ENVENENAMIENTO ARP

El envenenamiento ARP (en inglés *Address Resolution Protocol* o Protocolo de resolución de direcciones) es una técnica usada por atacantes en redes internas cuyo fin es obtener el tráfico de red circundante, aunque no esté destinado al sistema del propio intruso. Con este método, el atacante puede conseguir derivar la información hacia su propia tarjeta de red y así conseguir información sensible, bloquearla o incluso modificarla y mostrar datos erróneos a las víctimas.

Esta técnica no se basa en una vulnerabilidad concreta que pueda llegar a desaparecer con el tiempo, sino que se basa en un fallo de diseño de las redes TCP[1] (*Transmission Control Protocol*), y por tanto, es un método de ataque siempre válido y eficaz a menos que se tomen medidas específicas contra él.

I Conceptos previos

Antes de entender este tipo de ataque, es necesario conocer ciertos conceptos previos en los que se basa.

Dirección MAC

La dirección MAC (*Media Access Control*) es un identificador único que se asigna a todas y cada una de las tarjetas de red existentes. Este identificador se graba en una memoria especial de las mismas. Lo hace el propio fabricante de la tarjeta o dispositivo, y consiste en una serie de números que identifican unívocamente a esa tarjeta de red.

De esta secuencia de números se pueden deducir una serie de datos, como por ejemplo el fabricante (marca de la tarjeta). También es conocida como la dirección física, dirección hardware, etc.

Su formato es el siguiente: 12:34:56:78:9A:BC

Se trata de una codificación hexadecimal en pareja de 48 bits de información. Los 24 primeros bits (tres primeras parejas de números) identifican al fabricante del hardware, y los 24 bits restantes corresponden al número de serie asignado por el fabricante, lo que garantiza que dos tarjetas no puedan tener la misma dirección MAC.

[1] Protocolo de Internet mediante el cual varios programas pertenecientes a una misma red de datos crean conexiones entre ellos a través de las cuales puede enviarse flujo de datos.

Es posible obtener la dirección MAC de una tarjeta a través del sistema operativo (en el sistema operativo Windows se obtiene por línea de comandos, ejecutando la sentencia *ipconfig*).

Aunque, como se ha mencionado, la dirección MAC debe ser única por cada tarjeta de red, es el sistema operativo, en última instancia, el que la gestiona. Por tanto, es posible, indicar al sistema operativo que informe al resto de ordenadores en la red que la dirección MAC de una tarjeta es diferente a la real. Esta técnica conforma una de las bases del ataque de envenenamiento ARP.

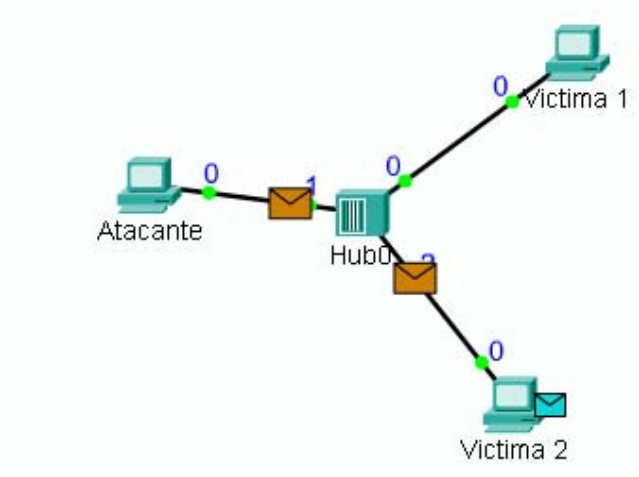
***Hubs*, *switches*, *routers*, puntos de acceso, etc.**

Los sistemas forman redes a través de dispositivos que los unen entre sí. En los inicios de las primeras redes, los ordenadores se conectaban entre sí a través de diferentes métodos y, en ocasiones, un solo cable. Además de los problemas de congestión y eficiencia, esto suponía un problema de privacidad para los datos ya que no existía confidencialidad en las comunicaciones de un sistema a otro en una red interna.

Conforme fueron creciendo el número de sistemas conectados, se hicieron necesarios dispositivos capaces de comunicar a todos los ordenadores entre sí.

Un *hub* es un simple multiplicador de la señal. Los ordenadores se conectan a él, y el dispositivo se encarga de repetir la señal al resto de cables de red conectados en él a través de sus puertos (también llamados bocas) disponibles. Así, con un *hub* el tráfico de un sistema a otro es replicado al resto. Esto conlleva un problema de seguridad y privacidad, por lo que es un dispositivo en desuso.

Ilustración 1: *Hub* replicando la información a todos los sistemas



Fuente: Programa Packet Tracer de CISCO

La misión del *switch*, en principio, es la misma que la del *hub*. Establece una comunicación de flujo de datos entre los sistemas conectados a él. La diferencia que presenta con el *hub* es que no se limita a multiplicar la señal a través de todos sus puertos, sino que recuerda a quién debe enviar la información y los datos solo fluyen desde el origen a su destino. Con la irrupción del *switch* se solucionó el problema de privacidad que presentaba el *hub*, pero al irrumpir la técnica del envenenamiento ARP, la privacidad en las redes internas volvió a presentar vulnerabilidades. Con el tiempo, el *switch* ha incorporado técnicas para evitarlo.

Un *router* es un sistema que conecta dos redes entre sí. A través de un *router* no se transmite la dirección MAC, solo la IP del sistema interno o la del propio *router* en su nombre.

Tanto el *hub* como el *switch* operan a nivel de MAC, es decir, no conciben el concepto de dirección IP, esto es muy significativo para comprender el ataque de envenenamiento ARP.

Subred

Una subred se puede definir como un sistema de red de ordenadores (o cualquier otro dispositivo) que están conectados a través de un *switch*, *hub* u otro punto de acceso cualquiera. En estos casos, la subred comparte un mismo rango de direcciones IP, donde cada sistema tiene una dirección IP diferente.

Cualquier sistema conectado a uno de los dispositivos mencionados y con una dirección IP en el rango adecuado, podrá comunicarse con el resto. En el momento en el que se interpone un *router* en una red, la subred termina y comienza otra, donde no se transmite la dirección MAC sino la dirección IP.

Se dice que una red está convenientemente segmentada cuando no existen en ella más ordenadores que los necesarios para llevar a cabo su trabajo y cuando entre las redes no existe la posibilidad de obtener el tráfico de otra a menos que así se especifique.

ARP (*Address Resolution Protocol*)

Se trata de un protocolo de red que sirve para determinar, a qué sistema concreto pertenece una IP. En una red local, ni las tarjetas de red ni los dispositivos que las unen (*switch*, puntos de acceso, etc.) entienden el protocolo IP. Eso es trabajo del sistema operativo. Estos dispositivos, en un nivel más bajo (cuando los datos todavía no han sido interpretados por el sistema operativo) solo son capaces de reconocer direcciones MAC (físicas).

Así, cuando un sistema conectado a una red quiere comunicarse con otro, debe enviar primero lo que se conoce como mensaje de difusión (*broadcast*) a toda la red usando

este protocolo de resolución de direcciones físicas (ARP). El mensaje es enviado y recibido por todas las tarjetas de red. El sistema operativo que lo recibe lo procesa y devuelve al interesado la dirección IP asociada a esa dirección MAC. Resumiendo, se trata del protocolo usado para que en la red exista una asociación "dirección MAC"-"dirección IP" y hacer así la comunicación más eficiente.

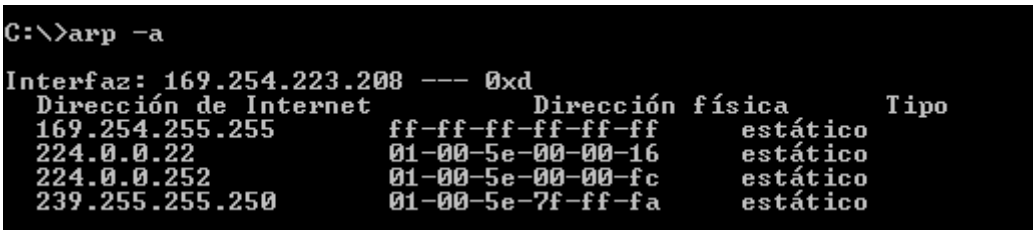
Caché ARP

Para que el sistema operativo no tenga que realizar esa consulta de difusión cada vez que necesita conocer la dirección IP asociada a una MAC (o viceversa), suele almacenarlo en una memoria interna llamada caché ARP.

La caché ARP puede ser consultada en cualquier ordenador de forma muy sencilla a través de una línea de comando: arp -a

Con el comando es posible obtener una lista actualizada de las direcciones IP y direcciones MAC correspondientes en una red. Cuando un nuevo dispositivo es conectado a la misma, o el sistema se comunica por primera vez con otro ordenador, se envía un nuevo mensaje de difusión. Si por el contrario la red se mantiene estable, el sistema solo consulta la mayor parte del tiempo su memoria caché.

Ilustración 2: Resultado de consultar la caché ARP en un sistema Windows conectado a una red



Fuente: INTECO

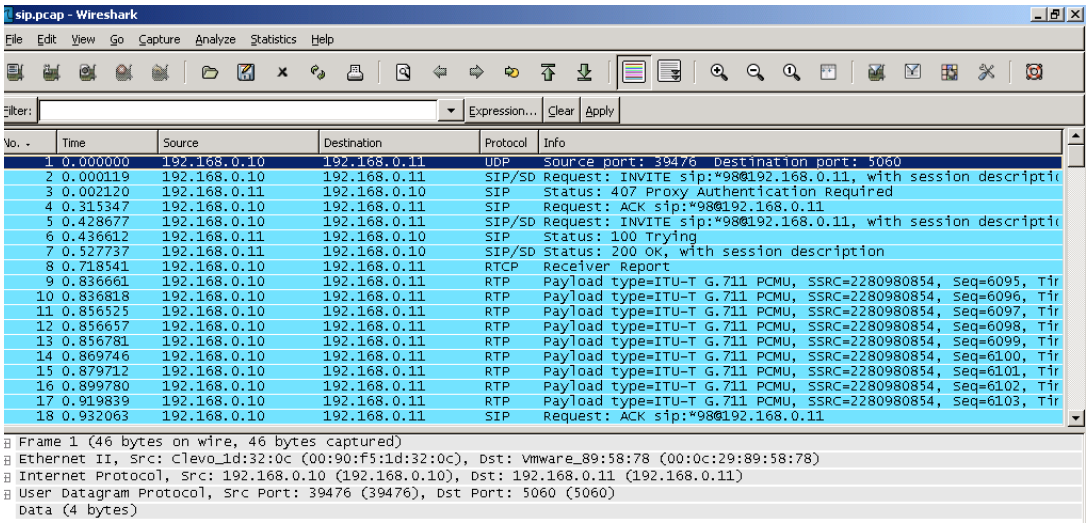
El envenenamiento ARP consiste precisamente en intentar modificar esa caché, de forma que el sistema operativo recuerde una asociación falsa entre dirección IP y dirección MAC.

Modo promiscuo

En una tarjeta de red, el sistema operativo se encarga de rechazar los paquetes de red que no están destinados a su dirección IP. Aunque tenga acceso al tráfico (por ejemplo si los sistemas están enlazados entre sí a través de un *hub*), si no le corresponden los datos, son descartados.

Existe, sin embargo la posibilidad de procesar esa información aunque no corresponda al sistema (por ejemplo, si llegan paquetes con una dirección IP de destino que no es la del sistema operativo que lo recibe). Los sistemas operativos pueden situar la tarjeta de red modo especial llamado modo promiscuo que permite procesar toda la información que les llegue. En un entorno con un *hub*, por ejemplo, es todo lo que se necesita para capturar el tráfico ajeno. En un entorno segmentado, la combinación del envenenamiento ARP con el hecho de poner la tarjeta en modo promiscuo, permite la obtención y procesamiento de tráfico ajeno y, por tanto, el ataque que se está describiendo.

Ilustración 3: *Wireshark* (uno de los *sniffers* más populares) obteniendo tráfico en modo promiscuo



Fuente: INTECO

II Cómo funciona el ataque

Una vez que disponemos de los conceptos previos, entender que conforma un ataque de envenenamiento ARP básico resulta sencillo. La idea es hacer pensar a un ordenador, que una dirección IP (un sistema operativo) está asociada con una MAC (una tarjeta de red) que no es realmente la suya. Esto, por definición del propio protocolo TCP, hará que los *switch* dirijan el tráfico al dispositivo de red que tenga esa dirección MAC.

Como se ha indicado, los *switch* (que a priori no permiten observar el tráfico ajeno) operan a nivel de MAC, esto quiere decir que no entienden el concepto de dirección IP, y por eso funciona el ataque.

En resumen, si se consigue confundir a la caché de cada sistema operativo donde se almacena la información de la pareja IP-MAC, y se le hace creer que la IP está asociada a otra MAC, será el dueño de esa MAC adonde se dirija realmente el tráfico cuando pase por un punto de acceso o un *switch*.

¿Y cómo se puede conseguir que una caché de un ordenador ajeno recuerde una información que no es real? El protocolo ARP, como se ha indicado anteriormente, permite enviar respuestas ante un mensaje de difusión, en el que cada ordenador se identifica con una MAC. El atacante solo tiene que construir paquetes de este tipo a nivel de red, y enviarlos al ordenador de la víctima, como si ésta hubiese realizado una pregunta que nunca ha formulado. Aunque parezca complejo, esto se lleva a cabo ejecutando un simple programa e indicándole los datos que se le quieren enviar a la víctima.

Así, el atacante que desea confundir la caché ARP de un sistema, solo tiene que enviar por red constante y regularmente (para que la caché no se actualice con los datos reales) una asociación IP-MAC errónea. Con estos datos en caché, el sistema queda confundido y envía siempre al dueño de esa MAC la información, aunque lo que desee realmente es enviarla al dueño de la dirección IP.

III Tipos de ataque

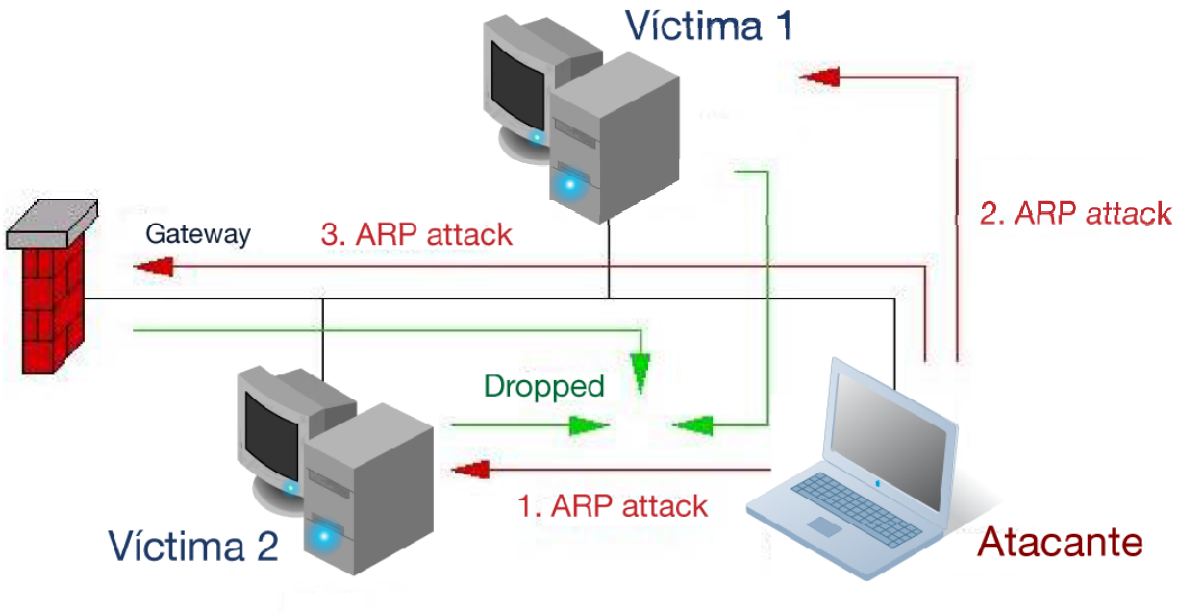
Las posibilidades de ataque son diversas dependiendo de con qué MAC se envenene la caché de la víctima.

ARP DoS

ARP *Denial of Service*. Consiste en hacer pensar a la víctima que una dirección IP está asociada a una dirección MAC que no existe. Por tanto, cada vez que la víctima desee comunicarse con esa dirección IP, el *switch* hace que el tráfico se dirija a un sistema inexistente y no llegue a su destino. La víctima ha perdido la comunicación con esa dirección IP en la red interna. Si la dirección IP es la de su puerta de acceso, pierde la conexión con el exterior.

Es el ataque más básico, y para ello el atacante solo debe enviar de forma regular paquetes de respuesta ARP especialmente manipulados, con una asociación falsa.

Ilustración 4: Esquema de ARP DoS



Fuente: INTECO

ARP *Sniffing*

¿Qué ocurre si el atacante hace pensar a la víctima que una dirección IP está asociada a su propia dirección MAC? Esto puede constituir el segundo tipo de ataque: la obtención de información.

En este caso el atacante indica a la víctima que una dirección IP está asociada a su MAC. Por tanto, todo ese tráfico es redirigido a él mismo. Habitualmente, en este caso la tarjeta de red rechaza estos datos, puesto que, aunque la MAC coincida, la dirección IP del atacante realmente es diferente a la del destino con el que la víctima quiere ponerse en contacto.

Es aquí donde entra en juego el modo promiscuo mencionado anteriormente. Si el atacante, además de enviar de forma regular paquetes de respuesta ARP especialmente manipulados (con una asociación falsa a la víctima) pone su tarjeta en modo promiscuo, puede ver la información que le llega y procesarla. En resumen: puede obtener la información que la víctima cree estar enviando a otro sistema.

ARP *hijacking* o *proxying*

En los casos descritos anteriormente, la víctima pierde la comunicación con el destino legítimo. Si el atacante desea realizar un ataque completo, debe además reenviar la información a ese destino legítimo. Este ordenador o dispositivo destino (podría tratarse

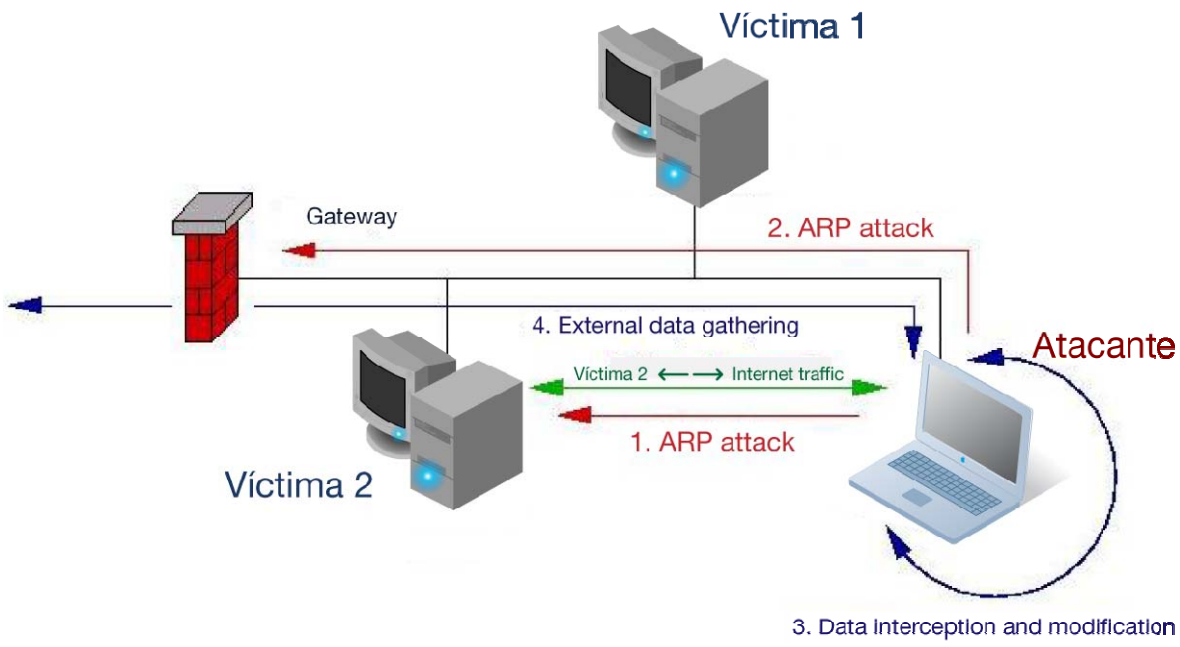
de la puerta de enlace) cuando reciba la información, responde a la víctima de forma normal, solo que la información previamente ha sido procesada por el atacante.

Si además el atacante realiza el mismo tipo de ataque de envenenamiento ARP con el sistema destino de la víctima, el ataque se completa y obtiene la información que circula en ambos sentidos. Ni la víctima ni el sistema destino (que se convierte a su vez en una segunda víctima) detectan nada.

En resumen, el atacante debe realizar tres pasos:

- Hacer creer a la víctima, que la MAC de la máquina con la que se quiere comunicar es la del atacante.
- Hacer creer a la otra víctima (máquina destino) que la MAC de la máquina con la que se quiere comunicar es la del atacante.
- Reenviar esta información a sus respectivos destinos una vez procesada por él.

Ilustración 5: Esquema de ataque de ARP *Proxying*



Fuente: INTECO

Un ejemplo práctico:

- **ORDENADOR A**: Puerta de enlace (*gateway*). Su MAC 01:01:01:01:01:01 y su IP 192.168.0.1
- **ORDENADOR B**: Víctima. Su MAC 02:02:02:02:02:02 y su IP 192.168.0.2

- **ORDENADOR C**: Atacante. Su MAC 03:03:03:03:03:03 y su IP 192.168.0.3

Desde el sistema del atacante se envían paquetes de respuesta ARP falsos a ORDEANDOR A Y ORDEANDOR B. En estos paquetes se le indica al ORDENADOR A que la dirección MAC del ORDENADOR B es la del atacante, quedando esta información almacenada en su caché ARP. Es necesario realizar la misma operación con la otra víctima.

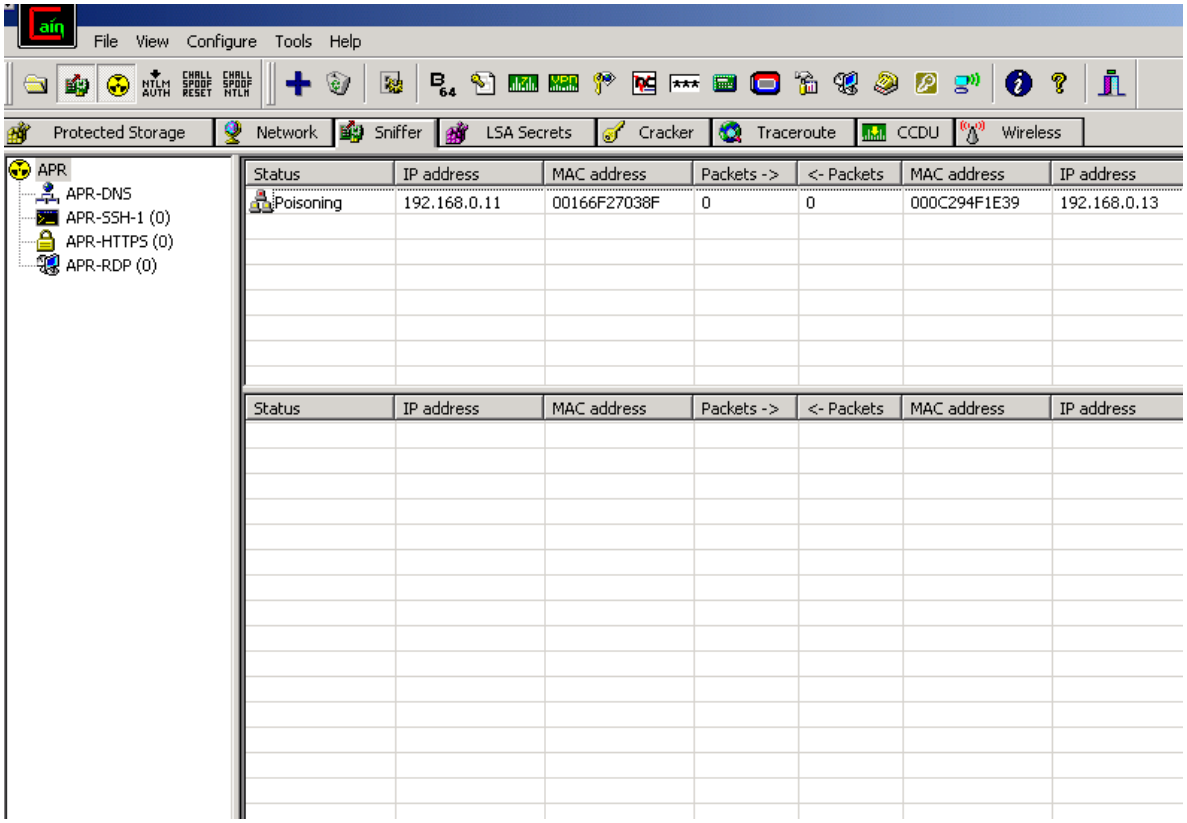
- Enviar a ORDENADOR A un paquete de tipo arp-reply informando que 192.168.0.2 tiene dirección MAC 03:03:03:03:03:03

- Enviar a ORDENADOR B un paquete de tipo arp-reply informando que 192.168.0.1 tiene dirección MAC 03:03:03:03:03:03

A su vez, el atacante se encarga de reenviar la información a sus destinos adecuados. A partir de ahora, lo paquetes de información que se envíen entre ambas llegan a la víctima.

Existen infinidad de programas capaces de realizar todos estos pasos con solo indicarles los datos adecuados. Quizás el más famoso sea “Caín” para Windows.

Ilustración 6: Caín ejecutando un ataque completo de envenenamiento ARP



Fuente: INTECO

IV Consejos de prevención

Existen numerosos métodos que se pueden aplicar en una red para prevenir que un atacante pueda llevar a cabo un ataque de envenenamiento ARP. Lo más efectivo es una adecuada combinación de todas ellas. A continuación se exponen algunos de los métodos preventivos más importantes.

- Es posible indicar al sistema operativo que la información en la caché ARP es estática y por tanto, no debe ser actualizada con la información que le provenga de la red. Esto prevendrá el ataque, pero puede resultar problemático en redes donde se actualicen los sistemas conectados a la red de forma regular.

- Los *switch* de gama alta, poseen funcionalidades específicas para prevenir este tipo de ataques. Es necesario configurarlos adecuadamente para que mantengan ellos mismos una asociación IP-MAC adecuada y prevengan estos ataques.

- Una adecuada segmentación de las subredes con *routers* y redes virtuales (otra de las funcionalidades de algunos *switch*) es la mejor prevención.

- Existen herramientas que permiten conocer si una tarjeta de red en una subred se encuentra en modo promiscuo. Esto puede indicar la existencia de un ataque de envenenamiento ARP.