PASSWORD CRACKING TOOLS

AIRCRACK-NG VS FERN WIFI WIRELESS CRACKER

Contenido

[1. Autores del trabajo, planificación y entrega 3](#_Toc513487386)

[1.1 Autores 3](#_Toc513487387)

[1.2 Planificación 3](#_Toc513487388)

[1.3 Entrega 3](#_Toc513487389)

[2. Requisitos del prototipo a implementar 4](#_Toc513487390)

[2.1 Requisitos funcionales 4](#_Toc513487391)

[2.2 Otros requisitos 4](#_Toc513487392)

[3. Criterios de comparación en la implementación 6](#_Toc513487393)

[3.1 Criterio 1: Exportar resultados 6](#_Toc513487394)

[3.2 Criterio 2: Ataque WPA 6](#_Toc513487395)

[3.3 Criterio 3: Ataque WPS 6](#_Toc513487396)

[3.4 Criterio 4: Ataques Simultáneos. 6](#_Toc513487397)

[3.5 Criterio 5: Sistema Operativo. 6](#_Toc513487398)

[3.6 Criterio 6: Dificultad de uso. 6](#_Toc513487399)

[3.7 Criterio 7: Interfaz gráfica. 6](#_Toc513487400)

[3.8 Criterio 8: Tiempo en estar operativo. 7](#_Toc513487401)

[3.9 Criterio 9: Requisitos mínimos. 7](#_Toc513487402)

[3.10 Criterio 10: Manual. 7](#_Toc513487403)

[3.11 Criterio 11: Tiempo de ejecución. 7](#_Toc513487404)

[3.12 Criterio 12: Tipos de escaneo. 7](#_Toc513487405)

[3.13 Criterio 13: Recomendación de Ataque. 7](#_Toc513487406)

[4. Proyecto de implementación de un prototipo del sistema utilizando la Aircrack-ng 8](#_Toc513487407)

[4.1 Documentación de diseño 8](#_Toc513487408)

[4.1.1 Diseño de la red 8](#_Toc513487409)

[4.2 Documentación de construcción 8](#_Toc513487410)

[4.2.1 Documentación ataque WPA2 9](#_Toc513487411)

[4.3 Documentación de pruebas 12](#_Toc513487412)

[13](#_Toc513487413)

[4.4 Documentación de instalación 13](#_Toc513487414)

[4.5 Manual de usuario 17](#_Toc513487415)

[5. Proyecto de implementación de un prototipo del sistema utilizando la tecnología Fern Wifi Cracker 19](#_Toc513487416)

[5.1 Documentación de diseño 19](#_Toc513487417)

[5.2 Documentación de construcción 19](#_Toc513487418)

[5.3 Documentación de pruebas 25](#_Toc513487419)

[5.4 Documentación de instalación 25](#_Toc513487420)

[5.5 Manual de usuario 26](#_Toc513487421)

[6. Comparación de las dos implementaciones 27](#_Toc513487422)

[6.1 Evaluación de los criterios en la implementación usando la tecnología A 27](#_Toc513487423)

[6.2 Evaluación de los criterios en la implementación usando la tecnología B 28](#_Toc513487424)

[7. Comparación de la implementación de las tecnologías 29](#_Toc513487425)

[8. Conclusiones 32](#_Toc513487426)

# 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

<https://github.com/Rijaelto/TG3>

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

* Informe del trabajo: con el nombre TG3\_final.docx
* Presentación del trabajo: TG3\_final.pptx
* Prototipos obtenidos implementando cada una de las tecnologías (deben incluir el código fuente y todos los archivos necesarios para la instalación y uso de cada prototipo):
  + PrototipoTecnologiaA\_final.zip (o .rar)
  + PrototipoTecnologiaB\_final.zip (o .rar).

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

# 2. Requisitos del prototipo a implementar

El objetivo del proyecto es comparar el comportamiento de las tecnologías Aircrack-ng y Fern Wifi Cracker a la hora de descifrar y crackear contraseñas de redes wifi. Para ello, vamos a realizar varios ataques a redes wifi con diferentes tipos de encriptación de contraseñas. Vamos a realizar los ataques sobre 2 tipos de encriptaciones: la encriptación WEP con el cifrado RC4 y la encriptación WPA2-PSK con e cifrado AES.

En el año 1997 se lanzo por primera vez un estándar de comunicaciones inalámbricas, el estándar IEEE 802.11, el llamado Wired Equivalent Privacy (WEP) que planteaba un algoritmo de seguridad para proteger los datos intercambiados a través de red, muy similar a la seguridad que proporcionaban más redes de cable.

El protocolo de seguridad WPA2, se lanzó en 2004 como el protocolo teóricamente seguro al 100%, que fue la segunda versión del protocolo WPA en el estándar IEEE 802.11i. Con este protocolo se cambio el algoritmo de encriptación que tenia WPA que era TKIP (Temporal Key Integrity Protocol) por el algoritmo AES (Advanced Encryption Standard). Este protocolo de seguridad ha sido el último y más eficiente protocolo que se ha usado en la seguridad de las redes wifi.

Ambos sistemas deberán evaluar los 2 protocolos de seguridad, para ello, ambos prototipos van a enseñar una demostración del uso de la tecnología para realizar la comprobación del grado de seguridad de ambos protocolos.

Los requisitos para ambos protocolos serán los mismos salvo el requisito de tipo de protocolo.

## 2.1 Requisitos funcionales

Los requisitos funcionales deben ser los mismos para las dos implementaciones.

