Ex. No.: 12 **Date:**

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

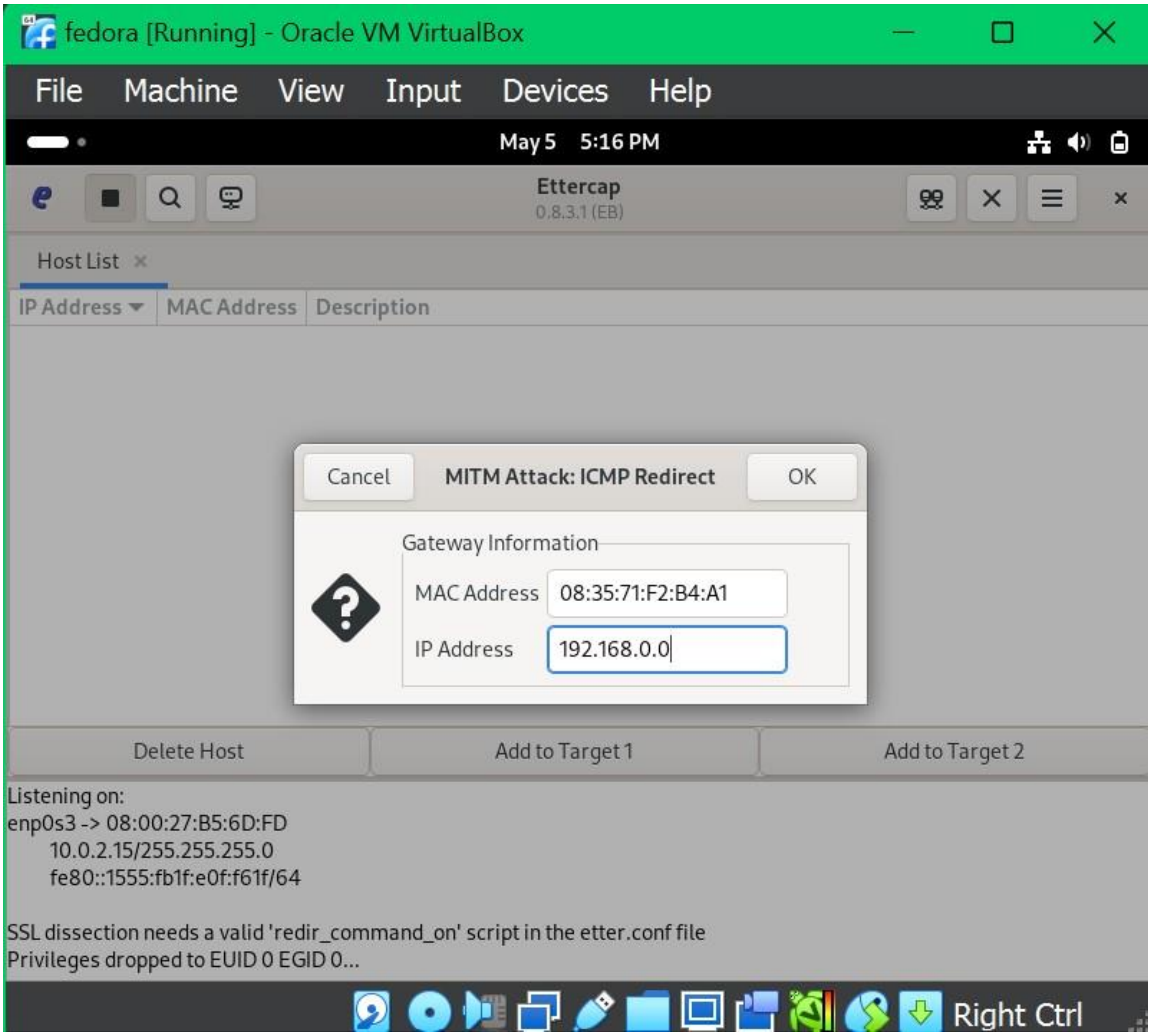
3. Next start ettercap in GTK

   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
```



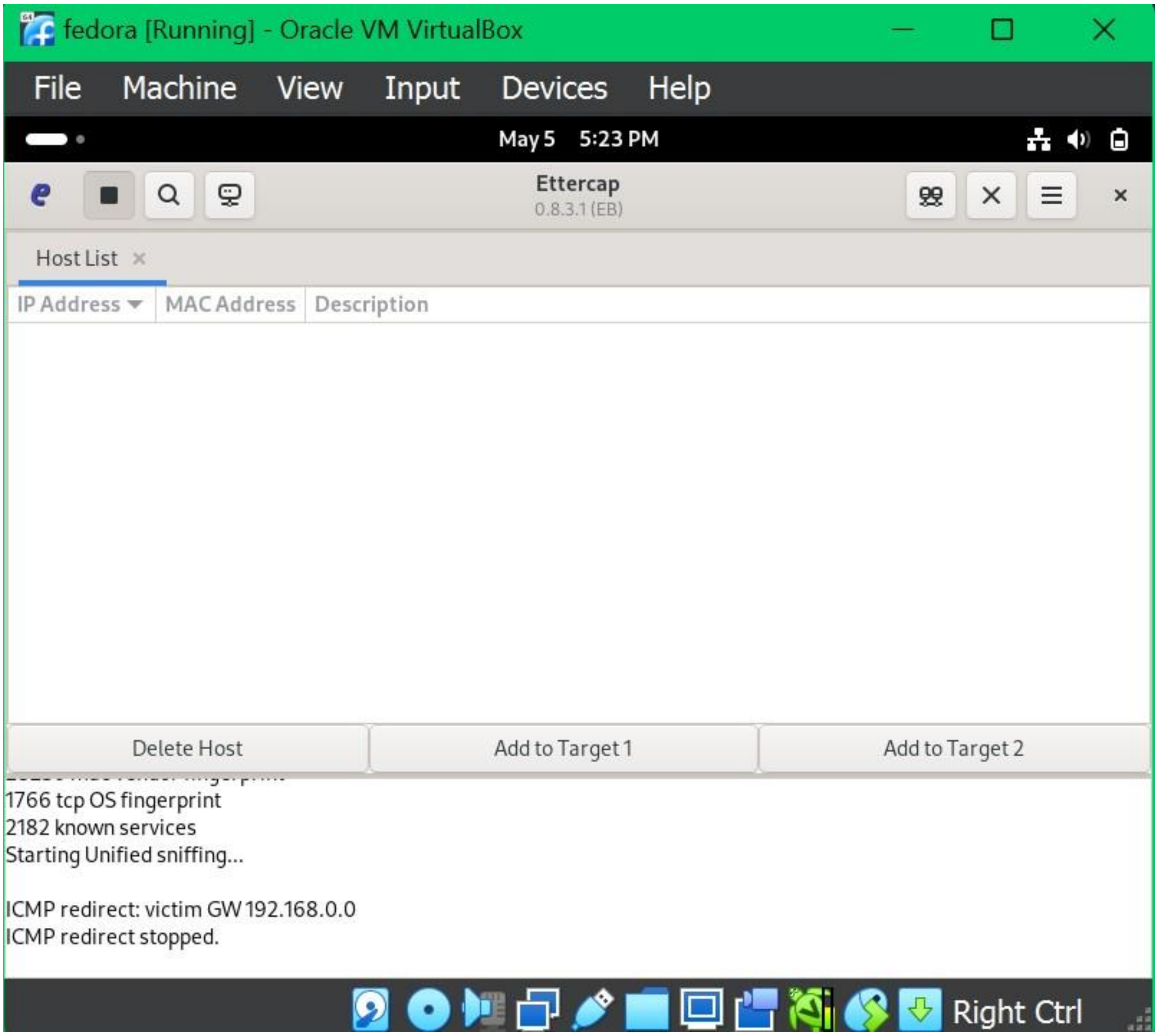
MITM Attack: ICMP Redirect

Gateway Information

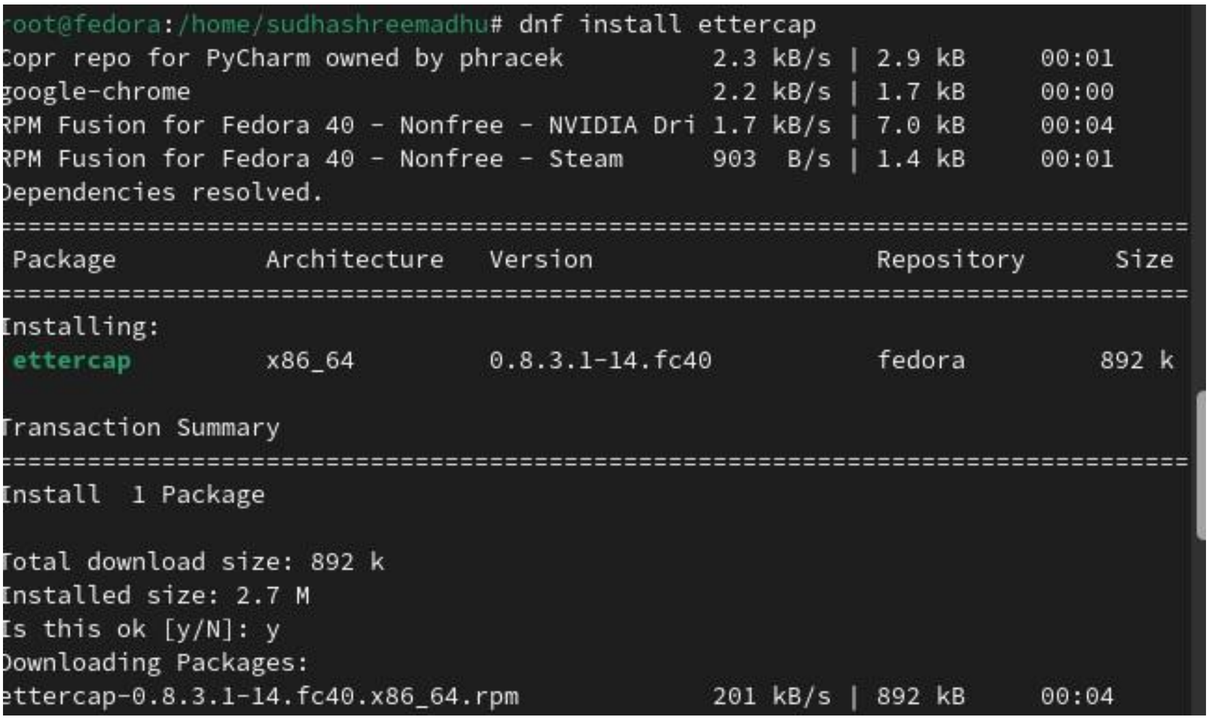
MAC Address: 08:35:71:F2:B4:A1

IP Address: 192.168.0.0

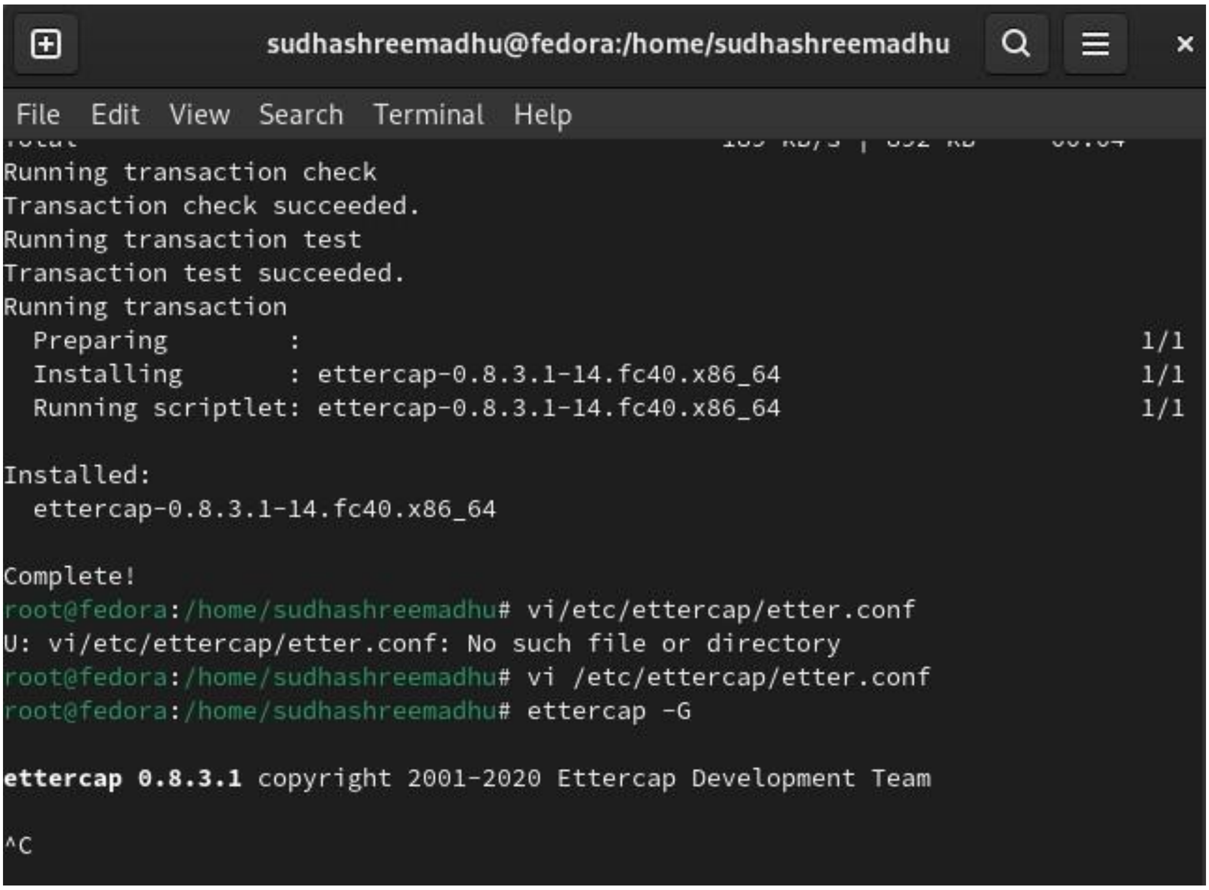
```
Listening on:
enp0s3 -> 08:00:27:B5:6D:FD
    10.0.2.15/255.255.255.0
    fe80::1555:fb1f:e0f:f61f/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 0 EGID 0...
```



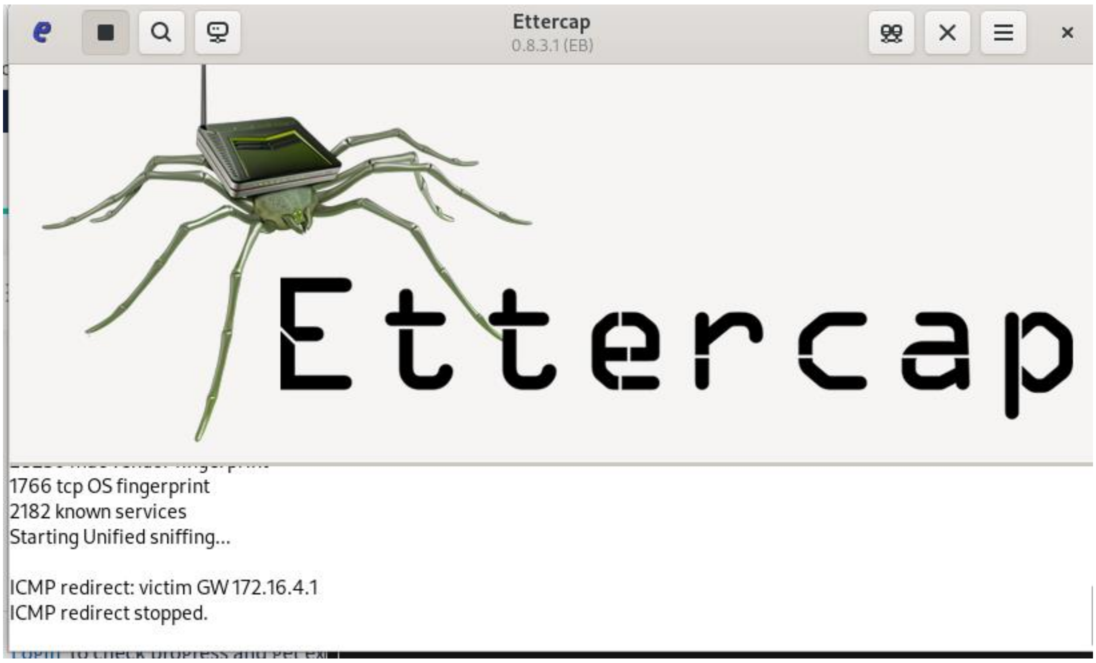
```
1766 tcp OS fingerprint
2182 known services
Starting Unified sniffing...

ICMP redirect: victim GW 192.168.0.0
ICMP redirect stopped.
```



```
oot@fedora:/home/sudhashreemadhu# dnf install ettercap
opr repo for PyCharm owned by phracek          2.3 kB/s | 2.9 kB     00:01
oogle-chrome                                   2.2 kB/s | 1.7 kB     00:00
PM Fusion for Fedora 40 - Nonfree - NVIDIA Dri 1.7 kB/s | 7.0 kB     00:04
PM Fusion for Fedora 40 - Nonfree - Steam      903  B/s | 1.4 kB     00:01
ependencies resolved.
===============================================================================
 Package          Architecture   Version                   Repository      Size
===============================================================================
nstalling:
 ettercap         x86_64         0.8.3.1-14.fc40           fedora         892 k

ransaction Summary
===============================================================================
nstall  1 Package

otal download size: 892 k
nstalled size: 2.7 M
s this ok [y/N]: y
ownloading Packages:
ttercap-0.8.3.1-14.fc40.x86_64.rpm             201 kB/s | 892 kB     00:04
```



```
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
```



```
1766 tcp OS fingerprint
2182 known services
Starting Unified sniffing...

ICMP redirect: victim GW 172.16.4.1
ICMP redirect stopped.
```

Result: