WEP, WPA/WPA2

Cracking

By: Alfa-Omega

Introduccion

En este manual explicare como crackear claves wep, wpa y wpa2, para ello utilizare el live cd de backtrack 3 (beta) y la suite aircrack (la suite aircrack ya viene incorporada en backtrack)

Wep crack

Bien, lo primero que tenemos que hacer antes de nada es poner nuestra tarjeta wireless en modo monitor, esto sirve para poder sniffar los paquetes de la red wireless a la que tenemos pensado acceder.

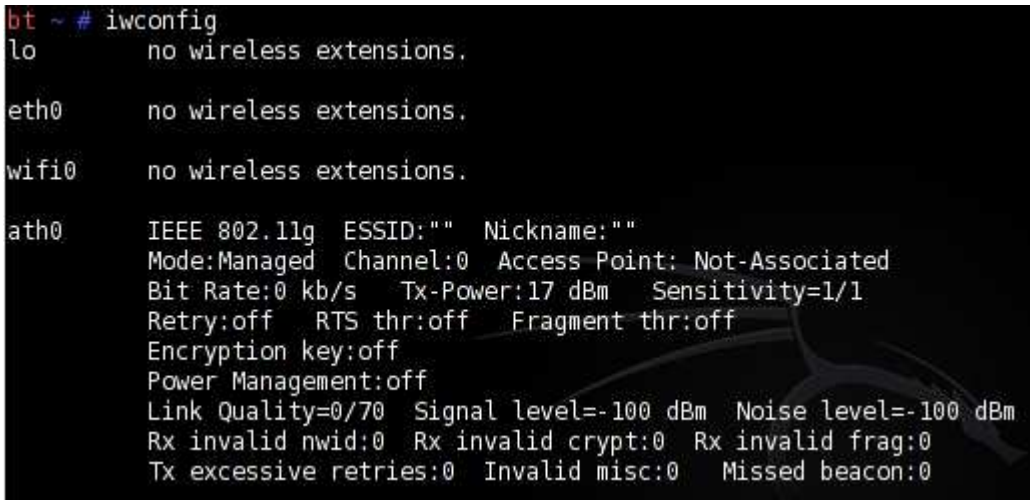
Para ello usaremos ***airmon-ng***, abrimos una Shell y escribimos el siguiente comando:

airmon-ng stop <interfaz>

donde ***<interfaz>*** es el nombre de la interfaz de vuestra tarjeta wireless

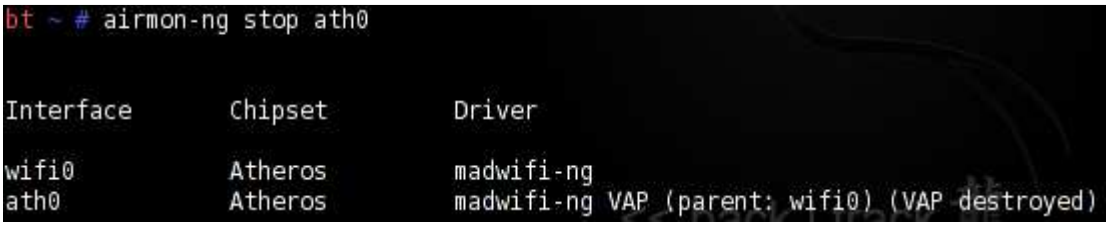
el flag ***stop*** sirve para "desactivar" la interfaz, para que posteriormente podamos ponerla en modo monitor…

si no sabes cual es el nombre de la interfaz de tu tarjeta wireless, escribe ***iwconfig*** en la Shell y te saldrá el nombre de la interfaz…



como se ve en la imagen el nombre de la interfaz de mi tarjeta wireless es ***ath0***, osea que en mi caso seria:

airmon-ng stop ath0



ahora usaremos el siguiente comando para poner la tarjeta en modo monitor:

airmon-ng start <interfaz>

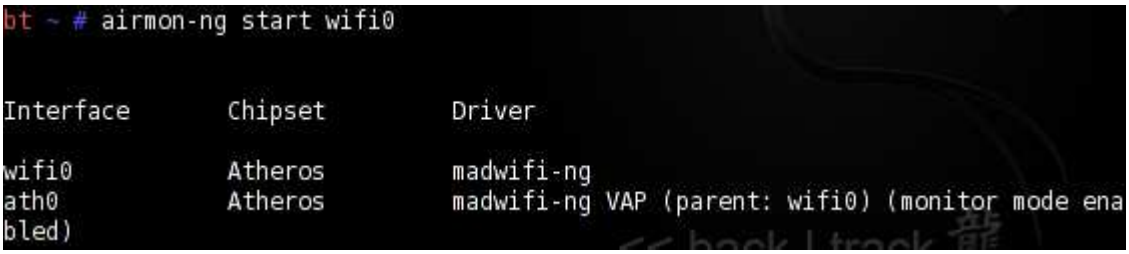
donde ***<interfaz>*** es el nombre de la interfaz de vuestra tarjeta wireless

el flag ***start*** sirve para poner la tarjeta en modo monitor

en mi caso seria…

airmon-ng start wifi0

en mi caso es ***wifi0*** en vez de ***ath0***, debido a que estoi usando los drivers madwifi-ng…



bueno, ahora ya estamos listos para empezar…

vamos a escanear las redes que tenemos a nuestro alcance…

para eso usaremos ***airodump-ng***, en la Shell escribe el siguiente comando:

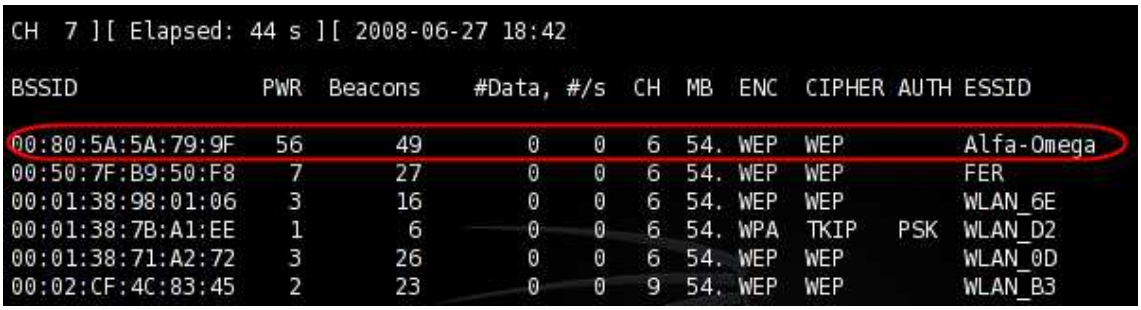
airodump-ng <interfaz>

donde ***<interfaz>*** es el nombre de la interfaz de vuestra tarjeta wireless

en mi caso seria:

airodump-ng ath0

y lo que se nos muestra es lo siguiente:



como se ve en la imagen tengo acceso a varias redes wireless

pero la malloria de ellas me dan una señal muy baja, si quereis crackear la pass de una red wireless con una señal tan baja os será muy difícil…

en mi caso intentare conectarme a la red “Alfa-Omega” que es la que mejor señal me da y además como se puede ver usa un cifrado WEP…

asi que voi a tomar un par de datos, vamos a apuntar la dirección mac (BSSID), el canal de la red y el nombre de la red (ESSID)

mac (BSSID): 00:80:5A:5A:79:9F

canal (CH): 6

nombre (ESSID): Alfa-Omega

bien, una vez tomados los datos ya podemos dejar de escanear las redes…

ahora vamos a capturar los paquetes de la red que nos interesa,

para ello usaremos ***airodump-ng*** otra vez

abrimos una Shell y escribimos:

airodump-ng -c 6 --bssid 00:80:5A:5A:79:9F -w captura ath0

repasemos los flags usados:

-c es el canal de la red wireless, en mi caso es el 6

--bssid es la dirección mac del punto de acceso al que le queremos crackear la pass en mi caso 00:80:5A:5A:79:9F (esto simplemente es un filtro para capturar únicamente los paquetes de la dirección mac indicada)

-w es el archivo donde se guardaran los paquetes que intercepta airodump-ng y que posteriormente usaremos para crackear la pass

ath0 es la interfaz de nuestra tarjeta

como se ve en la imagen el airodump esta capturando solo los paquetes de la red que le hemos indicado,

importante: no cierres la Shell donde tengas puesto el airodump-ng, porque sino dejara de sniffar los paquetes y el ataque no funcionara…

bien, ahora haremos una falsa autentificación, esto sirve para que el AP (Access poing, punto de acceso) no rechaze los paquetes que inyectaremos posteriormente

osea para que el AP acepte nuestros paquetes deberemos estar asociados a el, en caso de que conociésemos una dirección mac que estea asociada al AP pues podríamos usarla para inyectar paquetes, pero en este caso no conocemos ninguna, asi que usaremos la falsa autentificación.

Para ello usaremos ***aireplay-ng***, abre una nueva Shell y escribe el siguiente comando:

aireplay-ng -1 0 –e Alfa-Omega -a 00:80:5A:5A:79:9F -h 11:22:33:44:55:66 ath0

bien, repasemos los flags:

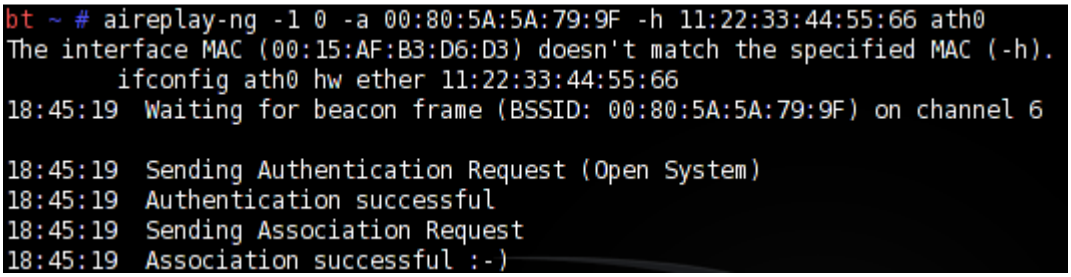
-1 es el flag que usa el aireplay para hacer la falsa autentificación, el ***0*** indica cada cuanto hace una falsa autentificación..

-e indica el ESSID del AP, osea… el nombre que tiene la red

-a es el BSSID del AP, osea… la dirección mac del punto de acceso

-h la mac que queremos que quede asociada con el AP, normalmente es mejor poner una mac inventada (como es el caso), pero también podríamos poner nuestra propia dirección mac (no es aconsejable, por razones de seguridad…)

ath0 es la interfaz de nuesta tarjeta



bien, ahora ya tenemos una dirección mac asociada con el AP, ya podemos inyectar paquetes,

lo que haremos a continuación será utilizar ***aireplay-ng*** para capturar peticiones ARP y volver a inyectarlas a la red, con esto generaremos paquetes que nos servirán para poder crackear la pass…

en una Shell escribimos lo siguiente:

aireplay-ng -3 -b 00:80:5A:5A:79:9F -h 11:22:33:44:55:66 ath0

repasemos los flags…

-3 este es el flag que usa aireplay para capturar y reenviar las peticiones ARP

-a es el BSSID del AP, la dirección mac del punto de acceso

-h la dirección mac que hemos asociado antes, o en caso de que sepamos alguna que ya estea asociada pues podemos usarla

ath0 es la interfaz de nuesta tarjeta

como vemos en la imagen el aireplay esta capturando paquetes, pero no captura ninguna petición ARP…. Asi que tenemos que esperar hasta que haya capturado unas 150.000 (esto puede llevar varios minutos)

bien, como vemos en la imagen ya hemos capturado unas 150.000 peticiones ARP, asi que ha llegado el momento decisivo…

vamos a crackear la clave wep…

para ello usaremos ***aircrack-ng***

abrimos una nueva Shell y escribimos el siguiente comando:

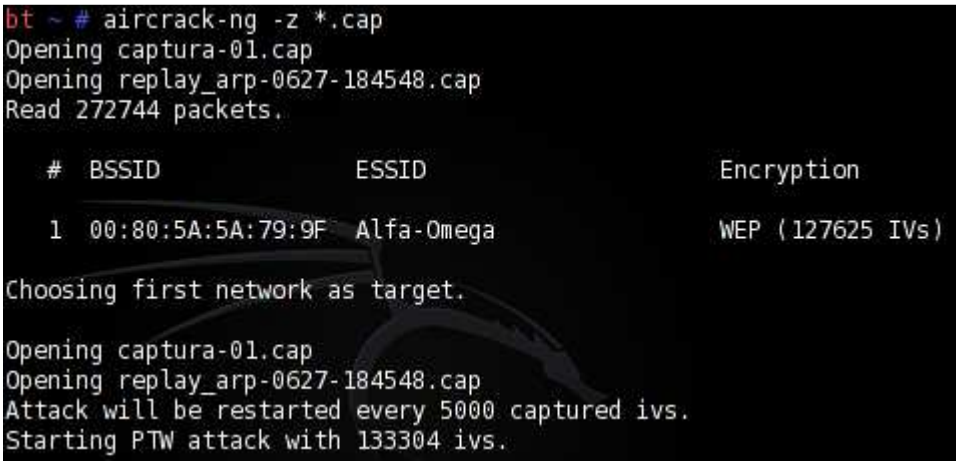
aircrack-ng -z *.cap

repasemos los flags:

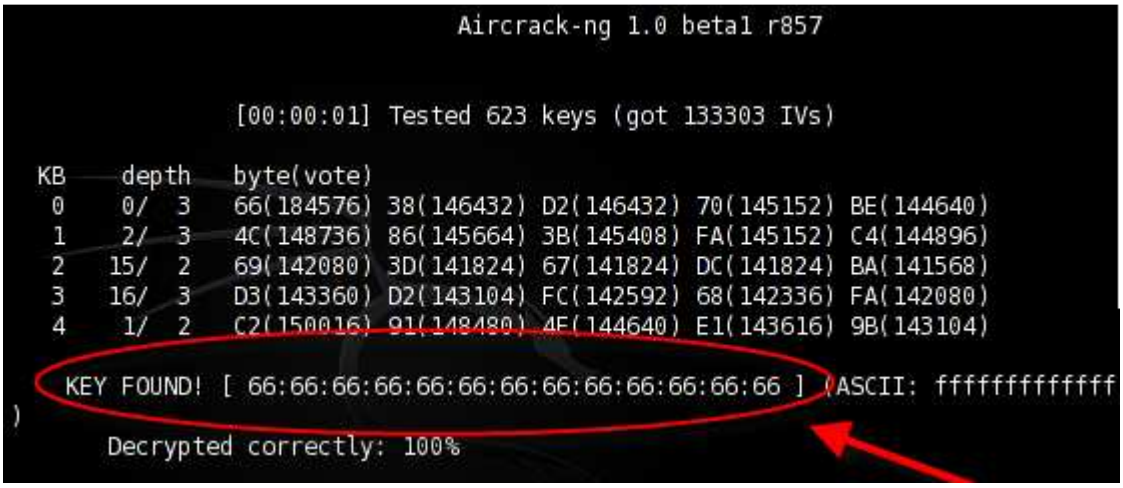
-z es el flag que usa aircrack para activar un tipo de crackeo rápido..

*.cap la ruta donde tengamos el archivo de captura de airodump, en mi caso el archivo esta en el directorio root asi que que no hace falta que ponga ruta, simplemente he puesto *.cap para que abra todos los archivos con extensión .cap..

Pulsamos enter….



Esperamos unos pocos segundos y…….



BINGO !!!!

Como se puede ver en la imagen:

