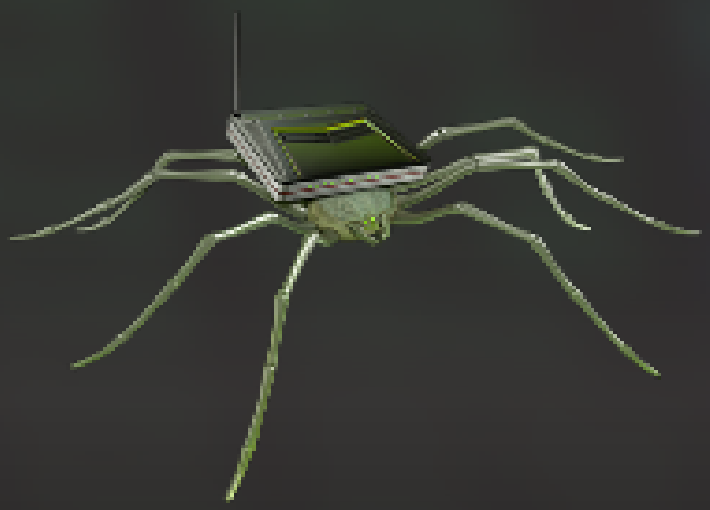
ATAQUE MAN IN THE MIDDLE MEDIANTE ARP Y DNS SPOOFING



SEGURIDAD INFORMÁTICA

JUAN CARLOS NAVIDAD GARCÍA

1. Instalar Ettercap:

Ettercap se instala con el comando:

- **sudo apt-get install ettercap-graphical**

```
jnav@ubuntu:~$ sudo apt-get install ettercap-graphical
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ethtool ettercap-common geoip-database libgeoip1 libluajit-5.1-2
  libluajit-5.1-common libnet1
Suggested packages:
  geoip-bin
The following NEW packages will be installed:
  ethtool ettercap-common ettercap-graphical geoip-database libgeoip1
  libluajit-5.1-2 libluajit-5.1-common libnet1
0 upgraded, 8 newly installed, 0 to remove and 170 not upgraded.
Need to get 4.458 kB of archives.
After this operation, 15,0 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

2. Configurar Ettercap:

Nos iremos al directorio del programa **Ettercap**, que se encuentra en ***/etc/ettercap*** y modificaremos los archivos **etter.conf** y **etter.dns**:

```
jnav@ubuntu:~$ cd /etc/ettercap
jnav@ubuntu:/etc/ettercap$ sudo nano etter.conf
```

```
  GNU nano 4.8                          etter.conf
##############################################################################
#                                                                            #
#  ettercap -- etter.conf -- configuration file                              #
#                                                                            #
#  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.                                       #
#                                                                            #
#                                                                            #
##############################################################################

[privs]
ec_uid = 0              # nobody is the default
ec_gid = 0              # nobody is the default
```

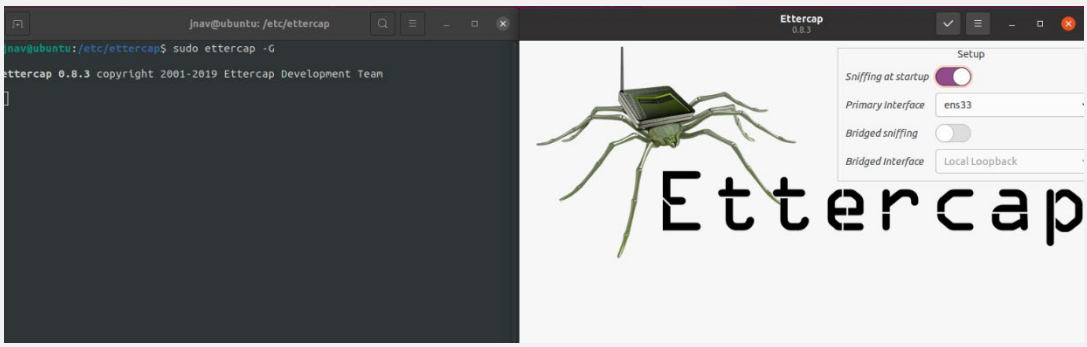
```
jnav@ubuntu:~$ cd /etc/ettercap
jnav@ubuntu:/etc/ettercap$ sudo nano etter.conf
[sudo] password for jnav:
jnav@ubuntu:/etc/ettercap$ sudo nano etter.dns
```

En el archivo **etter.dns** añadiremos la línea *** A <la ip de nuestro servidor>**. Esta línea sirve para que en vez de mostrar cualquier página (se traduce en la línea por el asterisco), se muestre la página que se encuentra en nuestro servidor (por eso nuestra IP que es donde se encuentra Apache)

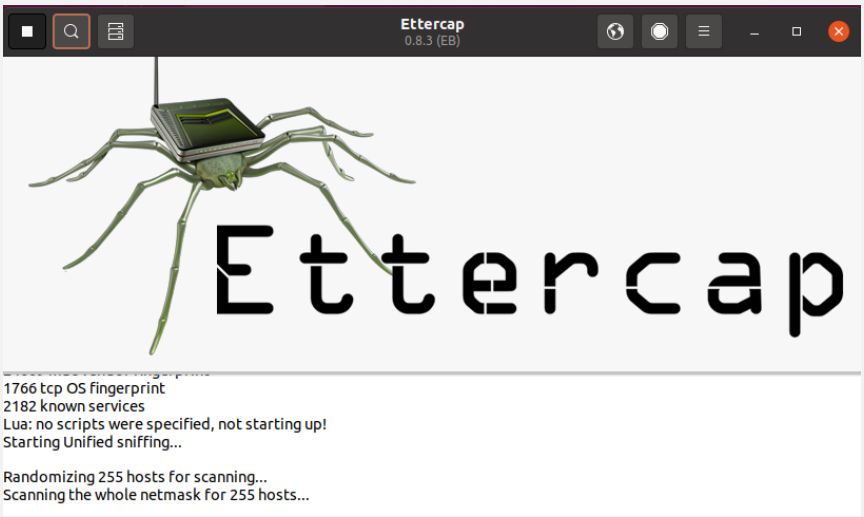
```
  GNU nano 4.8                          etter.dns                          Modified
# This messes up NetBIOS clients using DNS
# resolutions. I.e. Windows/Samba file sharing.
#

