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

MITM ATTACK WITH ETTERCAP

Ettercap Tool:

Ettercap is a well-known open-source tool used for conducting man-in-the-middle attacks on a local area network (LAN). It essentially functions as a network eavesdropper, allowing you to intercept traffic flowing between devices on the network.

- **Man-in-the-Middle Attacks:** By manipulating ARP (Address Resolution Protocol) Ettercap can position itself as an intermediary between two communicating devices. This allows it to intercept and potentially alter data flowing between them.

Ettercap's capabilities:

- **Packet Sniffing:** Ettercap can put your network interface in promiscuous mode, enabling it to capture all network traffic on the LAN segment, not just traffic directed to your device.
- **Man-in-the-Middle Attacks:** By manipulating ARP (Address Resolution Protocol) Ettercap can position itself as an intermediary between two communicating devices. This allows it to intercept and potentially alter data flowing between them.
- **Protocol Analysis:** Ettercap can dissect and analyze various network protocols, including some encrypted ones. This provides valuable insights into network communication patterns.
- **Data Injection and Filtering:** Ettercap can inject data packets into ongoing connections or filter out unwanted packets, enabling activities like modifying data streams.
- **Multiple Sniffing Modes:** Ettercap offers various sniffing modes, like IP-based, MAC-based, and ARP-based, catering to different network scenarios.

Ettercap is a powerful tool and should be used with caution. While it's valuable for ethical hackers and penetration testers to assess network security, using it for malicious purposes is illegal.

- Ettercap offers both a graphical user interface (GUI) and a command-line interface (CLI) for user convenience.
- Ettercap has plugin support, allowing you to extend its functionalities.

Conceptual Overview

The Vulnerability: ICMP (Internet Control Message Protocol) redirect messages are designed to inform a host that there is a better, more direct route to a particular destination. A malicious actor can send forged ICMP redirect messages to a target host, tricking it into routing its traffic through the attacker's machine.

The Attack:

- The attacker positions themselves on the network (or spoofs their IP address).
- The attacker observes traffic between the target host and a gateway (router).
- The attacker crafts and sends a forged ICMP redirect message to the target host. This message claims that the attacker's machine is the optimal route to the destination the target is trying to reach.
- The target host, believing the ICMP redirect, updates its routing table and starts sending traffic destined for the original target to the attacker's machine.
- The attacker can now intercept, modify, or forward this traffic, effectively becoming the "man in the middle."

Ettercap's Role (Hypothetically): Ettercap could be used to craft and send these forged ICMP redirect messages.

Aim:

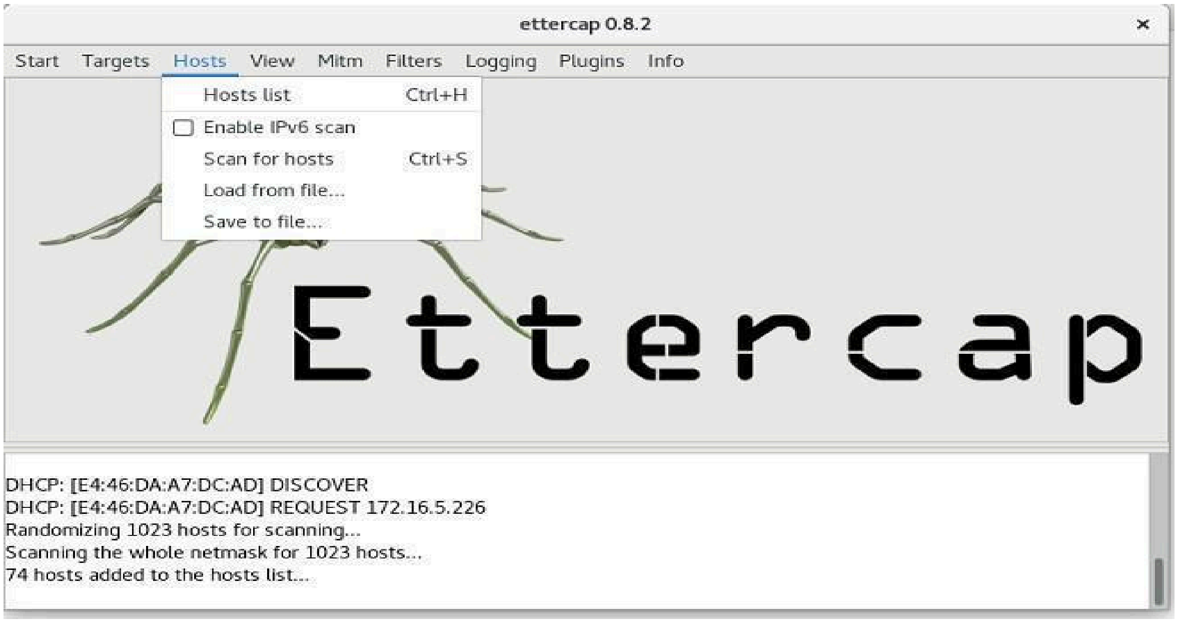
To initiate a MITM attack using ICMP redirect with Ettercap tool.

Algorithm:

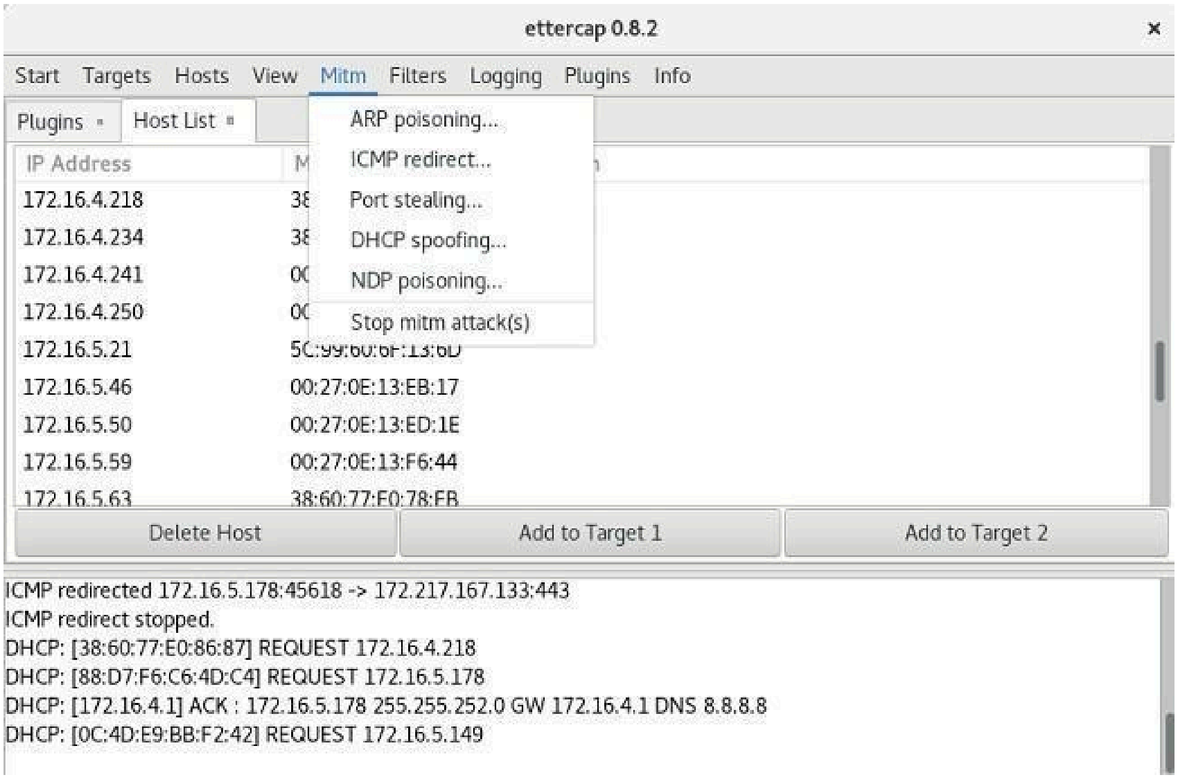
1. Install ettercap if not done already using the
   command- dnf install ettercap
2. Open etter.conf file and change the values of ec_uid and ec_gid to zero from
   default. vi /etc/ettercap/etter.conf
3. Next start ettercap in
   GTK ettercap -G
4. Click sniff, followed by unified sniffing.
5. Select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

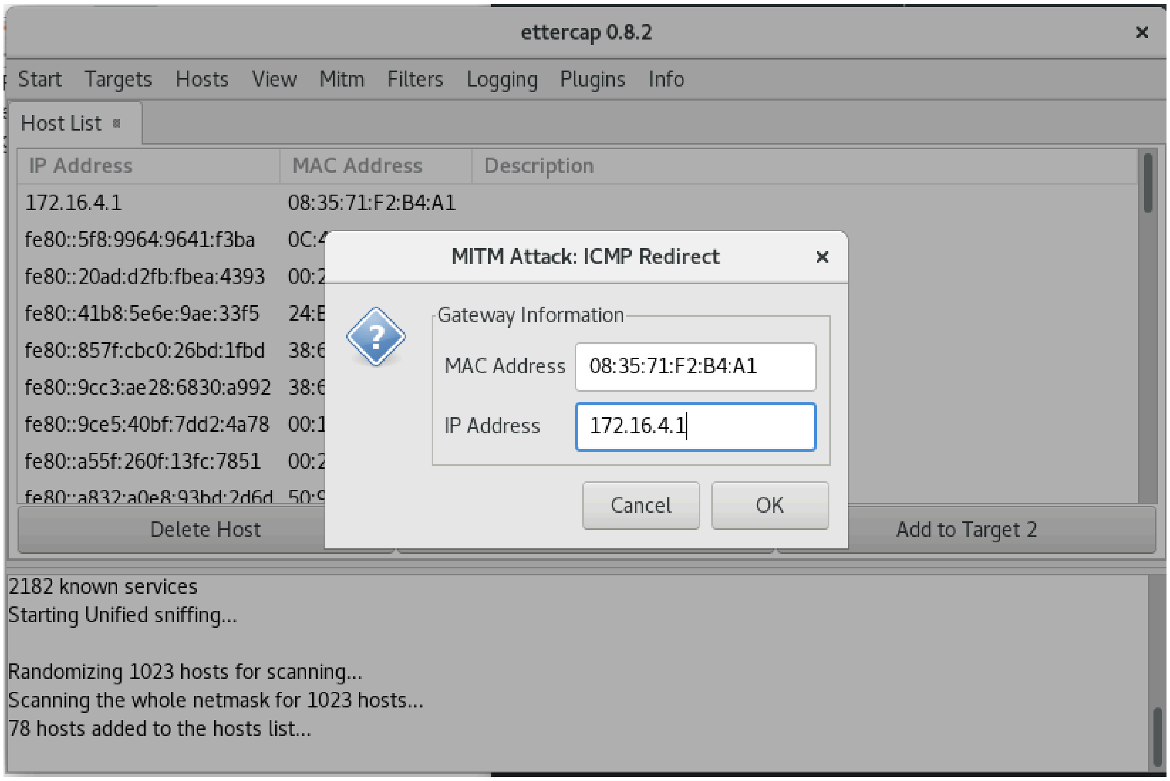


```
DHCP: [E4:46:DA:A7:DC:AD] DISCOVER
DHCP: [E4:46:DA:A7:DC:AD] REQUEST 172.16.5.226
Randomizing 1023 hosts for scanning...
Scanning the whole netmask for 1023 hosts...
74 hosts added to the hosts list...
```



IP Address	M
172.16.4.218	38
172.16.4.234	38
172.16.4.241	00
172.16.4.250	00
172.16.5.21	5C:99:60:6F:13:6D
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
172.16.5.63	38:60:77:E0:78:EB

```
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
```



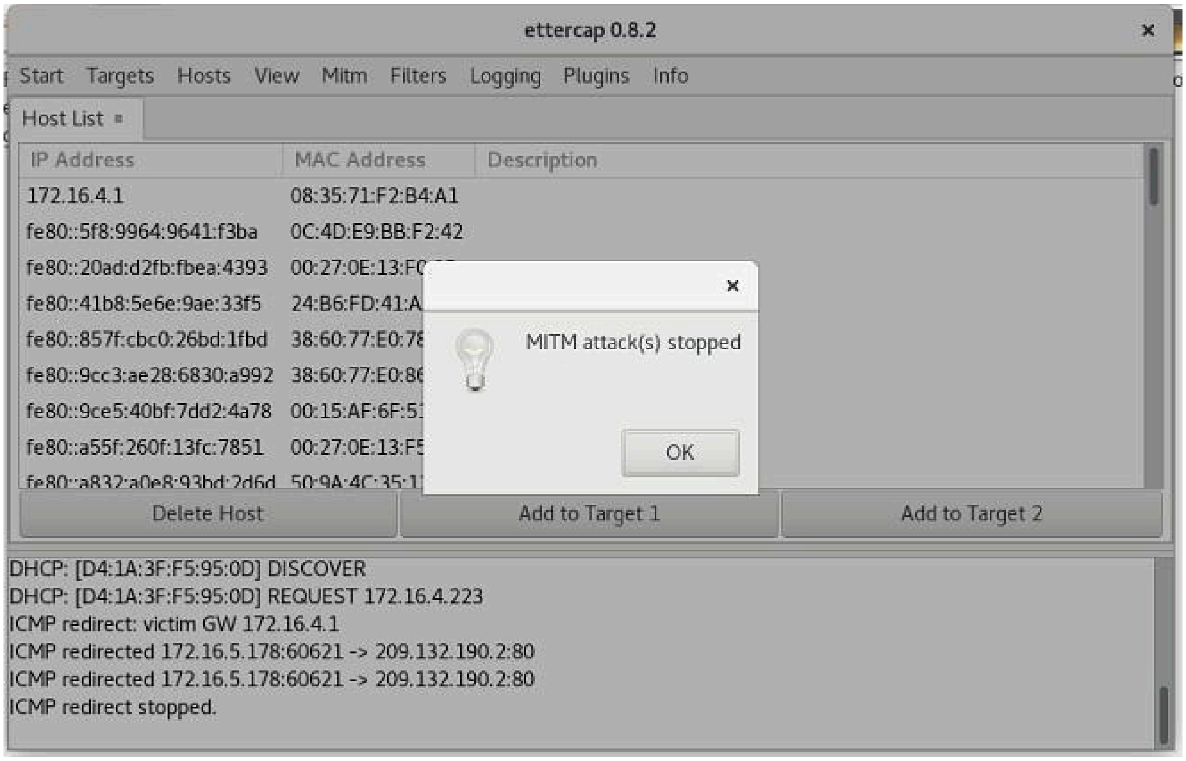
IP Address	MAC Address	Description
172.16.4.1	08:35:71:F2:B4:A1	
fe80::5f8:9964:9641:f3ba	0C:4	
fe80::20ad:d2fb:fbea:4393	00:2	
fe80::41b8:5e6e:9ae:33f5	24:E	
fe80::857f:cbc0:26bd:1fbd	38:6	
fe80::9cc3:ae28:6830:a992	38:6	
fe80::9ce5:40bf:7dd2:4a78	00:1	
fe80::a55f:260f:13fc:7851	00:2	
fe80::a832:a0e8:93bd:2d6d	50:9	

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

IP Address: 172.16.4.1

```
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...
```



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	00:27:0E:13:FC	
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:E0:8E	
fe80::9ce5:40bf:7dd2:4a78	00:15:AF:6F:5	
fe80::a55f:260f:13fc:7851	00:27:0E:13:F5	
fe80::a832:a0e8:93bd:2d6d	50:9A:4C:35:1	

MITM attack(s) stopped

```
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.
```