Ettercap: MITM Attack

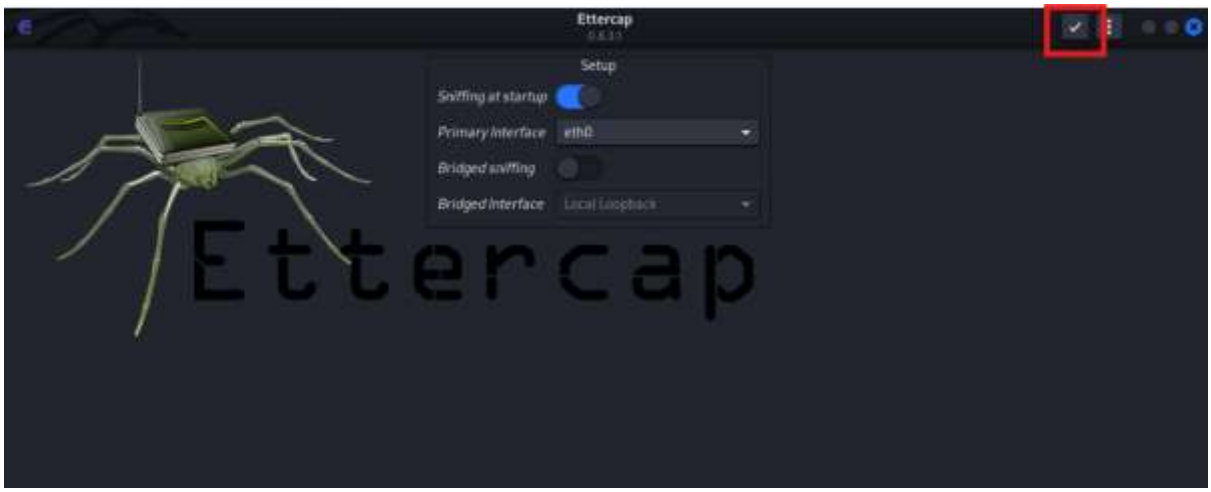
A Man-in-the-Middle (MITM) attack is a cyberattack where a malicious actor intercepts and potentially alters communication between two parties without their knowledge. By positioning themselves between the sender and receiver, the attacker can eavesdrop, steal sensitive information, or inject malicious content into the communication stream. Common techniques include spoofing Wi-Fi networks, DNS spoofing, HTTPS spoofing, and session hijacking. To prevent such attacks, it is essential to use strong encryption protocols like HTTPS and SSL/TLS, verify the legitimacy of certificates, avoid using public Wi-Fi without a VPN, enable two-factor authentication, and keep software updated to protect against vulnerabilities. These measures help ensure the security and integrity of digital communications.

Ettercap is a comprehensive suite for conducting Man-in-the-Middle (MITM) attacks on a network. It allows attackers to intercept, monitor, and manipulate network traffic between two parties, making it a powerful tool for both network security professionals and malicious actors. Ettercap can perform a variety of attacks, including ARP poisoning, DNS spoofing, and HTTP/HTTPS manipulation, enabling attackers to capture sensitive data such as passwords and session cookies. It features a user-friendly interface, which makes it accessible even to those with limited technical expertise. While Ettercap is often used for legitimate purposes such as

network analysis and security testing, its capabilities make it a significant threat in the hands of attackers aiming to exploit vulnerabilities in network communication.

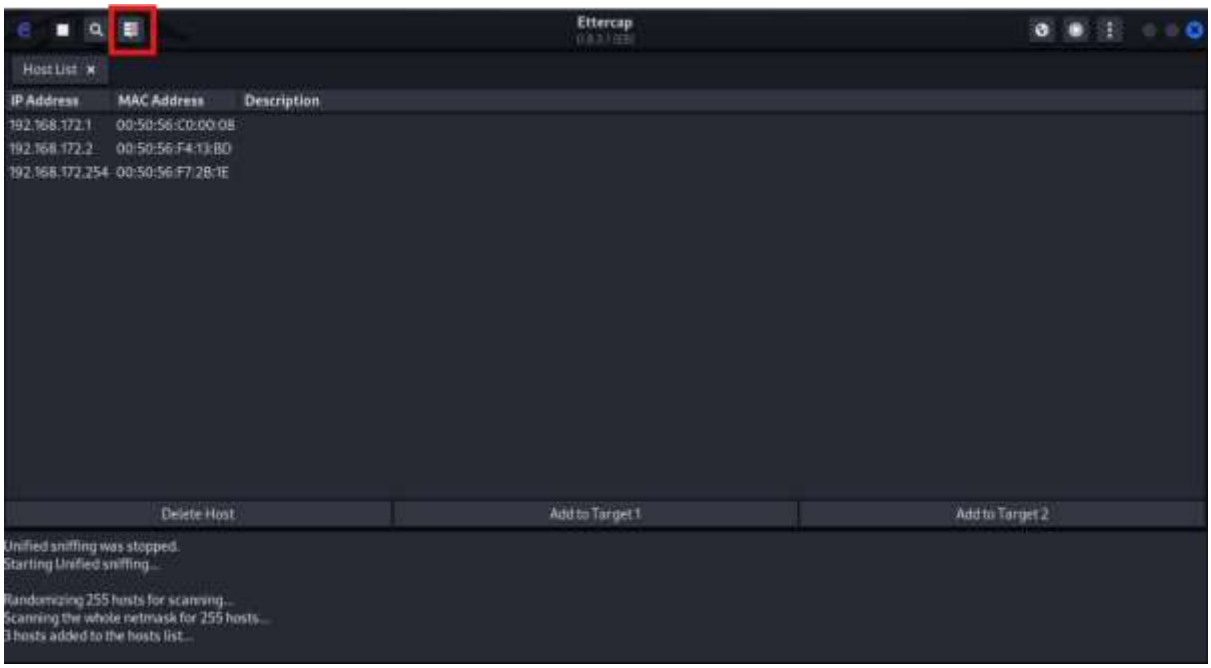
Examples: -

1. Firstly, open Ettercap Graphical and start the sniffing by clicking on Accept button from the top right corner.

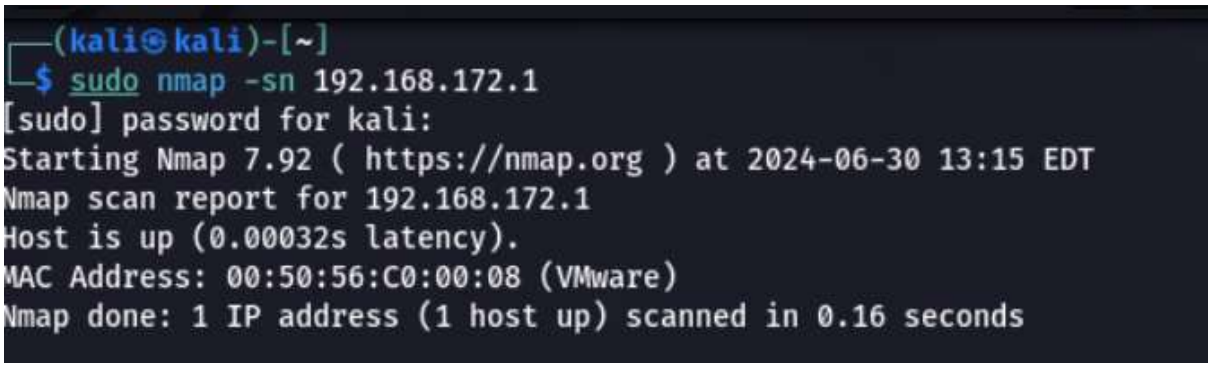


2. Click on the Scan for host button on the top left corner next to the Host List button to scan for hosts.

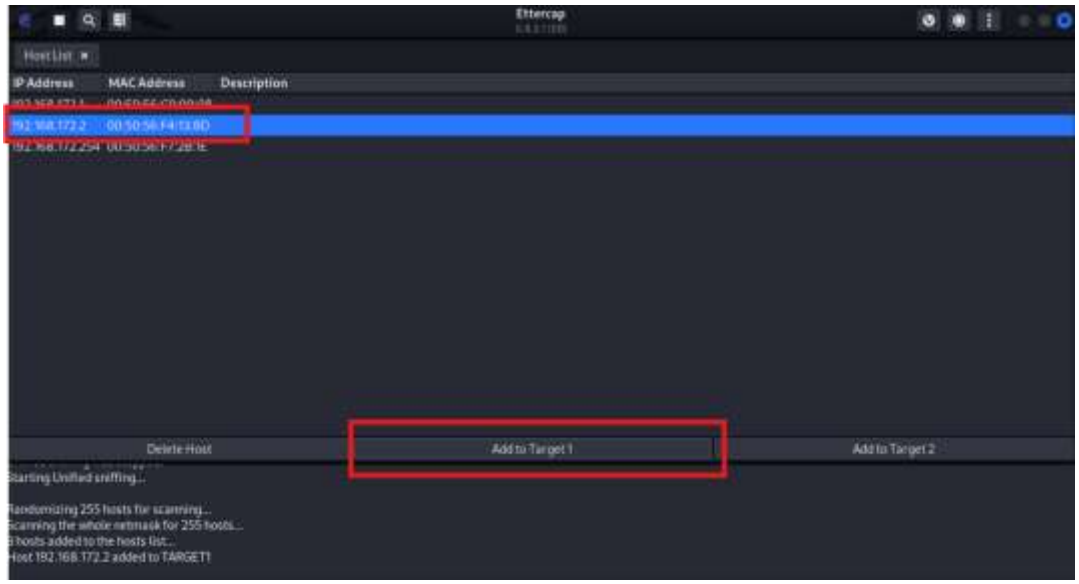
3. Now open a terminal and type sudo nmap -sn 192.168.172.1 to find out the known target on the network.



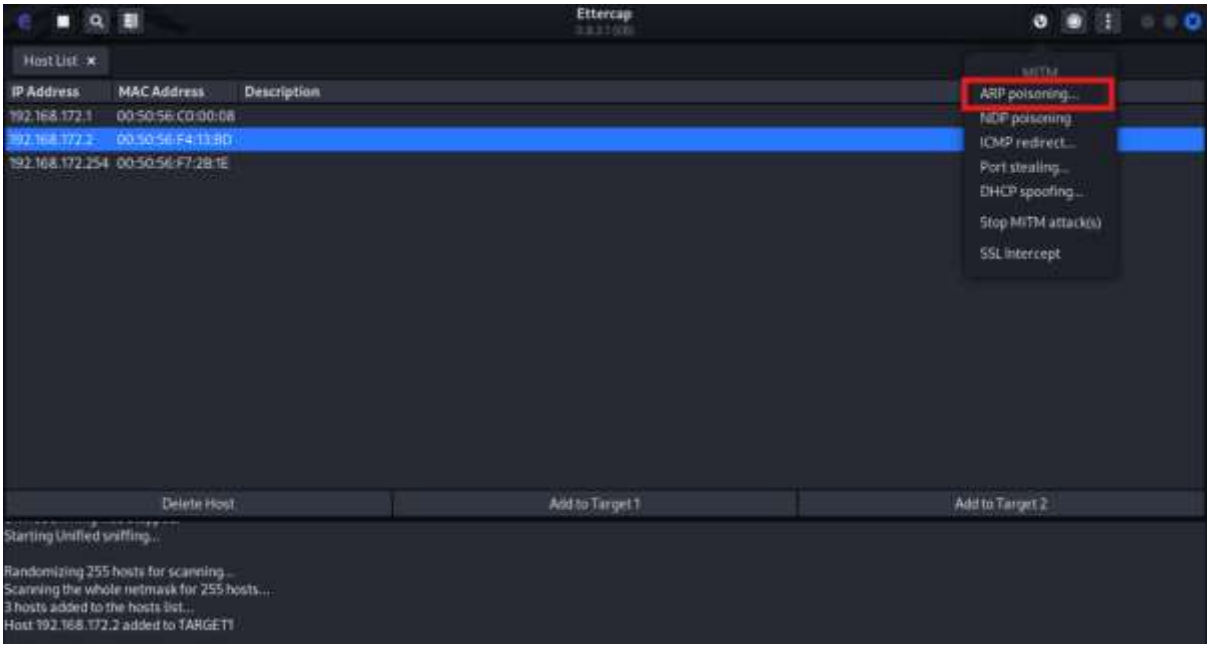
4. Now open a terminal and type sudo nmap -sn 192.168.172.1 to find out the known target on the network.



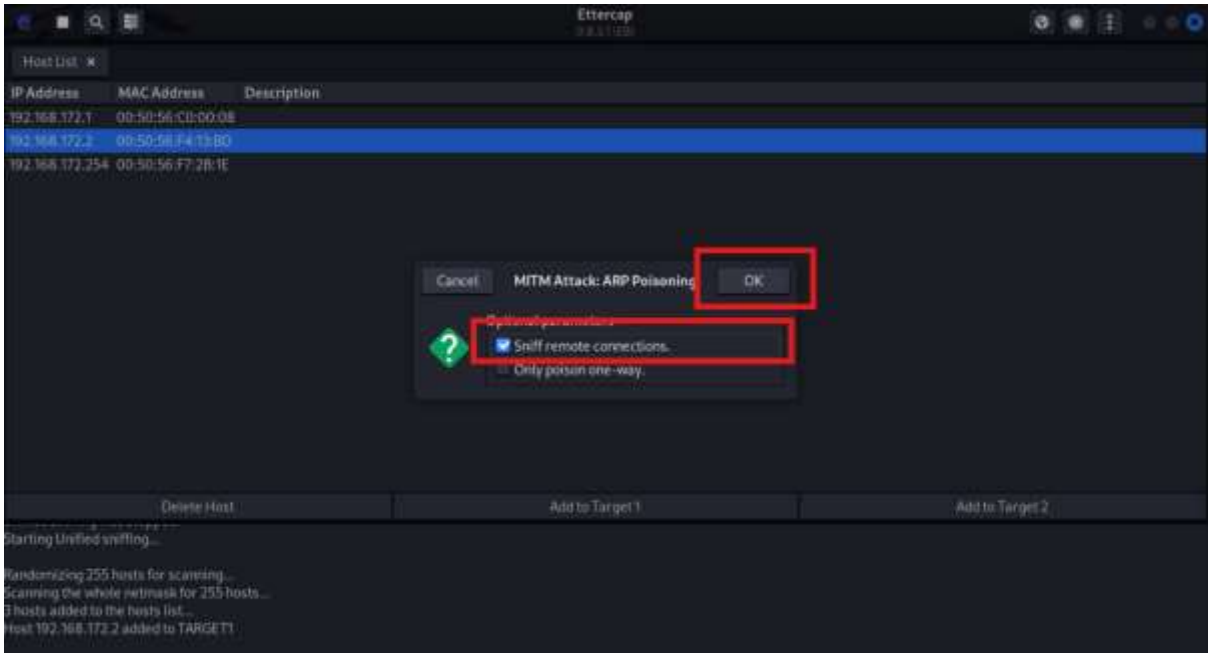
5. Now again get back into Ettercap, then select a host from the Host List and click on Add to Target 1. The host selected in this example is with the IP address 192.168.172.2



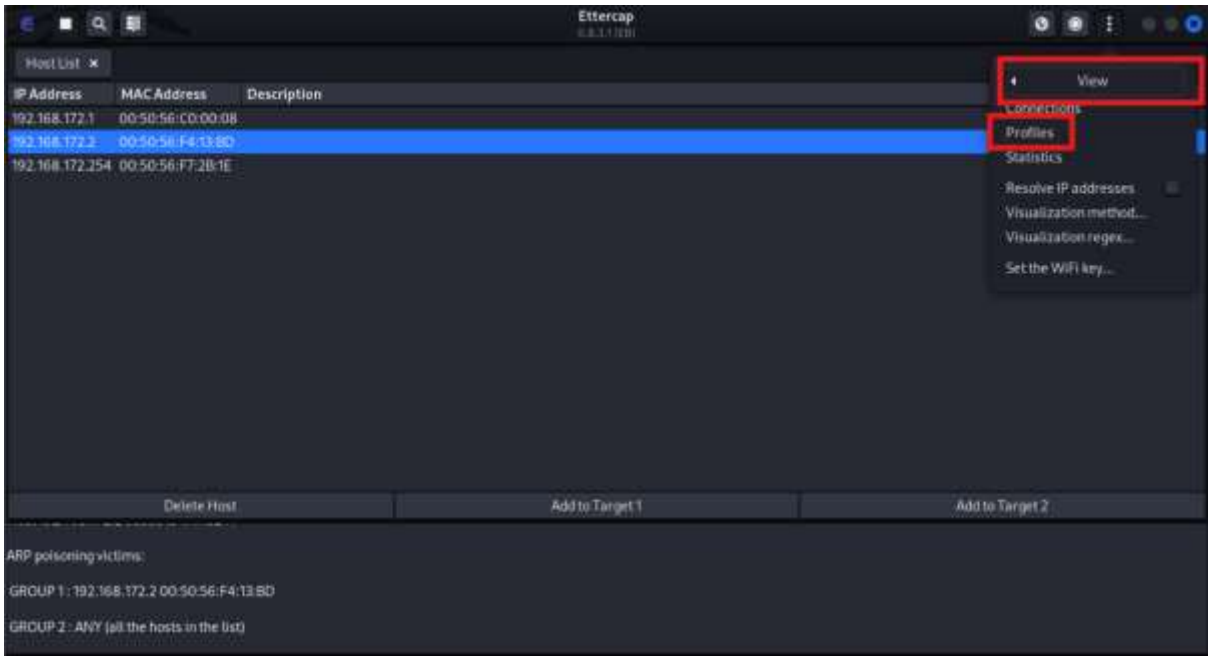
6. After the host has been added to the target, click on the MITM menu button in the top right corner, then select ARP poisoning .



7. Click on OK for the pop-up window to allow the Ettercap application to perform ARP poisoning for MITM attack.



8. In View, click on Profiles to be prompted with this tab.



9. The details of each IP address such as the hostname and the country will then be loaded out .Any traffics captured or actions that has been performed by the user can all be seen here.