Password cracking tools

AirCrack-NG VS Fern Wifi Wireless Cracker

Contenido

[1. Autores del trabajo, planificación y entrega 3](#_Toc509250568)

[1.1 Autores 3](#_Toc509250569)

[1.2 Planificación 3](#_Toc509250570)

[1.3 Entrega 3](#_Toc509250571)

[2. Descripción de las password cracking tools 3](#_Toc509250572)

[3. Fuentes de información (documentos) 4](#_Toc509250573)

[3.1 Fuentes generales 4](#_Toc509250574)

[3.1.1 Documentación oficial Kali Linux 4](#_Toc509250575)

[3.1.2 La Comunidad DragonJAR 4](#_Toc509250576)

[3.1.3 Securitybydefault 4](#_Toc509250577)

[3.1.4 Tesis del autor Chrysanthou Yiannis 5](#_Toc509250578)

[3.1.5 Ponencia de Passwordscon 5](#_Toc509250579)

[3.2 Fuentes sobre Aircrack-NG 5](#_Toc509250580)

[3.2.1 Página oficial de Aircrack 5](#_Toc509250581)

[3.2.2 Guía Xataka.com 5](#_Toc509250582)

[3.2.3 Guía Aircrack de universidad central de Grecia 5](#_Toc509250583)

[3.2.4 Tipos de ataques de la universidad de Alabama 5](#_Toc509250584)

[3.2.5 Documento sobre exploiting 6](#_Toc509250585)

[3.2.6 Libro gratuito 6](#_Toc509250586)

[3.3 Fuentes sobre Fern Wifi Wireless Cracker 6](#_Toc509250587)

[3.3.1 Pagina del desarrollador 6](#_Toc509250588)

[3.3.2 Herramientas de kali 6](#_Toc509250589)

[3.3.3 Videos de demostración 7](#_Toc509250590)

[4. Fuentes de información (cursos no gratuitos) 7](#_Toc509250591)

[4.1 Cursos no gratuitos generales 7](#_Toc509250592)

[4.1.1 Curso de verano de la Universidad de Alcalá 7](#_Toc509250593)

[4.1.2 The security sentinel 7](#_Toc509250594)

[4.1.3 Hacking ético en udemy 8](#_Toc509250595)

[4.1.4 Máster en ciberseguridad imf-formación 8](#_Toc509250596)

[4.1.5 Hacking ético akademus 8](#_Toc509250597)

[4.1.6 Hacking ético Securizame 9](#_Toc509250598)

[4.2 Cursos no gratuitos sobre Aircrack-NG 9](#_Toc509250599)

[4.2.1 Curso de dragonjar 9](#_Toc509250600)

[4.2.2 Curso de pentestmag 10](#_Toc509250601)

[4.2.3 Curso de Digital Tech Institute 10](#_Toc509250602)

[4.2.4 Curso de backtrackacademy 10](#_Toc509250603)

[4.3 Cursos no gratuitos sobre Fern Wifi Wireless Cracker 10](#_Toc509250604)

[4.3.1 Curso de Udemy por MBPSec 10](#_Toc509250605)

[4.3.2 Curso de Udemy de Eduardo Arriols Nuñez 10](#_Toc509250606)

[5. Fuentes de información (cursos gratuitos) 10](#_Toc509250607)

[5.1 Cursos gratuitos generalas 10](#_Toc509250608)

[5.1.1 Seguridad informática Miriadax 10](#_Toc509250609)

[5.1.2 Curso de seguridad esetec 11](#_Toc509250610)

[5.1.3 Curso de craking de Ricardo Narvaja 11](#_Toc509250611)

[5.1.4 Curso hacking edutin 11](#_Toc509250612)

[5.2 Cursos gratuitos sobre Aircrack-NG 11](#_Toc509250613)

[5.2.1 Curso de dragonjar 11](#_Toc509250614)

[5.2.2 Tutoriales de Aircrack 12](#_Toc509250615)

[5.2.3 Curso de pkred 12](#_Toc509250616)

[5.2.4 Curso de Marcos Mendoza 12](#_Toc509250617)

[5.3 Cursos gratuitos sobre Fern Wifi Wireless Cracker 12](#_Toc509250618)

[5.3.1 Blog de r4z0r 12](#_Toc509250619)

[5.3.2 Tutorial de hackthis 12](#_Toc509250620)

[6. Ayudas económicas para estudiar las tecnologías 13](#_Toc509250621)

[7. Recursos para implementar las tecnologías 15](#_Toc509250622)

[7.1 Recursos para implementar Aircrack 15](#_Toc509250623)

[7.1.1 Recursos gratuitos para implementar Aircrack 15](#_Toc509250624)

[7.1.2 Recursos no gratuitos para implementar Aircrack 15](#_Toc509250625)

[7.2 Recursos para implementar Fern WiFi Wireless Cracker 15](#_Toc509250626)

[7.2.1 Recursos gratuitos para implementar Fern WiFi Wireless Cracker 15](#_Toc509250627)

[7.2.2 Recursos no gratuitos para implementar Fern WiFi Wireless Cracker 15](#_Toc509250628)

[8. Conclusiones 16](#_Toc509250629)

# 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 TG1\_final.ocx
* Presentación del trabajo: TG1\_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/TG1>

# 2. Descripción de las password cracking tools

Una password (contraseña) es un frase, palabra o código secreto que permite validar un proceso de autenticación. Su secretismo es un método de protección, únicamente los conocedores de la contraseña pueden acceder a una información determinada u a un recurso.

El uso de contraseñas se remonta a la antigüedad, cuando únicamente aquellos que conocían el “santo y seña” podían acceder a determinados lugares y ya en la antigüedad se buscaba la manera de acabar con esa protección, escuchando atentamente escondido tras un arbusto, intentando leer los labios de quien pronunciaba la contraseña o con métodos un tanto más dolorosos.

El avance tecnológico no ha cambiado está situación, únicamente la ha modernizado, las contraseñas pueden ser ahora terriblemente complejas y los recursos para descubrirlas se han multiplicado.

Uno de esto recursos son las herramientas de crackeo de contraseñas. El proceso de crackeo consiste en descifrar, ya sea adivinando, recuperando o accediendo de alguna manera a la clave que se necesita, la dificultad para hacer esto será una de las medidas de la seguridad de un sistema.

En este trabajo estudiaremos dos herramientas de crackeo que deberían permitirnos acceder, por ejemplo, a redes WLAN con seguridad WEP. Analizaremos la información disponible sobre ellas, tanto gratuita como de pago y las ayudas disponibles para su estudio.

# 3. Fuentes de información (documentos)

En los sub-apartados de este apartado se deben indicar documentos de interés para aprender sobre el tipo de tecnología en general, y sobre cada una de las tecnologías elegidas.

Sobre cada documento se debe

## 3.1 Fuentes generales

### 3.1.1 Documentación oficial Kali Linux

En la página web <https://docs.kali.org/> encontramos la documentación oficial sobre Kali Linux. Se trata de una distribución GNU/Linux con más de 300 herramientas y aplicaciones relacionadas con la seguridad informática, destacando algunas tan conocidas como *Nmap*, que permite escanear los puertos de un sistema, el crackeador de contraseñas *John the Ripper* o la suite *Aircrack-ng* para comprobar la seguridad de las redes inalámbricas.

### 3.1.2 La Comunidad DragonJAR

En la página web <https://www.dragonjar.org/> ofrecen gran cantidad de contenido sobre seguridad informática, tutoriales, formación, foros, etc. La Comunidad DragonJAR, una de las comunidades de habla hispana referentes en el área de seguridad informática, y que en más de 15 años se ha caracterizado por ser el semillero virtual para quienes hoy son grandes profesionales en el ámbito de la seguridad informática, tanto en Colombia cómo en Latinoamérica.

Escribiendo la palabra *passwords* en su buscador nos aparecen varios enlaces a posts relacionados con el cracking de contraseñas.

### 3.1.3 Securitybydefault

<http://www.securitybydefault.com/> se trata de un blog donde se habla íntegramente sobre seguridad informática, un espacio donde profesionales comparten experiencias y hablan de los aspectos técnicos relacionados con la seguridad informática.

### 3.1.4 Tesis del autor Chrysanthou Yiannis

En el siguiente enlace <https://www.ma.rhul.ac.uk/static/techrep/2013/MA-2013-07.pdf> encontramos una tesis del autor Chrysanthou Yiannis de la Royal Holloway University of London, donde se explican las formas más populares de crackeo de contraseñas, además de desarrollar una técnica propia del autor.

### 3.1.5 Ponencia de Passwordscon

<https://www.youtube.com/watch?v=xhz_w_iZtVE>

En este enlace accedemos a una ponencia de Passwordscon in Las Vegas, donde vemos cómo las matemáticas y la estadística pueden ayudar al crackeo de contraseñas. Se explica como ejemplo la técnica de Markov.

## 3.2 Fuentes sobre Aircrack-NG

### 3.2.1 Página oficial de Aircrack

Página web oficial de la herramienta Aircrack-NG. En su página web oficial, se ofrece todo tipo de documentación, tutoriales, videos, una wiki, el código fuente de la herramienta en github y mucha más información sobre la suite de Aircrack-NG.

Enlace: <https://www.aircrack-ng.org/documentation.html>

### 3.2.2 Guía Xataka.com

La pagina web “Xataka.com” ofrece una guía de cómo usar la herramienta Aircrack-NG, con muchos detalles técnicos de lo que realmente hace la herramienta.

Enlace: <https://www.xataka.com/seguridad/caos-en-la-seguridad-wifi-un-repaso-a-las-vulnerabilidades-de-wep-wap-y-wap2>

### 3.2.3 Guía Aircrack de universidad central de Grecia

Es un documento PDF en el que varios profesores de la universidad central de Grecia explican los distintos protocolos de comunicaciones que existen en las redes de área local (WLAN) y como utilizar la herramienta Aicrack-NG para realizar ataques y explicar cómo funcionan dichos ataques.

Enlace: <https://pdfs.semanticscholar.org/7818/0b3c504fba41a000ac83c918c089c38f2eaf.pdf>

### 3.2.4 Tipos de ataques de la universidad de Alabama

Es un documento PDF en el que varios profesores de la universidad de Alabama en Huntsville y Frederick T. Sheldon del Oak Ridge National Laboratory, han escrito sobre los diferentes tipos de ataques que se pueden realizar a las redes Wifi de área local y como la herramienta Aircrack-NG dispone de los mecanismos para llevarlos a cabo.

Enlace: <http://eslared.net/walcs/walc2012/material/track4/Wireless/06193090.pdf>

### 3.2.5 Documento sobre exploiting

Es un documento PDF, el cual pues expuesto en el International Journal of Advanced Research in Computer Engineering & Technology, en el que se exponen varias manera de hacer expoiting con la herramienta Aircrack-NG en redes wifi con el sistema WPA (Wi-Fi Protected Access).

Enlace: <https://www.researchgate.net/publication/231178393_WPA_Exploitation_In_The_World_Of_Wireless_Network?enrichId=rgreq-bb85f6836a0a51094f3b29263d45eca1-XXX&enrichSource=Y292ZXJQYWdlOzIzMTE3ODM5MztBUzoxMDIwODM1MDQxMTU3MjFAMTQwMTM1MDAxMjk2OQ%3D%3D&el=1_x_3&_esc=publicationCoverPdf>

### 3.2.6 Libro gratuito

Esta fuente es un documento PDF que podría dar apoyo a un curso de seguridad informática básica, en el que se explican muchos conceptos de seguridad. Entre estos conceptos, en el capítulo 8 “Ataques y contramedidas” hay un apartado dedicado a “Ataques Wi-Fi: Aircrack-NG” en el que se enseña cómo utilizar la herramienta Aircrack-NG.

Enlace: <https://s3.amazonaws.com/academia.edu.documents/34758985/Seguridad_Informatica_McGraw-Hill_2013_-_www.FreeLibros.me_-_copia.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1521495088&Signature=MACFiLStHxsHsgKxftnPnEXTe3A%3D&response-content-disposition=inline%3B%20filename%3DSeguridad_Informatica_Mc_Graw-Hill_2013.pdf>

## 3.3 Fuentes sobre Fern Wifi Wireless Cracker

### 3.3.1 Pagina del desarrollador

<https://github.com/savio-code/fern-wifi-cracker>

Esta es la página principal del desarrollador de la aplicación y se trata de un repositorio del que podemos descargar la aplicación asi como una presentación de la misma indicando sus funcionalidades.

### 3.3.2 Herramientas de kali

<https://tools.kali.org/wireless-attacks/fern-wifi-cracker>

En el sistema operativo Kali Linux la aplicación viene ya preinstalada y aquí podemos encontrar una descripción de todos los tipos de contraseñas que puede crackear, así como la llamada que se ha de hacer en el sistema para abrir la aplicación.

### 3.3.3 Videos de demostración

<https://n0where.net/fern-wifi-cracker>

En esta página podemos ver una breve descripción de la aplicación y unos videos demostrativos del uso de esta.

# 4. Fuentes de información (cursos no gratuitos)

## 4.1 Cursos no gratuitos generales

### 4.1.1 Curso de verano de la Universidad de Alcalá

La Universidad de Alcalá ofrece un curso de verano sobre seguridad informática.

<https://drive.google.com/file/d/1ZigZtNe9n0O0CVaO877oxbGJQhh3Idrx/view>

Objetivos:

Formar a los alumnos en conceptos y herramientas avanzadas en ciberseguridad, desarrollo y aprendizaje de herramientas para hacking, redes sociales y redes TOR (Deep web)

### 4.1.2 The security sentinel

<https://thesecuritysentinel.es/curso/certificado-profesional-de-hacking-etico/>

* Este curso te proporciona los conocimientos necesarios a nivel conceptual y práctico para que puedas implementar en empresas y negocios, un sistema Integral de Seguridad Informática integral y perimetral, apoyado por el uso de Software Libre.
* Desarrollarás y adquirirás habilidades prácticas para la realización de auditorías de sistemas intrusivos, usando las técnicas de la Auditoria de T.I del tipo “Hacking Ético y/o Test de Penetración”.
* Conocerás los diferentes tipos de atacantes, así como a usar las diferentes técnicas y herramientas de intrusión utilizadas por los delincuentes informáticos para lograr violentar la seguridad de un sistema de información.
* Con este curso, podrás realizar sin problemas auditorías de Pentesting con su correspondiente informe profesional, además de conocer los métodos utilizados por los delincuentes cibernéticos para poder contrarrestar sus ataques.
* Este curso se ha definido con un 75% de práctica y un 25 % de teoría, lo que te facilitará mucho el aprendizaje y el aprovechamiento máximo de conocimientos.
* Orientar las auditorias intrusivas haciendo uso de las normas y buenas prácticas en seguridad de la información a nivel internacional.
* Aprender las técnicas de ataque y protección de las redes inalámbricas y las aplicaciones web dinámicas.
* Formar auditores técnicos e integrales en el tema de seguridad de la información.

### 4.1.3 Hacking ético en udemy

<https://www.udemy.com/kali-linux-pruebas-de-penetracion-y-hacking-etico-basico/?siteID=ycsZhk7mqJY-dLiMITU0NxTuFVAgSj.pcw&LSNPUBID=ycsZhk7mqJY>

En este curso el alumno aprenderá algunas de las técnicas básicas de Hacking Ético y Pruebas de Penetración en un entorno de pruebas de práctica 100% seguro.

El alumno comprenderá el potencial de Kali Linux y las herramientas que posee para realizar Pruebas de Penetración y Hacking Ético explotando software vulnerable y obteniendo una consola remota.

### 4.1.4 Máster en ciberseguridad imf-formación

<https://www.imf-formacion.com/masters-profesionales/master-seguridad-informatica-presencial>

OBJETIVOS DEL MÁSTER EN CIBERSEGURIDAD PRESENCIAL

Dotar al alumno de un conocimiento amplio y riguroso en disciplinas tales como **ciberinteligencia**, **análisis de malware**, **auditorías técnicas de redes y sistemas (hacking ético)**, **análisis forense y gestión de incidentes de seguridad**, **desarrollo seguro de aplicaciones web** y la **monitorización y correlación de eventos de seguridad** (por medio de tecnologías SIEM).

Los objetivos específicos que logrará el alumno son los siguientes:

* Obtener una visión global del ámbito de la ciberseguridad, conociendo los ataques más relevantes y cómo mitigarlos.
* Desarrollar competencias técnicas y aprender a usar herramientas que exploten al máximo sus conocimientos y habilidades para la realización de pruebas de intrusión en redes y sistemas.
* Adquirir la capacitación necesaria para obtener, mantener y procesar evidencias digitales usando herramientas y procedimientos específicos.
* Conocer el mundo de la ingeniería inversa y analizar código malicioso, asumiendo los procesos para comprender el funcionamiento de los ficheros que trabajan a bajo nivel en sistemas y redes.
* Asimilar los conocimientos precisos para gestionar y establecer políticas claras de seguridad para el componente móvil de los sistemas.
* Conocer de forma práctica los principios de la monitorización y correlación de eventos de seguridad, a través de informes reales.
* Formarse como desarrollador en programación segura y mejorar sus habilidades como auditor de seguridad en el análisis y evaluación del código fuente de las aplicaciones.

### 4.1.5 Hacking ético akademus

<https://www.akademus.es/cursos/hacking-etico-cero-cien/>

- Este curso te proporciona los conocimientos necesarios a nivel conceptual y práctico para que puedas implementar en empresas y negocios, un sistema integral de seguridad informática integral y perimetral, apoyado por el uso de Software libre.

- Desarrollarás y adquirirás habilidades prácticas para la realización de auditorías de sistemas intrusivos, usando las técnicas de la Auditoría de T.I del tipo "Hacking Ético y/o Test de Penetración".

- Conocerás los diferentes tipos de atacantes, así como a usar las diferentes técnicas y herramientas de intrusión utilizadas por los delincuentes informáticos para lograr violentar la seguridad de un sistema de información.

- Con este curso, podrás realizar sin problemas auditorías de Pentesting con su correspondiente informe profesional, además de conocer los métodos utilizados por los delincuentes cibernéticos para poder contrarrestar sus ataques.

### 4.1.6 Hacking ético Securizame

<https://cursos.securizame.com/courses/hacking-etico/>

En el curso se tratarán los principales temas relacionados con el hacking ético desde diferentes puntos de vista, permitiendo al alumno comprender y aprender a realizar test de intrusión para poder emitir conclusiones y minimizar los riesgos asociados en la exposición de un sistema informático a Internet, realización de auditoría interna, redes inalámbricas, etc.,

El curso tendrá una duración de 56 horas y está orientado a auditores, administradores de sistemas y especialistas en el sector de seguridad, con un conocimiento medio. Dado que se empezará con una introducción al hacking ético, también es accesible a aquellos profesionales que deseen iniciarse en el sector adquiriendo, al final del curso un muy buen nivel de conocimientos.

## 4.2 Cursos no gratuitos sobre Aircrack-NG

### 4.2.1 Curso de dragonjar

Este curso, es en modalidad online, lo imparten profesionales muy reconocidos en el mundo de la seguridad informática como son las personas que forman parte de la comunidad dragonjar. Ofrecen un contenido que se van actualizando constantemente. Entre esos contenidos se encuentra el de “Ataques actuales para redes inalámbricas” en el que se utiliza, entre otras, la herramienta Aircrack –NG.

El precio de este curso no es una cantidad en concreto, sino que es una suscripción anual de 1000 USD/año, por ello, los contenidos se van actualizando constantemente.

Enlace: <https://www.dragonjar.education/diplomado/>

### 4.2.2 Curso de pentestmag

En este online que se imparte gracias a la página web [www.pentestmag.com](http://www.pentestmag.com), se explica cómo hacer un test de seguridad en pentesting de redes Wi-Fi como un profesional. En el segundo módulo del curso, se estudia la herramienta Aircrack-NG.

Este curso no tiene un precio en concreto, sino que la pagina tiene la política de que cada usuario page una suscripción anual de 790 USD/año para que puedan acceder a los contenidos de este curso y de los demás cursos que imparten.

Enlace: <https://pentestmag.com/course/advanced-wireless-penetration-testing-15-2/>

### 4.2.3 Curso de Digital Tech Institute

Este curso lo imparte el Digital Tech Institute, está diseñado para empresas que quieran invertir en la formación de sus empleados y aumentar sus conocimientos en seguridad informática y hacking ético. En el módulo 4, de hacking ético, hay un apartado sobre ataques en redes inalámbricas, en el que se utilizara la herramienta Aircrack-NG.

Enlace: <http://www.digitaltechinstitute.com/formacion-in-company/itinerario-seguridad-it/#1484231461750-d6d95da4-788c>

### 4.2.4 Curso de backtrackacademy

En este curso se explican muchos conceptos sobre los protocolos y sistemas de las redes inalámbricas y como hacer tests de penetración en función de esos protocolos y sistemas. Para ello, entre otras herramientas, utilizan la herramienta Aircrack-NG.

Enlace: <https://backtrackacademy.com/curso/hacking-wireless>

## 4.3 Cursos no gratuitos sobre Fern Wifi Wireless Cracker

### 4.3.1 Curso de Udemy por MBPSec

<https://www.udemy.com/master-in-wi-fi-ethical-hacking/>

En Udemy hay un curso creado por MBPSec Tech el cual consiste en un video de 1 hora de duración acerca de hacking en el que se usa esta herramienta y cuyo precio es de 99.99€.

### 4.3.2 Curso de Udemy de Eduardo Arriols Nuñez

<https://www.udemy.com/curso-completo-de-hacking-etico/>

También en Udemy hay un curso más completo aun creado por Eduardo Arriols Nuñez acerca del hacking en el que se usa también esta herramienta y el curso completo consta de 20 horas de video y tiene un coste de 139.99€

# 5. Fuentes de información (cursos gratuitos)

## 5.1 Cursos gratuitos generales

### 5.1.1 Seguridad informática Miriadax

<https://miriadax.net/web/seguridad-informatica-practica/inicio?timestamp>=

El curso está diseñado para introducir al alumno en el autoaprendizaje práctico de la seguridad, de forma que, progresivamente, adquiera la experiencia necesaria para poder plantear y llevar a cabo sus propios ejercicios y pruebas. El curso incluye demostraciones y ejercicios que los estudiantes pueden reproducir y realizar en su propio ordenador, usando para ello el laboratorio NETinVM (http://netinvm.org).

### 5.1.2 Curso de seguridad esetec

<http://www.esetec.es/cursos/seguridad-informatica>

Este **curso de Seguridad informática**te permitirá garantizar la seguridad de los accesos y usos de la información registrada en equipos informáticos, así como del propio sistema, protegiéndose de los posibles ataques, identificando vulnerabilidades y aplicando sistemas de cifrado a las comunicaciones que se realicen hacia el exterior y en el interior de la organización.

### 5.1.3 Curso de craking de Ricardo Narvaja

<http://190.90.112.209/Primer_curso_de_cracking_de_Ricardo_Narvaja_completo.pdf>

Se explica en un curso sencillo las bases para crackear programas o mejor expresado las bases de la INGENIERIA REVERSIBLE que es el arte de revertir las protecciones que poseen ciertos programas para hacerlos accesibles a todos y no haya que pagar por usarlos.

### 5.1.4 Curso hacking edutin

<https://edutin.com/curso-de-hacking-3106>

Este curso gratis de programación Hacking te dará oportunidades de conocer como son los defectos de las páginas web, cuáles son sus mecanismos de seguridad, y también a protegerte de los conocedores del campo del hacking

## 5.2 Cursos gratuitos sobre Aircrack-NG

### 5.2.1 Curso de dragonjar

Este es un cuso que proporciona la web dragonjar, que es una comunidad hacker de Latinoamérica muy reconocida en el mundo de la seguridad informática ofrece un curso gratuito de introducción a pentesting, en el que un apartado de su formación es “Ataques actuales para redes inalámbricas” en el que utilizan la herramienta Aircrack-NG.

Enlace: <https://www.dragonjar.education/curso/como-se-realiza-un-pentest/>

### 5.2.2 Tutoriales de Aircrack

En este curso están todos los tutoriales que los desarrolladores de la herramienta proveen a los usuarios. En este curso se enseña desde como instalar la herramienta a los distintos tipos de ataques que es capaz de levar a cabo Aircrack-NG. Además, estos tutoriales han sido traducidos a otros idiomas para ayudar a los usuarios con su comprensión.

Enlace: <https://www.aircrack-ng.org/doku.php?id=tutorial>

### 5.2.3 Curso de pkred

Este es un curso que imparte la web [www.pkred.com](http://www.pkred.com) en el que le dedica un apartado al uso de la herramienta Aircrack-NG. En este curso, se enseña a utilizar la herramienta de una forma más avanzada y totalmente práctica.

Enlace: <https://pkred.com/publicaciones/Curso%20de%20Hacking%20Part%204.2%20::%20Claves%20Wifi,%20Aircrack-ng./595264d611f5ae34acd74bc5>

### 5.2.4 Curso de Marcos Mendoza

Este es un curso gratuito sobre “Wireless penetration testing con Kali Linux” impartido totalmente en la plataforma Youtube por Marcos Mendoza, en el que enseña a utilizar diferentes herramientas de la distribución de software libre Kali Linux tiene para hacer test de penetración en redes Wi-Fi. Y una de esas herramientas es AirCrack-NG.

Enlace:

<https://www.youtube.com/playlist?list=PL-G03HRCQgdFKAaW718J14tKDM63mGirL>

## 5.3 Cursos gratuitos sobre Fern Wifi Wireless Cracker

### 5.3.1 Blog de r4z0r

<https://r4z0rbl4ck.wordpress.com/2013/06/02/hackear-redes-wpa-con-fern-wifi-cracker-by-r4z0r/>

se trata de un blog en el que explica el funcionamiento de la aplicación paso por paso para ir realizando los pasos según se va leyendo con capturas de pantalla para así hacer mejor seguimiento de los avances en el uso de la aplicación.

### 5.3.2 Tutorial de hackthis

<https://www.hackthis.co.uk/forum/hacking-security/tutorials-articles/1818-cracking-wpa2-with-fern-wifi-cracker?page=2>

es un tutorial también de uso de la aplicación estructurado en los diferentes pasos que hay que realizar para la instalación y uso de la aplicación con capturas de pantalla para el seguimiento del tutorial.

# 6. Ayudas económicas para estudiar las tecnologías

Nosotros como equipo, podríamos pedir una ayuda para poder estudiar las tecnologías que hemos elegido, estas ayudas nos servirían para sufragar gastos ocasionados por la investigación, las ayudas a las que tenemos acceso las podríamos clasificar de la siguiente forma:

Beca general públicas de estudios universitarios.

Esta beca la otorga el ministerio de Educación y Ciencia, es una beca muy solicitada por gran cantidad de estudiantes, por eso esta beca tiene una serie de requisitos para poder optar a ella, a nivel general son tener nacionalidad española o de un país miembro de la comunidad europea, también los estudiantes no comunitarios podrán optar a esta beca siempre y cuando sus padres o ellos mismos trabajen en España. A nivel académico depende de los estudios que se vayan a cursar, si el alumno es recién ingresado en la universidad este tiene que matricularse de 60 créditos, si el alumno es de segundo debe haber superado el 60% de los créditos el curso anterior en las enseñanzas técnicas y un 80% si son el resto de las enseñanzas. A nivel económico según el nivel de renta familiar se determina tanto si el estudiante puede optar a la beca como a la cuantía y al tipo de ayudas que el estudiante puede acceder. Las becas sueles oscilar entre los 1500 y los 6000 euros.

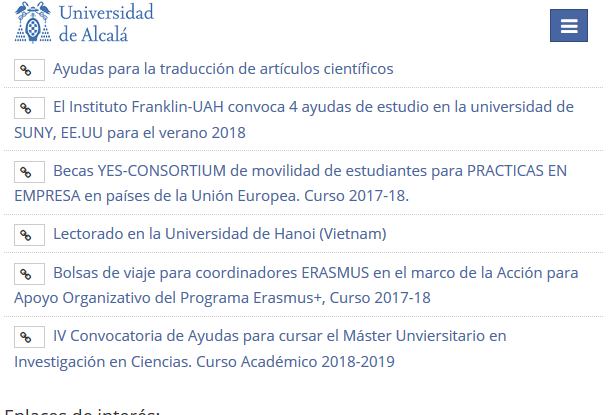
Estas becas las puede disfrutar cualquier estudiante universitario que curse una titulación oficial ya sea en la universidad pública o privada.

En caso de que tuviéramos que desplazarnos a una universidad distinta para seguir investigando podríamos optar por; becas erasmus si nuestro objetivo es salir fuera de España para investigar nuestra tecnología, esta beca es un programa de intercambio de estudiantes y profesores, para poder optar a esta beca el estudiante debe haber superado el primer curso de sus estudios y tener un nivel medio del idioma de la universidad a la cual asistiría. El importe de la beca seria 150 euros al mes abonados en diferentes plazos.

Si no queremos marcharnos de España tenemos la opción de pedir las becas SICUE anteriormente conocidas como becas Seneca, esta beca forma parte de un programa de intercambio de alumnos entre universidades españolas, para esta beca es necesario que el alumno tenga una determinada nota media, una determinado de créditos aprobados y que las asignaturas en las que se matricule sean obligatorias en su grado además de que no sean de segunda matricula.

Se ha sondeado también la posibilidad de pedir beca, que fueran extendidas por la comunidad autónoma de Madrid, podríamos optar si fuera el caso a las becas de excelencia, para optar a esta beca los estudiantes deben estar matriculados en cualquier centro de enseñanza universitaria de la comunidad de Madrid cursando un titulo oficial de enseñanza, además el alumno debe acreditar una media de 8.25 en enseñanzas de conocimientos de Ingeniería y Arquitectura.

Se ha tenido en cuenta las becas que ofrece la universidad de Alcalá de Henares a sus estudiantes, pero, nosotros no podemos optar a ella o no son de nuestra rama de conocimiento.



Becas de carácter privado

Aparte de las becas de carácter público otorgadas por el ministerio de educación, comunidades autónomas y universidades, también se puede optar a becas ofrecidas por entidades privadas como bancos, un ejemplo es el Banco Santander Hispano el cual tiene una gran cantidad de becas, de las cuales podríamos destacar Becas Iberoamérica Santander Grado las cueles promueven el intercambio entre alumnos de España y las principales universidades iberoamericanas, en esta beca participa la Universidad de Alcalá de Henares, a esta beca puede optar cualquier estudiante universitario.

Otra beca que podríamos destacar es Becas Iberoamérica Santander Investigación, es una beca que fomenta el intercambio de investigadores de España con universidades iberoamericanas, esta beca está dirigida a personal docente e investigadores.

Santander tiene una gran cantidad de becas con diferentes universidades como; Becas colaboración Universidad Politécnica de Madrid, la cual proporciona al alumno mejor formación a través de labores o tareas que le proporcionaran una formación transversal en ciertas competencias.

Aula universitaria del Estrecho. Universidad de Cádiz, son becas dirigidas para estudiantes universitarios que quisieran estudiar en Marruecos.

Becas y ayudas a la movilidad Investigadora estas becas están ofrecidas para investigadores y estudiantes de postgrado, y cubren tanto la estancia para predoctorado y postdoctorado.

Esto es una pequeña muestra de becas ofrecidas de forma privada todos los bancos y cajas tienen becas de estudios.

# 7. Recursos para implementar las tecnologías

## 7.1 Recursos para implementar Aircrack

### 7.1.1 Recursos gratuitos para implementar Aircrack

Aircrack

Lo más importante, el software que vamos a utilizar este lo podemos descargar desde la propia página, que posteriormente a ser descargado podremos utilizar para hacer las pruebas pertinentes.

Kalilinux

Esta versión de Linux la tendremos que instalar en nuestros ordenadores, este software nos brinda un perfecto ecosistema de pruebas y experimentación, ya que nos ofrece una sandbox además de múltiples herramientas más.

Router

Aunque parezca una obviedad necesitamos un router para poder crear redes wifi para poder atacarlas y hacer pruebas con ellas.

### 7.1.2 Recursos no gratuitos para implementar Aircrack

En este apartado no tenemos ningún recurso que sea de pago, más allá de un ordenador en el que ejecutar el programa.

## 7.2 Recursos para implementar Fern WiFi Wireless Cracker

### 7.2.1 Recursos gratuitos para implementar Fern WiFi Wireless Cracker

Fern WiFi Wireless Cracker

Lo más importante, el software que vamos a utilizar este lo podemos descargar desde la propia página, que posteriormente a ser descargado podremos utilizar para hacer las pruebas pertinentes.

Kalilinux

Esta versión de Linux la tendremos que instalar en nuestros ordenadores, este software nos brinda un perfecto ecosistema de pruebas y experimentación, ya que nos ofrece una sandbox además de múltiples herramientas más.

Router

Aunque parezca una obviedad necesitamos un router para poder crear redes wifi para poder atacarlas y hacer pruebas con ellas

### 7.2.2 Recursos no gratuitos para implementar Fern WiFi Wireless Cracker

En este apartado no tenemos ningún recurso que sea de pago, más allá de un ordenador en el que ejecutar el programa.

# 8. Conclusiones

Nos encontramos ante dos herramientas con una finalidad similar, pero que previsiblemente tienen características diferentes.

Decimos que previsiblemente tendrán características diferentes porque no se utilizan como herramientas sustitutivas la una de la otra en los entornos de trabajo en los que se usan.

El mayor ejemplo de esto es que en la distribución Kali Linux, especializada en realizar tests de penetración, trae instaladas las dos herramientas.

En cualquier caso, aún no hemos realizado ningún proceso de comparación de las dos herramientas, por lo que no aseguramos nada.

En cuanto a los recursos disponibles, nos ha resultado más fácil encontrar recursos de carácter general que formaciones más específicas.

Existen muchos cursos y formaciones tanto gratuitas como de pago que nos permiten formarnos en toda la tecnología que rodea el pentesting, pero a la vez también existen múltiple información con un carácter más desestructurado, como blogs o pequeños tutoriales, algo que parece razonable, teniendo en cuenta que mucha de estas herramientas son desarrollos de carácter individual o de grupos pequeños.

Si que resulta bastante más complicado encontrar cursos que estén centrados únicamente en una de estas herramientas, si que hay información sobre ellas, capítulos en libros dedicados a estas aplicaciones, o artículos que se centran en ellas, pero resulta difícil encontrar un curso entero de una sola de estas aplicaciones, algo que, si ocurre con otras aplicaciones, como Photoshop, aunque quizás en esto tengan algo que ver las dimensiones de las aplicaciones.

Asimismo, aunque uno puede centrarse en una sola de estas herramientas, la seguridad informática cuenta con muchas otras necesidades, es razonable que haya información de esas otras necesidades en los cursos sobre seguridad.

Mencionar que existen becas de estudio, pero no de carácter específico para el estudio de estas tecnologías, aunque como estudiantes de la universidad de Alcalá tenemos descuento en algunos de los cursos que se imparten sobre esta tecnología.

Por último, destacamos que el uso de estas aplicaciones no necesita de prácticamente ningún recurso más allá de la capacidad de crear una red inalámbrica con algún tipo de protección en forma de contraseña.