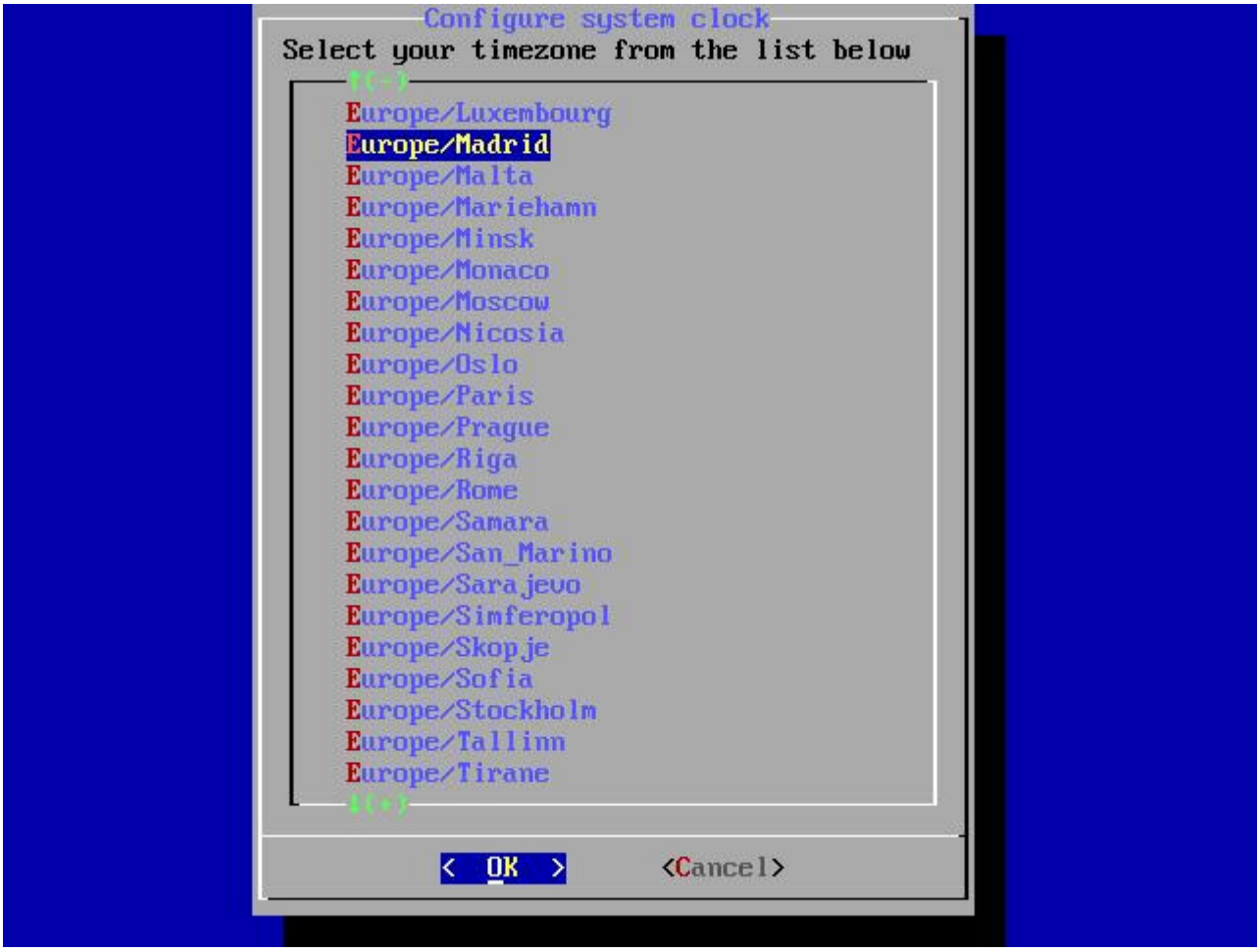
Seguridad Wireless: Wifiway 0.8 y Wifislax 3.1

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.

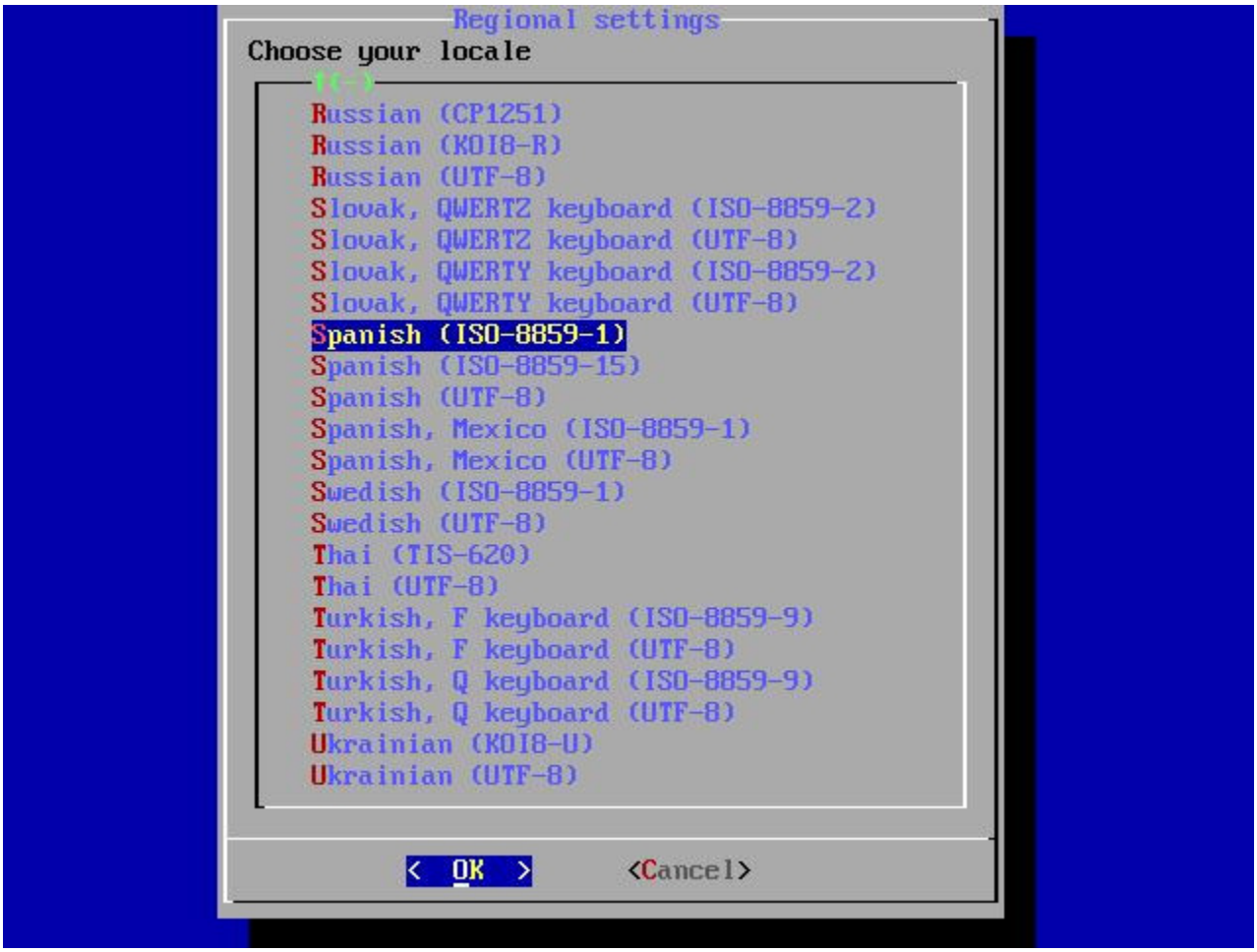
Primero, mirar si nuestro adaptador inalámbrico puede inyectar, en este listado podremos comprobar si nuestra tarjeta de red wifi puede hackear redes wifi o no- **AKI**.
Segundo, descargarnos la versión que más nos interese, Wifiway 0.8 o Wifislax 3.1.
Después, la grabamos a un CD o un pendrive y arrancamos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

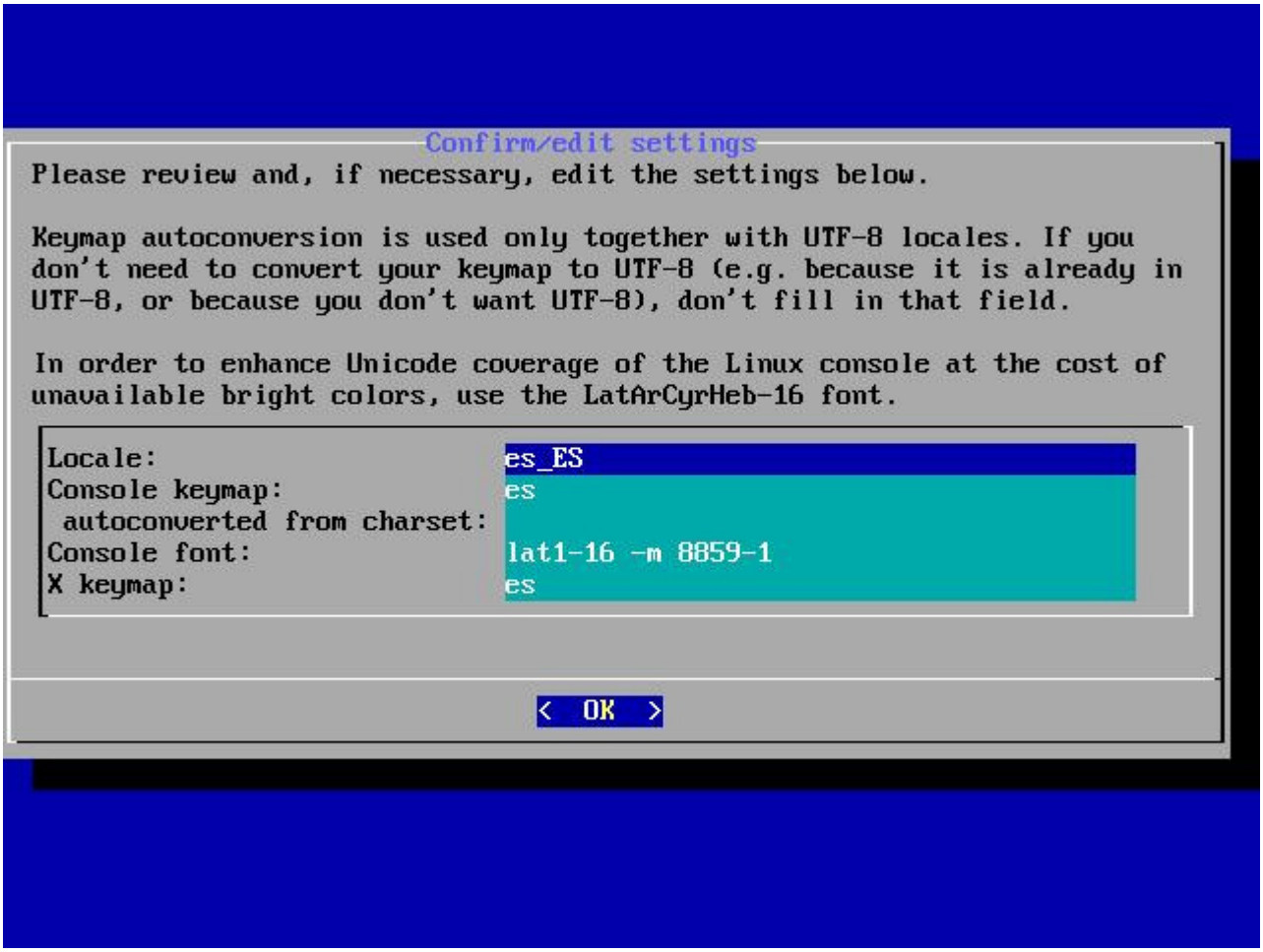


Durante el arranque, debemos indicarle una serie de datos, cómo la zona horaria, en mi caso selecciono "Europe/Madrid" & "OK",

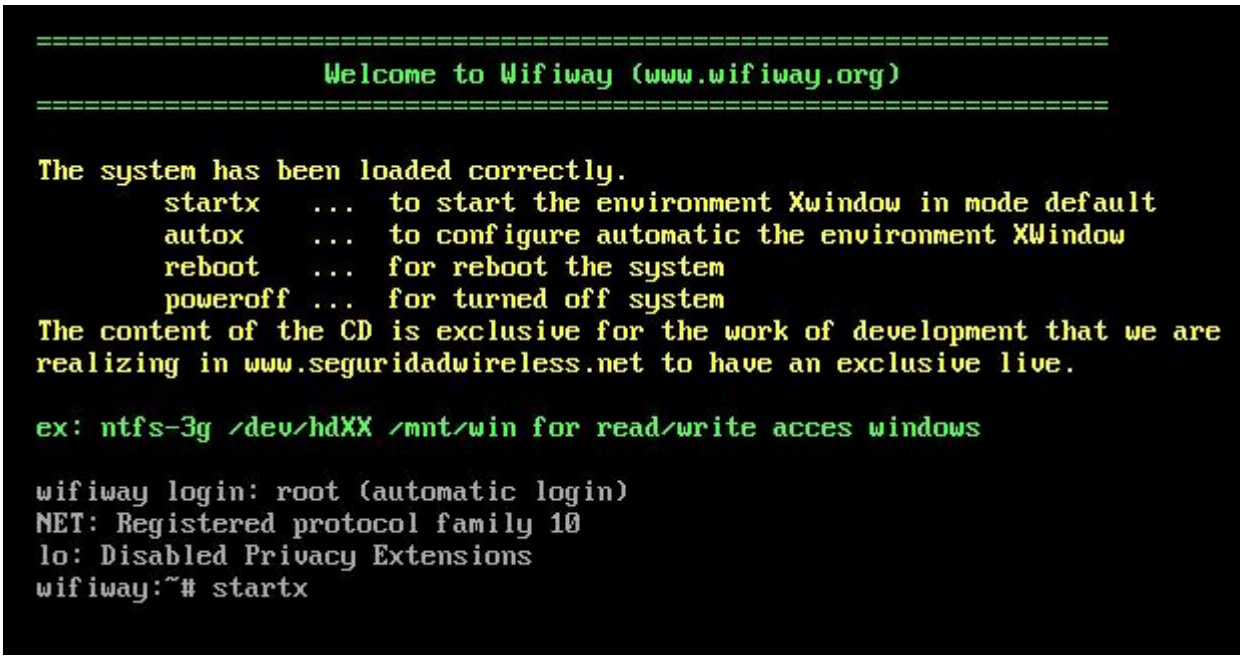
"Localtime"



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

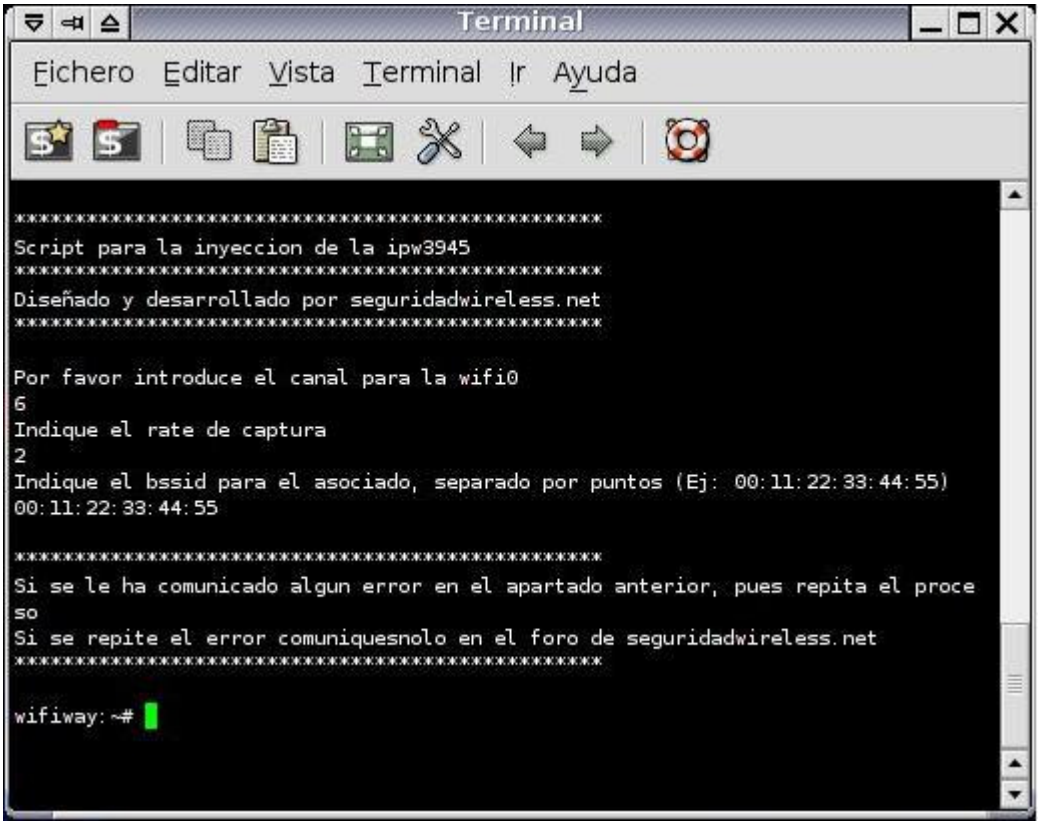


"OK"

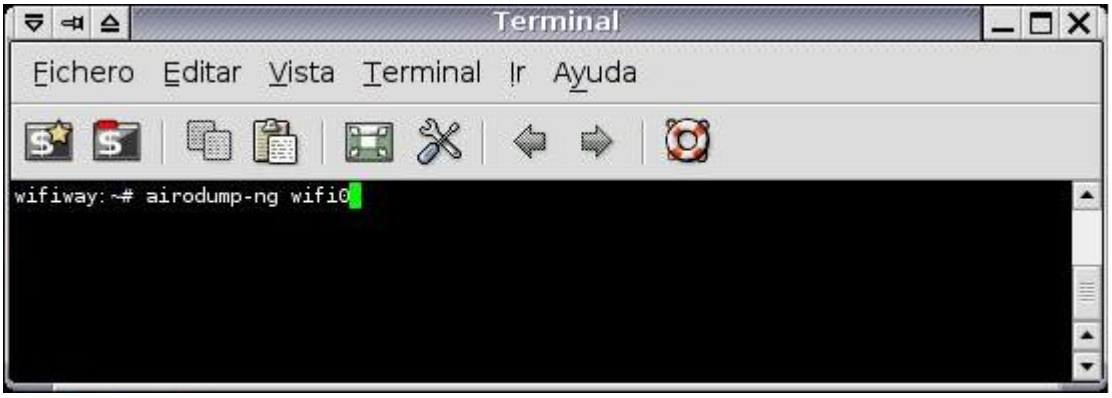


Bien, Wifiway ya ha arrancado, ahora basta con ejecutar los comandos o si eres un usuario torpecillo, podemos usar el entorno X, para ello ejecutamos: "startx",

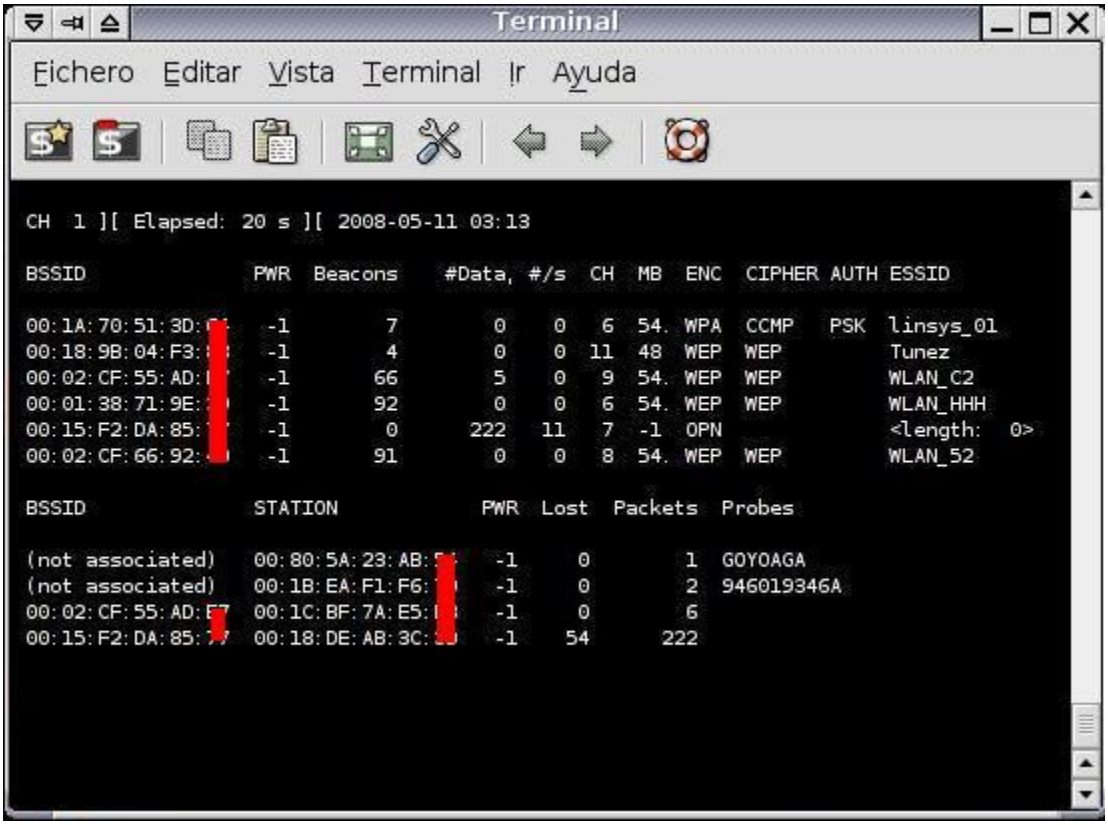
Ahora, en mi caso cargaré con un script que trae los drivers y configuración para mi adaptador, ejecutando. ipw3945_es.sh



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.

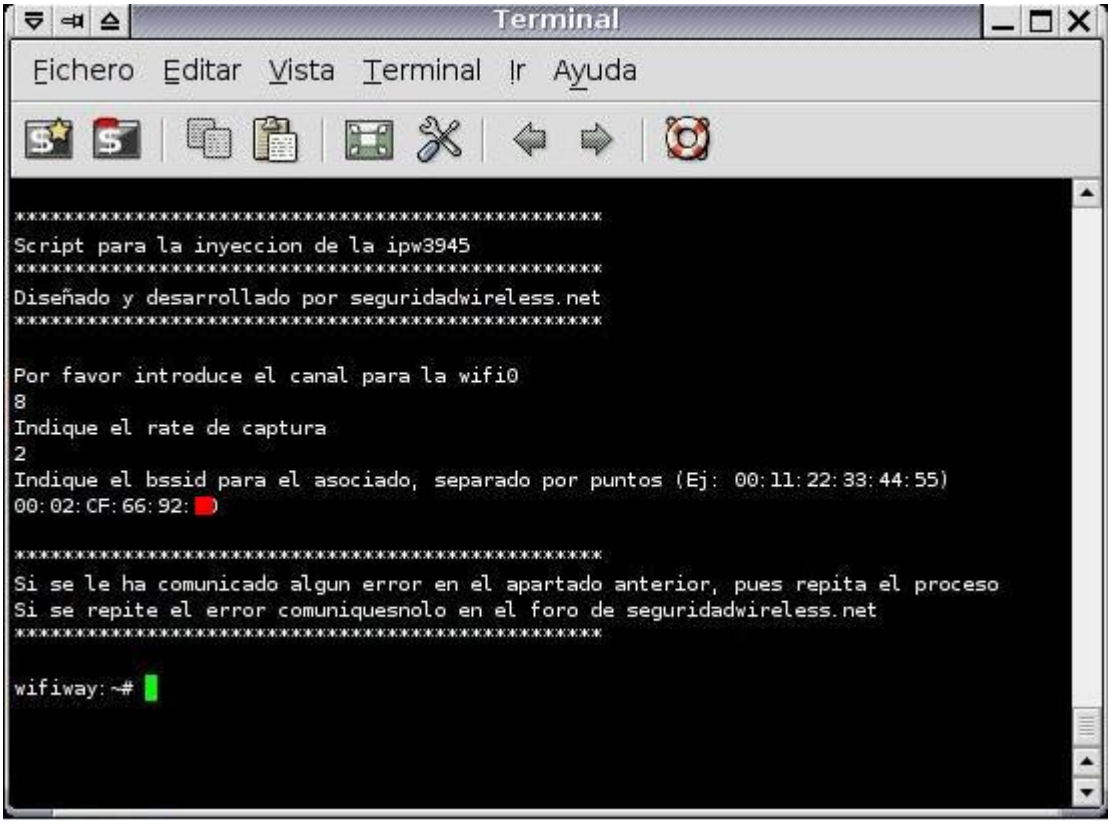


Con los drivers ya cargados y con el comando "airodump-ng wifi0" veremos las redes wifi que detecta nuestro adaptador y veremos los datos que necesitemos.



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).

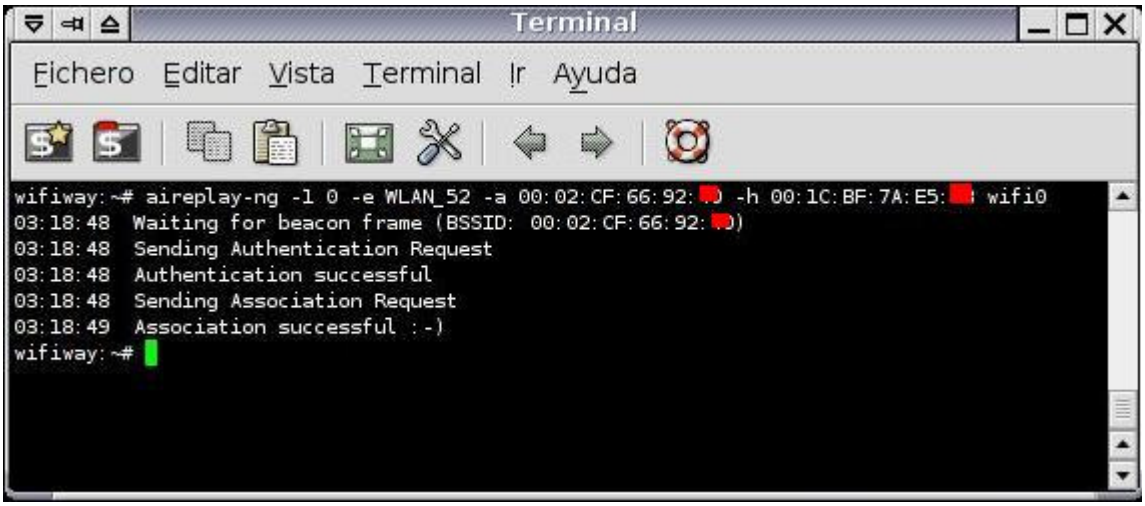
Ahora de nuevo ejecutamos el script para cambiar el canal y meter la MAC del AP que atacaremos... así que ejecutamos de nuevo "ipw3945_es.sh"



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!

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.



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,

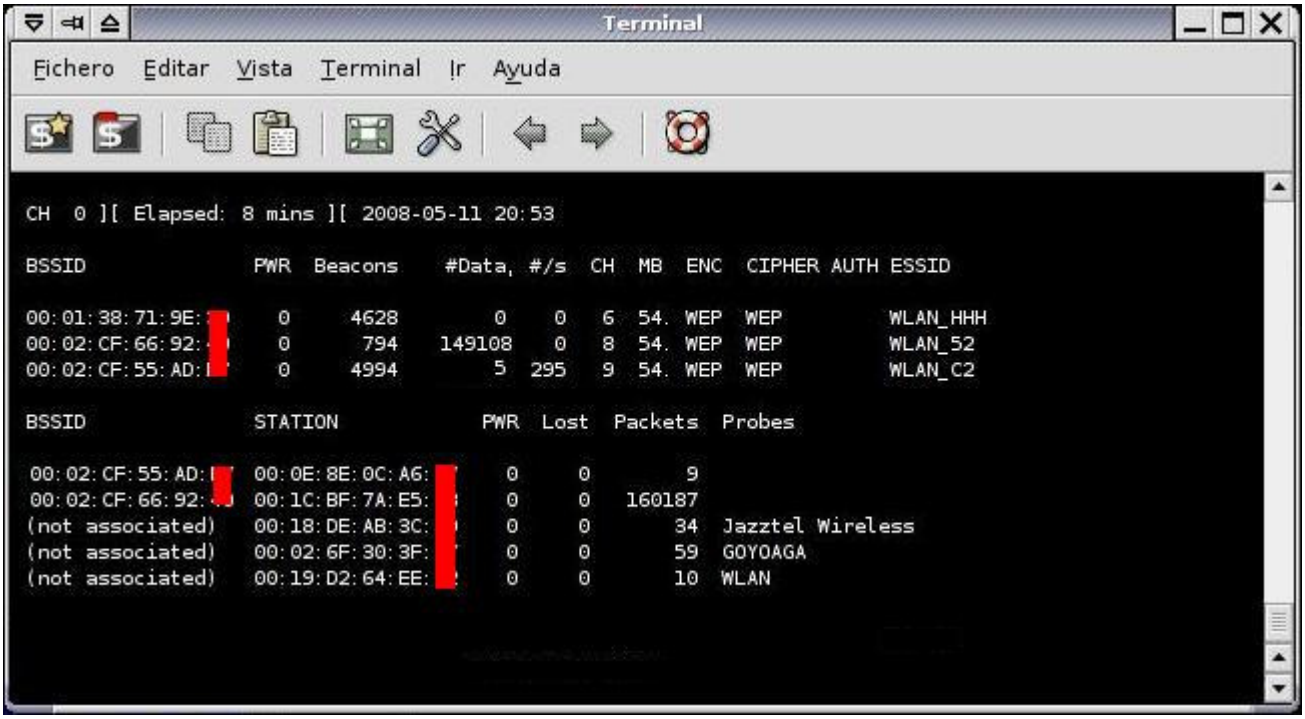
Ahora es cuando realmente inyectaremos paquetes al AP para generar tráfico y poder conseguir tráfico ARP, que nos servirá para inyectar más tráfico, y cuanto más tráfico tengámos, más fácil de sacar la clave WEP. Así que con el comando: "aireplay-ng -3 -b

MAC_AP -h MI_MAC wifi0" lo conseguiremos,

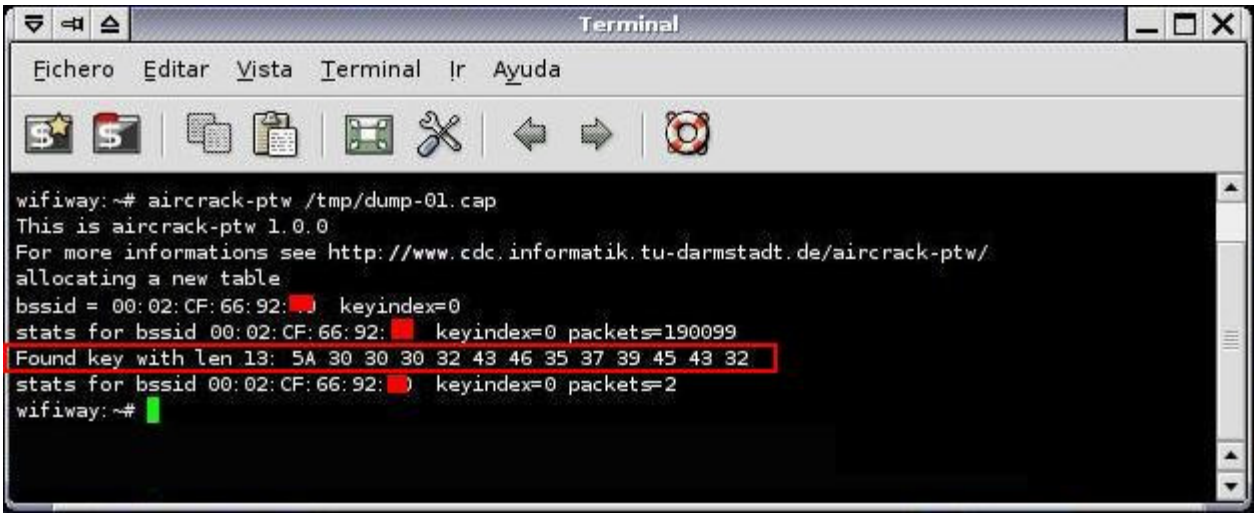
Esperamos mientras intenta inyectar para generar tráfico... vemos que ARP requests está a 0, le damos unos segundos y veremos cómo empieza a correr!

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

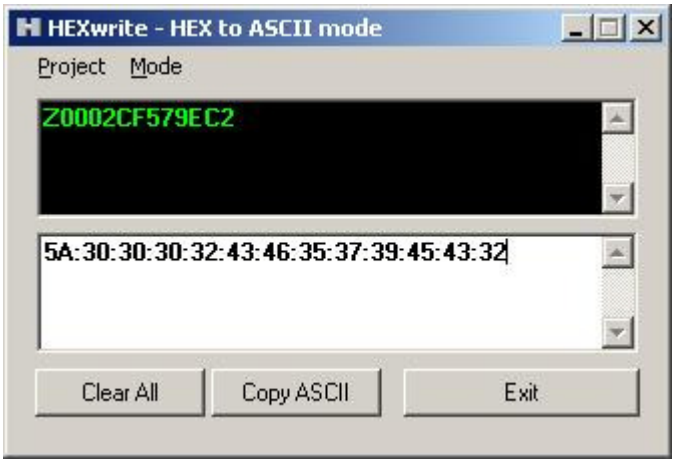
Abrimos un nuevo terminal, y vamos a grabar el tráfico, para ello, lo haremos con el comando "airodump-ng -w /tmp/dump rtap0"



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...



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