

Practica 3 – Obtener la contraseña de acceso a un Servidor FTP situado en nuestra red local al que no tenemos acceso autorizado.**Teoría:**

Sea un Servidor FTP situado en una red local conmutada tal que el atacante no tiene acceso autorizado porque desconoce una cuenta de usuario y contraseña válidas en el Servidor. Asimismo, el Servidor tampoco acepta acceso anónimo.

Sin embargo, el atacante sabe que cierto usuario víctima de su red local sí que tiene acceso autorizado al Servidor FTP.

El atacante puede sniffar la contraseña de acceso durante el proceso de autenticación del usuario víctima en el Servidor FTP.

En el caso de una red local compartida (hubs), sólo es necesario sniffar todos los paquetes que pasen por nuestra tarjeta de red, que serán los mismos que circulen por la red. De esta forma, cuando el usuario víctima inicie sesión, el paquete que contiene la contraseña de acceso será enviada a todos los equipos conectados al concentrador, entre ellos, nuestro equipo.

En el caso de una red local conmutada (switches), el tráfico entre el usuario víctima y el Servidor FTP sólo circulará entre estos dos equipos. El atacante debe alcanzar una posición de *Man in the Middle* si quiere ser capaz de sniffar este tráfico durante la conexión. A fin de lograr esta posición, el atacante debe envenenar las tablas ARP del equipo víctima y el Servidor FTP, de modo que el tráfico circule a través de su equipo: Víctima <-> Atacante <-> Servidor FTP.

Aplicación práctica:

Envenenamiento ARP + Sniffado

Escenario:

Atacante: 10.10.0.69

Víctima: 10.10.0.254

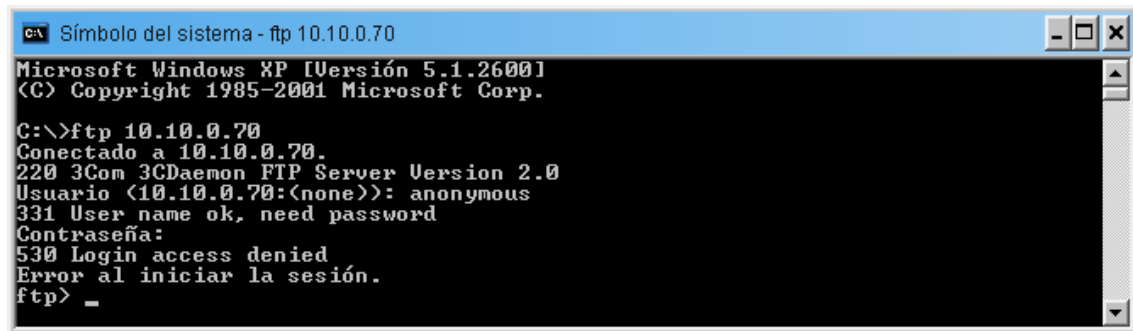
Servidor FTP: 10.10.0.70

Herramientas:

Vamos a utilizar el Sniffer Caín @ <http://www.oxid.it/>

Procedimiento:

1. Comprobamos que el equipo atacante no puede acceder al Servidor FTP utilizando la cuenta de usuario *anonymous*.



```

C:\>ftp 10.10.0.70
Conectado a 10.10.0.70.
220 3Com 3Cdaemon FTP Server Version 2.0
Usuario (10.10.0.70:(none)): anonymous
331 User name ok, need password
Contraseña:
530 Login access denied
Error al iniciar la sesión.
ftp> _

```

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

3. Envenenar las tablas ARP del equipo víctima y del Servidor FTP.

Las respectivas tablas ARP

- del equipo víctima:

Interfaz: 10.10.0.254 --- 0x2		
Dirección IP	Dirección física	Tipo
10.10.0.69	00-05-1c-0a-ab-92	dinámico
10.10.0.70	00-40-ca-3b-fd-e5	dinámico

- del Servidor FTP:

Interfaz: 10.10.0.70 --- 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:

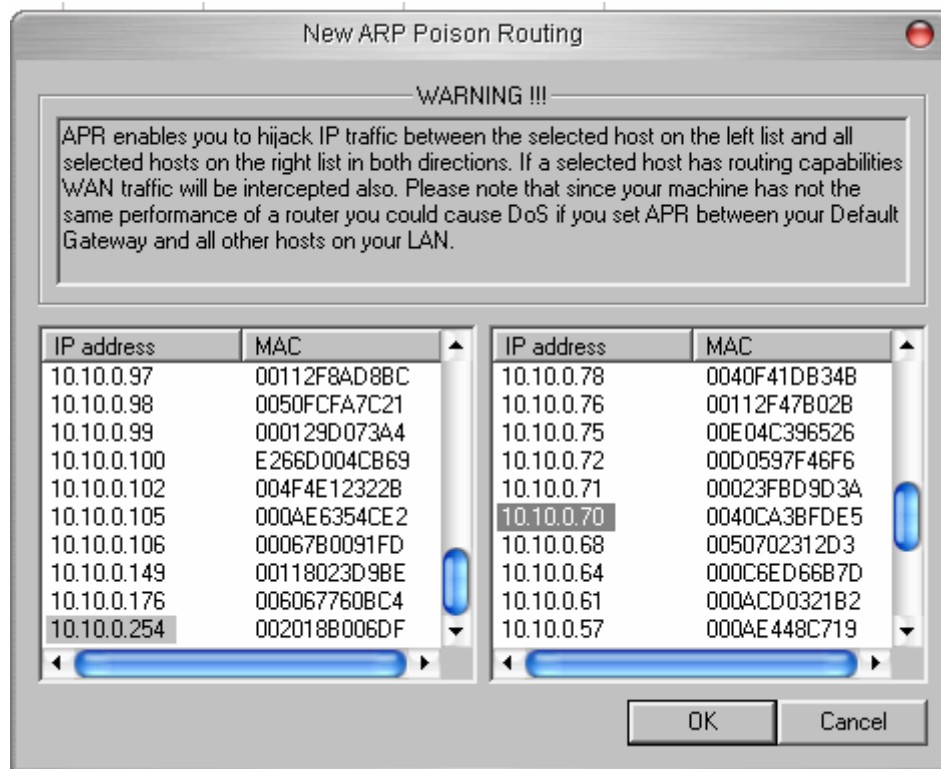
Interfaz: 10.10.0.254 --- 0x2		
Dirección IP	Dirección física	Tipo
10.10.0.69	00-05-1c-0a-ab-92	dinámico
10.10.0.70	00-05-1c-0a-ab-92	dinámico

- del Servidor FTP:

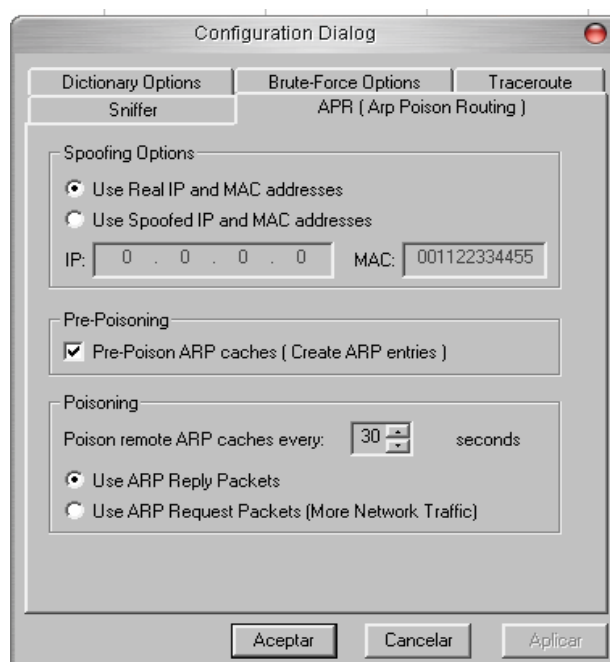
Interfaz: 10.10.0.70 --- 0x2		
Dirección IP	Dirección física	Tipo
10.10.0.69	00-05-1c-0a-ab-92	dinámico
10.10.0.254	00-05-1c-0a-ab-92	dinámico

Esto se puede efectuar de forma manual, generando periódicamente paquetes maliciosos con la utilidad Nemesis y habilitando ip_forwarding en el equipo atacante.

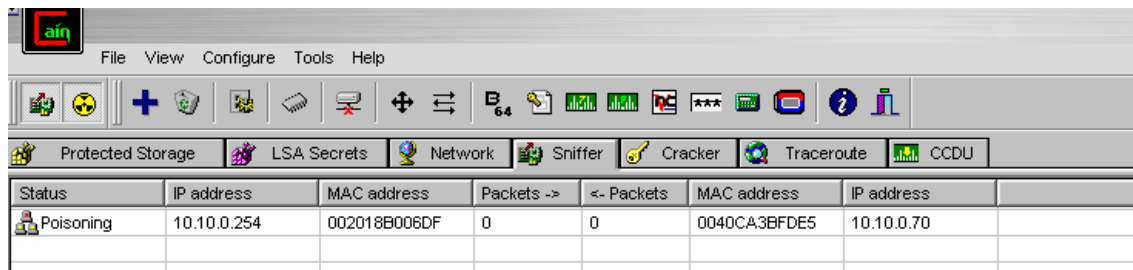
Sin embargo, el Sniffer Caín permite efectuar este proceso de forma sencilla y automática. En la pestaña *Sniffer*, subpestaña *APR*, pulsar el botón **+** y aparecerá el siguiente cuadro, donde podemos seleccionar los dos equipos de la red cuyas tablas ARP van a ser envenenadas:



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

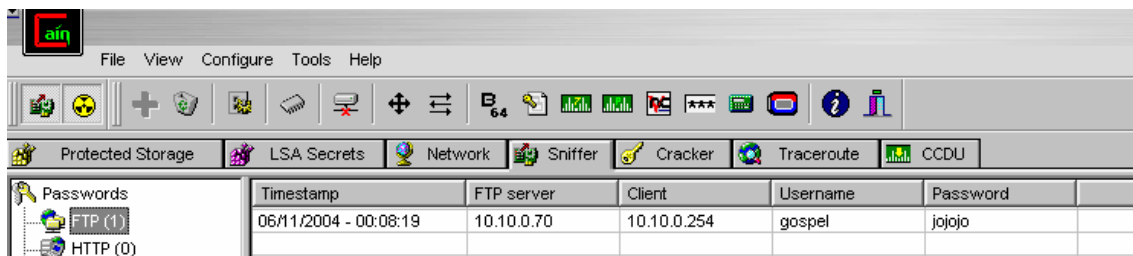


Activamos el Sniffer y el módulo de Envenenamiento ARP (*APR*):



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

4. Sólo queda esperar a que el usuario víctima inicie sesión en el Servidor FTP para que el Sniffer Caín situado en el equipo atacante intercepte el nombre del usuario y la contraseña de acceso. Cuando esto ocurra, Caín generará un log en la pestaña *Sniffer*, subpestaña *Passwords*, Protocolo *FTP*:



5. Una vez que el usuario atacante ya dispone de la cuenta de usuario y su contraseña válidas en el Servidor FTP, puede iniciar sesión en este:

