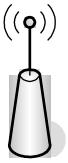
Rompiendo claves WEP.

Antes de iniciar el procedimiento para romper una clave WEP voy a explicar un poco el sistema de conexión a una red inalámbrica para que ampliemos un poco más el panorama de las técnicas de rompimiento de claves inalámbricas.

Acces Point(Punto de acceso): Como su nombre lo indica es un dispositivo que provee un punto para poder conectarse, en nuestro caso es un acceso inalámbrico. Lo abrebiaremos con las letras AP.

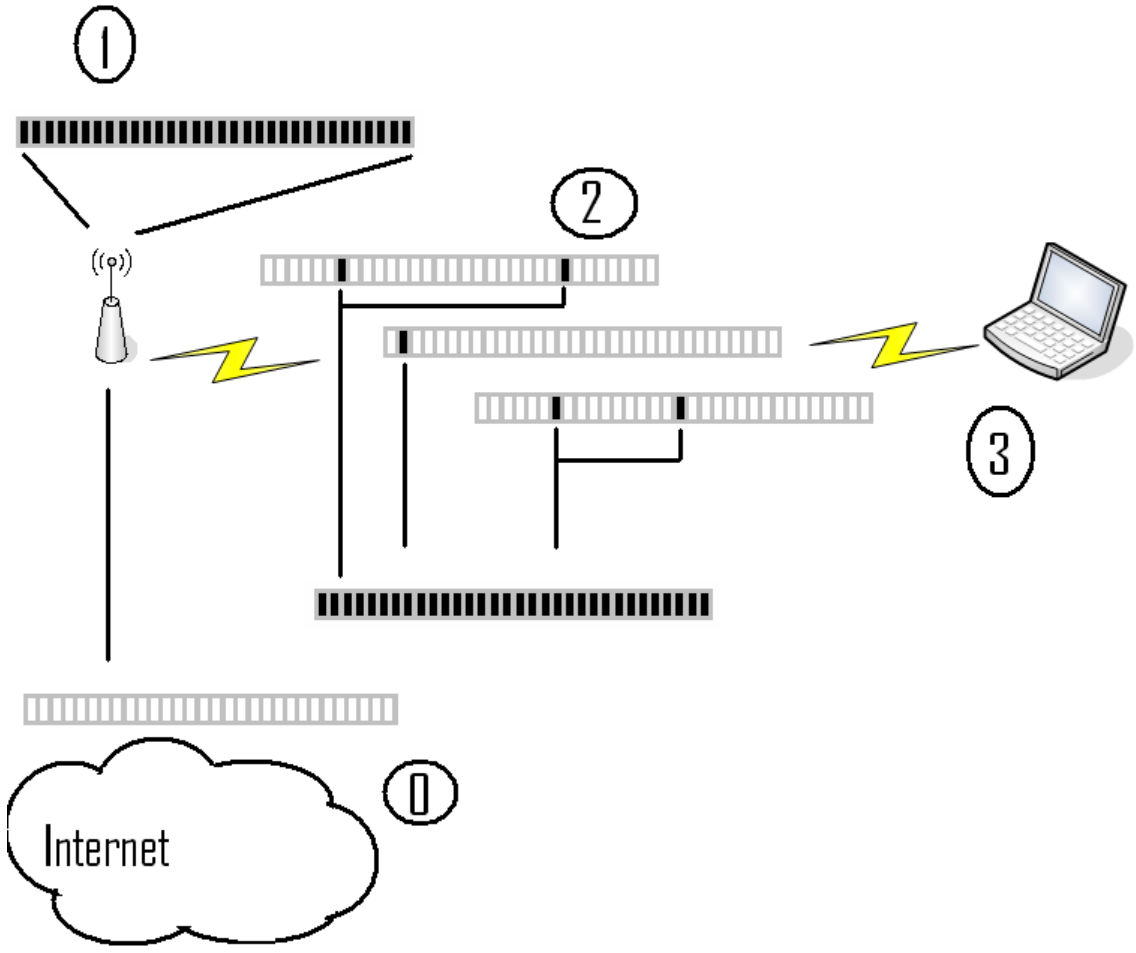
El AP emite una señal constante para indicar a los dispositivos al alcance que se encuentra funcionando y a la espera de una conexión. La condicion para establecer una conexión y que el AP responda a las peticiones del cliente son:



Que se encuentre al alcance necesario para tener una conexión de calidad sin perdida de paquetes.

En caso de que el AP este configurado para solicitar password, que el cliente proporcione el password correcto.

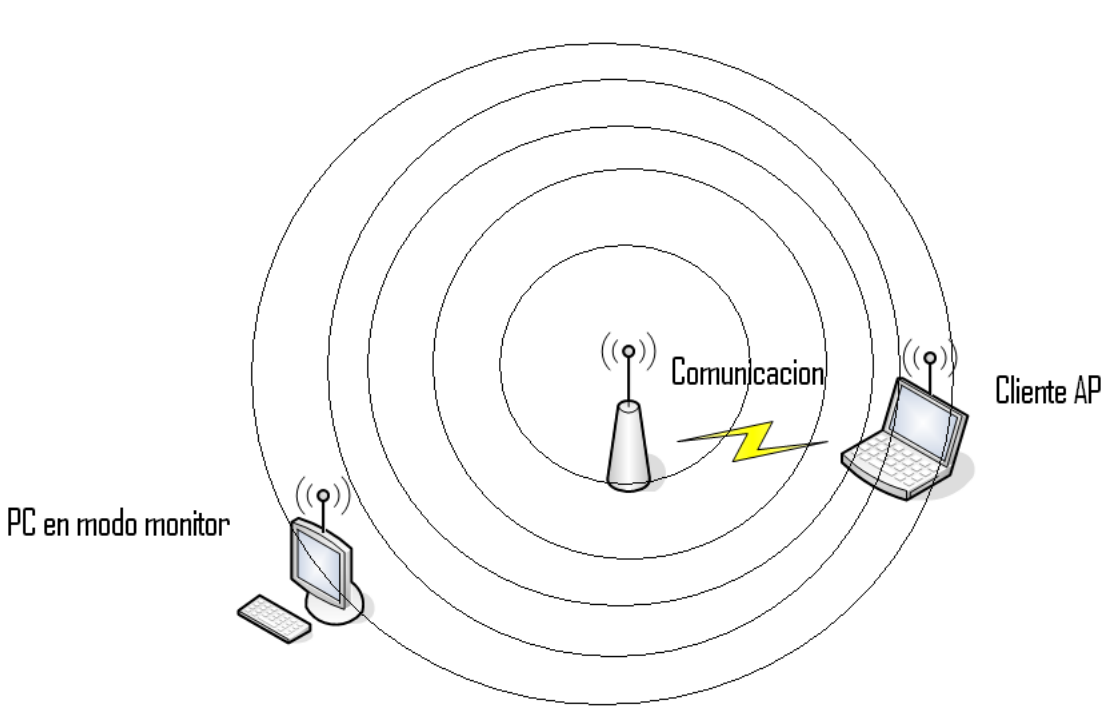
En el caso de las claves WEP, una parte de la clave viaja en cada paquete que envia el AP.
Por poner un ejemplo:Suponiendo que los cuadros gris con negro son la clave WEP que nos interesa conseguir. Y los cuadros blancos son los paquetes que envía el AP a una de las computadoras conectadas a el.



0) Los datos son solicitados por el AP a la Internet y la Internet responde enviando los datos necesarios(Cuadros en blanco), estos llegan al AP.
1) el AP verifica su registro de clave y convina la clave con el paqute procedente de Internet.
2) El AP envia los datos al dispositivo que solicito la consulta al AP.
3) El dispositivo recibe los datos junto con los bits pertenecientes a la clave WEP.

Podemos ver que es un esquema sensillo y no tan exacto, pero a grandes razgos ese es el funcionamiento, ahora lo que nos interesa a nosotros son esos pequeños cuadros negros para poder extraer la clave WEP del AP y poder conectarnos a el.

Generalmente el estado de una tarjeta inalambrica es de escucha y respuesta, pero en el caso de que nosotros enviemos una petición al AP y no recibamos respuesta o la respuesta esperada por nuestra computadora, simplemente esos paquetes seran ignorados por nuestra computadora, para que nosotros podamos obtener esos paquetes que son discriminados por no coincidir con la respuesta esperada por nuestra computadora, es necesario decirle a nuestra tarjeta que "escuche" todo, independientemente si es la respuesta que espera o no. A este estado de la tarjeta se le llama estado PROMISCUO o MONITOR.



Que pasa en este caso, un cliente validado le solicita información al AP, El AP no sabe ni tiene idea de donde se encuentra el cliente, y por el mismo funcionamiento de las frecuencias radiales, la respuesta es enviada en todas direcciones y como ya vimos, esa respuesta contiene parte de la clave que necesitamos. Nuestro PC ya se encuentra en modo monitor y almacenando en su disco los paquetes que captura. Para encontrar la clave se requieren un numero N de paquetes que tienen la clave. Una vez que tengamos los paquetes necesarios ya es posible extraer la clave de estos paquetes(No se el mecanismo exacto para la extracción de la clave).

Ahora bien, podemos ver a simple vista que una de las condiciones para capturar los paquetes, es que un cliente se encuentre conectado al AP y este enviando solicitando paquetes para que el AP

los envíe y poder nosotros capturarlos. Pues bien para no tener que esperar a que un cliente se conecte vamos a usar una técnica que mas adelante explicare.

Una vez explicado este proceso, vamos a pasar a la parte bonita de todo el asunto jejeje, digamos que es lo que estábamos esperando :p(A nadie le gusta tanto la teoría como la practica supongo).

Equipo necesario.

Computadora con tarjeta inalambrica

- Yo he utilizado una laptop HP v6000 con tarjeta broadcom y una tarjeta inalambrica Gíreles USB ENUWI-G2, en mi experiencia la tarjeta broadcom tiene poca compatibilidad para ponerse en modo monitor en el sistema operativo que recomendare, y ninguna con Windows XP. La tarjeta ENUWI-G2 me ha dado mucho mejor resultado que la tarjeta de la laptop, ademas el costo de la tarjeta ENUWI-G2 es muy bajo, posiblemente la tarjeta mas barata del mercado(180 pesos), talvez hay tarjetas con mas efectividad en cuanto alcance y eficiencia en la *inyeccion*

.

Sistema operativo Linux WIFIWAY o WIFISLAX

- Este lo descargan de Internet en forma de iso y lo queman en un CD, estas distribuciones de Linux ya traen todas las herramientas necesarias par efectuar todo el procedimiento. Pueden descargar el archivo torrent desde esta direccion:

  http://www.linux23.com/torrent/3115/wifiway-0.8-linux-for-wifi-wep-cracking-etc-www.softzone.org-1s-2l
  De todas formas si no llegaran a encontrarlo disponible ahí, pueden buscar en google como download WifiWay o Download WifiSlax.

Comencemos, una vez que tenemos el disco ya quemado lo introducimos en nuestro lector de CD y reiniciamos nuestra computadora, si tenemos configurado ya el inicio desde CD no tenemos que hacer nada mas que esperar, si no, hay que entrar al BIOS y configurar el arranque de la PC desde CD.

Dependiendo cual sea la distribución que descarguemos al inicio nos aparecera un menú, en el caso del WifiWay nos aparecen dos opciones, en el otro caso creo que entre 4 o 5 opciones, seleccionamos la opcion (1), iniciar WifiWay o WifiSlax.

En el caso de WifiWay comenzara a ejecutar una serie de pasos para cargar el S.O. y se detendra en una pantalla azul que prácticamente es irrelevante donde nos pregunta la zona horaria después de eso nos pregunta la configuración de nuetro teclado, para no estar después peleando buscando las teclas correctas, es necesario en ese paso configurar nuestro teclado de acuerdo al que tengamos, en mi caso y en la mayoria de los casos aquí, es Español(Mexico) o Español(Latinoamericano)
Una vez terminadas las pantallas azules apareceremos en un Prom. Con algunos textos, ahí debemos decirle al S.O. que queremos ingresar al modo grafico. Para lo cual teclearemos startx y enter.

Esto cargara el entorno grafico. Una vez en el entorno grafico podemos explorar todo lo que nos aparece en el S.O. Localizamos el lanzador de la consola, que es un icono generalmente de una pantalla de P.C. lo abrimos y nos posicionamos en el Prompt.

Nota: En Linux cuando se teclea alguna palabra o parte de una palabra y después la tecla TAB el sistema acompletara el faltante de las opciones disponibles.

En mi caso cuando inicio generalmente la tarjeta no esta dada de alta osea esta sin funcionar, para lo cual hay dos formas de levantarla y en general para la búsqueda de la clave se puede usar el mismo criterio.

La primera y mas facil es ejecutando un Script con el nombre de airoscript.es o airoscript.sh. utilizando el autocompletado podemos escribir:
>airos <TAB><TAB> y veremos que nos aparece una lista de posibilidades, podemos terminar de escribir la que necesitamos en este caso airoscript.sh o airoscript.es.

Al ejecutarse este script lo primero que nos pregunta es cual de la lista de tarjetas inalambricas queremos utilizar para el escaneo.

Después de esto nos aparece un menú con varias posibilidades, que van desde seleccionar victima, descifrar o atacar.

Lo primero que tenemos que hacer es escuchar las señales para seleccionar nuestra victima, si mal no recuerdo es la opcion 1

En esta parte del script les voy a poner un instructivo de Internet para no detenerme mucho en este metodo, ahí en Internet esta mejor explicado. Antes les comento que una vez seleccionada la tarjeta con este script, podemos salir de la ejecución del script para hacer los ataques de forma manual(Sin usar el Script).
http://videlanghelo.wordpress.com/2008/02/28/guia-rapida-para-crackear-wifis-con-wifislax/

http://es.wordpress.com/tag/airoscript/

Ahí hay dos ligas donde encontraran mas información.

En la liga 1 explican la cuestion de cómo levantar la tarjeta.

En mi caso la tarjeta cuando inicio aparece con el nombre de wlan0 o wlan1 o wifin en otros casos puede aparecer como wifi0 o wifi1 o wifin, depende de que dispositivo sea, por lo mismo para que no se rompan la cabeza les recomiendo usar el script, si el script no la reconoce entonces es mejor comprar otra tarjeta :p.

Bueno vamos ahora al otro metodo, que es hacer todo de forma manual:

Para seguir en este paso es necesario ya tener configurada nuestra tarjeta inalambrica, ahora lo que sigue sera comenzar a escuchar lo que hay en el aire, para ver que AP tenemos al alcance.

Abrimos una consola de comandos, ya habia mencionado que generalmente es un icono que aparece como una pantalla de P.C.

Nota: "***wifiway$>"*** no se tiene que teclear, es la representación del prompt. El nombre de "wlan" es suponiendo que ese sea el nombre de su dispositivo de tarjeta inalambrica.
Lo que aparezca entre <> sera teclas que hay q presionar.

Primero cambiamos nuestra MAC ADDRES
Wifiway$>ifconfig wlan0 down <enter>

Wifiway$>macchanger –m 11:22:33:44:55:66 wlan0 <enter>

Wifiway$>ifconfig wlan0 up <enter>

Después ejecutamos el comando airodump-ng para escuchar los AP.

Wifiway$>airodump-ng wlan <enter>

Nos aparecerar una pantalla con la lista de AP disponibles, la columna BSSID es la MAC Addres del AP, la segunda columan es la potencia con la que recibimos la señal, la 3ra no estoy seguro pero creo que es la calidad de la señal, después de ahí aparecen una columna que muestra los paquetes que se estan leiendo o que esta enviando el router, luego sigue una columna "data" que básicamente es la columna donde se muestran los paquetes utiles con la clave que se han capturado hasta el momento después aparece una columna con el canal en donde transmite el AP y después la columna con la velocidad de conexión del AP de 1Mb a 54Mb, una columna ESSID que es el nombre del AP. Y tambien hay una columna que nos dice que tipo de clave utiliza (WEP/WPA, etc)

Bueno hasta ahí nadamas hemos visto cuales son los AP al alcance, ahí debemos seleccionar el que mas nos guste para conseguir su clave. El criterio de selección sera primera por el tipo de clave(Recordemos que este tutorial es solo para claves WEP), el segundo criterio sera la intensidad con la que recibimos la señal.

Presionamos ctrl.+supr para que se detenga el escaneo.

Nota: Vamos a suponer que nuestra victima tiene un ESSID como 2WIRE1234 y su ESSID es DD:CC:BB:AA:99:88

Una vez seleccionada nuestra victima(Apuntar ESSID y/o CANAL).
Ahora usaremos el mismo comando anterior pero ahora le diremos que no solo monitoree los paquetes, si no que aparte los guarde en disco duro, para lo que nos posicionaremos en la carpeta donde se guardaran. Yo generalmente ingreso a una de los discos duros de mi PC, porque el sistema de archivos de la distribución que estamos usando, es en realidad virtual, por lo que haremos

Wifiway$>cd /mnt/ y presionamos la tecla <enter>
Wifiway$>ls y presionamos la tecla <enter>, en este paso apareceran una lista de los dispositivos de almacenamiento disponibles, en mi caso es un disco SATA por lo que aparece como una carpeta con el nombre sda1 o sda2 etc en otros casos puede aparecer como hdd1 o hdd2 etc, para saber si el dispositivo es uno de nuestros discos podemos entrar a el y ver que contiene, de la misma forma que el anterior ejemplo:

Wifiway$>cd /mnt/
Wifiway$>ls

/sda1 /sda2 /floppy /usb /cdrom

Wifiway$>cd sda1 <enter>
Wifiway$>ls <enter>
/Windows /Archivos de Programa /cualquier cosa

Se supondría que ese es mi disco C: de Windows, por lo cual sera aquí donde decido guardar el archivo con los paquetes capturados.

Una vez posicionados en la carpeta donde guardaremos los paquetes escribiremos el comando para comenzar a escuchar y guardar los paquetes.

Wifiway$>airodumpt-ng --channel 1 --ivs -w miArchivo wlan0

En esa instrucción le digo que escanee solo el canal 1, que capture solo paquetes ivs(Son los que contienen la clave), que escriba lo que captura en miArchivo y que lo haga con el dispositivo o tarjeta inalambrica wlan0.

Ahora nos aparecera una pantalla identica a la primera pero si nos damos cuenta solo apareceran los AP que transmiten por el canal 1.

Si se encuentra algun cliente conectado al AP veremos como comienza a subir la columna “data” entre mas clientes conectados el trafico es mayor y el numero crecera mas rapido. Pero que pasa si no hay clientes o si queremos acelerar el proceso de envio de paquetes utiles por parte del AP, pues en este punto lo que haremos sera engañar al AP y generar trafico ficticio lo que se llama en el proceso INYECCION.

Pare inyectar tendremos que abrir una consola diferente o utilizar la misma pero abrir otra pestaña, por ahí arriba de la consola se encuentra el icono si no lo encuentran da lo mismo abrir otra consola de comandos.

Pare este paso utilizaremos el comando aireplay-ng:
Si escribimos aireplay-ng --help podemos ver que nos aparecen las opciones del comando.

Para comenzar el proyecto de inyeccion primero tenemos que hacer una asociacion falsa con el AP decirle que nosotros somos un cliente y que nos envie paquetes.

Esto lo hacemos de la siguiente forma:

Wifiway$>aireplay-ng -1 0 –e 2WIRE1234 –a DD:CC:BB:AA:99:88 –h 00:11:22:33:44:55 wlan0 <enter>
nota: el cambio de linea es por el espacio de escritura :p pero todo es continuo, es probable que por el tamaño de la pantalla a ustedes no les pase o les pase con menos caracteres, asi es q no se fijen mucho en eso, de hecho si cambian el tamaño de la pantalla del prompt les va a dar algunos problemas, por la distribución Linux, a mi me pasa asi es que la dejo del tamaño que se abre.

En el comando anterior lo que hicimos fue decirle que se asociara al AP, la opcion -1 es la opcion *asociación* el 0 significa que lo haga indeterminado numero de veces, si ponemos un numero mayor a 0 intentara asociarse el numero que pongan, el –e le estamos diciendo que lo haga con el AP 2WIRE1234 y la opcion –a es la MAC addres del AP, el –h le estamos diciendo

que lo haga con la MAC addres de nuestra tarjeta y el wlan0 es el nombre de nuestra tarjeta inalambrica.

Nos aparecera información sobre el estado de la asociación, al lograrlo nos aparecera el siguiente texto:
Asociation sucssesfull :).

Si no lo hace a la primera aparecera información del porque podria ser, 1 es porque estamos lejos del AP y ahí tendriamos que cambiar la velocidad de la solicitud, por default es 54M, hay que cambiarlo a 1M ahí al finalizar la ejecución del comando nos dice como lo podemos hacer, es con
Wifiway$>iwconfig (no recuerdo bien el resto del comando pero busquenlo ahí donde les digo) <enter>
Una vez cambiado el rate de conexión repetir el paso del aireplay-ng.

Una vez asociados Asociation sucssesfull :) Lo siguiente es comenzar a inyectar paquetes, eso lo hacemos de la siguiente forma.

Wifiway$>aireplay-ng -3 –b DD:CC:BB:AA:99:88 –h 11:22:33:44:55:66 wlan0 <enter>

Esta linea lo que hace es decirle que inyecte paquetes (opcion -3) al BSSID de nuestra victima, que es (-b DD:CC:BB:AA:99:88) y que lo haga usando la mac addres 11:22:33:44:55:66 de la tarjeta inalambrica wlan0

Después de esto si fue exitoso comenzaremos a ver como los paqutes de la columna “data” comienzan a subir. Si esto pasa es que fueron exitosos nuestros procedimientos, ahora solo hay que esperar a tener unos 180,000 o mas paquetes para decodificar la clave cuando es una encriptación de 64 bits(la mayoria de la gente tiene esa encriptación, y Telmex entrega los routers con esa configuración asi es que no hay nada de que preocuparse). En caso de claves de 128 o mas, la cantidad de paquetes necesarios es mucho mayor.

Una vez que nuestro contador data llega a 180 mil o mas paquetes podemos ahora ejecutar el comando que desencriptara la clave

Para lo cual podemos abrir otra consola.

Wifiway$>aircrack-ng miArchivo_01.ivs <enter>
Ahí podemos usar la opcion –n 64(Wifiway$>aircrack-ng –n 64 miArchivo.ivs <enter>) para decirle que la clave que buscamos es de 64 bits, si no estamos seguros o dudamos que la clave es de 64 bits, sera mejor no poner nada.

miArchivo puede aparcer con un post fijo que es un numero. Acuerdence del <TAB> o del comando “ls” para localizar el que buscamos.
NOTAS FINALES: En caso de que por algun motivo cerremos la ventana donde estamos ejecutando el comando airodump-ng no se preocupen podemos volver a ejecutar
Wifiway$>airodumpt-ng --channel 1 --ivs -w miArchivo wlan0
Y se generara otro archivo miArchivo con un postfijo superior al primero, y la captura de esos paquetes podran utilizarse con la captura de los primeros paquetes, esto podemos hacerlo N veces.

Ejemplo, estoy capturando paquetes después de inyectar y ya tengo 100 mil, de pronto se va la luz y ups maldita sea ya hiba a la mitad :p tendre que comenzar de nuevo…. Noooo!!!!
No es necesario comenzar de nuevo simplemente comenzar el tutorial desde:

Wifiway$>airodumpt-ng --channel 1 --ivs -w miArchivo wlan0

Hasta comenzar a inyectar y capturar 80 mil paquetes mas, al tener los 80 mil paquetes ejecutamos el comando aircrack-ng pero ahora de la siguiente manera.

Wifiway$>aircrack-ng miArchivo_01.ivs miArchivo_02.ivs … miArchivo_nn.ivs <enter>

miArchivo_n.ivs donde n seria el archivo generado en la ejecución n de airodump-ng.

Otra cosa importante, yo les recomendaria comenzar usando el SCRIPT airoscript.es o airoscript.sh para que lo hagan de forma automatica y ven mas o menos los procesos, yo prefiero la forma manual, para mi ha sido mas efectiva, pero de la otra forma tambien es posible.

Se me olvidaba comentarles, que si tienen 1 tarjeta con esa tarjeta pueden hacer el proceso de lectura e inyeccion de paquetes, pero si tienen 2 con una pueden hacer el proceso de lectura e inyeccion y con la otra solamente inyectar, eso hara que la captura de paquetes sea mucho mas rapida, si tienen mas de dos, con una tarjeta leen e inyectan paquetes y con el resto inyectan, hay que tomar en cuenta que la velocidad de captura e inyeccion de paquetes depende de la distancia y calidad de la señal. Yo con esta tarjeta ENUWI-G2(Tiene que ser G2 la G1 no me sirvio :p) inyecto y leo a 300 paquetes por segundo con una calidad de señal de 75% ignoro donde se encuentre el AP, pero debe haber tarjetas con mayor velocidad y alcance.

Bueno hay muchos truquitos mas, que ahorita no recuerdo de todas formas ya tienen mi mail, si necesitan saber mas o salen dudas no duden en consultarme, les dejo la direccion de un video donde muestran el proceso a partir de que comenzamos a escanear en busca de AP.
http://es.youtube.com/watch?v=747YGnXwNuc

ESPERO QUE ESTE PEQUEÑO TUTORIAL LES SIRVA DE ALGO. NO SE OLVIDEN DE BUSCAR MAS INFORMACION AHÍ EN INTERNET, PALABRAS CLAVE PARA GOOGLE: claves wep, wifiway, wifislax, romper claves wep, claves wep 2wire, etc.

Tambien pueden bajarse la suit para Windows, pero hay pocas tarjetas que soportan el modo monitor en Windows, pero pueden probar primero con ese sistema operativo o buscar su tarjeta en la lista de tarjetas compatibles para Windows, en ese caso hay q descargarse aparte unos drivers especiales llamados wilddrivers o algo asi(prefiero LINUX).

PD: Disculpen el monton de faltas de ortografia :p(Ya se que para eso no hay disculpas, pero de todas formas jajajaja). AAAA tambien les recuerdo que estas tecnicas y programas no los hago yo, son programas que se encuentran en la red y que me he dedicado a leer un poco, el merito es de muchos otros.

“La información es un derecho universal que no debe depender del poder económico de unos cuantos.”

Atentamente: Patriota (http://www.radiovulgocracia.org.mx/)