Ex. No.: 12

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 commandettercap dnf install
- 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.

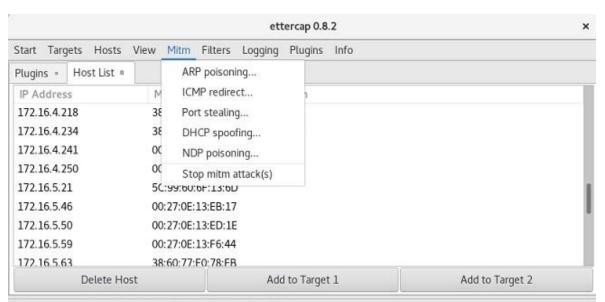
Output:

[root@localhost security lab]# dnf install ettercap

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

[root@localhost security lab]# ettercap -G





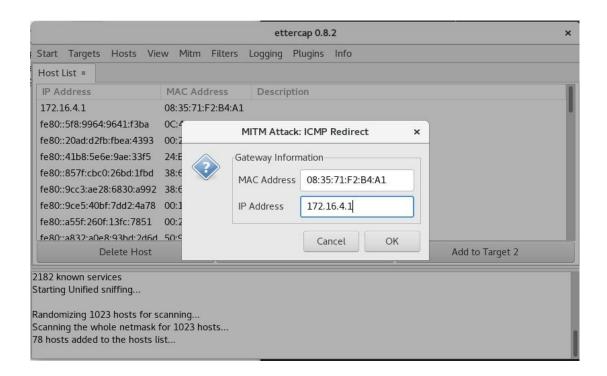
ICMP redirected 172.16.5.178:45618 -> 172.217.167.133:443

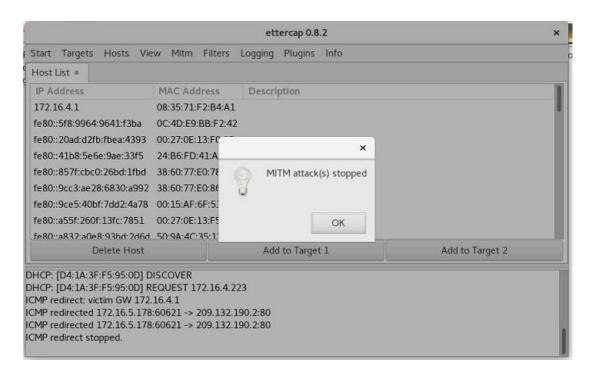
ICMP redirect stopped.

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: