Ex. No.: 12

Date:4/5/24 **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

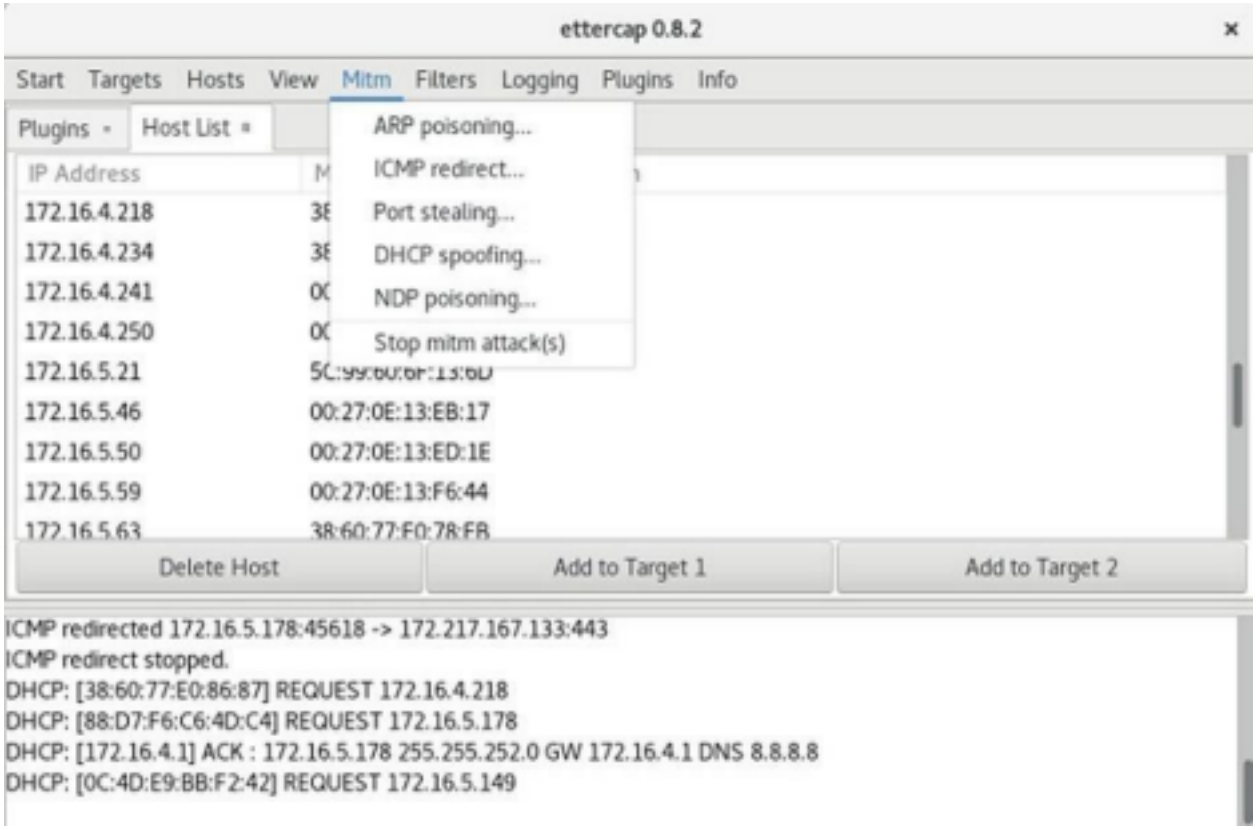
8.Now all traffic to that particular IP address is redirected to some other IP address. 9.Click MITM and followed by Stop to close the attack.

