Lab Report 32: Spoofing Your MAC Address with macchanger

Lab Number: 32

Lab Title: Spoofing your MAC address with macchanger

Tool Used: Kali Linux (with `macchanger`)

Objective:

To learn how to spoof (change) a network interface's MAC address using the `macchanger` tool in Kali Linux — for privacy, penetration testing, or evading detection on networks.

Background:

A **MAC (Media Access Control)** address is a unique identifier assigned to a network interface card (NIC). In certain scenarios, such as ethical hacking or evading network tracking, we may need to spoof this address.

`macchanger` is a Linux utility that allows you to:

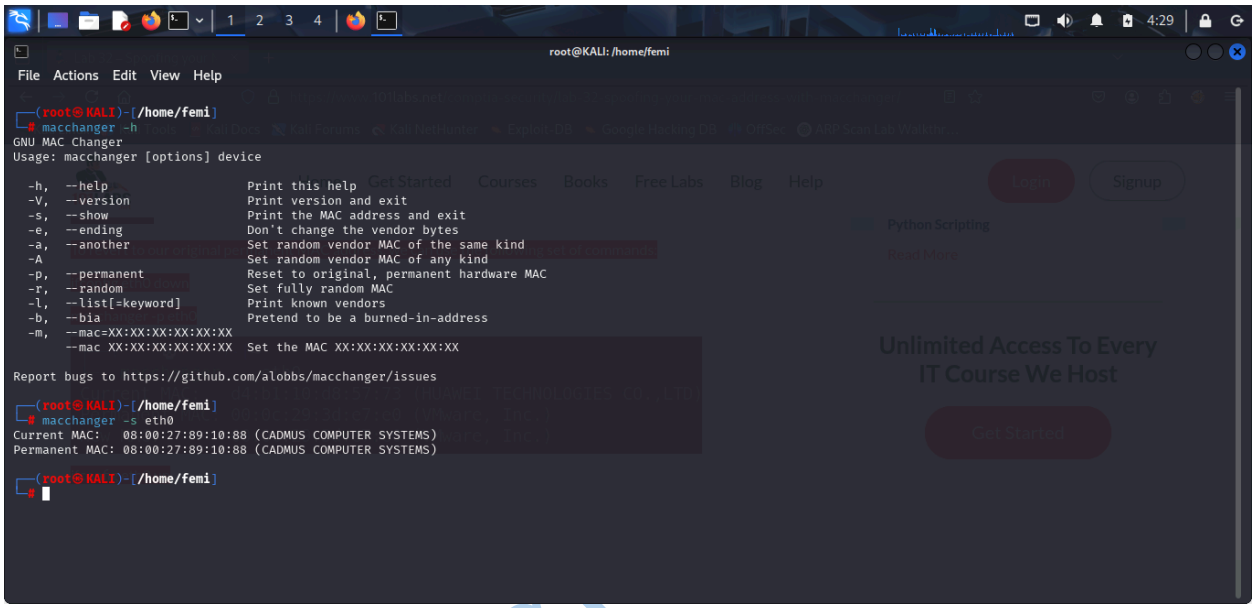
- View the current MAC address
- Randomize the MAC address
- Assign a specific MAC address
- Restore the original hardware MAC address

Lab Tasks and Execution:

Task 1: View Help Screen and Check Current MAC Address

Command(s) Used:

```
macchanger -h
macchanger -s eth0
```



Explanation:

- `macchanger -h`: Displays all options and usage instructions.
- `macchanger -s eth0`: Shows the current MAC address of the `eth0` interface.

