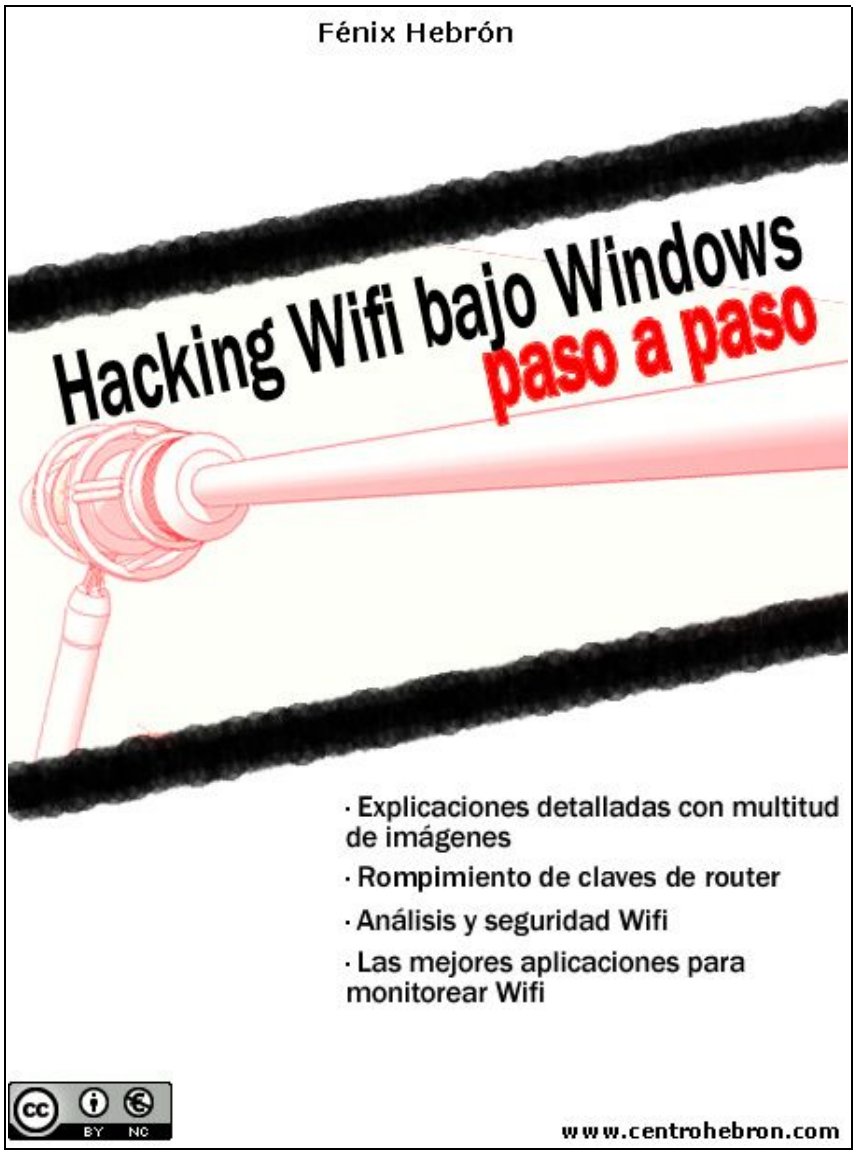
Hacking Wifi bajo Windows
paso a paso



Esta es una obra Creative Commons, se puede copiar, distribuir y divulgar gratuitamente, siempre y cuando se cite la fuente de procedencia y su autor.
No está permitida la venta de la presente obra.
CC. Fénix Hebrón
Fénix Hebrón es especialista en seguridad informática, betatester, experto en redes LAN/WAN y ha formado parte del equipo de desarrollo y programación de Arphean.
Contacto para sugerencias: centrohebron@gmail.com
Todas las explicaciones y procedimientos de éste manual han sido realizados bajo Windows XP SP1. En Windows XP SP2 o Windows Vista algunos de los programas aquí descritos no funcionan. Muchos de estos programas pueden contener virus, si decides probarlos, ¡hazlo siempre descargándolos de sitios de confianza y, preferiblemente, de la web de sus autores!

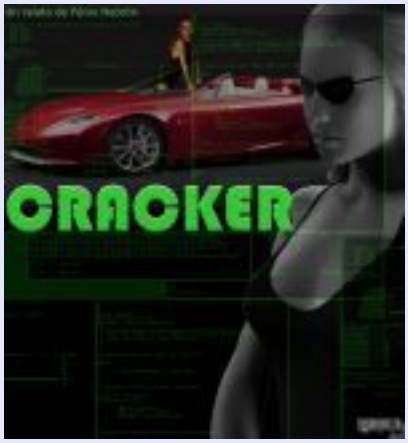
Nota: Todo el proceso de escaneo y desencriptación se ha realizado sobre una red propia y, cuando ésto no ha sido posible, se han simulado los pasos. En ningún momento, durante la realización del presente manual, se ha accedido a redes de terceros. Asimismo, la información de red (direcciones MAC, BSSID, etc.) son propias y/o simuladas, en ningún caso es información de redes confidenciales.

ADVERTENCIA

El presente trabajo se le ofrece únicamente con fines didácticos e informativos, no se aconseja su uso por los problemas de incompatibilidad que pueden derivarse. Algunos de los programas, aplicaciones o procedimientos que aparecen en éste manual pueden dañar severamente su equipo informático, por ello es desaconsejable su uso. En caso contrario, queda bajo su absoluta responsabilidad los posibles daños que puedan derivarse.
Asimismo, atacar y/o forzar redes ajenas está penado por ley, y es, además, una práctica que aumenta inútilmente el tráfico de una red, enlenteciéndola, con lo cual, siempre, debe utilizar los programas y conocimientos aquí mencionados para monitorizar o, en su caso, restaurar, su propia red, nunca redes wifi ajenas. La práctica del hacking o monitoreo de redes propias para solucionar problemas de compatibilidad o descubrir agujeros de seguridad no está penada, y es la única práctica que le aconsejamos.

PUBLICIDAD

Si te gusta el hacking, la programación y, en general, la informática, te gustará este libro. Un relato apasionante que te enganchará en su acción desde la primera hasta la última página.



Descárgalo ya, gratuitamente, desde
www.centrohebron.com

Preámbulo.
Desde los primeros tiempos de las redes wireless se ha venido hablando con insistencia sobre seguridad. Las compañías invierten no pocas cantidades de dinero para proteger su confidencialidad y salvaguardar la información, en muchas ocasiones de mucha importancia, que viaja por la red.

No han sido pocas las personas que me consultan de cuando en cuando preguntándome sobre las diversas formas de penetración en sus routers, y, también, muchas otras sobre cómo pueden configurar una red segura o detectar la vulnerabilidad real de la suya.

Desde el punto de vista doméstico la seguridad es menos importante, pero nunca viene mal conocer los puntos más débiles que puede tener nuestra red y, sobre todo, hay que tener en cuenta que la peor manera de protegerse es el desconocimiento, o la falta de información.

Comúnmente se piensa que una red wifi de última generación, con encriptado de alto nivel (de 256 bits o más) es poco menos que inasaltable. Nada más lejos de la realidad. Una persona con relativamente pocos conocimientos puede, sin mucho esfuerzo, hacerse con el password de nuestra red, y entrar en ella de manera fácil, aún con encriptación WEP2 o WPA-PSK de alta calidad.

Existen, también, multitud de herramientas que facilitan a los dueños de redes domésticas passwords que, supuestamente, son "muy difíciles de averiguar", pero hay que tener en cuenta que a las herramientas de hackeo de redes actuales, con los nuevos algoritmos de desencriptación (como el PTW) el formato del password les da prácticamente "lo mismo", ya están suficientemente pensadas para ello y pueden fácilmente averiguar ése tipo de claves. Por lo tanto estos generadores de passwords tan "eficientes" no son más que una forma de tranquilizar al propietario de la red haciéndole creer que está protegido, pero fuera de eso no cumplen ninguna función de protección.

¿Cómo, entonces, proteger nuestra red? Al final de éste manual dispones de algunos consejos para hacerlo pero, honestamente, creo que la mejor forma de proteger algo es conociendo cómo funciona y cómo se le puede asaltar. Sólo así podremos de verdad entender lo desprotegidos que podemos estar y, en su caso, podremos tomar las medidas que creamos más convenientes. Con ése objeto es por el cual he decidido realizar éste trabajo que tienes en tus manos.

Hardware necesario.
Para poder obtener el password de una red encriptada necesitamos unos drivers especiales, que puedan hacer a la tarjeta de red que tengamos entrar en "modo monitor". Por lo tanto, no sirven los drivers que "nos venden" cuando compramos la tarjeta. Tampoco sirven todas las tarjetas, ni adaptadores, aunque bien es cierto que a medida que pasa el tiempo cada vez más chips son compatibles.

¿Cómo podemos saber si nuestra tarjeta Wifi es compatible? Primero tendremos que averiguar qué chip posee. No te fíes de los fabricantes de la tarjeta, muchos de ellos no fabrican el chip. Podemos diferenciar cuatro tipos de chips aptos para entrar en "modo monitor", los cuales son:

Atheros
Oricono
Realtek
Aironet

Si tu tarjeta dispone de uno de dichos chips, entonces tendrás muchas posibilidades de que puedas usarla para obtener claves de red. La gran pregunta que le surge ahora a la mayoría es: "¿Y bien? ¿Cual es mi chip?". En Internet existen multitud de páginas donde especifican los chips que disponen cada tarjeta, dependiendo de su fabricante. Principalmente suelen ser en foros de Linux, Solaris o OpenBSD donde está dicha información, ya que los programadores de dichos sistemas operativos trabajan por chips, y no por fabricante, como estamos acostumbrados cuando usamos Windows.

Si desconocemos sitios específicos, podemos hacer una búsqueda por Google tipo "chip D-Link" y a continuación nuestro modelo en concreto, por ejemplo: "chip D-Link DW-450". Con un poco de suerte nos llegarán una serie de páginas con las que podemos empezar a buscar el chip que tenemos.

Una vez sepamos qué chip en concreto es el de nuestra tarjeta o adaptador de red, debemos confirmar que haya drivers para dicho adaptador. Drivers que, además, puedan hacerlo en modo monitor. ¿Cómo sabemos esto? Bueno, dar una respuesta específica, con la cantidad de tarjetas, marcas, modelos y adaptadores de red que existen, sería algo interminable. Lo mejor es que una vez conozcas el tipo de chip que posees, busques por su driver en modo monitor.

Modo Monitor.
Hasta ahora hemos hecho referencia muchas veces a estas dos palabras, y las oirás muchas veces cada vez que se hable de hacking wireless, pero, en concreto, ¿qué quiere decir?

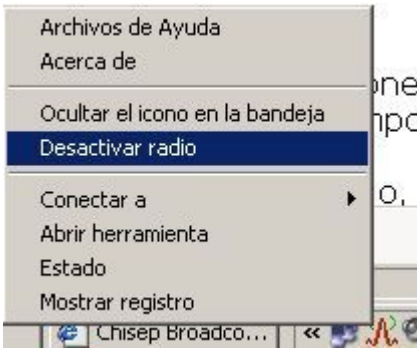
El Modo Monitor (o "promiscuo") significa que podemos capturar los paquetes de datos que se envíen por el aire, no nuestros paquetes en particular (como lo hace la tarjeta en modo normal y con su driver), sino **todos y cada uno de los paquetes que pasen a su alrededor, sean propios o ajenos**. Además, con éste modo -aunque no todos los drivers admiten ésto- podemos **inyectar tráfico** en la red que queremos entrar.

La "inyección de paquetes" es una estrategia más en el amplio abanico que podemos encontrar en el ataque a una red wifi. Se trata de enviar al router destino una serie de paquetes que él reconoce, mediante una **autentificación falsa** que hacemos en dicho router. Hay que tener en cuenta que para obtener la clave de una red no es imprescindible inyectar paquetes, la inyección se lleva a cabo cuando queremos ahorrar tiempo, o cuando el tráfico en ésa red de destino es muy bajo o nulo. En dichos casos creamos nosotros mismos un "tráfico artificial" que hará que el router emita sus preciados datos encriptados que nosotros, a su vez, captaremos para su posterior tratamiento y descodificación.

Instalación de drivers.
Ya tenemos los drivers de nuestro chip (aquí ya no tiene sentido hablar de nuestra tarjeta, puesto que la tarjeta o adaptador puede ser de un fabricante cualquiera, o, incluso, como ocurre muy a menudo, muchas tarjetas de diferentes fabricantes poseen el mismo fabricante de chip), la tarjeta (o adaptador USB) preparada, y ahora ya podemos afrontar el siguiente paso: su instalación.

En éste paso hay que tener mucho cuidado, y, de estar practicando, es mejor hacerlo en un ordenador que no temamos romper, ya que podemos tener dificultades con los drivers. También hay que destacar que muchos de los chips no pueden funcionar en modo monitor y en modo normal a la vez, por lo que, para continuar navegando por Internet y hacer uso de la red tendrás que volver a instalar los drivers que venían con tu tarjeta o adaptador. También es importante que tengas en cuenta que no es posible obtener paquetes de otra red si tienes otro adaptador funcionando, ya que en Windows causan problemas de adaptabilidad.

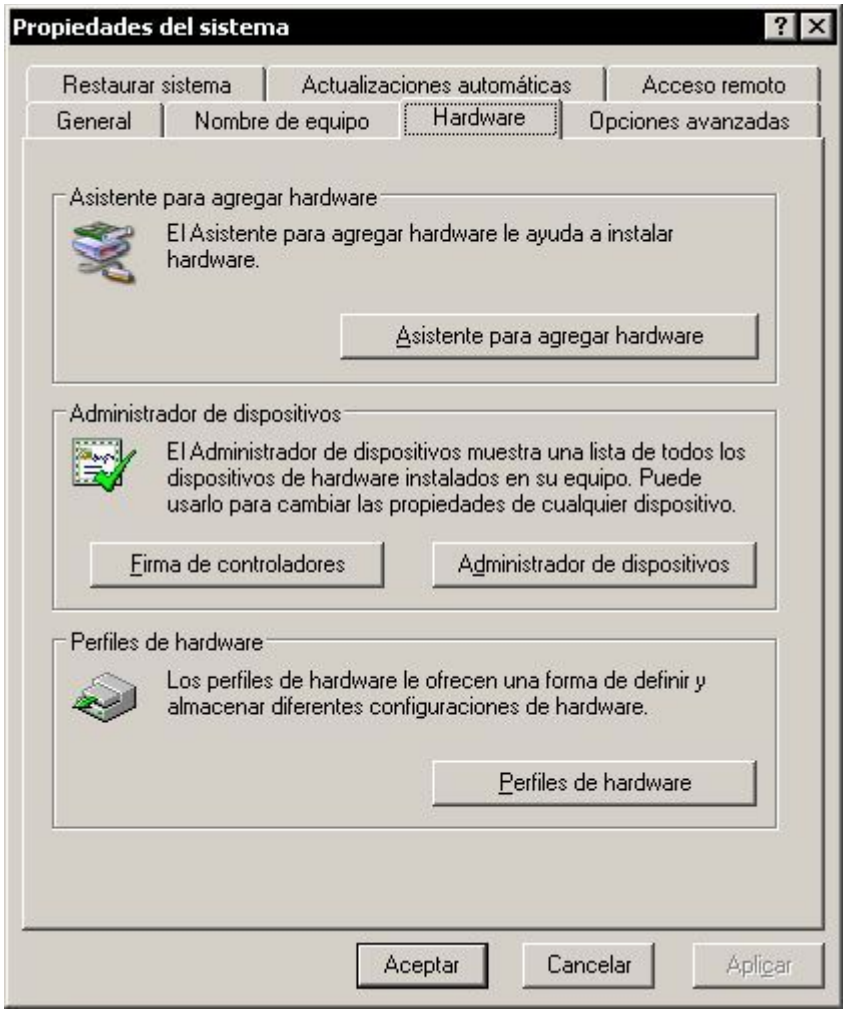
Por ello, antes de instalar los drivers para el modo monitor:
A/ Guarda los drivers originales de tu tarjeta para usarlos cuando dejes el modo monitor.
B/ No enciendas ni uses ningún otro adaptador o tarjeta wifi, sino únicamente la que vas a poner en modo monitor. Si tienes otro adaptador integrado, desactívale el radio antes de usar la otra tarjeta en modo monitor:



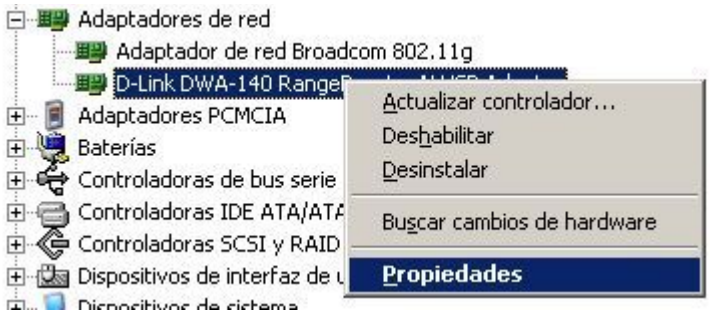
El procedimiento para instalar los drivers que usarás en modo monitor ha de ser realizado a mano, y, antes, deberás desinstalar los drivers de tu tarjeta anterior. Si no recuerdas cómo se hace, puedes consultar el manual que los chicos de Seguridad Wireless han colocado en su web:
http://hwagm.elhacker.net/windriver/monitordriver.htm

Cuando hayas instalado los drivers correctamente, podrás comenzar a utilizar las herramientas que usaremos para el monitoreo de la red. La primera de ellas será la que nos dirá si los propios drivers que has instalado son correctos y si pueden efectuar la tarea de recogida de paquetes.

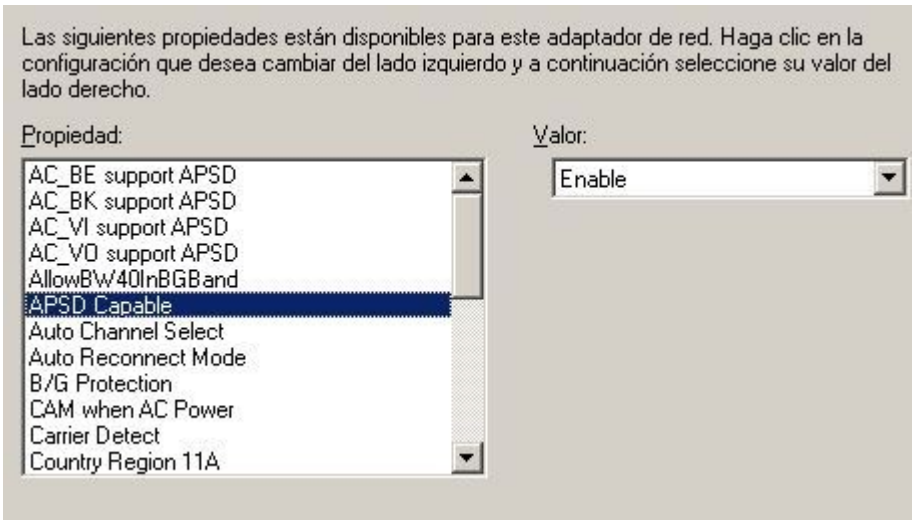
Pero antes de hacer eso aún queda un pequeño paso que dar. Debemos ir a las especificaciones de hardware de los drivers que acabamos de instalar (botón derecho del ratón sobre el icono "Mi PC" y seleccionar "Propiedades"; a continuación, de la pestaña "Hardware" elegir "Administrador de dispositivos":



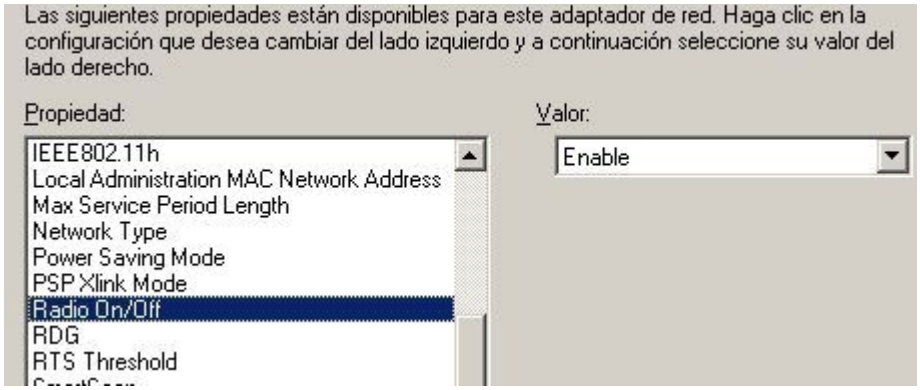
De la lista desplegable seleccionaremos nuestro adaptador de red (el que vamos a usar para el monitoreo):



Elegimos "Propiedades" y de las opciones que existen, activamos las que vemos necesarias para el funcionamiento en modo monitor. Este paso no es siempre necesario, pero sí conveniente:

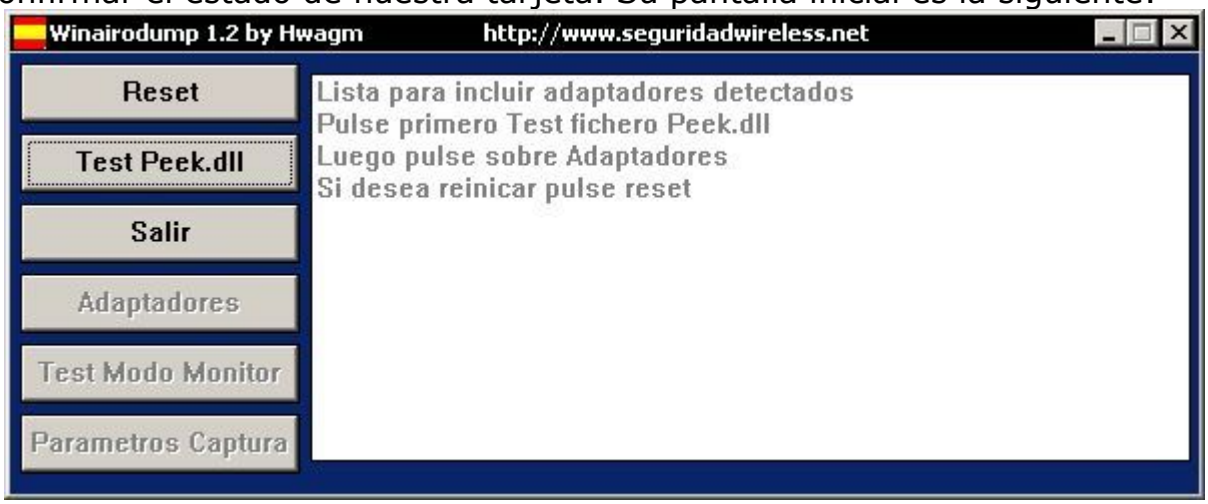


Desde aquí también podemos activar/desactivar la radio de los adaptadores que tengamos (caso de que no poseamos de utilidad externa, como hemos visto anteriormente):

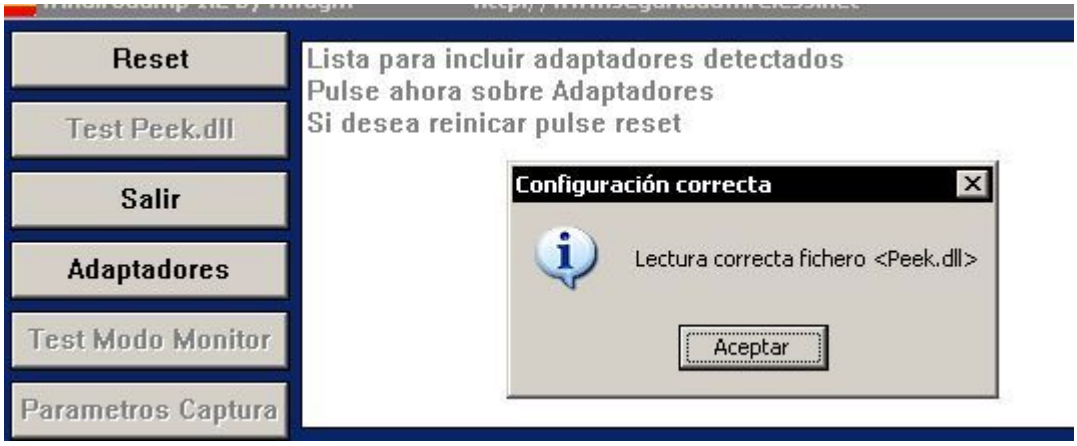


Verificación del modo monitor de nuestro adaptador.
Para confirmar que podemos trabajar en modo monitor tenemos la utilidad "winairdump":

Este programa es gratuito, y aparte de servirnos para capturar paquetes, nos es útil para confirmar el estado de nuestra tarjeta. Su pantalla inicial es la siguiente:

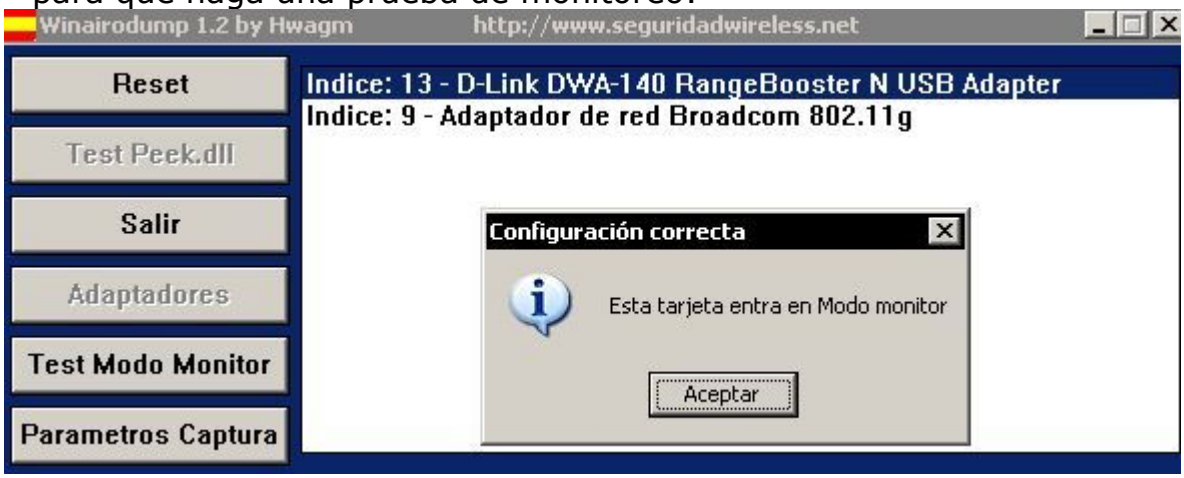


Pulsaremos sobre el botón "Test Peek.dll":



A continuación, y tras darle a "Aceptar", pulsaremos en el botón "Adaptadores", donde nos listará todos los que tengamos instalados en el sistema:

Tras ello, seleccionaremos el adaptador que vayamos a poner en modo monitor (cuyo índice es 13. Este índice es importante ya que lo necesitaremos después, por lo que podemos anotarlo). Una vez seleccionado el adaptador, le damos al botón "Test Modo Monitor" para que haga una prueba de monitoreo:



Si todo ha ido correcto, ya podemos cerrar el programa. En caso contrario nos aparecerá algo como lo siguiente:

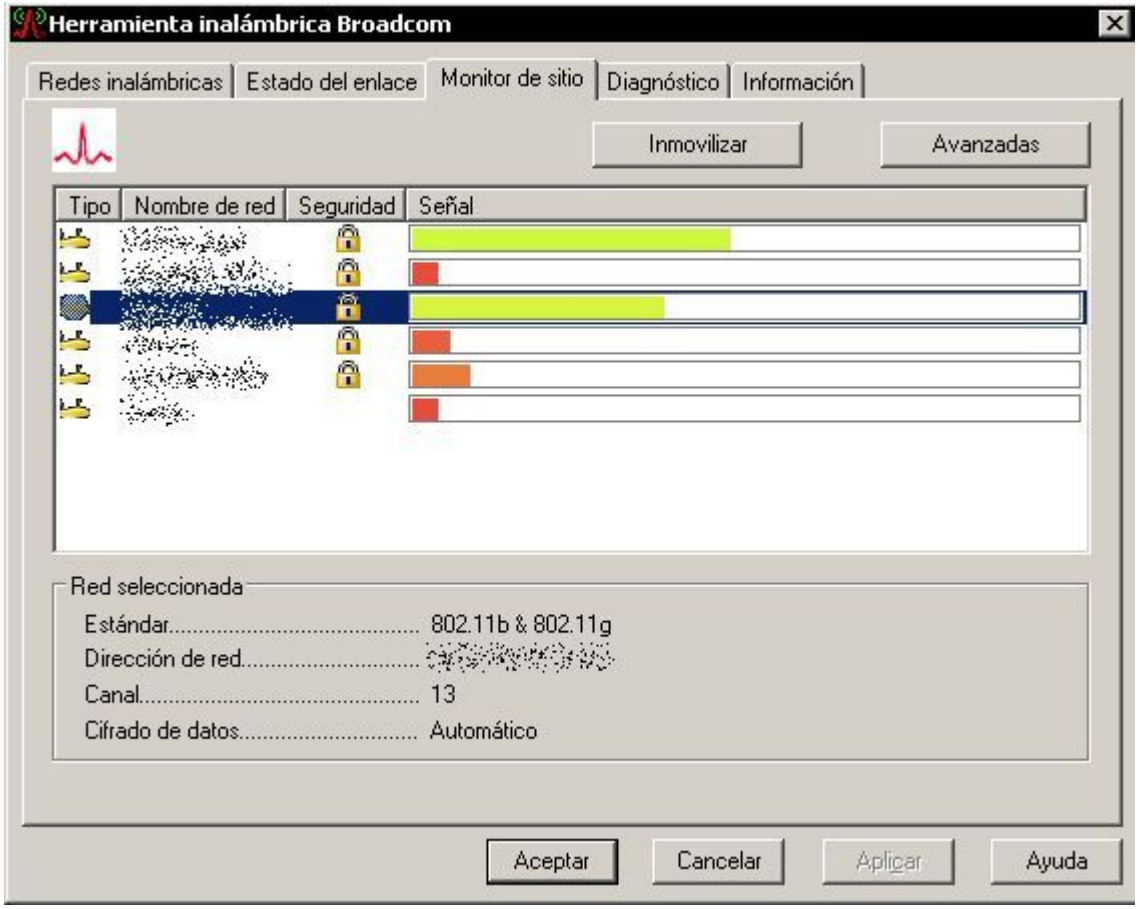
De ser este nuestro caso, tendremos las siguientes posibles causas:
- Que el driver que hemos descargado no esté correctamente instalado.
- Que el chip de nuestra tarjeta o adaptador de red no pueda trabajar en modo monitor con el driver que le hemos instalado.

Sea cual sea alguna de dichas causas, deberemos solucionarla porque, de lo contrario, no podremos continuar en los pasos siguientes.

Obtención de información de las redes Wifi.
Vamos a repasar los pasos que necesitamos dar para obtener la clave de una red Wifi:
1- Configurar nuestra tarjeta y ponerla en modo monitor.
2- Obtener la información necesaria de la red objetivo.
3- Obtener los paquetes de dicha red que viajan por el aire.
4- Desencriptar esos paquetes (previamente guardados) y obtener la clave.

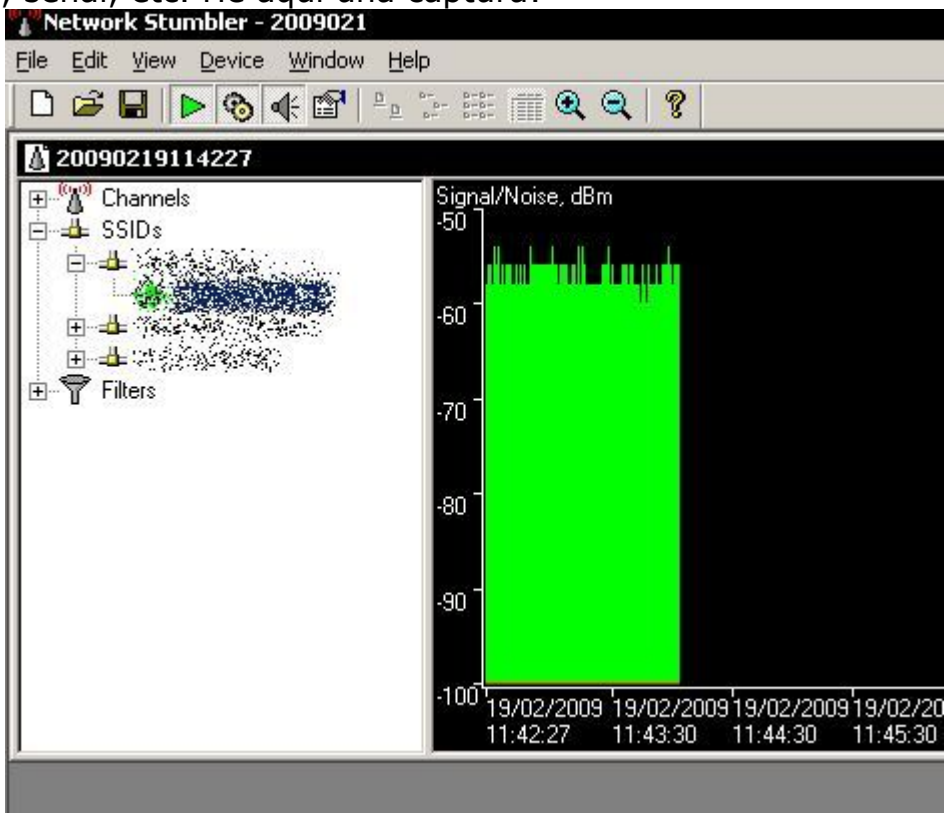
Para todas estas tareas se requieren de diferentes herramientas. Hemos visto algunas para preparar nuestro chip, ahora vamos a ver otras para poder obtener la información necesaria de las redes que están a nuestro alrededor.

Algunos de estos pasos se pueden obtener con cualquiera de los programas de seguimiento y scan de redes que integran casi todas las tarjetas del mercado. Éste es un ejemplo de uno de ellos:



Sin embargo existe una herramienta específica para la recogida de datos, se trata de Network Stumbler, cuyo icono de programa es el siguiente:

Con esta aplicación podremos obtener la dirección MAC de las estaciones, su SIID, así como potencia, señal, etc. He aquí una captura:



Todos estos datos deberemos anotarlos para posteriormente usarlos en el momento de la captura de paquetes, que vamos a ver a continuación.

Captura de paquetes: Airodump

Airodump es el programa más utilizado para la captura de datos con el fin de su procesamiento posterior. Aunque existen muchas versiones del programa, el icono del mismo para su funcionamiento en Windows es el siguiente:

Airodump-ng.exe, por su parte, es otra versión del mismo programa que funciona bajo MS-Dos y que viene integrado dentro de la suite denominada "aircrack-ng":

Nosotros vamos a utilizar el primero, ya que es mucho más intuitivo y trabaja mucho mejor en entornos Windows. Abrimos el programa con doble click y en su pantalla inicial nos informa de los dispositivos que tenemos en el sistema, y nos pide que elijamos uno para usarlo en modo monitor:

```
usage: airodump <nic index> <nic type> <channel(s)> <output prefix> [mac filter]


Known network adapters:

13  D-Link DWA-140 RangeBooster N USB Adapter
 9  Adaptador de red Broadcom 802.11g

Network interface index ->
```

Este es un buen momento para desactivar la radio de otros adaptadores o tarjetas que tengas (en caso de no haberlo hecho ya).
Como ya hemos visto, el índice que vamos a usar en nuestro caso es el 13 (cada tarjeta es diferente, por lo que variará el número de índice). Escribimos un 13 y le damos a la tecla intro:

```
Known network adapters:

13  D-Link DWA-140 RangeBooster N USB Adapter
 9  Adaptador de red Broadcom 802.11g

Network interface index -> 13


Interface types:  'o' = Orinoco/Realtek
                  'a' = Aironet/Atheros

Network interface type  -> _
```

Ahora nos pide que le informemos sobre la interface de red que vamos a usar, solo hay dos posibilidades, y debemos elegir una u otra dependiendo del chip que tengamos. En nuestro caso el chip es Realtek, por lo que escribiremos una "o" y pulsaremos intro:

```
Interface types:  'o' = Orinoco/Realtek
                  'a' = Aironet/Atheros

Network interface type  -> o

Channel list (0 = all)  ->
```

Ahora nos pide el número de canal **por el que va a escuchar**. Podemos seleccionar que escuche en todos los canales, en cuyo caso escribiremos un "0", pero como no queremos que haga tal cosa para que no recoja más *basura* de la necesaria, en nuestro caso pondremos el canal de la red a obtener el password, dicho canal sabremos en el canal Netstumbler, como ya se explicó en el paso anterior. A continuación nos solicita un nombre. Si la red se denomina, por ejemplo, "Markaplace", podemos elegir ese nombre para darle. En todo caso es indiferente, lo único que tenemos que tener en cuenta es que será el nombre que le dará a los archivos de los paquetes que capture, es decir: ese es el nombre de los archivos donde guardará los datos de la escucha. El nombre ha de ponerse sin extensión:

```
Network interface type  -> o

Channel list (0 = all)  -> 1

Output filename prefix  -> manualwifi

MAC filter (p = none)   ->
```

En nuestro caso hemos puesto de nombre "manualwifi". Ahora nos solicita la dirección MAC del canal que queremos escuchar. Esta dirección, que se escribirá en formato hexadecimal, la habremos obtenido también de Netstumbler, y la escribiremos con los dos puntos. Por ejemplo:
00:1C:F1:5F:E9:49

Esto es útil en el caso de que haya varias redes emitiendo por el mismo canal, de esta forma, el programa hará una selección entre ellas. Si escribimos "p", no filtrará las direcciones MAC y recogerá los datos de todas las redes que emitan en el canal que le hayamos puesto.

Una vez hecho ésto el programa pasará ya realmente a monitorear: el diodo luminoso de nuestro adaptador o tarjeta (caso de tenerlo) se apagará, y entrará a escuchar el tráfico de esa red. La pantalla que aparecerá será algo similar a la siguiente:

```
BSSID              CH  MB  ENC  PWR  Packets   LAN IP / # IVs   ESSID

[redacted]         -1  -1         5        2
                   -1  -1        20        2
                   -1  -1        20      187
```

En dicha pantalla se nos informa de los paquetes que recoge, el canal, las direcciones base y el nombre. No siempre están rellenados todos los campos, depende en gran medida del tráfico de la red, de las configuraciones y de lo que hayamos elegido a la hora de poner a trabajar el programa.

Anotar, además, que para cerrar Airdump podemos hacerlo con la combinación de teclas Ctr+C.

Lo que más nos importa ahora son los paquetes IV (Inicialization Vectors) que recoge. Cuantos más paquetes de este tipo tengamos, más posibilidades tendremos de averiguar la clave. Hay que tener en cuenta que no todos los paquetes que viajan por el aire son de éste tipo, comparativamente es un número bastante pequeño al tráfico habitual.

Desencriptador de paquetes: Aircrack

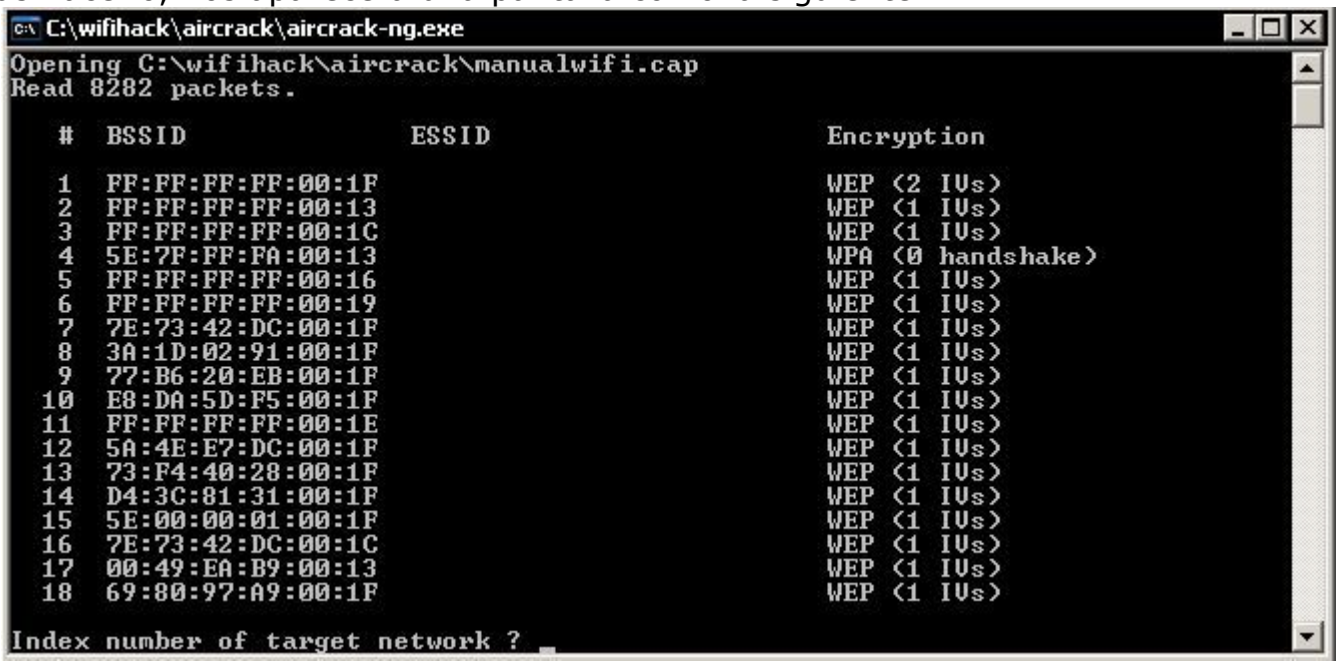
Aircrack podemos usarlo en modo Windows (aunque realmente no es 100% Windows, ya que se trata de un addon que lo simula y que no siempre trabaja adecuadamente), o en modo MS-Dos, que es mucho más eficiente.

Pero aquí vamos a ahorraros los engorrosos procedimientos de abrir una consola MS-Dos y ejecutar los comandos, sencillamente, vamos a decirle que desencripte la clave del archivo que acabamos de obtener. Como es un archivo pequeño, no obtendrá la clave de red, ya que lo hemos tenido monitoreando muy poco tiempo, pero como ejemplo sirve.

Simplemente, cogemos con el ratón el archivo .cap que nos haya grabado Airdump, y lo "dejamos caer" sobre el programa Aircrack-ng:

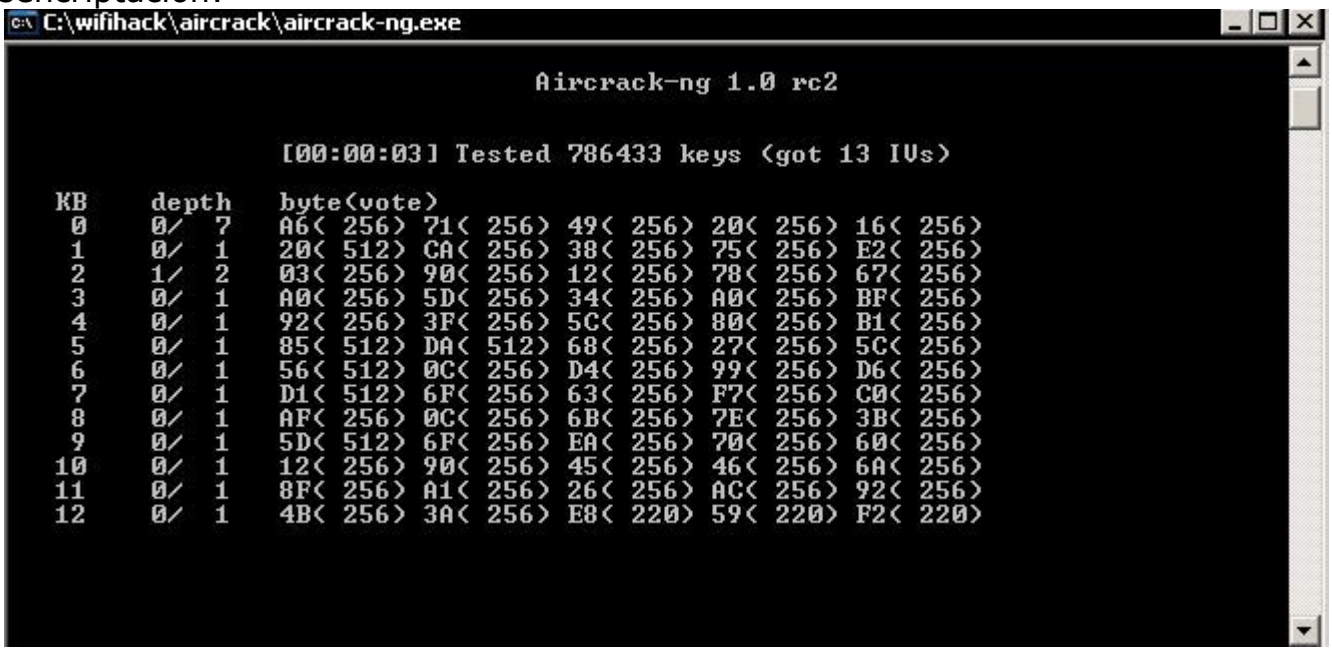
Esto podemos hacerlo cuantas veces queramos, aunque esté el programa Airdump trabajando. Simplemente tenemos que copiar el archivo .cap a la carpeta donde tengamos "Aircrack-ng.exe", y hacer éste procedimiento. Lo que no es conveniente hacer es tener ambos programas trabajando sobre el mismo archivo, ya que Aircrack va leyendo el mismo y no puede estar ya abierto por Airdump.

Tras hacerlo, nos aparecerá una pantalla como la siguiente:



Aquí vemos que nos dice los paquetes IVs capturados (en éste caso, como ya he mencionado, muy pocos e insuficientes para realizar una desencriptación) así como los BSSID.

Elegimos uno y pulsamos la tecla "intro", en donde realizará el propio proceso de desencriptación:



En caso de que hayamos obtenido un resultado satisfactorio, Aircrack nos informará de la clave en formato hexadecimal. Para que nos obtenga la clave en formato ASCII deberemos abrir el programa desde línea de comandos (para abrir una consola en MS-Dos sencillamente ve a inicio/ejecutar y escribe el comando "cmd", a continuación pulsa "Aceptar") y pasarle el modificador "-s" de la siguiente forma:

aircrack-ng -z -s *.cap

Donde:
-z utilizará el método PTW -sólo para claves WEP- que requiere pocos vectores.
-s nos dará la clave en formato ASCII
-*.cap seleccionará todos los ficheros .cap (es decir, los ficheros que nos ha obtenido Airdump) que tengamos en el directorio donde esté el programa Aircrack).

Si tenemos éxito, al final de la serie de números que vemos en la pantalla nos aparecerá algo similar a:
KEY FOUND! [12:34:56:78:90]

Con esa clave ya podremos acceder a la red que hayamos elegido. Por últimos, recordemos que podemos obtener todas las opciones de la suite Aircrack-ng simplemente accediendo desde MS-Dos y escribiendo el nombre del programa (.exe) que nos interese.

Accediendo a claves del router.
Otro procedimiento para obtener claves de red nos lo ofrece el programa "Wifi Decrypter", cuyo icono es el siguiente:

El uso de este programa es muy sencillo, y la única diferencia es dependiendo del tipo de router que nos interese.

Primero, de la lista desplegable tenemos que seleccionar el modelo de router, a continuación introduciremos su BSSID (que habremos obtenido del programa NetStumbler, como hemos visto anteriormente), y pulsamos el botón de "Obtener WEP". Nos aparecerá la clave en los tres campos, con tres posibilidades que podremos probar (todas ellas en formato hexadecimal).

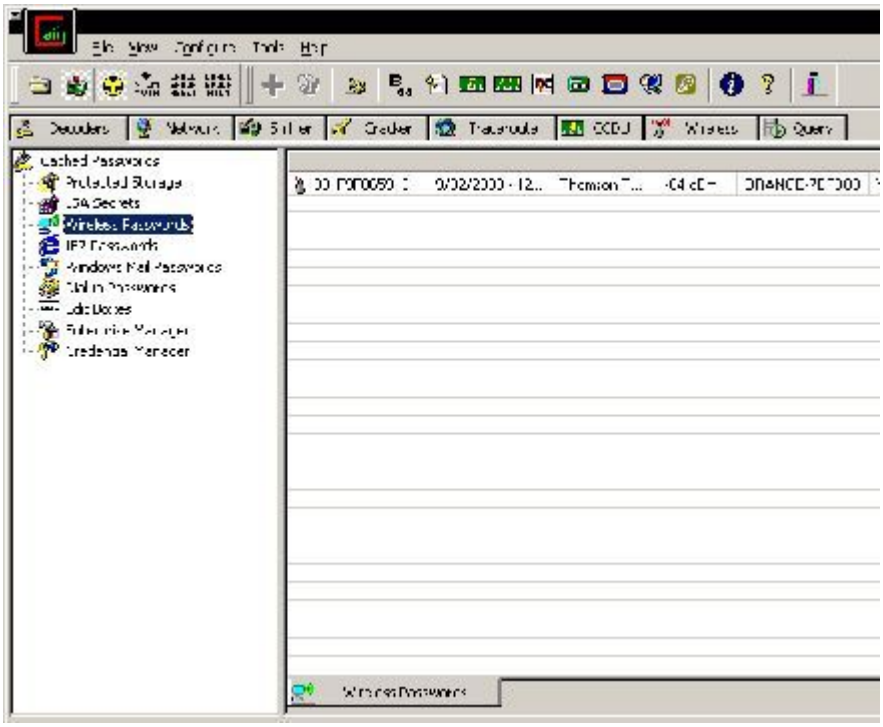
No obstante, el programa se acompaña de un completo manual al que es conveniente echar un vistazo antes de usarlo, por lo que no me extenderé más.

Sin embargo hay "un pequeño detalle" que no debemos olvidar: ¿y si desconocemos el modelo de router que tenemos o que nos ha enviado nuestro proveedor? Para eso existe una solución muy fácil, que veremos a continuación mediante el programa "Cain y Abel".

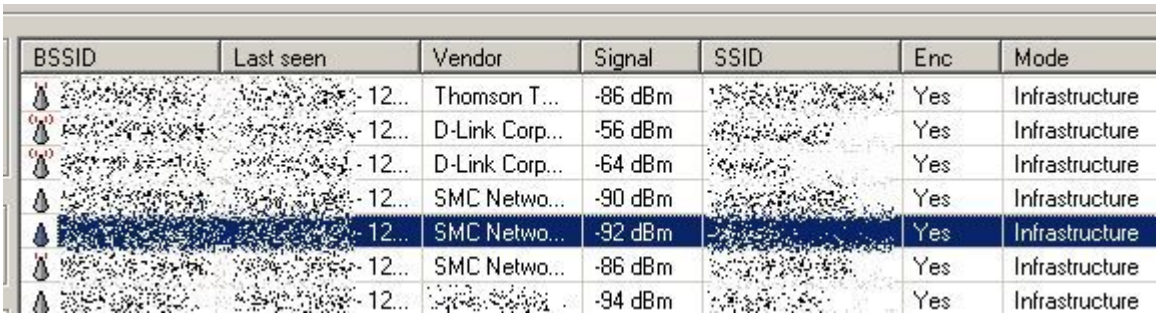
Rompiendo claves y obteniendo información: Caín y Abel.
Este programa permite obtener claves WEP fácilmente. Para hacerlo, nada más abrirlo seleccionamos la pestaña "Wireless Passwords", y, a continuación, la red de la lista principal, añadiéndola mediante el icono del "+" en la barra de tareas:

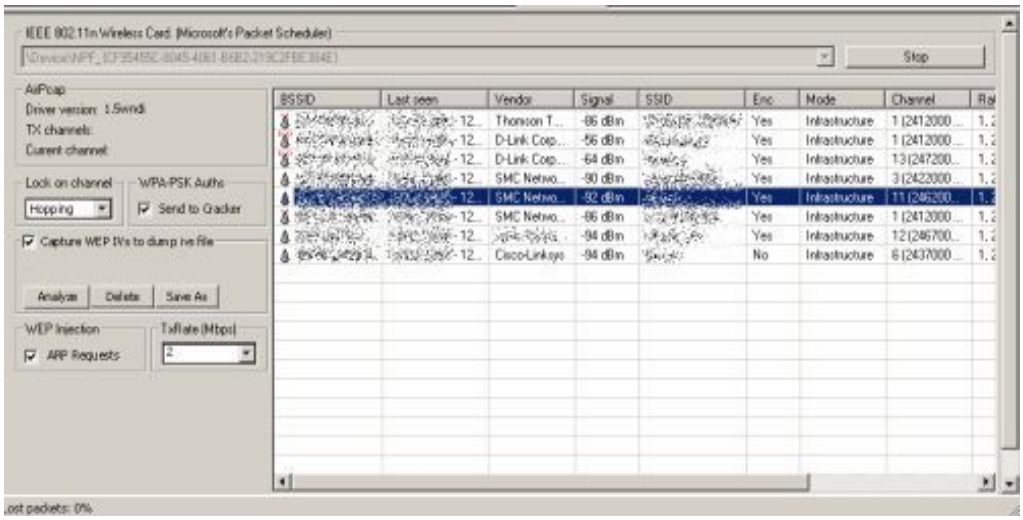
Si no se activa dicho icono significa que no podemos desencriptar la red, ya que los drivers instalados mediante la utilidad Wincap no son compatibles con nuestra tarjeta.

Una vez seleccionada la red, simplemente tendremos que hacer click con el botón derecho del ratón y elegir el tipo de ataque que queramos forzar para el password, entre cuyas opciones nos dirá: ataque por diccionario (mediante una lista de palabras que irá probando), ataque de fuerza bruta (mediante una serie de paquetes), y ataque criptográfico:



Otra de las opciones interesantes es que podemos conocer **el modelo de router** de las redes que estén a nuestro alrededor. Ello aparecerá en la pestaña Wireless, donde también, nos permitirá capturar paquetes de vectores (similar al Airdump que hemos visto anteriormente), y que guardará con la extensión .ivs. Dichos paquetes podremos usarlos por el mismo programa para analizar (pulsando el botón "Analyze") así como para inyectar datos de tráfico (en el apartado de WEP Injection). También permite actuar sobre redes con encriptación WPA-PSK.





Rompiendo claves y obteniendo información: CommView for Wifi.
A diferencia de los anteriores, "CommView for Wifi" es un programa de pago, y que incluye innumerables herramientas de acceso y monitoreo de redes Wifi. Funciona bajo Windows y comparte con "Caín y Abel" que utiliza las librerías de Wincap.

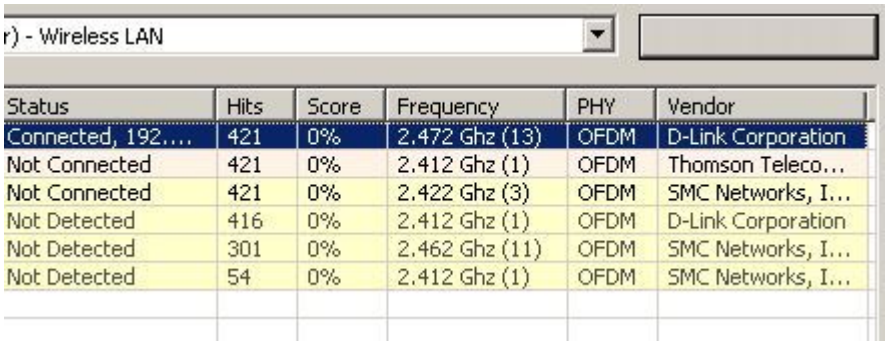
Estas librerías (que han de descargarse aparte) sólo son aptas para tarjetas Wifi, es decir, no nos funcionarán en adaptadores USB (es más, "Caín y Abel" ni siquiera accederá a la red con ellas), por lo que si disponemos de adaptadores Wifi no podemos usar ninguno de ellos, ya que para este caso Wincap fabrica adaptadores específicos que vende aparte.

Si estás interesado en éste programa, dispones de un amplio manual al que puedes acceder desde "Seguridad Wireless", por lo que no nos extenderemos más con él:
http://hwagm.elhacker.net/commview/monitorwin.htm

Seguridad y defensa inalámbrica: Wifi Hopper

Wifi Hopper es una más de las muchas herramientas de testeo de seguridad para redes que existen. Al igual que CommView, es una herramienta de pago, y permite tanto monitorizar nuestra propia red en busca de los puntos débiles que pueda tener, como permitirnos conectarnos a otras redes inseguras.

No posee herramientas de penetración propiamente dichas, pero sí nos da datos interesantes como las frecuencias de emisión, canales y, al igual que "Cain & Abel", el nombre del fabricante del router de las redes:



Status	Hits	Score	Frequency	PHY	Vendor
Connected, 192....	421	0%	2.472 Ghz (13)	OFDM	D-Link Corporation
Not Connected	421	0%	2.412 Ghz (1)	OFDM	Thomson Teleco...
Not Connected	421	0%	2.422 Ghz (3)	OFDM	SMC Networks, I...
Not Detected	416	0%	2.412 Ghz (1)	OFDM	D-Link Corporation
Not Detected	301	0%	2.462 Ghz (11)	OFDM	SMC Networks, I...
Not Detected	54	0%	2.412 Ghz (1)	OFDM	SMC Networks, I...

Con esta información "de por sí" poco podemos hacer, pero ya hemos visto que es muy útil para usarla en otro tipo de aplicaciones, así como de su PHY (OFDM, de "Orthogonal Frequency Division Multiplexing").

La frecuencia de operación es también otro dato interesante, que podemos usar para comparar con las demás redes y la potencia de nuestro router, la fuerza con la que nos llega la señal dependiendo de la distancia, etc.

Todos estos datos, si bien no son imprescindibles para la penetración o comprobación de la seguridad de las redes, sí son muy estimables en cuanto al monitoreo, incluso bastante más que los propios gráficos que poseen muchas de estas herramientas (Wifi Hopper no iba a ser menos y también puede presentarnos los datos en modo escala gráfica).

Hacking wireless desde dispositivos móviles.
Principalmente es Nokia con su 770 y 8xx quien posee las mejores herramientas de test y monitoreo de red, e incluso, de asalto inalámbrico y hackeo. Su uso no difiere mucho con el uso de este tipo de aplicaciones en Linux, con lo cual se sale del objeto de éste manual y nos referimos únicamente a ello para mencionar su existencia.

Windows Mobile también posee bastantes herramientas, centradas, en éste caso, en *sniffers* (captura y escucha de red) y terminales cliente. Incluso podemos encontrar para dicha plataforma un MiniStumbler con algunas de las funciones que hemos visto en el presente manual.

Sirva únicamente como primera acercamiento al lector las siguientes URLs:
http://www.irongeek.com/i.php?page=security/ppchack
http://www.irongeek.com/i.php?page=maemo/nokia-770-800-hacking-pen-testing

Cómo proteger nuestra red wifi.
Seamos realistas: no se puede proteger una red wifi. Cualquier hacker (o cracker) que desee entrar en tu red va a hacerlo. Da igual si le pones uno o mil candados, o si decides ponerle una clave de alta seguridad o no. La única diferencia puede ser que necesite un poco más de tiempo, pero tu vecino, o cualquier desconocido, puede usar tu red Wireless sin mucha complicación.

Si quieres proteger tu red, no uses wifi. Usa el cable, o métodos físicos, donde la transmisión de datos no se haga mediante ondas de radio, sino mediante elementos físicos.

Si, no obstante, no tienes otro remedio, aquí van una serie de consejos que te pueden servir:

- Cambia tu clave diariamente. En algunos sitios de seguridad aconsejan cambiar la clave de red (y de router, incluso) semanalmente. Pero eso no resultará molesto a quien de verdad le interese utilizar tu conexión. Cambia la clave que uses diariamente, aunque ésto no evitará que accedan a tu conexión, sí les causará más molestias, y, en última instancia, puede que tengas suerte y acaben eligiendo a otra víctima menos cuidadosa.

- Deja tu red libre. Muchas personas dejamos las redes Wifi libres cuando no las usamos para que acceda quienes lo necesiten. Esto no influye en la seguridad de tu red, más bien al contrario (un hacker o una persona que vaya a hacer daño, si ve una red libre, habitualmente, no suele fiarse de ella). Los que usan las redes libres son los que "no tienen conocimientos profundos", y, aunque tu red la use una persona experimentada, tampoco has de preocuparte, porque no pueden dañar físicamente ningún elemento que poseas. Si todo el mundo dejásemos las redes Wifi que tenemos libres, para el acceso de todos, los precios se abaratarían y se haría menos necesario herramientas de asalto a las redes. Mientras los precios de acceso a Internet sean caros y las redes libres tan limitadas y escasas en número, seguirá habiendo gente que esté obligada a hacer lo que sea por acceder. Piensa que alguien con una tarjeta wireless que no tenga conexión a Internet pero sí mucho tiempo libre, puede estar bombardeando los accesos wifi de su zona durante días enteros, incrementando inútilmente el tráfico. Si los ayuntamientos, asociaciones de vecinos y los propios particulares que tenemos acceso a Internet fuésemos un poco más "generosos" con las personas que carecen de dichos servicios, aún a día de hoy, haríamos que el vínculo del ciberespacio fuera un poco más humano, como debería de ser. Además, no está de mas realizar una buena obra de cuando en cuando, y permitir durante el tiempo que no la usemos que accedan a la Red seres anónimos es una de ellas.

Muchas personas argumentan ante esto que algunas Universidades y centros educativos bloquean los accesos a sus redes, cuando deberían ser las primeras en disponer de puntos abiertos ("hot spots"); pero la explicación es bien sencilla: el que determinados organismos sólo dejen usar las conexiones a sus miembros es debido a que si accediera todo el número de usuarios que los visita o están en la zona su red podría llegar a saturarse, quitándoles el servicio a ellos mismos. Esa es una de las principales razones por las que existe un "cupo de admisión" para el uso de Wireless en zonas concretas, porque, recordemos, el ancho de banda es limitado.

- Modifica tu dirección MAC: Hemos visto que es esencial conocer la dirección MAC de una red para poder atacarla y obtener su clave de acceso. Herramientas como "MAC Addres Charger": (http://www.technitium.com/tmac/index.html) nos permiten cambiar nuestra dirección MAC y, de éste modo, "engañar" a los hackers que intenten asaltarnos. No obstante tampoco es una herramienta definitiva (alguien que sepa nuestra contraseña entrará indiferentemente de que hayamos cambiado la MAC o no), pero como prevención es altamente eficaz.

Se aconseja que primero cambiemos la clave de acceso a nuestra red y, a continuación, cambiemos su MAC. De esta forma ya podremos ir variando la MAC cada poco tiempo.

No obstante volvemos sobre el punto anterior: cualquier hacker medianamente diestro puede obtener nuestra clave en unos pocos minutos, sobre todo si ésta es WEP de encriptación débil.

Conclusión.
Hemos visto algunas de las más útiles herramientas de monitoreo y penetración inalámbrica, y también hemos visto lo fácil que es introducirnos en una red privada que trabaje con el protocolo Wifi. Además, nos hemos detenido brevemente en aplicaciones para móviles, dejando palpable que cualquier persona con un dispositivo móvil puede obtener la clave de nuestra red Wifi sin muchos inconvenientes.

Por último, hemos hecho un pequeño repaso a la seguridad de nuestra propia red, dando unos consejos sobre cómo podemos defenderla de personas indeseables (principalmente hackers que pueden llegar a atorar nuestro ancho de banda) y la ética mínima de generosidad que debería imperar entre todos los usuarios y poseedores de redes.

El cometido del presente trabajo (presentar de forma amena y clara las herramientas de penetración inalámbricas) se ha cumplido, pues, con creces. Me gustaría apuntar, antes de dar por finalizado éste manual, la necesidad de que todos, organismos públicos y particulares, tengamos una mente más abierta y disponible para hacer accesible Internet al gran público, de lo cual nos beneficiaríamos la población entera y haríamos que las operadoras disminuyeran sus abusivos precios de conexión. Confiemos en que, en un futuro no muy lejano, podamos ser como los países más desarrollados, donde con prácticamente cualquier dispositivo uno puede hacer uso de la Red de redes de una forma sencilla y accesible, de esta forma, los hackers y la intromisión dejarían de tener sentido y la seguridad inalámbrica se centraría en los secretos oficiales e industriales, así como en el sector empresarial, que es donde tiene su auténtica razón de ser, para proteger las comunicaciones más importantes y necesarias.

Fénix Hebrón.

Contenido