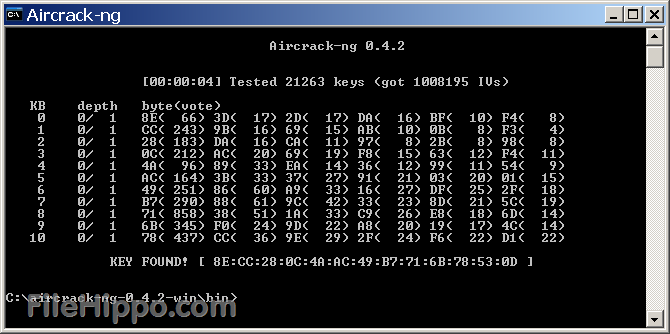
## 2.1 Descripción de Aircrack-NG

Aircrack-ng es un conjunto completo de herramientas para evaluar la seguridad de la red WiFi. Básicamente, se trata de herramientas que analizan los paquetes de red y a partir de estos paquetes y distintos algoritmos, crackean las redes WEP y WPA/WPA2-PSK. Además, contiene otras herramientas de auditoría de redes inalámbricas.



Aircrack-NG esta diseñada para ejecutarse en distribuciones Linux, aunque también tiene una versión para Windows.

En cuanto a las tarjetas de red inalámbricas, la suite de Aircrack-NG esta diseñada para trabajar con tarjetas de red con circuitos integrados Atheros y con circuitos integrados Ralink sin tener que configurar su funcionamiento. Aunque también se a logrado utilizar la suite de Aircrack-NG en otros circuitos, configurando en Linux dicho circuito.

Se enfoca en diferentes áreas de seguridad WiFi:

* Monitoreo: captura de paquetes y exportación de datos a archivos de texto para su posterior procesamiento por parte de herramientas de terceros.
* Ataque: ataques de repetición, desautenticación, puntos de acceso falsos y otros a través de la inyección de paquetes.
* Pruebas: Comprobación de tarjetas WiFi y capacidades del controlador (captura e inyección).
* Cracking: WEP y WPA PSK (WPA 1 y 2).
* Todas las herramientas son de línea de comandos, lo que permite secuencias de comandos pesadas. Muchas GUI se han aprovechado de esta característica. Funciona principalmente Linux, pero también Windows, OS X, FreeBSD, OpenBSD, NetBSD, Solaris e incluso eComStation 2.

Las herramientas que más se utilizan para las auditorias de redes inalámbricas son:

* Airdecap-ng: Descifra archivos de red capturados WEP, WPA WPA2.
* Aircrack-ng: Descifra la clave de los vectores de inicio.
* Airodump-ng: Escanea las redes y captura vectores de inicio).
* Aireplay-ng: Inyecta tráfico para elevar la captura de vectores de inicio.

Las herramientas que incluye la suite de aircrack-NG son:

* Airbase-ng
* Aircrack-ng
* Airdecap-ng
* Airdecloak-ng
* Airdriver-ng
* Aireplay-ng
* Airmon-ng
* Airodump-ng
* Airolib-ng
* Airserv-ng
* Airtun-ng
* Easside-ng
* Packetforge-ng
* Tkiptun-ng
* Wesside-ng
* Airdecloak-ng

## 

## 3.1 Categoría A: Genéricos

### 3.1.1 Criterio A.1: Precio de la herramienta

Nombre del criterio: Precio

Descripción: coste a pagar para utilizar la herramienta.

Tipo de valor: Texto libre

### 3.1.2 Criterio A.2: Licencia

Nombre del criterio: Licencia

Descripción: tipo de licencia de software necesaria para utilizar la herramienta (open source, privativa, etc).

Tipo de valor: Texto libre

### 3.1.3 Criterio A.3: Madurez y versiones del producto

Nombre del criterio: Madurez

Descripción: disponibilidad de versiones que mejoran la aplicación.

Tipo de valor: Texto libre

### 3.1.4 Criterio A.4: Desarrollador

Nombre del criterio: Desarrollador

Descripción: Nombre de la persona, institución o empresa que ha creado la herramienta.

Tipo de valor: Nombre

### 3.1.5 Criterio A.5: Idiomas

Nombre del criterio: Idiomas

Descripción: idiomas en los que la herramienta está disponible.

Tipo de valor: Texto libre

### 3.1.6 Criterio A.6: Popularidad

Nombre del criterio: Popularidad

Descripción: Grado de popularidad que tiene la herramienta dentro del sector de la seguridad informática.

Tipo de valor: Texto libre

### 3.1.7 Criterio A.7: Lenguaje de programación

Nombre del criterio: Lenguaje de programación

Descripción: lenguaje de programación en el que está escrita la herramienta.

Tipo de valor: Texto libre

## 3.2 Categoría B: Funcionalidad

### 3.2.2 Criterio B.1: Exportar resultados

Nombre del criterio: Exportar resultados.

Descripción: es posible exportar los resultados del los ataques en varios formatos.

Tipo de valor: Booleano (SI/NO).

### 3.2.3 Criterio B.2: Integración

Nombre del criterio: Integración con otras aplicaciones.

Descripción: capacidad para integrarse con otras herramientas para mejorar sus funcionalidades.

Tipo de valor: Texto libre.

### 3.2.4 Criterio B.3: Calidad de los resultados

Nombre del criterio: Calidad de los resultados.

Descripción: indicar el nivel de calidad de la información que proporciona la herramienta al dar los resultados.

Tipo de valor: Texto libre.

### 3.2.5 Criterio B.4: Tiempo de ejecución

Nombre del criterio: Tiempo de ejecución.

Descripción: indicar cuanto tiempo tarda en ejecutar los ataques de manera satisfactoria.

Tipo de valor: Texto libre.

### 3.2.6 Criterio B.5: Ataque WEP

Nombre del criterio: Ataque WEP.

Descripción: indicar si la herramienta es capaza de realizar ataques a redes inalámbricas con el cifrado de contraseña WEP.

Tipo de valor: Booleano (SI/NO).

### 3.2.7 Criterio B.8: Ataque WPA

Nombre del criterio: Ataque WPA.

Descripción: indicar si la herramienta es capaza de realizar ataques a redes inalámbricas con el cifrado de contraseña WPA.

Tipo de valor: Booleano (SI/NO).

### 3.2.8 Criterio B.9: Ataque WEP

Nombre del criterio: Ataque WPA 2.

Descripción: indicar si la herramienta es capaza de realizar ataques a redes inalámbricas con el cifrado de contraseña WPA 2.

Tipo de valor: Booleano (SI/NO).

### 3.2.9 Criterio B.10: Número de ataques simultáneos

Nombre del criterio: Número de ataques simultáneos.

Descripción: indicar el número de ataques simultáneos que puede realizar la herramienta.

Tipo de valor: Booleano (SI/NO).