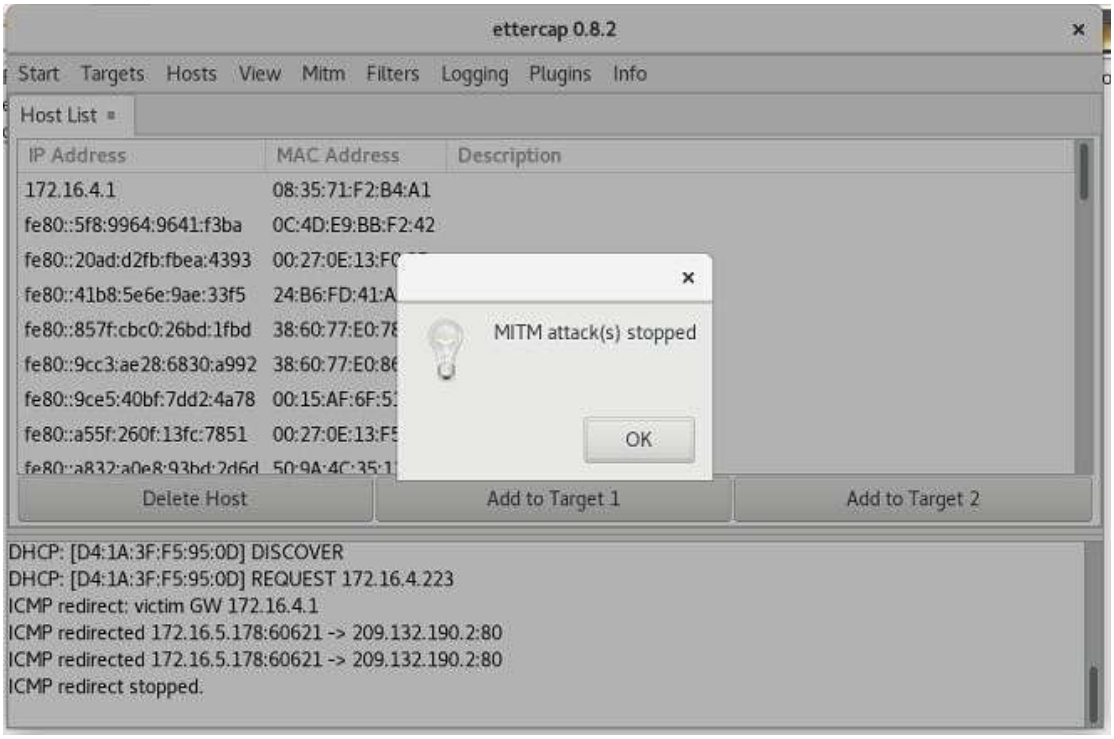

ETTECAP TOOL:

Ettercap is a well-known open-source tool used for conducting man-in-the-middle attacks on a local area network (LAN). It essentially functions as a network eavesdropper, allowing you to intercept traffic flowing between devices on the network.

- **Man-in-the-Middle Attacks:** By manipulating ARP (Address Resolution Protocol) Ettercap can position itself as an intermediary between two communicating devices. This allows it to intercept and potentially alter data flowing between them.

Ettercap's capabilities:

- **Packet Sniffing:** Ettercap can put your network interface in promiscuous mode, enabling it to capture all network traffic on the LAN segment, not just traffic directed to your device.
- **Man-in-the-Middle Attacks:** By manipulating ARP (Address Resolution Protocol) Ettercap can position itself as an intermediary between two communicating devices. This allows it to intercept and potentially alter data flowing between them.
- **Protocol Analysis:** Ettercap can dissect and analyze various network protocols, including some encrypted ones. This provides valuable insights into network communication patterns.
- **Data Injection and Filtering:** Ettercap can inject data packets into ongoing connections or filter out unwanted packets, enabling activities like modifying data streams.
- **Multiple Sniffing Modes:** Ettercap offers various sniffing modes, like IP-based, MAC-based, and ARP-based, catering to different network scenarios.

It's important to remember that Ettercap is a powerful tool and should be used with caution. While it's valuable for ethical hackers and penetration testers to assess network security, using it for malicious purposes is illegal.

- Ettercap offers both a graphical user interface (GUI) and a command-line interface (CLI) for user convenience.
- Ettercap has plugin support, allowing you to extend its functionalities.

To install **Ettercap** on Fedora using the terminal, follow these steps:

1. Update System Packages

First, update your system packages to ensure you have the latest repositories:

```
sudo dnf update -y
```

2. Install Ettercap

Ettercap is available in the Fedora repository. Install it using:

```
sudo dnf install -y ettercap
```

3. Verify Installation

Once installed, check the version to confirm:

```
ettercap --version
```

4. Run Ettercap

Ettercap can be run in graphical or command-line mode:

Graphical Mode (GUI):

```
sudo ettercap -G
```

Text-Based Interface (NCurses Mode):

```
sudo ettercap -C
```

Command-Line Mode:

```
sudo ettercap -T -Q
```

5. Allow Ettercap to Capture Packets

Since Ettercap requires root privileges for network sniffing, always run it with sudo. If you face issues, ensure your user is in the wheel group for sudo access.

RESULT:

In this experiment, we performed a MITM attack using Ettercap with ICMP redirects. We Observed how network traffic can be intercepted and redirected between hosts. This highlights the need for strong network security practices to prevent such attacks

WIFI HACKING 101

EXP.NO: 13 **DATE:08-04-2025**

AIM:

To understand and demonstrate how to capture and crack WPA/WPA2 personal Wi-Fi passwords using Aircrack-ng tools.

ALGORITHM:

1. Put the wireless interface into monitor mode.
2. Capture the 4-way handshake using airodump-ng.
3. (Optional) Deauthenticate a connected client to trigger handshake.
4. Use aircrack-ng with a wordlist to brute-force the password.
5. (Optional) Convert capture to HCCAPX format for GPU-based cracking with Hashcat.

OUTPUT:

How do you put the interface "wlan0" into monitor mode with Aircrack tools? (Full command)

airmon-ng start wlan0 ✓ Correct Answer

What is the new interface name likely to be after you enable monitor mode?

wlan0mon ✓ Correct Answer

What do you do if other processes are currently trying to use that network adapter?

airmon-ng check kill ✓ Correct Answer Hint

What tool from the aircrack-ng suite is used to create a capture?

airodump-ng ✓ Correct Answer

What flag do you use to set the BSSID to monitor?

--bssid ✓ Correct Answer Hint

And to set the channel?

--channel ✓ Correct Answer Hint

And how do you tell it to capture packets to a file?

-w ✓ Correct Answer Hint

What flag do we use to specify a BSSID to attack?

-b ✓ Correct Answer Hint

What flag do we use to specify a wordlist?

-w ✓ Correct Answer Hint

How do we create a HCCAPX in order to use hashcat to crack the password?

-j ✓ Correct Answer Hint

Using the rockyou wordlist, crack the password in the attached capture. What's the password?

greeneggsandham ✓ Correct Answer Hint

Where is password cracking likely to be fastest, CPU or GPU?

GPU ✓ Correct Answer Hint

RESULT:

In this experiment, we demonstrated the process of capturing and cracking WPA2 Passwords using tools like Air cracking and Hashcat. The experiment also highlighted that GPU-based cracking is faster than CPU-based cracking.