

**MITM ATTACK WITH ETTERCAP**

**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
```

```
swetha277@fedora:~$ su root
Password:
root@fedora:/home/swetha277# dnf install ettercap
Fedora 40 - x86_64 -Updates          2.4 kB/s | 5.8 kB    00:02
Fedora 40 - x86_64 -Updates          319 kB/s | 1.1 MB    00:03
```

```
Last metadata expiration check: 0:00:03 ago on Mon 06 May 2024 07:52:20 PM IST.
Dependencies resolved.
```

```
=====
Package           Architecture      Version           Repository        Size
=====
Installing:
ettercap           x86_64            0.8.3.1-14.fc40   fedora            892 k
```

#### Transaction Summary

```
=====
Install 1 Package
```

```
Total download size: 892 k
```

```
Installed size: 2.7 M
```

```
Is this ok [y/N]: y
```

```
Downloading Packages:
```

```
ettercap-0.8.3.1-14.fc40.x86_64.rpm          963 kB/s | 892 kB    00:00
```

```
-----
Total                                          818 kB/s | 892 kB    00.01
```

```
Is this ok [y/N]: y
```

```
Downloading Packages:
```

```
ettercap-0.8.3.1-14.fc40.x86_64.rpm          963 kB/s | 892 kB    00:00
```

```
-----
Total
```

```
Running transaction check
```

```
Transaction check succeeded.
```

```
Running transaction test
```

```
Transaction test succeeded
```

```
Running transaction
```

```
  Preparing           :                               1/1
```

```
  Installing          : ettercap-0.8.3.1-14.fc40.x86_64 1/1
```

```
  Running scriptlet: ettercap-0.8.3.1-14.fc40.x86_64 1/1
```

```
Installed:
```

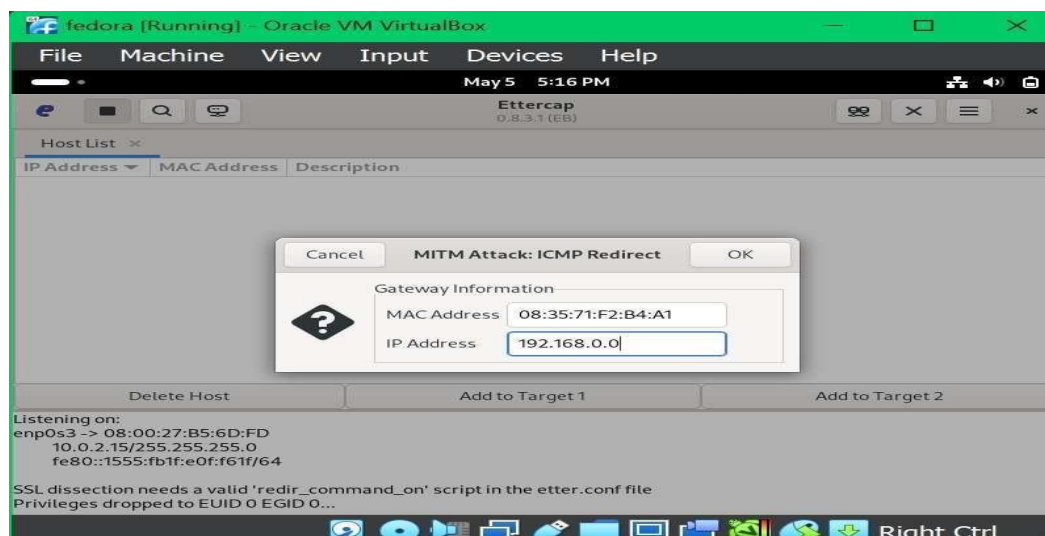
```
ettercap-0.8.3.1-14.fc40.x86_64
```



```
Complete!
```

```
root@fedora:/home/swetha277# vi /etc/ettercap/etter.conf
```

```
root@fedora: /home/swetha277# ettercap -6
```





```
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```






Ettercap

0.8.3.1 (EB)



Host List 

IP Address	MAC Address	Description
------------	-------------	-------------

Delete Host

Add to Target 1

Add to Target 2

1766 tcp OS fingerprint

2182 known services

Starting Unified sniffing...

ICMP redirect: victim GW 192.168.0.0

ICMP redirect stopped.

**Result:**