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/registrador 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 accesamos 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:

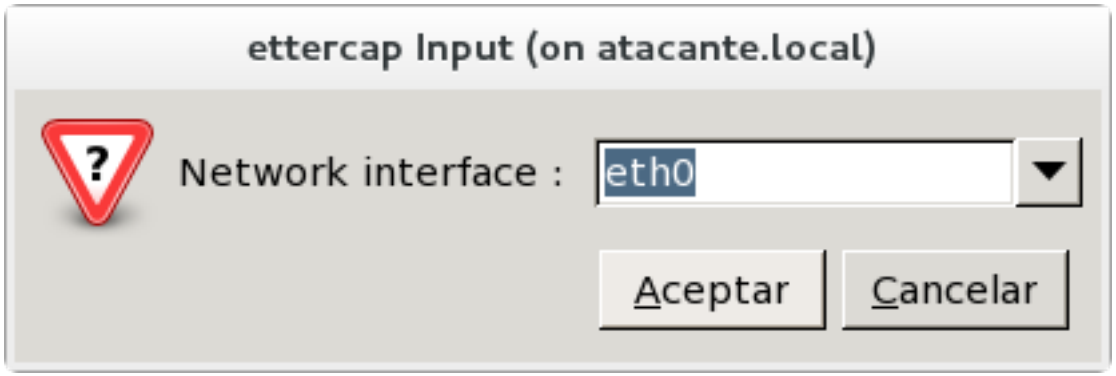
```
# ssh -XYC root@redes1.puceing.edu.
ec -p2232
```

El Envenenamiento

Abrimos etercap: `# ettercap -G`

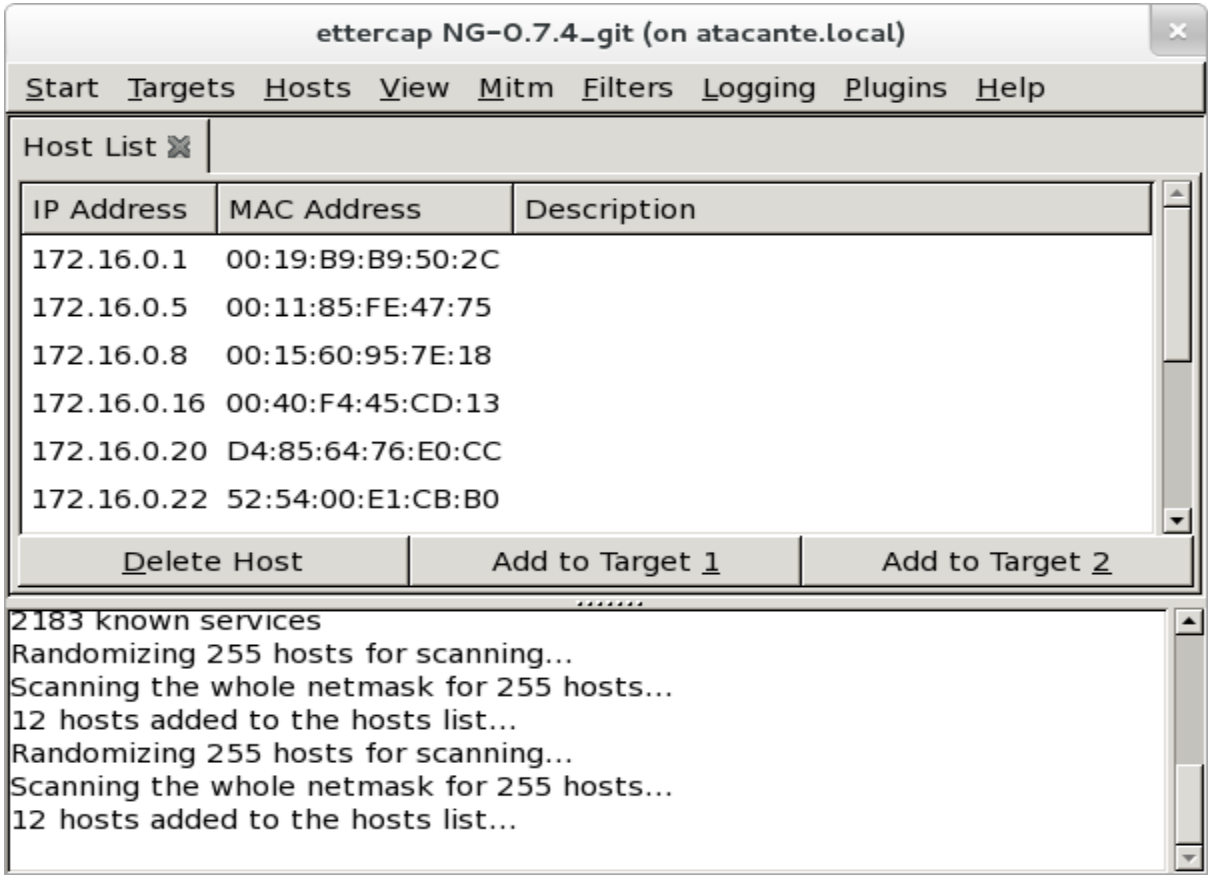
El Envenenamiento

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.