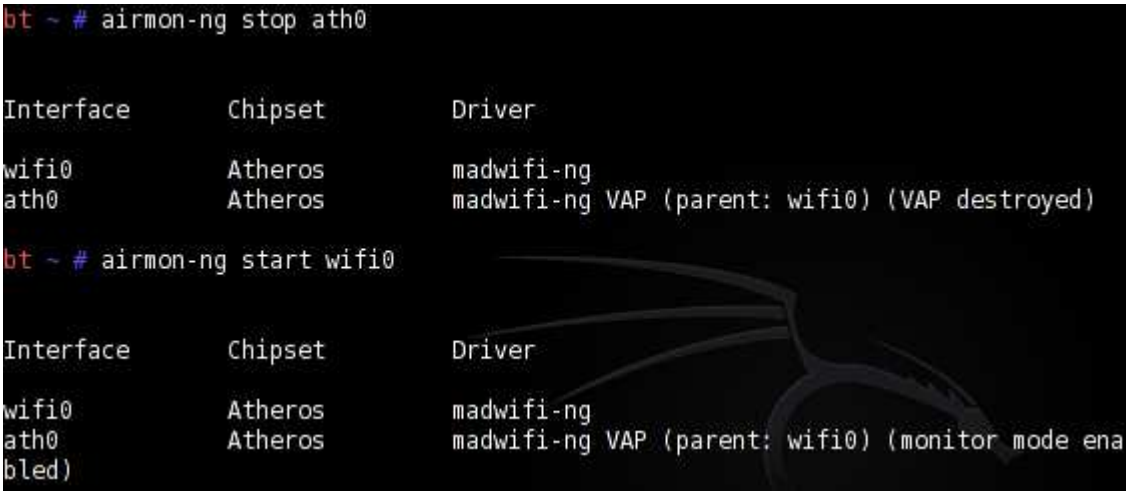
KEY FOUND! [66:66:66:66:66:66:66:66:66:66:66:66:66]

La clave es tan larga porque es de 128bits…

WPA/WPA2 Crack

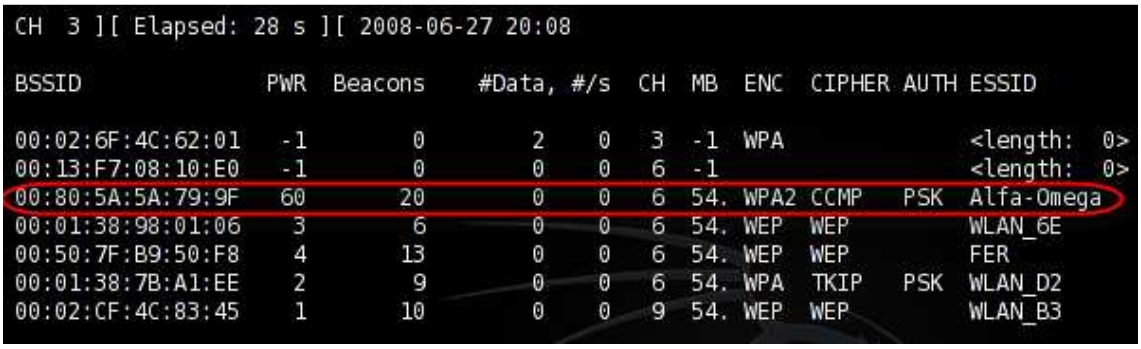
Ahora pasare a explicar como crackear pass wpa/wpa2, (el sistema es el mismo para los dos tipos de cifrados)

Bueno, antes de nada tenemos que seguir el mismo procedimiento que en el wep crack y poner la tarjeta en modo monitor usando airmon-ng…



Una vez lo tengamos hecho… empezamos…

Al igual que en el wep crack primero vamos a escanear para saber las redes a las que podemos acceder

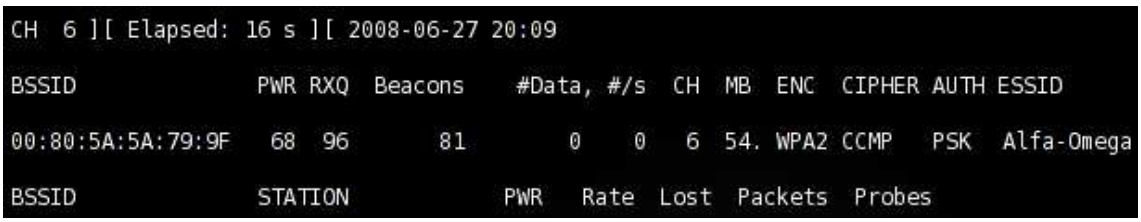


Como vemos la red de Alfa-Omega es una victima perfecta… tiene una buena señal y un cifrado WPA2, asi que vamos a por esa… al igual que antes apuntamos lo datos.. mac(bssid), cannel(CH) y nombre(essid).