En la siguiente tabla se indicará el catálogo de requisitos funcionales del sistema.

| **REQ.** | **DESCRIPCIÓN** |
| --- | --- |
| RF01 | El sistema deberá utilizar el protocolo de encriptación WPA2 |
| RF02 | El sistema será capaz de utilizar una tarjeta de red en modo monitor |
| RF03 | El sistema será capaz de absorber trafico de paquetes de red wifi |
| RF04 | El sistema será capaz de inyectar trafico en la red objetivo |
| RF05 | El sistema será capaz de realizar ataques de des autenticación |
| RF06 | El sistema deberá ser capaz de realizar ataques de fuerza bruta |
| RF07 | El sistema deberá sacar los resultado del ataque en documento de texto |
| RF08 | El sistema será capaz de capturar el trafico los datos necesarios para elaborar un handshake |

RF: REQUISITO FUNCIONAL

## 2.2 Otros requisitos

Se pueden incluir aquí otros requisitos para el prototipo que no puedan considerarse como funcionales. Por ejemplo, requisitos de datos, de seguridad, de interfaz de usuario, de rendimientos, etc.

Se puede dejar libertad

En la siguiente tabla se indicará el catálogo de requisitos no funcionales del sistema.

| **REQ.** | **DESCRIPCIÓN** |
| --- | --- |
| RNI01 | El punto de acceso a la red debe ser un punto de acceso wifi |
| RNI02 | El punto de acceso debe tener una potencia (power o pwr) suficiente para que la maquina sea capaza de capturar tráfico |
| RNI03 | La tarjeta de red debe ser una tarjeta de red wifi |
| RNI04 | Se debe poder utilizar la interfaz de la tarjeta de red en la maquina que realiza los ataques |

# 3. Criterios de comparación en la implementación

## 3.1 Criterio 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 Criterio 2: 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).*

## 3.3 Criterio 3: Ataque WPS

*Nombre del criterio: Ataque WPS.*

*Descripción: indicar si la herramienta es capaz de realizar ataques ante vulnerabilidades del sistema WPS.*

*Tipo de valor: Booleano (SI/NO).*

## 3.4 Criterio 4: Ataques Simultáneos.

*Nombre del criterio: Número de ataques simultáneos.*

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

*Tipo de valor: Texto libre.*

## 3.5 Criterio 5: Sistema Operativo.

*Nombre del criterio: Disponibilidad en Windows, Linux y Ma.*

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

*Tipo de valor: Booleano (SI/NO).*

## 3.6 Criterio 6: Dificultad de uso.

*Nombre del criterio: Dificultad*

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

*Tipo de valor: Horas.*

## 3.7 Criterio 7: Interfaz gráfica.

*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.*

## 3.8 Criterio 8: Tiempo en estar operativo.

*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: Texto libre.*

## 3.9 Criterio 9: Requisitos mínimos.

*Nombre del criterio: Requisitos*

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

*Tipo de valor: Texto libre.*

## 3.10 Criterio 10: Manual.

*Nombre del criterio: Manual*

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

*Tipo de valor: Texto libre.*

## 3.11 Criterio 11: 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.*

## 3.12 Criterio 12: Tipos de escaneo.

*Nombre del criterio: Tipos de escaneo.*

*Descripción: Al existir la posibilidad en el software de elegir el tipo de escaneo que deseamos realizar, queremos observar cual de ellos es mejor.*

*Tipo de valor: Texto libre.*

## 3.13 Criterio 13: Recomendación de Ataque.

*Nombre del criterio: Recomendación del ataque.*

*Descripción: Al existir la posibilidad en el software de elegir el tipo de ataque que deseamos realizar, queremos observar cuál de ellos es mejor.*

*Tipo de valor: Texto libre*

# 4. Proyecto de implementación de un prototipo del sistema utilizando la Aircrack-ng

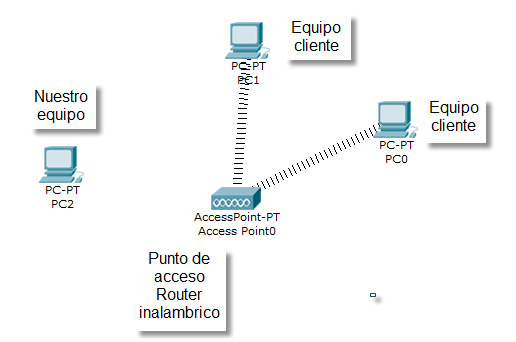
## 4.1 Documentación de diseño

El prototipo consiste en un video en el que se va a explicar y a ejecutar un ataque a redes wifi con el protocolo de seguridad WPA.

En el caso del protocolo de seguridad WPA2, se va a enseñar cómo realizar ataques de desautenticación para capturar datos de handshakes para después, a través de una herramienta de la suite de Aircrack-ng descifrar la contraseña de la red wifi a través de un ataque de fuerza bruta.

### 4.1.1 Diseño de la red

La red a la que se va a intentar crackear la contraseña va a ser una red wireless, más concretamente una red wifi. Esta red va a ser una red de infraestructura, es decir, una red que va a tener al menos un punto de acceso. Dentro de las redes de infraestructura va a ser una red BSS (Basic Service Set) lo que significa que la red solo va a tener un punto de acceso y que la cobertura de la red va a ser la abarcada por el punto de acceso.



El ataque se va a realizar desde el PC2 de la imagen anterior, y en la red, como vemos en la imagen, va a haber al menos un equipo conectado al punto de acceso, ya que va a ser muy importante para realizar el ataque de des autenticación.

## 4.2 Documentación de construcción

Como en nuestro caso, el prototipo consiste en un ataque a redes wifi a través de la tecnología Aircrack-ng, debemos documentar el ataque.

### 4.2.1 Documentación ataque WPA2

Lo primero que tenemos que tener conectado a la maquina es una tarjeta de red wifi, la maquina debe de ser capaz de utilizar su interfaz wifi. Para ello, en nuestro caso, como vamos a utilizar una maquina virtual con el sistema operativo Wifislax, vamos a utilizar una tarjeta de red externa a la maquina anfitriona, que se va a conectar por usb:

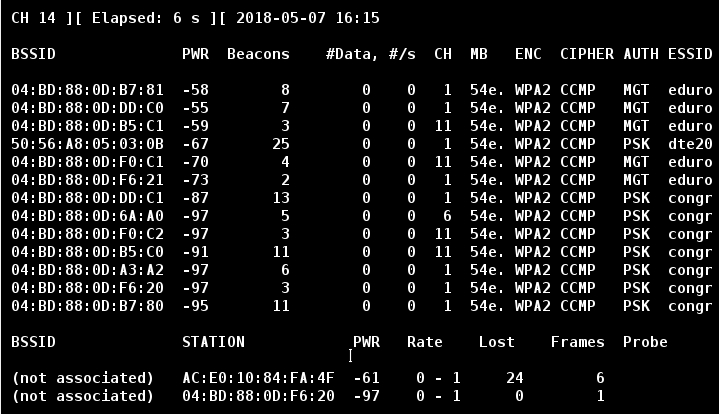


A continuación, establecemos la tarjeta de red en modo monitor, para que pueda capturar tráfico de redes a las que no está conectada. Para ello, abrimos una terminal y utilizamos el siguiente comando: **airmon-ng start [Nombre de la interfaz de la tarjeta de red].**



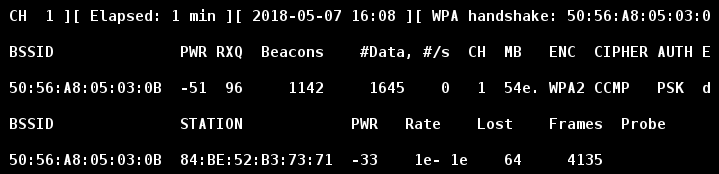
Una vez hemos puesto la tarjeta de red en modo monitor, podemos empezar a capturar todo el tráfico que sea capaz de alcanzar la tarjeta de red, y así poder ver que redes wifi están activas a nuestro alrededor. Para ello, utilizamos el comando **airodump-ng [Nombre tarjeta de red en modo monitor]**



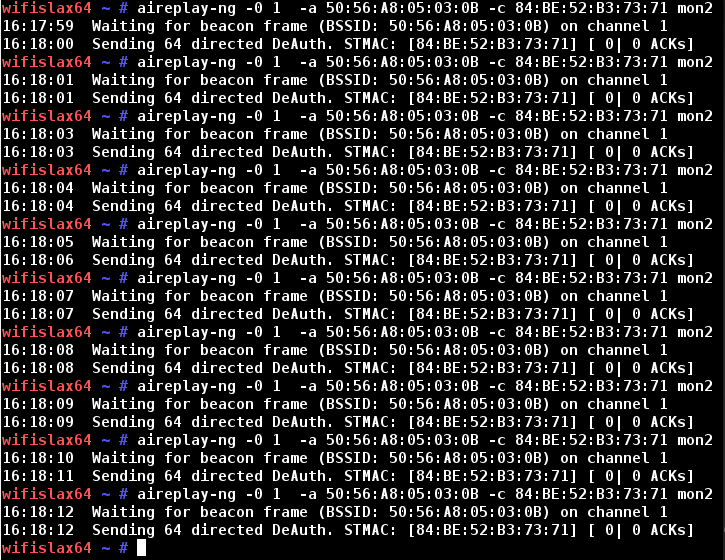


Una vez que hemos encontrado la red que queremos atacar, abrimos otra terminal para capturar los datos del handshake. Estos datos son los que nos van a ayudar a descifrar la contraseña de la red con un ataque de fuerza bruta, que es la manera para descifrar claves WPA2. Para ello, utilizamos el siguiente comando: **airodump-ng –c [canal de la red objetivo] --bssid [Dirección MAC de la red objetivo] –w [dirección en la que alojar el archivo con los datos del handshake] [nombre de la tarjeta de red en modo monitor].**



