ARP Poisoning - 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.

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.

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 sólo fluyen desde el origen a su destino. Con la irrupción del switch se soluciona 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. 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.

Autor: Fabian Martinez Portantier

Fuentes: INTECO (www.inteco.es)