**1. Autores del trabajo, planificación y entrega**

**1.1 Autores**

En este apartado se debe indicar el número de grupo y los nombres de los autores, poniendo en primer lugar al coordinador del grupo.

**1.2 Planificación**

En este apartado se debe incluir un enlace (URL) compartido a la planificación del trabajo utilizando una herramienta online de diagramación Gantt (por ejemplo, GanttPro, versión gratuita).

Hay que tener en cuenta que cada participante del grupo debe tener asignadas tareas que sumen al menos 45 horas. El peso de este trabajo en la calificación total de la asignatura es de un 30%, por tanto requiere de una dedicación de 45 horas del total de 150 horas de la asignatura.

**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:

* 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 WEP |
| RF02 | El sistema deberá utilizar el protocolo de encriptación WPA2 |
| RF03 | El sistema será capaz de utilizar una tarjeta de red en modo monitor |
| RF04 | El sistema será capaz de absorber trafico de paquetes de red wifi |
| RF05 | El sistema será capaz de inyectar trafico en la red objetivo |
| RF06 | El sistema será capaz de realizar ataques de des autenticación |
| RF07 | El sistema deberá ser capaz de realizar ataques de fuerza bruta |
| RF08 | El sistema deberá sacar los resultado del ataque en documento de texto |
| RF09 | El sistema será capaz de capturar el trafico los datos necesarios para elaborar un handshake |
| RF10 | El sistema será capaz de realizar ataques chopchop (protocolo WEP) |

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: 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.*

**3.3 Criterio 3: 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.*

**3.4 Criterio 4: 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).*

**3.5 Criterio 5: 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).*

**3.6 criterio 6: 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).*

**3.7 criterio 7: 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).*

**3.8 Criterio 8: Dificultad de uso.**

*Nombre del criterio: Dificultad*

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

*Tipo de valor: Horas.*

**3.9 Criterio 9: 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.*

**3.10 Criterio 10: 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.*

**3.11 Criterio 11: Requisitos mínimos.**

*Nombre del criterio: Requisitos*

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

*Tipo de valor: Texto libre.*

**3.12 Criterio 12: Manual.**

*Nombre del criterio: Manual*

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

*Tipo de valor: Texto libre.*

**3.13 Criterio 13: 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.*

**3.14 Criterio 14: 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.*

**3.15 Criterio 15: 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**

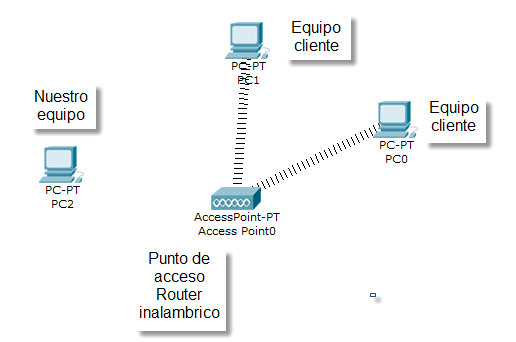
El prototipo se va a dividir en 2 videos en los que se va a explicar y a ejecutar dos ataques a redes wifi, uno con protocolo de seguridad WEP y otro con el protocolo de seguridad WPA.

En el caso del protocolo de seguridad WEP, se va a enseñar como lanzar un ataque “chopchop” con el que se podrá descifrar la contraseña de dicha red wifi.

En el caso del protocolo de seguridad WPA2, se va a enseñar como realizar ataques de des autenticación 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.

**4.1.1Diseño de la red**

La red a la que se va a intentar crackear la contraseña va a ser una red wireless, mas 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 va a ser 2 ataques a redes wifi a través de la tecnología Aircrack-ng, debemos documentar los dos tipos de ataque por separado, a pesar de que tengan cosas en común.

**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].**

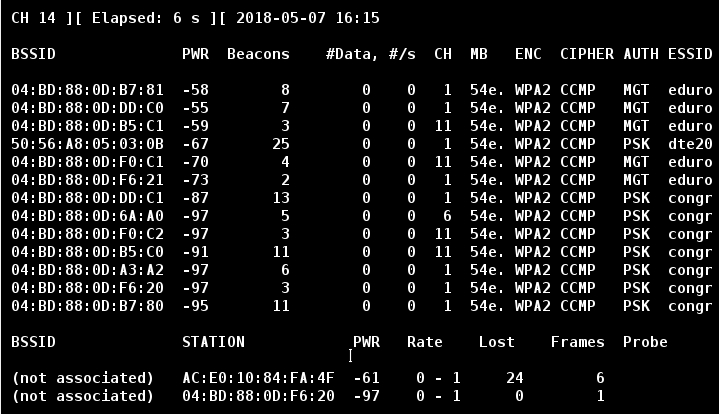
FOTO MODO MONITOR



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]**

FOTO REDES WIFI DISPONIBLES

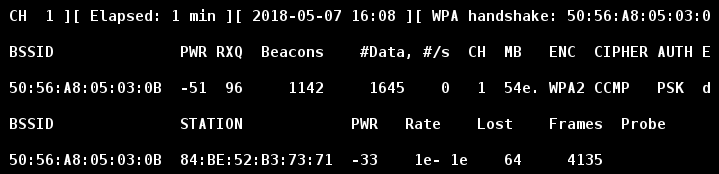




Una vez que hemos encontrado la red que queremos atacar, abrimos otra terminal para capturar los datos del handshake. Estos datos son los que nos van a ayudar a descifrar la contraseña de la red con un ataque de fuerza bruta, que es la manera para descifrar claves WPA2. Para ello, utilizamos el siguiente 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].**

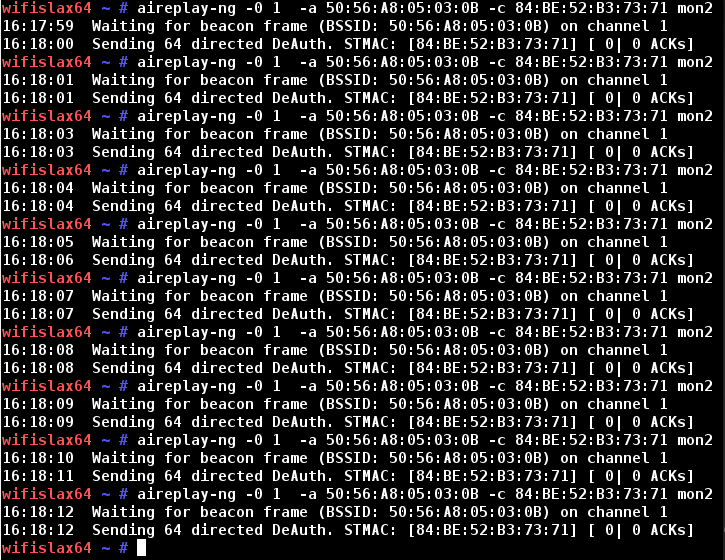
FOTO CAPTURA HANDSHAKE





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].**

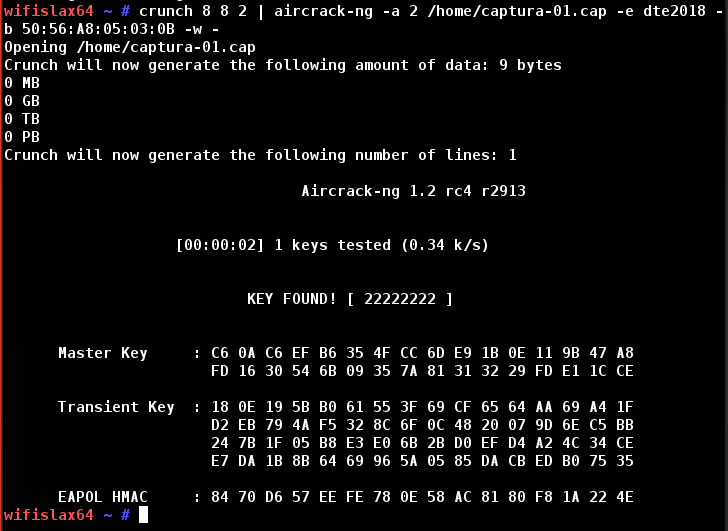
FOTO ATAQUE DE DESAUTENTICACION



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 -].**

FOTO ATAQUE FUERZA BRUTA



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

FOTO CONECTADO A LA RED

**4.2.2 Documentación ataque WEP**

Igual que en el caso de WPA2, tenemos que conectar una tarjeta de red wifi externa:



Igual que antes, ponemos la tarjeta de red en modo monitor. Para ello, abrimos una terminal y utilizamos el siguiente comando: **airmon-ng start [Nombre de la interfaz de la tarjeta de red].**

FOTO MODO MONITOR

Para realizar este ataque, vamos a utilizar la herramienta airoscript-ng, la cual nos va a ir guiando para realizar el ataque. Lo primero que nos va a pedir es la tarjeta de red a utilizar, le indicamos la que anteriormente hemos puesto en modo monitor:

FOTO ELEGIR TARJETA DE RED

Después elegimos la opción 1 de escanear y escaneamos solo las redes WEP:

FOTO MENU y FOTO BUSCAR REDES

Una vez que hemos encontrado la red que queremos atacar lo podemos parar con ctrl + C y volver al menú principal. Y pulsamos la opción seleccionar para seleccionar la red que queremos atacar:

FOTO SELECCIONAR OBJETIVO

Y no seleccionamos ningún cliente, solo la red. A continuación, en el menú principal seleccionamos la opción de atacar y dentro del menú de ataques seleccionamos el ataque chochop:

FOTO MENU ATAQUES

Seleccionamos la opción chopchop y se nos abrirán 3 ventanas, una arriba a la izquierda que informa de los datos que se están obteniendo de la red, otra abajo a la derecha de la pantalla, que informa de la interacción entre la tarjeta de red y el router objetivo y otra a la izquierda abajo en la que se va a interactuar indicando que si se quiere hacer el ataque con la letra “y”. Una vez que pulsamos la “y” se va a ir generando más datos para sacar la clave.

FOTO TRES VENTANAS

Como este ataque puede tardar mucho, porque se necesita muchos datos que almacenar (entre 20000 y 40000 DATA), cuando acabe el primer ataque, volvemos a la terminal de airoscript-ng y podremos hacer una inyección de trafico con la opción “Chopchop inyection”.

FOTO MENU

Una vez lo seleccionemos, en la ventana con la que hemos interaccionado anteriormente nos volverá a pedir que pongamos la letra “y” y la ponemos para llevar a cabo el ataque:

FOTO DE CÓMO SUBE EL NUMERO DE DATA

Una vez que tenemos DATA suficiente, volvemos a la ventana de airoscript-ng y pulsamos la opción de crackear y nos saldrá un menú y le indicaremos la opción de aircrack-ng y si tenemos los datos suficientes descifraremos la clave, si no es asi, cerramos la ventana y volvemos ha realizar el proceso de crackeo:

FOTO VENTANA PRINCIPAL

FOTO ELEGIR FORMA DE CRACKEO

FOTO CONTRASEÑA ENCONTRADA

**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.

FOTO NO ESTA LA CONTRASEÑA EN EL DICCIONARIO

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.

FOTO NO ESTA LA CONTRASEÑA EN EL DICCIONARIO

**4.4 Documentación de instalación**

Para instalar Aircrack-ng lo mas fácil es instalar una maquina virtual con un sitema 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 paginas web oficiales y descargarlos:

Virtualbox

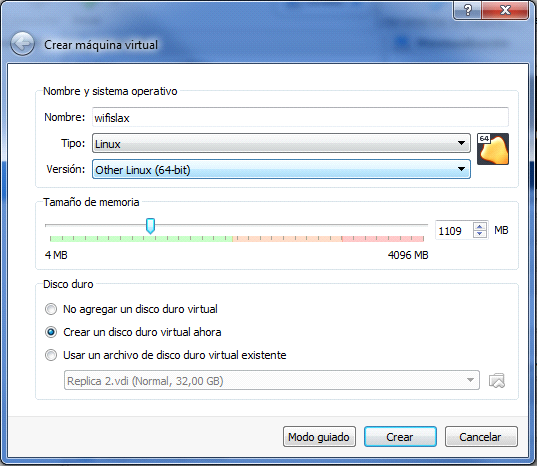


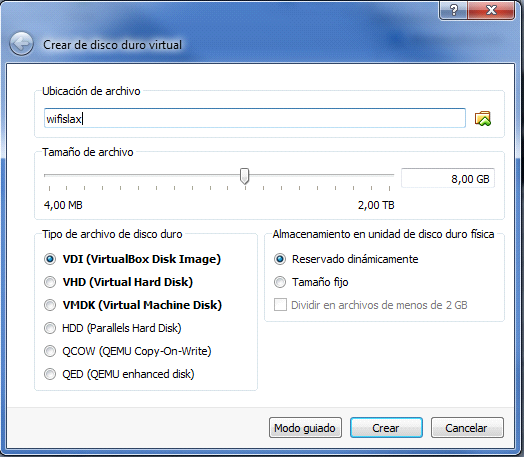
Wifislax



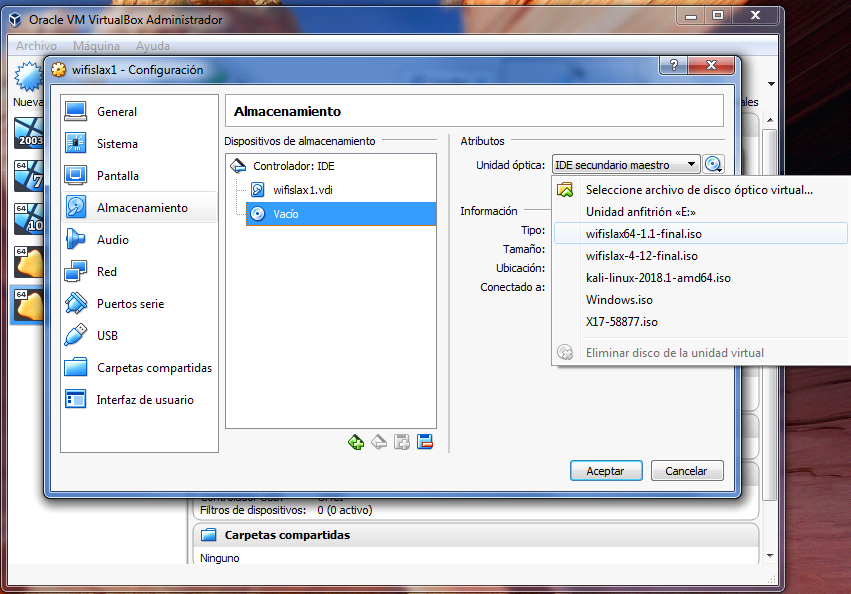
Una vez que los hemos descargado, solo falta crear la maquina virtual con la imagen del sistema operativo y tendremos todo preparado para utilizar el programa aircrack-ng.

Creamos la maquina virtual:





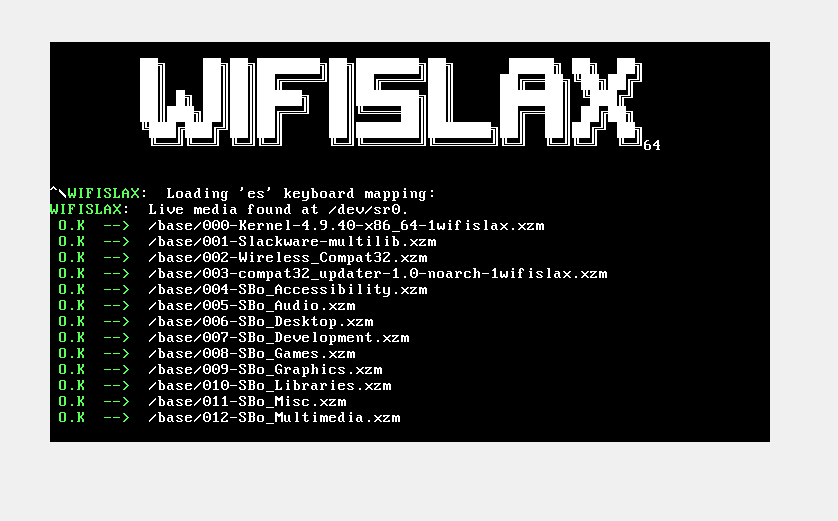
Le asociamos la imagen del sistema operativo:



Y la iniciamos:



Seleccionamos la primera opción:





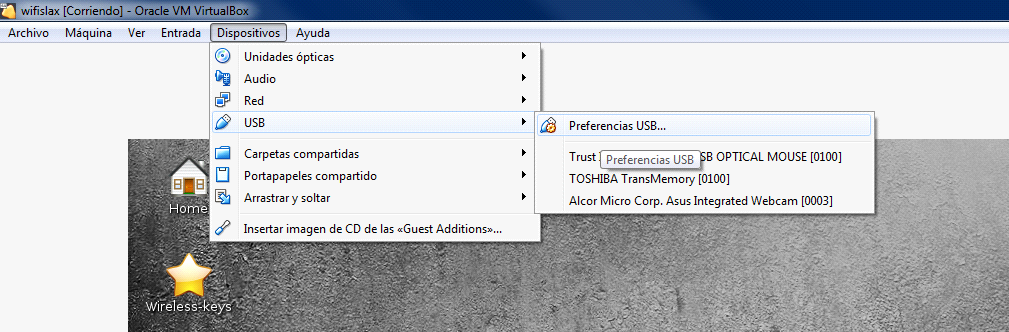
Y ya podemos iniciar la maquina.

**4.5 Manual de usuario**

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

FOTO MAQUINA VIRTUAL Y AIRCRACK PREPARADO

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 B**

Se trata de incluir en este apartado la documentación del desarrollo del proyecto de implementación, utilizando la tecnología B, del sistema cuyos requisitos funcionales se enumeraron en el apartado 2.

**5.1 Documentación de diseño**

Hay que incluir la descripción del diseño del prototipo, incluyendo diagramas, y el diseño de la interfaz de usuario.

**5.2 Documentación de construcción**

Hay que incluir una descripción de la construcción del prototipo, incluyendo algún extracto de código fuente. No es necesario todo el código. Sólo algún extracto para ver cómo se ha comentado.

**5.3 Documentación de pruebas**

Casos de prueba establecidos y resultados de las pruebas y acciones de corrección. No es creíble que no hayan aparecido errores en los caso de prueba.

**5.4 Documentación de instalación**

Descripción suficiente para que una persona que no ha participado en el proyecto pueda instalar el prototipo.

**5.5 Manual de usuario**

Descripción suficiente para que una persona que no ha participado en el proyecto pueda utilizar toda la funcionalidad que ofrece el prototipo. Que debe coincidir con los requisitos funcionales incluidos en el apartado 2.

**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 |  |
| Calidad de los resultados |  |
| Tiempo de Ejecución |  |
| Ataque WEP |  |
| Ataque WPS |  |
| Ataque Simultáneos |  |
| Sistema Operativos |  |
| Dificultad de uso |  |
| Interfaz grafica |  |
| Tiempo en estar operativo |  |
| Requisitos Mínimos |  |
| Manual |  |
| Tiempo de ejecución |  |
| Tipos de escaneo |  |
| Recomendación de ataques. |  |

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 |  |
| Calidad de los resultados |  |
| Tiempo de Ejecución |  |
| Ataque WEP |  |
| Ataque WPS |  |
| Ataque Simultáneos |  |
| Sistema Operativos |  |
| Dificultad de uso |  |
| Interfaz grafica |  |
| Tiempo en estar operativo |  |
| Requisitos Mínimos |  |
| Manual |  |
| Tiempo de ejecución |  |
| Tipos de escaneo |  |
| Recomendación de ataques. |  |

**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 |  |  |  |
| Calidad de los resultados |  |  |  |
| Tiempo de Ejecución |  |  |  |
| Ataque WEP |  |  |  |
| Ataque WPS |  |  |  |
| Ataque Simultáneos |  |  |  |
| Sistemas Operativos |  |  |  |
| Dificultad de Uso |  |  |  |
| Interfaz Grafica |  |  |  |
| Tiempo en estar Operativo |  |  |  |
| Requisitos Mínimos. |  |  |  |
| Manual |  |  |  |
| Tiempo de Ejecución. |  |  |  |
| Tipos de Escaneo |  |  |  |
| Recomendación de Ataque |  |  |  |

**8. Conclusiones**

A partir de la información incluida en el apartado 7 y de la experiencia al realizar el trabajo, el grupo debe estar en condiciones de manifestar su opinión sobre la implementación del sistema utilizando ambas tecnologías, y debe plasmarla en este apartado, indicando las ventajas e inconvenientes más relevantes de utilizar una u otra tecnología para implementar el sistema.

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

(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.)