La conexión es más lenta que de costumbre, demasiado lenta (mas lenta que Torguga con turbo integrado) para que la causa sea un fallo de tu operadora. Controlas la configuración, haces unas cuantas pruebas... un momento: ¿es posible que el vecino esté conectado a tu router inalámbricoy use la conexión para descargar películas a destajo y encima salir con tu mujer? (seguro conde anda por ahí)? Pues sí.
En este tutorial te enseñare a identificar los intrusos en tu red y a tomar medidas para expulsarlos definitivamente. De paso, aprovechare para comentarte cuáles son las protecciones más eficaces y cuáles, por el contrario, sólo hacen perder el tiempo.
Detección del intruso inalámbrico:
Las redes WiFi son particularmente vulnerables (como Linux más o menos) a intrusiones externas. Si tu señal carece de cifrado, o bien te has olvidado de activarlo o bien quieres compartirla con todo el mundo (en ese caso, sólo te interesará echar a los pillos). Pero, aun con cifrado, es posible que alguien se cuele por los motivos más diversos.

Hay varios síntomas que indican la presencia de un intruso (elcondemontecristo)en una red WiFi doméstica. Con todos tus Pc 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. Un usuario de megaupload por ejemplo, puede encontrarse de repente con la IP bloqueada por una descarga que se esté realizando desde su router... pero no desde tu Pc. La sensación de pérdida de ancho de banda es difícil de cuantificar: programas como **BASPEED** O **NETWORX** te ayudarán a confirmarla pero el más efectivo es el que uso yo **ADSLNET.**
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 en línea de comandos, es la interesante Fing.
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 de tu Pc ajeno puede quitarte de dudas. Ve a Inicio > Ejecutar y escribe \\ seguidas por la IP detectada. ¡Sé bueno!
Por último, siempre te queda el panel de control del router: ábrelo escribiendo la dirección 192.168.1.1 o 172.168.0.1 en el navegador, introduce usuario y contraseña que normalmente es admin 1234 (si no las conoces, busca las de tu aparato en RouterPasswords.com o CIRT) 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.
El último sistema consiste en ir tocando todos los timbres del vecindario, entrar en las casas y examinar los PCes hasta dar con el sospechoso. Un método poco práctico...
Levantar las defensas: lo que sirve y lo que no
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.

MEDIDAS INÚTILES:

*** 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, un programa capaz de hallar claves WEP en poco tiempo.
*** Filtrado MAC:** restringir la navegación a las direcciones MAC de tus PCes 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 y poco más.
¿Son totalmente inútiles esas medidas de seguridad?
Depende del nivel de conocimientos de tus vecinos. El uso de AirCrack o programas parecidos no está tan difundido en determinados barrios; es improbable, por ejemplo, que una amable ancianita lo use para ahorrarse unos cuartos, aunque cosas más raras se han visto. WEP, ocultar el SSID o filtrar las direcciones MAC tan sólo impedirán conexiones casuales de quien busca redes abiertas.

MEDIDAS QUE FUNCIONAN:

*** 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 del router para tener la última palabra sobre la conexión.

¿Y si lo dejo abierto?
¿Eres una persona generosa? Dejar el router abierto -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 (sean cuales sean).
Si optas por compartir la conexión, asegúrate de usar un router sofisticado y que te de pleno 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 No CatSplash para saludar a los visitantes.

Bueno acá termina el tuto espero que aparte de reírse con algunas gastadas a mis compañeros de quierowarez.org aprendan algo más sobre redes **wi fi** los saluda GianmarcoTV

Importante si copias este tuto y pegas en otra web por favor da la fuente se te agradecerá

Idea original de QuieroWares. Los genios de la web