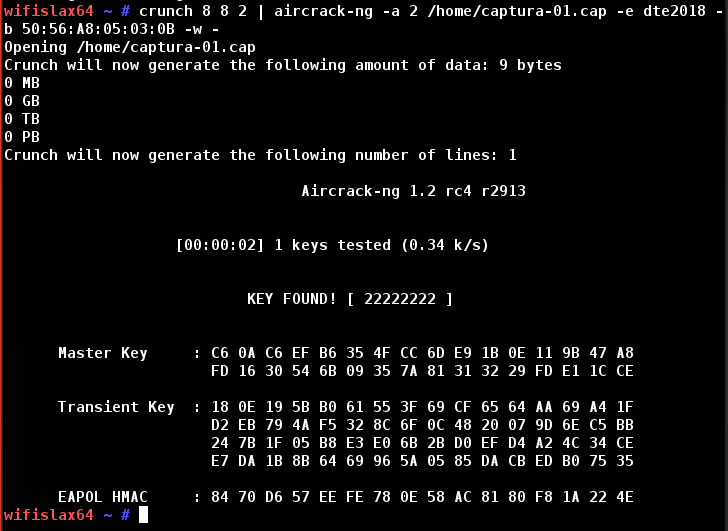


El handshake se da cuando un cliente de la red se conecta al punto de acceso de la red, en ese momento se pueden capturar muchos datos que luego van a ser relevantes para descifrar la contraseña. Podríamos esperar a que cualquier cliente de la red se conecte pero esto podría dilatarse mucho en el tiempo. Por eso, mientras estamos capturando los datos para encontrar el handshake, nosotros realizamos un ataque de desautenticacion para que uno de los clientes de la red se desautentique y se vuelva a autenticar y poder acceder a los datos del handshake. Realizamos ese ataque varias veces para capturar el máximo numero de datos posible para que se pueda después descifrar la clave. Para ello, ejecutamos el siguiente comando en una terminal en varias ocasiones: **aireplay-ng –o [Nº de veces que se desautentica] –a** **[Dirección MAC de la red objetivo] –c [Dirección MAC de un cliente de la red] [nombre de la tarjeta de red en modo monitor].**



Por último, una vez hemos capturado el handshake, comparamos ese handshake con un diccionario de contraseñas o en nuestro caso lo que hacemos es que como sabemos la marca del router y sabemos que de fabrica las contraseñas de las las redes wifi son de 8 caracteres y utilizan los número 1-4 y las letra a-d, utilizamos una herramienta llamada crunch para crear cadenas de caracteres de 8 caracteres combinando dichos caracteres y a la vez compararlo con el handshake:

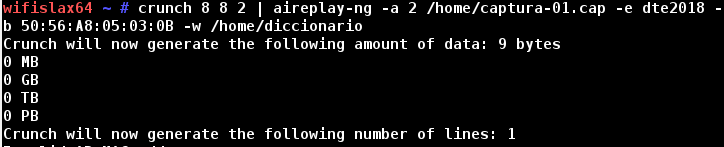
**Crunch 8 8 1234abcd | aircrack-ng –a [tipo de ataque, elegiremos el 2 el de fuerza bruta]** **[dirección en la que está alojado el archivo con los datos del handshake] –e [ESSID] –b [Dirección MAC de la red objetivo] –w [Ruta del diccionario, en nuestro caso no hay diccionario, pondremos -].**



Ya tendríamos la contraseña con la que conectarnos a la red:

## 4.3 Documentación de pruebas

En la primera prueba, intentamos el descifrar una contraseña de un router distinto al que sabíamos los tipos de caracteres que utilizaban en las contraseñas con protocolo de encriptación WPA2 y a pesar de utilizar un diccionario con muchísimas contraseñas como es el diccionario rockyou no se pudo hacer coincidir ninguna contraseña del diccionario con los datos del handshake.



En otra prueba, no capturamos muchos datos para el handshake y a pesar de tener dentro del diccionario la contraseña, no se pudo hacer coincidir la contraseña con los datos del handshake.

## 

## 4.4 Documentación de instalación

Para instalar Aircrack-ng lo más fácil es instalar una maquina virtual con un sistema operativo basado en Linux como KALI o WIFISLAX en el que vienen incluidas todas las herramientas de la suite de aircrack-ng. Para ello, nosotros hemos utilizado virtualbox y el sistema operativo wifislax.

Lo primero es ir a sus páginas web oficiales y descargarlos:

Virtualbox

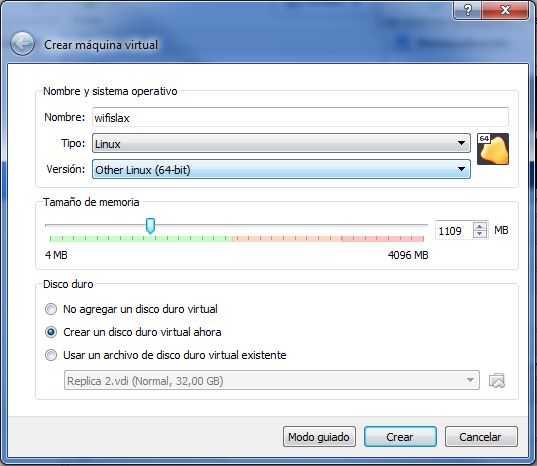


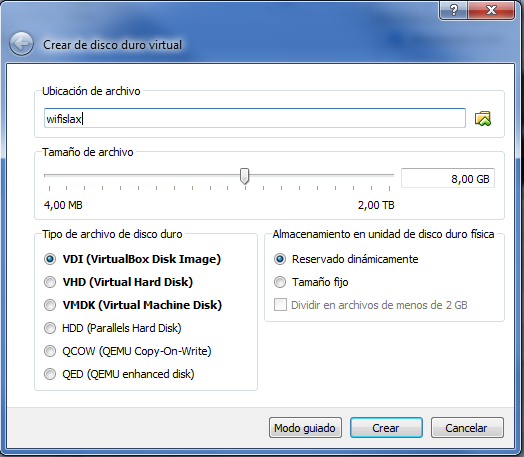
Wifislax



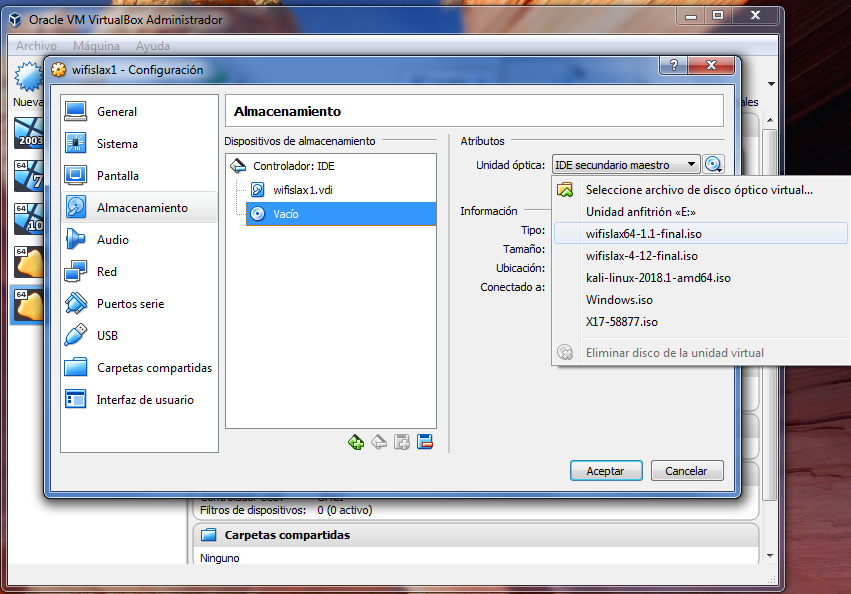
Una vez que los hemos descargado, solo falta crear la maquina virtual con la imagen del sistema operativo y tendremos todo preparado para utilizar el programa Aaircrack-ng.

Creamos la maquina virtual:





Le asociamos la imagen del sistema operativo:



Y la iniciamos:



Seleccionamos la primera opción:



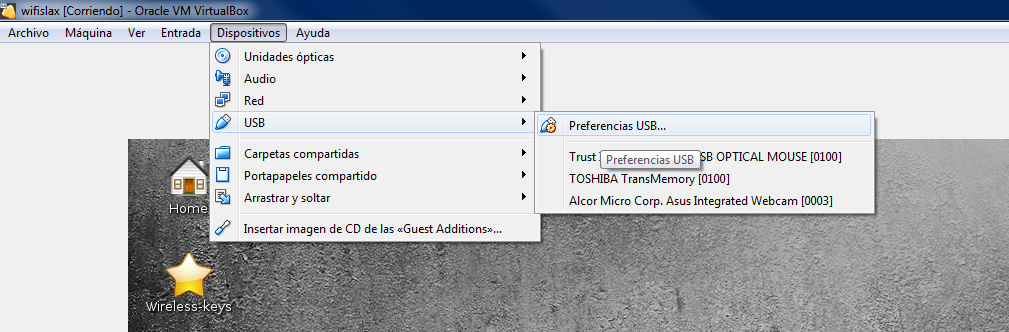


Y ya podemos iniciar la maquina.

## 4.5 Manual de usuario

Lo primero debe de seguir la documentación de la instalación para tener el equipo preparado para realizar el ataque:

Una vez se ha instalado la maquina virtual solo hay que vincular la tarjeta de red, en la pestaña dispositivos-USB y pulsamos al controlador de la tarjeta de red inalámbrica:



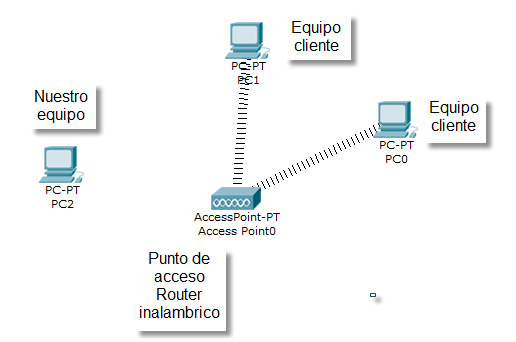
Una vez que ya hemos vinculado la tarjeta de red wifi, solo tenemos que seguir los pasos relatados en la documentación de construcción del prototipo.

# 5. Proyecto de implementación de un prototipo del sistema utilizando la tecnología Fern Wifi Cracker

El prototipo consiste en un video en el que se va a explicar y a ejecutar un ataque a redes wifi con el protocolo de seguridad WPA.

## 5.1 Documentación de diseño

La red a la que se va a intentar crackear la contraseña va a ser una red wireless, más concretamente una red wifi. Esta red va a ser una red de infraestructura, es decir, una red que va a tener al menos un punto de acceso. Dentro de las redes de infraestructura va a ser una red BSS (Basic Service Set) lo que significa que la red solo va a tener un punto de acceso y que la cobertura de la red va a ser la abarcada por el punto de acceso.



El ataque se va a realizar desde el PC2 de la imagen anterior, y en la red, como vemos en la imagen, va a haber al menos un equipo conectado al punto de acceso, ya que va a ser muy importante para realizar el ataque de des autenticación.

## 5.2 Documentación de construcción

**5.2.1 Ataque a red WPA**

Una vez tenemos instalada la distribución de Linux junto con la aplicación abrimos el programa Fern Wifi Cracker.

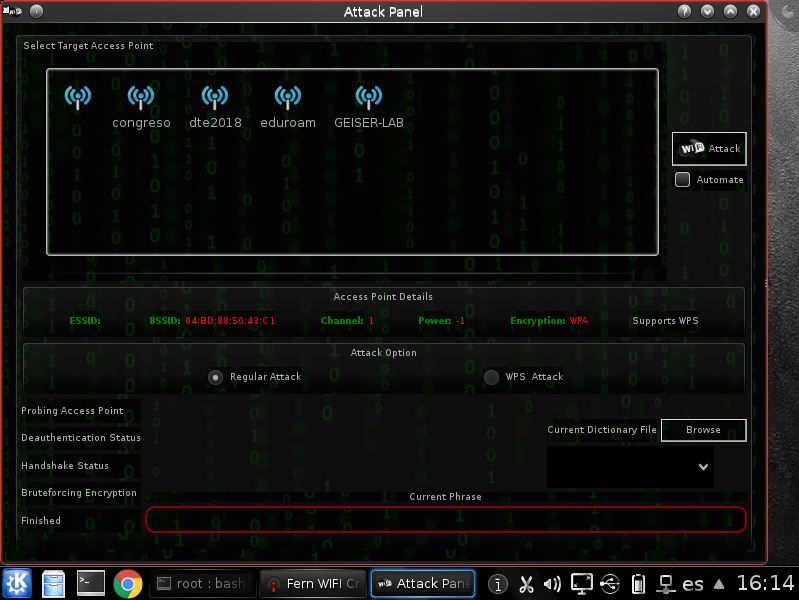
Seleccionamos la interfaz de red que vamos a usar para realizar la auditoria wifi.

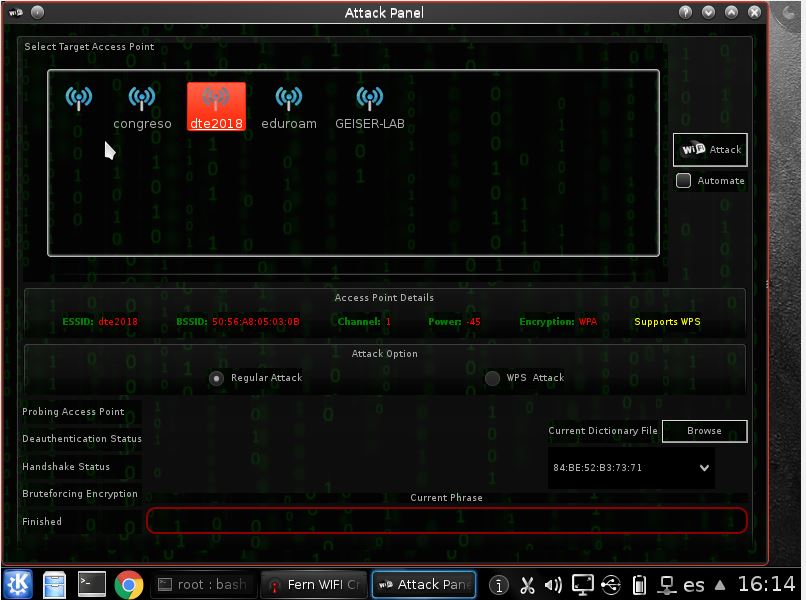
Pulsamos donde dice “Scan for Acces Points” y nos aparecen las diferentes redes wifi que tenemos al alcance de nuestra antena.



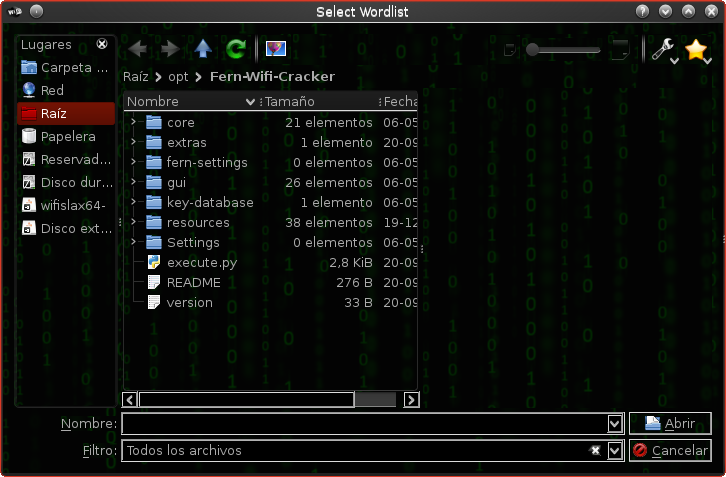
Seleccionamos la red de la que queremos averiguar la contraseña y nos aparecerá una pantalla en la que nos dirá la información de dicha red.







En el apartado donde dice “probing Access Point” seleccionamos “Browse” para elegir el archivo con el diccionario de contraseñas que tenemos para averiguar la contraseña.

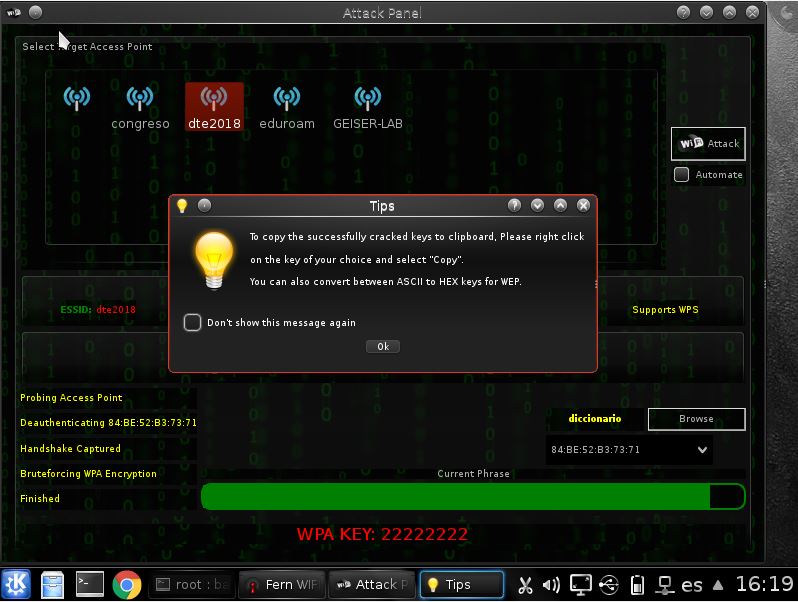




Durante el proceso completo es necesario que haya otro dispositivo conectado a la red ya que para poder hacer las pruebas el sistema captura el tráfico que genera el dispositivo que ya está conectado a la red. Cuando hayamos hecho estos pasos habremos desconectado al otro dispositivo de la red por lo que tenemos que esperar a que se vuelca a conectar para seguir el proceso.



