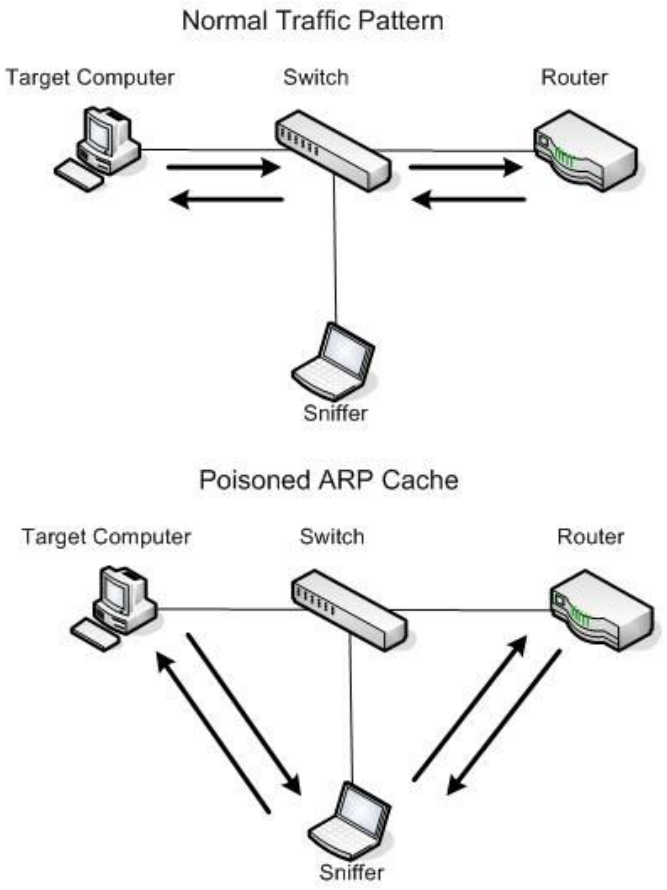
ARP Poisoning - Funcionamiento

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/IP, hará que los switches dirijan el tráfico al dispositivo de red que tenga esa dirección MAC.

Como se ha indicado, los switches (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 sólo 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 indicando 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.



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.

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:

1) Hacer creer a la víctima, que la MAC de la máquina con la que se quiere comunicar es la del atacante.

2) Hacer creer a la otra víctima (máquina destino) que la MAC de la máquina con la que se quiere comunicar es la del atacante.

3) Reenviar esta información a sus respectivos destinos una vez procesada por él.

Un ejemplo práctico:

ORDENADOR A: Puerta de enlace (gateway).

MAC = 01:01:01:01:01:01

IP = 192.168.0.1

ORDENADOR B: Víctima.

MAC = 02:02:02:02:02:02

IP = 192.168.0.2

ORDENADOR C: Atacante

MAC = 03:03:03:03:03:03

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.

1) 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

2) 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 "Cain & Abel" para Windows. También disponemos de "Ettercap" (Windows y Linux) y Dsniff (Linux).

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 switches 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 switches) 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.

Autor: Fabian Martinez Portantier

Fuentes: INTECO (www.inteco.es)