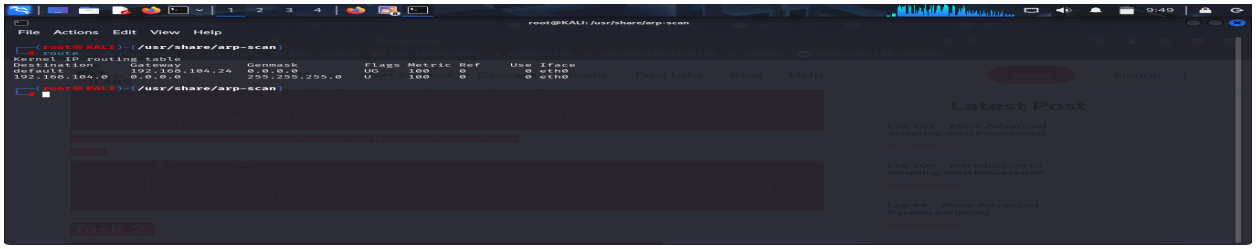
Why?

Displays available command options and usage.

Always good to know what flags (e.g. -n, add, del, reject) are available.

✅ Step 1.3: View the Current Routing Table

route



What it shows:

Destination network

Gateway (next hop)

Genmask (subnet mask)

Flags (e.g. U for up, G for gateway)

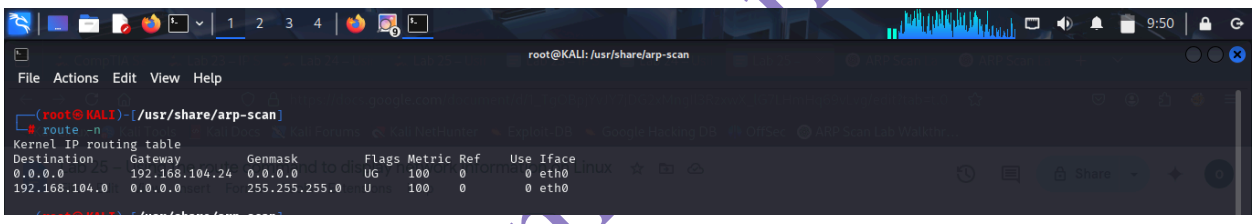
Interface used

Why?

This shows how your Linux system routes traffic to different destinations.

- Task 2: View the Routing Table in Numeric Format

route -n



Why use -n?

Prevents DNS name resolution.

Shows raw IP addresses, which is:

Faster

More reliable for scripting and debugging

Avoids confusion if DNS fails

✅ Tip: Always use -n for a faster, cleaner output when troubleshooting.

- Task 3: Add a Default Gateway

route add default gw 192.168.1.1

Replace 192.168.1.1 with your actual gateway IP.

Why?

The default gateway handles all traffic not destined for the local network.

Without a default gateway, your system can't access the internet or remote networks.

✅ Use Case: After a network reconfiguration or VPN setup, you may need to manually set your default gateway.

🔹 Task 4: View the Routing Cache

```
route -Cn
```

What this shows:

The cached routes the kernel is using for faster packet routing.

Why?

Helps you troubleshoot dynamic routing behavior.

If routing changes dynamically or appears inconsistent, check the cache.

✅ Note: This command may not work or be deprecated on some newer distros.

🔹 Task 5: Block Routing to a Specific Host

```
route add -host 192.168.1.51 reject
```

What this does:

Tells the kernel to reject traffic to that host.

Why?

This is a quick and simple way to block a specific IP address without using a firewall.

✅ Real-world use: Block access to a malicious or suspicious IP without installing or configuring iptables or firewalld.

🔹 Task 6: View Routing Table with Modern ip Command

```
ip route
```

Why?

ip route is the modern and preferred tool for viewing and modifying routes.

It's part of the iproute2 suite and replaces the older route command.

Output Example:

```
default via 192.168.1.1 dev eth0
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.100
```

✅ Tip: Use ip for scripting and working with advanced routing options.

🔹 Task 7: Delete the Default Gateway

```
route del default
```

⚠️ Warning:

Doing this will disconnect your system from external networks.

Make sure you note down your gateway IP before deleting it!

Why?

You may need to reset your routing table during troubleshooting or reconfiguration.

🔹 Task 8: View IPv4 and IPv6 Routes Separately

✅ View IPv4 Routes Only:

```
ip -4 route
```

✅ View IPv6 Routes Only:

```
ip -6 route
```

Why?

On dual-stack systems (IPv4 + IPv6), these filters help isolate issues.

Useful for:

- Debugging specific IP family issues

Ensuring both protocol versions are configured correctly