

# WiFiSlax 3.1



Sergio González

Félix Ortega

Alberto Moreno

# ¿Qué es WiFiSlax?



# ¿Qué es WiFiSlax?

- Es una metadistribución linux
- Live CD basado en Slax
- Inicialmente, BackTrack remasterizado
- Orientada hacia la Seguridad Wireless
- Traducida al castellano
- Facilita su uso a los usuarios habituados a entornos 'graficos'
- Instalable

# ¿Qué es WiFiSlax?

- Live CD totalmente funcional
- Kernel 2.6.21.5
- KDE 3.5.7
  - También incluye git y scripts Compiz Fusion
- Automonta nuevas unidades
  - Con escritura sobre NTFS
- Automonta nuevos dispositivos
  - Dispositivos inalámbricos / mouse / etc

## Navegadores:

- Opera 9.02
- Firefox 2.0.0.5
  - NoScript
  - Torbutton
  - Tamper Data
  - Web Developeretc...
- Konqueror 3.5.7

# ¿Qué diferencia a WiFiSlax?

- Orientada a la AUDITORÍA de seguridad wireless
- Herramientas mas actuales para AUDITORÍA Inalámbrica
- Posee los controladores de los chipsets mas comunes en nuestros equipos informáticos
- Facilita su uso a los no iniciados en Linux
  - Lanzadores
  - Ayuda básica en castellano

# ¿Quién está detrás de WiFiSlax?



## ● La comunidad de elhacker.net

Index: <http://www.elhacker.net/>

Subforo HW:

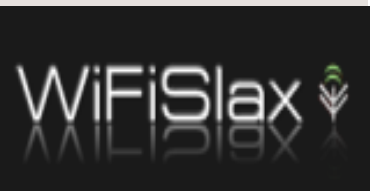
<http://foro.elhacker.net/index.php/board,48.0.html>



## ● Seguridadwireless.net

Index: <http://www.seguridadwireless.net/>

Foro: <http://www.seguridadwireless.net/foro/index.php>



## ● WiFiSlax.com

Index: <http://www.wifislax.com/>

# ¿Qué puedo encontrar en WiFiSlax?

## Aplicaciones de Auditoría

- Asistencia chipset
- Herramientas Wireless
  - Kismet, machanger, etc
- Suite aircrack y aircrack-ng
- Estudio de cifrado (WEP, WPA y WPA2)
- Nmap, amap, etc...
- Lanzadores de asistencia para conexión
- Herramientas BlueTooth
- gFTP 2.0.18 / GpsDrive 2.10

# ¿Qué puedo encontrar en WiFiSlax?

## + aplicaciones de Auditoría

- Nmap Front End 4.11
- Yersinia 0.7
- Wireshark
- etthercap
- THC-Hydra
- SQLquery
- IKE-Scan
- PSK-Crack
- Etc

# ¿Qué puedo encontrar en WiFiSlax?

## Aplicaciones de Auditoría Wireless

- Suite tradicional **aircrack-spanish**

Esta suite es la tradicional suite creada por Devine al que tanto admiramos y que fue traducida por Uxio

- Suite actual **aircrack-ng-ME**

Esta suite es desarrollada por Mr.X, pero con los parches añadidos por thefkboss

- **aircrack-ptw-spanish**

Herramienta optimizada por la universidad de Darmstadt traducida por Stilo16v

<http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>

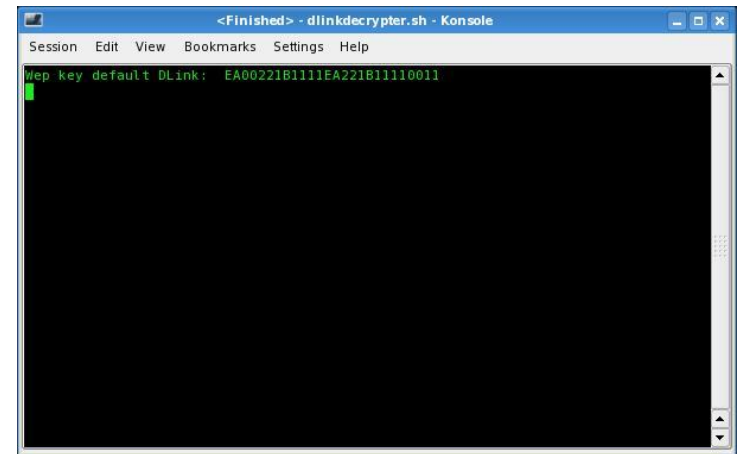
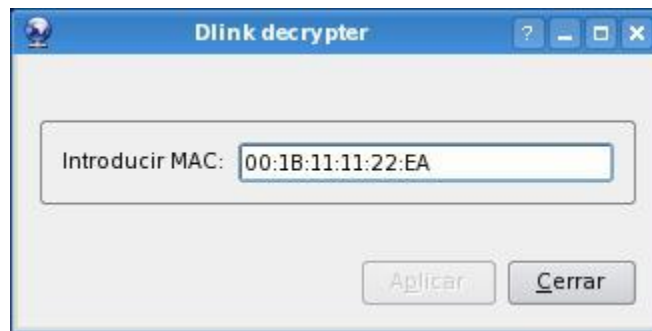
# ¿Qué puedo encontrar en WiFiSlax?

## Aplicaciones de Auditoría Wireless

### ● Wlan decrypter



### ● Dlink decrypter



# ¿Qué puedo encontrar en WiFiSlax?



```
Shell - Airoscript
Session Edit View Bookmarks Settings Help

Bienvenido a Airoscript

Airoscript es una herramienta educativa
para el conocimiento del funcionamiento de las seguridad WIFI
Si hubiese errores pon la variable DEBUG a 1
Esto te permitira ver los errores en el xterm
Rutas de capturas en /root/swireless/airoscript/
Para Tratamiento WPA colocar fichero wordlist
en /root/swireless/wordlist/

Visita: seguridadwireless.net & wifislax.com

Este mensaje desaparecera en pocos segundos
```

```
Shell - Airoscript
Session Edit View Bookmarks Settings Help

Selecciona el interface wifi a usar:

1) ath0
2) wifil
3) rausb0
#?
```

```
Shell - Airoscript
Session Edit View Bookmarks Settings Help

1. Scan ==> Escanear para encontrar objetivos
2. Select ==> Selección de objetivo: Host y Cliente
3. Attack ==> Lanzar ataque
4. Crack ==> Empezar a buscar la clave con aircrack
5. Configure ==> Configurar PC para conexión usando la clave encontrada y DHCP
6. Associate ==> Intentar asociar a AP usando cliente falso
7. Deauth ==> Desconectar cliente(s) del objetivo
8. Reset ==> Cerrar todos los procesos y resetear tarjeta(pcmcia socket)
9. Monitor ==> Activar modo monitor usando airmo-ng
10. Quit
11. AUTO ==> pasos 1,2,3
12. Borrar ==> Elimina archivos /root/swireless/airoscript/
13. Crack 2 ==> Empezar a buscar la clave con aircrack usando diccionario WLAN
14. Borrar 2 ==> Borrar diccionarios /root/swireless/wordlist/
15. Crack 3 ==> Empezar a buscar la clave con aircrack usando diccionario DLINK

1) 1 3) 3 5) 5 7) 7 9) 9 11) 11 13) 13 15) 15
2) 2 4) 4 6) 6 8) 8 10) 10 12) 12 14) 14
#?
```

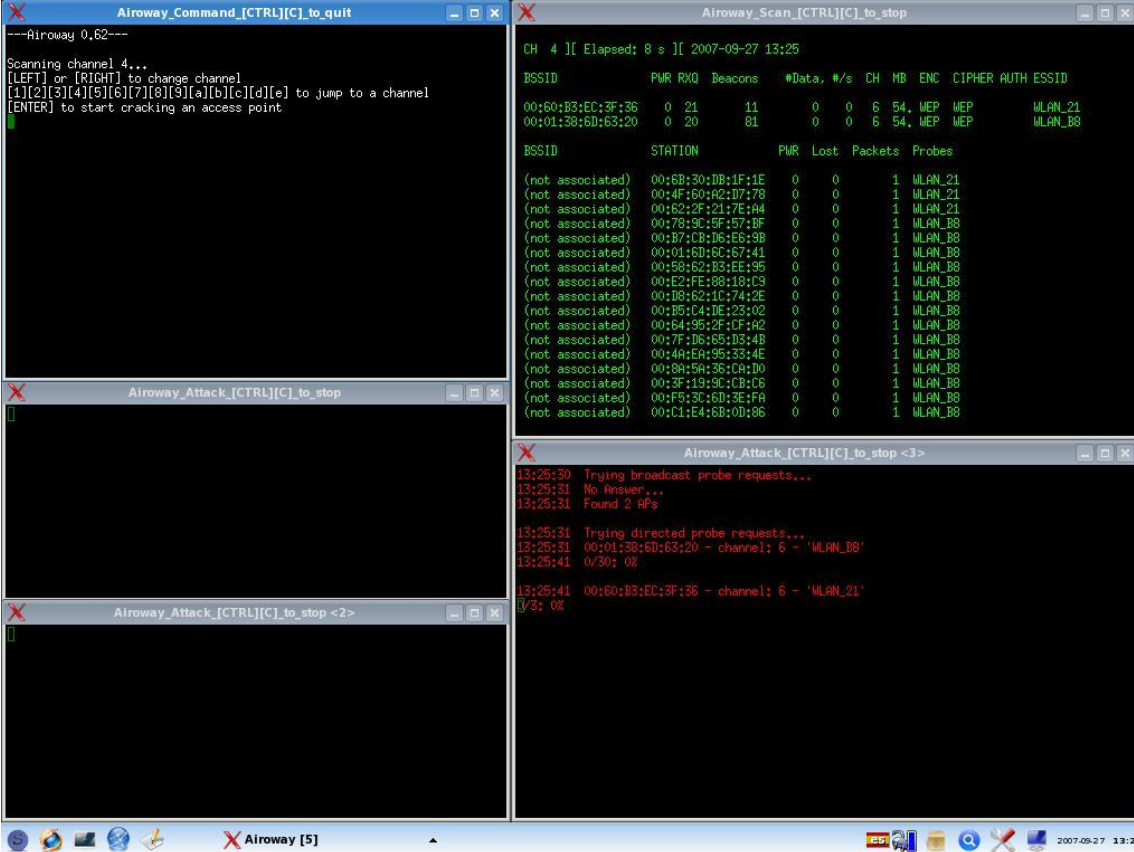
# ¿Qué puedo encontrar en WiFiSlax?

 Airoscript

DEMO

# ¿Qué puedo encontrar en WiFiSlax?

## Airoway



The screenshot displays the Airoway software interface with several windows open:



- Airoway\_Command [CTRL][C]\_to\_quit**: Shows the main menu with options for scanning channels, changing channels, jumping to a channel, and starting a cracking attempt.
- Airoway\_Scan [CTRL][C]\_to\_stop**: Displays scan results for channel 4. It shows two BSSIDs: 00:60:B3:EC:3F:36 (WLAN\_21) and 00:01:38:6D:63:20 (WLAN\_BB). Below this is a table of detected stations.
- Airoway\_Attack [CTRL][C]\_to\_stop**: Shows the attack process, including broadcast and directed probe requests.
- Airoway\_Attack [CTRL][C]\_to\_stop <3>**: Shows the results of the attack, indicating that 2 APs were found.
- Airoway\_Attack [CTRL][C]\_to\_stop <2>**: Shows the results of the attack, indicating that 0/30: 0% of the attack was successful.

BSSID	STATION	PWR	Lost	Packets	Probes
(not associated)	00:6B:30:DB:1F:1E	0	0	1	WLAN_21
(not associated)	00:4F:60:A2:D7:78	0	0	1	WLAN_21
(not associated)	00:E2:2F:21:7E:94	0	0	1	WLAN_21
(not associated)	00:78:9C:5F:57:8F	0	0	1	WLAN_BB
(not associated)	00:B7:CB:D6:E6:8B	0	0	1	WLAN_BB
(not associated)	00:01:6D:6C:67:41	0	0	1	WLAN_BB
(not associated)	00:58:62:83:EE:95	0	0	1	WLAN_BB
(not associated)	00:E2:FE:88:18:C9	0	0	1	WLAN_BB
(not associated)	00:D8:62:1C:74:2E	0	0	1	WLAN_BB
(not associated)	00:B5:C4:DE:23:02	0	0	1	WLAN_BB
(not associated)	00:64:95:2F:CF:A2	0	0	1	WLAN_BB
(not associated)	00:7F:D6:65:D3:4B	0	0	1	WLAN_BB
(not associated)	00:4A:EA:95:33:4E	0	0	1	WLAN_BB
(not associated)	00:5A:5A:3E:0A:D0	0	0	1	WLAN_BB
(not associated)	00:3F:19:9C:0B:C6	0	0	1	WLAN_BB
(not associated)	00:F5:3C:6D:3E:FA	0	0	1	WLAN_BB
(not associated)	00:C1:E4:6B:0D:86	0	0	1	WLAN_BB



# ¿Qué puedo encontrar en WiFiSlax?

## Recomposición de sesiones TCP:

### **airdecap-ng**

-  Campos de formularios sin cifrado SSL
-  Sin cifrado, WEP, WPA, WPA2

### **Wireshark**

-  Sin cifrado, WEP y WPA
-  Voz sobre IP

# ¿Qué puedo encontrar en WiFiSlax?

## Inyección de paquetes:

### **aireplay-ng**

-  Inyección de tráfico wireless

### **Wireshark**

-  Módulo de inyección

# ¿Qué pretende WiFiSlax?

- Perder el miedo a GNU/Linux
- Mejorar la seguridad inalámbrica
- Abandonar WEP y WPA
- Potenciar nuevos estándares de seguridad
- Concienciar al usuario
- Fomentar interés en seguridad

# Controladores de dispositivos inalámbricos

- Prism54
- Madwifi-ng
- Wlan-ng
- HostAP
- Ralink rt2570
- Ralink rt2500
- Ralink rt73 **INYECCIÓN**
- Ralink rt61
- Ralink rt8187
- Zydas ZD1201
- Zydas ZD1211rw
- Zydas ZD1211b
- IPW2100
- IPW2200 **INYECCIÓN**
- IPW3945 **INYECCIÓN**
- Realtek rtl8180
- Realtek rtl8185
- Realtek rtl8187
- Broadcom **INYECCIÓN**

# ¿Qué pretende WiFiSlax?

- Facilidad de uso con independencia del driver
- Lanzadores:
  - - Broadcom bcm43xx
  - - Intel IPW2200, IPW3945
  - - Ralink rt2570, rt73
  - - Prism
  - - Realtek rt815/rt 8180, rt8187
  - - Atheros mode monitor, mode managed
  
- ¿Problemas con tu tarjeta?
  - usbview, lsusb, lspci, dmesg, etc...

# ¿Qué pretende WiFiSlax?

- Eliminar los cifrados mal implementados
- No existen claves robutas
- Concienciar al usuario de verdad

**Por n-esima vez:**

**WEP ES INSEGURO**

● WPA2 ¿seguro?

Cowpatty ;-)

## DEMO

# ¿Instalar WiFiSlax?

## ● Gestores de arranque

- LILO
- LILO con Windows
- GRUB



# Integración de en Wifislax

## ● Proyecto de colaboración

- Seguridad Wireless
- El Blog de Gospel

## ● Características

- Incluye TODAS las herramientas de auditoría de seguridad Bluetooth
- Lanzadores intuitivos para ejecutar aplicaciones



# Integración de en Wifislax

- Incluye herramientas de escaneo
  - BlueZ utils: hcitool, sdptool, l2ping, rfcomm, ...
  - BlueZScanner: escaner de dispositivos
  - Redfang: descubrimiento de equipos ocultos
  - OBEX utils: OpenOBEX, ObexFTP, ...
  - BlueZSpammer: hot spot para envíos masivos



# Integración de Bluetooth® en Wifislax

## ● Permite lanzar los siguientes ataques

### ● Teléfonos antiguos

- Bluebug
- Bluesnarf
- Helomoto



### ● Teléfonos modernos

- Blueline (Motorola)
- Blue MAC Spoofing



### ● Manos libres

- Car Whisperer



# Ataque Blue MAC Spoofing

● Credenciales de seguridad en Bluetooth, ¡la realidad!

## ● AUTORIZACIÓN

- Se basa en la dirección BD\_ADDR de dispositivo
- Si existe en la lista de dispositivos de confianza, queda autorizado

## ● AUTENTICACIÓN

- Se basa en la dirección BD\_ADDR + clave de enlace
- Si la clave en enlace generada durante el emparejamiento con ese dispositivo coincide, queda autenticado

# Ataque Blue MAC Spoofing

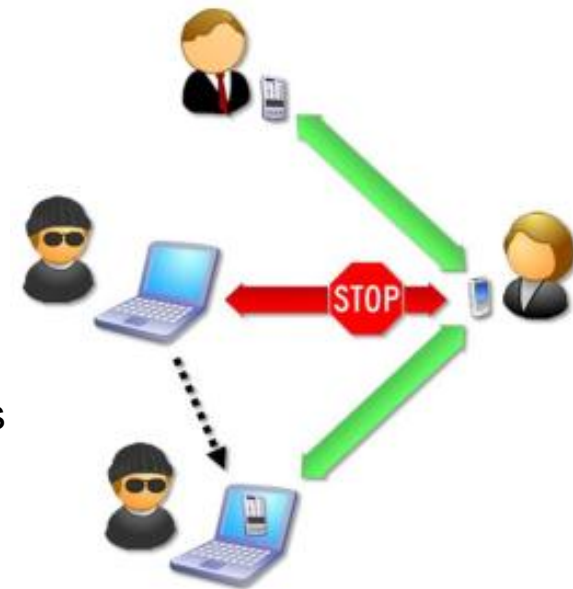
- ¿Qué pasa si un atacante suplanta la dirección BD\_ADDR de un dispositivo de confianza?
- ¿Y si tiene acceso a la clave de enlace de uno de los dispositivos emparejados?

# Ataque Blue MAC Spoofing

Permite suplantar la identidad de un dispositivo de confianza para atacar un teléfono y utilizar sus credenciales para acceder a perfiles que requieren autenticación y/o autorización

## ● Se puede desarrollar en dos niveles

- Suplantación de la dirección BD\_ADDR de un dispositivo de confianza para acceder a perfiles que requieren autorización (Perfil OBEX Object Push)
- Suplantación de la dirección BD\_ADDR y obtención de la clave de enlace generada durante el emparejamiento para acceder a perfiles que requieren autenticación
  - Perfil de Acceso Telefónico a Redes
  - Perfil OBEX File Transfer



Demo



- RFID Tool spanish
  - Ya disponible en WiFiSlax-mini
- Modulo Karma
  - ¿Público?
- Bluetooth Sniffing
  - BTSniff para chipsets CSR
  - ¿BTCrack para Linux?

# Creative Commons Attribution-NoDerivs 2.0

## You are free:

- to copy, distribute, display, and perform this work
- to make commercial use of this work

## Under the following conditions:



**Attribution.** You must give the original author credit.



**No Derivative Works.** You may not alter, transform, or build upon this work.

For any reuse or distribution, you must make clear to others the license terms of this work.

Any of these conditions can be waived if you get permission from the author.

**Your fair use and other rights are in no way affected by the above.**

This work is licensed under the Creative Commons Attribution-NoDerivs License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nd/2.0/> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

Conferencias **FIST**

# WiFiSlax 3.1

**FIST Conference**



**Madrid, Septiembre 2007**

***E-mail: WiFiSlax alt+64 elhacker.net***

[www.wifislax.com](http://www.wifislax.com)

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

[www.fistconference.org](http://www.fistconference.org)