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

MITM ATTACK WITH ETTERCAP

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

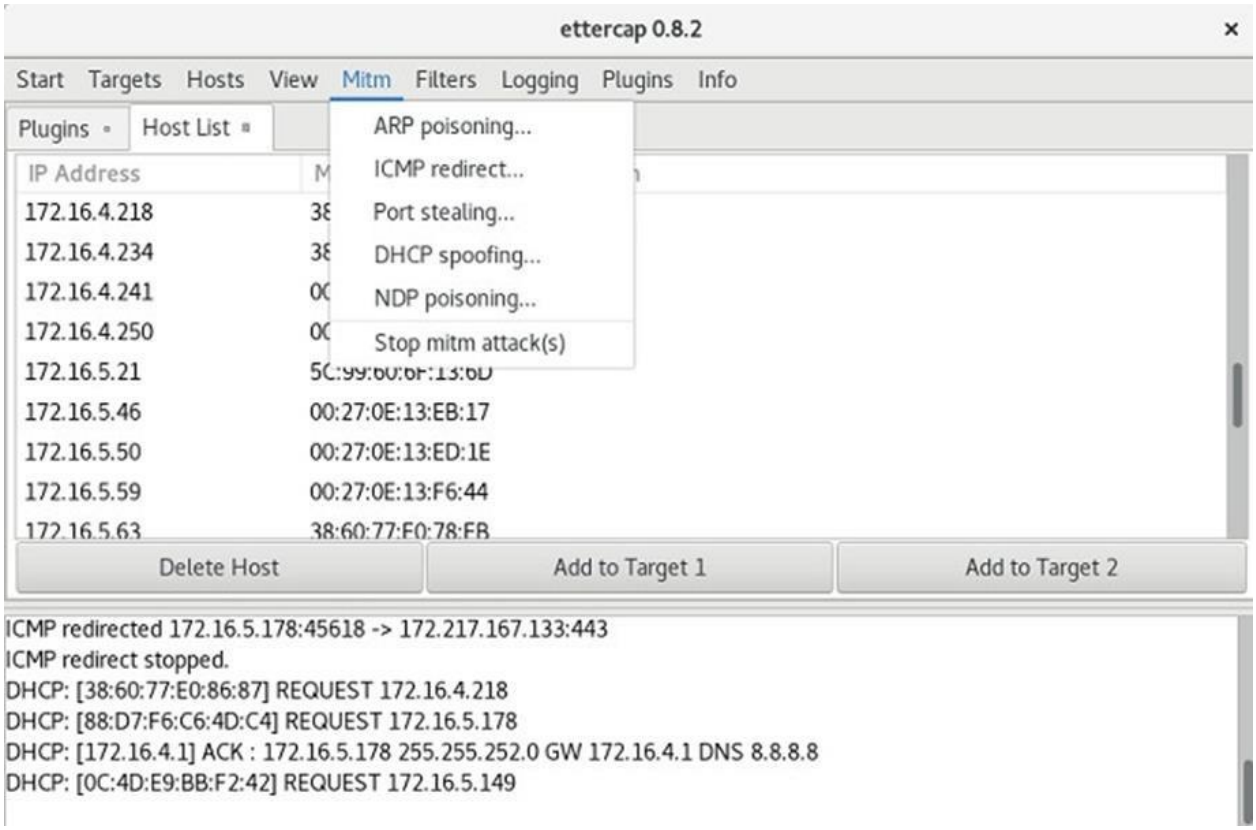
Algorithm:

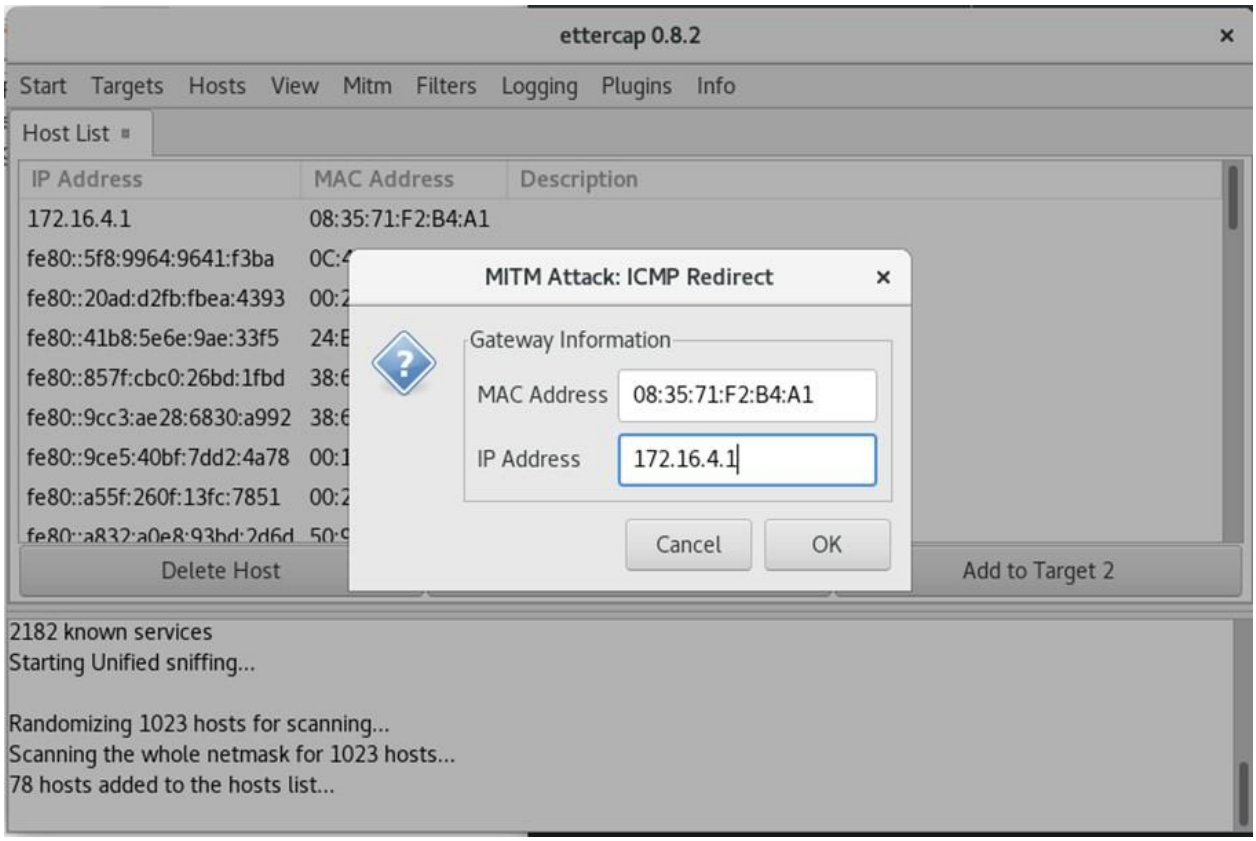
1.Install ettercap if not done already using the command- dnf install ettercap
2.Open etter.conf file and change the values of ec_uid and ec_gid to zero from default. vi /etc/ettercap/etter.conf
3.Next start ettercap in GTK ettercap -G
4.Click sniff, followed by unified sniffing.
5.Select the interface 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.

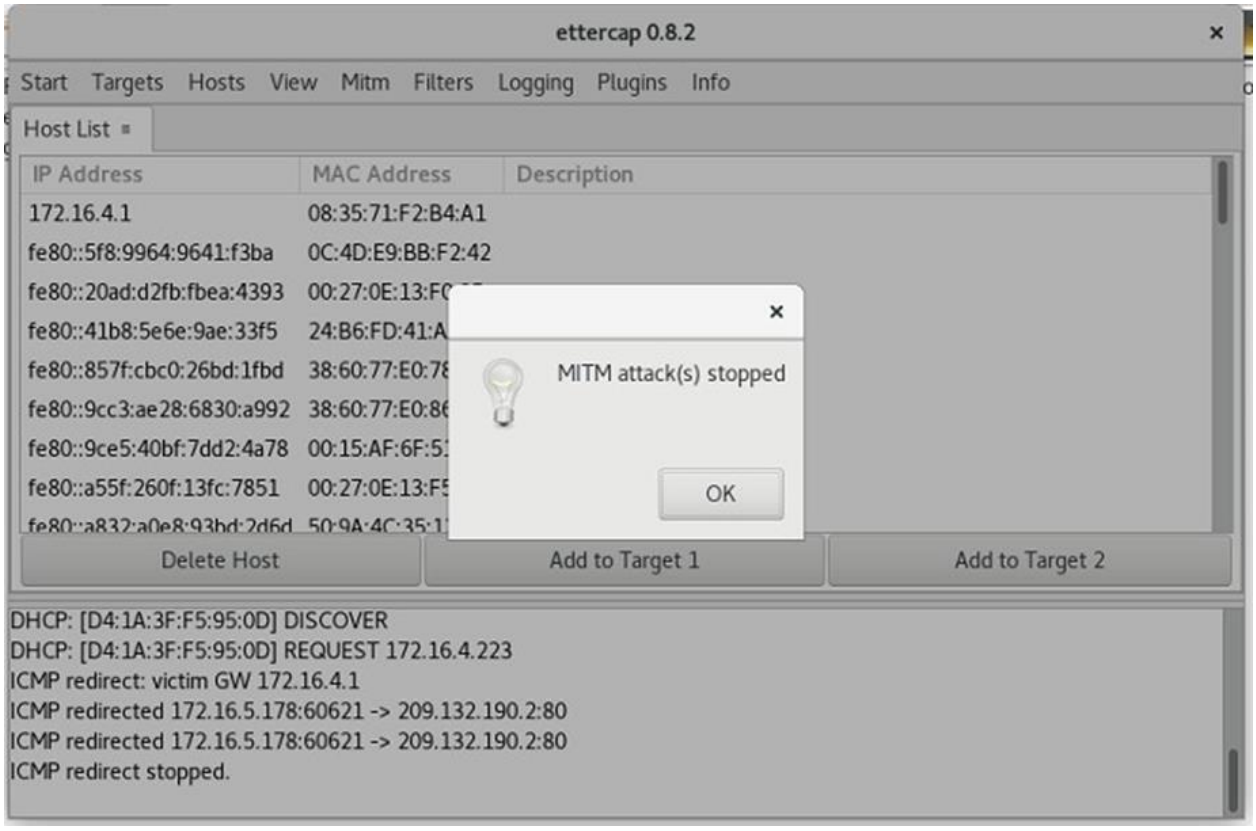
Output:

[root@localhost security lab]# dnf install ettercap
[root@localhost security lab]# vi /etc/ettercap/etter.conf
[root@localhost security lab]# ettercap –G


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Hosts list Ctrl+H
Enable IPv6 scan
Scan for hosts Ctrl+S
Load from file...
Save to file...
Ettercap
DHCP: [E4:46:DA:A7:DC:AD] DISCOVER
DHCP: [E4:46:DA:A7:DC:AD] REQUEST 172.16.5.226
Randomizing 1023 hosts for scanning...
Scanning the whole netmask for 1023 hosts...
74 hosts added to the hosts list...


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


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List
IP Address MAC Address Description
172.16.4.1 08:35:71:F2:B4:A1
fe80::5f8:9964:9641:f3ba
fe80::20ad:d2fb:fbea:4393
fe80::41b8:5e6e:9ae:33f5
fe80::857f:cbc0:26bd:1fbd
fe80::9cc3:ae28:6830:a992
fe80::9ce5:40bf:7dd2:4a78
fe80::a55f:260f:13fc:7851
MITM Attack: ICMP Redirect
Gateway Information
MAC Address 08:35:71:F2:B4:A1
IP Address 172.16.4.1
Cancel OK
Delete Host
Add to Target 2
2182 known services
Starting Unified sniffing...
Randomizing 1023 hosts for scanning...
Scanning the whole netmask for 1023 hosts...
78 hosts added to the hosts list...


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List
IP Address MAC Address Description
172.16.4.1 08:35:71:F2:B4:A1
fe80::5f8:9964:9641:f3ba 0C:4D:E9:BB:F2:42
fe80::20ad:d2fb:fbea:4393
fe80::41b8:5e6e:9ae:33f5 24:B6:FD:41:A
fe80::857f:cbc0:26bd:1fbd 38:60:77:E0:78
fe80::9cc3:ae28:6830:a992 38:60:77:E0:86
fe80::9ce5:40bf:7dd2:4a78 00:15:AF:6F:51
fe80::a55f:260f:13fc:7851 00:27:0E:13:F5
MITM attack(s) stopped
OK
Delete Host
Add to Target 1
Add to Target 2
DHCP: [D4:1A:3F:F5:95:0D] DISCOVER
DHCP: [D4:1A:3F:F5:95:0D] REQUEST 172.16.4.223
ICMP redirect: victim GW 172.16.4.1
ICMP redirected 172.16.5.178:60621 -> 209.132.190.2:80
ICMP redirected 172.16.5.178:60621 -> 209.132.190.2:80
ICMP redirect stopped.

Result: