APRENDERAPROGRAMAR.COM

CÓMO OBTENER CLAVES O CONTRASEÑAS DE REDES WIFI (CRACKING "A POR NARANJAS") ¿SON SEGURAS LAS REDES INALÁMBRICAS? (DV00107D)

Sección: Divulgación
Categoría: Tendencias en programación

Fecha revisión: 2029

Resumen: Quizás hayas oído hablar de que es posible conectarse a redes wifi existentes en tu entorno (por ejemplo, la de tu vecino). ¿Es posible? ¿Cómo se hace y qué dificultad y problemas tiene hacerlo?

Autor: Alex Rodríguez

LAS REDES WIFI

A partir del año 2000 se consolidó y fue en aumento el uso de una tecnología basada en la conexión a internet sin cables: las denominadas redes wifi. Wifi hace alusión al estándar adoptado a nivel internacional, que se incorpora a todos los ordenadores, tablets, teléfonos de última generación, etc. que permiten que con cualquier dispositivo nos podamos conectar a cualquier wifi (se supone que conociendo la clave de acceso).

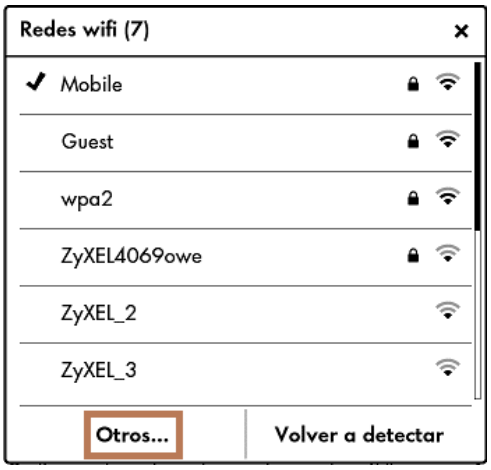
¿SON SEGURAS LAS REDES WIFI?

Una red wifi está formada por multitud de elementos: dispositivos electrónicos de la red como un modem, equipos cliente u ordenadores y otros dispositivos que se conectan a la red, y software que permite el funcionamiento de todo esto para conseguir un objetivo como puede ser recibir y enviar información a través de internet. La seguridad de una red wifi depende pues de varios factores, al igual que la seguridad de una vivienda. Lo que sí podemos tener claro es que la seguridad absoluta no existe. A lo más que podemos aspirar es a tener una seguridad razonable en la mayoría de los casos.

Si piensas en una vivienda, comprobarás que entrar a ella depende de diversos factores. El grosor y robustez de la puerta, el espesor de las paredes, la existencia de puntos débiles o huecos como chimeneas o ventanas y cómo estén protegidos, etc. Una red wifi también tiene su puerta y sus puntos débiles, que pueden estar mejor o peor protegidos. Y por supuesto, al igual que en una vivienda, lo más fácil para entrar en una red wifi es “entrar con la llave”.

CLASIFICACIÓN DE REDES WIFI ENTRE REDES ABIERTAS Y CERRADAS

Una primera clasificación de redes wifi podría llevarnos a dividir las redes wifi en redes abiertas y redes cerradas. Por red abierta entendemos aquella que no tiene establecida una restricción de acceso o más claramente: una red a la que podemos conectarnos libremente sin necesidad de contraseña simplemente porque no nos la pide. Cuando utilizamos Windows, un iPhone, una tablet o cualquier dispositivo y buscamos la lista de redes wifi, las redes protegidas con contraseña suelen aparecer señaladas con un pequeño candado junto a su nombre, mientras que las redes abiertas no tienen candado.



Una red puede estar abierta por diversos motivos como:

a) El propietario de la red la mantiene abierta por ignorancia o simplemente porque le da igual que otras personas se conecten.
b) Nos encontramos en algún lugar como una biblioteca, un aeropuerto, una cafetería, un colegio, o cerca de ellos, donde ofrecen el acceso gratuito a una red wifi.
c) Nos encontramos ante alguien que quiere que nos conectemos a su red para tratar de robar información que le pueda resultar de interés (por ejemplo, nuestro número de tarjeta de crédito).

¿Es seguro conectarse a una red abierta? Depende. Un aspecto clave es conocer quién administra la red: se supone que por ejemplo en un aeropuerto habrá profesionales administrando la red, no piratas informáticos tratando de robarnos información. En cambio, si estamos en algún lugar donde hay una red abierta y no sabemos quién está detrás de ella, puede existir mayor inseguridad. Esto no significa que detrás de cualquier red abierta desconocida haya un saboteador o delincuente, simplemente apuntamos a que el riesgo es mayor.

Una prudencia elemental puede ser la siguiente: usa una red abierta solo para navegar y ver páginas web sin introducir información sensible durante la navegación (no introduzcas tu login y password para acceder a sitios web o correo electrónico y mucho menos datos sensibles como tus datos de acceso a banca electrónica o tu número de tarjeta bancaria).

CLASIFICACIÓN DE REDES WIFI CERRADAS EN BASE AL TIPO DE SEGURIDAD

Las redes wifi cerradas podrían clasificarse de distintas maneras. Una habitual es en base al tipo de seguridad que implementan. La seguridad podríamos verla como el tipo de puerta y cerradura que tienen. Hay redes cuya seguridad es débil, algo así como una puerta de cartón piedra con un simple picaporte, y redes cuya seguridad es más fuerte, supongamos que del tipo puerta blindada. Pero como ya hemos indicado, no existe seguridad absoluta. Podemos disponer de una puerta blindada, pero si es fácil para una tercera persona determinar cómo es su llave y fabricarla, de poco nos valdrá el blindaje. Queremos decir con esto que la seguridad comprende múltiples aspectos, no solo uno.

Los tipos de seguridad más habituales que encontramos en las redes wifi comunes son las siguientes:

- **WEP y WEP2:** wep corresponde a las siglas de wired equivalent privacity o privacidad equivalente al cableado, siglas que por cierto con el tiempo resultaron bastante desafortunadas. Este estándar de seguridad puede considerarse obsoleto: después de ser distribuido y utilizado en miles de módems por todo el mundo, se descubrieron fallos de seguridad que hacen que este tipo de redes puedan hackearse (obtener su contraseña sin permiso del propietario) de forma bastante sencilla. Hoy día puede considerarse que está cayendo en desuso, aunque todavía existen muchos hogares donde se sigue utilizando.

- **WPA y WPA2:** wpa corresponde a las siglas de wifi protected access o acceso wifi protegido. En general es un tipo de seguridad más robusta y de más difícil hackeo, aunque también se conocen vulnerabilidades de distintos tipos por las que se puede acceder, con mayor o menor dificultad, a este tipo de redes.

Otras: empresas e instituciones pueden utilizar sus propias redes con protocolos de seguridad especiales.

TENGO UNA RED WIFI Y NO QUIERO QUE SE CONECTEN EXTRAÑOS

La mejor forma de que no se conecte nadie extraño a tu red wifi es no tener red wifi. Esto viene a ser algo así como la mejor forma de que no te atraquen en un supermercado es no ir al supermercado. Pero si aún así quieres tener una red wifi (o ir al supermercado), puedes adoptar distintas medidas de seguridad según te preocupe el que alguien se conecte a la red.

¿En qué medida debe preocuparte que alguien se conecte a tu red? Pues hoy en día por lo general los contratos de banda ancha por el cual una compañía telefónica o de telecomunicaciones te da acceso a internet y te instala una red wifi (también puedes hacerlo tú mismo, pero en la mayoría de los hogares son los técnicos de la empresa quienes hacen el trabajo) suponen que pagas una cuota fija mensual, independientemente de que uses más o menos internet. Esto viene siendo algo así como un contrato por el cual tú puedes ir a la tienda y llevarte naranjas, y da igual que en un mes te lleves 10 kilos de naranjas o que te lleves 3000 kilos, que siempre te van a cobrar lo mismo. ¿Lógico? Pues no lo parece mucho, pero en fin, esto sería tema para otra discusión. El caso es que si alguien se conecta a tu red se lleva naranjas, y tú al final pagas lo mismo. Mientras no te incomode no tendría por qué ser motivo de preocupación. Al fin y al cabo, ¿qué más da que se lleven unas cuantas naranjas? El problema puede venir si quien se conecta empieza a molestarte cuando tú quieres coger naranjas y no puedes porque otro lo está haciendo. La compañía tiene una capacidad de servicio, digamos que te puede servir 20 Mb de información por segundo. Si tú usas 10 Mb y tu vecino conectado usa 3 Mb, te siguen sobrando Mb. Prácticamente ni te vas a enterar de que tienes a tu vecino conectado. En cambio si tú usas 10 Mb y todos tus vecinos de tu bloque más los del bloque de enfrente están conectados, puede ocurrir que estén usando 19 Mb. Y la compañía quizás intente atender a todos y te deje a ti con un servicio de 1 Mb cuando tú querías usar 10. Esto ¿en qué se traduce? Normalmente en la expresión: “la red no va”, “esto va muy lento”, “no me están dando lo que yo contraté”, etc.

Otro motivo de preocupación podría ser el que intentaran acceder a tu ordenador a través de la red: esto sería realmente difícil. Tendrían que darse una serie de circunstancias extraordinarias para que esto llegara a ocurrir por lo que no vamos a prestarle atención a este aspecto.

Si después de todo esto decides que quieres dedicar tiempo a tratar de evitar que los extraños se conecten a tu red puedes tomar las siguientes medidas:

a) Si tienes un modem con seguridad wep (mira en la placa en la parte trasera del modem) llama a tu compañía y solicítales que te cambien el modem a una seguridad más elevada como WPA2.

b) Si tienes un modem con seguridad WPA, comprueba si se encuentra dentro de los modems con vulnerabilidades conocidas. Esto puedes hacerlo investigando un poco por tu cuenta o pidiéndole ayuda a algún programador o informático que pueda ayudarte. Si fuera así, pide que te lo cambien por otro modelo sin vulnerabilidad conocida.

c) Medida muy elemental pero muy efectiva: apaga el modem cuando no lo estés usando.

QUIERO CRACKEAR UNA RED WIFI

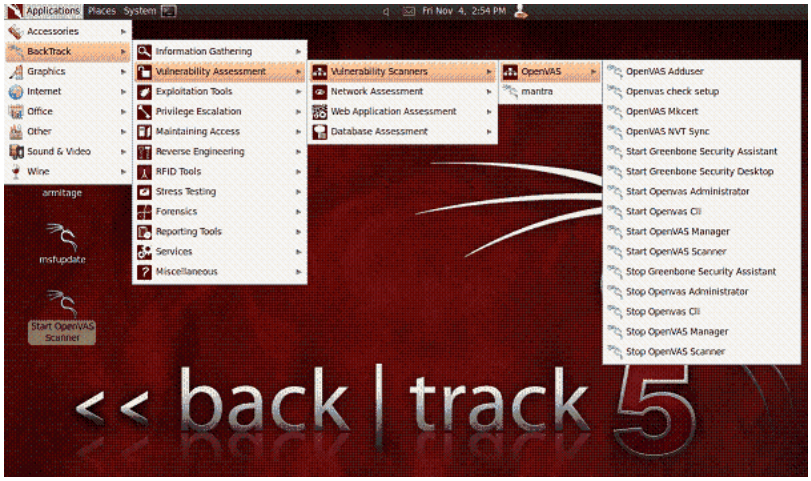
Si quieres acceder a una red wifi de un vecino o similar sin tener la clave, no lo tienes fácil ni difícil. Digamos que dedicándole unas pocas de horas con seguridad podrás obtener las claves de unas cuantas redes.

¿Es necesario tener conocimientos avanzados de informática o programación para crackear una red? Pues la verdad es que no. Si los tienes, posiblemente te ayudarán, pero si no los tienes te bastará ser un usuario un poco avanzado de ordenadores, ya que existen muchos programas preparados para el crackeo de redes sin necesidad de extensos conocimientos.

Si te vas a decidir a intentar cracker redes sin tener conocimientos previos o avanzados, la única advertencia que te haríamos es “quizás obtengas alguna red rápidamente, pero en general prepárate para dedicar largas horas a aprender a usar las herramientas y a tratar de pescar redes”.

Los pasos más habituales que siguen quienes quieren probar suerte es leer un tutorial y descargar una herramienta para el crackeo. Vamos a citar algunas herramientas y páginas web donde podrás “instruirte” si esa es tu intención:

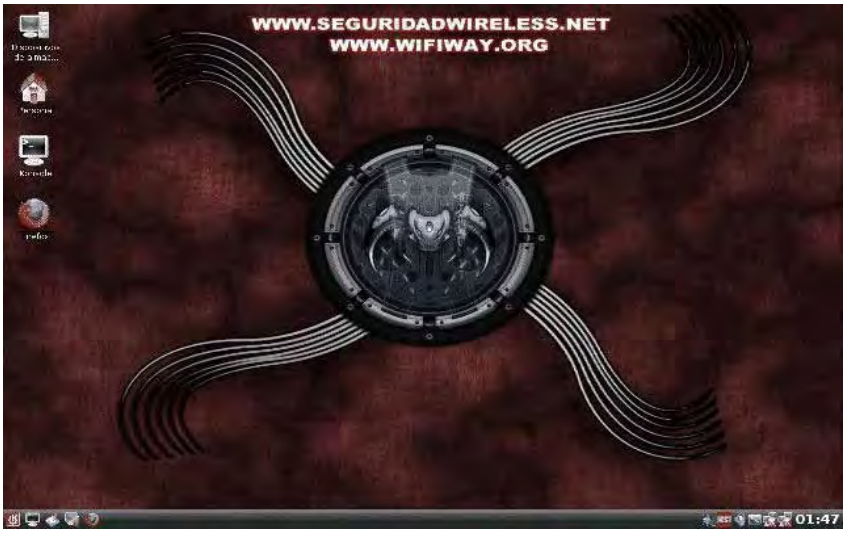
BACKTRACK



Backtrack es un clásico dentro del cracking. Se trata de una distribución del sistema operativo Linux que viene preparada especialmente para el crackeo de redes wifi (oficialmente se dice que es una herramienta para auditoría de redes wifi). Han ido apareciendo diferentes versiones con el tiempo.

Existen numerosos tutoriales para su uso en internet. Puede descargarse gratutitamente. La web oficial es http://www.backtrack-linux.org/

WIFIWAY



Otra distribución Linux que incorpora multitud de herramientas. Algunas de ellas de más fácil uso que backTrack al tener un entorno más amigable, al contrario que backTrack, que funciona principalmente en entorno consolas.

También existen numerosos tutoriales para su uso en internet. Puede descargarse gratutitamente. La web oficial es http://www.wifiway.org/

OTROS

Hay otras herramientas muy usadas como wifislax. Puedes informarte en http://www.wifislax.com/ y en http://www.seguridadwireless.net/

Y finalmente hay decenas de herramientas más... no tenemos espacio para citarlas todas. Algunas son para entornos Windows y otras para entornos Linux.

LOS CONSEJOS FINALES PARA LOS APRENDICES DE HACKERS

Si vas a gastar (o malgastar, según se vea) tu tiempo en intentar obtener contraseñas de redes, te damos un par de consejos básicos:

1) Comprueba que dispones de una tarjeta wifi en tu ordenador que permita el modo monitor. No todas las tarjetas lo permiten. Si tu tarjeta no lo permite, siempre tienes opción de usar una tarjeta en un pendrive usb conectada mediante un puerto usb. Son baratas.

2) Aunque hay herramientas para Windows, te recomendaríamos que uses Linux. No hace falta que te pases a Linux, simplemente aprender a arrancar un live cd en tu ordenador y el manejo básico de alguna herramienta.

Finalmente ten en cuenta que el cracking no es legal, aunque suele considerarse una cuestión "menor". No vas a acabar en la cárcel por crackear un par de redes, aunque tampoco nadie te va a recomendar explícitamente hacerlo. En general verás que todas las herramientas existentes indican que son "para auditoría de redes" (que por cierto también sirven para eso).