Usamos ***airodump-ng*** para capturar los paquetes

Es exactamente el mismo comando que para el wep crack…

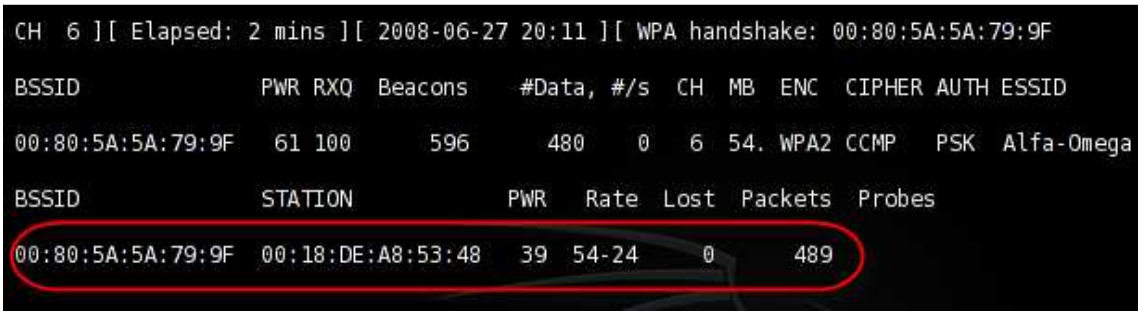
airodump-ng –c 6 --bssid 00:80:5A:5A:79:9F –w captura ath0



bien… aora supuestamente tendriamos que esperar a que capture el handshake… que es lo que nos interesa realmente, pero esto puede tardar muchisimo tiempo, tendríamos que esperar a que se conecte algún cliente,

pero…. Si vemos que hay algún cliente conectado a la red, lo que podemos hacer es desautentificarle de la red, para que se vuelva a autentificar y asi conseguir el handshake y poder crackear la pass…

para saber si hay algún cliente conectado nos vamos a la shell donde tenemos puesto el ***airodump-ng*** y miramos en la parte de abajo si hay algún cliente conectado:



genial!!! Estoy de suerte, hay un cliente conectado a la red (mejor dicho… acabo de coger mi otro portátil y lo he conectado a la red xD)

ahora cogemos los datos del cliente conectado, solo nos hace falta la mac del cliente..

bien, para desautentificar vamos a usar el ***aireplay-ng***

abrimos una Shell y escribimos el siguiente comando:

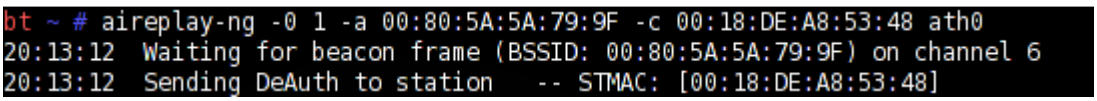
aireplay-ng -0 1 -a 00:80:5A:5A:79:9F -c 00:18:DE:A8:53:48 ath0

repasemos los flags..

-0 es el flag usado para desautentificar el 1 indica las veces que se mandara la desautentificacion

-a es la dirección mac del AP

-c es la dirección mac del cliente que queremos desautentificar



Ahora solo tenemos que crackear…

Al igual que antes usaremos ***aircrack-ng***

Abrimos una Shell y escribimos:

aircrack-ng –w pass *.cap

repasemos los flags:

-w es la ruta del diccionario que usaremos para crackear , en mi caso tengo el diccionario en el directorio root asi que ya no me hace falta poner la ruta, con el nombre basta

****.cap*** la ruta donde tengamos el archivo de captura de airodump, en mi caso el archivo esta en el directorio root asi que que no hace falta que ponga ruta, simplemente he puesto *.cap para que abra todos los archivos con extensión .cap..

Pulsamos enter…

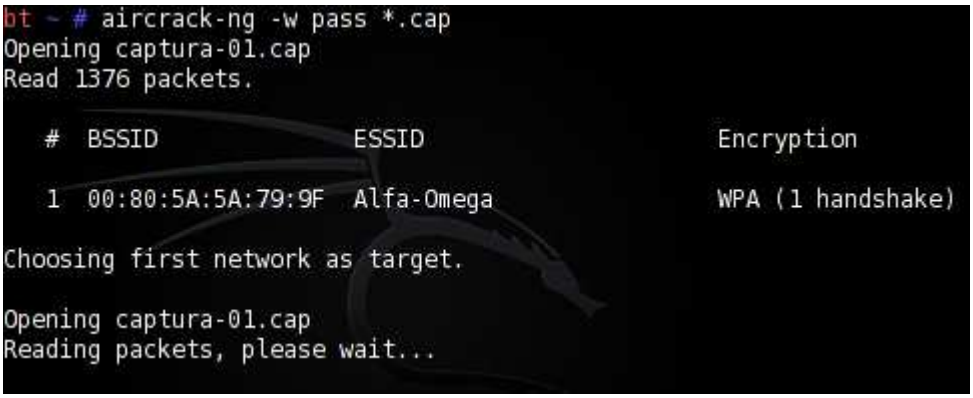
Si el airodump-ng no capturo el handshake se mostrara un mensage diciendo que no se ha capturado ningún handshake

Entonces tendremos que volver a desautentificar a algún cliente conectado para que podamos hacernos con los paquetes handshake

Si el airodump-ng capturo el handshake empezara el crackeo…

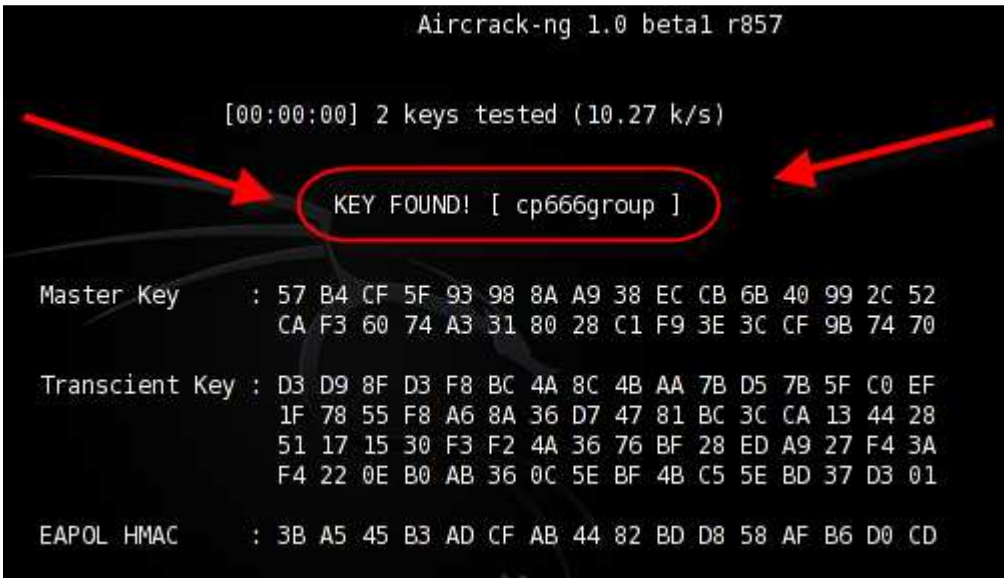
Esto puede tardar 5 minutos o 5 semanas… depende del diccionario que useis…

En mi caso…



…apenas unos segundos…

…y…



BINGO!!!!!!

Pass conseguida…

Como evitar que crackeen mi pass???

Bueno… aquí pondré un par de consejos para evitar que entren en vuestras redes sin vuestro consentimiento.

1º cuando os vallais a comprar un router aseguraros de que soporte cifrados wpa/wpa2 son los mas seguros que existen oi en dia…

2º cuando vallais a poner una clave a la red, procurar que tenga mas de 15 caracteres y que sea una pass Alfa-Numerica (con números y letras)

3º si podeis… configurar vuestro router para que solo acepte las direcciones mac que vosotros queráis…

Estos consejos no evitan al 100% que entren en tu red, pero ayudan mucho…

ESTE MANUAL HA SIDO ESCRITO PARA LA COMUNIDAD DE PROGRAMADORES DE
666

WWW.CP666GROUP.COM
WWW.CP666GROUP.COM/foro

Manual escrito por Alfa-Omega