Una vez esté conectado nuevamente podemos pulsar en el botón “Attack” y el programa capturará el tráfico de paquetes entre el dispositivo y el emisor de la red y buscará la clave en el diccionario de contraseñas que habíamos seleccionado.



## 5.3 Documentación de pruebas

En la prueba con la red WPA si el diccionario no incluye todas las posibles combinaciones de contraseñas que puede existir con la longitud de caracteres adecuados a la contraseña existente el resultado final es que no encontrará la contraseña que tiene la red. Por norma general las contraseñas WPA tienen una longitud media de 10 caracteres lo que implica tener un diccionario de contraseñas muy grande.

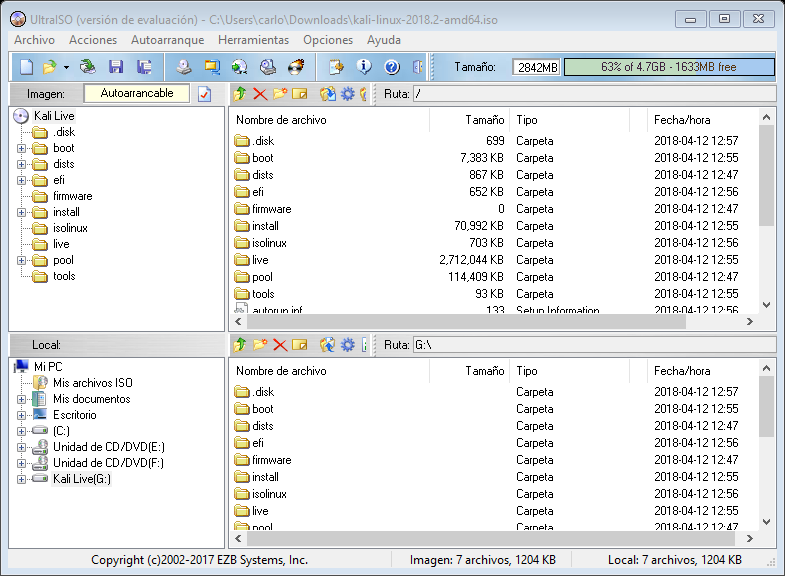
Para las redes WEP el resultado de las pruebas es algo más sencillo ya que no dependemos de ningún diccionario de contraseñas pero como se comenta en el apartado en que realizamos el ataque si no hay muchos dispositivos conectados a la red el tiempo que el sistema averigüe la contraseña llevará horas.

## 5.4 Documentación de instalación

Para la instalación del software del sistema lo que haremos es crear un Pen Drive USB arrancable con la distribución de Linux WifiSlax en la que viene instalada la aplicación que vamos a utilizar.

Como ya tenemos de las pruebas anteriores la distribucion WifiSlax ahora en lugar de hacerlo en una maquina virtual vamos a instalarla en un PenDrive arrancable de manera que usemos la tarjeta de red que tiene integrada el ordenador de las pruebas.

También descargamos el programa UltraISO con el cual podemos crear un USB arrancable a partir de una imagen ISO que tengamos en nuestro PC.



Iniciamos ya el PC con la distribución de Linux arrancando el ordenador desde el USB.

## 5.5 Manual de usuario

En este caso la distribución WifiSlax reconoce automáticamente la tarjeta de red que está integrada por lo que desde la aplicación únicamente seleccionamos la interfaz de red wifi disponible.

# 6. Comparación de las dos implementaciones

Se trata de dar valores a los criterios de comparación definidos en el apartado 3 sobre la implementación de cada uno de los prototipos.

## 6.1 Evaluación de los criterios en la implementación usando la tecnología A

Debe incluir al menos una tabla con la siguiente estructura.

| **CRITERIO** | **EVALUACIÓN** |
| --- | --- |
| Exportar Resultados | SI |
| Ataque WPA | Si |
| Ataque WPS | SI |
| Ataque Simultáneos | SI |
| Sistema Operativos | Se puede ejecutar en Linux |
| Dificultad de uso | Requiere estudiar en que se basan los ataques para poder utilizar la herramienta. |
| Interfaz grafica | No es una interfaz grafica pero si que es un menú de opciones en una terminal |
| Tiempo en estar operativo | 10 o 15 segundos |
| Requisitos Mínimos | Requiere tener una tarjeta de red WIFI que se pueda poner en modo monitor |
| Manual | El manual ayuda mucho a la utilización del programa |
| Tiempo de ejecución | Depende del tipo de ataque y del tamaño del diccionario. Ataque WEP 5 a 10 min. Ataque WPA 10 a 60 min |
| Tipos de escaneo | Puede hacer escaneos solo por redes WEP o solo por redes WPA y también puede escanear sin filtros, que escanea todos los tipos de redes |
| Recomendación de ataques. | Si recomienda atacar a las redes a las que la señal es más fuerte y a las redes con peor seguridad. |

Y algunos comentarios aclaratorios sobre aquellos criterios cuyo valor indicado en la tabla no sea suficiente para entenderlo.

## 6.2 Evaluación de los criterios en la implementación usando la tecnología B

| **CRITERIO** | **EVALUACIÓN** |
| --- | --- |
| Exportar Resultados | Si |
| Ataque WPA | Si |
| Ataque WPS | Si |
| Ataque Simultáneos | No |
| Sistema Operativos | Se puede utilizar en Linux |
| Dificultad de uso | Es muy fácil de utilizar solo hay que leer lo que pide la interfaz |
| Interfaz grafica | Si |
| Tiempo en estar operativo | En 5 y 10 seg |
| Requisitos Mínimos | Necesita poder utilizar una tarjeta de red wifi en modo monitor |
| Manual | Tiene un buen manual, ayuda a entender con realizar los ataques |
| Tiempo de ejecución | Depende del tipo de ataque y del tamaño del diccionario. Ataque WEP 10 a 15 min. Ataque WPA 10 a 60 min |
| Tipos de escaneo | Puede escanear por redes WPA y por redes WEP. No hace escaneos sin filtros. |
| Recomendación de ataques. | No recomienda a que red atacar. |

# 7. Comparación de la implementación 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

| **CRITERIOS** | **TECNOLOGÍA A** | **TECNOLOGÍA B** | **COMENTARIOS** |
| --- | --- | --- | --- |
| Exportar resultados | Si | Si | Los exportan en un txt. |
| Ataque WPA | SI | SI | Equivalente |
| Ataque WPS | SI | Si | Equivalente |
| Ataque Simultáneos | SI | No | Aircrack-NG permite la automatización mediante scripts |
| Sistemas Operativos | Se puede ejecutar en Linux | Se puede utilizar en Linux | Equivalente |
| Dificultad de Uso | Requiere estudiar en que se basan los ataques para poder utilizar la herramienta. | Es muy fácil de utilizar solo hay que leer lo que pide la interfaz | Fern es mucho más fácil de usar, pero Aircrack tiene una herramienta que se llama airoscript que facilita su uso. |
| Interfaz Grafica | No es una interfaz gráfica, pero sí que es un menú de opciones en una terminal | Si | Fern tiene, pero airoscript es también una interfaz gráfica, aunque mucho más simple y no hace uso del ratón. |
| Tiempo en estar Operativo | 10 o 15 segundos | En 5 y 10 segundos | Muy breve en ambas |
| Requisitos Mínimos. | Requiere tener una tarjeta de red WIFI que se pueda poner en modo monitor | Necesita poder utilizar una tarjeta de red wifi en modo monitor | Equivalente |
| Manual | El manual ayuda mucho a la utilización del programa | Tiene un buen manual, ayuda a entender cómo realizar los ataques | Equivalente |
| Tiempo de Ejecución. | Depende del tipo de ataque y del tamaño del diccionario. Ataque WPA 10 a 60 min | Depende del tipo de ataque y del tamaño del diccionario. Ataque WPA 10 a 60 min | Equivalente |
| Tipos de Escaneo | Puede hacer escaneos solo por redes WEP o solo por redes WPA y también puede escanear sin filtros, que escanea todos los tipos de redes | Puede escanear por redes WPA y por redes WEP. No hace escaneos sin filtros. | Aircrack-NG puedes hacer escaneos sin filtros. |
| Recomendación de Ataque | Si recomienda atacar a las redes a las que la señal es más fuerte y a las redes con peor seguridad. | No recomienda a que red atacar. | Aircrack-NG marca con un símbolo al lado de la MAC la mejor red para atacar. |

# 8. Conclusiones

Después del desarrollo de ambos prototipos extremos varias conclusiones.

En primer lugar, queremos y consideramos que es riguroso, indicar que nuestros prototipos han consistido en el desarrollo de múltiples pruebas y escenarios, no tratándose de un desarrollo de código, salvo en el caso de un pequeño script para una de las pruebas.

Destacamos que de estas pruebas hemos extraído valiosa información, por ejemplo, que el hardware a nivel de procesamiento, que en un principio podía parecer una de las limitaciones más importantes de estas herramientas, no lo es. Indicamos esto porque obtener una clave sin un diccionario se torna tremendamente difícil y superados un numero determinado de caracteres, entorno a los 8, el tiempo medio de ataque se dilata tanto que deja de ser una operación viable, por lo menos, con los recursos de que se puede disponer con cierta normalidad.

Además de esto, también determinamos que el principal elemento diferenciador entre ambas herramientas, la interfaz, que en un principio pensábamos que iba a ser un factor determinante en la usabilidad, puede llegar a ser un factor determinante, pero en contra. Explicamos esto, la consola de comandos es necesaria con ambas tecnologías, pero llegado un determinado momento en el prototipo de Fern, se deja de usar, y se comienza a usar la interfaz gráfica, pero la dificultad que puede suponer no disponer de interfaz grafica existe en ambas tecnologías, con el agravante de que Fern no permite valerse de los recursos propios de la consola de comandos, como el uso de scripts para automatizar o la mayor velocidad que puede tener un usuario con cierta experiencia.

Asimismo, aunque Aircrack puede parecer en un principio más compleja, por lo anteriormente expuesto, es una herramienta que transmite mucha más información durante su uso, por un lado, en cierta manera te enseña como se realizan los ataques y por otro lado sabes en cada momento que clase de ataque se esta haciendo, ofrece un mayor control.

Por estas razones concluimos que Aircrack-ng es una herramienta más completa y mejor en todos los aspectos y solo recomendaríamos el uso de Fern Wifi para un usuario con ninguna experiencia.