



Utilizamos herramientas de monitorización de ARP para buscar intrusos en nuestra red local

# Estrecha Vigilancia

Seguramente tenga el lector un cortafuegos, pero ¿qué pasa si el intruso actúa desde dentro? Estas herramientas de monitorización de ARPs son capaces de detectar el más mínimo cambio y alertarnos de un posible ataque local. **POR CHRIS BINNIE**

**E**quipos de desarrollo de todo el mundo trabajan duro para que el software de nuestros sistemas esté siempre lo más actualizado posible. Además, los cortafuegos impiden que los atacantes accedan a nuestros sistemas y redes desde Internet. ¿Pero qué pasa si el ataque se produce desde dentro de la red local?

Uno de los requisitos de casi cualquier red local es la asignación de direcciones IP. Con el fin de comunicarse con la red de una manera funcional (que no sea, por ejemplo, recolectar datos desde una conexión inalámbrica), los potenciales intrusos deben asignarse primero una dirección IP dentro de la red. Esto es común tanto a redes cableadas como a inalámbricas. Dicha IP podría ser una dirección libre o incluso una que ya esté siendo usada por otro dispositivo.

Si el atacante se asigna una IP en uso, suele ser porque planea hacer algún tipo de espionaje o una redirección de servicios. Bajo ciertas circunstancias, podría tratar de hacer creer al resto de equipos

que él es alguna máquina de la red. Dicho de otro modo, el atacante clona la dirección MAC que en teoría es única para cada tarjeta de red y que siempre es la misma. Aquellos ataques en los que el intruso se asocia una dirección IP existente con el fin de filtrar y suplantar las comunicaciones se denomina comúnmente MITM o *Man-In-The-Middle*, porque el atacante se sitúa entre las máquinas que intervienen en la comunicación a espiar. Redirigir un servicio puede ser tan sencillo como alterar una entrada de dirección MAC en una máquina para hacerle creer que su servidor de nombres es otro; cuando la máquina engañada quiera acceder al sitio web de su entidad bancaria, resolverá su dirección IP usando un servidor de nombres malicioso y acabará,

por tanto, visitando un sitio falso y proporcionando sus datos personales al atacante.

Lo ideal sería que no sólo supiéramos cuándo ha cambiado la dirección MAC asociada a una dirección IP, sino además saber cuándo se ha asignado una nueva IP.

En este artículo presentamos varias herramientas útiles con las que, mediante el uso del protocolo ARP (*Address Resolution Protocol*), podremos conocer los cambios producidos sobre las asignaciones de la red local.

## Arpwatch

Arpwatch es una herramienta sencilla que vigila las direcciones IP de la red y analiza cambios sospechosos. ARP construye una tabla que contiene las correspondencias entre los dispositivos de la red y las direcciones IP que usan, pre-

### Arpwatch - New Station

★ Chris Binnie

```
hostname: inkjet-printer
ip address: 192.168.1.223
interface: eth1
ethernet address: 00:15:af:18:29:f5
ethernet vendor: AzureWave Technologies, Inc.
timestamp: Thursday, January 27, 2012 14:55:38 +0000
```

Figura 1: El log de Arpwatch proporciona detalles simples sobre cada evento.

La diferencia

entre esto...

guntando a cada dispositivo de la red “¿Quién usa tal dirección IP?” hasta que alguno responda “Yo tengo esa dirección IP”. Su simplicidad hace que sea fácil de depurar, pero también propenso a abusos, como por ejemplo los ataques MITM mencionados anteriormente.

Arpwatch monitoriza las respuestas ARP en busca de cambios y envía un email al administrador en caso de que ocurra algo sospechoso. Además de proporcionar una forma sencilla de auditar el número de direcciones IP en uso en una red, es un sistema de detección temprana que se puede configurar para que escuche en varias interfaces a la vez (tanto de cable como inalámbricas).

Cabe aclarar que en algunas redes se utiliza el falseamiento de ARP para redirigir legítimamente el tráfico con algún propósito concreto. Imaginemos por ejemplo un cibercafé en el que, hasta que el sitio nos da paso, se redirige a todo el mundo a una página con la política de uso o las condiciones del local.

Mediante el seguimiento de los dispositivos de la red con un archivo de logs por interfaz, donde guarda la información relativa a cuándo y qué dirección IP se asignó a cada dirección MAC, Arpwatch hace fácilmente accesible una información que de otro modo pasaría prácticamente desapercibida.

Los logs de Arpwatch guardan las direcciones MAC, las direcciones IP asociadas, las marcas de tiempo de las últimas actividades, los nombres de dispositivo (alias o nombres DNS), y las interfaces desde las que se observó dicha actividad. En la Figura 1 se muestran en detalle los logs generados por Arpwatch.

Las notificaciones que Arpwatch envía por email pueden alertar al usuario casi al instante. Los informes están bastante limpios y se podrían, por tanto, formatear como mensajes SMS (mensajes de texto) si fuese necesario. En la Figura 2 se puede apreciar la brevedad de dichos emails de notificación.

El primer segmento de una dirección MAC se suele corresponder (aunque no siempre) con la identificación del fabricante o el distribuidor de la tarjeta de red, que se pueden consultar fácilmente mediante bases de datos en línea. También existe una asignación formal de estos identificadores en la IEEE [1], pero no es tan práctico. A través de esta tabla se facilita la identificación de los dispositivos desconocidos, minimizando el número de falsas alarmas.

Una vez sepa la dirección MAC del atacante y posiblemente si se trata de un portátil o smartphone, se pueden utilizar pistas de los datos del proveedor (siempre y cuando no hayan sido alterados) para trazar la actividad del dispositivo en la LAN. Incluso si cambia de dirección MAC, al menos se nos alertará de este hecho.

## Arping

La herramienta más típica a la hora de comprobar direcciones ARP duplicadas en la red local es Arping. Al igual que Ping, que envía peticiones y queda a la espera de que se

|                   |               |            |                  |
|-------------------|---------------|------------|------------------|
| 00:24:af:93:43:c5 | 192.168.1.254 | 1296140384 | wifi-router eth1 |
| 02:51:02:43:06:08 | 192.168.1.34  | 1296140384 | unknown eth1     |
| 00:1a:af:81:19:e0 | 192.168.1.223 | 1296140138 | printer eth1     |

Figura 2: Los hechos: notificación de Arpwatch por correo electrónico.



... y esto...



... es el especial  
MIGRACIÓN de  
Linux Magazine.

# Win2Lin

Especial migración  
a la venta en abril en  
quioscos y tienda de

**LINUX**  
MAGAZINE

[www.linux-magazine.es/tienda](http://www.linux-magazine.es/tienda)

```

ARPING 192.168.1.65 from 192.168.1.123 eth0
Unicast reply from 192.168.1.65 [00:01:27:af:d7:4a] 0.114ms
Unicast reply from 192.168.1.65 [00:01:27:af:d7:4a] 0.105ms
Unicast reply from 192.168.1.65 [00:01:27:af:d7:4a] 0.202ms
Unicast reply from 192.168.1.65 [00:01:27:af:d7:4a] 0.103ms
Sent 4 probes - Received 4 response(s)

```

Figura 3: Si las respuestas son idénticas, no hay duplicidades en la red.

## Rendimiento de ArpON

ArpON ha sido diseñado con el objetivo de ser eficiente, de ahí que no sea demasiado opulento en lo que a funcionalidades se refiere. Existe una herramienta alternativa, llamada S-Arp (ARP Seguro), que añade una capa de cifrado para proporcionar una mayor seguridad, pero que ralentiza el protocolo ARP al incrementar las necesidades de procesamiento e inyectar datos extra en el flujo de datos.

produzca una respuesta, Arping envía sus peticiones a la red local (o dominio de difusión). Algunas implementaciones de Arping, además de simplemente preguntar por la dirección MAC de una dirección IP determinada, pregunta también a la inversa, es decir, qué dirección IP tiene una dirección MAC dada.

Esa funcionalidad extra que posee Arp de comprobar a la inversa es de vital importancia en ciertos escenarios de ataque. En el siguiente ejemplo se le pide a Arping que busque duplicidades relativas a una dirección IP:

```
arping -d 97.98.99.100 -I eth1
```

Combinada con las alertas emitidas por Arpwatch, para informarnos de los cambios ocurridos en la red, esta herramienta nos dice si hay dispositivos que comparten una misma dirección IP (que pueden derivar en fallos de conexión o en intentos de ataques MITM). El comando anterior envía cuatro peticiones a través de la interfaz de red *eth1*, preguntando “¿Quién tiene esta dirección IP?” y queda a la espera de respuestas. En la Figura 3 se muestran cuatro respuestas idénticas que indican que sólo hay una única dirección MAC asociada a esa dirección IP y que, por tanto, no hay duplicidades en la red.

