

Ex. No.:

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
```

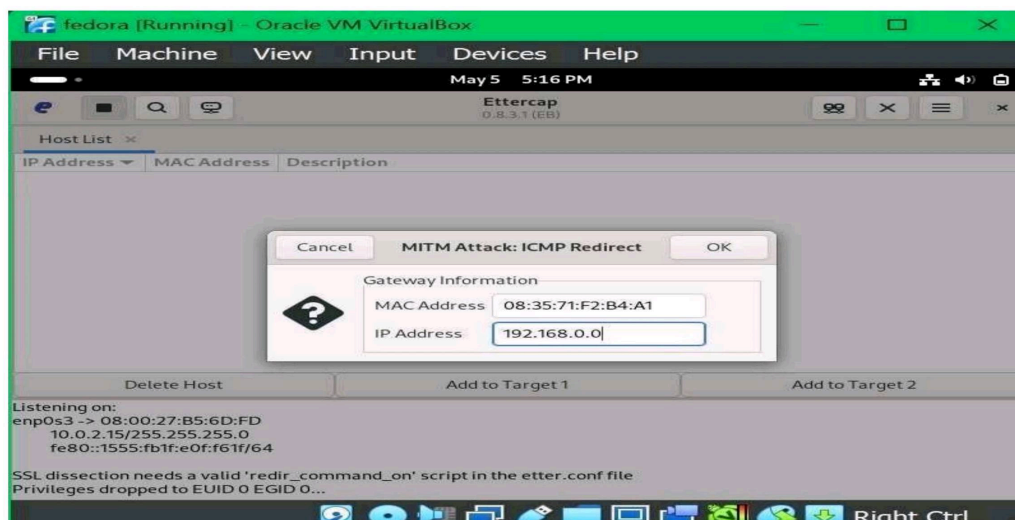
```
[root@localhost security lab]# vi /etc/ettercap/etter.conf
```


```
[root@localhost security lab]# ettercap -G
```

```
May 8 8:22 PM
root@thirueswaran-Inspiron-3443: /home/thirueswaran

Unpacking liblua5.1-common (2.1.0-beta3+git20220320+dfsg-4.1) ...
Selecting previously unselected package liblua5.1-2:amd64.
Preparing to unpack .../4-liblua5.1-2_2.1.0-beta3+git20220320+dfsg-4.1_amd64.deb ...
Unpacking liblua5.1-2:amd64 (2.1.0-beta3+git20220320+dfsg-4.1) ...
Selecting previously unselected package libnet1:amd64.
Preparing to unpack .../5-libnet1_1.1.6+dfsg-3.2_amd64.deb ...
Unpacking libnet1:amd64 (1.1.6+dfsg-3.2) ...
Selecting previously unselected package ettercap-common.
Preparing to unpack .../6-ettercap-common_1%3a0.8.3.1-12_amd64.deb ...
Unpacking ettercap-common (1:0.8.3.1-12) ...
Selecting previously unselected package ettercap-graphical.
Preparing to unpack .../7-ettercap-graphical_1%3a0.8.3.1-12_amd64.deb ...
Unpacking ettercap-graphical (1:0.8.3.1-12) ...
Setting up libnet1:amd64 (1.1.6+dfsg-3.2) ...
Setting up liblua5.1-common (2.1.0-beta3+git20220320+dfsg-4.1) ...
Setting up libgeoip1:amd64 (1.6.12-11) ...
Setting up geoip-database (20230704-1) ...
Setting up ethtool (1:6.5-1ubuntu0.1) ...
Setting up liblua5.1-2:amd64 (2.1.0-beta3+git20220320+dfsg-4.1) ...
Setting up ettercap-common (1:0.8.3.1-12) ...
Setting up ettercap-graphical (1:0.8.3.1-12) ...
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for mailcap (3.70+nmuiubuntu1) ...
Processing triggers for desktop-file-utils (0.26-1ubuntu5) ...
Processing triggers for gnome-menus (3.36.0-1.1ubuntu1) ...
Processing triggers for libc-bin (2.38-1ubuntu6.2) ...
root@thirueswaran-Inspiron-3443:/home/thirueswaran# vi /etc/ettercap/etter.conf
root@thirueswaran-Inspiron-3443:/home/thirueswaran# ettercap -G



ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
root@thirueswaran-Inspiron-3443:/home/thirueswaran#
```










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: