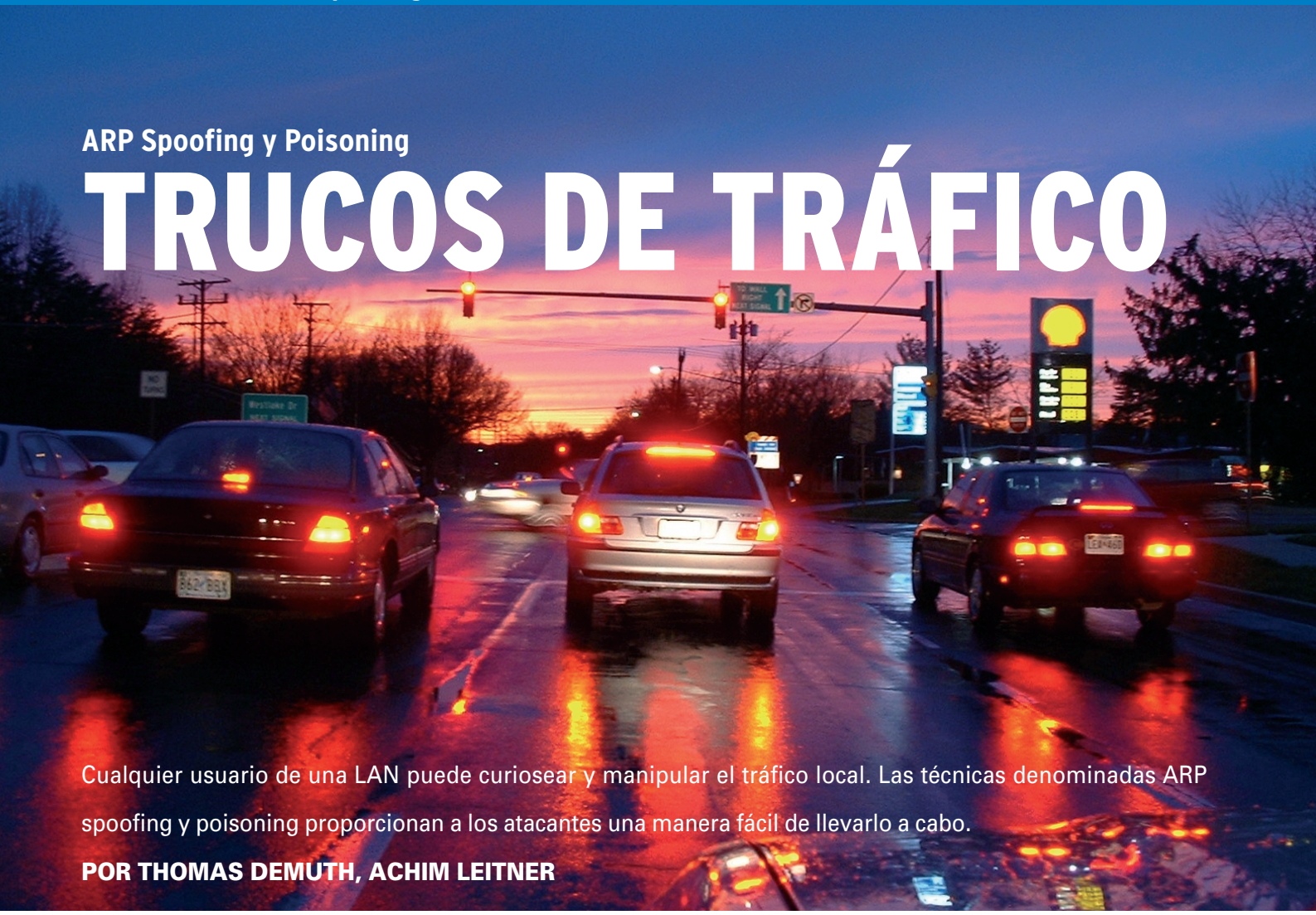

ARP Spoofing y Poisoning

TRUCOS DE TRÁFICO

Cualquier usuario de una LAN puede curiosear y manipular el tráfico local. Las técnicas denominadas ARP spoofing y poisoning proporcionan a los atacantes una manera fácil de llevarlo a cabo.

POR THOMAS DEMUTH, ACHIM LEITNER

Curiosidad, venganza o espionaje industrial pueden ser las razones por las que desde dentro de su propia red un atacante pueda realizar sus fechorías. Las estadísticas confirman que entre el 70 y 80 por ciento de los ataques efectuados a una red proceden desde dentro de la misma [1]. Los administradores pasan bastante tiempo impidiendo estos ataques internos ya que proteger la red desde dentro es mucho más difícil que protegerla frente a ataques externos.

Una de las técnicas más formidables de ataques internos es la que se conoce como ARP spoofing. ARP spoofing coloca a un atacante en una posición en la que puede espiar y manipular el tráfico local. El ataque conocido como *el hombre de en medio* es fácil de realizar gracias a un software sofisticado, incluso los atacantes con muy pocos conocimientos sobre redes disponen de buenas utilidades para llevar a cabo su cometido con éxito.

¿Cómo funciona ARP?

El protocolo ARP se publicó en Noviembre de 1982 como RFC 826 [2] por David C. Plumier. Como la seguridad en las tecnologías de la información no era un factor importante en aquella época, el objetivo era simplemente proporcionar funcionalidad. ARP transforma direcciones IP a direcciones MAC. Si el cliente C necesita enviar un paquete al servidor S, tiene que saber cual es la dirección MAC de S si ambas máquinas están dentro de la misma subred. Incluso si S reside en una red diferente, C aún necesita la MAC -en este caso, la dirección del router que reenviará el paquete. El router se hará cargo de todo lo demás.

Para averiguar la dirección MAC, C retransmite una solicitud ARP a todas las máquinas de la red local, preguntando "¿Quién tiene la dirección IP a.b.c.d?". La máquina que tiene dicha dirección IP responde indicándole al cliente su dirección MAC (Figura 1).

Como se muestra en la Figura 2, un paquete ARP se transporta como información dentro de una trama Ethernet. Para permitir que esto pueda hacerse, el valor de 0x8006 se coloca en la cabecera de la trama en el campo tipo – esto le indica al destino que se trata de un paquete ARP.

Como sería muy costoso el tener que retransmitir solicitudes ARP y esperar las respuestas antes de enviar datos, cada pila IP contienen una tabla ARP, también conocida como ARP caché (Figura 3). La caché contiene una tabla con las direcciones IP y las direcciones MAC correspondientes. La tabla puede albergar entradas estáticas (por ejemplo, aquellas generadas por un usuario) y entradas dinámicas (aquellas que ha ido aprendiendo a través del protocolo ARP). Las entradas dinámicas a menudo son válidas para períodos cortos de tiempo, normalmente unos cuantos minutos.

Efectuando ataques en la LAN

Como ARP no realiza ningún intento por protegerse frente paquetes manipulados, es vulnerable a una serie de ataques. Los más comunes son MAC spoofing, MAC flooding y ARP spoofing.

MAC spoofing implica que el atacante debe usar una dirección fuente MAC manipulada. Esta técnica tiene sentido si los privilegios van ligados a una dirección MAC. Muchos administradores de WLAN

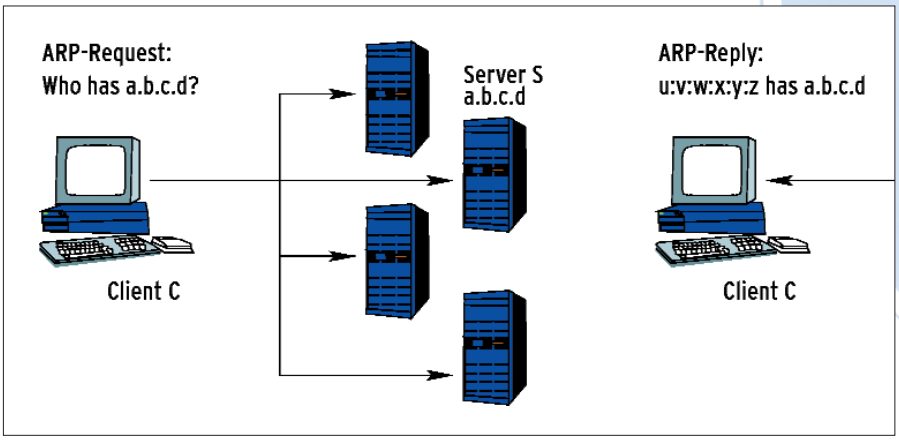

Figura 1: El cliente utiliza ARP para averiguar la dirección MAC del servidor en la LAN antes de enviar paquetes a este servidor. La petición a "Who has " se transmite a todas las máquinas en la LAN. El nodo con la dirección pedida responderá directamente a la máquina que pregunta.

(Wireless LAN) ponen la dirección MAC de los usuarios autorizados en una lista de control de acceso. Esto es una medida de seguridad débil ya que es fácil de vulnerar. El atacante tan sólo tiene que conocer una dirección privilegiada y usarla cuando la máquina con dicha dirección esté apagada. MAC spoofing es útil cuando los atacantes quieren proteger su identidad.

Hay una forma bastante sencilla de impedir esta clase de ataques en una red cableada: muchos switches permiten seguridad a nivel de puertos. El switch tan sólo aprende la dirección MAC una sola vez y la almacena permanentemente. A partir de este momento, el switch no aceptará ninguna otra dirección MAC fuente conectada a ese puerto. Este mecanismo es efectivo frente a los ataques MAC spoofing. Como punto negativo se tiene que el administrador debe reconfigurar el switch cada vez que se cambie la red.

La seguridad a nivel de puertos puede también proteger la red frente a otra clase de ataques. El ataque conocido como MAC flooding está diseñado para echar abajo la seguridad a nivel de puertos de un switch.

Al contrario que los hubs, los switches usan tablas CAM (Memoria de contenido direccionable), que especifican el puerto correspondiente a cada dirección MAC del switch. El switch tan solo enviará paquetes a través del puerto que conduzca a la máquina destino.

Los atacantes pueden deshabilitar esta funcionalidad sobrecargando el switch con direcciones -la tabla CAM solo puede contener un número determinado de direcciones. Si el ataque tiene éxito, se consigue que el switch funcione como un hub y esto permite que las comunicaciones sean visibles por cualquier puerto.

ARP Poisoning

El tercer ataque no es tan fácil de detectar y no hay contramedidas simples. El ataque se basa en un ARP spoofing, donde el atacante deliberadamente transmite un paquete ARP falso. ARP poisoning es un tipo específico de ARP spoofing cuyo objetivo es manipular (envenenar en inglés, de ahí el nombre) las tablas ARP de otras máquinas.

Como los sistemas operativos no suelen comprobar si una respuesta ARP es realmente la contestación a una solicitud ARP enviada previamente, la información de la dirección de la respuesta es almacenada en la caché. En los sistemas Windows los atacantes pueden incluso

Direcciones de la LAN: Conceptos Básicos

Si dos ordenadores en una red quieren charlar, necesitan una forma de identificación entre ellos unívoca. Ethernet utiliza un número de 48-bit (6 byte), que es asignado por el fabricante. La denominada dirección MAC (Control de Acceso al Medio) es única en el mundo. Esto permite a los usuarios añadir (más o menos) tantos adaptadores Ethernet como quieran a la LAN. Sin switches o bridges Ethernet usa broadcasting; esto es, cada paquete en el cable se envía a cada nodo de cada segmento de la red. Pero solo el destino pretendido aceptará el paquete, mientras todos los otros nodos lo ignorarán.

Esta solución es sorprendentemente fácil, pero no se adapta bien en diversos entornos. Todo el que esté conectado al medio común comparte el ancho de banda. Los bridges y los switches reducen la situación dividiendo la red en múltiples segmentos y aprendiendo qué direcciones MAC están disponibles a través de los puertos (tabla CAM, Content Addressable Memory). Esto permite a estos dispositivos transmitir paquetes sólo a los segmentos donde se encuentra la máquina destino. Sin cada segmento, los nodos de la red pueden enviarse paquetes unos a otros sin interferencias con comunicaciones en otros segmentos.

Este principio no es aplicable a todas las redes. Cada switch necesita conocer el entorno que le rodea. Para manejar esto, los creadores de Internet presentaron un esquema de direcciones basados en las direcciones IP. Las direcciones IP tienen una longitud de 32 bits (4 bytes) y comprende una red y una sección de host. La máscara de red le dice qué parte de las direcciones se refiere a la red y qué parte identifica al host.

Las redes individuales que forman Internet están conectadas por routers. Los routers sólo necesitan conocer direcciones de red para enviar paquetes de forma correcta. Mientras se asignan direcciones IP, la LAN continua utilizando sólo direcciones MAC. Pero sería un inconveniente para cada programa que necesite conocer ambas direcciones IP y las direcciones MAC. Aquí es donde ARP (Address Resolution Protocol) puede ayudar proporcionando la dirección MAC que coincida con una dirección IP. El administrador no necesita configurar esto – es decir, no hay necesidad de configurar las coincidencias entre direcciones IP/MAC. Como parte negativa, la automatización lleva a un gran problema de seguridad, que discutiremos con más detalle en este artículo.

Junto con ARP, también está RARP (Reverse ARP, [3]). De forma similar a DHCP, un servidor RARP asigna una dirección IP a una máquina basada en el conocimiento de la dirección MAC del equipo. Como RARP no pasa ningún otro parámetro (nombre del servidor, dirección del gateway, máscara de red), hoy en día es muy extraño usarlo.

modificar entradas declaradas por los usuarios como estáticas.

Realizando esto se permite que un atacante monitorice el diálogo entre un cliente y un servidor y utilizando la técnica del "hombre de en medio", manipule el diálogo. El hombre en medio manipula las entradas del servidor en caché ARP del cliente, haciendo creer al cliente que la dirección MAC del atacante es en realidad la dirección del servidor. El mismo truco se usa para el servidor.

Si el cliente quiere hablar con el servidor, comprobará su tabla ARP manipulada y enviará el paquete a la dirección MAC del atacante. Esto permite al atacante leer y modificar el paquete antes de reenviarlo al servidor. Entonces el servidor supone que el paquete fue enviado directamente por el cliente. La respuesta del servidor de nuevo va al atacante, que la reenvía al cliente. Si el servidor reside en otra subred, el atacante tan solo tiene que lanzar su ataque contra el router.

Desde luego, un atacante puede provocar una denegación de servicio simplemente descartando cualquier paquete recibido. Para manipular los datos, el atacante simplemente tiene que reenviar datos diferentes a los que reciba. Los atacantes pueden fácilmente recolectar contraseñas, ya que el número del puerto les permite averiguar el protocolo usado e identificar las credenciales del usuario basándose en este conocimiento.

Precaución incluso con SSL y SSH

Las conexiones encriptadas no son automáticamente inmunes, como demuestran diversas herramientas ARP. Estos programas están ahora disponibles para varios sistemas operativos (véase el cuadro titulado "Exploits para ARP").

Además de la funcionalidad de ARP poisoning, incluye implementaciones para clientes y servidores de SSL (Secure Socket Layer), TLS (Transport Layer Security), SSH (Secure Shell) o PPTP (Point to Point Tunneling Protocol).

Accediendo a un servidor web SSL, el navegador alerta al usuario que algo va mal con el certificado para la conexión. Pero hay muchos usuarios que no comprenden la importancia de la alerta y simplemente la ignoran. El hecho de que muchos servidores usen un certificado generado por ellos mismos hace que dichas alertas sean relativamente frecuentes; de hecho, se suele hacer clic y simplemente ignorar el mensaje. Un error en algunas versiones del navegador Internet Explorer hace que sea posible atacar las conexiones SSL sin que el navegador ni siquiera muestre la alerta.

El ataque a SSH sigue un patrón similar (Figura 4). Si el cliente ya conoce la clave del lado del servidor, mostrará un mensaje claro (Figura 5). Pero muchos usuarios y administradores ignoran el aviso, suponiendo que alguien ha cambiado la clave del servidor. Pocos protocolos o implementaciones son inmunes. (IPsec es una excepción. IPsec rehúsa trabajar si algo va mal con el proceso de autenticación).

A causa de este problema, casi cualquier clase de comunicación interna es vulnerable. Hay incluso herramientas

Herramientas de Explotación ARP

A continuación nombraremos algunos programas que permiten a los atacantes explotar las vulnerabilidades de ARP. Los administradores pueden utilizar estas herramientas para testear sus propias redes. Son bastante útiles para demostrar la severidad de los ataques ARP. El problema de seguridad real, por supuesto, no es el hecho de que estas herramientas existan, ya que ARP es relativamente inseguro.

ARP-SK: Los programadores describen sus herramientas como una Navaja Suiza para ARP; está disponible para versiones Unix y Windows. El programa puede manipular las tablas ARP en varios dispositivos. *http://www.arp-sk.org*

Arpoc y WCI: Este programa para Unix y Windows realiza un ataque tipo hombre de en medio en la LAN. Contesta a cada petición ARP que alcanza la máquina con una respuesta ARP manipulada y reenvía cualquier paquete de entrega no local al router apropiado. *http://www.phenoelit.de/arpoc/*

Arpoison: Una herramienta de línea de comandos que crea un paquete ARP manipulado. El usuario puede especificar la fuente y la dirección IP/MAC de la tarjeta. *http://arpoison.sourceforge.net*

Brian: Esta herramienta extremadamente simple (comprendido en un sólo fichero C) utiliza ARP poisoning para deshabilitar las interconexiones en la LAN. Esto permite a un atacante fisgonear todo el tráfico en la red. *http://www.bournemouthbynight.co.uk/tools/*

Cain & Abel: Este sofisticado software de Windows comenzó como una herramienta de recuperación de claves. Fisgonea la red y utiliza una variedad de técnicas para descifrar claves encriptadas. La versión 2.5 de la herramienta fue la primera en introducir ARP poisoning, que permite a los atacantes fisgonear el tráfico IP en la LAN. El programa ataca conexiones SSH y HTTPS. *http://www.oxid.it/cain.html/*

Dsniff: Los programas individuales en esta suite de herramientas llevan a cabo distintas tareas. Dsniff, Filesnarf, Mailsnarf, Msgsnarf, Urlsnarf y Webspy fisgonean la red y cogen datos interesantes (como claves, correos y ficheros). Arpspoof, Dnsspoof y Macof permiten a los administradores y atacantes acceder a datos que un switch normalmente protege. Sshmitm y Webmitm soportan el ataque hombre de en medio en SSH y HTTPS (aunque el autor se refiere a ellos como ataques Monkey in the Middle). *http://naughty.monkey.org/~dugsong/dsniff/*

Ettercap: Un potente programa con una interfaz basada en texto (ver Figura 4); la última versión también tiene un interfaz Gtk. Las acciones se realizan automáticamente, con la herramienta se muestran tarjetas potenciales en una ventana. Junto a Sniffing, los ataques ARP y la obtención de claves automáticas, Ettercap también puede manipular datos sin una conexión. El programa también ataca conexiones SSHv1 y SSL (utilizando las técnicas del ataque del hombre de en medio). *http://ettercap.sourceforge.net*

Hunt: Las conexiones fallidas, fisgoneo de datos y secuestro de sesiones. La herramienta utiliza manipulación ARP y otras técnicas. *http://packetstormsecurity.nl/sniffers/hunt/*

Juggernaut: En 1997, Phrack Magazine publicó Juggernaut, el predecesor de la mayoría de los sniffers actuales con capacidad para manipular la caché ARP. *http://www.phrack.org/show.php?p=50&a=6*

Parasite: El servicio Parasite fisgonea la LAN y responde a peticiones ARP con respuestas ARP manipuladas. La herramienta permite gradualmente a la máquina establecerse por sí misma como un hombre de en medio para cualquier comunicación en la red. *http://www.thc.org/releases.php*

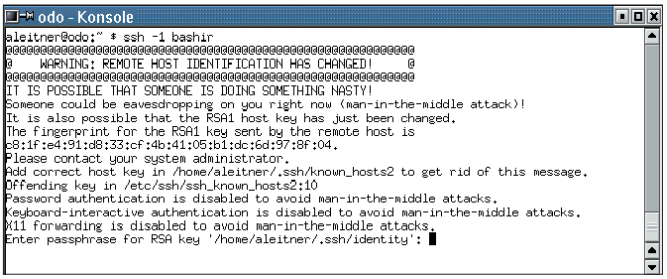

Figura 5: Durante el ataque Ettercap (Figura 4), el cliente (odo en este ejemplo) recibe una clave modificada del servidor. La clave proviene del atacante y no del servidor solicitado (bashir). Si el usuario escoge ignorar la advertencia, la conexión será fisgoneada.

para novatos que pueden obtener contraseñas de unos 50 protocolos. Como este ataque sucede a nivel ARP y normalmente tan solo los accesos IP son registrados los atacantes de hoy en día se sienten bastante seguros ya que nadie se percatará de que ellos están al acecho.

Impidiendo los ataques ARP

Una posible solución para impedir los ataques ARP sería imposibilitar la descarga y ejecución de software externo, aunque esta regla es extremadamente difícil de llevar a cabo. Los administradores tendrían que restringir el uso de la conexión a Internet. HTTP, HTTPS, FTP y el correo electrónico hacen que le sea fácil a un atacante infiltrarse dentro de la red software dañino. Los administradores tendrían también que prohibir el uso de disquetes, CDs, además de dispositivos móviles como portátiles y PDAs. Debido a las restricciones de uso, esta solución es inviable.

Si se usa Linux en la red interna y no se le da a los usuarios los permisos de root, se pueden evitar la mayoría de los ataques: los usuarios necesitan los privilegios de root para enviar paquetes ARP dañinos. Sin embargo, como administrador, no se tiene una forma efectiva de impedir que los usuarios arranquen sus máquinas desde un CD o que conecten sus portátiles a la red.

Las entradas ARP estáticas pueden ayudar a impedir los ataques ARP, pero la mayoría de los administradores querrán evitar el esfuerzo titánico que supone el asignar las direcciones manualmente para todas las máquinas. Como el sistema operativo de Microsoft permite a los atacantes manipular incluso las entradas ARP estáticas asignadas manualmente, conseguir un entorno seguro es realmente difícil.

Esta solución tan sólo tiene sentido en pequeñas redes, ya que el número de entradas ARP crece proporcionalmente al cuadrado del número de adaptadores de red. Dicho de otro modo, harían falta 9900 entradas para un sistema con cien máquinas (99 para cada uno de ellos). Esto implica un enorme esfuerzo de administración, especialmente si se tienen que resolver problemas de red.

Echándole un ojo

Arpwatch [4] es una herramienta de código abierto para plataformas UNIX

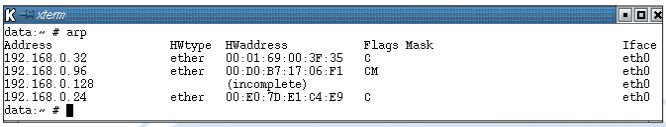

Figura 3: La tabla ARP en un sistema Linux con una entrada incompleta, una entrada estática y dos entradas dinámicas (C: completa, M: estática).

que monitoriza las actividades ARP inusuales. La máquina que ejecuta Arpwatch lee la información de direccionamiento almacenada en cada paquete ARP que pasa por ella y almacena esta información en una base de datos. Si el dato no coincide con las entradas ya almacenadas, Arpwatch envía un correo al administrador avisándole. El autor dice que la herramienta soporta SNMP, aunque nos ha resultado imposible confirmarlo en nuestro laboratorio.

Actualmente, la mayoría de las redes usan direcciones IP dinámicas asignadas por DHCP (Dynamic Host Configuration Protocol). En esta clase de entornos, Arpwatch devolverá gran cantidad de avisos de falsos positivos ya que avisará de cualquier cambio producido por las direcciones IP/MAC.

ARP-Guard [5], un producto reciente de ISL, funciona dentro del marco de una arquitectura gestionada por sensores. Múltiples sensores monitorizan la información ARP y envían dicha información al sistema de gestión, que analiza los mensajes y alerta a los administradores en el caso de que se produzca un ataque. Esta arquitectura hace que ARP-Guard se adapte bien tanto en redes pequeñas como en grandes redes y el interfaz basado en web que dispone hace que sea apreciado por los administradores.

ARP-Guard tiene sensores LAN y SNMP. Los sensores LAN funcionan como Arpwatch o cualquier sistema IDS, analizando cualquier paquete ARP que el sensor lea. Por el contrario, el sensor SNMP usa el protocolo SNMP para conectarse a los dispositivos existentes y preguntarle por sus tablas ARP.

Los sistemas de detección de intrusos, IDS, (véase el cuadro titulado "Snort y ARP") también son capaces de detectar ataques ARP, pero normalmente se instalan en las fronteras de la red. Pero a muchos negocios, simplemente no les vale la pena instalar un IDS en la red interna. Además, los empleados podrían sentir que están dentro del "Gran Hermano" bajo la mirada del administrador de la red. El administrador puede ver todo el tráfico de la red y además monitorizar el acceso de la plantilla. La utilidad de esta solución es cuestionable, como la mayoría de los sistemas IDS simplemente ignoran el tráfico ARP. Y por último, el sistema al completo podría colapsar al enfrentarse a ataques de tipo ARP poisoning en combinación con la asignación dinámica de direcciones IP.

La criptografía al rescate

Los protocolos criptográficos (IPsec sobre todo) se aseguran de la confidencialidad, autenticidad e integridad de los datos, los ataques ARP se reducen simplemente a una denegación de servicios. Cualquier intento de fisgonear o manipular los datos fracasarán. Sin embargo, pasará algún tiempo hasta que IPsec y otros protocolos criptográficos se instalen y configuren correctamente dentro de las redes internas.

Hay un grupo de investigadores que solicitan que ARP sea reemplazado con una versión más segura [7]. S-ARP se basa en criptografía, un CA (Autoridad de Certificación) y mensajes ARP firmados digitalmente. Sin embargo, se cuestiona si vale realmente la pena: IPsec proporciona mucha más protección con el mismo esfuerzo, donde S-ARP tan solo protege ARP. Lo único que ARP tiene a su favor es que implica menor sobrecarga de CPU en los sistemas.

Otras técnicas de Prevención

Agunos fabricantes de cortafuegos y routers sostienen que sus productos son capaces de detectar ataques ARP spoofing, pero estrictamente esto no es verdad ya que estos sistemas tan solo pue-

Snort y ARP

Snort [6] es un ejemplo sobresaliente de lo que es un IDS para redes. Este sistema de detección de intrusiones ayuda a los administradores a detectar ataques en una red en una fase temprana, permitiendo implementar contramedidas. Snort dispone de un preprocesador Arpspoof con cuatro mecanismos de detección.

- Para cada petición ARP que detecta, el preprocesador Arpspoof valida la dirección fuente en el cuadro Ethernet contra la dirección fuente el paquete ARP. Si ambas direcciones no coinciden, emite una advertencia. El envenenamiento ARP no implica la utilización de direcciones diferentes en estos campos, por lo que no se detectaría un ataque en todos los casos.
- Para respuestas ARP, se lleva a cabo una comparación de direcciones fuente y destino. Si una de estas comparaciones no coinciden, Snort emite una advertencia. Como en el caso anterior, esto no detectaría envenenamiento ARP *per se*, aunque sí Proxy ARP. Por otro lado, esta técnica a menudo es legítima e involucra una máquina que contesta peticiones ARP en delegación de otra máquina.
- El sistema alerta en el caso de peticiones ARP que se envían a direcciones unicast en vez de a broadcast. Aunque este comportamiento no se conforma al estándar (que tiene más de 20 años), existen buenas razones para ello. Sin embargo, un auténtico ARP no necesita "unicastear" peticiones, por tanto, al igual que más arriba, este mecanismo podría fallar a la hora de detectar una ataque de envenenamiento.
- Snort comprueba todos los paquetes ARP basándose en una lista de direcciones IP y MAC proporcionadas por el administrador. Si la dirección IP está en la lista, el IDS leerá su correspondiente dirección MAC de la lista y la comparará con la dirección MAC del paquete y del cuadro Ethernet. En el caso de discrepancia, Snort emite una advertencia. Este mecanismo sólo es útil para redes pequeñas, al ser el esfuerzo de configuración demasiado grande en otros casos. No hay ninguna manera de utilizar esta funcionalidad de manera consistente con asignación dinámica de direcciones (DHCP).

En otras palabras, la capacidad de Snort para la detección de envenenamiento ARP es limitada, al igual que en el caso de otros Sistemas de Detección de Intrusiones.

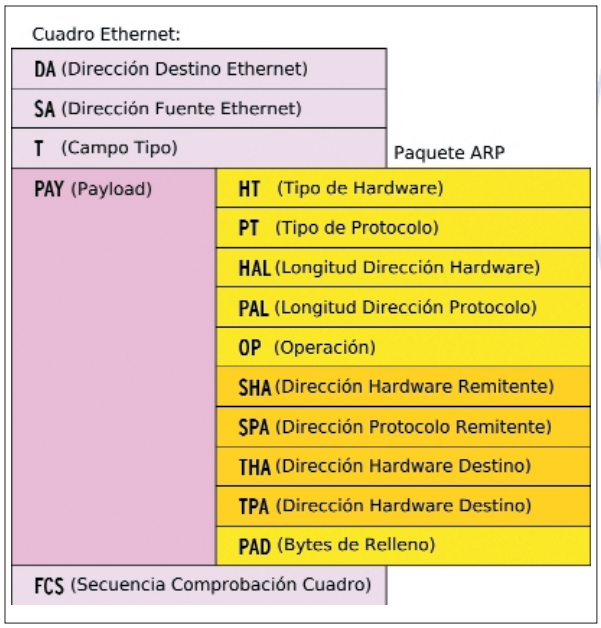

Figura 2: Un paquete ARP se transmite como contenido de la trama Ethernet. Los campos con el tipo y la longitud de las direcciones en cada paquete son seguidos por el código y los datos de destino.

den detectar y registrar modificaciones de sus propias tablas ARP y no tienen forma de saber si el cambio se ha producido por una causa legítima.

Dividir la red en un gran número de subredes y asignar un pequeño número de usuarios a cada subred puede ayudar a limitar la exposición a ataques ARP. Los switches, que permiten a los administradores manejar el tráfico de red, proporcionan protección contra ataques ARP y sirven también para gestionar el tráfico. Como contrapunto, esta clase de switch es caro, aumenta el volumen de trabajo de los administradores y pueden tener el efecto de bloquear algunas aplicaciones.

Algunos desarrolladores intentan añadir protección a la pila IP en los dispositivos terminales. El parche Antidote [8] le indica a una máquina Linux que envíe una solicitud a la dirección MAC previa antes de cambiar una entrada ARP. La máquina sólo cambiará la entrada si la solicitud a la dirección previa no es respondida. De nuevo, esta solución no proporciona ninguna protección real frente al sabotaje. El atacante puede simplemente asegurarse de que el ataque suceda cuando la máquina con la dirección MAC previa esté apagada o sea inalcanzable. En el caso de que haya bastante sobrecarga o que se tenga una solución de balanceo de carga, el parche puede causar que la comunicación a estos sistemas falle.

Otra alternativa para protegerse contra ataques ARP poisoning es impedir el reasignamiento de direcciones MAC-IP existentes. El parche Anticap [9] implementa este comportamiento para Linux, FreeBSD y NetBSD. Solaris tiene una opción similar, que requiere que un temporizador expire antes de aplicar el cambio. Este comportamiento se puede configurar libremente, sin embargo, una solución como el parche Anticap solamente protege sistemas que están encendidos permanentemente y los atacantes no tendrán ningún problema de manipular las entradas nuevas una vez que las entradas en la caché hayan expirado.

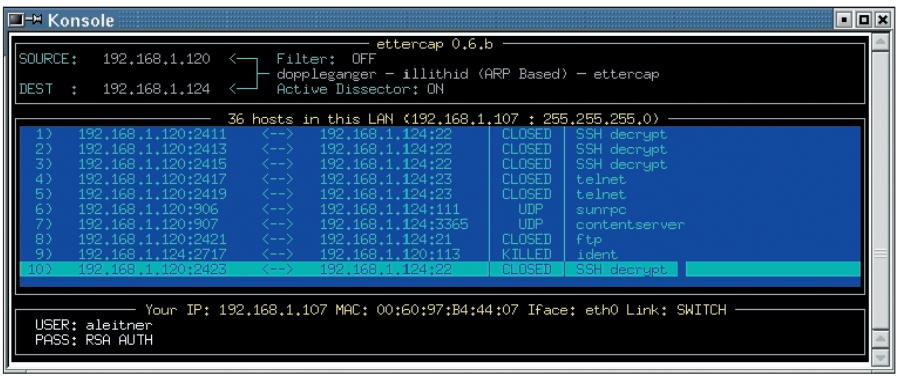

Figura 4: Ettercap esperando para una conexión entre 192.168.1.120 y 192.168.1.124 (fuente y destino, arriba a la izquierda). La herramienta puede fisgonear telnet y FTP. Utiliza un ataque tipo hombre de en medio en SSHv1 para desencriptar la conexión.

El kernel 2.4 de Linux o posteriores ya no reaccionan frente a respuestas ARP no solicitadas. Desafortunadamente, este mecanismo se puede saltar fácilmente, como explica el fichero *readme* de Ettercap. El kernel siempre tiene que procesar las solicitudes ARP. Como al kernel se le pasa una combinación de dirección IP y dirección MAC (de la fuente), añade estos datos a su caché ARP. Así que el atacante tan solo tiene que enviar una solicitud ARP manipulada. Ettercap envía una combinación de solicitud y respuesta, y cualquier sistema responderá a una de estas técnicas.

La protección incorporada dentro de la pila IP es menos potente para impedir el ARP spoofing. Si un atacante responde a una solicitud ARP más rápido que la máquina a la que realmente se le está enviando la solicitud, el atacante gana la carrera y su dirección es la que se añade a la tabla ARP.

Sin protección

Las técnicas actuales no pueden proporcionar una protección completa frente a ataques ARP, pero puede armarse con sistemas IDS y sensores especializados en la manipulación ARP para detectar la mayoría de los intentos. Para estar completamente seguro, hay que instalar IPsec en la red. Ignorar el problema no es una buena solución a menos que se tenga una confianza plena en todos los usuarios que accedan a la red. ■

RECURSOS

[1] Encuesta KPMG: *http://www.kpmg.com/about/press.asp?cid=469*

[2] Address Resolution Protocol, RFC 826: *http://www.ietf.org/rfc/rfc826.txt*

[3] Reverse ARP, RFC 903: *http://www.ietf.org/rfc/rfc903.txt*

[4] Arpwatch: *http://www-nrg.ee.lbl.gov* y *http://www.securityfocus.com/tools/142*

[5] ARP-Guard: *https://www.arp-guard.com*

[6] Snort: *http://www.snort.org*

[7] Secure ARP: *http://security.dico.unimi.it/research.en.html#sarpd* y *http://www.acsac.org/2003/papers/111.pdf*

[8] Parche Antidote: *http://www.securityfocus.com/archive/1/299929*

[9] Parche Anticap: *http://cvs.antifork.org/cvsweb.cgi/anticap/*