

Ex. No.: 10

Date: 01.11.24

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`

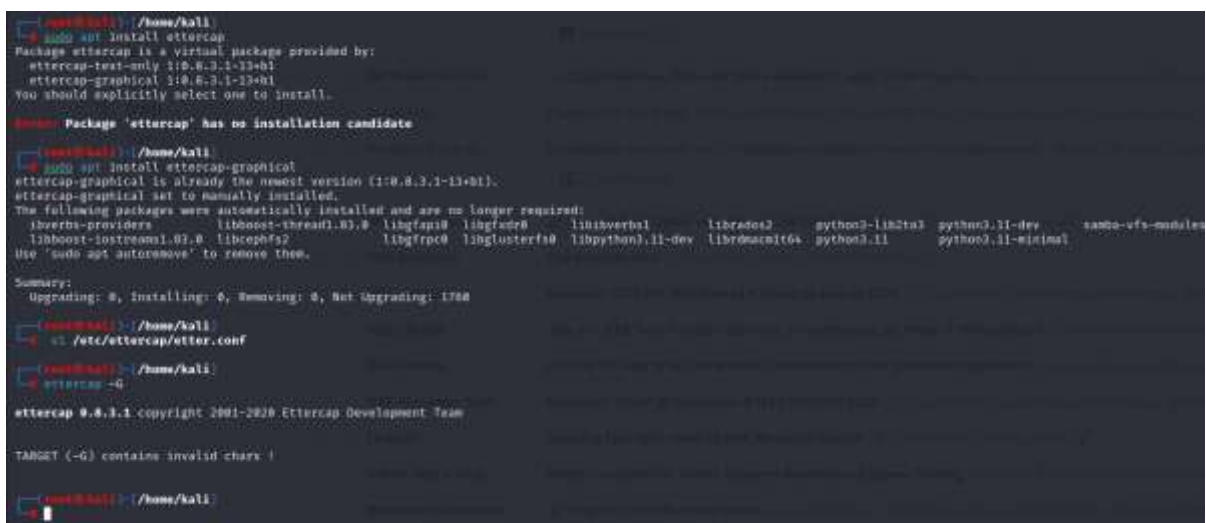
4. Click sniff, followed by unified sniffing.
5. Select the interface connected to the network.
6. Next ettercap should load into attack mode by clicking Hosts followed by Scan for Hosts
7. Click Host List and choose the IP address for ICMP redirect
8. Now all traffic to that particular IP address is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



```
root@kali: ~# sudo apt install ettercap
Package ettercap is a virtual package provided by:
  ettercap-text-only 1:0.8.3.1-13+b1
  ettercap-graphical 1:0.8.3.1-13+b1
You should explicitly select one to install.

Error: Package 'ettercap' has no installation candidate

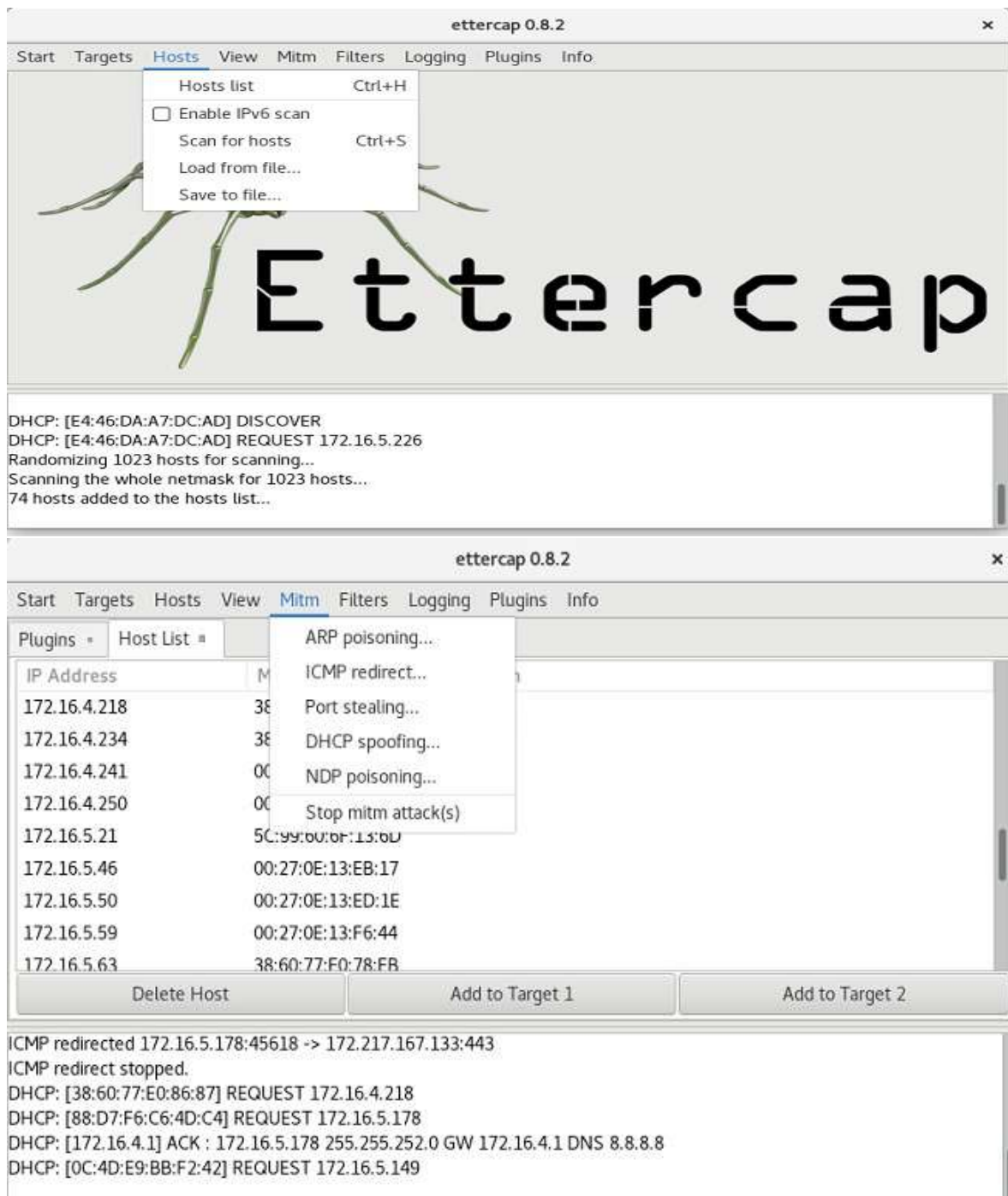
root@kali: ~# sudo apt install ettercap-graphical
ettercap-graphical is already the newest version (1:0.8.3.1-13+b1).
ettercap-graphical set to manually installed.
The following packages were automatically installed and are no longer required:
  libverbs-providers libboost-thread1.83.0 libgfan0 libgfrdr0 libisverbal librados2 python3-lib2to3 python3.11-dev samba-ufs-modules
