

El Día a Día del Administrador de Sistemas: Arpalert

UNA MIRADA A ARP

Las políticas corporativas prohíben la conexión no autorizada de hardware a la red de la empresa, sobreviniendo las consecuencias oportunas en el caso de que no se cumplan. Parece razonable. Pero actualmente, ¿cómo se localiza a alguien que está intentando engancharse ilegalmente con un portátil a su red?

POR CHARLY KÜHNAST

MI elección como guardian es Arpalert [1]. Su creador, Thierry Fournier, recomienda enviar el siguiente conjuro para despertar a la bestia salvaje:

```
./configure --prefix=/usr/local
make
make install
```

Esta serie de comandos coloca al programa C en `/usr/local/sbin`, y al fichero de configuración `arpalert.conf` en `/usr/local/etc/arpalert`.

En Ningún Sitio como en Casa

Para mi primer experimento decidí utilizar una red que me proporciona la mejor visibilidad, vamos, la red de mi oficina en casa. Es fin de semana y mi mujer se ha ido a la biblioteca municipal, así que no debería de tener más de cuatro o cinco equipos en red. Hice lo siguiente para lanzar Arpalert:

```
/usr/local/sbin/arpalert
```

Luego me senté a ver qué pasaba. Rápidamente la herramienta supuso que quería utilizar `eth0`; buena elección, es el único adaptador de red del equipo. Si tienes más de un adaptador de red, debe-

```
calzone:/usr/local/sbin~ ./arpalert
Sep 17 11:43:56 arpalert: [./capture.c 101] Auto selected device: eth0
Sep 17 11:44:20 arpalert: seq=1, mac=00:26:54:0a:aa:0b, ip=10.0.0.150, type=new
Sep 17 11:44:21 arpalert: seq=2, mac=00:0F:3D:AB:71:74, ip=10.0.0.249, type=new
Sep 17 11:44:21 arpalert: seq=3, mac=00:04:00:F3:C7:39, ip=10.0.0.199, type=new
Sep 17 11:44:22 arpalert: seq=4, mac=00:50:8B:5E:A0:2C, ip=10.0.0.254, type=new
charly@calzone:~>
```

```
calzone:/home/charly # /usr/local/sbin/arpalert
Sep 17 11:55:21 arpalert: [./capture.c 101] Auto selected device: eth0
Sep 17 12:02:37 arpalert: seq=4, mac=00:08:54:3f:d5:3a, ip=0.0.0.0, type=new_mac
```

Figuras 1 y 2: Arpalert detecta las MACs de cuatro dispositivos (arriba). Las alarmas se saltan a las doce y dos minutos: una máquina desconocida se ha conectado (abajo).

rias ayudar a Arpalert a configurarlo con la opción `-i` para que apunte a la interfaz correcta.

Omití el parámetro `-d` del servidor, aunque esta opción es necesaria para monitorizar en su pantalla lo que Arpalert está haciendo. A partir de este punto es cuando empiezan a suceder cosas interesantes: mi perro guardián detecta las MACs de las cuatro máquinas en una rápida sucesión, incluyendo una impresora y un punto de acceso WLAN (ver Figura 1), escribiendo las direcciones en formato `MAC dirección IP` en `/usr/local/var/lib/arpalert/arpalert.leases`.

Como se trata de una red pequeña, me aseguré de que Arpalert había aprendido las direcciones importantes. Salí del programa y copié el fichero de direcciones, `arpalert.leases`, a `/usr/local/etc/arpalert/maclist.allow` antes de relanzar Arpalert. De ahora en adelante Arpalert mostrará un mensaje en la consola, o creará una entrada en el registro, si detecta una dirección que no está definida en `maclist.allow`.

Para probar esto reinicié uno de los equipos y me aseguré de que me alertara

de la presencia de un equipo nuevo (Figura 2). La dirección IP es 0.0.0.0, porque en este punto al servidor de DHCP aún no se le ha asignado ninguna. Utilicé la opción `-e` para indicarle a Arpalert que ejecutase un script. El script podría enviarme un correo electrónico o hacer algo un poco más drástico, como modificar mis reglas de filtros de paquetes.

Primeras Conclusiones

Arpalert funciona perfectamente en mi mini-red y estoy convencido que será utilizado por todos aquellos que posean redes pequeñas y muy seguras, como inalámbricas con una o dos docenas de equipos. En grandes entornos, sin embargo, precisará mucha más atención manual, aunque de todas formas funciona. Los segmentos y las VLANs probablemente tropezarán con Arpalert. ■

RECURSOS

[1] Arpalert: <http://www.arpalert.org>

SYSADMIN

Antivirus con SAMBA 58

Enseñamos como proteger una red Windows de malware desde un servidor SAMBA.

Optimización 62

Los mejores trucos para sacarle el máximo rendimiento a servidores web, de correo y de ficheros.