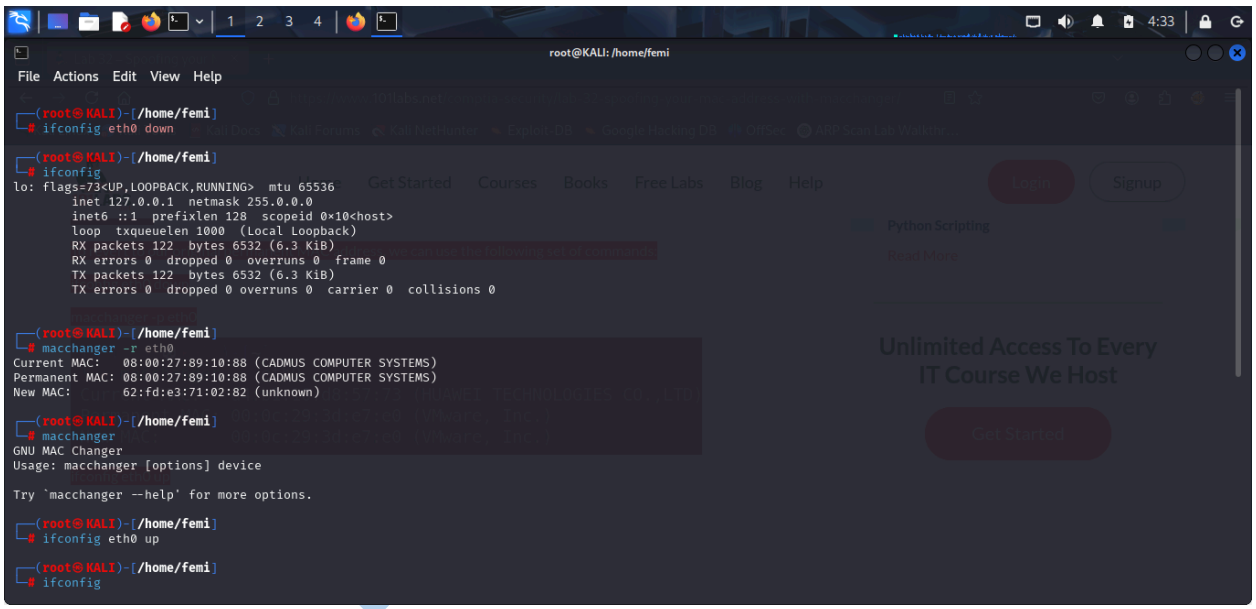
Observation:

The original hardware MAC address and current address are displayed.

Task 2: Change MAC Address to a Random Value

Step-by-Step Commands:

```
ifconfig eth0 down
ifconfig
macchanger -r eth0
macchanger
ifconfig eth0 up
ifconfig
macchanger -s eth0
```



Explanation:

- `ifconfig eth0 down`: Disables the interface so changes can be made.
- `macchanger -r eth0`: Assigns a random MAC address to the interface.
- `ifconfig eth0 up`: Brings the interface back online.
- `macchanger -s eth0`: Confirms that the MAC address has changed.

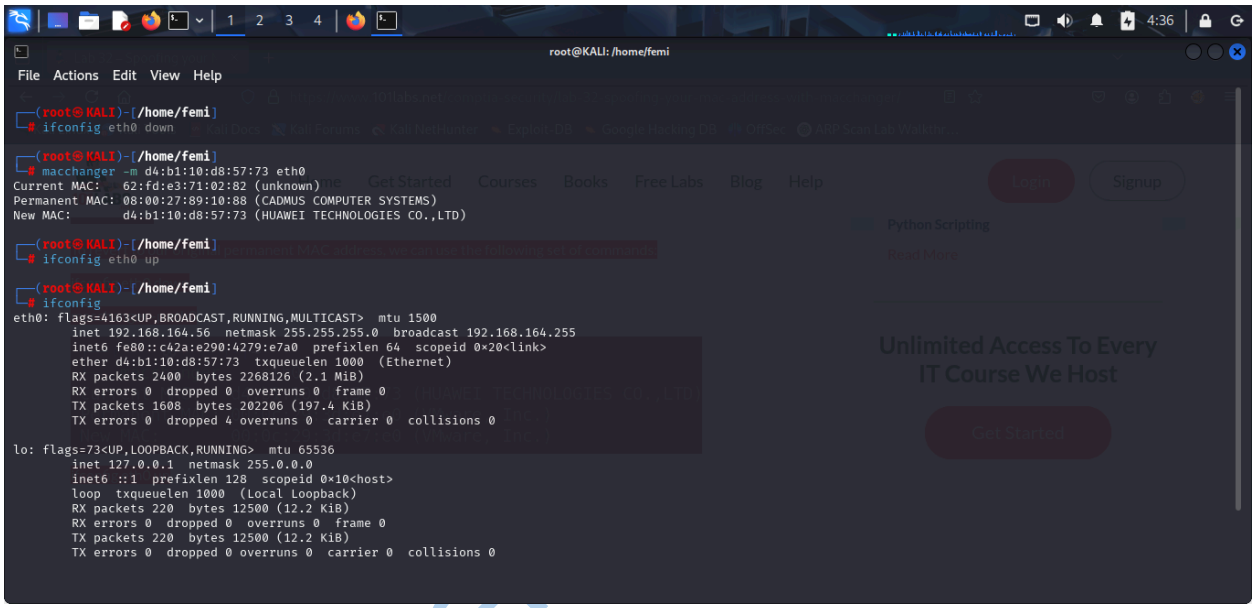
Result:

The MAC address was successfully changed to a random value.

Task 3: Set a Specific MAC Address (Manual Spoofing)

Step-by-Step Commands:

```
ifconfig eth0 down
macchanger -m d4:b1:10:d8:57:73 eth0
macchanger
ifconfig eth0 up
ifconfig
macchanger -s eth0
```



Explanation:

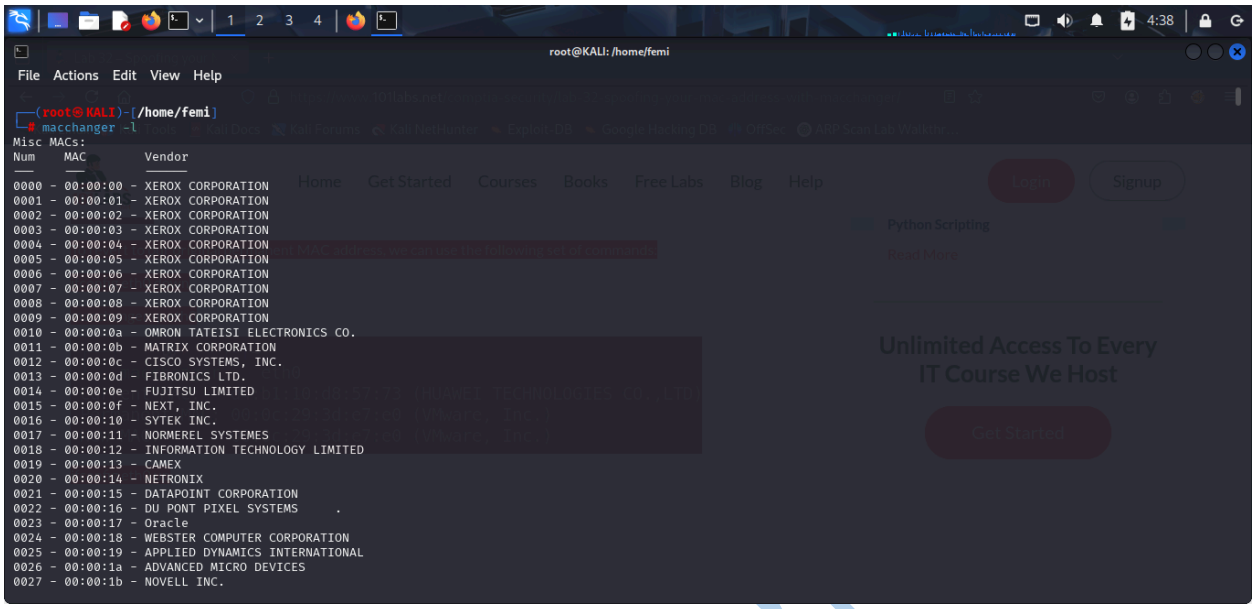
- `-m [address]`: Allows setting a specific MAC address manually.
- This is useful if we want to impersonate a specific device or vendor.

Result:

The MAC address was changed successfully to the specified value.

Task 4: List Vendor MAC Prefixes:

```
macchanger -l
```



Explanation:

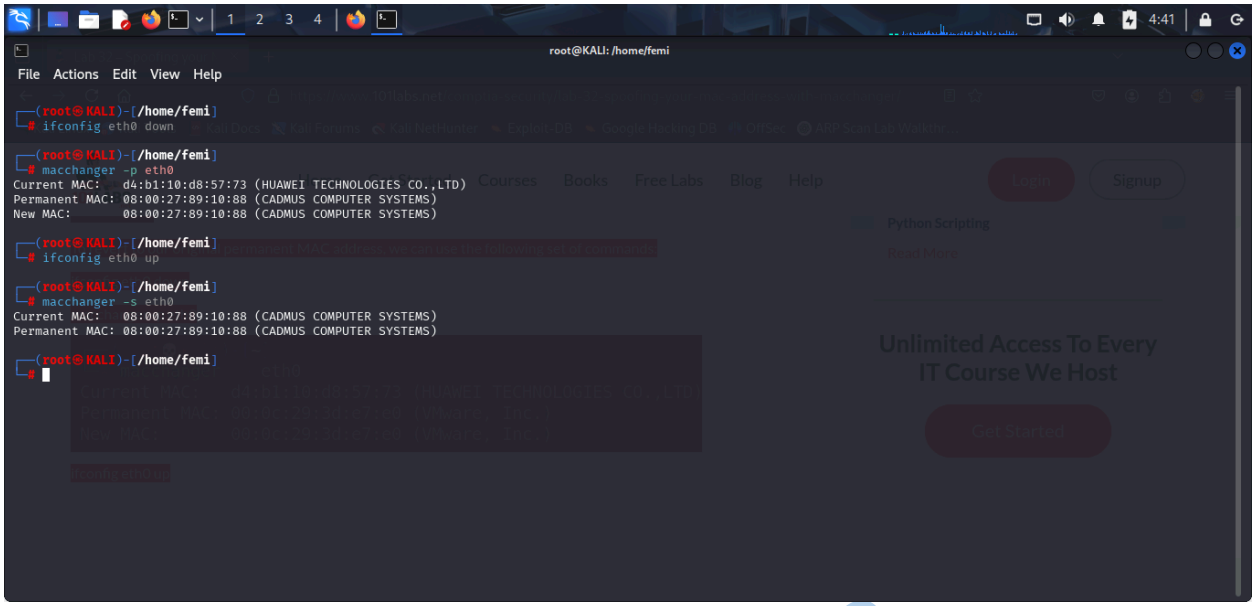
- Lists known MAC address prefixes assigned to hardware vendors.
- Useful if we want to spoof as a device from a specific company like Apple, Cisco, etc.

Observation:
A large list of vendors and their MAC prefixes was displayed.

Task 5: Revert to Original MAC Address

Step-by-Step Commands:

```
ifconfig eth0 down
macchanger -p eth0
macchanger
ifconfig eth0 up
```



Explanation:

- `-p`: Resets the MAC address back to the permanent hardware MAC.
- Useful after completing tests or audits to restore normal network behavior.

Result:
MAC address was successfully restored to its original state.

Conclusion:

This lab demonstrated how to effectively:

- View and understand a MAC address.
- Randomize or manually spoof a MAC address using `macchanger`.
- Masquerade as a specific device vendor.
- Restore the original hardware address after testing.

Real-World Use Case:
During penetration testing, changing the MAC address can help avoid detection by MAC-based filtering systems or intrusion detection systems (IDS).

- `macchanger -s eth0` before and after changing
- The `ifconfig` output showing the interface down and up
- The list of vendors using `macchanger -l`