## ArpON

Ahora que ya sabemos cómo detectar ataques ARP y recibir informes, cabe

preguntarse si existe alguna otra herramienta capaz de ofrecer un método más sofisticado y automatizado para combatir este tipo de ataques localizados.

La herramienta se llama ArpON, que significa *Arp handler InspectiON*.

Mientras que Arpwatch sólo informa de los problemas detectados, relegando al usuario las acciones a llevar a cabo, ArpON ha sido diseñado para automatizar la resolución de los problemas siguiendo una serie de políticas predefinidas. En el sitio web de ArpON [2] se pueden conocer todos los detalles del paquete, incluidos varios diagramas, muy útiles para los principiantes.

Además de sus capacidades de monitorización básica de ARP, ArpON cuenta con más munición en su arsenal. Por ejemplo, en las sesiones de ArpON también se pueden detectar automáticamente y resolver interceptaciones de sesiones o el secuestro de conversaciones web o de correo electrónico.

ArpON mantiene la pizarra siempre bien limpia, creando una caché fresca de entradas ARP desde el principio, eliminando así la posibilidad de corromper la caché de ARP con información falsa o engañosa (a este tipo de ataque se le conoce como envenenamiento de la caché ARP). A diferencia de otras herramientas de monitorización de ARP, ArpON impide activamente que se actualicen nuevas entradas sin una entrada de confianza en su caché, ignorando esencialmente todo lo demás y evitando así el ataque incluso antes de que comience.

Hay tres niveles de despliegue de ArpON. El despliegue de un nodo de monitorización en un dispositivo puede proporcionar protección unidireccional, mientras que un demonio instalado puede tomar la caché de ARP y contrastar los cambios con efectividad. Para una protección bidireccional hacen falta al menos dos nodos de monitorización, posibilitando la interceptación de tráfico entre ambos nodos, de manera que se pueda descifrar el tráfico del ataque y reaccionar en consonancia. Para que pueda funcionar en modo de protección distribuida se debe instalar ArpON en todos los dispositivos de la red. Cabe

aclarar que en este caso quedarán desprotegidos todos los dispositivos que no estén ejecutando ArpON, por lo que este modo de funcionamiento probablemente sólo sea adecuado para pequeñas redes de dispositivos homogéneos, como por ejemplo una pequeña red (o subred) de un clúster o de servidores de correo.

ArpON cuenta con un diseño no-invasivo, tratando de no alterar el protocolo ARP, que fue creado teniendo en mente unas redes de datos muy antiguas y que se podría mejorar para lidiar con los ataques de hoy en día. Independientemente de los problemas inherentes a ARP, éste cuenta con un rendimiento muy alto debido a su simplicidad, rendimiento que no se ve alterado tampoco por ArpON. ArpON es útil también en redes gestionadas por DHCP, donde los dispositivos obtienen una dirección IP cada vez que acceden a la red.

También existe la posibilidad de deshabilitar partes de ArpON para crear un laboratorio de pruebas propio con el que realizar ejercicios interesantes.

## Conclusión

ArpON está actualmente disponible para Linux, Mac OS X, FreeBSD, NetBSD y OpenBSD, pero aún no ha sido portado a Windows. Existen herramientas parecidas para Windows y otros sistemas operativos. Para Windows, hay un producto llamado WinARP Watch. Para Linux, Unix y BSD – también está Arpalert. Cada una de estas alternativas varía en cuanto a funcionalidades. Aunque Arpwatch es excelente, ninguna otra herramienta llega al nivel de sofisticación de ArpON.

Conjugadas con los conocimientos de un administrador experimentado, las herramientas de monitorización de ARP suponen un medio potentísimo, incluso con la función de bloqueo automático de ataques deshabilitada. Estas herramientas, con el nivel de detalle de sus informes, ofrecen una capa adicional de seguridad y protección tanto para redes domésticas como para redes industriales. ■

## RECURSOS

[1] Relación entre direcciones MAC y fabricantes: <http://standards.ieee.org/develop/regauth/oui/oui.txt>

[2] ArpON: <http://arpon.sourceforge.net>