  libboost-iostreams1.83.0 libcephfs2 libgfrpc0 libglusterfs0 libpython3.11-dev librados2 python3.11 python3.11-minimal
Use 'sudo apt autoremove' to remove them.

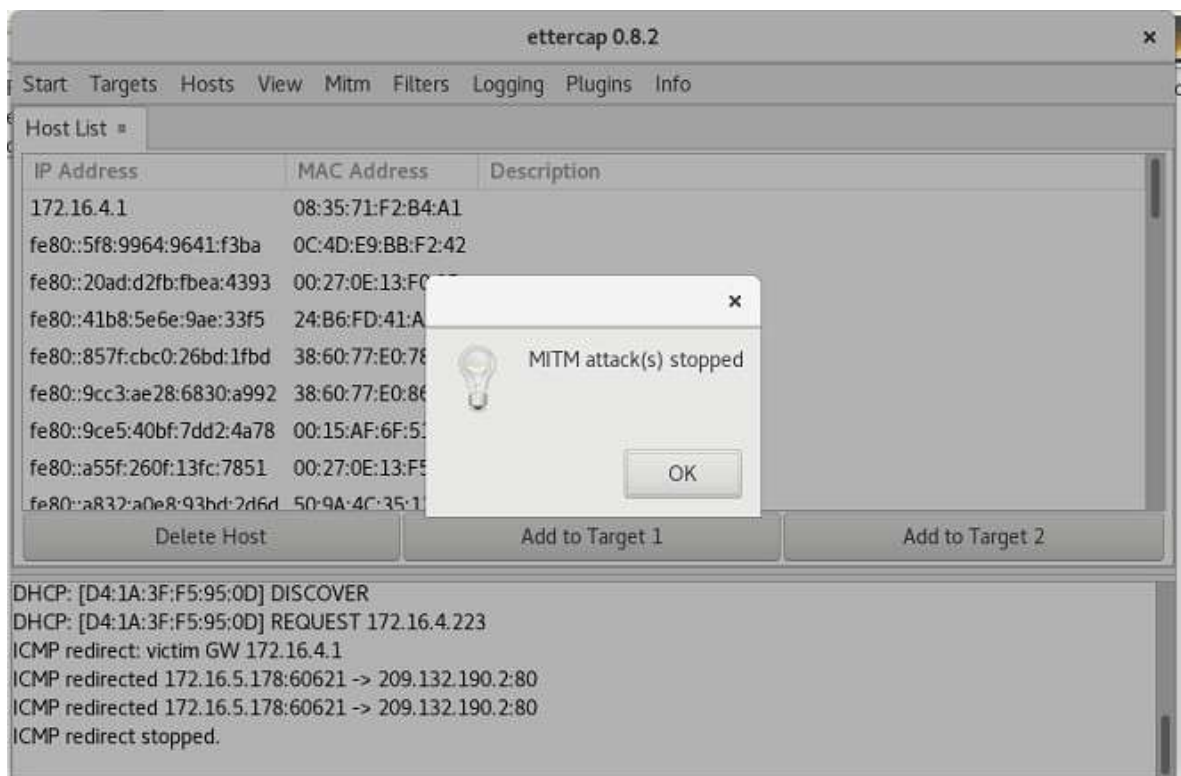
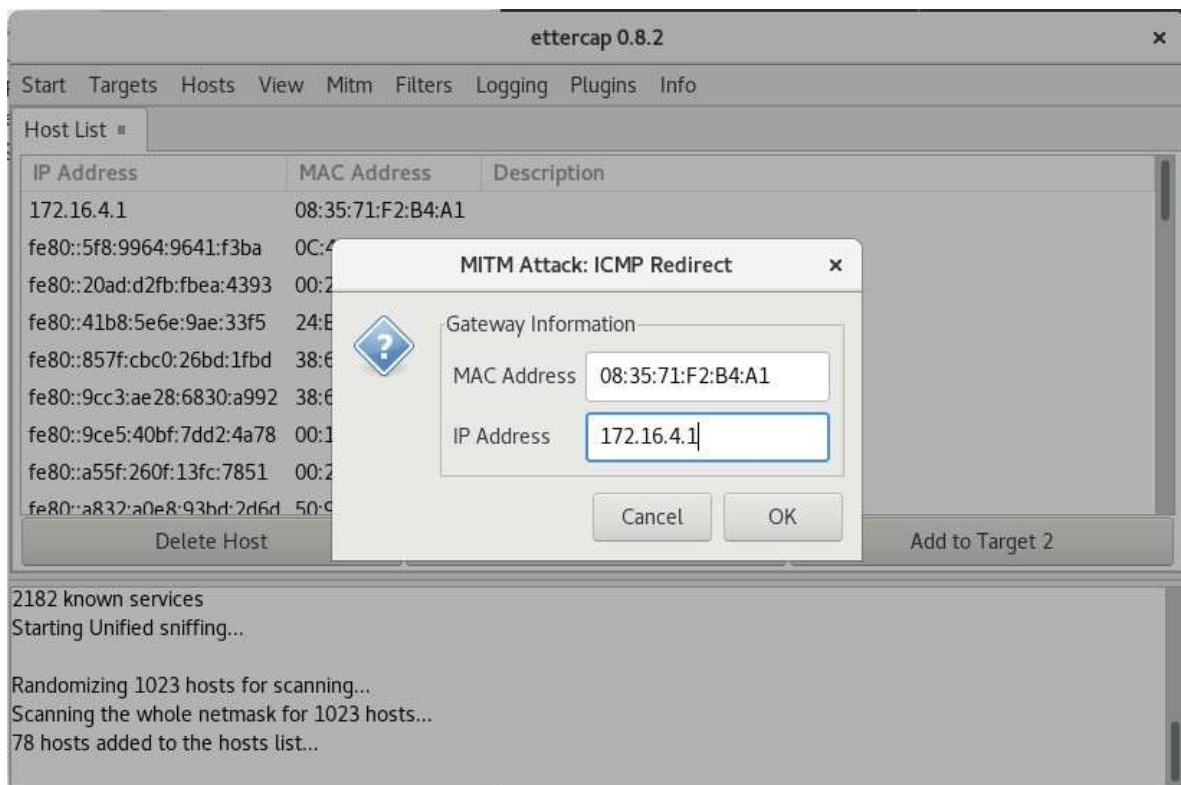
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1780

root@kali: ~# sudo apt install ettercap-graphical
root@kali: ~# vi /etc/ettercap/etter.conf
root@kali: ~# ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

TARGET (-G) contains invalid char !
```





Result: Thus the MITM attack has been successfully executed using Ettercap tool.