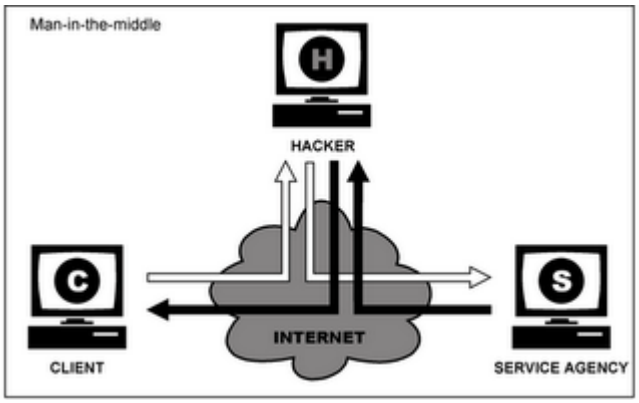
Using Ettercap for ARP Poisoning

Ettercap is a suite for man in the middle attacks on **LAN** (local area network). It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols (even ciphered ones) and includes many features for network and host analysis. In this tutorial i will explain how to sniff (user names, passwords) in **LAN** using Ettercap

Man-in-The-Middle Attack

The man-in-the-middle attack (also known as a bucket-brigade attack and abbreviated MITM) is a form of active **eavesdropping** in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the **attacker**.



There are several kinds of man-in-the-middle attacks that we can perform, but in this tutorial we will see attacks based on the ARP protocol.

ARP Poisoning

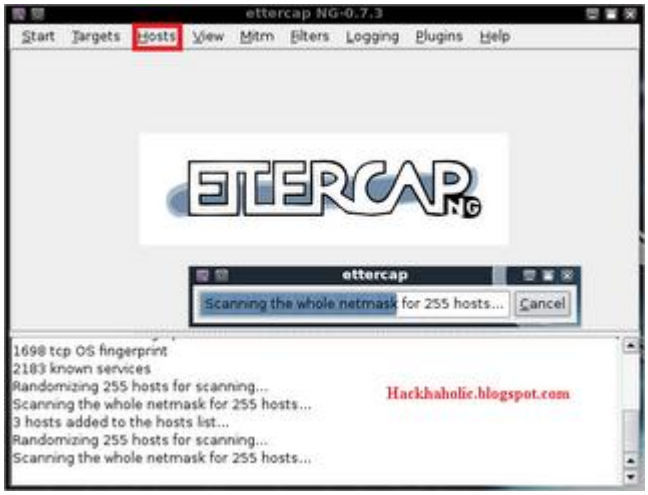
Address Resolution Protocol (ARP) spoofing, also known as ARP flooding, ARP poisoning or ARP Poison **Routing (APR),** is a technique used to attack an Ethernet wired or wireless network. ARP Spoofing may allow an attacker to sniff data frames on a local area network **(LAN)**, .

Man-in-The-Middle Attack Using Ettercap

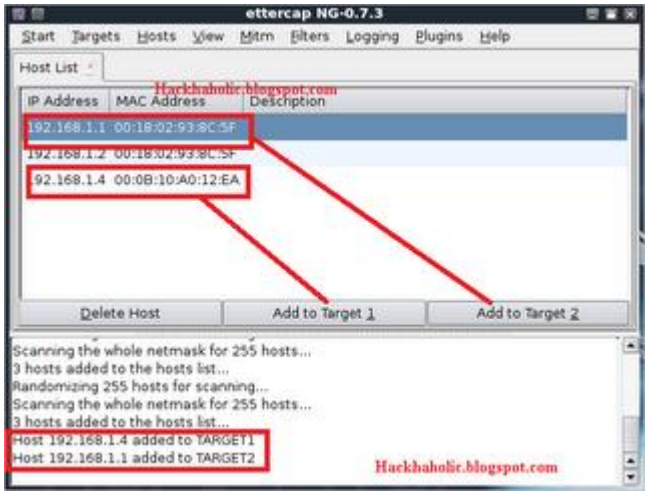
1. First download Ettercap from **http://ettercap.sourceforge.net/download.php**

2. After installation open Ettercap, select **sniff** mode and select your **network interface** as shown

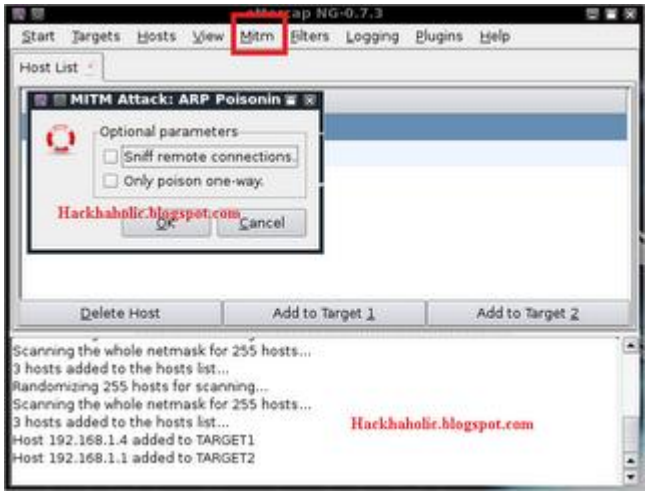
3. Now scan for hosts in your subnet by going to **Hosts ---> scan for hosts**



4. Now open **host list** from **hosts tab** and select the IP address of the **victim** as target 1 and IP address of the **router** as target 2:



5. Now start ARP poisoning by going to **mitm ---> ARP Poisoning**



6. Finally start the sniffer by going to **start ---> start sniffing.** Now if the victim logs into any unencrypted channel it should be possible to capture their user name and password etc.