Antes que nada comentar que este texto, esta basado principalmente en el que hizo Aironjack es decir simplemente he cogido su manual con su permiso y lo he ampliado, añadiendo y ampliando algunos puntos que veia flojos.

http://foro.elhacker.net/index.php/topic,56008.msg270070.html#msg270070

INTRODUCCION

Bien en este post vamos a intentar explicar la (in)seguridad de una red wireless domestica, ya que no nos meteremos en seguridad para gente más avanzada, me refiero a las VPN y a los túneles IPSEC, entre otros métodos de seguridad.

Lo que conseguiremos con esto es aprender a acceder a una red inalámbrica (wireless, wlan...) ajena, que herramientas necesitamos para ello, y así utilizar su ancho de banda para conectarse a Internet, adquirir datos, archivos o simplemente para comprender el tema, y así montar una red segura, aprendiendo de las vulnerabilidades de este tipo de redes.

IMPORTANTE: Recordad que meterse en una red ajena y utilizar su ancho de banda reservado para Internet es ilegal.

No nos centraremos en como penetrar en un sistema que se encuentre tras un router.

Todo sobre hacking de una máquina en red que se conecta a través de un router en:

http://foro.elhacker.net/index.php/topic,62799.msg287872.html#msg287872
Bueno también comentar que tampoco hablaremos de los tipos de ondas, espectros. Tampoco hablaremos de la distancia, del ruido y demás factores que hacen que perdamos calidad de señal, tampoco hablaremos de las normativas ni estándares (como mucho nombrarlos), es decir lo que son conceptos básicos de las redes wlan, los dejaremos de lado. Ya que para esto (y muchísimo más) tenéis a vuestra disposición el taller wifi de Vic_Thor, en el foro de HxC (HackxCrack). Os dejo la URL:

http://www.hackxcrack.com/phpBB2/viewtopic.php?t=21310

Por último y antes de empezar, este post va dirigido a todas las personas que no dejan de postear una y otra vez la misma duda, quizás sea sin saberlo, pero que la solución es muy parecida, en definitiva este post va dirigido a usuarios de Windows.

Añadir, que las posibilidades que nos brindan los drivers desarrollados para Windows no tienen ni punto de comparación con los desarrollados para Linux. Aunque la mayoría sabremos que los fabricantes de hardware se olvidan de los usuarios que utilizan otros sistemas operativos, que no sean Windows, es decir, aparte de Linux, MAC-OS, Free-BSD, Novell, etcétera.

Una imagen de la tira Escomposlinux.org viene muy al caso 

En Windows nos conformaremos con poder poner nuestra tarjeta en modo monitor (ya hablaremos de ello mas tarde) y poder así monitorear o sniffar el tráfico de la red.

Después de esta introducción o aclaración... empecemos con los dispositivos wireless

Adaptadores inalámbricos

Bueno este hardware es el que no permite conectar con otros dispositivos inalámbricos, sin necesidad de utilizar un cable, como pueden ser otros adaptadores inalámbricos, routers inalámbricos, y un largo etcétera.
Se presentan en muchos formatos, pero sobretodo, para los PCs de sobremesa en PCI y para los pórtateles en PCMCIA o CARDBUS (parecidos, pero no son lo mismo) y últimamente también aparecen en USB.

Los AP (Access Point)

Normalmente suelen ser un módem-router (en las conexiones domésticas) ya que son muchos lo proveedores de Internet (ISP) que con sus ofertas wifi ofrecen un router inalámbrico que al mismo tiempo funcionan como modem. Por lo tanto, no todas las redes inalámbricas tienen porque tener conexión a Internet, aunque la mayoría la tendrán por lo que he comentado anteriormente.

Hablemos ahora un poco sobre la configuración de routers. Bien, estos routers contienen como un "servidor" que nos permite acceder a su configuración, donde podremos activar a parte de configurar todos los elementos de seguridad (WEP, ACL, DHCP…) de que disponga nuestro router, también podremos configurar el direccionamiento de los puertos (NAT), aunque esto ya se aleja del tema de seguridad para entrar en este tipo de redes.

Ya hablaremos de los elementos de seguridad más tarde, por ahora que se os quede que para configurar todos esos parámetros debemos acceder al router.

Para ello los router disponen como de un servidor, normalmente Web, aunque también pueden ser por Telnet, o incluso por FTP (para subir archivos de configuración ROM).
Para acceder a ellos usualmente se pone en la barra de direcciones de nuestro navegador la IP del router (usualmente 192.168.1.1 o 192.168.1.0) o si preferimos por Telnet pues hacer telnet a la IP.
Para entrar a la configuración nos pedirá un user y un password, o simplemente un password, también depende del modelo del router.
Por lo tanto podemos concluir que es muy importante averiguar con que router estamos tratando y buscar un manual sobre éste en la pagina del fabricante, a no ser que el router sea nuestro y ya poseamos uno, por lo tanto muy importante leerlo.
También hablaremos de cómo sacar el password de un router en este tipo de redes.

Comentar que con algunos programas, que yo conozca solo con linux, podemos hacer funcionar dos adaptadores inalámbricos en un mismo PC como un AP (hostAP) pero de eso ya hablaremos en otra ocasión si surge, por ahora, este post intenta centrarse en la seguridad de redes.
Entonces algunos os preguntareis por que lo comento, pues bien para aquellos curiosos, que piensen un minuto en ello. Así es, también se podría incluir en el tema de seguridad ya que pensando otra vez más, imaginemos la de cosas que podríamos hacer si engañásemos a todos los dispositivos de la red, para que creyesen que nuestro adaptador inalámbrico es el AP de la red inalámbrica, así crearíamos un man-in-the-middle pero para redes inalámbricas.

Pero repito que en este post no hablaremos sobre ello. oohh que pena!! 

Volviendo a los adaptadores inalambricos,

¿Que los diferencia? ¿Que hace que sea tan importante su elección?

Aparte de la sensibilidad de recepción, la potencia de salida, la posibilidad de añadir una antena (conectores...) el estándar o protocolo que utiliza (IEEE 802.11a/b/g), la posibilidad de calibrar la potencia de emision... etcetera.
Como ya he dicho antes no iba hablar sobre esto, os recomiendo que visitéis el taller WIFI que al principio comentaba.

Bien, pues aparte de todo esto, una diferencia muy importante y que no nos la especifican ni en la caja, ni en el manual de instrucciones ni en ningún sitio, es el CHIPSET.
Bien hay distintos chipsets, los mas “famosos” son:

- Intersil Prism
- Atheros
- Hermes u Orinoco
- Cisco Aironet
- TI (Texas Intruments)
- Realtek
- Symbol
- Atmel
- Y bastantes mas

Pues bien, la cuestión, esta en averiguar que chipset incorpora nuestra tarjeta.
Se añade una pequeña dificultad y es que cada fabricante (Conceptronic, Intel, Dlink …) cada modelo (c54C, 2200BG, 520G) e incluso cada revision (-G520+, 2200BG+) no tienen porque tener el mismo chipset, es decir diferentes fabricante pueden coincidir en dos modelos en el mismo chipset, aunque sean diferentes fabricantes, es como si el mundo de los chipsets no estuviese ligado al de los fabricantes.

Por lo tanto se elaboró una lista, bastante extensa, con fabricante, modelo e incluso algunas revisiones. Os dejo la URL:

http://www.linux-wlan.org/docs/wlan_adapters.html.gz

Si vuestra tarjeta no sale en la lista, buscad en Google.

Bien como en este post, hablamos para Windows, recomendare una tarjeta que tenga un chipset Atheros o Realtek, que según la pagina Web del programa AirCrack, tiene una compatibilidad 100%.

Eso si necesitaremos los drivers que anteriormente he comentado de WildPackets:

http://www.wildpackets.com/support/hardware/airopeek

Visitamos esta Web y como vemos hay un listado de tarjetas compatibles (aún hay muchas mas dentro de los enlaces de los drivers), como vemos no solo hay con chipset Atheros o Realtek, sino alguna Symbol, Agere…, buscamos a ver si esta nuestra tarjeta, pero si no lo

esta, nos descargamos un driver de un enlace que ponga el chipset de nuestra tarjeta.
Por ejemplo si nuestra tarjeta no está por ninguna lado, pero sabemos, gracias a la lista de adaptadores que nuestra tarjeta tiene una Atheros, pues vamos al enlace y nos descargamos el driver para Atheros (repito: aunque no este nuestra tarjeta escrita por ninguna lado), si tenemos una tarjeta con chipset Realtek, pues igual.

INSTALACION DEL DRIVER

Pasemos a instalar el driver que nos hemos descargado.

- Descomprimís el archivo.
- Ejecutamos: compmgmt.msc
- Allí dentro vamos al Administrado de Dispositivos
- Miramos los adaptadores de red
- Allí dentro debe estar nuestra tarjeta inalámbrica instalada
- Botón derecho del ratón y le damos a actualizar
- Desea que Windows se conecte…. ¿? NO!
- Instalar desde una ubicación…
- Incluir esta ubicación en la búsqueda y quitamos la marca de buscar en CDs.
- Examinamos y buscamos el *.inf que descomprimimos al principio.
- Si nuestra tarjeta sale por los menus que salen, pues la seleccionamos
- Si no sale, le damos al genérico de Atheros (por ejemplo)
- Después de que se instale, reiniciamos.

Ya tenemos los drivers de WildPackets instalados.

Bien ahora ya podremos poner la tarjeta en modo monitor, y así poder sniffar paquetes con el AiroPeek, Ethreal, Airodump….

CAPTURANDO PAQUETES Y AVERIGUADNO EL CIFRADO

El programa que recomiendo en Windows para averiguar el cifrado Wep, es el Aircrack muy fácil de utilizar e intuitivo.
Y además porque incluye el Airodump, un programa para capturar paquetes, también muy fácil de utilizar.

Antes que nada una descripción de lo que haremos, en dos líneas:

- Primero capturaremos paquetes con el Airodump.
- Segundo una vez con suficientes paquetes validos, averiguaremos el cifrado.

Primero que nada, donde descargar los programas, los dos programas, se encuentran en un mismo archivo ZIP, aquí:

http://www.cr0.net:8040/code/network/aircrack-2.1.zip

Lo que ocurre es que en este ZIP, no encontrareis algunos archivos esenciales:
- Peek.dll
- Peek5.sys
- MSVCR70.dll

Podéis buscarlos por Internet y copiarlos a misma carpeta donde esta “aircrack.exe” y “Airodump.exe”

Una vez tengáis el Airodump extraído, los archivos estos en la misma carpeta y vuestra tarjeta con los drivers compatibles instalados, ya lo tenemos todo para empezar a esnifar la red.

Así que ejecutamos el Airodump.exe, una vez abierto detectara todas las tarjeta habilitadas en el sistema de forma automática, introducimos el numero que hay a la izquierda de la tarjeta inalámbrica.

El siguiente paso es seleccionar el tipo de interfaz de la red, (Atheros, Aironet / Orinoco Realtek), pues depende cada uno del driver y de la tarjeta que tenga.

El siguiente paso es elegir el canal. Si pones cero, dará por entendido que no quieres filtrar ningún canal y los esnifara todos, útil si no sabes el canal de la red que quieres esnifar.

El siguiente es el nombre del archivo donde guardara los paquetes, no hace falta poner ninguna extensión, ya que automáticamente ya la crea.

El siguiente sirve para filtrar MACs, es decir el programas solo aceptara los paquetes de la MAC que escribas, el formato debe ser 00:00:00:00:00, es decir hay que añadir los dos puntos ":". Por supuesto para no filtrar ninguna y procesar todos los paquetes de todas las MACs, tendréis que escribir una "p" y listo. Se puede combinar con el filtrado por canales sin problemas.

Por ultimo si todo ha ido bien empezara a capturar paquetes.
Pues bien dependiendo de la cantidad de trafico que haya, puedes tardar mas tiempo o menos, es logico a mayor cantidad de trafico mas IVs nos llegaran.

Mas o menos con un millon de IVs es suficiente para una llave de 128 bits (104 bits reales) para una de 64 pues la mitad  , claro que yo os recomiendo que por si acaso no pareis de capturar, es decir imaginaros que estais capturando paquetes y llega al millon, pues en vez de detenerlo y pasar a crackearlo, pues cojeis vuestro archivo.cap que por momentos ira creciendo y haceis una copia de él en la misma carpeta, todo esto sin parar el airodump.

Esto os lo digo, por experiencia propia, ya que a veces, como el crackear un cifrado no es una ciencia totalmente cierta, pues a veces el programa nos muestra un desagradable mensaje, eso si muy educado  que dice "No luck, sorry" y como habia parado el airodump tuve que empezar a capturar mas paquetes, pero desde cero.

Si veis que capturais muy poco o si simplemente no cojeis ningun IVs, podria ser por esto:

- Aseguraos que es WEP y no WPA
- Que no esteis demasiado lejos y solo te lleguen los Beacon Frames
- Si vuestra tarjeta no es compatible con el 802.11g, y el AP solo emite en 802.11g y no en 802.11b, no os funcionará.
- Si aparte de esa red existen otra, prueba a especificar la MAC del AP (BSSID)

Tambien puede ser que vuestro driver este mal instalado. Revisarlo.

CRACKEANDO CON AIRCRACK

Por supuesto el programa, tambien es muy facil de utilizar. Pero voy a intentar explicar las opciones para que no hayan dudas.
Comentar que el programa tambien funciona en linea de comandos. Para los que les gusta 

Este es el programa
Citar

```
                aircrack 2.1 - (C) 2004 Christophe Devine

                     usage: aircrack <pcap filename(s)>
```

```
5 : debug - specify beginning of the key
4 : bruteforce fudge factor (current: 2)
3 : packet MAC filter: 00:00:00:00:00:00
2 : WEP key length in bits, current: 128
1 : read IVs from  a specified pcap file
  0 : start cracking (with 0 WEP IVs)
```

Bien la opcion 5: esto nunca lo he utilizado, pero creo que sirve para especificar tu una llave y ver cuanto tarda en crackearl aunque creo que no es eso. La verdad no estoy nada seguro :\

Bien la opcion 4: yo esto no lo tocaria a no ser que repetidamente os salga el mensaje de "No luck, sorry". Bien lo que hace exactamente no lo se. Pero sirve para aumentar la cantidad de llaves a probar. Es decir si con 5000 llaves no encuentra la clave acertada, pues aumentas el numero (por defecto 2) y asi probara mas llaves posibles.

Bien la opcion 3: No creo que haga falta mencionarla, simplemente es un filtro de paquetes que solo acepta los de la MAC introducida. Bueno la forma debe ser con los dos puntos ":"

Bien la opcion 2: Sirve para especificar la longitud de la llave. Por defecto es 128 (lo mas común). Comentar una ventaja y es que imaginaros que no sabeis si sera de 128 o de 64, pues bien, vosotros lo dejais como esta por defecto (128 bits) y si es de 64 bits la sacara de todas formas.

Bien la 1: lo que hace es leer los paquetes validos (IVs) del archivo.cap y enumerarlos. Solo hay que introducir el nombre del archivo (este debe estar en la misma carpeta y hay que incluir la extension, normalmente .cap)

Bien la 0: pues eso empieza a crackear.

Cuando acabe pondrá un mensaje de **KEY FOUND**, y ya la teneis.

Ha sido facilisimo, eso si caputara paquetes a veces se hace insoportable.

Después de aprender como crackear un cifrado WEP, ya podemos pasar a otros puntos de seguridad en una red inalámbrica.

Comentar que antes de intentar hacer cualquiera de las cosas que explicare un par de definiciones.

Beacons, beacons frames, balizas de autenticacion: son tramas que emiten los puntos de acceso, o en su defecto los routers inalámbricos, para que otros puntos de acceso o tarjetas inalámbricas sepan que existe un punto de acceso activo por las cercanías.
ESSID (SSID): es una cadena de texto de hasta 32 caracteres, se emite por defecto en los beacons frames, se utilizan para diferenciar diferentes redes inalámbricas en un mismo canal. Por lo tanto es muy importante conocerlo. Por eso mismo es otra medida de seguridad. Ya hablaremos de ello.

Dos cosas muy importantes no solo en la redes 802.11, sino en todos los aspectos: debeis cambiar los pass por defecto, por ejemplo tanto como el ESSID, como la password de acceso a la configuracion del router. Asi como acutalizar los firmwares de vuestro hardware, para tapar ciertos agujeros que podrian tener y que podrian ocasionar por ejemplo una denegacion de servicio (DoS), aunque nadie (o casi nadie :\) se salva de una denegacion de servicio por ondas microondas, jejeje.

Detectando redes inalambricas y accediendo a ellas:

Bien esta parte es muy sencilla, aunque puede complicarse.
Simplemente con el NetStumbler:
Aquí para descargarlo:

http://www.netstumbler.com/downloads/netstumblerinstaller_0_4_0.exe

Aquí para descargarte el manual (incluido un FAQ para errores y demás)

http://www.netstumbler.com/downloads/netstumbler_v0.4.0_release_notes.pdf

Una vez tenemos este programita instalado detectaremos la gran mayoría de redes.

A no ser que los beacons frames estén desactivados, o que los beacons esten activos pero el ESSID este oculto (muy pocas veces se dan estos casos pero los intentare explicar como solucionarlo).

Nota de seguridad: Bien esta es una medida de seguridad, no todos los routers lo permiten, lo ideal seria que se dejasen de emitir beacons, aunque si no puede, algunos routers lo que permiten es ocultar el ESSID en los beacons frames.

Aunque de muy poco sirve, si tenemos nuestra tarjeta en modo prosmicuo, simplemente tenemos que poner nuestra tarjeta a escuchar, ejecutar el airodump, sin ningun filtro, ni para los canales ni para las MAC de los APs (BSSID), de este modo caputaremos todos lo paquetes que andan sueltos por ahi.

Si los beacons estan desactivados (cosa muy pero que muy poco habitual) como no tenemos linux y no podemos desauntenificar a un cliente de la red para que automaticamente se reconecte y asi poder ver la beacon que le manda el AP, pues lo unico que podemos hacer es esperar que algun cliente se conecte, pero ya digo que esto se da muy poquisimas veces.

Una vez detectada la red y averiguada su WEP (si es que tiene)

Una vez tenemos esto (es importante volver a instalar los drivers anteriores de la tarjeta), intentamos conectarnos o asociarnos a la red, (por favor antes configurad vuestra tarjeta para activar DHCP, es decir para que el router os de una IP automaticamente).

Yo personalmente prefiero utilizar el software que viene con la tarjeta que utilizar la herramienta wireless de Windows.

Pero como cada programa es diferente, explicare algo sobre la herramienta de Windows.

Cuando sale una imagen de un candado y dice "**Esta red tiene seguridad habilitada**"o algo por el estilo, esto significa que tiene el cifrado activo, y por lo tanto necesitas una clave, la que antes conseguiste.
No intentes conectarte a una de estas redes sin saber la clave.

Cuando te sabes la clave o simplemente no esta activado el cifrado, pero te sale un mensaje de "**Conectividad Nula o Limitada**", no te asustes, en el caso de este tipo de redes, seguramente sea:

Porque la llave WEP que metiste no es la acertada (si la sacaste con Aircrack, reescribela) y podeis comprobarlo porque no recibireis ningun paquete, esto lo podeis mirar pinchando en el icono de la barra de tareas. Pues en recibido habra cero.

O tambien puede ser porque el router tiene desactivado el DHCP, es decir los clientes deben configurar su IP, su mascara y su puerta de enlace, y por lo tanto deben saber en que subred se encuentra configurada la conexion, asi como la puerta de enlace (los mas usuales son del tipo 192.168.xxx.xxx).
Para averiguar la puerta de enlace, por ejemplo y mas datos debemos volver a instalar los drivers de WildPackets y monitorizar un poco de trafico y con un analizador de paquetes (si en la red esta activado WEP, debemos desencriptar los paquetes, el ethreal creo que no lo hace pero el AiroPeek, si que lo hace), averiguarlos (esto no es un proceso automatico, es decir teneis que intentar comprender la estructura del paquete, si tengo algo de tiempo, subire algunas imagenes como ejemplo).

Bueno y una vez sabiendo la puerta de enlace, ya podemos configurar nuestra IP y la puerta de enlace, por supuesto.(la mascara de subred casi siempre es 255.255.255.0).

Una vez configurada la puerta de enlace y todo lo demás, si la red no tiene ningun tipo de seguridad en capas mas altas (Ipsec, SSH) que casi seguro si es una red domestica no tendrá, ya deberiamos de poder tener conexion a Internet.
Pero por supuesto deberemos volver a instalar los drivers originales de la tarjeta.

Si la red tiene un filtro para MACs (ACL), es decir solo acepta la lista de MACs configurada en el router, la cosa tambien se soluciona muy facilmente, por ejemplo el NetStumbler no dice la BSSID, es decir la MAC del AP (el router, normalmente), cambiando la MAC de nuestra tarjeta inalambrica, podremos entrar a la red sin problemas con el ACL.
Una vez dentro si conseguimos entrar al router podriamos añadir a la tabla de MACs una MAC un tanto rarilla (para que el administrador no sospechase). Y asi no tener que utilizar la misma que el AP.
El suguiente punto trata de como entrar al router.

Para cambiar la MAC, existe un programa muy basico y sencillo, que nos viene al pelo, etherchange:

http://www.ntsecurity.nu/downloads/etherchange.exe

Accediendo al router (AP) de nuestra red para configurarlo

Para acceder al router simplemente hay que poner como URL, la puerta de enlace, o si preferiís y se puede por telnet, pues haciendo telnet a la puerta de enlace.

Todos los routers vienen con nombre de usuario y contraseña por defecto de fábrica. Aunque si el administrador consiguio activar algunos de lo metodos de seguridad que antes hemos saltado, seguramente la haya cambiado.

Una lista de USERS y PASSWORDS de bastantes router.

http://www.phenoelit.de/dpl/dpl.html

Sacando la contraseña de un router:

http://foro.elhacker.net/index.php/topic,62224.0.html

Bueno aqui os comento un poco, pero visitad en enlace.

Bien hay varios metodos para sacarlo, darle a la cabeza.
Uno de los mas sencillos es con el envenenmiento ARP o ARP Spoofing.

Con el cain lo teneis muy fácil, e incluso teneis un manual de Gospel, que ojalá lo hubiese encontrado antes.

http://foro.elhacker.net/index.php/topic,45618.0.html

Miraros los titulos, decir que el servidor ftp podria servir, yu que la configuracion de un router se podria decir que es con un servidor web.

Bien una vez envenenado, simplemente hay que esperar, a que el admin se conecte y escriba su password.

No creo que haya algun router con https, pero tambien habla de ello.

Otra forma tambien es esnifar el trafico y aplicar un filtro solo para http. Con ethreal por ejemplo o Airopeek (la tarjeta en modo monitor, por favor)

Tambien podeis hacerlo a lo bestia, aunque no o lo recomiendo, mediante fuerza bruta. Con alguna herramienta como WebCrack o algo parecido, sinceramente no me gusta esta tactica, pero alla vosotros.

Y mas tacticas os lo dejo para vuestra imaginacion. Como por ejemplo buscar ina vulnerabilidad del router, etc...

Conviene aclarar que la contraseña del router no es la contraseña de red ni mucho menos. La contraseña de red como ya hemos dicho es la llave WEP, y la contraseña del router sirver para entrar a su configuración, donde podremos redireccionar puertos hacia nuestro PC, desactivar firewalls....

CONCLUSION

La redes 802.11 son como un arma de doble filo, por un lado esta la parte buena:

- Su ahorro en cableado
- Su movilidad
- Etcetera...

Pero por otro lado tambien son muy vulnerables (por ahora). Y por lo tanto se puede atentar facilmente contra nuestra privacida, a no ser que tengamos conocimientos elevados sobre redes.

Para acabar comentar, algunos puntos muy basicos que debemos tener en cuenta para proteger nuestra red:

- Activar el cifrado WEP, cuantos mayor longitud (mas bits) mejor, cambiarlo frecuentemente.
- Desactivar el broadcasting, emision de frames de autenticacion.
- Ocultar el ESSID y cambiar su nombre.(la longitud en este caso no importa)
- Activar ACL (filtrado de MACs)
- Desactivar el DHCP del router y cambiar su pass de acceso, asi como actualizar su firmware.