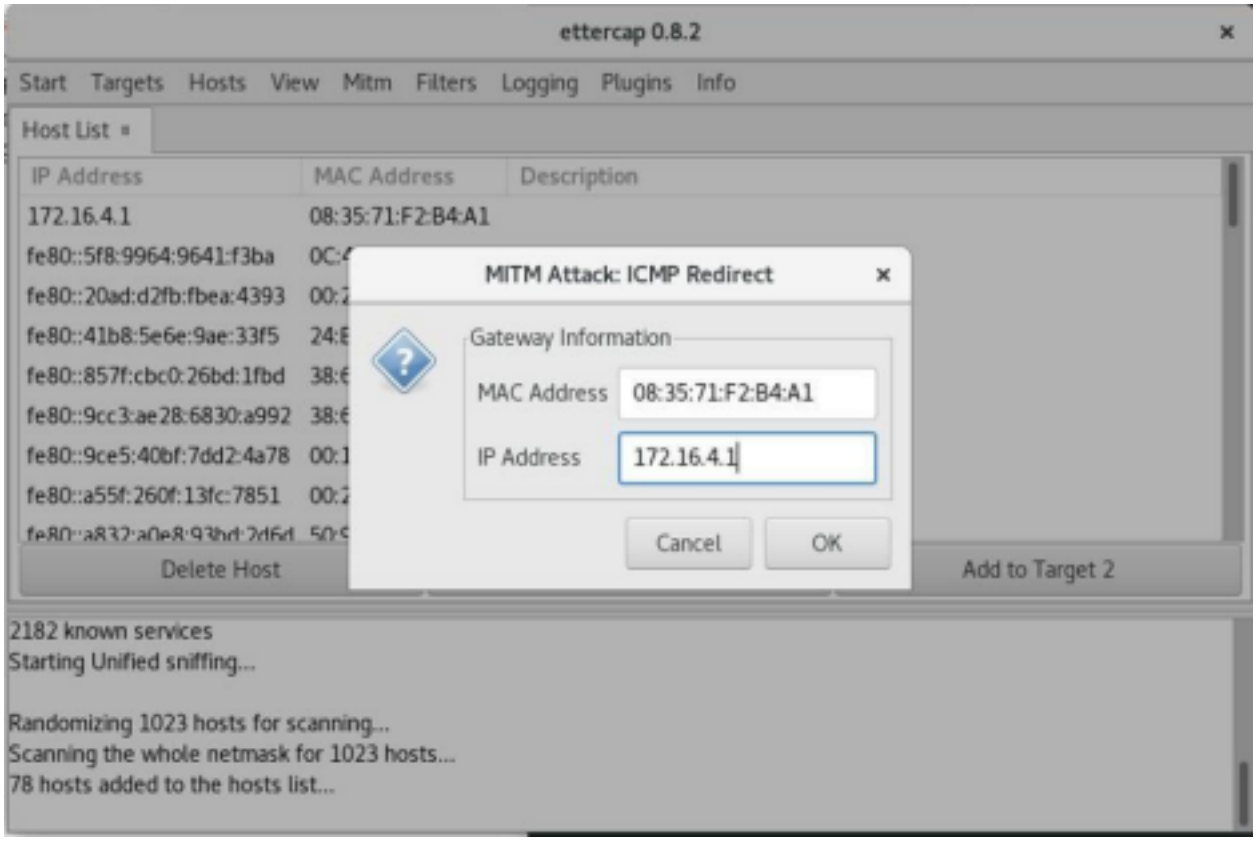
Output:

[root@localhost security lab]# dnf install ettercap

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

[root@localhost security lab]# ettercap –G


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Plugins
Host List
ARP poisoning...
ICMP redirect...
Port stealing...
DHCP spoofing...
NDP poisoning...
Stop mitm attack(s)
IP Address
172.16.4.218
172.16.4.234
172.16.4.241
172.16.4.250
172.16.5.21
172.16.5.46 00:27:0E:13:EB:17
172.16.5.50 00:27:0E:13:ED:1E
172.16.5.59 00:27:0E:13:F6:44
Delete Host
Add to Target 1
Add to Target 2
ICMP redirected 172.16.5.178:45618 -> 172.217.167.133:443
ICMP redirect stopped.
DHCP: [38:60:77:E0:86:87] REQUEST 172.16.4.218
DHCP: [88:D7:F6:C6:4D:C4] REQUEST 172.16.5.178
DHCP: [172.16.4.1] ACK : 172.16.5.178 255.255.252.0 GW 172.16.4.1 DNS 8.8.8.8
DHCP: [0C:4D:E9:BB:F2:42] REQUEST 172.16.5.149



Result: To initiate a MITM attack using ICMP redirect with Ettercap tool has been Executed successfully.