LAB-PC*  WINS  127.0.0.1

##############################################
# some service discovery examples

xmpp-server._tcp.jabber.org SRV 192.168.1.10:5269
ldap._udp.mynet.com SRV [2001:db8:c001:beef::1]:389

##############################################
# little example for TXT records
#

naga.org TXT "v=spf1 ip4:192.168.1.2 ip6:2001:db8:d0b1:beef::2 -all"
* A 192.168.1.100
# vim:ts=8:noexpandtab


^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text^T To Spell  ^_ Go To Line
```

3. Iniciar Ettercap:

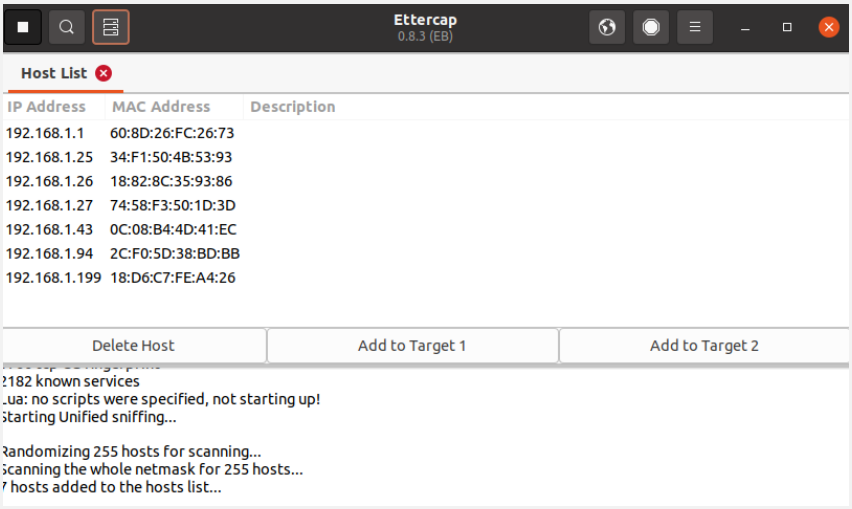
Para iniciar **Ettercap**, lo podemos iniciar desde la misma interfaz gráfica o por terminal de comandos, se utiliza el comando: **sudo ettercap -G**.
Una vez abierto **Ettercap**, pulsamos sobre el **tick** para iniciar el programa:



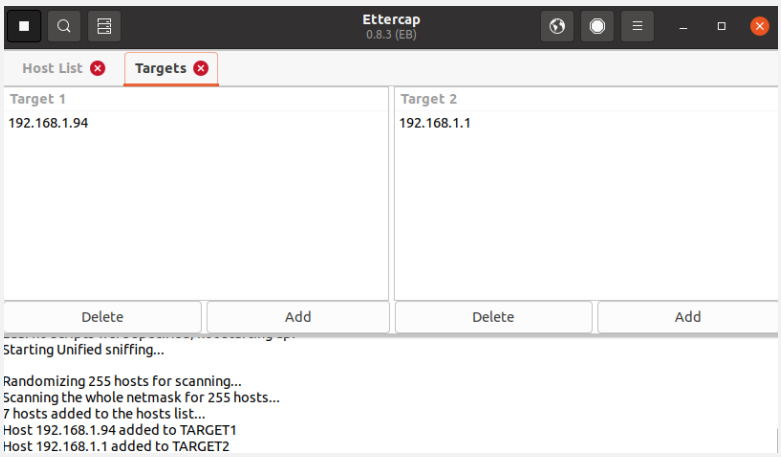
Le daremos a la **lupa** para iniciar la **búsqueda de hosts** en la red:



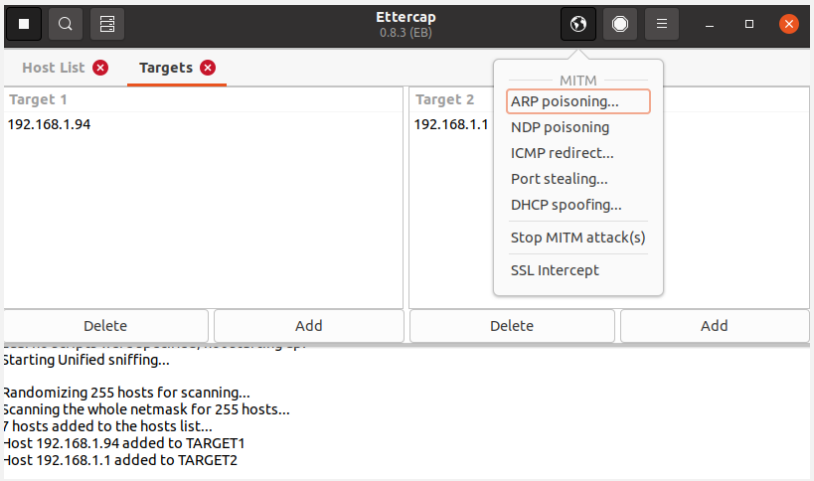
Pulsaremos sobre la **biblioteca** que se encuentra al lado de la **lupa** para que nos salgan los **hosts buscados**:

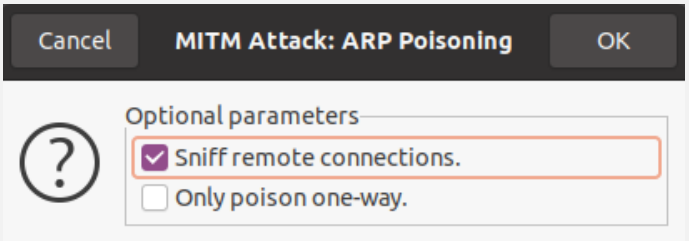


En **target 1** seleccionaremos el equipo con el que vamos a hacer la búsqueda o que queremos atacar y en **target 2** la puerta de enlace de nuestra red.

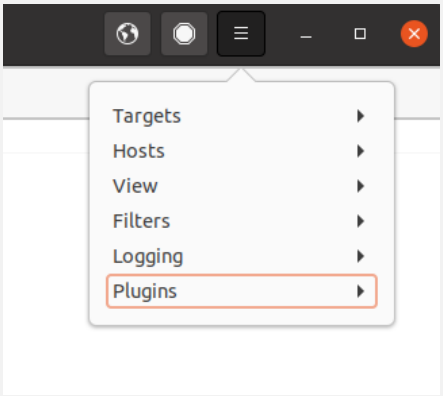


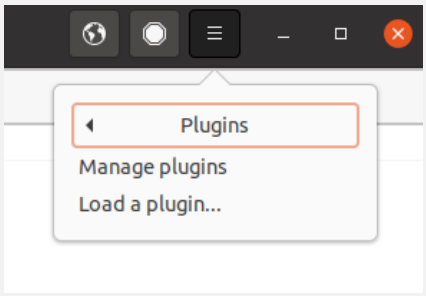
Ahora le daremos a la **bola del mundo** y le daremos a **ARP poisoning** para iniciar el ataque por **ARP spoofing**:

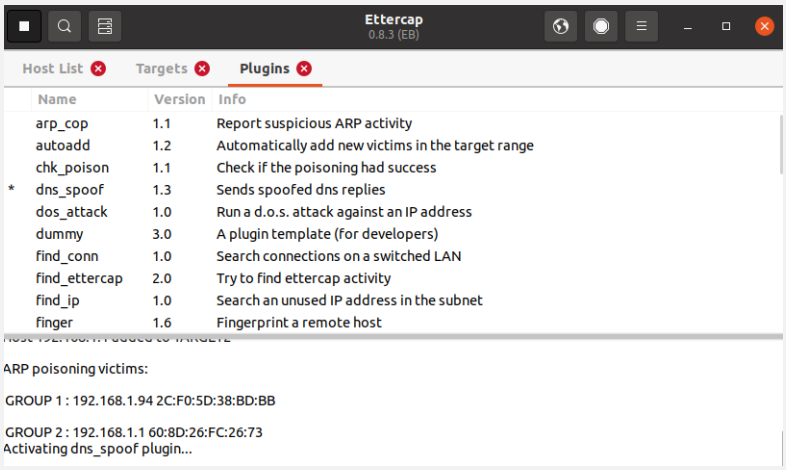




Ahora, le daremos a las **tres rayas horizontales**, le daremos a **plugins** y posteriormente a **manage plugins** para iniciar el **DNS Spoofing**:







Una vez iniciados ambos ataques de **ARP** y **DNS**, nos iremos al equipo que hemos añadido como **target 1**, buscaremos cualquier página como la de **Los Cerros** y nos debería de aparecer la **página principal de Apache**.