

(In)seguridad Wireless

Autor: svoboda

Email: thamatos2001@aroba@gmail.com

Licencia



<http://creativecommons.org/licenses/by-nc/2.5/es/deed.es> CL

<http://creativecommons.org/licenses/by-nc/2.5/es/legalcode.es>

1 - Introducción

Hoy en día lo más habitual es que la gente tenga en sus casas una línea con conexión a internet de banda ancha, y algo también muy común es el hecho de que casi todas estas conexiones tienen un punto acceso wireless. ¿Cuántos de nosotros no hemos encendido el portátil y hemos detectado multitud de redes de nuestros vecinos?

La cuestión es que a pesar de lo extendida que esta la tecnología inalámbrica y del conocimiento de su existencia que tiene casi todo el mundo, sorprende ver que muchas de estas redes carecen de cualquier mecanismo de seguridad. Muchas de ellas están abiertas sin ningún tipo de cifrado, y en la mayoría de los casos los puntos de acceso o dispositivos tienen las claves por defecto aún puestas.

El objetivo del presente texto es hacer llegar a todo el mundo, de forma fácil y sencilla, unos conceptos básicos de seguridad para la configuración de sus redes inalámbricas. La idea es ir comentando y explicando las diferentes opciones disponibles, unos pequeños consejos y explicar el porqué de estos métodos.

2 - ¿Por qué necesitamos seguridad?

Como ya he comentado anteriormente, hoy en día, todo el mundo sabe que es una red inalámbrica, aún así nunca esta de más una pequeña definición.

Una red inalámbrica es una red en la que no se utilizan medios físicos para la transmisión de la señal. Esta transmisión se hace por medio de ondas a través del aire o el espacio. Los únicos dispositivos físicos existentes en este tipo de redes son los receptores y emisores de la señal.

Una vez enunciada esta pequeña definición, se puede ver fácilmente cual es el principal motivo por el que se necesitan unos medios de seguridad adecuados para nuestras redes. A

diferencia de las redes cableadas donde la señal va por un medio físico controlado y para su acceso ha ella hay que tener acceso a este medio físico, en las redes inalámbricas la señal va por el aire, con lo cual cualquier persona con un receptor puede acceder a esta señal y hacer con ella lo que quiera. Por este motivo se recomienda tener un mínimo de seguridad para dificultar los accesos a nuestra red, la utilización de esta y la protección de los datos que enviamos nosotros mismos a través de ella.

3 – Principios básicos, dispositivos y cifrados

En primer lugar, para el despliegue y puesta en funcionamiento de una red inalámbrica necesitamos el dispositivo emisor de señales o punto de acceso. Generalmente suele ser un dispositivo *router* o *routermodem* facilitado por nuestro ISP (compañía de conexión) o adquirido en alguna tienda.

La mayoría de estos dispositivos, una vez conectados, ofrecen un interfaz de configuración basado en web (accesible a través del navegador) el cual nos permite cambiar los parámetros de configuración de este dispositivo. Para acceder a ellos, generalmente, solo se necesita una dirección IP, un usuario y una contraseña localizados en el manual de instrucciones. Pues bien, esta es la primera debilidad de nuestra red. Estos tres datos que vienen por defecto configurados inicialmente en el punto de acceso son conocidos, de hecho, en internet hay páginas con enormes listas de estos parámetros por defecto, con lo cual cualquiera en el radio de acción nuestra red podrá acceder a ella y modificar a su antojo cualquier configuración de nuestro punto de acceso. Dejarnos sin acceso a nosotros mismos, redirigirnos a páginas no deseadas, etc ...

Para solucionar esto, la primera medida que vamos a tomar es la de acceder al dispositivo y cambiar los parámetros de usuario y contraseña que vienen por defecto. Como siempre para las contraseñas se recomienda que sean largas, con caracteres alfa-numéricos y demás símbolos de teclado permitidos. Con esto dificultaremos el acceso y control del dispositivo por parte de individuos externos a la red.

A pesar de todo esto, si por algún motivo nos cortan el acceso al punto de acceso cambiando los credenciales de usuario y contraseña, siempre podremos echar mano del botón de *reset* que poseen la mayoría de puntos de acceso.

Una vez cambiadas las credenciales de acceso al dispositivo, el siguiente paso será configurarlo según indique nuestro manual. Uno de estos pasos de configuración es el de seleccionar la encriptación que se de sea para la red. Este es otro punto importante para la seguridad de nuestra red inalámbrica. El cifrado de la red impide que el contenido de los paquetes de información transmitidos a través de esta sea fácilmente leído por alguien que este a la escucha.

El dispositivo nos ofrece varias opciones, aquí por facilidad de comprensión las vamos a agrupar en tres grupos:

- La primera opción es la de dejar la red abierta, sin ningún tipo de cifrado, por supuesto, esta opción es la que debemos evitar a toda costa ya que cualquier usuario malintencionado que este a la escucha podría fácilmente ver el contenido de la información enviada por la red.
- La segunda opción es la de encriptarla mediante cifrado WEP, esta opción ya empieza a ser interesante ya que establece un nivel mínimo de cifrado en nuestra comunicación, ofreciéndonos de este modo algo de seguridad.
- La tercera opción es la de cifrado WPA, esta si que es la opción más segura para cifrar nuestra red. Generalmente, los puntos de acceso ofrecen varias posibilidades de cifrado WPA, que son las diferentes versiones existentes de este método de cifrado. Evidentemente, siempre que se pueda, se recomienda el método más moderno.

Una vez establecidas las tres opciones que nos ofrecen los puntos de acceso vamos a apuntar diferentes razones para seleccionar unos u otros según nuestras posibilidades o necesidades. No pretendo entrar en detalles técnicos sobre la diferencia de seguridad entre un cifrado y otro o los motivos de esta diferencia, de esto ya se hablará en apartados posteriores, simplemente voy a nombrar algo a tener en cuenta a la hora de decantarse por una opción u otra.

Una de la principales cosas a tener en cuenta, es la complejidad de los dispositivos que vamos a conectar a nuestra red. Evidentemente la mejor opción y la que se debería recomendar es la de cifrado WPA, pero claro si nuestros dispositivos no la van a soportar no tiene sentido utilizarla. Para averiguar esto simplemente hay que fijarse en los detalles de los dispositivos. Por poner un ejemplo para ilustrar esto al lector, los portátiles aceptan las tres opciones, mientras que un dispositivo con la Nintendo DS no implementa el soporte para WPA. Así que antes de elegir cifrado el usuario deberá mirar que dispositivos desea conectar.

En el caso de vernos forzados a usar una solución basada en WEP, se recomienda utilizar otros métodos de defensa que se nombrarán en el apartado siguiente. En el caso de seleccionar una solución WPA, aunque no son tan necesarios otros métodos de defensa, nunca están de más, pero esto ya se deja a elección del usuario.

Con estas dos consideraciones, la de modificación de las credenciales por defecto del punto de acceso y la del cifrado de nuestra red ya podemos considerarnos un poco más seguros, y a menos disuadir a una gran cantidad de gente de utilizar nuestra red.

4 – Aumentando nuestra seguridad

Como ya se ha comentado, en este apartado se van a comentar métodos para mejorar nuestra seguridad un poquito más. En el caso de haber seleccionado un cifrado WEP se recomienda utilizar alguno o varios de los métodos nombrados a continuación para intentar evitar las debilidades de este cifrado. En el caso de haber seleccionado un cifrado WPA no se considera tan necesario el añadir los siguientes métodos, pero nunca están de más.

Una de las opciones a tener en cuenta es la potencia de transmisión de nuestro punto de acceso. Todos tienen un alcance determinado, por ejemplo 120 metros, en caso de que nuestras necesidades no requieran una cobertura de señal tan amplia podemos disminuir la potencia de señal dificultando de este modo la captura de la señal sin nuestra supervisión.

Otra recomendación, sería la de desactivar el servicio de DHCP. Este es el encargado de la asignación de direcciones IP a los dispositivos que se conectan a nuestra red. En caso de tener una red con una configuración fija, es decir, a la que siempre acceden las mismas máquinas, podemos hacer esta asignación de forma manual y de este modo no permitir que se le asigne una IP válida a máquinas externas .

Podemos establecer filtros de MAC o de IP, de este modo solo las máquinas que nosotros hayamos introducido en las reglas de los diferentes filtros podrán utilizar nuestra red.

Finalmente, la última opción que vamos a nombrar en el presente documento, es la de ocultar la identidad de la red. Por lo general, el punto de acceso junto con su señal transmite su nombre para así poder ser fácilmente localizado por los usuarios, evitando el envío de este nombre cualquier atacante tendrá más difícil centrar su objetivo ya que de los paquetes que capturará en el aire tendrá que discernir cuales son de nuestra red y cuales no.

Todas las recomendaciones anteriores harán que nuestra red sea un poquito más segura, y que podamos utilizarla con más tranquilidad.

5 – Métodos de ataque

En este apartado no se va a entrar en mucho detalle en como realizar los diferentes ataques a una red inalámbrica, pero si que se va a nombrar y comentar algo sobre ellos relacionándolos con los métodos de defensa vistos anteriormente.

En primer lugar dejar claro que los ataques a las redes inalámbricas se basan todos en la captura de los paquetes que circulan por el aire. Existe la posibilidad de colocar las tarjetas de red en un modo conocido como “*monitor*” el cual permite capturar paquete que no vayan dirigidos a un

ordenador. Esta captura permite el posterior análisis de los paquetes para conseguir la intrusión en la red deseada.

Los ataques se pueden dividir en dos tipos. Los ataques activos y los ataques pasivos. Los pasivos son aquellos en los que el atacante simplemente se dedica a la captura de paquetes y el análisis de estos. Estos ataques desafortunadamente son indetectables, ya que el atacante en ningún momento interactúa con nuestra red. El otro tipo de ataque son los activos, generalmente realizados con ordenadores con dos tarjetas de red o con dos ordenadores. El método consiste en que mientras que uno de los ordenadores se dedica a la captura y análisis de paquetes, el otro se dedica a interactuar con el punto de acceso para generar un tráfico elevado de estos paquetes. Estos ataques sí que son detectables mirando los *logs* de conexión y dándose cuenta del incremento de tráfico que se produce.

Además, dentro de estos ataques existen varias técnicas para intentar evitar los métodos de seguridad antes expuestos.

Frente al filtro de MAC e IP tendríamos la posibilidad de fingir estas dos características tomándolas de un ordenador existente legítimamente en la red. Esto se realizaría mediante la captura de paquetes legítimos de la red y la consulta de sus parámetros. Existen muchos programas capaces de llevar esta tarea de falsificación en la red.

Frente a la disminución de potencia de nuestro punto de acceso, existe la posibilidad de utilizar antenas direccionables con las que apuntar al punto de acceso para así conseguir una mayor cobertura de señal y seguir capturando paquetes sin ningún problema. Por ejemplo, podemos consultar en la red tutoriales de como crear una con un lata de *“pringles”*.

Y finalmente, frente al cifrado WEP, existe la posibilidad de realizar ataques estadísticos para detectar la contraseña utilizada en el cifrado. Por esto, si es posible, se ha recomendado a lo largo del documento el cifrado WPA.

6 - Conclusión

En definitiva como hemos comprobado, para todo método de seguridad existe un método de ataque o a la inversa según se quiera mirar. Más de un lector estoy seguro que estará pensando que entonces no habrá forma de proteger totalmente nuestra red. No me siento calificado para dar una respuesta tajante a esta pregunta, pero lo que sí puedo afirmar es que si se siguen todos los pasos nombrados en el presente documento, al menos, lo pondremos muy difícil y disuadiremos a mucha gente de intentar utilizar sin permiso nuestra red.

7 – Esquema rápido

- Cambiar credenciales por defecto de punto de acceso (contraseñas fuertes)
- Cifrar nuestra conexión (comprobar compatibilidad de dispositivos a conectar)
- Disminuir potencia de la señal.
- Desactivar servidor DHCP
- Filtros MAC e IP
- Ocultar identidad de la red

Espero que a todos aquellos que estéis un poco preocupados por vuestra seguridad os sirva de ayuda este texto.