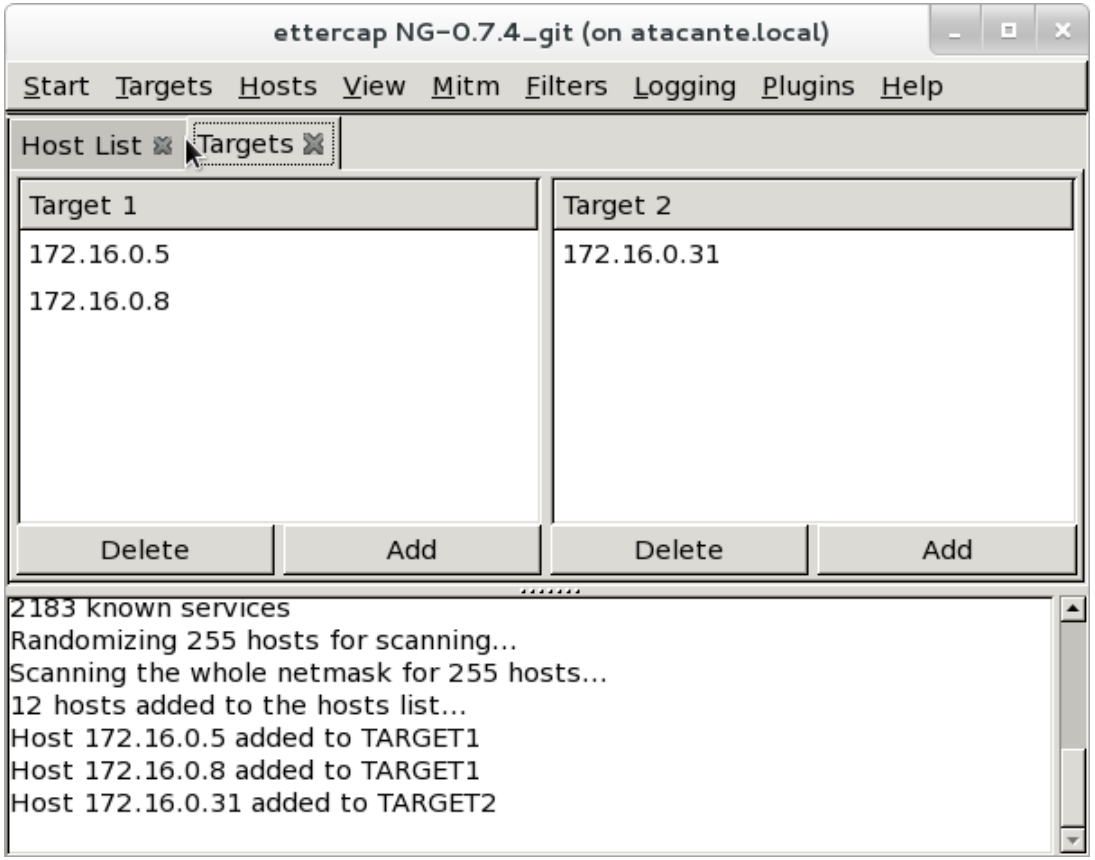
El Envenenamiento

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.

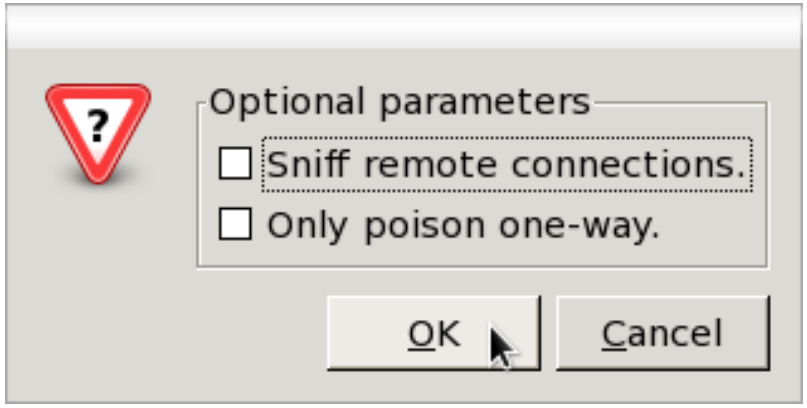
El Envenenamiento

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



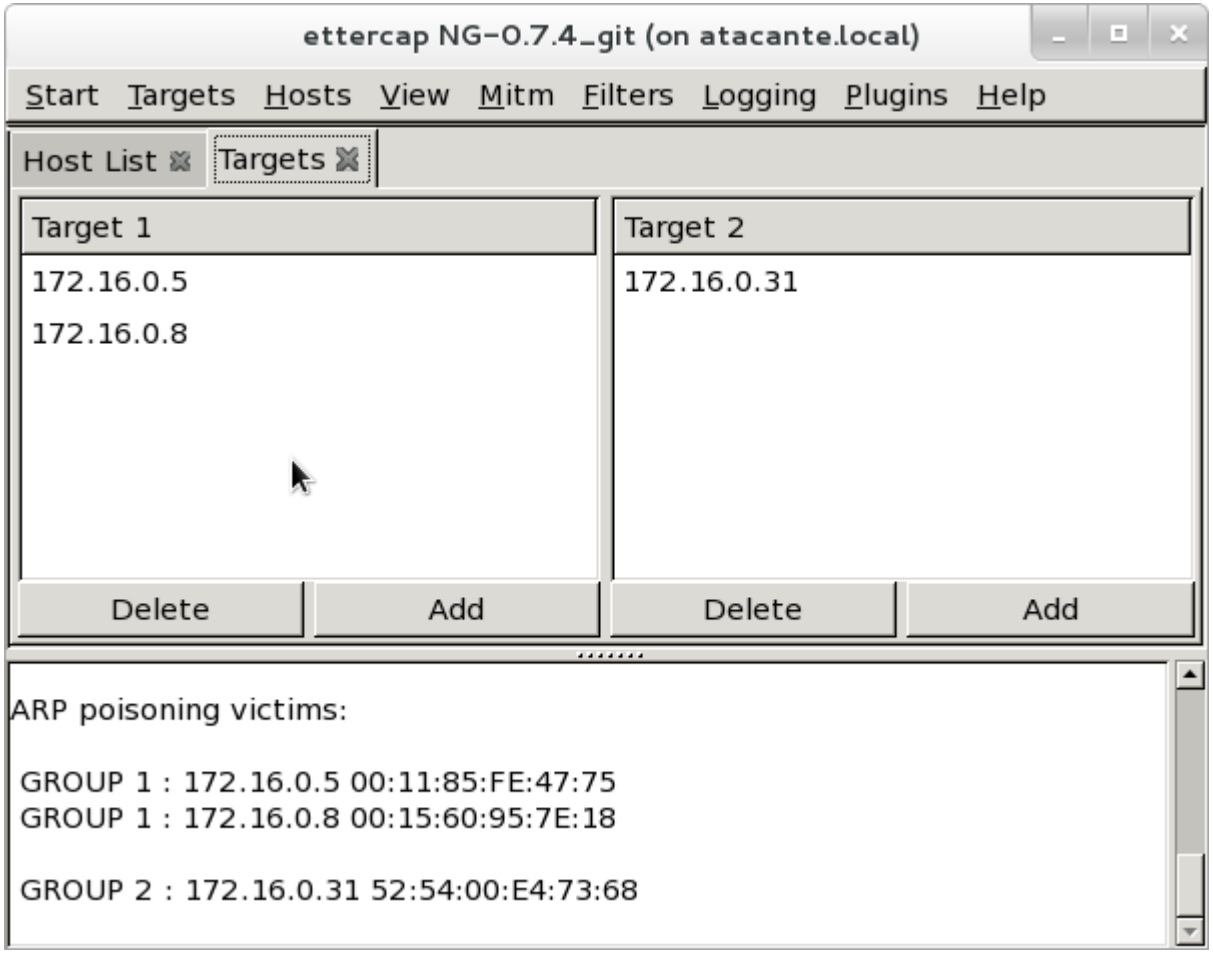
El Envenenamiento

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



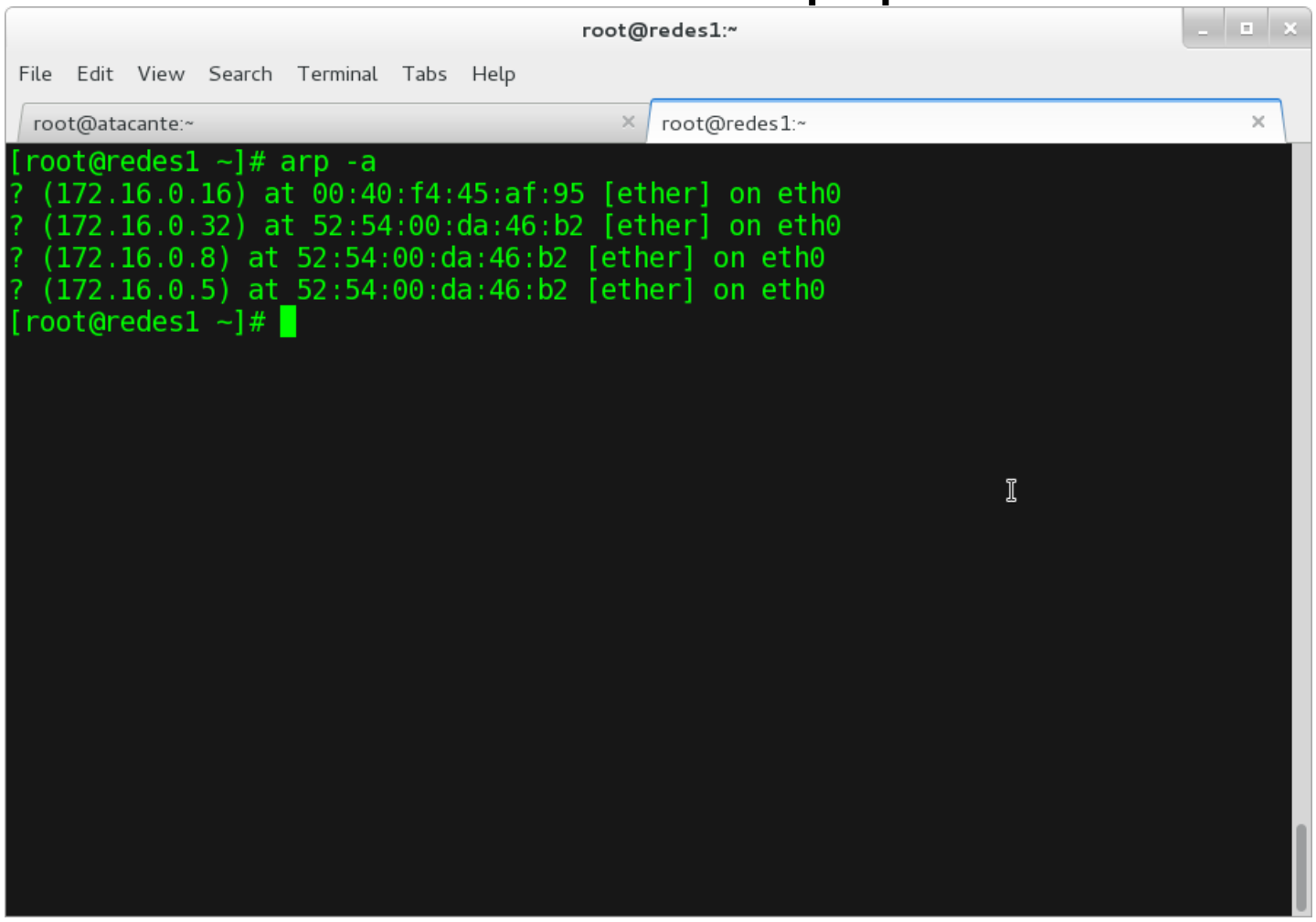
El Envenenamiento

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



El Envenenamiento

Revisamos la tabla ARP del equipo víctima



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.

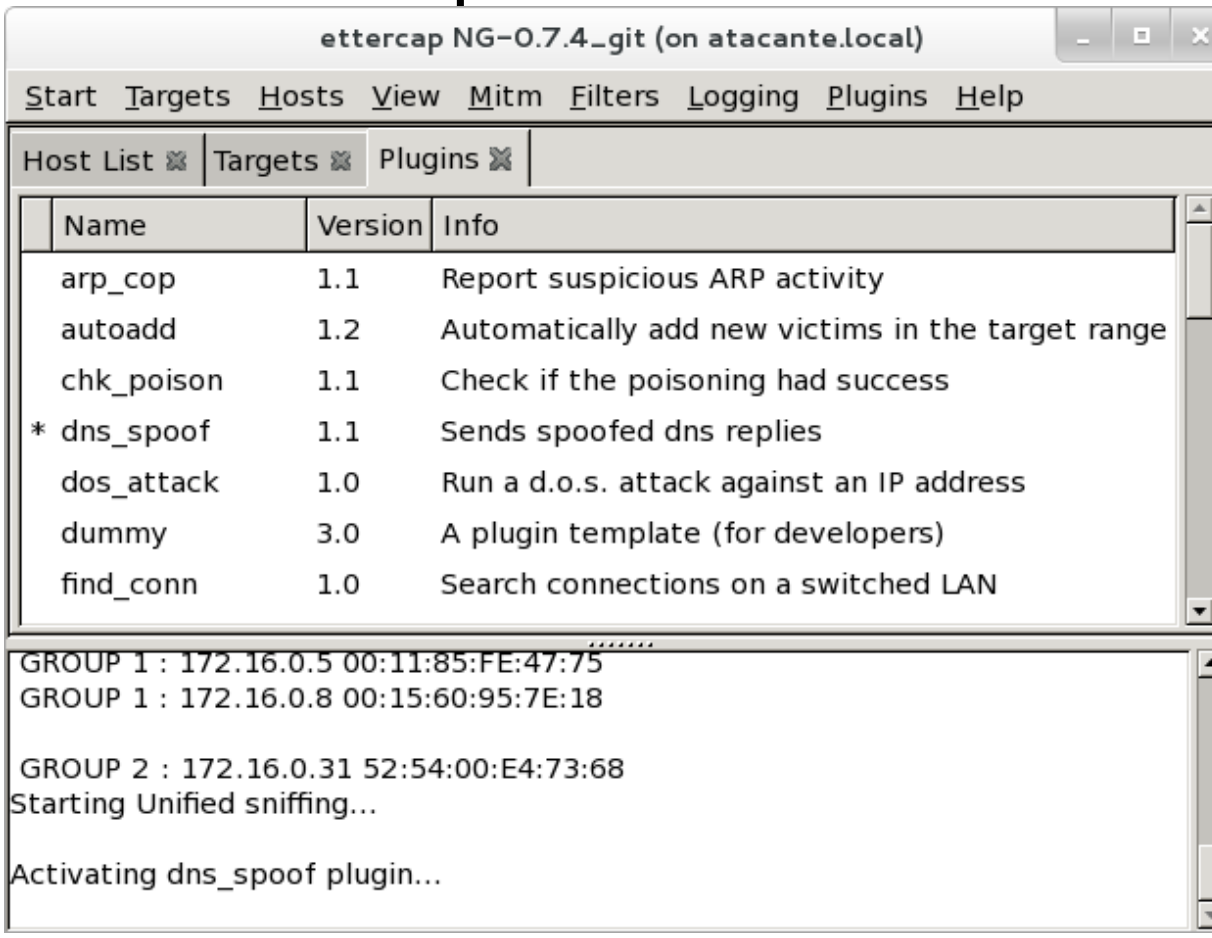
`* A 172.16.0.32`

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.

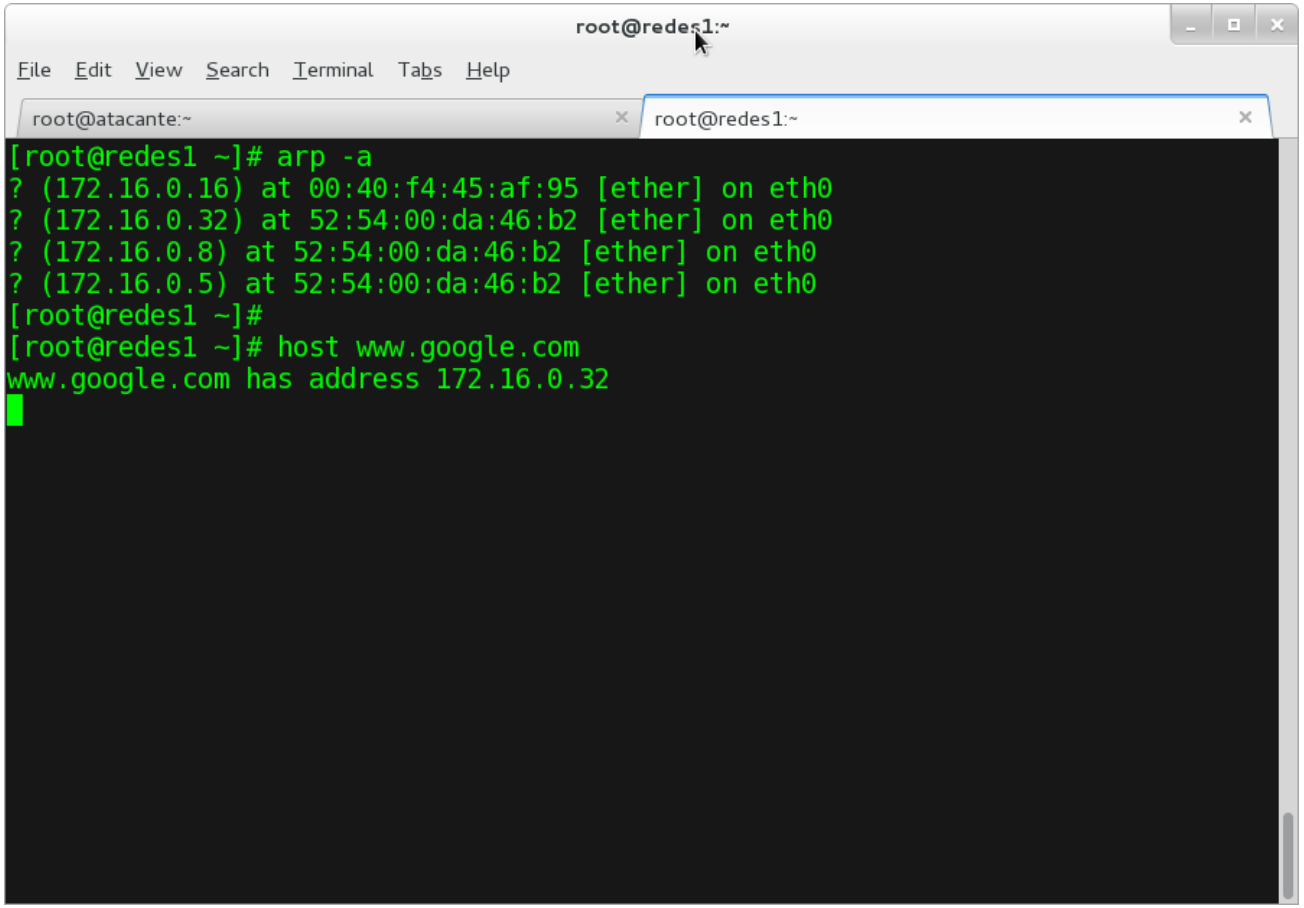
El Envenenamiento

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



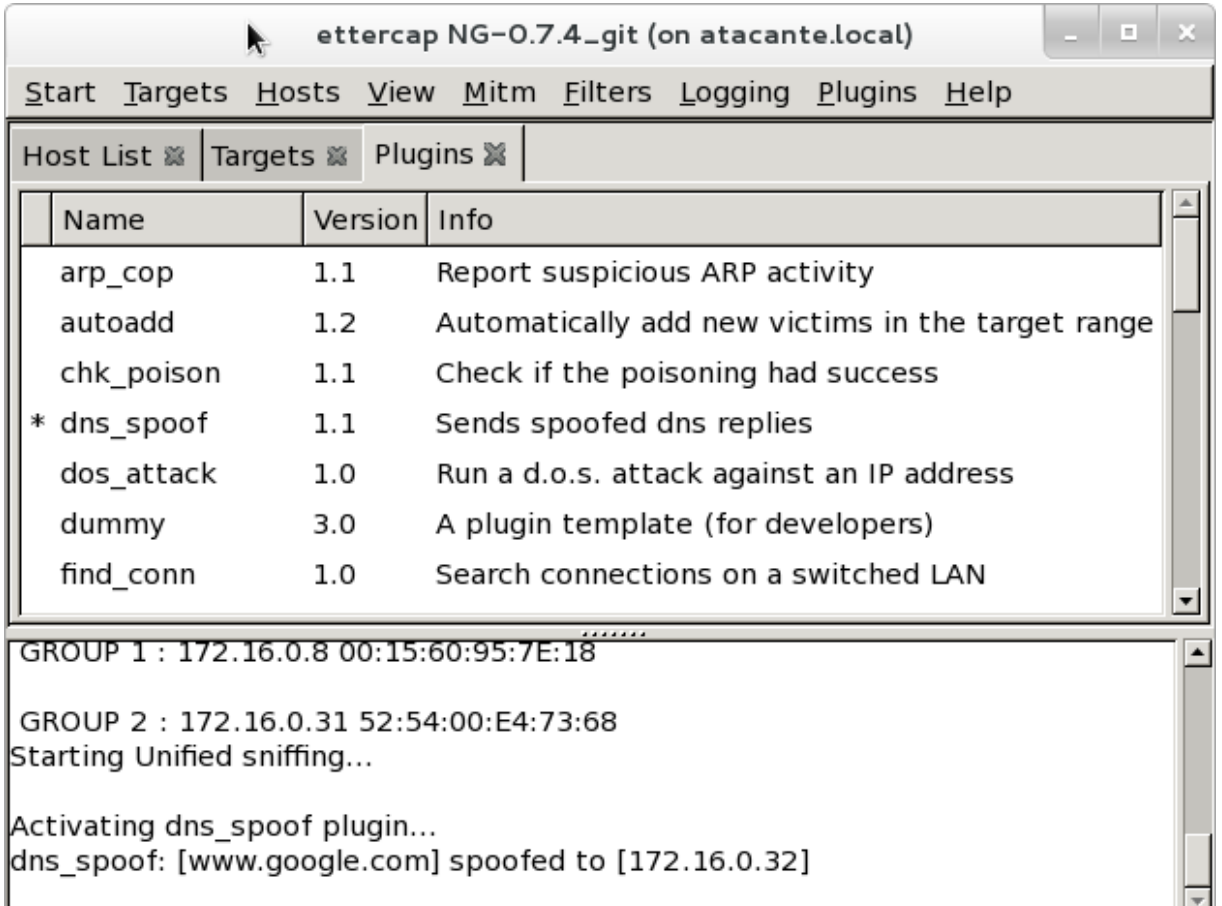
El Envenenamiento

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



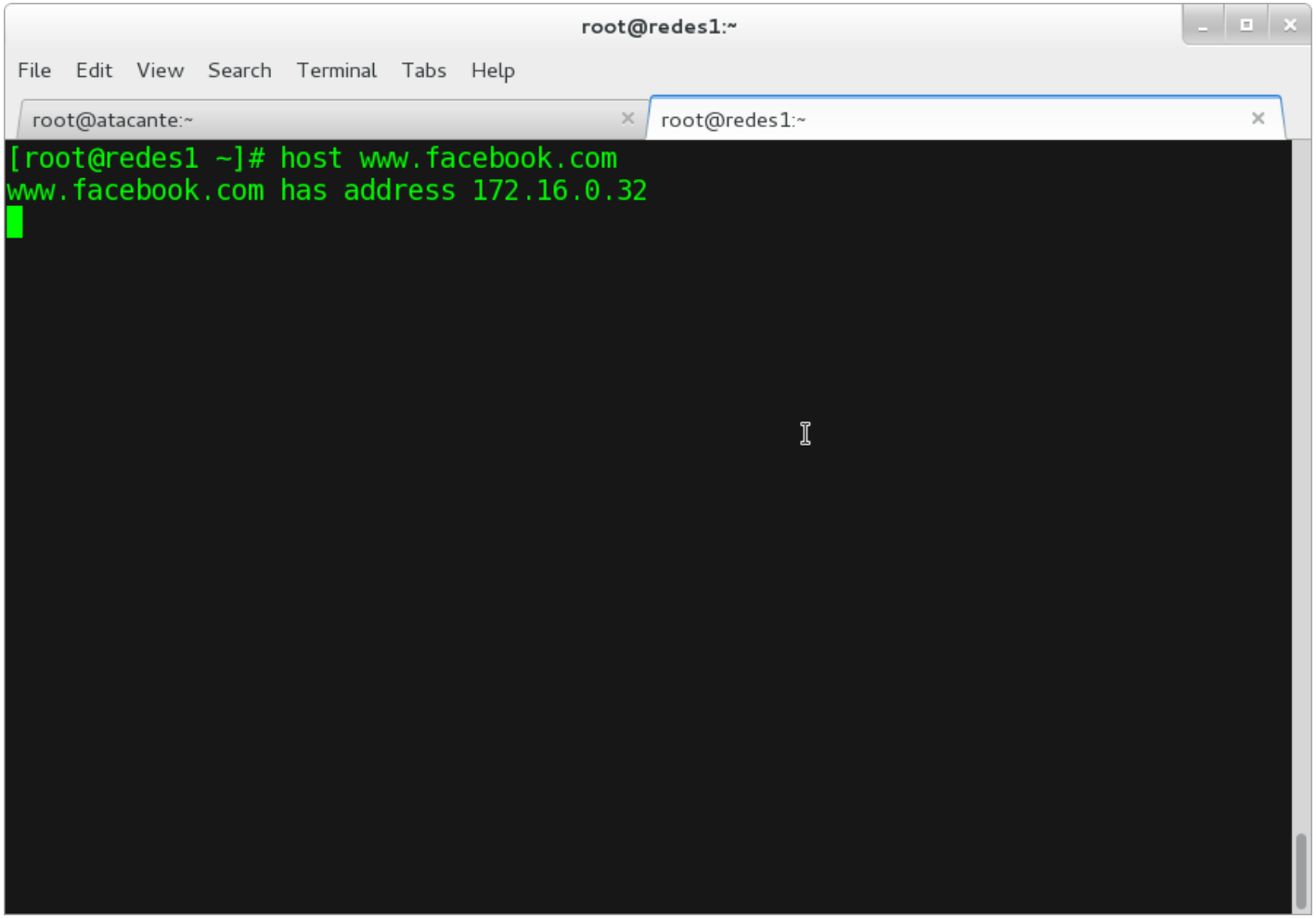
El Envenenamiento

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



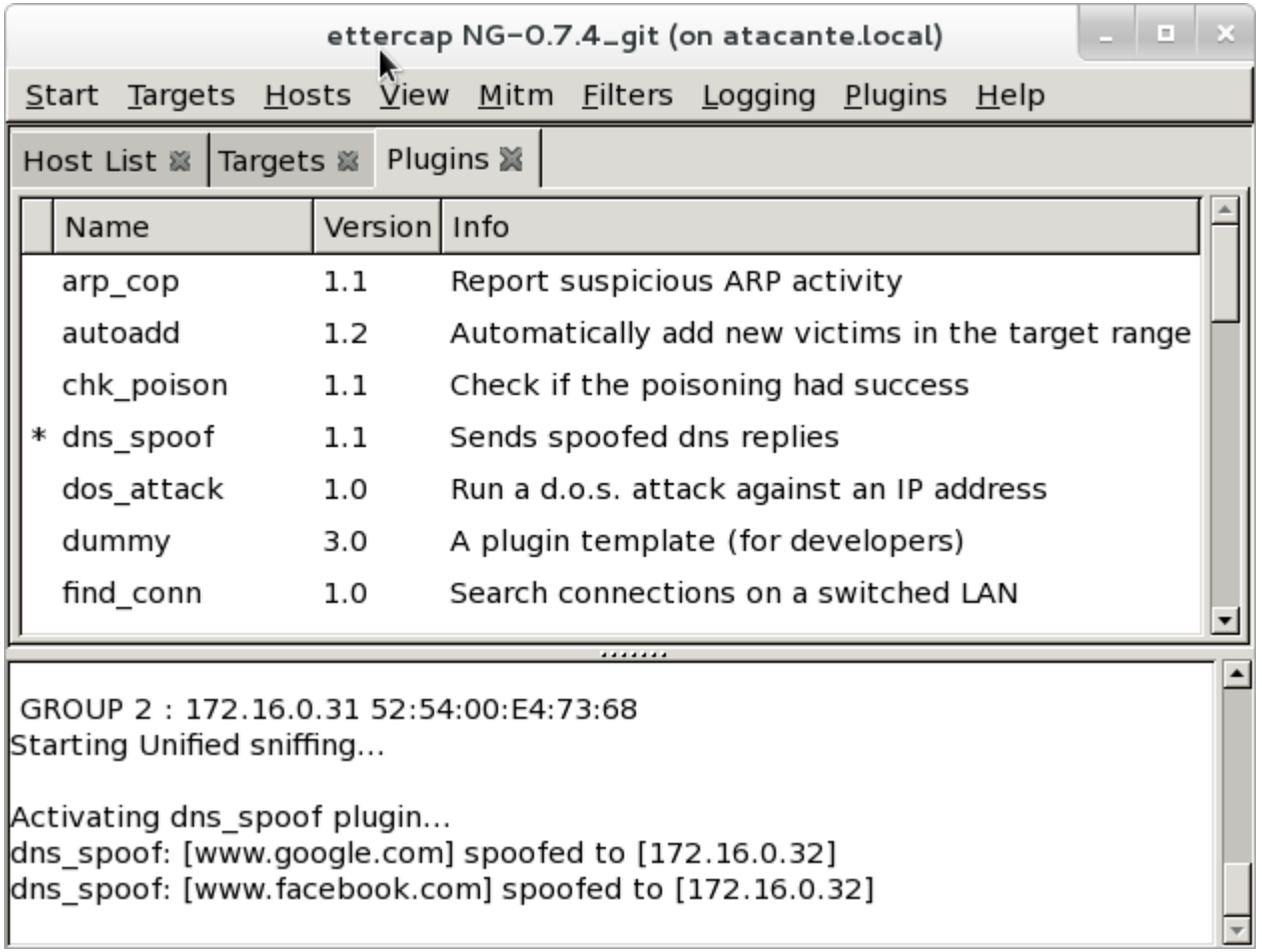
El Envenenamiento

En el caso de facebook



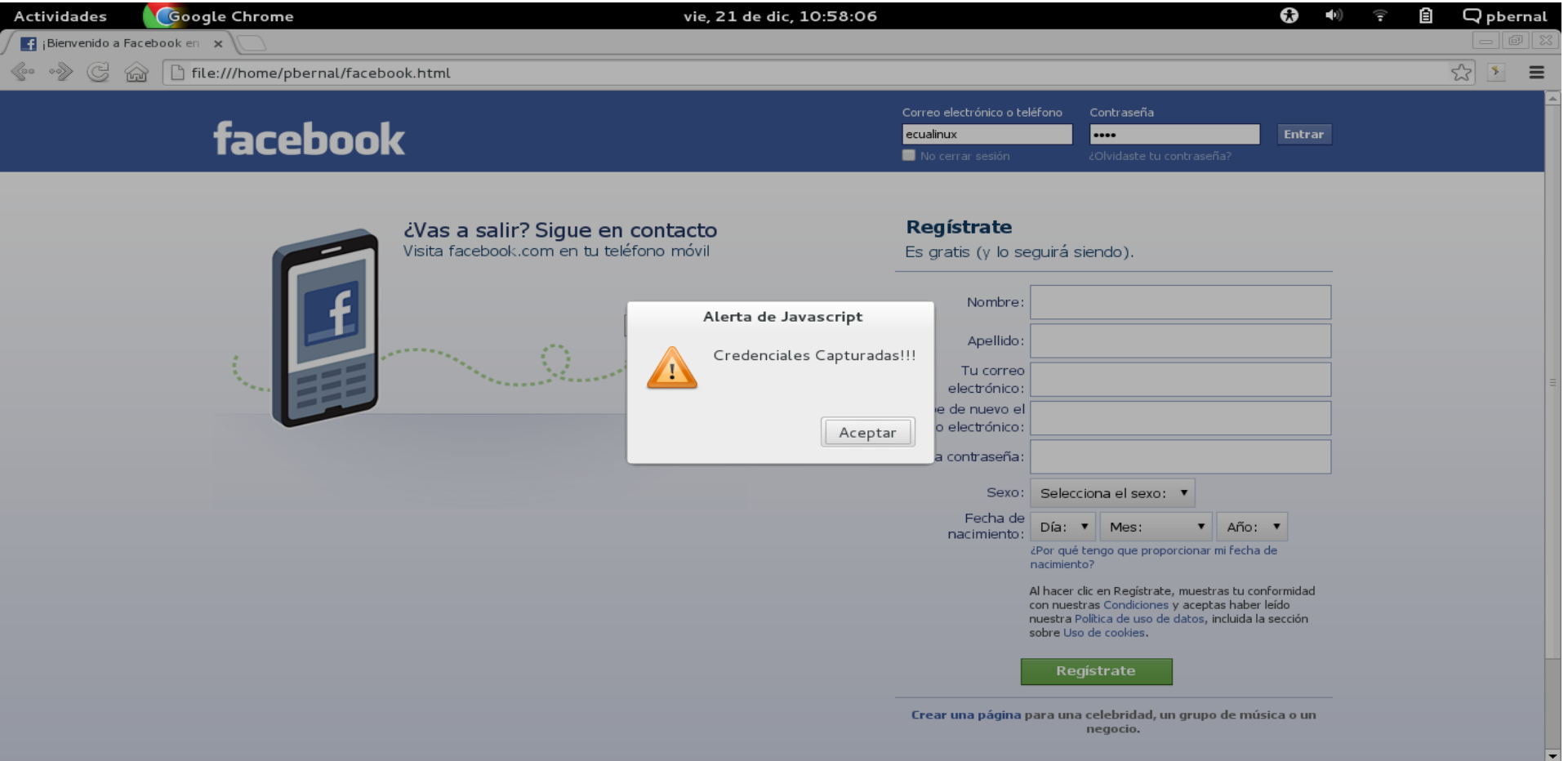
El Envenenamiento

Viendo este caso en el Ethercap



El Envenenamiento

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



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.