CÓMO DETECTAR Y ECHAR INTRUSOS DE TU RED WIFI

Las redes WiFi son particularmente vulnerables a intrusiones externas. Aun en el caso de que tu conexión esté protegida con cifrado, es posible...

Fabrizio Ferri-Benedetti |

12 Noviembre 2013

Las redes WiFi son particularmente vulnerables a intrusiones externas. Aun en el caso de que tu conexión esté protegida con cifrado, es posible que alguien se cuele por los motivos más diversos.

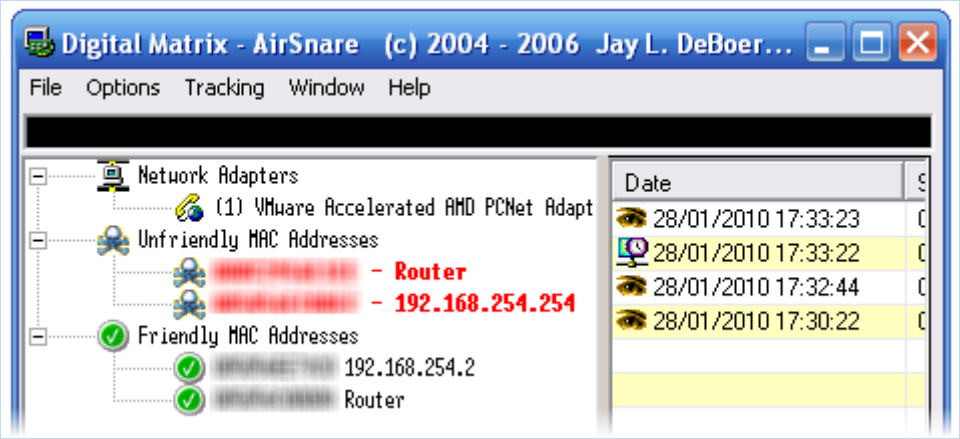
En este tutorial te enseñaremos a identificar los intrusos en tu red y a tomar medidas para expulsarlos definitivamente. De paso, aprovecharemos para comentarte cuáles son las protecciones más eficaces. ¡Síguenos!

Paso 1: medir la velocidad de tu conexión

Hay varios síntomas que indican la presencia de un intruso en una red WiFi doméstica. Con todos tus ordenadores y dispositivos apagados o desconectados de la Red, mira las luces de actividad del router: un parpadeo rápido y continuado indica que hay dispositivos conectados y transmitiendo un gran flujo de información.

La intrusión, en caso de que el vecino se porte mal, afectará también la velocidad de descarga a la que estés acostumbrado. La sensación de pérdida de ancho de banda es difícil de cuantificar:

programas como BASpeed, JD's Auto Speed Tester, NetTraffic oNetWorx te ayudarán a confirmarla.



AirSnare acaba de encontrar varios "intrusos" (dispositivos desconocidos)

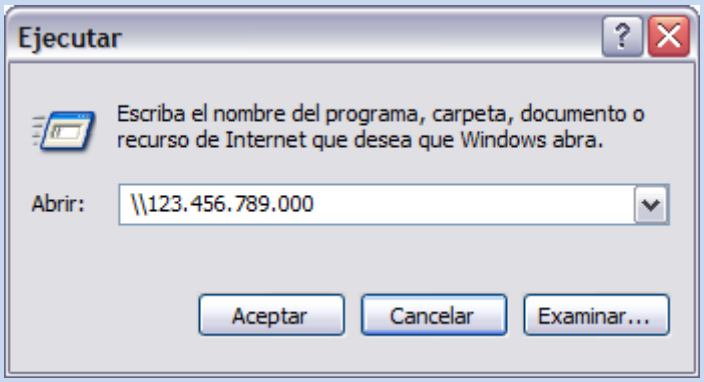
Paso 2: detectar a los intrusos

Hay herramientas dedicadas a la caza de intrusos. La primera y más conocida es AirSnare, que lleva sin actualizarse unos cuantos años, pero que en muchas máquinas funciona todavía sin problemas. AirSnare "escucha" el tráfico que pasa por el adaptador de red hasta obtener todas las direcciones MAC conectadas a la red local. Una utilidad similar, aunque sin interfaz gráfica, es la interesante Fing, que también cuenta con versión para Android.

Zamzon Wireless hace lo mismo, mas carece de todas las opciones de AirSnare, como el envío de mensajes o el registro de eventos. AirSnare, además, emite avisos acústicos cada vez que descubra una dirección desconocida

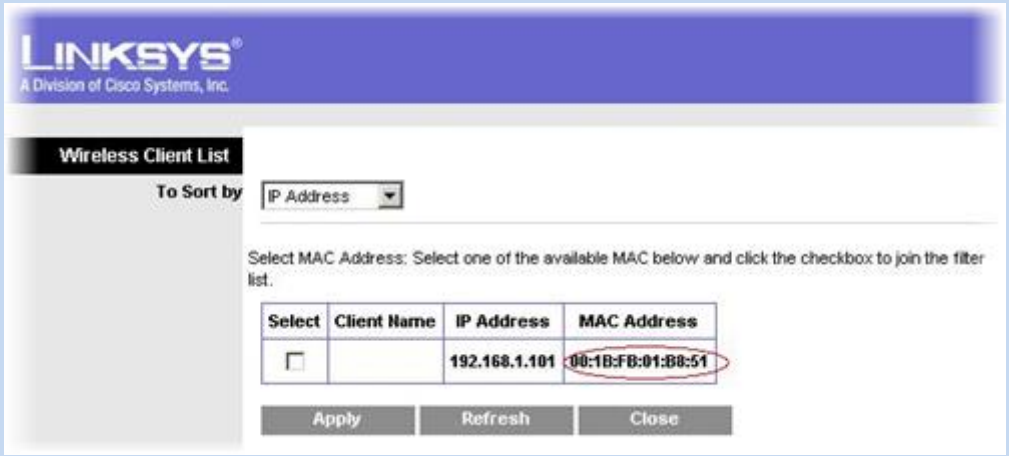
¿Quieres estar totalmente seguro de que lo que has detectado es un intruso? A veces, intentar el acceso a los recursos compartidos del ordenador ajeno puede quitarte de dudas. Ve

a Inicio > Ejecutar y escribe \\ seguidas por la IP detectada. ¡Sé bueno!



Si el intruso no tiene cortafuegos y comparte carpetas, esto será divertido

Por último, siempre te queda el panel de control del router: ábrelo escribiendo la dirección192.168.1.1 o 172.168.0.1 en el navegador, introduce usuario y contraseña (si no las conoces, busca las de tu aparato con Router Passwords) y navega hasta un menú llamado "Wireless Clients", "Connected Clients" o similar. Lo reconocerás por una tabla en la que se muestran direcciones IP locales y direcciones MAC. Ten en cuenta que cada dispositivo que tengas en casa (como las consolas) tendrá su propia IP.



Bien, no hay intrusos. Puedo dormir tranquilo.

El último sistema consiste en ir tocando todos los timbres del vecindario, entrar en las casas y examinar los ordenadores hasta dar con el sospechoso. Aunque es un método poco práctico...

Paso 3: proteger tu conexión WiFi

Has comprobado que alguien entró en tu red inalámbrica sin dificultad; ahora es el momento de reforzar las murallas y tapar agujeros para que eso no vuelva a pasar. Hay unas cuantas cosas que NO funcionan y que, por lo tanto, deberías evitar a la hora de proteger la red. Cosas como:

Cifrado WEP: es de sobra conocido que este tipo de cifrado se ha quedado obsoleto. La razón principal por la cual se sigue usando es la compatibilidad con adaptadores 802.11b, y es quizá por ello que muchos ISP lo activan por defecto. ¿Que por qué es inseguro? Cada hijo de vecino mínimamente espabilado sabe usar Aircrack...

Filtrado MAC: restringir la navegación a las direcciones MAC de tus ordenadores es tentador, pero inútil. Con las direcciones detectadas por el intruso y utilidades como MacMakeUp, que cambian la dirección del dispositivo, el mac-spoofing se lleva a cabo en segundos. Lo que sí podría ocurrir es que te quedaras fuera de tu red.

Ocultar el SSID: ocultar el nombre de la red inalámbrica es como caminar detrás de una puerta y pretender que nadie te ve. Sí es interesante, por otro lado, cambiar el nombre del SSID por algo que no se parezca al nombre por defecto o se pueda relacionar con tu ubicación. Prueba con algo simpático como "GTFO" o "HolaPollo".

Apagar el router: es cierto, un router apagado es un router a prueba de intrusos... y también un trasto inútil. Apagar el router durante los periodos de inactividad es bueno para ahorrar energía, pero poco más.

¿Son totalmente inútiles esas medidas de seguridad? Depende del nivel de conocimientos de tus vecinos. En general, sólo impedirán conexiones casuales de quien busca redes abiertas. En cambio, hay otras medidas de seguridad para proteger tu conexión WiFi que sí que son eficaces. Por ejemplo:

Cifrado WPA/WPA2: la tecnología de cifrado WPA, compatible con adaptadores 802.11g o superiores, es mucho más fuerte que WEP. Cualquier router dispone de WPA-PSK; en lugar de un código hexadecimal, hay una frase de paso de longitud variable (que debe ser resistente a ataques de diccionario).
¿Tienes WPA2-AES? Es la más robusta.

Cambiar la contraseña del router: es lo primero que debes hacer. El hipotético intruso querrá abrir puertos en el router para usar su programa P2P favorito u ocultar sus movimientos. Cambia la contraseña que tiene tu router por defecto para tener la última palabra sobre la conexión.

Pintura Anti-WiFi: una solución original consiste en cubrir las paredes de tu piso con una capa de pintura especial que impide el paso de señales WiFi. Lástima que no esté a la venta todavía...

¿Y si dejo abierta mi red WiFi?

¿Eres una persona generosa? Dejar el router abierto - aunque con la contraseña de administración cambiada - es una excelente forma de ganar amigos, aunque hay muchos motivos por los cuales no resulta recomendable, como la pérdida de velocidad (causada

por quien descarga datos a tope) o el uso de la conexión con fines ilegales. Una forma interesante de compartir y sacarle provecho a tu conexión es crear un FON Spot.

Bromas como ésta sólo son posibles con routers sofisticados

Si optas por compartir la conexión, asegúrate de usar un router de calidad y que te dépleno control sobre la red. Algunos modelos ejecutan su propia versión de Linux. Un ejemplo de las virguerías que pueden llegar a hacerse lo da Upside-Down-Ternet, un método para que el intruso navegue, sí, pero con las imágenes al revés. ¿No es divertido? Otra idea interesante es configurar una página de inicio con NoCatSplash para saludar a los visitantes.

Para los más tradicionales

La red más segura es la cableada. Cincuenta metros de cable Ethernet cuestan unos 25€, aseguran una calidad de conexión máxima y son relativamente discretos, especialmente si los pasas por los conductos de servicio que se ven en los pisos de nueva construcción.

Lo difícil es aprender a "grimpar" (crimpar o corrugar) el cable, esto es, a insertar los numerosos cables coloreados en los conectores de plástico. Aquí tienes un tutorial con imágenes. Y tender el cable puede ser una pesadilla o lo más divertido del mundo, dependiendo de lo mucho que te guste el bricolaje.

Este artículo fue publicado por primera vez el 29/01/2010, y actualizado el 05/11/2013.