PASSWORD CRACKING TOOLS

AirCrack-NG VS Fern Wifi Wireless Cracker

Contenido

[1. Autores del trabajo, planificación y entrega 3](#_Toc510691139)

[1.1 Autores 3](#_Toc510691140)

[1.2 Planificación 3](#_Toc510691141)

[1.3 Entrega 3](#_Toc510691142)

[2. Descripción de las tecnologías 4](#_Toc510691143)

[2.1 Descripción de Aircrack-NG 4](#_Toc510691144)

[2.2 Descripción de Fern Wifi Cracker 4](#_Toc510691145)

[3. Criterios de comparación 5](#_Toc510691146)

[3.1 Categoría A: Genericos 5](#_Toc510691147)

[3.1.1 Criterio A.1: Nombre 5](#_Toc510691148)

[3.1.2 Criterio A.2: Nombre 6](#_Toc510691149)

[3.1.n Criterio A.n: Nombre 6](#_Toc510691150)

[3.2 Categoría B: Funcionalidad 6](#_Toc510691151)

[3.2.1 Criterio B.1: Nombre 6](#_Toc510691152)

[3.2.2 Criterio B.2: Nombre 6](#_Toc510691153)

[3.2.n Criterio B.n: Nombre 6](#_Toc510691154)

[3.3 Categoría C: Usabilidad 6](#_Toc510691155)

[3.3.1 Criterio Z.1: Nombre 6](#_Toc510691156)

[3.3.2 Criterio Z.2: Nombre 6](#_Toc510691157)

[3.3.n Criterio Z.n: Nombre 6](#_Toc510691158)

[3.4 Categoría D: Soporte 6](#_Toc510691159)

[4. Evaluación de los criterios por tecnología 7](#_Toc510691160)

[4.1 Evaluación de los criterios para Aircrack-NG 7](#_Toc510691161)

[4.2 Evaluación de los criterios para Fern Wifi Cracker 7](#_Toc510691162)

[5. Comparación de las tecnologías 8](#_Toc510691163)

[6. Recomendaciones 10](#_Toc510691164)

[6.1 Situación y escenario 1 10](#_Toc510691165)

[6.1.1 Descripción de la situación 10](#_Toc510691166)

[6.1.2 Recomendación de tecnología a utilizar 10](#_Toc510691167)

[6.2 Situación y escenario 2 10](#_Toc510691168)

[6.2.1 Descripción de la situación 10](#_Toc510691169)

[6.2.2 Recomendación de tecnología a utilizar 10](#_Toc510691170)

[6.3 Situación y escenario 3 10](#_Toc510691171)

[6.4 Situación y escenario 4 10](#_Toc510691172)

[7. Conclusión 11](#_Toc510691173)

# 1. Autores del trabajo, planificación y entrega

## 1.1 Autores

Numero de grupo TG6

Miembros del grupo:

Ernesto Martín Doménech

Jorge La fuente Grande

Tomasz Tomaszewski

Carlos Modesto Pérez

Javier Utande Medina

## 1.2 Planificación

No es posible obtener un enlace a la planificación desde la herramienta GanttPro sin una cuenta Pro.

Debido a eso se ha admitido en la planificación al profesor de la asignatura, se puede revisar la planificación directamente desde la web.

## 1.3 Entrega

En este apartado debe incluirse un enlace (URL) a un repositorio en GitHub o en BitBucket creado para el trabajo.

En dicho repositorio debe encontrarse, al menos los siguientes archivos en la rama máster:

* Trabajo terminado: del trabajo terminado con el nombre TG2\_final.ocx
* Presentación del trabajo: TG2\_final.pptx

Dichos archivos serán los que se tendrán en cuenta para la calificación del trabajo.

Enlace al repositorio de GitHub:

https://github.com/Rijaelto/TG2

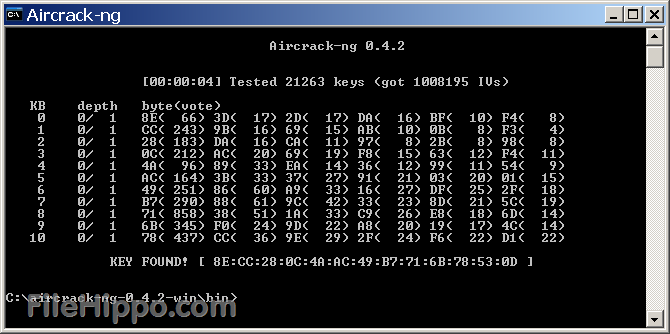
# 2. Descripción de las tecnologías

En los siguientes apartados se debe describir brevemente cada tecnología a comparar.

Se pueden incluir imágenes copiadas y pegadas desde diversas fuentes de información, siempre que debajo de cada una se indique la fuente (al menos la URL).

## 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:

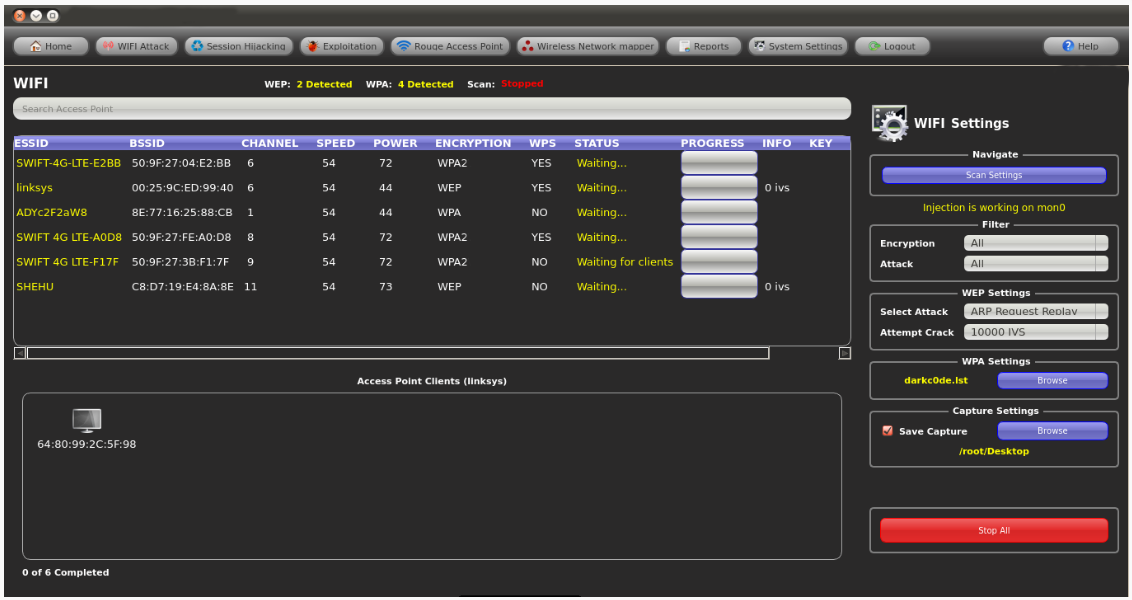
* Airdecap-ng: Descifra archivos de red capturados WEP, WPA WPA2.
* Aircrack-ng: Descifra la clave de los vectores de inicio.
* Airodump-ng: Escanea las redes y captura vectores de inicio).
* Aireplay-ng: Inyecta tráfico para elevar la captura de vectores de inicio.

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

## 2.2 Descripción de Fern Wifi Cracker

Fern Wifi Cracker es una suite de auditoria y ataques de seguridad de redes Wifi escrito en lenguaje de programación Python. El programa es capaz de crackear y recuperar contraseñas de redes wifi del tipo WEP, WPA, WPS.El programa está diseñado y probado para funcionar en el sistema operativo Linux.

El programa cuenta con una interfaz gráfica bastante amigable en la que podemos encontrar todas las funciones de las que consta el software.

Fern Wifi Cracker tiene automatizadas todas las operaciones que hay que hacer para realizar una auditoria Wifi de manera que solo tenemos que seleccionar la red que queremos auditar y marcar las posibles variables que queramos para los resultados de la auditoria y el sistema se encarga de realizar todas las operaciones necesarias y mostrará el resultado final.

# 3. Criterios de comparación

En los sub-apartados de este apartado se deben indicar cada uno de los criterios (también llamados factores, propiedades, características, indicadores, etc.), que se usarán en la comparación.

Los criterios deben organizarse en categorías (al menos 3 categorías). El número de criterios totales no puede ser inferior a 20.

Las categorías dependerán del tipo de tecnología, pueden ser categorías como “General”, “Utilidades”, “Rendimiento”, etc.

Los criterios a definir en cada categoría también dependerán del tipo de tecnologías a comparar. En el siguiente apartado hay algunos ejemplos.

## 3.1 Categoría A: Genericos

### 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 de 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).

## 3.3 Categoría C: Usabilidad

### 3.3.1 Criterio C.1: Instalación

*Nombre del criterio: Instalación*

*Descripción: Dificultad del proceso de instalación.*

*Tipo de valor: Texto libre.*

### 3.3.2 Criterio C.2: Idiomas

*Nombre del criterio:* Idiomas

*Descripción: Idiomas disponibles.*

*Tipo de valor: Texto libre.*

### 3.3.3 Criterio C.3: Interfaz

*Nombre del criterio:* Interfaz

*Descripción: Indica si existe interfaz de usuario gráfica y si esta interfaz de usuario es fácil de usar.*

*Tipo de valor: Texto libre.*

### 3.3.4 Criterio C.4: Dificultad

*Nombre del criterio: Dificultad*

*Descripción: Tiempo aproximado que se tarda en aprender a usar la aplicación.*

*Tipo de valor: Horas*

### 3.3.5 Criterio C.5: Windows

*Nombre del criterio: Disponibilidad en Windows*

*Descripción: Indica la disponibilidad de la aplicación el sistema operativo.*

*Tipo de valor: Positivo o negativo.*

### 3.3.6 Criterio C.6: Linux

*Nombre del criterio: Disponibilidad en Linux*

*Descripción: Indica la disponibilidad de la aplicación el sistema operativo.*

*Tipo de valor: Positivo o negativo.*

### 3.3.7 Criterio C.7: MAC

*Nombre del criterio: Disponibilidad en MAC*

*Descripción: Indica la disponibilidad de la aplicación el sistema operativo.*

*Tipo de valor: Positivo o negativo.*

### 3.3.8 Criterio C.8: Tiempo en estar operativa

*Nombre del criterio: Tiempo que tarda en iniciar la aplicación*

*Descripción: Indica el tiempo que tarda en iniciar la aplicación sobre un sistema ya iniciado.*

*Tipo de valor: Positivo o negativo.*

### 3.3.9 Criterio C.9: Requisitos mínimos

*Nombre del criterio: Requisitos*

*Descripción: Requisitos mínimos de hardware para utilizar la aplicación*

*Tipo de valor: Texto libre.*

## 3.4 Categoría D: Soporte

### 3.4.1 Criterio D.1: Soporte técnico

*Nombre del criterio: Soporte técnico*

*Descripción: Ayudas y soporte técnico disponible para uso de la aplicación o para la consulta sobre errores.*

*Tipo de valor: Texto libre.*

### 3.4.2 Criterio D.2: Manual

*Nombre del criterio: Manual*

*Descripción: Documento técnico oficial de guía de uso e instalación de la herramienta*

*Tipo de valor: Texto libre.*

### 3.4.3 Criterio D.3: FAQ

*Nombre del criterio: FAQ*

*Descripción: Existencia de una página o método de consulta de preguntas frecuentes.*

*Tipo de valor: Valor positivo o negativo.*

### 3.4.4 Criterio D.4: Garantía

*Nombre del criterio: Garantía de la aplicación.*

*Descripción: Indica si existe o no garantía para el uso de la aplicación y cual es.*

*Tipo de valor: Texto libre.*

### 3.4.5 Criterio D.5: Información

*Nombre del criterio: Información disponible.*

*Descripción: Indica la cantidad de información disponible para la aplicación.*

*Tipo de valor: Texto libre.*

# 4. Evaluación de los criterios por tecnología

## 4.1 Evaluación de los criterios para Aircrack-NG

|  |  |
| --- | --- |
| CRITERIOS | EVALUACIÓN |
| Criterio A.1: Precio de la herramienta | Gratuita |
| Criterio A.2: Licencia | Open Source, [GPL v2](https://www.gnu.org/licenses/gpl-2.0.html) ([Local copy](http://www.aircrack-ng.org/LICENSE)), [BSD 3 Clause](https://opensource.org/licenses/BSD-3-Clause), [OpenSSL](http://www.aircrack-ng.org/LICENSE.OpenSSL) |
| Criterio A.3: Madurez y Versiones | [Versión 1.2 RC 5](https://download.aircrack-ng.org/aircrack-ng-1.2-rc5.tar.gz), 3 abril 2018 |
| Criterio A.4: Desarrollador | Thomas d’Otreppe |
| Criterio A.5: Idioma | Inglés |
| Criterio A.6: Popularidad |  |
| Criterio A.7: Lenguaje de programación | Lenguaje ensamblador y C |
| Criterio B.1: Exportar resultados | Si |
| Criterio B.2: Integración | Kali Linux |
| Criterio B.3: Calidad de los resultados | Tiene un interfaz gráfico bastante intuitivo con facilidad de ver los resultados |
| Criterio B.4: Tiempo de ejecución | En función del tipo de contraseña a explotar y de la librería de datos disponible |
| Criterio B.5: Ataque WEP | Si |
| Criterio B.6: Ataque WPA | Si |
| Criterio B.7: Ataque WPA2 | Si |
| Criterio B.8: Ataques simultáneos | Si |
| Criterio C.1: Instalación | Fácil y rápida instalación |
| Criterio C.2: Idiomas | Inglés |
| Criterio C.3: Interfaz | Si, línea de comandos |
| Criterio C.4: Dificultad | 4 horas |
| Criterio C.5: Windows | Si |
| Criterio C.6: Linux | Si |
| Criterio C.7: MAC | Si |
| Criterio C.8: Tiempo en estar operativa | 40 segundos |
| Criterio C.9: Requisitos mínimos |  |
| Criterio D.1: Soporte técnico | Si, existe en su web el llamado “wiki”, donde se encuentra gran cantidad de información para resolver errores |
| Criterio D.2: Manual | Hay manuales oficiales en la pagina web oficil de la herramienta |
| Criterio D.3: FAQ | Si |
| Criterio D.4: Garantía |  |
| Criterio D.5: Información | Existe una gran cantidad de información para utilizar la herramienta |

* Criterio A.2: Licencia

Imagen que contiene captura de pantalla

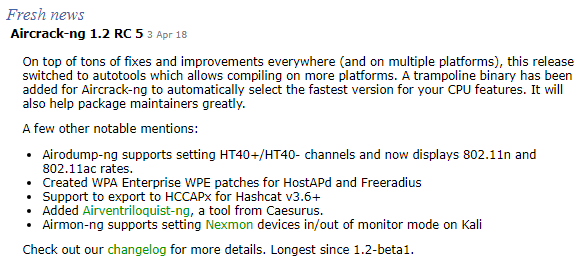
Descripción generada con confianza muy alta

* Criterio A.3: Madurez y Versiones

Imagen que contiene captura de pantalla

Descripción generada con confianza muy alta

Versión mas actual:



En la página web oficial <http://www.aircrack-ng.org/install.html> encontramos diversos tutoriales sobre la instalación de aircrack-ng.

* Criterio C.1: Instalación

Imagen que contiene captura de pantalla

Descripción generada con confianza muy alta

A continuación, se muestra una captura de pantalla de la página web oficial <http://www.aircrack-ng.org/support.html> y <http://www.aircrack-ng.org/documentation.html> donde se pueden encontrar los siguientes criterios:

* Criterio D.1: Soporte técnico
* Criterio D.2: Manual
* Criterio D.3: FAQ
* Criterio D.5: Información

Imagen que contiene captura de pantalla

Descripción generada con confianza muy alta

## 4.2 Evaluación de los criterios para Fern Wifi Cracker

**Imagen que contiene captura de pantalla

Descripción generada con confianza muy alta**

## 4.2 Evaluación de los criterios para Fern Wifi Cracker

|  |  |
| --- | --- |
| CRITERIOS | EVALUACIÓN |
| Criterio A.1: Precio de la herramienta | Desde 0$ hasta 160$ |
| Criterio A.2: Licencia | Open Source |
| Criterio A.3: Madurez y Versiones | Version 2.2 |
| Criterio A.4: Desarrollador | Savio-code |
| Criterio A.5: Idioma | Ingles |
| Criterio A.6: Popularidad | Software Reciente con 1336744 usuarios |
| Criterio A.7: Lenguaje de programación | Python |
| Criterio A.8: Instalación | Funciona en sistema Linux |
| Criterio B.1: Interfaz | SI |
| Criterio B.2: Exportar resultados | SI |
| Criterio B.3: Integración | Es una herramienta independiente que no tiene hasta el momento integración dentro de otras herramientas |
| Criterio B.4: Calidad de los resultados | Tiene un interfaz gráfico bastante intuitivo con facilidad de ver los resultados |
| Criterio B.5: Tiempo de ejecucion | En función de el tipo de contraseña a explotar y de la librería de datos disponible |
| Criterio B.6: Ataque WEP | SI |
| Criterio B.7: Ataque WPA | SI |
| Criterio B.8: Ataque WPA2 | SI |
| Criterio B.9: Ataques simultaneos | NO |
| Criterio C.1: Instalación | Fácil y rápida instalación |
| Criterio C.2: Idiomas | Inglés |
| Criterio C.3: Interfaz | Si, interfaz grafica |
| Criterio C.4: Dificultad | 4 horas |
| Criterio C.5: Windows | No |
| Criterio C.6: Linux | Si |
| Criterio C.7: MAC | No |
| Criterio C.8: Tiempo en estar operativa | 40 segundos |
| Criterio C.9: Requisitos mínimos |  |
| Criterio D.1: Soporte técnico | Si, tienen un email de soporte con servicio 24/7 |
| Criterio D.2: Manual | Hay manuales oficiales en la página web oficial de la herramienta |
| Criterio D.3: FAQ | Si |
| Criterio D.4: Garantía |  |
| Criterio D.5: Información | La información principal se encuentra en la web de la compañía. |

# 5. Comparación de las tecnologías

Debe incluir al menos una tabla resumen, en sección de página horizontal, cruzando los criterios y los valores de cada tecnología. Con una columna de comentarios sobre la comparación

Esta tabla anterior es obligatoria y deben completarla los autores del trabajo, aunque se pueden incluir otros gráficos o tablas complementarias copiadas y pegadas desde diversas fuentes de información, siempre que debajo de cada uno se indique la fuente (al menos la URL).

|  |  |  |  |
| --- | --- | --- | --- |
| CRITERIOS | TECNOLOGÍA A | TECNOLOGÍA B | COMENTARIOS |
| A.1 Precio de la Herramienta | Aircrack-NG | Fern Wifi Cracker | Las dos tecnologías se pueden conseguir gratuitamente |
| A.2 Licencia | Aircrack-NG | Fern Wifi Cracker | Las dos tienen la licencia Open Source aunque la tecnología A tiene mas |
| A.3 Madurez y Versiones | Aircrack-NG | Fern Wifi Cracker | La tecnología B tiene más versiones |
| A.4 Desarrollador | Aircrack-NG | Fern Wifi Cracker | Han sido desarrollados por dos individuos concretos |
| A.5 Idioma | Aircrack-NG | Fern Wifi Cracker | Es el mismo |
| A.6 Popularidad | Aircrack-NG | Fern Wifi Cracker | La tecnología A es más popular porque lleva mas tiempo en el mercado |
| A.7 Lenguaje de programación | Aircrack-NG | Fern Wifi Cracker | La tecnología B a sido desarrollada con un lenguajes mas potente y actual como es Python. |
| A.8 Instalación | Aircrack-NG | Fern Wifi Cracker | Funciona en sistemas Linux |
| B.1 Exportar resultados | Aircrack-NG | Fern Wifi Cracker | Las dos lo permiten, aunque la tecnología B va todo por interfaz |
| B.2 Integración | Aircrack-NG | Fern Wifi Cracker | La tecnología A esta integrada en Kali Linux y la tecnología B esta deforma independiente |
| B.3 Calidad de los resultados | Aircrack-NG | Fern Wifi Cracker | Las dos tienen una interfaz que permite ver fácilmente los resultados |
| B.4 Tiempo de ejecución. | Aircrack-NG | Fern Wifi Cracker | Dependerá de la contraseña y del tipo de librería que dispondremos |
| B.5 Ataque WEP | Aircrack-NG | Fern Wifi Cracker | Son iguales |
| B.6 Ataque WPA | Aircrack-NG | Fern Wifi Cracker | Son iguales |
| B.7 Ataque WPA2 | Aircrack-NG | Fern Wifi Cracker | Son iguales |
| B.8 Ataques simultáneos | Aircrack-NG | Fern Wifi Cracker | La tecnología A si los tiene la tecnología B no |
| C.1 Instalación | Aircrack-NG | Fern Wifi Cracker | Las dos son fáciles de instalar |
| C.2 Idiomas | Aircrack-NG | Fern Wifi Cracker | Las dos son en ingles |

|  |  |  |  |
| --- | --- | --- | --- |
| C.3 Interfaz | Aircrack-NG | Fern Wifi Cracker | Las dos disponen de interfaz la tecnología A de comandos y la tecnología B grafica |
| C.4 Dificultad | Aircrack-NG | Fern Wifi Cracker | Tienen la misma dificultad |
| C.5 Windows | Aircrack-NG | Fern Wifi Cracker | La tecnología B no está para Windows |
| C.6 Linux | Aircrack-NG | Fern Wifi Cracker | Son iguales |
| C.7 MAC | Aircrack-NG | Fern Wifi Cracker | La tecnología B no está disponible para MAC |
| C.8 tiempo en estar operativo | Aircrack-NG | Fern Wifi Cracker | Son iguales o las diferencias no son apreciables |
| C.9 Requisitos mínimos | Aircrack-NG | Fern Wifi Cracker | La tecnología B tiene más requisitos que la tecnología A para funcionar |
| D.1 Soporte Técnico | Aircrack-NG | Fern Wifi Cracker | Las dos tienen |
| D.2 Manual | Aircrack-NG | Fern Wifi Cracker | Las dos tienen |

|  |  |  |  |
| --- | --- | --- | --- |
| D.3 FAQ | Aircrack-NG | Fern Wifi Cracker | Las dos tienen |
| D.4 Garantía | Aircrack-NG | Fern Wifi Cracker |  |
| D.5 Informacion | Aircrack-NG | Fern Wifi Cracker | Hay más información de la tecnología A que de la tecnología B |

# 6. Recomendaciones

Deben platearse posibles situaciones de uso, y recomendar justificadamente una u otra tecnología en función de la situación. Al menos 2 situaciones diferentes.

## 6.1 Situación y escenario 1

### 6.1.1 Descripción de la situación

*La residencia de estudiantes de la Universidad de Alcalá está experimentando una serie de problemas en su conexión WiFi, se sabe que tienen una clave WEP y sospechan que gente externa a la residencia acude al lugar para aprovecharse de su Wi Fi. Quieren que se haga un estudio para saber si el sistema de cifrado WEP es vulnerable y otros usuarios acceden a su red.*

### 6.1.2 Recomendación de tecnología a utilizar

|  |  |  |
| --- | --- | --- |
| **Criterios relevantes para la decisión** | **Ventajas tecnología 1** Aircrack-ng | **Ventajas tecnología 2** Fern WiFi Cracker |
| Criterio B.2: Integración | La herramienta se encuentra integrada en Kali Linux, pero puede instalarse la suite de aircrack-ng de forma independiente. | Es una herramienta independiente que no tiene hasta el momento integración dentro de otras herramientas. |
| Criterio B.1: Exportar resultados | Los resultados pueden ser exportados en diferentes formatos para su posterior análisis. | Los resultados pueden ser exportados en diferentes formatos para su posterior análisis. |
| Criterio B.4: Tiempo de ejecución | En función del tipo de contraseña a explotar y de la librería de datos disponible | Según el tipo de contraseña a explotar y de la librería de datos disponible |
| Criterio B.5: Ataque WEP | Es capaz de atacar contraseñas con cifrado WEP | Permite el ataque a contraseñas WEP |

Efectivamente, los problemas de conexión experimentados se deben a que el sistema de cifrado WEP que utilizan es muy débil. Cualquier persona con conocimientos en informática y con el software adecuado puede violar la seguridad de la contraseña.

Este problema, probablemente se debe a que las personas responsables de la instalación de los puntos de acceso dejaron la contraseña por defecto que estos tenían. El cifrado WEP puede disuadir del uso sin autorización de una red privada, pero sin proporcionar verdadera protección.

Para obtener la clave WEP de un punto de acceso, necesitamos muchos vectores de inicialización (IVs). El tráfico de red habitual no genera de forma rápida suficientes IVs. Teóricamente, si tenemos paciencia, podemos conseguir suficientes IVs para crackear la clave WEP únicamente capturando el tráfico de la red. Pero como la mayoría de nosotros no tenemos paciencia, usamos una técnica de inyección para aumentar la velocidad del proceso de captura. La inyección implica que se envíen al punto de acceso (AP) paquetes de forma continua y muy rápido. Esto permite capturar un gran número de IVs en un periodo corto de tiempo

Recomendamos el uso de la herramienta Aircrack-ng simplemente por el hecho de que existe un mayor volumen de documentación y tutoriales sobre como violar la seguridad de contraseñas WEP, las dos herramientas son igual de efectivas a la hora de explotar vulnerabilidades de este sistema de cifrado.

## 6.2 Situación y escenario 2

### 6.2.1 Descripción de la situación

Un compañero de clase sospecha que algún puede estar conectado a su WiFi, nos comenta que su contraseña está protegida con el sistema de cifrado WPA2. Nos comenta que quiere poner a prueba la seguridad de su contraseña y que quiere hacerlo el mismo, pero nos dice que su PC esta averiado y que el único equipo del que dispone en su casa es una Raspberry pi 3.

### 6.2.2 Recomendación de tecnología a utilizar

|  |  |  |
| --- | --- | --- |
| **Criterios relevantes para la decisión** | **Ventajas tecnología 1** Aircrack-ng | **Ventajas tecnología 2** Fern WiFi Cracker |
| Criterio B.2: Integración | La herramienta se encuentra integrada en Kali Linux, pero puede instalarse la suite de aircrack-ng de forma independiente. | Es una herramienta independiente que no tiene hasta el momento integración dentro de otras herramientas. |
| Criterio B.1: Exportar resultados | Los resultados pueden ser exportados en diferentes formatos para su posterior análisis. | Los resultados pueden ser exportados en diferentes formatos para su posterior análisis. |
| Criterio B.4: Tiempo de ejecución | En función del tipo de contraseña a explotar y de la librería de datos disponible | Según el tipo de contraseña a explotar y de la librería de datos disponible |
| Criterio B.7: Ataque WPA2 | Es capaz de atacar contraseñas con cifrado WPA2. | Permite el ataque a contraseñas WPA2. |
| Criterio C.6: Linux | Puede instalarse en sistemas operativos Linux. | Permite su instalación en sistemas operativos Linux. |
|  |  |  |

Aunque el sistema de cifrado WPA2 es el más seguro, las sospechas de nuestro amigo pueden ser ciertas, debido a que el investigador de seguridad Mathy Vanhoef vuelve no obstante a demostrar que nuestras conexiones WiFi siguen sin estar protegidas aun cuando usemos el protocolo WPA2. Los llamados KRACKs (Key Reinstallation AttaCKs) permiten que los atacantes puedan "acceder a la información que hasta ahora se asumía que estaba cifrada de forma segura".

La debilidad en el sistema WPA2-PSK es que la contraseña cifrada es compartida en lo que se conoce como el 4-vías. Cuando un cliente se autentica en el punto de acceso (AP), el cliente y el AP pasan por un proceso de 4 pasos para autenticar al usuario a la AP. Si somos capaces de agarrar la contraseña en ese momento, entonces podemos tratar de descifrarlo.

Para saber si realmente la contraseña de nuestro amigo es segura le recomendamos utilizar Aircrack-ng por los siguientes motivos. Él únicamente dispone de una Raspberry pi 3, para este tipo de dispositivos existe una distribución de Kali Linux el cual trae integrada la suite de Aircrack-ng. Simplemente tendrá que descargar la iso de Kali Linux para Raspberry e instalarla.

## 6.3 Situación y escenario 3

### 6.3.1 Descripción de la situación

Una empresa que tiene un local de atención al público quiere ofrecer una red wifi para clientes y aparte tener una red wifi propia para sus sistemas y el router que tienen para esta red puede configurarse una contraseña wifi WPA que es la que viene por defecto en el aparato. Se hace un análisis de seguridad de la contraseña que viene preconfigurada en el router para ver si es óptima o es preferible crear una nueva.

### 6.3.2 Recomendación de tecnología a utilizar

|  |  |  |
| --- | --- | --- |
| **Criterios relevantes para la decisión** | **Ventajas tecnología 1** Aircrack-ng | **Ventajas tecnología 2** Fern WiFi Cracker |
| Criterio B.2: Integración | La herramienta se encuentra integrada en Kali Linux, pero puede instalarse la suite de aircrack-ng de forma independiente. | Es una herramienta independiente que no tiene hasta el momento integración dentro de otras herramientas. |
| Criterio B.1: Exportar resultados | Los resultados pueden ser exportados en diferentes formatos para su posterior análisis. | Los resultados pueden ser exportados en diferentes formatos para su posterior análisis. |
| Criterio B.4: Tiempo de ejecución | En función del tipo de contraseña a explotar y de la librería de datos disponible | Según el tipo de contraseña a explotar y de la librería de datos disponible |
| Criterio B.7: Ataque WPA | Es capaz de atacar contraseñas con cifrado WPA. | Permite el ataque a contraseñas WPA. |
| Criterio C.6: Linux | Puede instalarse en sistemas operativos Linux. | Permite su instalación en sistemas operativos Linux. |

El cifrado de contraseñas WPA no es el más seguro que exista en la actualidad ya que existe el cifrado WPA2 pero ya que es del que se dispone por el router a usar.

Para comprobar la seguridad de la red al no ser un usuario muy avanzado de informática le recomendamos descargar el programa fern Wifi Cracker que dispone de una versión gratuita de prueba con la cual gracias a su interfaz gráfica y su uso sencillo podrá comprobar la seguridad de la contraseña.

## 6.4 Situación y escenario 4

|  |  |  |
| --- | --- | --- |
| **Criterios relevantes para la decisión** | **Ventajas tecnología 1** Aircrack-ng | **Ventajas tecnología 2** Fern WiFi Cracker |
| Criterio B.2: Integración | La herramienta se encuentra integrada en Kali Linux, pero puede instalarse la suite de aircrack-ng de forma independiente. | Es una herramienta independiente que no tiene hasta el momento integración dentro de otras herramientas. |
| Criterio B.1: Exportar resultados | Los resultados pueden ser exportados en diferentes formatos para su posterior análisis. | Los resultados pueden ser exportados en diferentes formatos para su posterior análisis. |
| Criterio B.4: Tiempo de ejecución | En función del tipo de contraseña a explotar y de la librería de datos disponible | Según el tipo de contraseña a explotar y de la librería de datos disponible |
| Criterio C.6: Linux | Puede instalarse en sistemas operativos Linux | Permite su instalación en sistemas operativos Linux |

La situación que hemos elegido es un ataque ARP Spoofing el cual se desarrolla de la siguiente manera.

La persona que quiera atacarnos enviara mensajes falsificados ARP a un determinada LAN, el objetivo es que el atacante vincule su dirección MAC con una dirección IP “oficial” de la red que está atacando, si el atacante consigue vincular su MAC a la dirección IP, este podrá recibir cualquier mensaje o podrá filtrar el tráfico de esa red o podrá acceder a cualquier información que se pueda acceder con esa IP, modificar cualquier información, retener cualquier información.

Tras presentar la situación la herramienta que recomiendo para realizar esta situación es Aircrack-NG, debido a sus funcionalidades dado que con ella podemos localizar nuestra MAC descubrir la contraseña de la wifi que vamos a utilizar y así poder infectar

---------------------------

(Hay que cumplir la estructura básica indicada de secciones. Pero si se desea se pueden añadir otras secciones como anexos. Por ejemplo, alguna encuesta de opinión realizada sobre las tecnologías, etc.)

# 7. Conclusión