**ARP Poison**

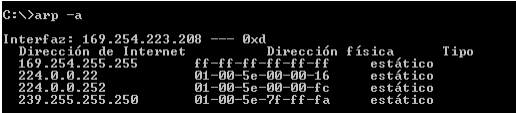
El envenenamiento ARP (en inglés Address Resolution Protocol o Protocolo de resolución de direcciones) es una técnica usada por atacantes en redes internas cuyo fin es obtener el tráfico de red circundante, aunque no esté destinado al sistema del propio intruso. Con este método, el atacante puede conseguir 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 (Transmission Control Protocol), y por tanto, es un método de ataque siempre válido y eficaz a menos que se tomen medidas específicas contra él.

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.



Resultado de consultar la caché ARP en un sistema Windows conectado a una red.

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.

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.

**ARP FLOODING**

|  |
| --- |
| Varios programas de malware han sido descritos como causantes de los ataques Address Resolution Protocol (ARP) al inundar la red con respuestas erróneas.  El ARP es parte del Protocolo de Internet (IP) que es responsable de mapear la dirección IP de un ordenador con su dirección MAC.  Una comunicación de ARP normal comienza cuando un ordenador envía un paquete a una dirección IP específica. Se emite una petición ARP, conocida como *¿Quién es* , paquete que solicita la dirección MAC del ordenador con la dirección IP específica. El dicho ordenador a continuación, envía una respuesta que contiene su dirección MAC. La solicitud original procedente de un ordenador a continuación, mantiene un registro de la dirección MAC en su caché ARP.  En ARP inundaciones, el sistema afectado envía respuestas ARP a todos los sistemas conectados a una red, haciendo que las entradas incorrectas en la caché ARP. El resultado es que el sistema afectado es incapaz de resolver las direcciones IP y MAC, debido a las entradas erróneas en la caché ARP. El sistema afectado no es capaz de conectarse a cualquier otro sistema de la red.  Los siguientes programas de malware se encuentran para ser capaz de ARP Flooding:   * [BKDR\_DELF.BJE](http://www.trendmicro.com/vinfoMalware.aspx?language=us&name=BKDR_DELF.BJE) * [BKDR\_NPFECT.A](http://www.trendmicro.com/vinfoMalware.aspx?language=us&name=BKDR_NPFECT.A) * [TROJ\_AGENT.BSD](http://www.trendmicro.com/vinfoMalware.aspx?language=us&name=TROJ_AGENT.BSD) * TROJ\_AGENT.BZS * TROJ\_AGENT.CBX * TROJ\_AGENT.CDT * [TROJ\_DELF.BOC](http://www.trendmicro.com/vinfoMalware.aspx?language=us&name=TROJ_DELF.BOC) * [TROJ\_DELF.BRK](http://www.trendmicro.com/vinfoMalware.aspx?language=us&name=TROJ_DELF.BRK) * [TROJ\_VANTI.CJ](http://www.trendmicro.com/vinfoMalware.aspx?language=us&name=TROJ_VANTI.CJ) * [TSPY\_LMIR.ET](http://www.trendmicro.com/vinfoMalware.aspx?language=us&name=TSPY_LMIR.ET) * [TSPY\_LINEAGE.BAM](http://www.trendmicro.com/vinfoMalware.aspx?language=us&name=TSPY_LINEAGE.BAM)   Otra posibilidad es cómo detectar el tráfico de red, que incluye las redes basadas en conmutadores. A pesar de que la red conmutada está diseñado para redirigir el tráfico a un host en particular, el envío de una fuerte cantidad de paquetes ARP a las fuerzas del interruptor que le permite operar en un *modo a prueba de fallos* , que funciona como un concentrador. Como sabemos, los centros envían paquetes a todos los hosts en la red, por lo que el tráfico de red sniffing fácil. |