

Kismet, Aircrack-ng y Karmetasploit

SEGURIDAD SIN CABLES

Cómo encontrar, rastrear, romper y suplantar redes inalámbricas. **POR KURT SEIFRIED**

Quizá sea el lector uno de esos usuarios reacios que aún mantiene sus redes cableadas en vez de sumarse a la moda de comunicar los aparatos de casa de forma inalámbrica (como sus amigos, familiares, vecinos, etc.). Parece como si todo el mundo estuviese adquiriendo puntos de acceso de cuarenta euros y equipos portátiles, que para la mayoría son mucho más baratos y sencillos de operar que Ethernet. Aunque probablemente, después de leer este artículo, otros opten por cablear también sus redes.

Búsqueda de Redes Inalámbricas

A fin de comprobar qué hay de cierto en la aseveración de que las redes inalámbricas están de moda, lo primero que haremos será buscar redes inalámbricas. Una de las mejores herramientas para llevar a cabo esta tarea es *Kismet*, incluida en casi todas las distribuciones. Muchas distros traen una versión antigua (2008) de este programa, así que para empezar lo descargamos [1], lo descomprimos, ejecutamos el script *configure* y hacemos *make* y *make install*. Hay que tener en cuenta que *Kismet* necesita privilegios de root para ejecutarse, ya que se comunica directamente con el hardware, por lo que debemos ejecutarlo bien como root o bien mediante *sudo*, o también podemos instalarlo con *suid root* y añadir usuarios al grupo *kismet*. Aclaremos que cualquier usuario perteneciente a este grupo tendrá privilegios suficientes para tras-

tear las interfaces de red, por lo que hay que tener cuidado en este sentido.

```
cd /directorio/kismet-source/
./config
make
make dep
make install
```

Kismet consta de tres componentes principales: el robot, el servidor y el cliente. El robot captura el tráfico de red y lo envía al servidor, que puede estar ejecutándose en la misma máquina o en una remota. El servidor recopila y coteja los datos, mientras que el cliente se conecta a él y proporciona una interfaz basada en texto en tiempo real. Esta arquitectura permite tener varios sistemas, incluyendo puntos de acceso inalámbricos con firmware personalizado (como el WRT54G), y alimentar de datos todos ellos a un único servidor.

Para ejecutar *Kismet*, simplemente iniciamos *kismet_client*, el cual nos ofrece la opción de arrancar el servidor y comenzar con la recopilación de datos. Se crean entonces varios archivos, incluidos los de datos de GPS – que sirven para mapear redes a ubicaciones físicas en caso de disponer de GPS en el sistema –, los de red – que se muestran en un listado con las redes y clientes encontrados, el canal en que se encuentra cada uno de ellos y todos los detalles de configuración que se nos puedan pasar por la cabeza –, así como un archivo que es una captura en formato PCAP.

Cabe destacar que en caso de ejecutar *Kismet* con una sola fuente de captura (una sola tarjeta inalámbrica), éste tendrá que alternar entre los distintos canales para poder cubrirlos todos (once, doce, o trece canales, dependiendo del país en que se encuentre). De esta forma se detectan todas las redes disponibles pero se generan archivos de captura fragmentados, puesto que se recibe tráfico de una red, luego de otra, y así sucesivamente. La solución a este problema es sencilla: comprar más adaptadores inalámbricos (USB ya funciona muy bien) para añadir más interfaces de captura.

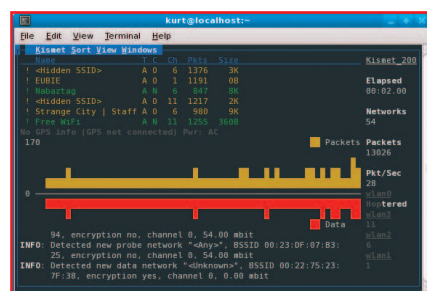


Figura 1: Cliente de *Kismet* con cuatro fuentes de captura.

Con cuatro fuentes ya se tiene un buen rendimiento. De ese modo podemos dedicar una tarjeta para cada canal principal (el primero, el sexto y el onceavo) y dejar la otra para alternar entre el resto de canales, asegurando por tanto que se descubrirán todas las redes y que se maximizará la cantidad de datos capturados (Figura 1). Para configurar *Kismet* basta con añadir las siguientes líneas al archivo *kismet.conf*:

```
channellist=hopl:2
2,3,4,5,7,8,9,10
ncsource=wlan0:hop=false,
channel=1
ncsource=wlan1:hop=false,
channel=6
ncsource=wlan2:hop=false,
channel=11
ncsource=wlan3:hop=true,??
channellist=hopl
```

En una prueba que hicimos, fuimos a una cafetería de la zona con *Kismet* y descubrimos, en pocos minutos, más de cuarenta

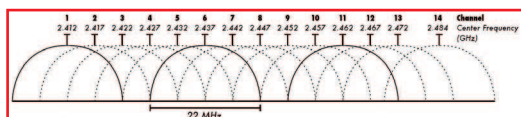


Figura 2: Diagrama de frecuencias por canales [10] (reproducido bajo la licencia CC-BY-SA [11]).

redes. En un segundo intento en otra cafetería más abajo en la misma calle pero desde un segundo piso, con una mejor visibilidad hacia el resto de edificios, cazamos más de setenta redes. Aproximadamente la mitad de ellas carecían de protección mediante cifrado. Muchas eran puntos de acceso por pago, mientras que algunas sólo tenían un cliente, probablemente porque se trataba de redes domésticas individuales. Lo más interesante es que podíamos capturar las direcciones MAC de clientes de redes de pago, siendo que la mayoría de esas redes filtran el acceso basándose en la dirección MAC del cliente una vez se autentica éste. Así, conociendo la dirección MAC adecuada, es posible acceder gratuitamente a este tipo de redes.

Evitando el Cifrado

Lo mejor que nos puede ocurrir al tratar de sobrepasar la protección de una de estas redes es que ni haga falta porque no esté protegida siquiera, como ocurre con la mitad de ellas. A la hora de acceder a una red cifrada, sin embargo, hay que recordar que los estándares de cifrado inalámbrico WEP y WPA son bastante débiles. La mayoría de las distribuciones incluyen Aircrack-ng [2], una herramienta para la averiguación de claves WEP y WPA. Para usarla, basta con ejecutar el programa *airoscrip*t, que nos proporciona una interfaz basada en texto. Los más vagos

Canales de Redes Inalámbricas

Aunque es posible enviar datos a través de hasta trece canales inalámbricos (once en América del Norte, doce en Japón y trece en la mayor parte del resto del mundo) [9], los canales se superponen ligeramente, lo que significa que sólo tres de ellos (el primero, el sexto y el onceavo) están separados realmente (Figura 2). Si una persona difunde datos en el primer canal y otra lo hace en el segundo, ambas compartirán parte de la frecuencia, pudiéndose producir colisiones, así como otros problemas que podrían reducir el ancho de banda disponible. Por este motivo, la mayoría de las redes inalámbricas están presentes en los canales primero, sexto y onceavo.

pueden escoger la opción *auto*, con la que el programa seleccionará y atacará una red automáticamente.

Ataque a Clientes Inalámbricos

Es mucha la gente que se centra en proteger su infraestructura inalámbrica (cifrado, control de acceso, etc.) pero se olvida de los clientes. Estando dentro del radio de acción de una red inalámbrica, podemos hacernos pasar por un punto de acceso legítimo y convencer a los clientes de éste para que se conecten a nosotros. Entonces, podemos conectar nuestra propia máquina al punto de acceso real, haciendo de proxy y modificando el tráfico que pase por nosotros. Este ataque se conoce como “punto de acceso pícaro” (*rogue access point*). Se puede implementar con la herramienta Karmetasploit, anteriormente llamada *Karma* y actualmente integrada en el proyecto *Metasploit*. En un artículo anterior de esta publicación [3] se explica cómo descargar e instalar Metasploit. Una vez instalados Metasploit y Aircrack-ng, simplemente se habrá de ejecutar un servidor de DHCP y asociarlo a la interfaz inalámbrica, de manera que los clientes puedan obtener la información necesaria para la configuración de su interfaz de red. Luego, ejecutamos Metasploit con los módulos *server* – para llevar a cabo ataques de *man-in-the-middle* – y *autopwn* – para inyectar contenidos maliciosos en páginas web (véase la documentación de Karmetasploit [4]). También se puede usar un proxy web transparente y tener un poco de diversión [5].

Cifrado Inalámbrico

Incluso en redes inalámbricas dotadas de algún tipo de cifrado sólido, la contraseña usada para asegurar la red se ha de compartir por todos los clientes inalámbricos. Por ello, cualquiera que gane acceso a la red en un momento determinado obtendrá una copia de dicha contraseña. En redes de gran tamaño, hay bastantes posibilidades de que la contraseña acabe siendo pública. A modo de anécdota, decir que la primera cafetería de las dos que visitamos tenía la contraseña impresa en un cartel sobre la caja. Esto es motivo más que suficiente para asegurarnos de que todo el tráfico de la red esté realmente protegido por algún tipo de cifrado y de que nos estamos conectando a servidores legítimos y no a algún servidor *man-in-the-middle*, como pueda ser por ejemplo un módulo Karmetasploit.

Protegernos

Ni el usuario más precavido está a salvo. La mayoría de las redes inalámbricas de pago no están protegidas por cifrado, ya que el proveedor tendría que compartir la contraseña con todos sus clientes. Un atacante podría obtener fácilmente una copia de la clave y descifrar el tráfico. Incluso aunque un proveedor proteja convenientemente mediante cifrado SSL su pasarela de pago, no hay nada que impida a algún cliente conectado analizar el tráfico o capturar contraseñas, por ejemplo. Al cifrar la red entera la dotamos de dicha protección, como explicábamos en el artículo “Pasadizos Secretos” [6]. Si no se dispone de un servidor a través del cual enviar el tráfico VPN, quizá interese probar el servicio VPN IPREDator [7]. IPREDator proporciona una conexión VPN cifrada mediante PPTP [8] por cinco euros mensuales, entunelando todo el tráfico hasta Suecia, donde unas estrictas leyes en materia de privacidad evitarán cualquier acceso ilegítimo. ■

RECURSOS

- [1] Kismet: <http://www.kismetwireless.net>
- [2] Aircrack-ng: <http://www.aircrack-ng.org/>
- [3] “Metasploit”, por Kurt Seifried, Linux Magazine, Número 47, pág. 8. http://www.linux-magazine.es/issue/47/008-009_Inseguridades47.pdf
- [4] KARMA + Metasploit 3 == Karmetasploit: <http://trac.metasploit.com/wiki/Karmetasploit>
- [5] Upside-Down-Ternet: <http://www.ex-parrot.com/pete/upside-down-ternet.html>
- [6] “Pasadizos Secretos”, por Kurt Seifried, Linux Magazine, Número 48, pág. 8. http://www.linux-magazine.es/issue/48/008-009_Inseguridades48.pdf
- [7] IPREDator: <https://www.ipredator.se/>
- [8] “Cerrado y Secreto”, por James Stanger, Linux Magazine, Número 46, pág. 18. <http://www.linux-magazine.es/issue/46/018-022VPNsLM46.pdf>
- [9] Listado de canales para LAN inalámbrica: http://en.wikipedia.org/wiki/List_of_WLAN_channels
- [10] Gráfico ilustrando las frecuencias usadas en redes inalámbricas: http://en.wikipedia.org/wiki/File:2.4_GHz_Wi-Fi_channels_%28802.11b_g_WLAN%29.png
- [11] Atribución Creative Commons y Licencia ShareAlike: http://commons.wikimedia.org/wiki/Commons:Reusing_content_outside_Wikimedia