# MITM ATTACK WITH ETTERCAP

**EXP.NO: 12**

**AIM:**

To initiate a MITM attack using ICMP redirect with Ettercap tool.

**ALGORITHM:**

1. Install ettercap if not done already using the command

   dnf install ettercap

2. Open etter.conf file and change the values of ec_uid and ec_gid to zero from default.

   vi /etc/ettercap/etter.conf

3. Next start ettercap in GTK

   ettercap -G

4. Click sniff, followed by unified sniffing.
5. Select the interface connected to the network.
6. Next ettercap should load into attack mode by clicking Hosts followed by Scan for Hosts 7. Click Host List and choose the IP address for ICMP redirect
8. Now all traffic to that particular IP address is redirected to some other IP address.
9. Click MITM and followed by Stop to close the attack.



**OUTPUT:**

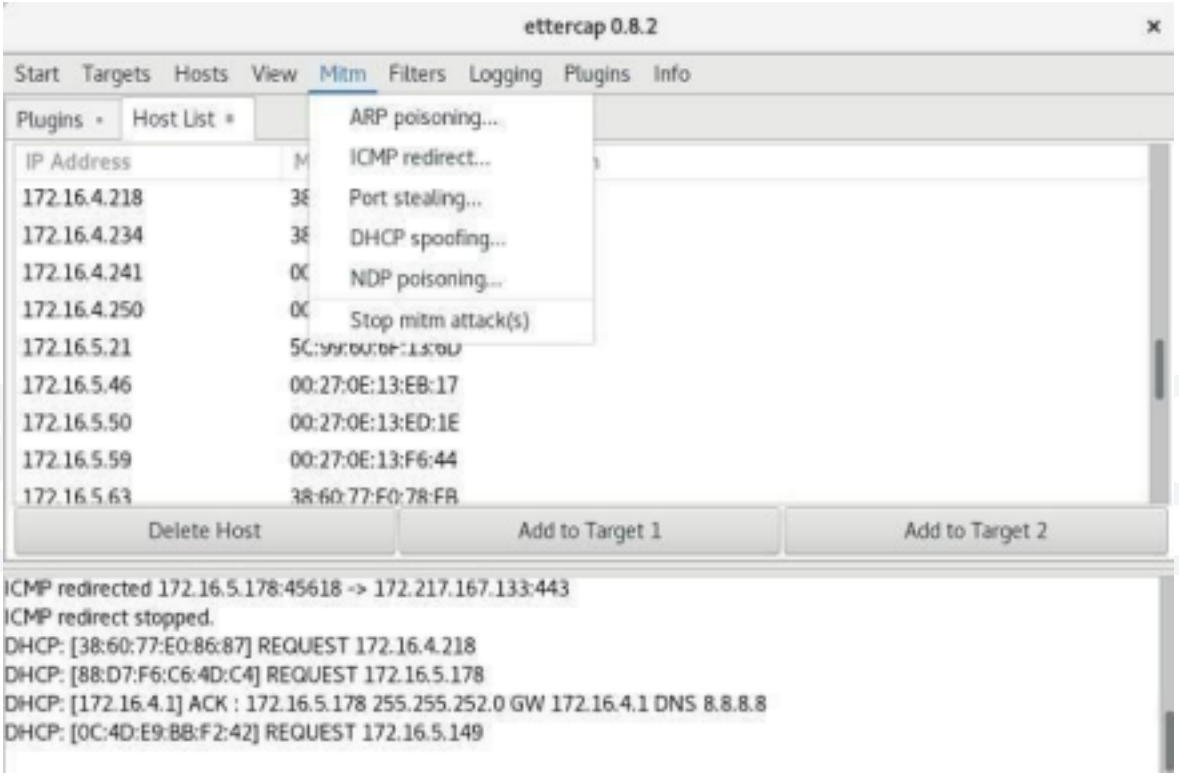
[root@localhost security lab]# dnf install ettercap

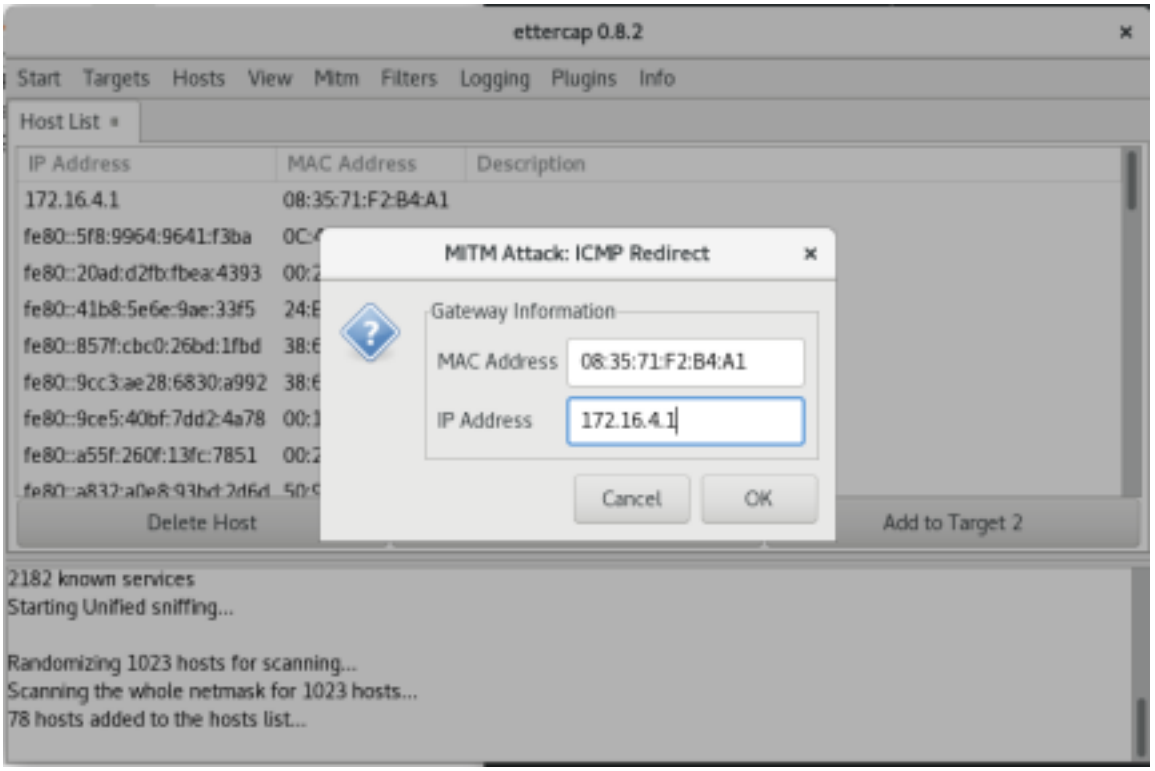
[root@localhost security lab]# vi /etc/ettercap/etter.conf

[root@localhost security lab]# ettercap –G

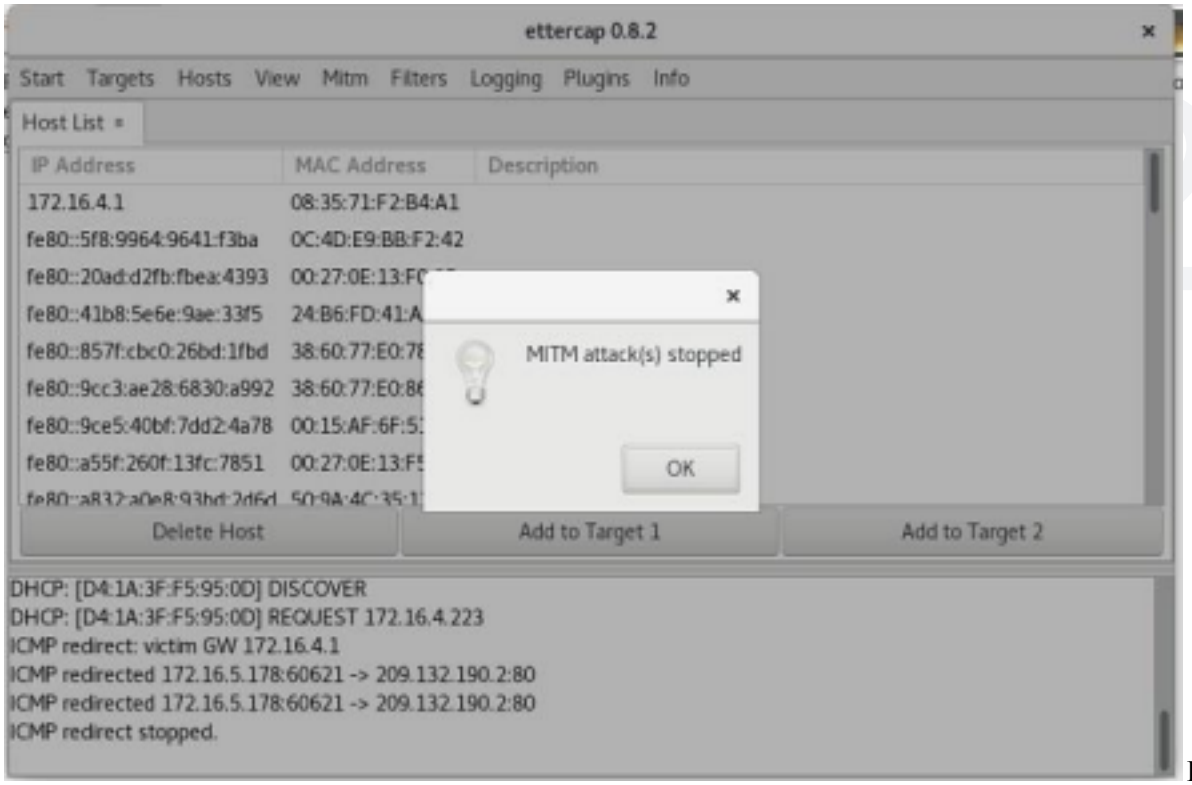

ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Hosts list Ctrl+H
Enable IPv6 scan
Scan for hosts Ctrl+S
Load from file...
Save to file...
Ettercap
DHCP: [E4:46:DA:A7:DC:AD] DISCOVER
DHCP: [E4:46:DA:A7:DC:AD] REQUEST 172.16.5.226
Randomizing 1023 hosts for scanning...
Scanning the whole netmask for 1023 hosts...
74 hosts added to the hosts list...




ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Plugins
Host List
ARP poisoning...
ICMP redirect...
Port stealing...
DHCP spoofing...
NDP poisoning...
Stop mitm attack(s)
IP Address
172.16.4.218
172.16.4.234
172.16.4.241
172.16.4.250
172.16.5.21
172.16.5.46 00:27:0E:13:EB:17
172.16.5.50 00:27:0E:13:ED:1E
172.16.5.59 00:27:0E:13:F6:44
Delete Host
Add to Target 1
Add to Target 2
ICMP redirected 172.16.5.178:45618 -> 172.217.167.133:443
ICMP redirect stopped.
DHCP: [38:60:77:E0:86:87] REQUEST 172.16.4.218
DHCP: [88:D7:F6:C6:4D:C4] REQUEST 172.16.5.178
DHCP: [172.16.4.1] ACK : 172.16.5.178 255.255.252.0 GW 172.16.4.1 DNS 8.8.8.8
DHCP: [0C:4D:E9:BB:F2:42] REQUEST 172.16.5.149






**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