



REDES WIRELESS

SANTIAGO PEÑARANDA MEJIA

BUENO LO PRIMERO QUE VAMOS HACER ES PONER NUESTRA INTERFAZ DE RED EN MODO **MONITOR** PARA PODER LOCALIZAR LAS REDES **WIRELESS** CERCANAS. ESTO LO HACEMOS CON EL SIGUIENTE COMANDO.

AQUÍ LO QUE HACEMOS ES MATAR TODOS LOS PROCESOS DE RED QUE SE ESTEN EJECUTANDO AHORA MISMO EN LA MÁQUINA, PARA QUE NO HAYA NINGUNA INTERRUPCIÓN NI NADA.

```
[root@parrot]-[/home/santo]
#airmon-ng check kill

Killing these processes:

    PID Name
    3630 wpa_supplicant

[root@parrot]-[/home/santo]
#
```

UNA VEZ YA MATADO CUALQUIER INTERFAZ O PROCESO QUE SE ESTUVIERE EJECUTANDO EN LA MAQUINA AHORA SI VAMOS A PRENDER NUESTRA INTERFAZ DE RED, CON EL SIGUIENTE COMANDO

```
[root@parrot]-[/home/santo]
#airmon-ng start wlxf0a7314b0cf7
```

Y COMO PODEMOS COMPROBAR YA ESTÁ EN MODO MONITOR NUESTRA INTERFAZ DE RED

```
#iwconfig
lo          no wireless extensions.

ens33      no wireless extensions.

wlsx0a7314b0cf7 IEEE 802.11bgn ESSID:"Luciana_Nora" Nickname:"WIFI@RTL8821A"
Mode:Monitor Frequency:2.457 GHz Access Point: 88:DE:7C:E0:F8:FF
Sensitivity:0/0
Retry:off RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=1/100 Signal level=1/100 Noise level=0/100
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0
```

AHORA LO QUE VAMOS HACER ES LOCALIZAR REDES WIRELESS CERCANAS, PARA ELLO ESCRIBIMOS EL SIGUIENTE COMANDO

```
[root@parrot]-[/home/santo]
#airodump-ng wlan0
```

Y AL EJECUTAR ESTE COMANDO AUTOMÁTICAMENTE VAMOS A LOCALIZAR LAS REDES WIRELESS CERCANAS A NOSOTROS

```
BSSID          PWR Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
F4:F6:47:FD:63:C4 -88      2         0  0  11  130  WPA2 CCMP PSK WIFI_MESH_63C4
54:46:17:F1:52:99 -77      8         0  0  6  130  WPA2 CCMP PSK E546
F4:69:42:3F:E9:DF -84      0         1  0  10  -1  WPA                <length: 0>
CC:ED:DC:F5:D1:F8 -78     14         0  0  4  130  WPA2 CCMP PSK MOVISTAR_D1F8
80:29:94:AB:B7:B3 -68     10         0  0  6  130  WPA2 CCMP PSK Tech_D0006601
D4:60:E3:03:44:21 -82      0         0  0  -1  -1                <length: 0>
B0:C2:87:E9:C3:7F -81      2         0  0  1  130  WPA2 CCMP PSK R-Wlan 1140
10:27:F5:61:D4:10 -82     11         0  0  4  270  WPA2 CCMP PSK TP-Link_D410
D4:60:E3:2E:F2:91 -69     14         0  0  13  130  WPA2 CCMP PSK ANITA
4C:AB:F8:E7:EC:2F -79      4        34  7  11  130  WPA2 CCMP PSK MOVISTAR_EC20
E8:6E:44:07:1C:44 -74     10         0  0  7  360  WPA2 CCMP PSK DIGIFIBRA-XNyP
1C:3B:F3:25:95:5D -81      4         2  0  6  130  WPA2 CCMP PSK BLACKHAND_EXT
FC:12:63:67:C8:BF -83      5         0  0  6  130  WPA2 CCMP PSK MOVISTAR_C8B0
86:36:54:4C:F2:22 -77      7         0  0  6  720  WPA2 CCMP PSK F220
56:46:17:C1:52:99 -76     12         0  0  6  130  WPA2 CCMP PSK <length: 0>
CC:D4:A1:88:59:FB -79      4         2  0  6  130  WPA2 CCMP PSK MOVISTAR_59FA
F4:CA:E7:3D:5C:36 -42     13         7  0  1  195  WPA2 CCMP PSK Livebox6-5C37
B2:C2:87:E9:C3:70 -83      4         0  0  1  130  WPA2 CCMP MGT wificlientesR
F6:0E:F3:08:31:BE -83      6        27  0  1  720  WPA2 CCMP PSK 31BC
5C:A6:E6:4D:2E:E4 -84     10       143  50  1  130  WPA2 CCMP PSK 31BC_EXT
88:DE:7C:E0:F8:FF -86      3         0  0  10  130  WPA2 CCMP PSK Luciana_Nora
Quitting...
[red prompt][root@parrot]-[/home/santo]
[red prompt][root@parrot]-[/home/santo]
[red prompt][root@parrot]-[/home/santo]
```

Ahora vamos hacer una pequeña descripción de mi propia red de mi casa, primero localizamos el objetivo.

```
CC:D4:A1:88:59:FB -79      4         2  0  6  130  WPA2 CCMP PSK MOVISTAR_59FA
F4:CA:E7:3D:5C:36 -42     13         7  0  1  195  WPA2 CCMP PSK Livebox6-5C37
B2:C2:87:E9:C3:70 -83      4         0  0  1  130  WPA2 CCMP MGT wificlientesR
```

Las características más claras e importantes para nosotros son:

- CANAL: 1
- ESSID: LIVEBOX6-5C37
- BSSID: F4:CA:E7:3D:5C:36

Y PUES YA ESTARÍA, ESTO SERÍA TODO. CHAO Y GRACIAS