

- [Home](#)
- [Contacto](#)
- [Servicios](#)
- [Aviso Legal](#)
- [Tienda Online](#)
- [Contenido](#)
- [Enlaces](#)
- [Clásico](#)
- [Videos Youtube](#)
- [Destacados](#)
- [App android](#)
- [Foro](#)
- [RSS](#)
- [Help](#)



Seguridad Wireless

Manual seguridad alta con configuración WPA-PSK

[1.- Introducción](#)

[2.- Requisitos](#)

[3.- Configuración punto de acceso/router y tarjeta wireless \(WPA-PSK\)](#)

[4.- Configuración de tarjeta para WPA-PSK](#)

[5.- Captura general y particular](#)

[6.- Desautenticación de clientes legítimos](#)

[7.- Recuperación de la clave secreta](#)

[1.- Introducción](#)

- Una vez analizadas las inseguras que son las redes inalámbricas con cifrado WEP y facilidad con que se pueden recuperar claves WEP mediante técnicas de reinyección de tráfico, desautenticación, autenticación falsa y captura de datos, se nos plantea el reto de comprobar la seguridad de las redes WPA. No voy a explicar todo el rollo de este tipo de seguridad, además que no me lo se, sino la pauta a seguir para demostrar que siguen siendo inseguras (aunque ya no tanto según se configuren), pero según su configuración realmente

podemos estar bastantes tranquilos. Hay varias formas de seguridad vía WPA (al menos eso creo yo), pero vamos fundamentalmente las mas habituales usadas por la mayoría de nuestras redes domesticas del tipo WPA-PSK si entrar en servidores RADIUS. La configuración mediante encriptación WEP no depende de una buena configuración, simplemente son inseguras. Las WPA-PSK pueden ser muy seguras, pero siempre que estén bien configuradas.

Solo citar que este tipo de protección difiere de las WEP en que la clave es dinámica, o sea que cambia cada cierto tiempo y es especifica para cada terminal (si estoy equivocado es igual ya que lo que vamos a realizar es un ejemplo de aplicación practica, de como lo haría un posible atacante no autorizado).

Pero antes de llegar a la demostración tenemos que explicar algunos conceptos teóricos muy básicos.

Los routers y las tarjetas inalámbricas deben de tener una clave secreta para una autenticación inicial, para que lo entendáis, como en el Microsoft Windows 2000 Server donde es necesario indicar un nombre de usuario y una clave para tener acceso a los recursos, pues esto diremos en groso modo que es igual. O por ejemplo cualquier foro donde se nos pide un nombre de usuario y una contraseña.

Por lo tanto vamos a ir a la caza de esta clave secreta y así simulamos un virtual ataque, de esta forma en función de los resultados podemos prevenir y configurar nuestro sistema para lograr un alto grado de seguridad wireless.

No es necesario sniffar mucho trafico, no es cantidad sino calidad. Y solo se puede coger en el momento que un cliente se autentifica con su punto de acceso. Por eso, aunque la cantidad de trafico no es importante su nivel de seguridad es mucho mayor debido a que los posibles atacantes deben tener paciencia para encontrar el trafico correcto. Este trafico correcto donde se realizan las presentaciones entre estaciones cliente y los punto de acceso se le denomina como "[handshake](#)".

Puede hacerse tanto en windows como en linux. Con la premisa que el numero de tarjetas que permiten el ataque 0 (desautenticación de clientes) es mucho mayor en linux. Cuando se efectúan ataques 0, dichos clientes que llamare legítimos se vuelvan a autenticar sobre todo si es windows quien controla la conexión inalámbrica y no las aplicaciones propias de las tarjetas inalámbricas. En este ultimo caso, esta reasociación automática es mas difícil de detectar y analizar. Pero que conste que con paciencia y sin efectuar ningún tipo de ataque se puede conseguir, simplemente con observar y capturar el trafico y que este se produzca en el momento de la conexión entre cliente y punto de acceso.

Parece sencillo verdad (ya no hacen falta millares de datos capturados), pues no, realmente no es tan sencillo y se puede afirmar que el nivel de seguridad es mayor.

Se debe esta afirmación a la siguiente cuestión: Una vez obtenido el trafico correcto (con un solo "handshake" nos vale) hay que compararlo con las palabras de un diccionario (o sea por método de la fuerza bruta). Dichos diccionarios son meros ficheros secuenciales donde en cada línea hay diferentes caracteres escritos. Y es en estos momentos el punto vital para determinar si una red inalámbrica puede ser o no ser segura, y solo dependerá de nosotros mismos, al contrario que las WEP donde nunca dependerá de nosotros ya que por definición son inseguras totalmente.

Imaginar que vais aun cajero a sacar dinero y no sabéis la contraseña pues bien tenemos 1 entre 10000 posibilidades. Es poco y si lo cajeros nos dejaran mas de 3 intentos sin bloquear la cuenta se haría fácilmente probando varios días.

Con WPA-PSK y la suite del Aircrack no tenemos limitación de intentos ya que lo hacemos fuera del acceso directo (vamos como si tu tuvieras en tu casa una pequeña caja de seguridad con 4 dígitos y probaras todas las combinaciones posibles).

Pero, la clave secreta de este tipo de seguridad no tiene que porque ser de 4 números decimales (como son las claves de los cajeros) sino que puede variar entre 8 y 63 caracteres ASCII si se ejecuta el asistente para redes

inalámbricas del Windows XP Profesional SP2. Cada carácter ASCII a su vez puede tener diferentes posibilidades, pues un simple calculo de posibilidades nos dice que el numero total de combinaciones corresponde al numero de caracteres ASCII elevado entre 8 y 63 en funciona de la longitud de la clave. Es cierto que no todos los caracteres ASCII podrán ser utilizados como dentro de las claves, pero el numero final sigue siendo muy elevado.

Por ejemplo, contar solo con números y letras, en total unos 37 mas o menos. Si la clave es de 8 caracteres, las combinaciones posibles serian 3.51247×10^{12} y si fuera de 6.3E+98, y eso sin diferenciar entra mayúsculas y minúsculas. Pues no hay diccionario en el mundo que lleve todas esas combinaciones. Pero si usamos nombres propios tales como "Feliciano", "Isabelle" o de animales tales como "rinoceronte" o genéricas como "Internet" estas si suelen estar en los diccionarios. Pero por ejemplo "ql9sj3rs7f" si seria una clave buena, solo que tendemos a no usarlas de este tipo, mal hecho, algo similar a las claves de nuestros correos electrónicos y accesos a paginas registradas donde siempre usamos las mismas, y sin encima son medianamente difíciles de recordad, además las apuntamos y las pegamos en la pantalla del monitor.

[Parece que podemos empezar a respirar tranquilo de que nadie que no este autorizado pueda acceder a nuestra red inalámbrica y absorber nuestro ancho de banda de conexión a internet.](#)

Por lo tanto nunca elaboréis una clave mediante el sistema personal que el ser humano tiene para recordar las cosas, yo personalmente uso claves que casi siempre olvido y posteriormente tengo que resetar el punto de acceso para poder cambiarla.

Dicho esto, solo cabe añadir que esta demostración esta ideada para que podamos probarlo con nuestros propios equipos y comprobar el nivel de seguridad de vuestras instalaciones inalámbricas. Siempre lo diré que hay que ponerse en el lugar de las personas que tienen conocimientos para acceder a nuestras redes inalámbricas, hay que estar mas preparados que ellos, y una simulación de ataque real con nuestros propios equipos nos permitirá obtener resultados dignos de valorar.



2.- Requisitos

- Como dije anteriormente las pruebas las realizaremos con nuestros propios equipos, entonces necesitaremos de lo siguiente:

1.- Un router inalámbrico que incorpore seguridad tipo WPA-PSK, los Zyxel que vienen en el kit ADSL de telefónica pueden valer. Si no tenemos un router vale lo mismo para un punto de acceso, pero yo lo explicare para este router. Tampoco es necesario exclusivamente un router, sino mas concretamente un [punto de acceso](#), pero dichos routers ya lo llevan incorporado.

2.- Un pc (sea el que sea) pero con 2 tarjetas wireless, una para el trabajo normal y otra para la captura de datos, por lo tanto la tarjeta con la conexión normal debe de permitir la seguridad WPA-PSK y la tarjeta para captura debe de permitir el modo monitor y ataque 0 para linux y/o windows. Si solo se permite el modo monitor también vale pero estaremos mas limitado. Yo en linux lo explicare con el ataque 0. Si queréis ver como se efectúa un ataque 0 (de desautenticación) en windows solo tenéis que acceder al [Manual de inyección de trafico en windows](#).

3.- Sistema operativo: Yo lo voy a explicar para Linux, pero vale para windows.

Nota: No voy a explicar como se configura la tarjeta para seguridad WPA-PSK para Windows ya que es muy fácil y después de leer como funciona un poco esto creo que lo sabréis hacer, además si explicare como se configura el router, una vez visto lo del router entenderéis como hacerlo con vuestra tarjeta para Windows.

Si explicare como configurar para Linux vuestra tarjeta para que trabaje con seguridad WPA-PSK, pero lo haré para la Conceptronic C54RI que usaba en mis inicios, lo importante aquí no es la configuración sino como se ataca ese sistema.

Para configurar la tarjeta de captura creo que todos ya sabemos como hacerlo en Windows y en Linux.

3.- Configuración punto de acceso/router y tarjeta wireless (WPA-PSK)

Entramos en la configuración de nuestro router vía http o con la aplicación de configuración propia de el. Lo bueno es que por http puede hacerse tanto en Linux y en Windows y es la mejor manera para mi (vosotros hacerlo como mejor sepáis o queráis).

Debemos de encontrar una sección en el router parecida a esta:

Wireless LAN - 802.1x/WPA

802.1x Authentication

Wireless Port Control: Authentication Required (v)

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Key Management Protocol

WPA-PSK (v)

Pre-Shared Key: josemaria

☐ WPA Mixed Mode

Group Data Privacy: TKIP (v)

WPA Group Key Update Timer: 1800 (In Seconds)

Back Apply Cancel

Debe de estar en la sección de Wireless Lan y en el apartado de 802.1x/WPA.

En **Wireless Port Control** seleccionamos **Authentication Required**.

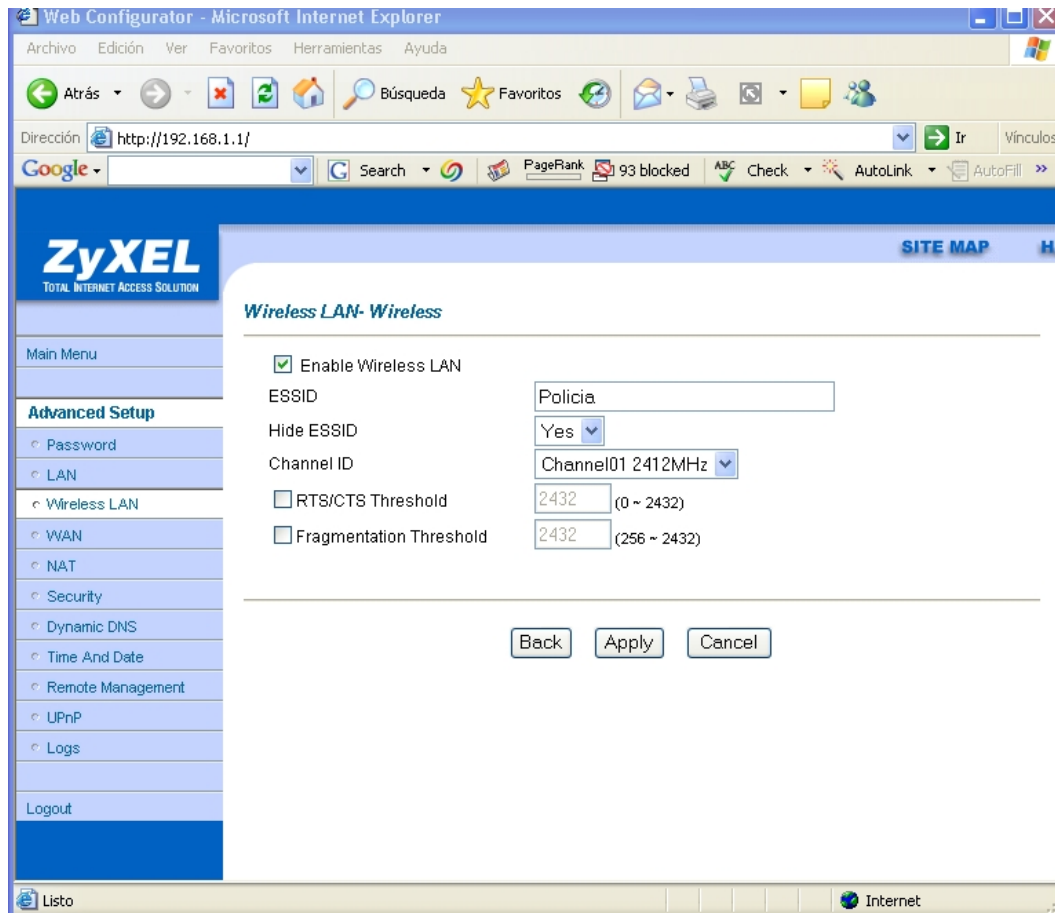
De los timer paso de ellos, pero si están a cero poner algún valor, los que están aquí reflejados pueden valer.

En **Key Management Protocol** seleccionamos **WPA-PSK**.

En **Group Data Privacy** seleccionamos **TKIP**.

Y en **Pre-Shared Key** ponemos la **clave secreta** que es lo que queremos descubrir, en mi caso puse "josemaria" (sin las comillas) que pudiera ser perfectamente mi nombre.

Ahora dentro de **Wireless LAN** nos vamos hasta el **apartado Wireless**.



Habilitamos "**Enable Wireless LAN**".

Ponemos el nombre de red (**essid**), en este caso "**Policia**".

En este captura el **essid** esta configurado para permanecer oculto. Pero para estas pruebas lo habilitaremos. En el caso que estuviera oculto seria los mismo ya que ya sabemos como obtenerlo y además no importa para este tipo de ataques.

Pongo el canal 1, aunque es igual el que sea. Y de **RTS** y **fragmentación** ni los comento, total no se ni para que se usan.

Bueno pinchamos sobre el boto "**Aply**" y ya tenemos listo el router para que trabaje de forma inalámbrica y con seguridad WPA-PSK.

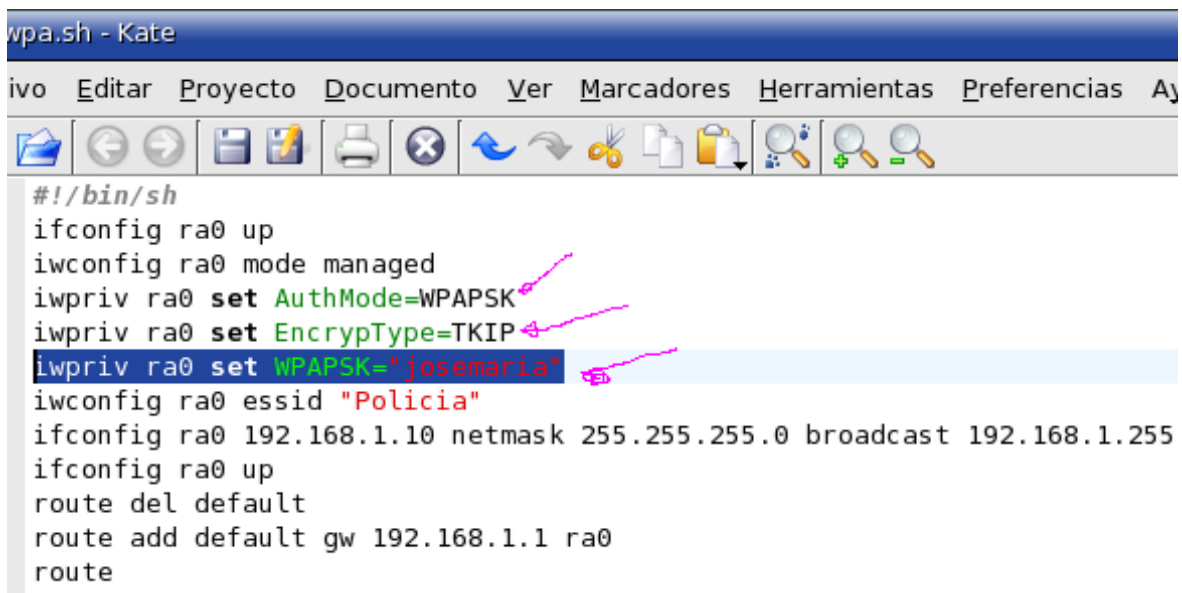
4.- Configuración de la tarjeta para WPA-PSK

Explico como hacerlo en Linux para una Conceptronic C54RI con el chipset de Ralink RT2500

Supongo que será válido para cualquier tarjeta con el chipset de Ralink RT2500, como por ejemplo la Conceptronic C54RC.

Preparo una script para configurar esta tarjeta (el nombre de la script le ponéis el que queráis)

Hay va la captura de pantalla:



```
#!/bin/sh
ifconfig ra0 up
iwconfig ra0 mode managed
iwpriv ra0 set AuthMode=WPA-PSK
iwpriv ra0 set EncrypType=TKIP
iwpriv ra0 set WPAPSK="josemaria"
iwconfig ra0 essid "Policia"
ifconfig ra0 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
ifconfig ra0 up
route del default
route add default gw 192.168.1.1 ra0
route
```

Tal cual, creo que no es necesario comentar nada. Solo decir que para otras tarjetas abra formas alternativa y/o diferentes de realizarlo. Por ejemplo la suite del wpa_supplicant (o alguna forma especifica). Este donde este la ejecutamos, en este caso: `./wpa.sh`

No hace falta ni siquiera que comprobéis el acceso a Internet, con lo que tenemos en estos momentos ya es suficiente para seguir trabajando.

5.- Captura general y particular

Bien vamos a lo que realmente importa. Llegados a este punto, todos ya sabemos como funciona el modo monitor.

El estudio de la inseguridad lo haré con mi D-LINK G520 chipset súper G Rev. B3 de atheros ([Interface ath0](#)).

Activo la tarjeta mediante el comando apropiado y ejecuto "`airmon-ng start ath0`", recordar que la interfaz poder ser de otro tipo.

Por ejemplo para los drivers basados en mac80211, despues de ejecutar el comando `airmon-ng` la interface de trabajo seria `mon0`.

Vemos que todo va bien. Para Windows ya sabéis, ejecutáis el programa airodump-ng y la tarjeta con sus drivers específicos para modo monitor.

Ahora pasamos a la captura general de todas los canales, en Windows lo mismo, con el airodump-ng.

Comando: `airodump-ng ath0 file 0`

Las demás señales que vemos, en el caso que nos ocupa no importan y por ética profesional y personal las oculto, lo importante es que vemos la señal wireless creada por nosotros con el router y la tarjeta C54RI. Vemos la MAC del router, la MAC del cliente, el essid y el canal.

Ahora tomamos nota de todo los datos y los introducimos en la aplicación en el CCW1, o simplemente los apuntamos.

Tanto para Windows y Linux cerramos la captura.

Para Windows abrimos de nuevo el airodump-ng y le colocamos que capture solo en el **canal 1**. A la respuesta **y/n** del airodump-ng en Windows, respondemos no, para de esta forma solo tener un fichero del tipo: *.cap. Es decir los ficheros *.ivs donde solo se incluyen vectores IV no validos para este tipo de seguridad. Los IVs solo serán validos para la recuperación de claves para redes inalámbricas con encriptación WEP.

Ejecutamos: "airmon-ng start ath0 1 "

Ahora abrimos de nuevo el airodump-ng.

airodump-ng ath0 policiawpa 1

Ya lo tenemos preparado para la captura de datos.

Vemos de nuevo el router y el cliente, o sea la C54RI.

No pasa nada, realizamos el **ataque 0** sea en linux o en windows con la aplicación que usemos.

6.- Desautenticación de clientes legítimos.

Realizamos el ataque 0:

aireplay-ng -0 5 ath0 -a MAC_AP -c MAC_CLIENTE

Pero ojo, para que sea efectivo probar con diferentes velocidades.

Citar: **iwconfig ath0 rate 54M** hasta **iwconfig ath0 rate 24M**

Como yo uso este programa lo preparo todo desde el y me ahorro escribir bastante código, ya que el programa lo hace por mi.

Queda bastante claro, primero iniciamos el proceso de captura y mientras se esta en ello, realizamos el ataque 0. Hay modelos de tarjetas y de drivers que permiten hacerlo con la misma tarjeta, es decir en este caso la atheros (capturar y inyectar).

Y que obtenemos después del ataque 0: Vemos que el trafico a aumentado. En el caso que siempre hubiera trafico dejar la captura unos minutos para que se produzca de forma correcta el intercambio de claves entre cliente y punto de acceso. En este mismo momento también se produce el intercambio del nombre de la red (essid) y aunque estuviera ocultado podría determinarse muy fácilmente.

7.- Recuperación de la clave secreta

Abro una shell (de la forma que sea) y ejecuto:

aircrack-ng -a 2 -w /ruta_diccionario/diccionario policiawpa.cap

El fichero esta en *.cap por que no le pasamos el argumento 1 al airodump-ng, y es así como lo queremos.

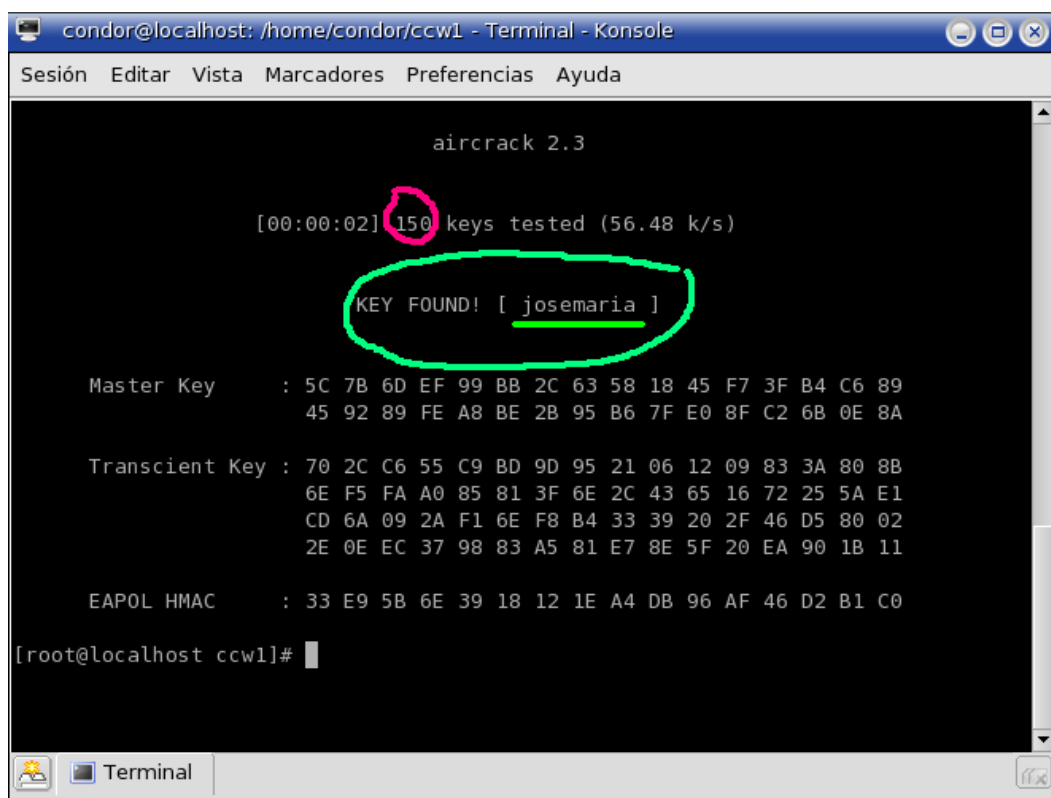
La ruta (**ruta_diccionario**) es cualquier carpeta y se debe de poner de forma completa. El diccionario es un mero fichero básico de texto secuencial (sin añadidos como por ejemplo pudieran ser los ficheros de Word). En cada línea de este fichero nos encontraremos con diferentes caracteres (**en definitiva claves de comprobación**).

Tanto manual de seguridad alta con cifrado WPA-PSK y solo hemos obtenido un handshake, pues bien tranquilos con eso es suficiente.

Existen multitud de zonas en Internet donde se pueden conseguir de forma gratuita los diccionarios aquí comentados, pero que en ningún momento informare de donde bajarlos, al ser posiblemente pagina de forma muy temporal.

Si el diccionario es bueno y la clave no es muy difícil puede tardar mucho o infinito, cuando acabe de leer todas la claves y esta no corresponda a la real, en dicha aplicación nos saldrá la palabra EOF (final de fichero), pues bien no desesperéis y os tocara usar otro diccionario. Y si nunca dais con ella, pues **enhorabuena**, ya tienes configurada tu red inalámbrica de forma segura, pero el 100% nunca lo tendrás, esto nunca lo olvides.....

Si tenéis vuestra red wireless configurada con un bajo de nivel de seguridad (siempre hablamos de WPA-PSK) os saldrá:



```
condor@localhost: /home/condor/ccw1 - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

aircrack 2.3

[00:00:02] 150 keys tested (56.48 k/s)

KEY FOUND! [ josemaria ]

Master Key      : 5C 7B 6D EF 99 BB 2C 63 58 18 45 F7 3F B4 C6 89
                  45 92 89 FE A8 BE 2B 95 B6 7F E0 8F C2 6B 0E 8A

Transcient Key  : 70 2C C6 55 C9 BD 9D 95 21 06 12 09 83 3A 80 8B
                  6E F5 FA A0 85 81 3F 6E 2C 43 65 16 72 25 5A E1
                  CD 6A 09 2A F1 6E F8 B4 33 39 20 2F 46 D5 80 02
                  2E 0E EC 37 98 83 A5 81 E7 8E 5F 20 EA 90 1B 11

EAPOL HMAC      : 33 E9 5B 6E 39 18 12 1E A4 DB 96 AF 46 D2 B1 C0

[root@localhost ccw1]#
```

Consejo: Si después de varios días no la encontráis y en lugar de estar contentos os ponéis de los nervios y quizás dudéis si realmente estas herramientas de auditoria wireless funcionan bien, hacerme caso, abrir el diccionario con un editor normal de texto (el que queráis) y en cualquier línea del mismo añadir una fila con el nombre secreto. Veréis como si la encuentra, comprobando que el estudio es valido, tanto para resultados negativos como positivos para la recuperación de claves WPA-PSK.

Ya se que esto ultimo parece poco serio para comprobar un nivel de seguridad, pero que sepáis que lo importante en este tipo de configuración es capturar el trafico correcto, y determinar el uso de claves fueras de la lógica normal no contempladas en ningún diccionario, solo así se consigue un alto rendimiento de la configuración de seguridad en sistemas inalámbricos o wireless.

En el caso de un atacante real sobre nuestra red wireless, no podrá añadir ninguna clave al diccionario ya que obviamente no la sabrá. Así tendremos seguro lo que es mas importante; sabremos como configurar nuestros equipos wireless para darle una mayor seguridad a todo el sistema (vamos si no eres capaz de recuperar una clave WPA-PSK, no tengas dudas de que realmente es segura, ya que la mejor defensa es un buen ataque y siempre hay que analizar tu sistema desde el punto de vista del atacante y corregirlo en ese sentido, hay que

estar lo mas preparado posible).

También citar que hemos hablado de la versión 2.3 de la suite del programa que ceo C. Devine pero existen versiones mas actualizadas.

Yo creo que podemos estar tranquilos con este tipo de protección de que nadie nos quitara ancho de banda, pero solo..... si usamos una contraseña realmente difícil de encontrar en un diccionario.



©Hwagm - www.seguridadwireless.net