

Ex. No.: 12

Date:

MITM ATTACK WITH ETTERCAP

Aim:

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

Algorithm:

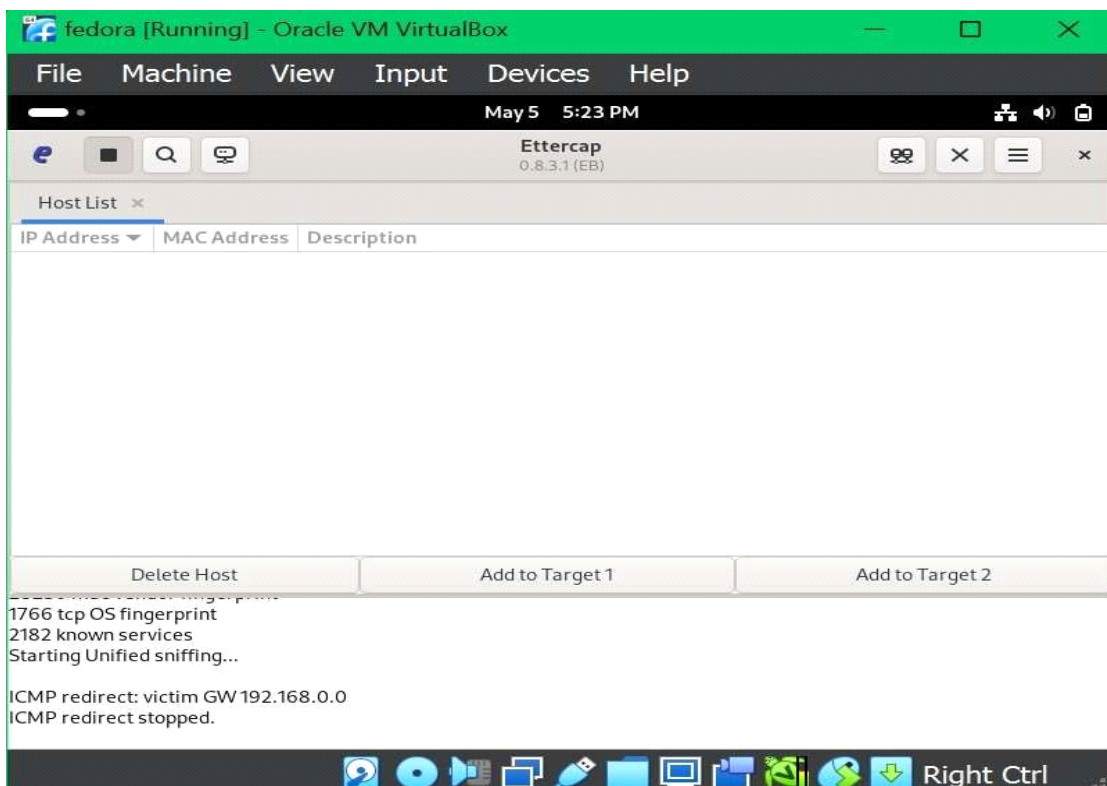
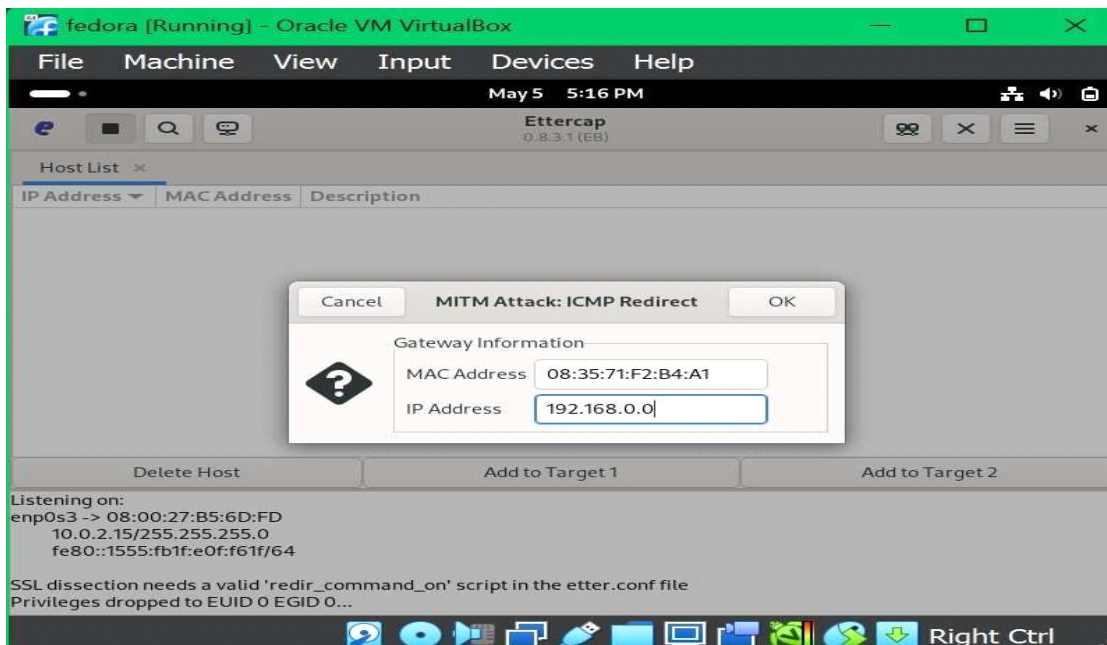
- Install ettercap if not done already using
the command-dnf install ettercap
- Open etter.conf file and change the values of ec_uid and ec_gid to zero from default.
vi /etc/ettercap/etter.conf
- Next start ettercap in
GTK ettercap -G
- Click sniff, followed by unified sniffing.
- Select the interface connected to the network.
- Next ettercap should load into attack mode by clicking Hosts followed by Scan for Hosts
- Click Host List and choose the IP address for ICMP redirect
- Now all traffic to that particular IP address is redirected to some other IP address.
- 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@fedora:/home/sudhashreemadhu# dnf install ettercap
Copr repo for PyCharm owned by phracek          2.3 kB/s | 2.9 kB      00:01
google-chrome                                2.2 kB/s | 1.7 kB      00:00
RPM Fusion for Fedora 40 - Nonfree - NVIDIA Dri 1.7 kB/s | 7.0 kB      00:04
RPM Fusion for Fedora 40 - Nonfree - Steam      903 B/s | 1.4 kB      00:01
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            201 kB/s | 892 kB      00:04

```

```

+ sudhashreemadhu@fedora:/home/sudhashreemadhu  Q  ≡  x
File Edit View Search Terminal Help
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/sudhashreemadhu# vi/etc/ettercap/etter.conf
U: vi/etc/ettercap/etter.conf: No such file or directory
root@fedora:/home/sudhashreemadhu# vi /etc/ettercap/etter.conf
root@fedora:/home/sudhashreemadhu# ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
^C

```



Result: