Vulnerabilidades en redes Wifi

María Elena Fernández-Oliva Madrigal
Máster en Ingeniería de Telecomunicación
Área de Telemática

Jose Lopez Vicario
Xavi Vilajosana Guillen

7 de enero de 2020

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Vulnerabilidades en redes Wifi*
Nombre del autor:	*María Elena Fernández-Oliva Madrigal*
Nombre del consultor/a:	*José López Vicario*
Nombre del PRA:	*Xavi Vilajosana Guillen*
Fecha de entrega:	01/2020
Titulación:	*Máster en Ingeniería de Telecomunicación*
Área del Trabajo Final:	*Telemática*
Idioma del trabajo:	*Español*
Palabras clave	*Vulnerabilidades, Wireless, Protección*

Resumen del Trabajo:

En este documento se hace un estudio de las redes Wifi, con la finalidad de concienciar al lector de las vulnerabilidades de estas redes debido a su naturaleza insegura que hace muy fácil un ataque a su red si no se siguen los protocolos y medidas pertinentes.

Este documento es adecuado tanto para lectores que no tengan conocimientos previos de redes, como para aquellos con conocimientos medios que quieran hacer auditorías de red para conocer sus puntos débiles y hacerlas más seguras.

Para ello, se divide el documento en tres partes: primero, se hace una contextualización de las redes Wireless donde se conocen sus principales elementos y arquitectura, en segundo lugar, se explican los diferentes protocolos que existen en la actualidad (WEP, WPA y WPA2) finalizando con una comparativa entre ellos, por último, en la parte práctica se realizan diferentes ataques con el fin de que el lector pueda protegerse ante estos, dando consejos de seguridad que el lector pueda aplicar a sus propias redes.

Finalmente, se concluye que el protocolo que se debe utilizar es WPA2, demostrando la importancia de la encriptación en estas redes. También se concluye que se debe cambiar la contraseña del punto de acceso por defecto y la importancia de incorporar contraseñas fuertes. También se recomienda tener siempre actualizados los puntos de acceso y dispositivos de una red, además de tomar medidas de seguridad extra como filtrado por MAC. Por último, se comentan varias herramientas con las que el lector puede hacer auditorias de red.

Abstract:

This document is a study of the Wi-Fi networks, and it pretends to raise the reader's awareness of the vulnerabilities of these networks due to their insecure nature, that makes an attack on their network very easy if proper protocols and measures are not followed

This document is suitable for readers who do not have prior knowledge of networks, as well as for those with average knowledge who want to audit their network to know their weaknesses and make it more secure.

To do this, the document is divided into three parts, first, there is a contextualization of the Wireless networks where the reader can understand its main elements and architecture, secondly, the different protocols that exist today are explained (WEP, WPA and WPA2) ending with a comparison between them, finally, in the practical part different attacks are carried out so the reader can protect himself against them, giving security advices that can be applied on his own networks.

Finally, it is concluded that the protocol that must be used is WPA2, demonstrating the importance of encryption in these networks. It is also concluded that the default password of the access point must be changed and the importance of incorporating strong passwords. It is also recommended to always update the access points and devices on a network, in addition to taking extra security measures such as MAC filtering. Finally, several tools with which the reader can perform network audits are discussed.

Índice

Lista de figuras

Aviso legal:

El objetivo de este documento es meramente educativo, y todas las pruebas y herramientas deben utilizarse con dispositivos propios o teniendo permiso para utilizarlas por parte del propietario de la red.

El uso indebido de la información de este documento puede dar lugar a cargos penales contra las personas en cuestión.

Estas herramientas deben utilizarse para realizar ataques a redes propias para identificar sus vulnerabilidades y poder mitigarlas para así poder protegerse frente a posibles atacantes.

Información adicional:

En las capturas realizadas se ocultarán las direcciones MAC de los dispositivos y los nombres completos de las redes por motivos de seguridad y privacidad.

1. Introducción

1.1 Contexto y justificación del Trabajo

Hoy en día las redes Wifi son utilizadas en una gran variedad de ámbitos personales y profesionales, en ordenadores portátiles, televisiones, teléfonos móviles, consolas, reproductores de música, etc. Las redes Wifi son cada vez más populares gracias a la movilidad, la comodidad y la facilidad de conexión que estas ofrecen, ya que las señales se transmiten a través de radiofrecuencia por el aire sin necesidad de conexión física con un punto de acceso. El problema de este tipo de conexiones son los riesgos de seguridad que dichas facilidades conllevan, y mientras en las redes cableadas es necesario un acceso físico a la red, en las redes inalámbricas un usuario ajeno a la red podría interceptar los paquetes que se transmiten o incluso modificar o inyectar nuevos paquetes a la red sin necesidad de conexión física, simplemente estando en un lugar donde alcance la cobertura de dicha red.

Conscientes de la importancia de la seguridad de las redes Wifi, se han desarrollado algoritmos de seguridad, que han ido pasado por muchos cambios y mejoras desde los años 90 para hacerse más seguros y eficaces, incluso actualmente se siguen desarrollando nuevos algoritmos.

WEP, WPA y WPA2 son los algoritmos de seguridad inalámbrica utilizados actualmente, y que tratan de evitar que usuarios no deseados se conecten a la red, además de ofrecer cifrado de datos.

1.2 Objetivos del Trabajo

Los objetivos principales son los siguientes:

- Realizar un estudio de las redes con un enfoque en las Wireless, desde los tipos de redes que existen o los elementos que la componen hasta los estándares que se utilizan.

- Comprender los diferentes tipos de algoritmos de seguridad, sus características, funcionamiento y encriptación.

- Hacer un análisis de las vulnerabilidades que se encuentran hoy en día, comprobando si realmente se pueden vulnerar y la facilidad o dificultad con la que se puede hacer.

- Ofrecer consejos de seguridad para aumentar la seguridad en el ámbito de las redes Wireless.

1.3 Enfoque y método seguido

Para alcanzar estos objetivos, se divide el proyecto en las siguientes fases:

- Fase inicial, elección de la temática, definición de objetivos y planificación del trabajo.

- Fase de investigación, primera toma de contacto, comprensión del funcionamiento general de las redes wifi, sus componentes principales y características, profundizaje en la seguridad, estudio de los diferentes algoritmos de seguridad y su evolución. Conclusión de la fase con la elaboración de los puntos 2 y 3 del documento.

- Fase de investigación de las distintas vulnerabilidades conocidas en cada algoritmo, investigación en organismos gubernamentales, en empresas fabricantes, en libros enfocados a la seguridad y en blogs de ciberseguridad.

- Fase de investigación de los diferentes ataques que se pueden realizar a las redes wifi, recogida de información de códigos de GitHub, de diferentes plataformas para realizar auditorías/ataques, publicaciones de agencias de seguridad, etc.

- Montaje del laboratorio de testeo, configuración de los puntos de acceso que serán atacados, instalación de las herramientas necesarias. y realización de diferentes ataques a redes Wifi. Se concluye con la elaboración del documento en el que se recoge el resultado de las pruebas realizadas.

- Realización del punto final: Conclusiones.

- Elaboración de la presentación del proyecto

1.4 Planificación del Trabajo

Para llevar a cabo el proyecto se realiza la siguiente planificación temporal inicial expuesta en la tabla:

Title	Start date	Due date
Vulnerabilidades en redes WiFi		
Elección de la temática	9/19/19	9/19/19
Entrega inicial de la elección de la temática	9/25/19	9/25/19
Investigación y documentación general sobre redes Wifi	9/19/19	9/25/19
PEC 1 - Plan de trabajo	9/25/19	10/2/19
Investigación inicial: Redes Wifi en la actualidad	9/25/19	9/27/19
Elaboración del punto 1.1: Contexto y justificación del trabajo	9/30/19	9/30/19
Elaboración del punto 1.2: Objetivos del trabajo	9/30/19	9/30/19
Investigación inicial: Algoritmos de seguridad	9/25/19	9/30/19
Elaboración del punto 1.3: Enfoque y método que se seguirá	10/1/19	10/1/19
Elaboración del punto 1.4: Planificación del trabajo	10/1/19	10/1/19
PEC 2 - Primera entrega del proyecto	10/2/19	11/13/19
Investigación inicial: Protocolos de seguridad de redes Wifi	10/2/19	10/14/19
Análisis profundo del protocolo de seguridad WEP	10/14/19	10/21/19
Elaboración del punto 2.1: Protocolo WEP	10/21/19	10/25/19
Análisis profundo del protocolo de seguridad WPA	10/25/19	11/1/19
Elaboración del punto 2.2: Protocolo WPA	11/1/19	11/4/19
Análisis profundo del protocolo de seguridad WPA2	11/4/19	11/11/19
Elaboración del punto 2.3: Protocolo WPA2	11/11/19	11/13/19
PEC 3 - Segunda entrega del proyecto	11/13/19	12/18/19
Investigación sobre las vulnerabilidades en WEP	11/13/19	11/18/19
Elaboración del punto 3.1: Vulnerabilidades WEP	11/18/19	11/19/19
Investigación sobre las vulnerabilidades en WPA	11/19/19	11/22/19
Elaboración del punto 3.2: Vulnerabilidades WPA	11/22/19	11/25/19
Investigación sobre las vulnerabilidades en WPA2	11/25/19	11/28/19
Elaboración del punto 3.3: Vulnerabilidades WPA2	11/28/19	11/29/19
Investigación sobre posibles ataques a redes Wifi	11/29/19	12/6/19
Montaje del laboratorio de pruebas	12/6/19	12/11/19
Realización de los ataques a redes Wifi	12/12/19	12/16/19
Elaboración del punto 4: Parte práctica	12/16/19	12/18/19
Elaboración de las conclusiones del proyecto	12/18/19	12/23/19
Elaboración de la memoria final	12/23/19	1/7/20
Realización de la presentación del proyecto	1/7/20	1/10/20

Ilustración 1: Planificación inicial del trabajo

Utilizando un diagrama de Gantt se ven los diferentes hitos de forma general:

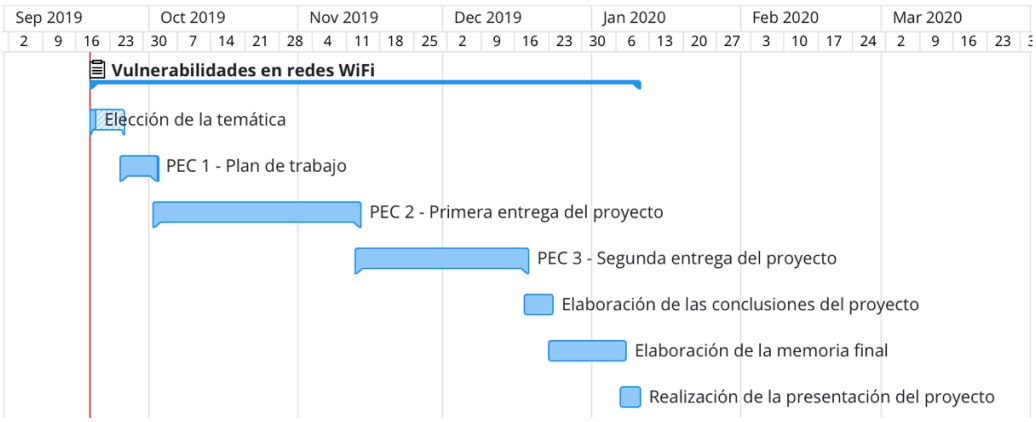


Ilustración 2: Diagrama de Gantt de la planificación inicial

A continuación, se ven los hitos desglosados:

Ilustración 3: Diagrama de Gantt de la planificación inicial desglosada

Durante la evolución del proyecto, la evolución temporal ha sufrido los siguientes cambios:

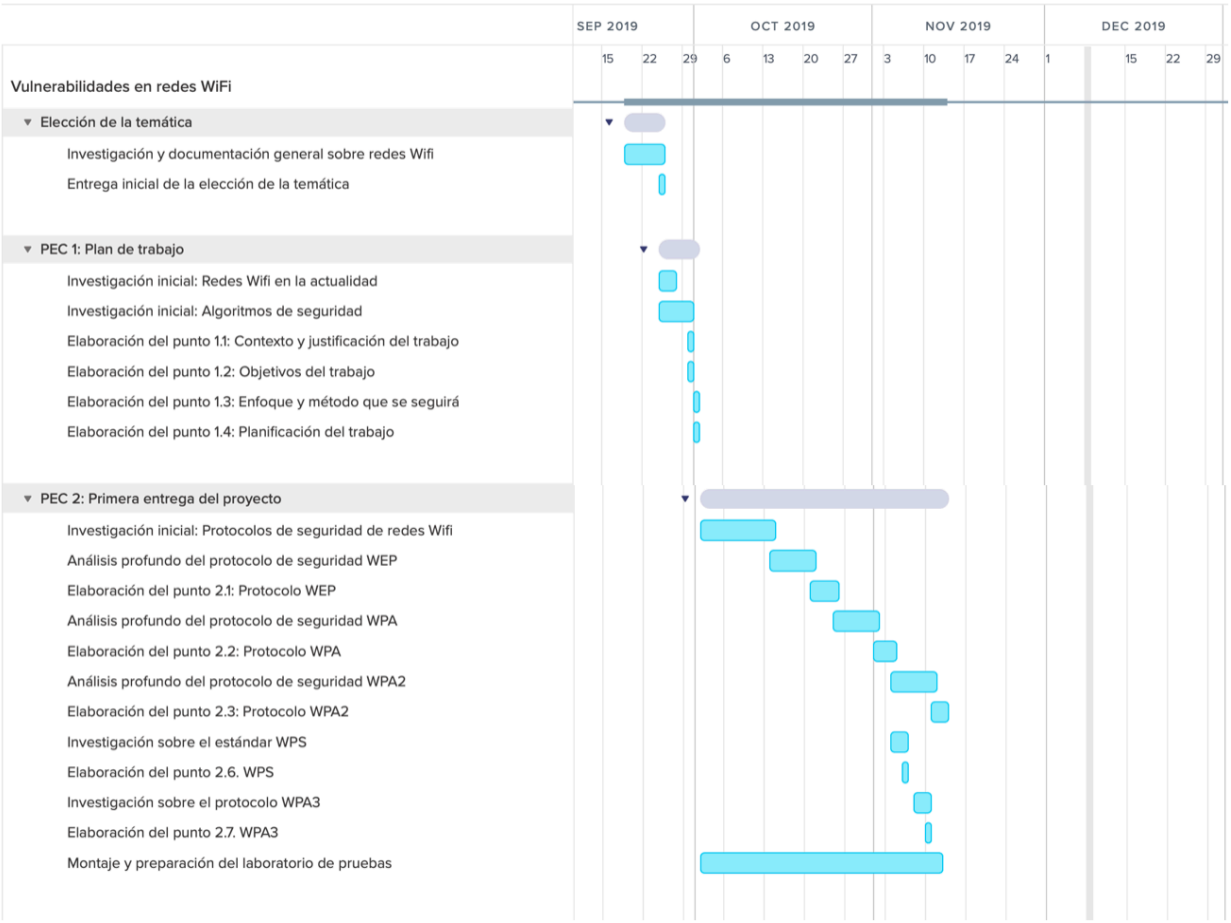


Ilustración 4: Modificaciones en el diagrama de Gantt en las PEC1 y PEC2

En primer lugar, para la primera entrega del proyecto (PEC2) se añaden los puntos de investigación del estándar WPS y del protocolo WPA3, ya que, por un lado, el estándar WPS trabaja junto con los protocolos de seguridad actuales, y por tanto se incluye en el documento, por otro lado, actualmente se está desarrollando el nuevo protocolo WPA3 y también ha resultado interesante incluirlo.

Finalmente, y como la parte práctica puede llevar bastante tiempo, se decide realizar el montaje del laboratorio en paralelo con esta PEC2, ya que la instalación correcta de una máquina virtual, las posibles incompatibilidades de sistemas operativos o antenas que se puedan encontrar, etc., es un aspecto clave para poder realizar las pruebas a tiempo.

Para la PEC3 también se realizan cambios en la planificación, que quedaría de la siguiente manera:

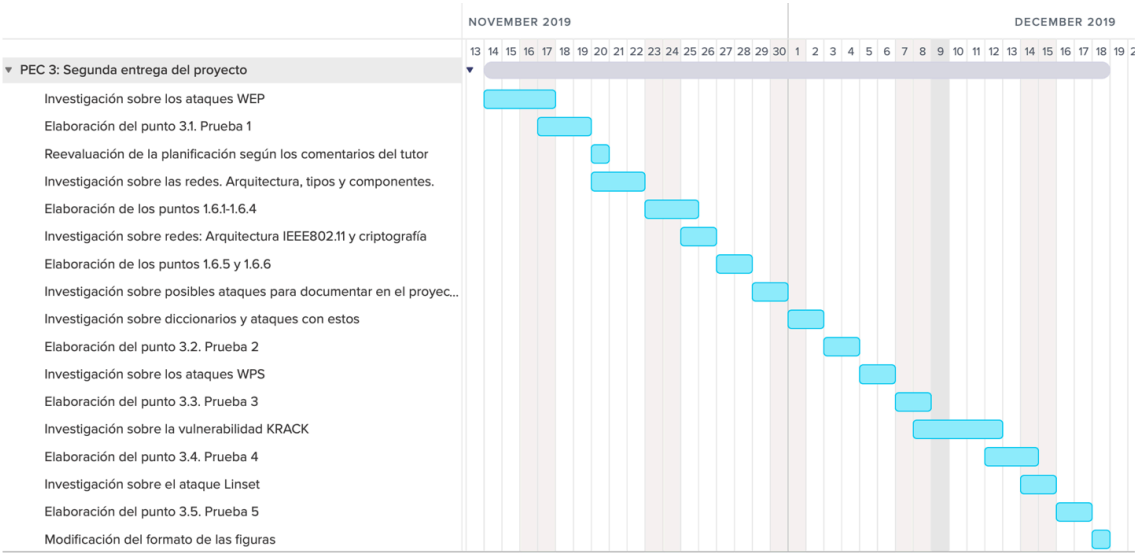


Ilustración 5: Modificaciones en el diagrama de Gantt en la PEC3

Al ver diferentes proyectos, se cambia la planificación de las pruebas para adecuarlas más a simular situaciones en las que el lector se puede encontrar en su red Wifi, y así aportar consejos de seguridad más convenientes.

Adicionalmente, se amplía la contextualización del proyecto, añadiendo en el punto 2 una introducción a las redes, arquitectura de las redes en los modos ISO y TCP/IP, tipos de redes, elementos que conforman una red, arquitectura IEEE.802.11 y criptografía.

Por último, se añade la última parte de la planificación: Entrega de la memoria final:

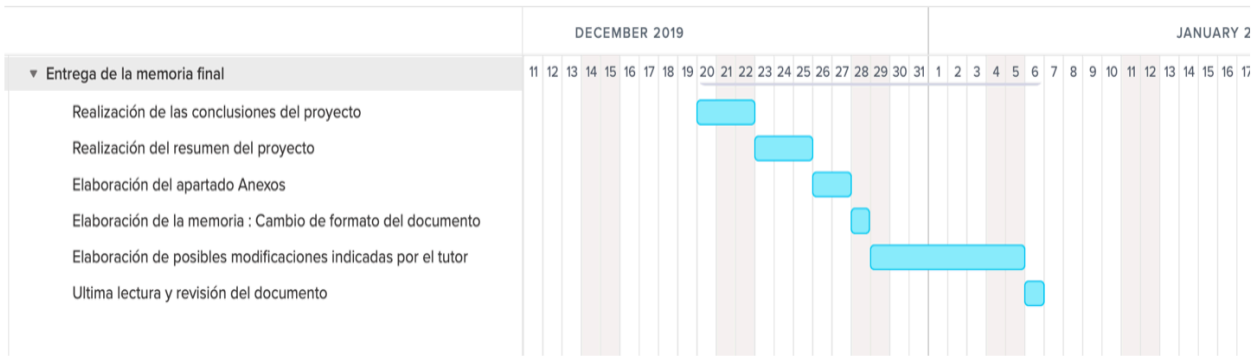


Ilustración 6: Diagrama de Gantt de la entrega de la memoria final

La planificación queda finalmente de la siguiente manera:

		Start Date	End Date
1	Vulnerabilidades en redes WiFi	2019-09-19	2020-01-06
1.1	Elección de la temática	2019-09-19	2019-09-25
1.1.1	Investigación y documentación general sobre redes Wifi	2019-09-19	2019-09-25
1.1.2	Entrega inicial de la elección de la temática	2019-09-25	2019-09-25
1.2	PEC 1: Plan de trabajo	2019-09-25	2019-10-01
1.2.1	Investigación inicial: Redes Wifi en la actualidad	2019-09-25	2019-09-27
1.2.2	Investigación inicial: Algoritmos de seguridad	2019-09-25	2019-09-30
1.2.3	Elaboración del punto 1.1: Contexto y justificación del trabajo	2019-09-30	2019-09-30
1.2.4	Elaboración del punto 1.2: Objetivos del trabajo	2019-09-30	2019-09-30
1.2.5	Elaboración del punto 1.3: Enfoque y método que se seguirá	2019-10-01	2019-10-01
1.2.6	Elaboración del punto 1.4: Planificación del trabajo	2019-10-01	2019-10-01
1.3	PEC 2: Primera entrega del proyecto	2019-10-02	2019-11-13
1.3.1	Investigación inicial: Protocolos de seguridad de redes Wifi	2019-10-02	2019-10-14
1.3.2	Análisis profundo del protocolo de seguridad WEP	2019-10-14	2019-10-21
1.3.3	Elaboración del punto 2.1: Protocolo WEP	2019-10-21	2019-10-25
1.3.4	Análisis profundo del protocolo de seguridad WPA	2019-10-25	2019-11-01
1.3.5	Elaboración del punto 2.2: Protocolo WPA	2019-11-01	2019-11-04
1.3.6	Análisis profundo del protocolo de seguridad WPA2	2019-11-04	2019-11-11
1.3.7	Elaboración del punto 2.3: Protocolo WPA2	2019-11-11	2019-11-13
1.3.8	Investigación sobre el estándar WPS	2019-11-04	2019-11-06
1.3.9	Elaboración del punto 2.6. WPS	2019-11-06	2019-11-06
1.3.10	Investigación sobre el protocolo WPA3	2019-11-08	2019-11-10
1.3.11	Elaboración del punto 2.7. WPA3	2019-11-10	2019-11-10
1.3.12	Montaje y preparación del laboratorio de pruebas	2019-10-02	2019-11-12

Ilustración 7: Planificación modificada de las PECS 1 y 2.

1.4	PEC 3: Segunda entrega del proyecto	2019-11-14	2019-12-18
1.4.1	Investigación sobre los ataques WEP	2019-11-14	2019-11-17
1.4.2	Elaboración del punto 3.1. Prueba 1	2019-11-17	2019-11-19
1.4.3	Reevaluación de la planificación según los comentarios del tutor	2019-11-20	2019-11-20
1.4.4	Investigación sobre las redes. Arquitectura, tipos y componentes.	2019-11-20	2019-11-22
1.4.5	Elaboración de los puntos 1.6.1-1.6.4	2019-11-23	2019-11-25
1.4.6	Investigación sobre redes: Arquitectura IEEE802.11 y criptografía	2019-11-25	2019-11-26
1.4.7	Elaboración de los puntos 1.6.5 y 1.6.6	2019-11-27	2019-11-28
1.4.8	Investigación sobre posibles ataques para documentar en el proyecto	2019-11-29	2019-11-30
1.4.9	Investigación sobre diccionarios y ataques con estos	2019-12-01	2019-12-02
1.4.10	Elaboración del punto 3.2. Prueba 2	2019-12-03	2019-12-04
1.4.11	Investigación sobre los ataques WPS	2019-12-05	2019-12-06
1.4.12	Elaboración del punto 3.3. Prueba 3	2019-12-07	2019-12-08
1.4.13	Investigación sobre la vulnerabilidad KRACK	2019-12-08	2019-12-12
1.4.14	Elaboración del punto 3.4. Prueba 4	2019-12-12	2019-12-14
1.4.15	Investigación sobre el ataque Linset	2019-12-14	2019-12-15
1.4.16	Elaboración del punto 3.5. Prueba 5	2019-12-16	2019-12-17
1.4.17	Modificación del formato de las figuras	2019-12-18	2019-12-18
1.5	Entrega de la memoria final	2019-12-20	2020-01-06
1.5.1	Realización de las conclusiones del proyecto	2019-12-20	2019-12-22
1.5.2	Realización del resumen del proyecto	2019-12-23	2019-12-25
1.5.3	Elaboración del apartado Anexos	2019-12-26	2019-12-27
1.5.4	Elaboración de la memoria : Cambio de formato del documento	2019-12-28	2019-12-28
1.5.5	Elaboración de posibles modificaciones indicadas por el tutor	2019-12-29	2020-01-05
1.5.6	Ultima lectura y revisión del documento	2020-01-06	2020-01-06

Ilustración 8: Planificación modificada de la PEC3 y la memoria final

1.5 Breve sumario de productos obtenidos

Para realizar la parte práctica se necesitan diferentes softwares que se explicarán con detalle más adelante, además de un punto de acceso que admite el protocolo WEP, un punto de acceso vulnerable a WPS y un punto de acceso obtenido en el momento de la realización de este TFM parcheado. También se necesitará una antena que acepte modo monitor (en este escenario se utiliza la antena Alfa Network AWUS036NH con un chipset Ralink RT3070).

1.6 Breve descripción de los otros capítulos de la memoria

La memoria consta de cuatro capítulos:

- En el primero se comenta el contexto de las redes Wifi, los objetivos y método seguidos a lo largo del trabajo, la planificación inicial y su evolución, y los productos obtenidos.

- En un segundo capitulo se hace una contextualización de las redes Wifi dentro de las redes en general explicando los conceptos básicos de red, arquitectura y tipos de red, así como la particularización en las redes Wifi con sus componentes, la arquitectura IEEE 802.11 y se dan unas breves pinceladas al concepto de criptografía debido a su importancia en las redes Wireless.

- En el tercer capítulo se estudian los diferentes protocolos que se utilizan en las redes wifi en la actualidad (WEP, WPA y WPA2), viendo las características principales de cada uno de ellos, la encriptación que utilizan y la autenticación. Por otro lado, se hace un estudio del estándar WPS, utilizado juntamente con los protocolos WPA y WPA2 para facilitar la conexión de los clientes a la red. Por último, se comenta el protocolo WPA3 con las ventajas que traerá consigo, aunque en el momento de la redacción de este documento todavía no está publicado de manera oficial.

- En el cuarto capítulo se realizarán 5 ataques. En el primero se pondrá a prueba la seguridad de la encriptación del protocolo WEP, en el segundo se pondrá a prueba un punto de acceso con una contraseña débil, además de dar información al lector sobre los diccionarios de contraseñas que son los que contienen las contraseñas débiles. En el tercer ataque se pone a prueba el estándar WPS, explicando por qué se considera inseguro y explicando cómo se puede obtener el PIN WPS. En el cuarto ataque se introduce la última vulnerabilidad del protocolo WPA2

conocido con el ataque KRACK, y se hacen pruebas en diferentes dispositivos para ver si son vulnerables, además de resaltar la importancia de las actualizaciones de software de nuestros dispositivos. El quinto ataque trata de engañar a un usuario de la red para que él mismo proporcione la contraseña del punto de acceso, el objetivo de este último ataque es dar a conocer al lector estas técnicas que realizan los atacantes, para no poder ser engañado y poder protegerse.

- Finalmente se encuentra el apartado de conclusiones del proyecto, que incluye un resumen con las buenas prácticas que se deben seguir para tener una red Wifi segura.

2. Introducción a las redes inalámbricas

Antes de profundizar en los diferentes protocolos de seguridad de las redes Wireless, se quiere exponer en el documento una breve introducción donde se explicarán las diferentes redes Wifi, sus componentes, arquitectura y estándares por los que se rigen.

2.1. ¿Qué es una red?

En primer lugar, se quiere dejar claro con lo que se refiere al hablar de una red. Según la definición numero 10 de la RAE, se define red como un *"Conjunto de computadoras o de equipos informáticos conectados entre sí y que pueden intercambiar información."* Esto aplica tanto a redes cableadas como a redes Wireless (sin cable). Mientras que en la definición más simple se ve que la principal función de las redes es permitir el intercambio de información, según ha ido avanzando la tecnología y las necesidades de la sociedad, las redes se han tenido que ir adaptando para permitir mayor movilidad y comodidad, y de aquí surgen las redes Wireless.

2.2. Arquitectura de redes

Para entender el funcionamiento de una red, es importante entender su estructura, así se ve que las redes se rigen por una estructura de capas en las cuales se agrupan todos los procesos que permiten una comunicación efectiva. Se encuentran dos modelos de capas por excelencia: El modelo OSI y el modelo TCP/IP (o DoD).

El modelo OSI es un modelo jerárquico, que surge para permitir que las redes de diferentes proveedores interoperen dividiendo el proceso de comunicación de la red en componentes más pequeños y simples, lo que facilita el desarrollo, diseño y solución de problemas de los componentes. Además, se estandarizan los diferentes componentes de red, permitiendo tanto la comunicación entre diferentes componentes de software y hardware, como el desarrollo por parte de diferentes proveedores. Además, con el modelo por capas se dividen los desarrollos permitiendo un desarrollo mucho más rápido y eficaz.

En este modelo se encuentran 7 capas, y se ponen diferentes ejemplos en cada una de ellas:

- La capa física: Con protocolos como IEEE 802.11, con USB ethernet o bluetooth, se comunica directamente con los diversos tipos de medios de comunicación enviando y recibiendo bits en la forma necesaria y especificando los requisitos para activar, mantener y desactivar un enlace físico entre sistemas finales.

- La capa de enlace de datos, con PPP, ATM o Ethernet, proporciona la transmisión física de datos y maneja el flujo, la topología y posibles errores.

- La capa de red utiliza protocolos como IP, ARP, ICMP o IPSec, y se encarga de administrar el direccionamiento de dispositivos, buscar la ubicación de los dispositivos en la red y determinar la mejor manera de enviar y recibir datos.

• La capa de transporte utiliza TCP o UDP según el tamaño de los datos a transmitir, la importancia de que se pierda algún paquete, la necesidad de transmisión de manera rápida, etc. Esta capa segmenta y vuelve a juntar los datos en una sola secuencia de datos, y proporciona servicios de transporte de datos de extremo a extremo.

• La capa de sesión, con protocolos como NetBIOS o PPTP, es responsable de configurar, administrar y apagar las sesiones entre usuarios manteniendo separados los datos del usuario, además de controlar el diálogo entre dispositivos.

• La capa de presentación, utilizando protocolos como SSL o TLS actúa como un traductor, presentando la información a la capa de aplicación.

• La capa de aplicación utiliza protocolos como FTP, HTTP, SND, Telnet o SNMP, y es la capa donde los usuarios se comunican directamente con el dispositivo, como por ejemplo en la descarga de archivos o en la visita a una página web.

Por otra parte, el modelo TCP/IP surge también como un modelo de capas jerárquico, pero más “condensado” que el modelo OSI, como se ve a continuación. Este modelo evolucionó rápidamente y quedó bajo el programa del gobierno de los Estados Unidos quien aprobaba cualquier nuevo estándar publicado asegurándose de que pasaban unos mínimos criterios.

En el modelo TCP/IP únicamente se encuentran 4 capas:

- La capa de aplicación (que correspondería a las capas de aplicación, presentación y sesión).
- La capa de transporte (como en OSI).
- La capa de internet (que correspondería a la capa de red del modelo OSI).
- La capa de acceso al medio (que correspondería a las capas física y de enlace de datos).

A continuación, se ilustra en la figura 9 la representación comparativa entre las diferentes capas de los dos modelos:

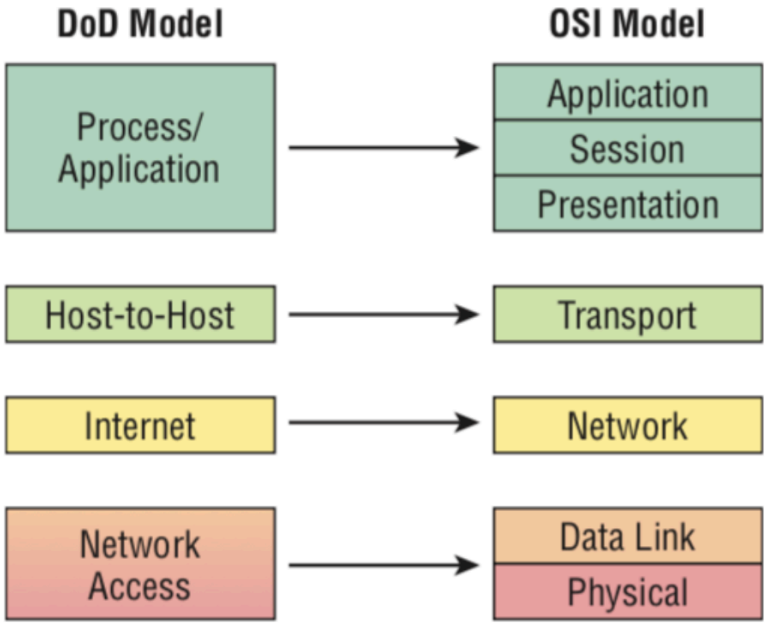


Ilustración 9: Comparativa de los modelos DoD vs OSI, (Lammle, 2013)

En este apartado se han comentado los dos modelos de arquitectura principales que ayudan a comprender el funcionamiento de las redes, pero, aunque es un tema muy extenso e interesante, este documento no se extenderá más en el funcionamiento de las diferentes capas y de los diferentes protocolos. Para aquellos que quieran profundizar en este tema se recomienda la lectura de la guía de estudio del CCNA Routing and switching de Cisco, donde se explica de forma práctica y clara, sin necesidad de conocimientos previos, el proceso de comunicación en las redes. (Lammle, 2013)

2.3. Tipos de redes

Según su alcance se pueden dividir las redes en:

- Red de área personal (1m) o PAN (Personal Area Network).
- Red de área local (10m-1km) o LAN (Local Area Network).
- Red de área metropolitana (10km) o MAN (Metropolitan Area Network).
- Red de área amplia (100km-1000km) o WAN (Wide Area Network).
- Internet (10000km).

En la figura 10 se representan gráficamente los diferentes tipos de redes con los diferentes estándares:

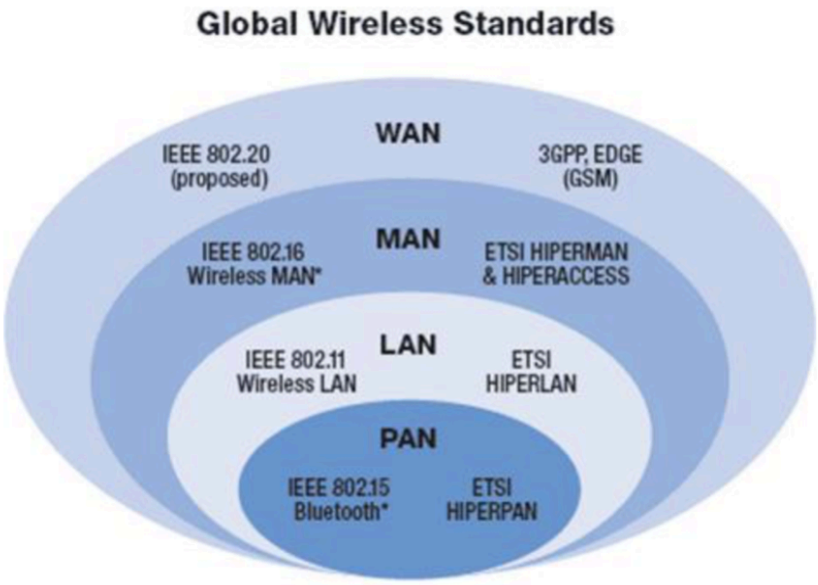


Ilustración 10: Tipos de redes según el alcance

Este documento se centra en las redes de área local (LAN), con un alcance de 10m-1km, basadas en su mayoría en ethernet, ya sea por cable de par trenzado o de forma inalámbrica bajo el estándar IEEE 802.11.

En la siguiente figura se ilustra una Red de área local (LAN), donde la parte a corresponde a una red Wireless y la parte b corresponde a una red cableada.

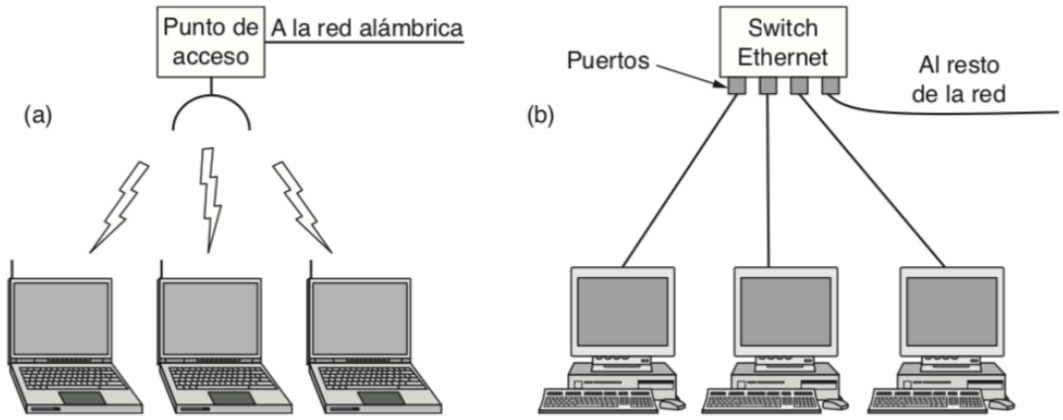


Ilustración 11: Esquema de redes LAN Wireless vs cableadas. (PEARSON, 2012)

(Lammle, 2013) (PEARSON, 2012)

Además, las redes LAN Wireless se pueden dividir en dos tipos según la forma de intercambio de datos desde el punto de vista de los dispositivos que se conectan a la red:

- Redes Ad Hoc: En ellas no hay puntos de acceso ni routers. Los dispositivos se conectan entre sí de forma directa. En la figura 12 se representa de manera visual una red Ad Hoc.

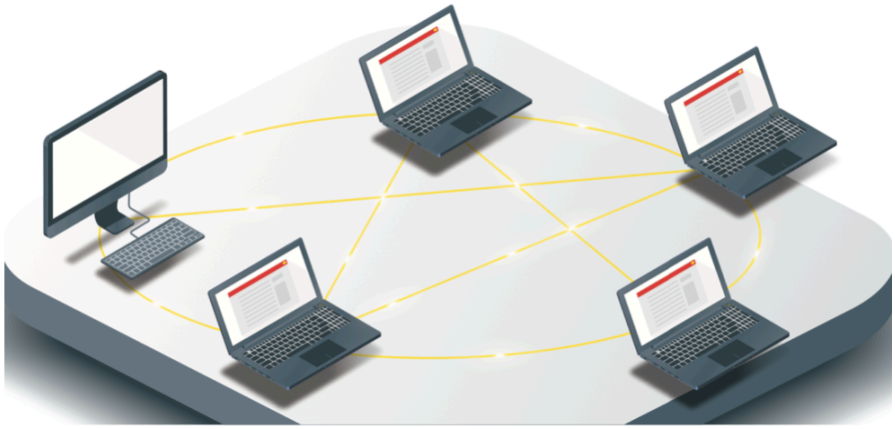


Ilustración 12: Redes Ad hoc, (INCIBE, 2018)

- Redes de infraestructura: Son las redes utilizadas normalmente en empresas y hogares, en ellas se utiliza un router o un punto de acceso por el que se accede a los distintos recursos de red. En la figura 13 se representa una red en modo infraestructura. (INCIBE, 2018)

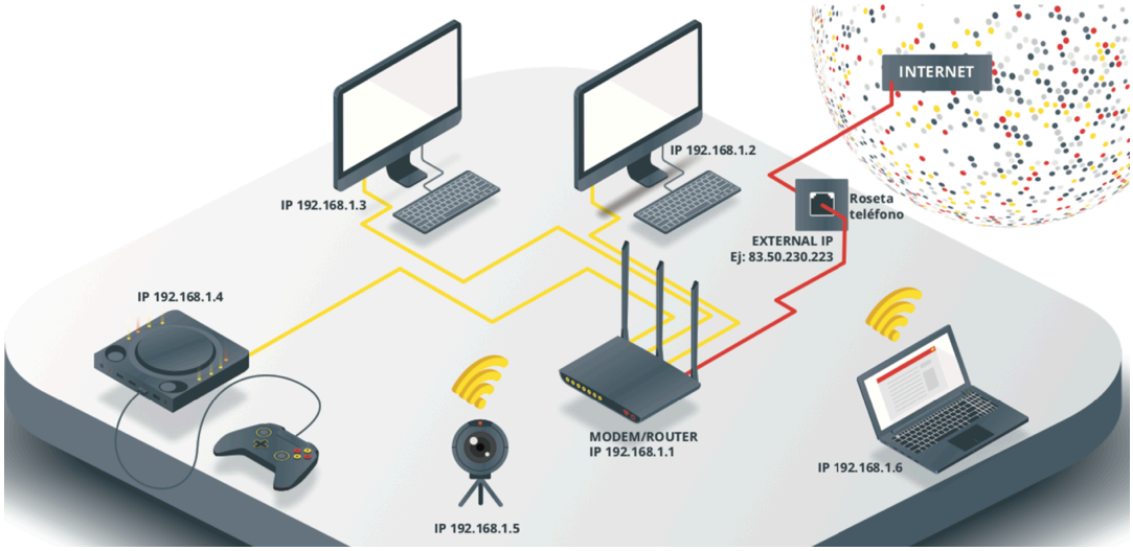


Ilustración 13: Red en modo infraestructura, (INCIBE, 2018)

2.4. Componentes de las redes Wireless

Como se ve en las representaciones anteriores, hay dos elementos clave que componen las redes Wireless: Por un lado, el punto de acceso (disponible solo en modo infraestructura), o Access Point, que es capaz de realizar una conexión entre diferentes dispositivos clientes o entre un dispositivo cliente con el resto de la red. Además, es utilizado como Gateway (o puerta de enlace) hacia internet.

Por otro lado, se encuentran los dispositivos cliente, que pueden ser móviles, tablets, portátiles, etc., y que solicitan la conexión al punto de acceso (en el caso de modo infraestructura), para acceder a la red.

2.5. Arquitectura IEEE 802.11

IEEE 802.11 se introdujo como estándar dedicado a las redes LAN inalámbricas, y es creada por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), que emite una lista de estándares que está en continua expansión. Sus especificaciones se centran en las capas física y de control de acceso al medio del modelo OSI.

- IEEE 802.11 (o IEE802.11 Legacy) se publicó en 1997, y fue el primer estándar de las redes LAN inalámbricas. Aquí se creaba una base sólida desde la que desarrollar reglas comunes, y en esta primera propuesta se permitían velocidades de 1Mbps y 2Mbps en una banda de 2,5GHz.

- IEEE 802.11a se publicó en 1999, y permitía una mayor velocidad de transferencia, contando con hasta 54 Mbps, en una frecuencia de 5GHz.

- IEEE 802.11b también se publicó en 1999. Permite una velocidad máxima de transmisión de 11 Mbps, funcionando en la banda de 2,4 GHz.

- IEEE 802.11c se utiliza para la comunicación entre dos redes diferentes, y permite utilizar en la capa de enlace de datos el IEEE 802.11d, que se comenta a continuación, con dispositivos compatibles con 802.11

- IEEE 802.11d está enfocado a la compatibilidad de dispositivos de manera internacional, permitiendo el intercambio de información en diferentes frecuencias.

- IEEE 802.11e añade características de calidad de servicio evitando cuellos de botella, mejorando la latencia y añadiendo soporte multimedia permitiendo compatibilidad. Por otro lado, añade corrección de errores y mejoras en la integración control de capas, así el estándar permite tráfico a tiempo real cualquier entorno, introduciendo nuevos mecanismos en la capa de control de acceso al medio e introduciendo el llamado HCF (Hybrid Coordination Function).

- IEEE 802.11f se centra en los puntos de acceso, y permite que los productos tengan mayor compatibilidad. Se añade la itinerancia, permitiendo a un cliente cambiarse de un punto de acceso a otro mientras está en movimiento según el punto de acceso más cercano a este. Esto se consigue utilizando el protocolo IAPP.

- IEEE 802.11g fue publicado en 2003, y utiliza la banda de 2,4 GHz con una velocidad de 54 Mbps, (notoriamente mejor que en EEE802.11b, y siendo compatible con este, ya que utiliza las mismas frecuencias).

- IEEE 802.11h fue publicado en 2003 para resolver los problemas que puedan causar la existencia de sistemas radar y satélites, para ello se incluye la capacidad de gestión dinámica de frecuencia y potencia de transmisión. Esto fue derivado de los requerimientos de la ERO (Oficina Europea de Radiocomunicaciones) y por las posteriores recomendaciones de la ITU (Unión Internacional de Telecomunicaciones).

- IEEE 802.11i implementa el WPA2 en 2004, para mitigar las vulnerabilidades de autenticación y codificación.

- IEEE 802.11j fue diseñado principalmente para convivir con las normas japonesas permitiendo la comunicación en las bandas de 4,9 a 5 GHz.

- IEEE 802.11k mejora la gestión de las redes inalámbricas permitiendo que los puntos de acceso puedan calcular y valorar los recursos de los clientes.

- IEEE 802.11n utiliza la tecnología MIMO que permite utilizar varios canales a la vez gracias a la incorporación de varias antenas y trabaja tanto en 2,4 GHz como en 5 GHz. Además, admite una velocidad de 600 Mbps en la capa física.

- IEEE 802.11p trabaja en las frecuencias de 5,90 GHz-6,20 GHz, y está enfocado en comunicaciones de corto alcance que permite la comunicación entre vehículos y estos y dispositivos de carretera, además de WAVE (acceso inalámbrico en entornos de vehículos).

- IEEE 802.11r permite establecer protocolos de seguridad para identificar a un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él, y una transición entre nodos de menos de 50 ms (importante en las comunicaciones VoIP).

- IEEE 802.11v se publica en 2011 y se centra en la configuración vía remota de los dispositivos cliente, permitiendo tanto la configuración como la supervisión y actualización de los clientes.

- IEEE 802.11w está enfocado en mitigar la vulnerabilidad del envío de información del sistema en tramas no protegidas, aumentando la seguridad en la autenticación y la codificación.

- IEEE 802.11ac fue publicada en 2014. y consigue velocidades de 1,3 Gbps en la banda de frecuencia de 5GHz.

- IEEE 802.11ax (o Wifi de 6ª generación) opera en las bandas de 2.4 GHz y 5 GHz e introduce OFDMA mejorando la eficiencia espectral, y aunque todavía no se ha publicado de manera oficial, algunos proveedores como Cisco, ya proporcionan puntos de acceso con Wifi de 6ª generación (Cisco, s.f.)

La Wifi Alliance es una organización sin ánimo de lucro que promueve la tecnología Wifi, y certifica los productos Wifi que se ajustan a las normas de interoperabilidad. La forman empresas como 3Com, Cisco y Motorola, y los principales patrocinadores de esta alianza son las grandes empresas fabricantes de dispositivos que hacen uso del Wifi, como Apple, Samsung, Sony, LG, Cisco, Broadcom, Intel, Qualcomm, Motorola o Microsoft. (TestdeVelocidad, s.f.) (IEEE, s.f.)

2.6. Criptografía y su importancia

La RAE (Real Academia de la lengua Española) define la criptografía como el *"arte de escribir con clave secreta o de un modo enigmático"*, cuyo objetivo se ve definido en el documento "Criptografía avanzada" (Rotger, 2017)),*" La criptografía tiene como objetivo la transmisión o almacenamiento de mensajes indescifrables para todo receptor que no disponga de la clave del algoritmo de descifrado".* Con esto en mente, se puede pensar que efectivamente es una parte importante en las redes Wireless debido a su naturaleza.

A continuación, se ven los 4 puntos clave que aborda la criptografía, y especialmente en el ámbito de la seguridad informática, los cuales explican por qué hoy en día se cifran las comunicaciones:

- Confidencialidad: En primer lugar, la criptografía protege la confidencialidad de la información, incluso cuando esta información queda comprometida ante un tercero. La información encriptada es inservible ante terceros sin las claves de desencriptación requeridas.

- Autenticación: La criptografía también aborda la autenticación, por medio de certificados digitales, firmas digitales o infraestructuras de clave pública, cerciorando que el emisor es realmente quien dice ser o que el receptor es al que realmente se envía la información.

- Integridad: Otro punto clave de la criptografía es el de asegurar la integridad del mensaje o de la información transmitida por un medio (utilizando por ejemplo validación de hashes), con esto, el

receptor se asegura de que el mensaje enviado por el emisor es el mismo que el que recibe, y que no ha sido manipulado por un tercero durante la transmisión del mensaje.

- No repudio: Por último, esto es similar a la autenticación, pero mientras que ésta primera hace referencia al emisor y al receptor, el no repudio se produce frente a un tercero. Se trata de que un emisor no puede negar que ha hecho un envío porque el receptor tiene pruebas de esto o que el receptor no puede negar la recepción del mensaje porque el emisor tiene pruebas de esto.

Este último punto es el más complicado de entender, por eso se explica con el siguiente ejemplo:

Si utilizando la aplicación WhatsApp un emisor A envía un mensaje a un receptor B, y este lo recibe (con un doble tick), A no puede negar que ha enviado el mensaje, ya que B tiene pruebas de que ha recibido ese mensaje (tiene el propio mensaje), y por otro lado, B no puede negar que ha recibido el mensaje, ya que A tiene pruebas de ello (aparece un doble tick debido a la recepción).

Debido a que as redes Wifi transmiten información por un medio en el que si un tercero está dentro del rango de comunicación puede interceptar los mensajes, es muy importante tener en cuenta la criptografía a la hora de diseñar estas comunicaciones, ya que, de no ser así, serían comunicaciones totalmente transparentes para cualquier persona. Así pues, en este tipo de redes se utilizan todos los puntos para mantener a salvo las comunicaciones, ya que es necesario autenticar al emisor/receptor, mantener la información de manera confidencial en el caso en el que los mensajes sean interceptados por un tercero, y tener certeza de que el mensaje recibido es el mismo que se ha enviado.

Por esto, es muy importante crear algoritmos de cifrados sólidos para que estos puntos no puedan ser vulnerados, y esto mismo se verá en la parte práctica, ya que al fin y al cabo cuando se hace un ataque se querrán vulnerar algunos de estos puntos.

2.7. Estado del arte

Debido a la importancia de la seguridad en las redes de los usuarios, y una vez se tiene un conocimiento general de las redes wifi, se han visto diferentes trabajos de investigación de otros autores que abordan la seguridad en las redes Wifi, pero con el rápido avance de la tecnología, en este trabajo se quiere realizar una investigación actualizada, además de aportar recomendaciones de seguridad para poder enfrentar las vulnerabilidades que existen en las redes Wireless a día de hoy, para ello, además de dar al lector la oportunidad de experimentar estas

vulnerabilidades en la parte práctica, para entender realmente que cualquier persona con pocos conocimientos de redes puede explotar estas vulnerabilidades y por qué se deberían seguir los consejos de seguridad al elegir una configuración u otra, se añadirán comentarios adicionales durante el transcurso de este documento para poder entender qué se recomienda en cada caso.

3. Protocolos de seguridad

A continuación, se describen los diferentes protocolos de seguridad, además del estándar WPS.

3.1. Protocolo WEP

El protocolo WEP (Wired Equivalent Privacy o Privacidad Equivalente al Cable) es el mecanismo de cifrado que fue incluido en la primera versión del estándar IEEE 802.11 en 1997, cuyos objetivos eran tanto proporcionar una seguridad y una confidencialidad similar a la de las redes cableadas mediante cifrado, como evitar que usuarios ajenos a la red pudieran acceder a esta gracias a la autenticación. (utsfm, s.f.), (UPC, s.f.) (INCIBE, s.f.)

3.1.1. Cifrado WEP

WEP utiliza el algoritmo RC4 (Rivest Cipher 4) para cifrar las comunicaciones, uno de los algoritmos de cifrado de flujo basados en software más utilizados en el mundo gracias a su bajo coste computacional tanto en el cifrado como en el descifrado, y a su sencillez de implementación en hardware y software. Este algoritmo está incluido en otros protocolos como por ejemplo SSL (Secure Sockets Layer) para comunicaciones seguras punto a punto, donde el algoritmo RC4 proporciona confidencialidad. (tech-faq, s.f.)

Para el proceso de cifrado se utiliza la comprobación de redundancia cíclica de 32 bits (o CRC-32) proporcionando integridad al protocolo. CRC-32 es un mecanismo de detección de errores que añade información redundante permitiendo detectar cambios en los datos que son transmitidos. El mecanismo recibe una entrada de flujo variable y devuelve un flujo de longitud fija y un “checksum” que se añade a la información para que posteriormente se pueda verificar que la información corresponde con este y no ha sido modificada por errores de transmisión.

Una vez conocidos los términos RC4 y CRC-32 se ve su implicación en el protocolo WEP, donde el procedimiento de cifrado sigue los pasos que se ven en la siguiente figura:

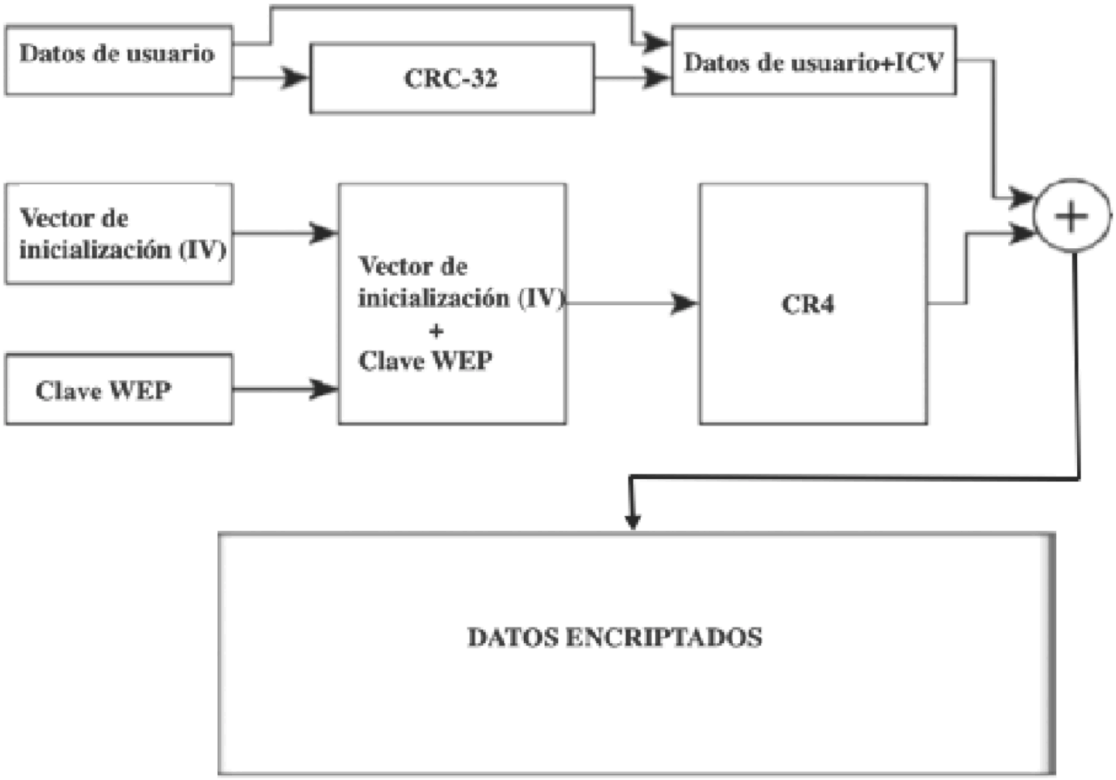


Ilustración 14: Encriptación WEP, (grandmetric, 2018)

El esquema de la figura se explica con los siguientes pasos:

- Por un lado, se calcula el CRC de 32 bits de los datos, agregando el vector de verificación de integridad (ICV) a los datos, lo que se ve en la parte superior de la figura. En este paso cabe destacar que es un método utilizado para detectar posibles errores de transmisión, pero no es confiable en la verificación de integridad de los mensajes.

- Por otro lado, como se ve en la parte inferior de la figura, se realiza el cifrado RC4 utilizando como semilla la suma de una contraseña (root Key o WEP key) que comparten todos los usuarios autorizados y un vector de inicialización (IV) que cambia en cada paquete que se transmite, ocupando 64 o 128 bits. A continuación, el generador pseudoaleatorio de RC4 crea una secuencia de la misma longitud que la del mensaje+ICV.

- Por último, a partir de los dos primeros pasos se crean los datos encriptados. (grandmetric2, 2018) (tech-faq, s.f.) (Prieto, s.f.)

El esquema de la trama quedaría de la siguiente manera ilustrado en la figura:

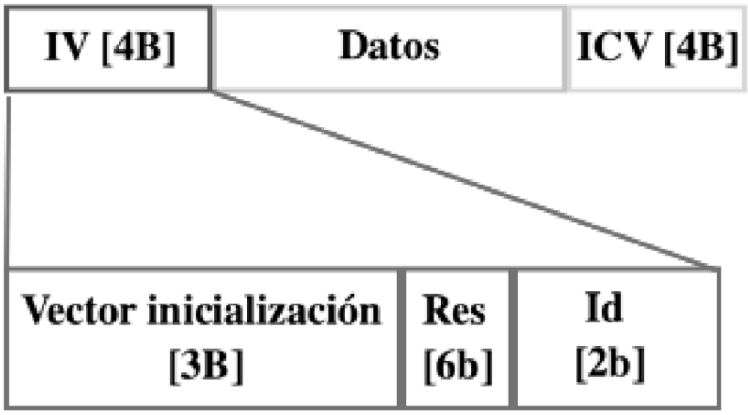


Ilustración 15: Esquema de una trama WEP

Y simplemente se añadiría una cabecera al principio y un FCS (Frame Check Sequence) de 4B al final.

3.1.2. Autenticación WEP

El proceso de autenticación permite verificar la identidad del remitente. En el protocolo WEP las claves se autentican utilizando dos métodos diferentes:

1. Autenticación de sistema abierto: En este método la clave WEP es abierta (no es secreta) y todos los usuarios tienen permiso para acceder a la WLAN.

   El método de autenticación de sistemas abierto es el siguiente:

   - El cliente hace una petición de autenticación abierta
   - El punto de acceso envía una confirmación al cliente

   A continuación, en la siguiente figura se representa este esquema de manera gráfica:

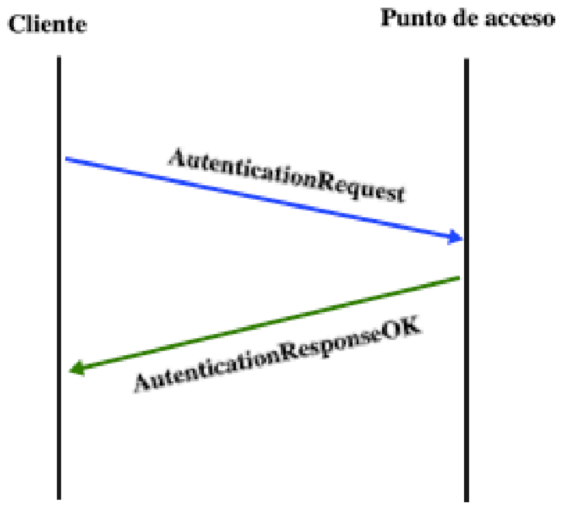


Ilustración 16: Esquema de autenticación de sistema abierto

   En este esquema la flecha azul representa la petición de autenticación del cliente al punto de acceso, y la flecha verde la confirmación que realiza el punto de acceso al cliente.

2. Autenticación de clave compartida: En este método, la clave compartida restringe el acceso a la WLAN, siendo esta necesaria para que las redes asocien y cifren los datos que se comparten entre todos los componentes de la red.

El método de autenticación de clave compartida se divide en las siguientes fases:

- El cliente envía una petición de autenticación al Punto de Acceso
- El punto de acceso devuelve un reto
- El cliente cifra el reto utilizando la clave WEP
- El cliente envía el reto cifrado al punto de acceso en otra petición de autenticación.
- El Punto de Acceso descifra la petición cifrada y lo compara con el original, si coinciden, el punto de acceso envía una confirmación al cliente, en caso contrario envía una denegación.

En la siguiente figura se representa este esquema de forma gráfica:

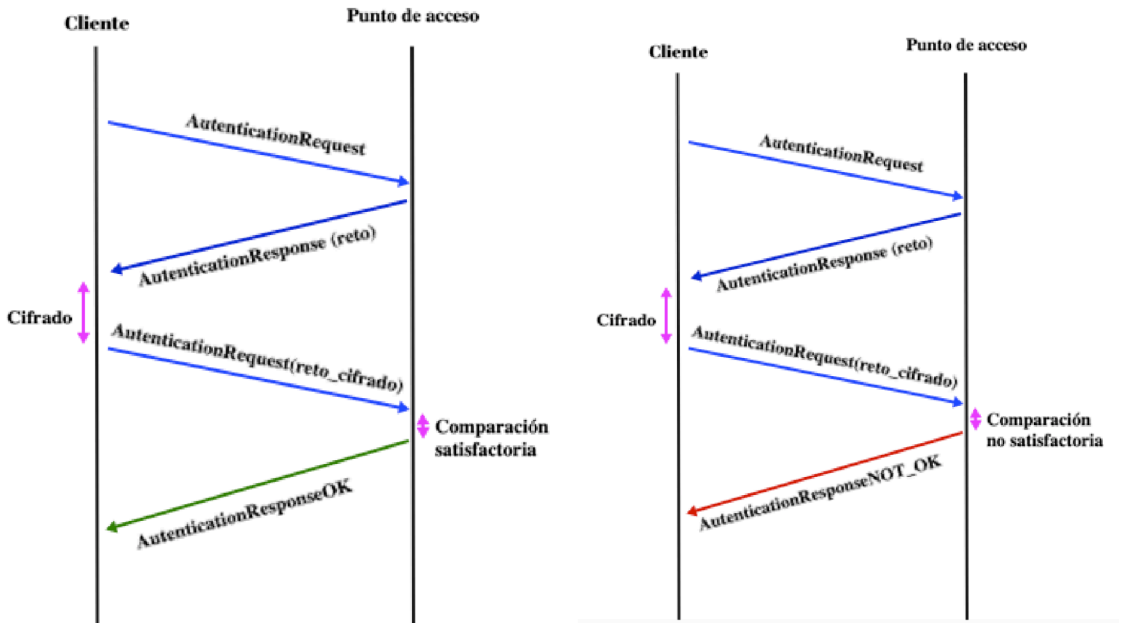


Ilustración 17: Esquema de autenticación de clave compartida

En la figura anterior se representa en la parte izquierda el esquema de una autenticación satisfactoria y en la derecha una autenticación fallida. Después de las dos primeras flechas en las que se pide autenticación y se devuelve un reto respectivamente, el cliente realiza el cifrado. La tercera flecha representa el reto cifrado y tras la comparación, la última flecha representa la autorización o denegación.

Comentarios adicionales: Aunque no se recomienda la utilización del protocolo WEP para ningún tipo de red (ni siquiera pública) debido a su

pobre encriptación, se ve como opción ligeramente más segura la autenticación de sistema abierto, aunque parezca que no tiene sentido con lo que se acaba de exponer en las figuras anteriores. Si la encriptación WEP fuera fuerte o media sí tendría sentido utilizar un método de autenticación de clave compartida, y este sería el elegido. El problema reside en la débil encriptación del protocolo debido a los IVs y claves cortas que permanecen estáticas, lo que hace que un atacante pueda conseguir la clave WEP de manera muy sencilla.

3.1.3. Evoluciones de WEP

Debido a la inseguridad de la red inalámbrica que se vio con este mecanismo, y a las vulnerabilidades que se han ido publicando sobre este protocolo, se han llevado a cabo diferentes versiones de WEP. A pesar de que la alternativa más sonada es el cambio directo a 802.11i (WPA y WPA2), también se encuentran otras versiones del protocolo que se ven a continuación: (WEP, s.f.)

- WEP2: En este caso se utiliza un cifrado y un IV de 128 bits (se había visto que en WEP el IV podía ser de mínimo 60 bits y máximo 128). WEP2 fue presentado tras la publicación de WPA y WPA2 como mejora del protocolo WEP y, entre otros, para aquellos dispositivos que debido a restricciones hardware no soportaban WPA2. Con esta modificación se intenta abordar la eliminación de la deficiencia del duplicado de IV y de los ataques de fuerza bruta, aunque al seguir utilizando el mismo algoritmo de cifrado, estas vulnerabilidades no se eliminaban. Más adelante se ve cómo evoluciona este algoritmo de cifrado con los diferentes protocolos.

- WEP Plus: En esta versión de WEP se aumenta ligeramente la seguridad fortaleciendo los IVs (lo que se consigue suprimiendo los IVs débiles), el hándicap es que para que esto sea eficaz debe estar configurado WEP plus en cliente y en punto de acceso simultáneamente.

- WEP Dinámico: En esta versión, las claves WEP varían dinámicamente. El cliente utiliza dos claves: una clave predeterminada, que se comparte con todos los clientes y una clave de asignación única entre el cliente y el punto de acceso. Al utilizar estas claves dinámicas se obtiene la ventaja de reducir la frecuencia de utilización de cada clave y la periodicidad de cambio de las claves, lo que aumenta la seguridad con respecto al protocolo WEP tradicional. (ecured, s.f.).

Comentarios adicionales: Aún con las nuevas versiones del protocolo WEP, aunque se mejora la seguridad y es recomendable utilizar

versiones WEP que el protocolo WEP sin versionar, estos protocolos siguen teniendo una seguridad débil y no se recomienda utilizarlos.

3.2. Protocolo WPA

El protocolo WPA (Wi-Fi Protected Access) surge en 2003 como respuesta del IEEE por la necesidad de corregir las deficiencias de seguridad del protocolo WEP, incluyéndose en la versión del estándar 802.11i. Se caracteriza por ser un protocolo más robusto basándose en el mismo hardware que WEP permitiendo así mejorar la seguridad tan solo con una actualización del firmware.

3.2.1. Cifrado WPA

En el cifrado WPA, como en WEP, se realiza la operación XOR de los datos del usuario y la secuencia pseudoaleatoria de RC4, pero esta vez será mucho más robusto en seguridad. A continuación, se representa gráficamente el cifrado WPA:

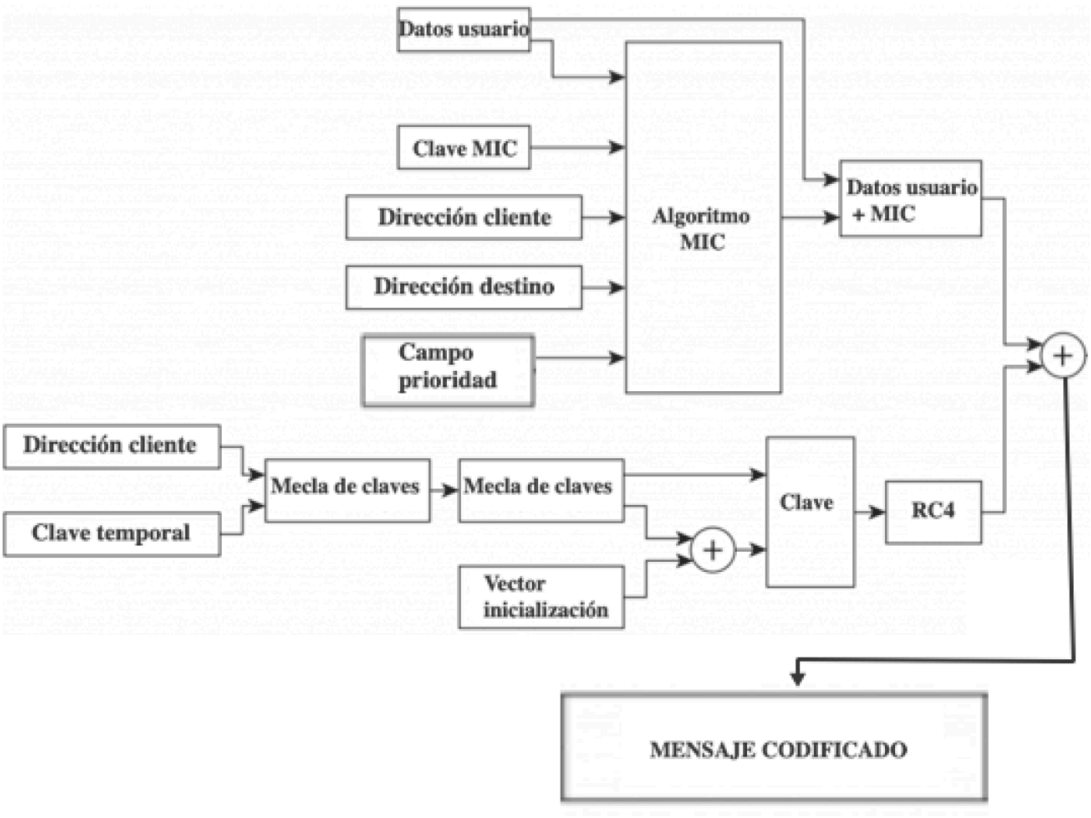


Ilustración 18: Cifrado WPA, (grandmetric2, 2018)

A continuación, se explica la figura anterior:

En primer lugar, para los datos de usuario, WPA hace uso de TKIP (Temporal Key Integrity Protocol) en vez de CRC para proporcionar integridad al mensaje. Se utiliza un código de integridad de mensaje (MIC) que utiliza tanto los datos del usuario como la dirección del cliente, la dirección de destino, el campo de prioridad y la clave MIC.

Al mismo tiempo, como se ve en la parte inferior de la figura, el protocolo TKIP empieza con una clave temporal compartida entre cliente y punto de acceso de 128 bits que se combina con la dirección MAC del cliente.

A esa combinación se añade un vector de inicialización de 128 bits asegurando que cada estación utilice diferentes flujos claves para cifrar los datos.

Igual que en el protocolo WEP, se utiliza RC4 (se trata de una implementación de hardware y no era posible actualizarlo) para el cifrado de datos para proporcionar confidencialidad, pero cambiando las claves cada 10000 paquetes añadiendo mayor seguridad.

3.2.2. Autenticación WPA

En WPA actualmente hay dos modos de autenticación diferentes dependiendo del tamaño y del propósito de la red: Modo empresa y modo personal.

1. Modo de empresa o servidor de autenticación: Diseñado para grandes entidades como empresas, centros educativos o gobierno, este modo utiliza un servidor de autenticación 802.1X, ya que no se pueden poner todos los identificadores de usuario y claves en cada uno de los numerosos puntos de acceso (a veces se ponen dos o más servidores, por redundancia). Este servidor genera diferentes claves y certificados y los distribuye para cada usuario. Mas adelante se explica en detalle las fases de autenticación del 802.1X incluyendo esquemas gráficos.

2. Modo personal o clave precompartida: Diseñado para casas y redes pequeñas como entornos del small office/home office (SOHO). Este modo no requiere autenticación de servidor. Cada dispositivo encripta el trafico de red de la clave de encriptación (desde 128 hasta 256 bits) pre-compartida.

Comentarios adicionales: En este documento se recomienda el uso de WPA frente al uso de WEP si no hay ninguna otra opción, ya que se considera más seguro, aunque no se considera que tenga una encriptación suficientemente sólida hoy en día, y no se recomienda en general el uso de este protocolo.

3.3. WPA2

El protocolo WPA2 estuvo disponible a principios del 2004, pero no fue requerido oficialmente hasta el año 2006 en los puntos de acceso. En este momento, los fabricantes comenzaron a producir la nueva generación de puntos de acceso apoyados en el protocolo WPA2, que utiliza el algoritmo de cifrado AES, que se explicará con detalle en este apartado, y que permitía cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2.

Este nuevo protocolo se hizo esencial para hacer frente a las vulnerabilidades de WPA, pero esta vez sí se requirió un cambio de hardware, ya que no era suficiente con hacer una actualización de firmware como ocurría con el cambio WEP-WPA, lo que se convirtió en un gran inconveniente, que se suavizaba con el hecho de la nueva implementación de un protocolo mucho más seguro, aun así, los productos certificados para WPA2 aseguran que, pese a los nuevos requerimientos de hardware, la interoperabilidad con otros protocolos de seguridad anteriores se consiga.

Este nuevo protocolo incluye el intercambio dinámico de la clave, un cifrado mucho más fuerte, y la autenticación de usuario. Para conseguir esto se implementan dos grandes novedades: Por un lado, la utilización del estándar AES (Advanced Encryption Standard), que se hace obligatorio en WPA2 mejorando la encriptación frente a TKIP (aunque TKIP también está disponible para la compatibilidad con dispositivos con hardware WPA), y además se utiliza CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) para asegurar la integridad y la autenticidad de los mensajes. (elo, s.f.) (helpdeskgeek, s.f.)

Comentarios adicionales: Se trata de un protocolo bastante seguro y es el que se recomienda a cualquier usuario que tenga un punto de acceso o un cliente en una red wifi, y actualmente en su modo empresa el más seguro del mercado, aunque en 2017 se descubrió la primera vulnerabilidad, de la que se hablará en el apartado 4.6.

3.3.1. Cifrado WPA2

El cifrado utilizado es AES, un conjunto de reglas que definen el diseño de la estructura y que recoge entre otros el uso del Rijandel symmetric block cipher, que puede procesar bloques de datos de 128 bits usando cipher keys de 128, 192 y 256 bits. Actualmente AES se considera muy seguro, tanto que es utilizado por la NASA para asegurar documentos categorizados como “top secret”. El algoritmo llamado "Rijndael", era sobresaliente tanto en rendimiento como en seguridad y flexibilidad. Hoy en día no existe un ataque viable (desde el punto de vista del tiempo que tomaría) contra AES, y es por eso por lo que es el estándar utilizado para los datos más sensibles (NASA, gobiernos, bancos, etc.).

Se trata de un cifrado de estructura de bloques en los que se hacen varias permutaciones, sustituciones y operaciones lineales repitiéndose en diferentes rondas, y en cada ronda se calcula una clave circular única a partir de la clave de cifrado que se une en los posteriores cálculos. (boxcryptor, s.f.)

El protocolo de seguridad utilizado en WPA2 es CCMP, que sigue el estándar AES para cifrar datos confidenciales.
CCMP combina el modo de cifrado CTR con el modo de autenticación CBC-MAC para proteger la integridad. A continuación, se enumeran algunas de las ventajas que tiene el protocolo CCMP:

- En primer lugar, con CCMP se hace fácil la distinción y el manejo de mensajes en los que diferentes partes están destinadas únicamente a ser autenticadas y no encriptadas, y esto se hace sin ninguna sobrecarga adicional de texto cifrado.

- Su combinación de CTR y CBC-MAC hace que sea fácil su implementación gracias a que son tecnologías “antiguas” que se conocen muy bien, que se han analizado ampliamente y de las que hay mucha documentación, que se han ido optimizando y que son confiables, por tanto, se descartan posibles lagunas en la implementación.

- Los derechos de propiedad intelectual de CCMP se han liberado, por lo que son de dominio público. (citeseerx, s.f.)

A continuación, se ilustra un diagrama ejemplo de un CTR, que logra el cifrado de datos. El cifrado AES en modo contador se aplica a segmentos separados de datos de contenido. Cada segmento de datos debe encriptarse usando AES en modo contador:

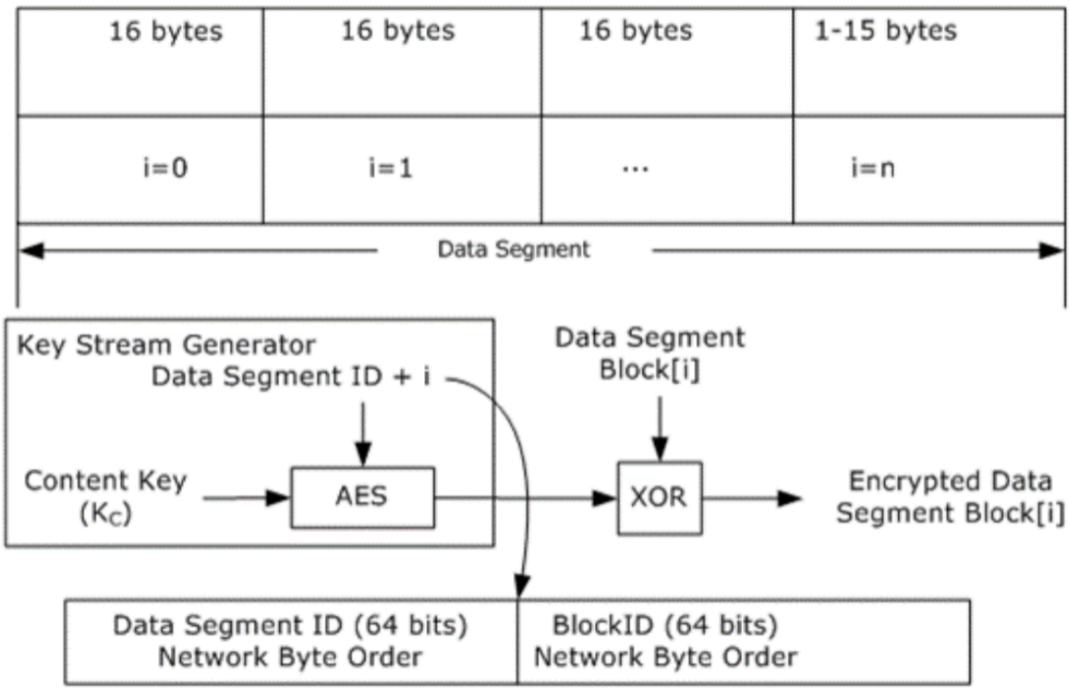


Ilustración 19: Cifrado AES, (microsoft, 2019)

El contenido cifrado se crea al hacer la operación XOR entre los datos a encriptar y la secuencia de claves generada por AES. La secuencia generada por AES serán bloques de 16 bytes de secuencia de claves, y a su entrada se encuentra la clave de cifrado de contenido (KC) y la concatenación de 128 bits de una ID de segmento de datos y la ID de bloque dentro del segmento de datos.

Por otro lado, CBC-MAC se utiliza para generar un componente de autenticación como resultado del proceso de encriptación, lo que aporta una gran mejora frente a las implementaciones anteriores del código de integridad de mensajes (MIC), donde para poder verificar la integridad era necesario un algoritmo adicional y separado. En este modo se encadenan XORs entre texto encriptado y texto plano del bloque siguiente, así pues, el texto cifrado del bloque anterior sirve como

"fingerprint" del bloque actual. Por tanto, cualquier cambio se propagará en los siguientes bloques. En la siguiente figura se presenta CBC-MAC de manera gráfica:

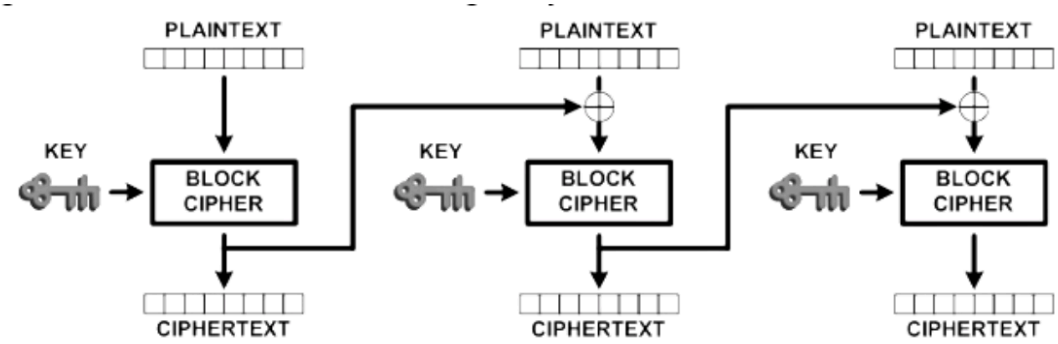


Ilustración 20: CBC – MAC, (cissp, s.f.)

Así pues, cuando los datos pasen por el cifrador CCMP se obtendrá una trama de la siguiente forma, como se ve en la figura:

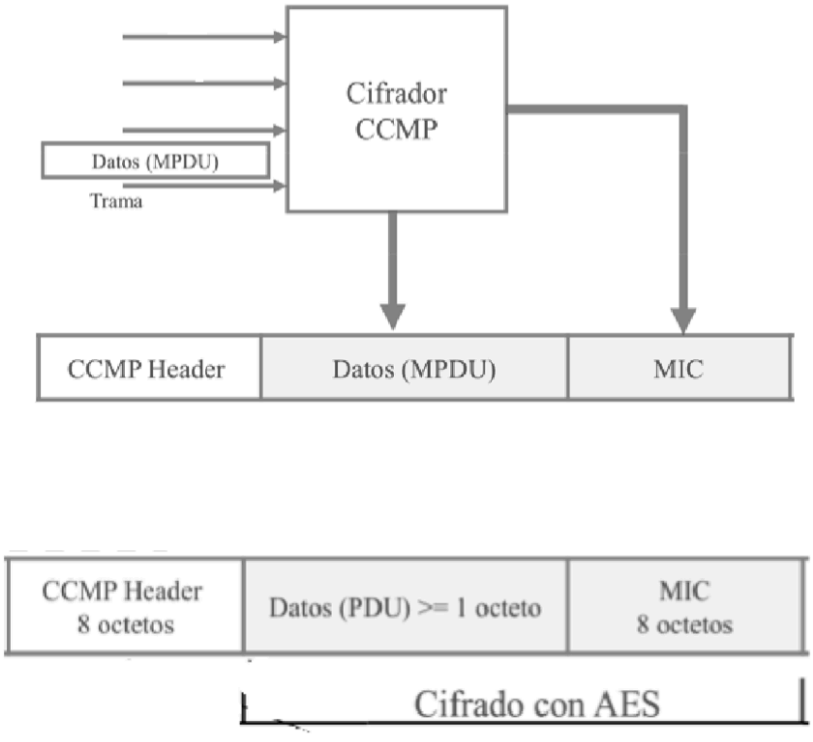


Ilustración 21: Trama WPA2, (ConferenciaUPM, s.f.)

3.3.2. Autenticación WPA2

En WPA2 también hay dos modos de autenticación:

- Modo de empresa o servidor de autenticación: Utilizando 802.1X, que se explica a continuación, y que está diseñado para entornos corporativos o grandes entornos donde prime la seguridad, utilizando un servidor de autenticación (normalmente RADIUS) generando diferentes claves y certificados para cada usuario.

- Modo personal o clave precompartida (Pre-shared key): Diseñado para pequeñas redes donde no es necesaria una gran seguridad, y donde cada cliente encripta el trafico de red de la clave de encriptación pre-compartida

3.4. Autenticación 802.1X

Las fases de autenticación de este modo son las siguientes:

- En primer lugar, el punto de acceso (al que se llamará autenticador) y el cliente (al que se llamará suplicante) se preasocian utilizando el framework de autenticación EAP (Extensible Authentication Protocol), donde se establece una negociación de la política de seguridad que posteriormente les va a llevar a una asociación completa. Para ello, el autenticador envía una petición de Autenticación al cliente, el mensaje de Request tiene un campo de Tipo, en el cual el cliente debe responder que es lo que está solicitando, ya sea Identidad, Notificación, Nak, MD5-Challenge, One-Time Password (OTP), Generic Token-Card (GTC), Tipos Expandidos o Experimental. El suplicante envía una resupesta al autenticado con el campo tipo solicitado. Una vez recibida la respuesta, el autenticador envía otra petición y así sucesivamente continuando según sea necesario hasta que la autenticación sea satisfactoria o hasta que el autenticador no pueda autenticar al cliente.

- En la segunda fase, se realizará la autenticación con el servidor de autenticación a través de una petición de acceso desde el autenticador al servidor de autenticación. En caso de que la autenticación sea satisfactoria, el servidor de autenticación envía una MK (Máster Key o clave maestra al autenticador) que utilizará posteriormente.

- En la tercera fase (4-Way-handshake) se realiza la derivación y distribución de clave, de la derivación de la MK donde en suplicante y autenticador obtienen una PMK de 256 bits. En una

primera trama el autenticador envía un anonce aleatorio, y el cliente calcula la PTK (Pairwise Transient Key) de 512 bits mediante una función pseudoaleatoria que se dividen en 5 trozos (si es TKIP) o de 348 bits que se dividen en 3 trozos (si es CCMP). A continuación, el cliente envía una segunda trama con un Snonce aleatorio y con un MIC que es calculado con los primeros bits de la PTK. Seguidamente el autenticador verifica el MIC y calculo y cifra la clave de grupo (GTK) enviándosela cifrada al cliente junto con el MIC. Por último, el cliente verifica el MIC, guarda la clave de grupo recogida y se establece la conexión. Es en este momento cuando se abre el puerto 802.1x del autenticador.

- Por último, se realiza la asociación y el intercambio cifrado de información.

A continuación, en la siguiente figura, se muestra el esquema general del proceso de autenticación con las diferentes fases que se acaban de explicar:

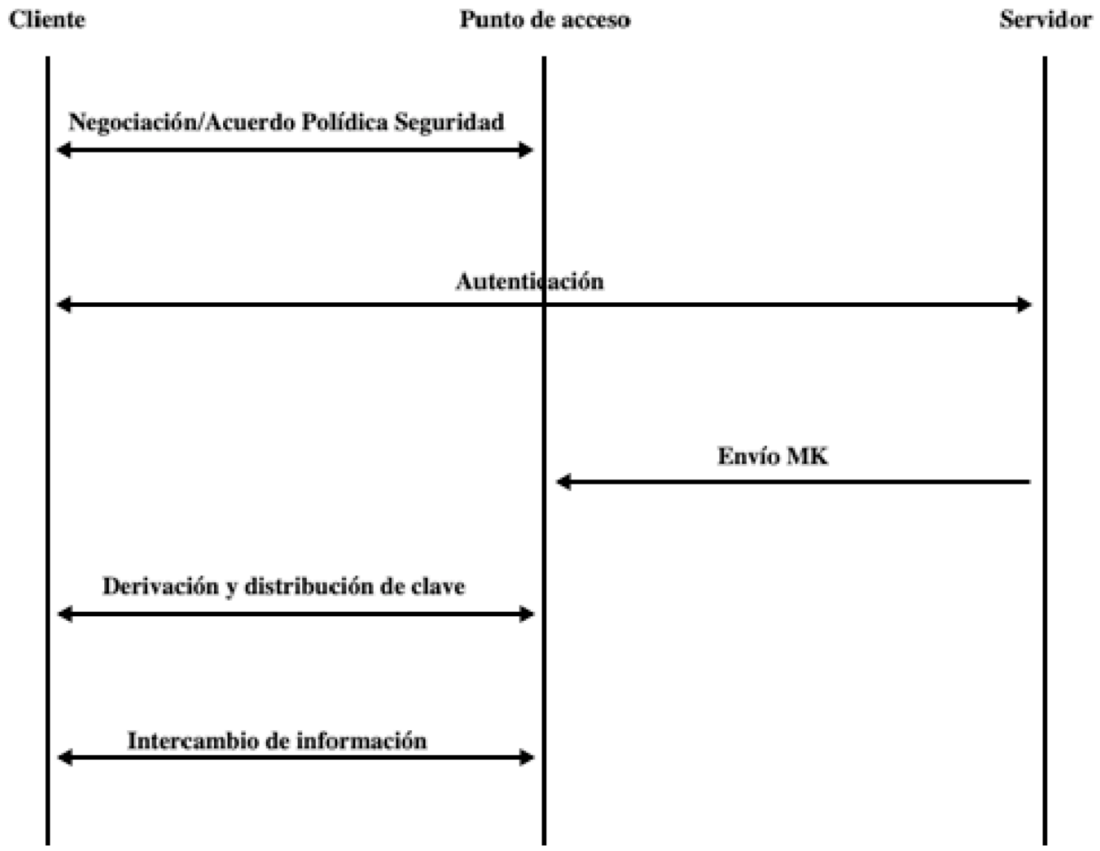


Ilustración 22: Esquema de autenticación 802.1X

Además, también se muestra la fase 4-Way-handshake explicada anteriormente:

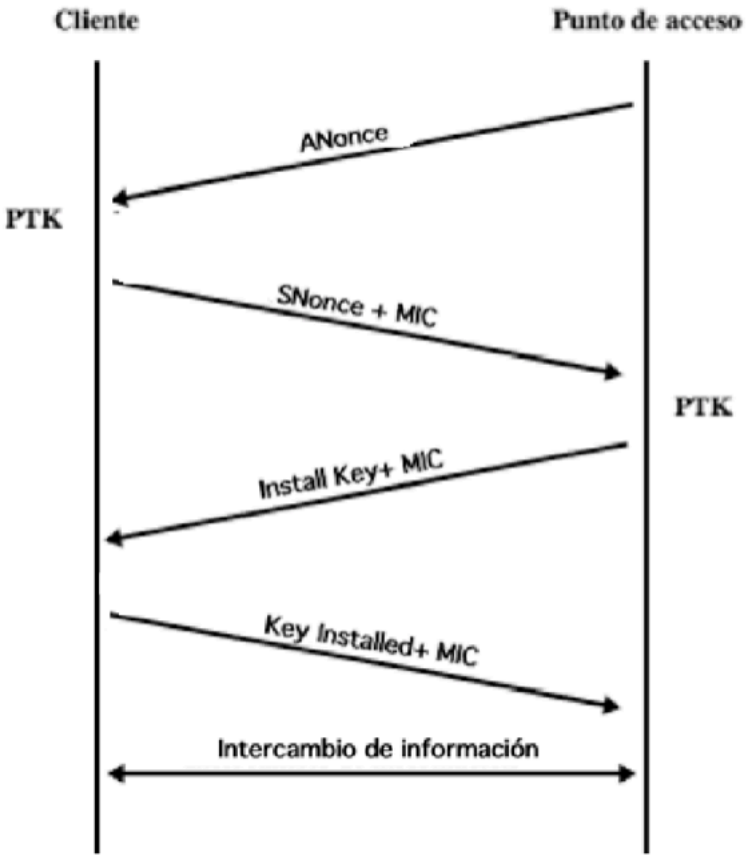


Ilustración 23: 4-Way-handshake

3.5. Comparativa WEP vs WPA vs WPA2

A continuación, a modo resumen se presenta la tabla comparativa de las diferentes encriptaciones, autenticaciones y principales características de los protocolos de seguridad:

	WEP	**WPA**	**WPA2**
Significado	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access V2
Encriptación	RC4	TKIP (RC4) / MIC	CCMP (AES) / CBC - MAC
Autenticación	PSK	Enterprise: 802.1x con EAP y RADIUS	Enterprise: 802.1x con EAP y RADIUS
		Personal: PSK	Personal: PSK
Tamaño del IV	24 bits	48 bits	48 bits
Características principales	-Protección a redes inalámbricas vulnerables	-IV Extendido -Claves dinámicas -Incluye MAC del emisor	-Algoritmo de mayor complejidad -Tramas convertidas por operaciones matriciales
Vulnerabilidades	-Claves muy débiles -IV pequeño -Llaves estáticas -Encriptación débil	-Claves generadas pseudoaleatorias que pueden estar en diccionarios -Claves personalizadas débiles -Autenticación con handshake visible	-Claves pseudoaleatorias que pueden estar en diccionarios -Claves personalizadas débiles

Comentarios adicionales: En este documento se recomienda la utilización del protocolo WPA2, que utiliza una encriptación AES convirtiéndolo en la solución más segura, aunque además, en cualquiera de los protocolos se pueden utilizar medidas de seguridad adicionales limitando el acceso a la red desde el punto de acceso, configurando el punto de acceso para que sólo admita unos protocolos específicos o unas direcciones MAC/direcciones IP especificas, así pues, si se configura el punto de acceso para que sólo admita unas direcciones

MAC, cualquier dispositivo con una dirección MAC diferente a las que se han especificado no podrá entrar en la red. Esto no es fiable al cien por cien, ya que un atacante podría observar las direcciones MAC de los dispositivos que están conectados a una red y “recrear” esa dirección MAC en su dispositivo atacante, no obstante, se pondrán muchas más dificultades para que éste pueda llevar a cabo un ataque satisfactorio. Además, también se pueden llevar a cabo monitorizaciones de la red para saber qué clientes se conectan a la red.

Hoy en día ninguna red o sistema se puede considerar cien por cien seguro, y esto se ve en los ataques zero-day que han ido ocurriendo a lo largo de la historia. Un ataque zero-day es aquel que explota vulnerabilidades que generalmente son desconocidas tanto para la gente como para el fabricante del producto. Son los ataques más peligrosos, pero también los menos comunes, como por ejemplo el ataque de Stuxnet que en 2010 infectó la central nuclear Natanz de Irán. Teniendo esto en cuenta, y sabiendo que no hay sistema impenetrable, es importante proteger las redes lo máximo posible y al menos evitar estar expuesto a las vulnerabilidades publicadas y conocidas por cualquier persona que tenga acceso a internet, además de poner todas las trabas posibles para que un atacante desista de intentar acceder a la red.
Si un atacante ve una red con cifrado WEP y otra con cifrado WPA2, accederá a la red WEP sin pensarlo dos veces, ya que la diferencia de tiempo que le tomará acceder a una red o a otra sería abismal, por tanto, se deben tomar todas las medidas necesarias para proteger una red y lo más importante, nunca quedarse por detrás, evitando ser la víctima más fácil y débil.

3.6. WPS

Para facilitar y simplificar el proceso de configuración de seguridad de las redes Wifi, en 2007 se lanzó el estándar WPS (WiFi Protected Setup). Es verdad que no es un protocolo de seguridad en sí, pero este estándar se podrá utilizar adicionalmente a los protocolos y afectará de forma notoria a la seguridad y a las vulnerabilidades de las redes Wireless WPA y WPA2, por eso es importante incluirlo en este apartado.

El estándar WPS permite una configuración sencilla mediante cuatro modos diferentes para el intercambio de credenciales: PIN (Personal Identification Number), PBC (Push Button Configuration), NFC (Near Field Communications) y USB (Universal Serial Bus), y es utilizado mayormente en redes domésticas.

Para explicar estos modos, primero se describen los tres elementos principales que existen en WPS y las tres interfaces:

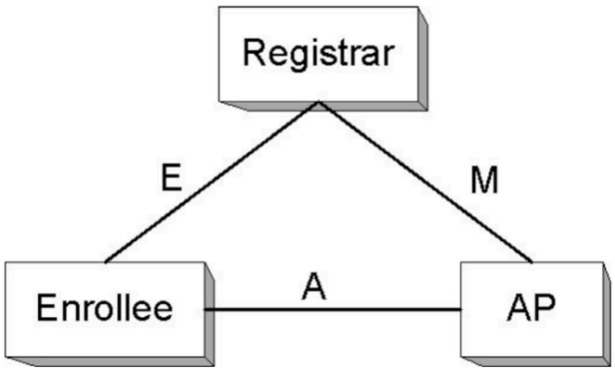


Ilustración 24: Esquema de los elementos WPS (boxcryptor, s.f.)

- Registrar: El dispositivo que genera y elimina credenciales (puede ser AP o cliente)

- Enrollee: Nuevo cliente que quiere unirse a la red

- .Authenticator: AP mediador entre Registrar y Enrollee.

- La interfaz E, entre el Enerollee y el Registrar permite que el Registrar descubra y emita credenciales de WLAN para el Enrollee.

- La ínterfaz M, entre el Autenticador y el Registrar, permite a un Registrar externo administrar el AP WPS.

- La interfaz A, entre el Enrollee y el Autenticador, permite el descubrimiento de la WLAN de WPS y permite la comunicación entre el Enroller y el AP.

En el modo PIN, hay un código PIN conocido por Registrar y que debe ser conocido por el Enrollee para iniciar la conexión, aunque en este caso el Enrollee no necesitará ningún otro tipo de conexión a la red, lo que lo hace bastante insegura.

En el modo PBC, la conexión se hace al presionar un botón (físico o virtual) tanto en el Registrar como en el Enrollee. En el tiempo entre que se pulsa en el Registrar hasta que se pulsa en el Enrollee, cualquier otra estación próxima puede ganar acceso a la red.

En el modo NFC, la tecnología de autenticación es NFC, y cualquier Enrollee próximo al Registrar obtiene autenticación, por lo que cualquier usuario que tenga acceso físico al Registrar, puede obtener credenciales válidas.

Por último, en el modo USB, las credenciales de autenticación se obtienen mediante un dispositivo USB y se transfieren desde Registrar hasta Enrollee.

(Ruz Maluenda, Riveros Vasquez, & Varas Escobar, s.f.) (RovingNotes, s.f.) (Alliance, December 2006)

Comentarios adicionales: Este trabajo se centra en la seguridad de las redes Wifi, y no se recomienda el uso de WPS ni en redes empresariales ni en redes personales.

3.7. WPA3

En 2017 se descubrió la primera vulnerabilidad del protocolo de seguridad WPA2, y aunque actualmente se considera bastante seguro, se ha hecho necesario un nuevo protocolo de seguridad llamado WPA3 como sucesor del actual WPA2 para evitar ésta y otras posibles vulnerabilidades que puedan encontrarse en el futuro en WPA2.

WPA3 fue anunciado en 2018, por la WiFi Alliance, y contará con un modo personal y un modo enterprise de 128 y 192 bits de cifrado respectivamente, además de confidencialidad de envío, con mejoras que ayudarán a garantizar la privacidad de las comunicaciones inalámbricas.

Las ventajas que ofrecerá este nuevo protocolo son las siguientes:

- Reducir los problemas de seguridad provocados por contraseñas débiles, añadiendo mas protección frente a ataques de fuerza bruta.

- Configuraciones más simples de cara a los usuarios.

- Mayor protección en redes públicas, cifrando el tráfico entre cliente y punto de acceso.

- Robustez en el cifrado con arquitectura de seguridad de 192 bits, pensado para el tratamiento de datos confidenciales, enfocado en empresas, entidades gubernamentales, centros educacionales, etc.

- Evita que un atacante pueda descifrar el tráfico capturado con la característica WPA3 Forward Secrecy.

Por lo tanto, *"WPA3 reemplazará a WPA2 mejorando en gran medida los mecanismos de autenticación y configuración, dotando a los dispositivos de más resistencia ante contraseñas poco seguras y potenciando el uso de protocolos criptográficos robustos"*. (INCIBE, 2019)

4.Parte práctica

4.1. Introducción

En esta parte se quiere comprobar si realmente, hoy en día, las redes Wifi son seguras, y cómo se puede proteger una red ante posibles atacantes, para esto se han seleccionado cinco pruebas que realmente pueden ayudar al lector a tomar las medidas necesarias para prevenir o defenderse frente a un ataque.

En primer lugar, se hará un ataque a una red con encriptación débil utilizando el protocolo WEP, poniendo a prueba la encriptación RC4 para demostrar la facilidad con la que ésta se puede vulnerar.

En segundo lugar, se hará un ataque a una contraseña débil, para demostrar la simplicidad con la que se puede acceder a una red cuyo punto de acceso tiene una contraseña débil.

En tercer lugar, se realizará un ataque a una red que utiliza el estándar WPS, con el fin de probar que la utilización de este estándar hace que la red sea más vulnerable.

En cuarto lugar, se comprobará si se poseen dispositivos vulnerables a la vulnerabilidad Krack, ofreciendo esta herramienta para que el lector pueda comprobar sus dispositivos y realzando la importancia de las actualizaciones de software.

Por último, se realizará una prueba de ingeniería social donde se recrea un ataque a un cliente de la red para que sea éste quien proporcione las credenciales válidas. Con esta prueba se pretende advertir al lector de este tipo de ataques para que pueda evitarlos en un futuro.

4.2. Validación de las pruebas

La validación de pruebas se define de la siguiente manera:

1. Para el ataque de encriptación débil se considerará válida siempre que se consiga obtener la clave del punto de acceso, esto además permitirá desencriptar los mensajes que viajan por la red.

2. Para el ataque por contraseña débil, se considerará válido siempre que se consiga la contraseña a partir de un diccionario (este será un diccionario creado específicamente para esta prueba ya que no se cuenta con un punto de acceso con una contraseña real sino con una recreación y la contraseña realmente es conocida)

3. Para el ataque por pin WPS, se considerará válida siempre que se consiga el PIN WPS.

4. Para el ataque KRACK se considerará válida siempre que el cliente se conecte al punto de acceso recreado y se reciba un handshake, en este punto se valorará si el cliente es vulnerable o no.

5. Para el robo de contraseña al cliente, se considera la prueba como válida siempre que se obtenga la contraseña del punto de Acceso.

4.3. Prueba 1: Encriptación débil. Protocolo WEP.

La parte práctica comienza analizando el protocolo WEP, cuya gran vulnerabilidad es el cifrado utilizado RC4 que se ha comentado anteriormente y que no proporciona un encriptado suficientemente sólido, permitiendo descifrar las claves al escuchar una cantidad de paquetes suficientes por parte de un tercero.

Para obtener la clave de un punto de acceso WEP simplemente se necesita un número suficiente de IVs (en esta prueba se ha conseguido con unos 22.000 IVs) que se consiguen capturando el tráfico de la red durante un largo periodo de tiempo, que se puede reducir a minutos si se realiza una inyección de paquetes para estimular paquetes de respuesta.

Con estos paquetes capturados se puede descifrar la clave fácilmente como se puede estudiar en el documento *"Weaknesses in the Key Scheduling Algorithm of RC4"* (Fluhrer, Mantin, & Shamir, 2001), donde se publica el estudio sobre los problemas de este cifrado. En este documento no se profundizará de manera técnica sobre el desencriptado, pero el enlace al estudio estará en las referencias para aquellos que quieran entender la explicación matemática.
Actualmente en muchos entornos de pentesting y en Kali Linux hay herramientas para desencriptar la clave.

Aunque hoy en día los puntos de acceso Wifi no tienen la opción de encriptado WEP, para la prueba se ha utilizado un punto de acceso antiguo para poder demostrar la sencillez con la que se puede encontrar la clave de un punto de acceso que utiliza el protocolo WEP.

Para esto, se utiliza un PC con una máquina virtual con Kali Linux, una antena Alfa Network AWUS036NH con un chipset Ralink RT3070, y un punto de acceso que utiliza el protocolo WEP, el esquema se recrea a continuación:

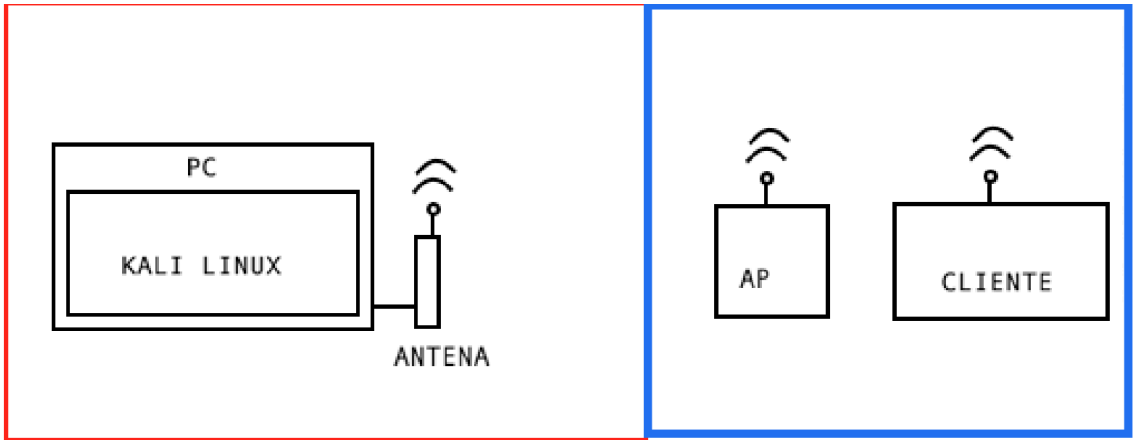


Ilustración 25: Esquema escenario WEP

Donde el recuadro azul recrea la conexión real entre un cliente y el punto de acceso y el recuadro rojo representa al atacante.

El atacante al escanear las redes, si está al alcance de la red azul, encontrará la red con protocolo WEP, como se ve en la siguiente imagen.

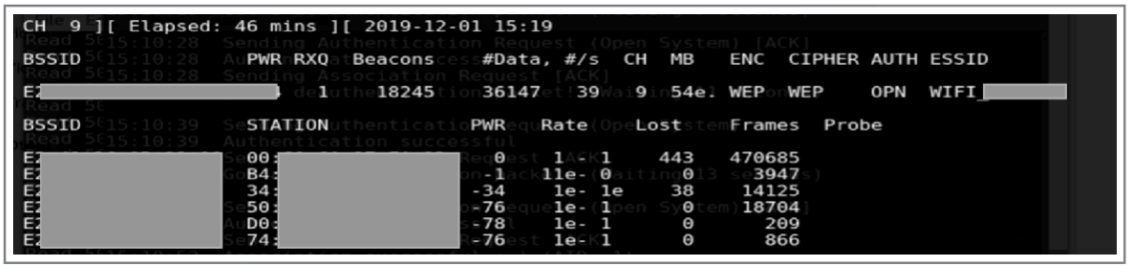


Ilustración 26: Punto de acceso WEP

Una vez seleccionada la víctima, se guardan en un fichero los IVs capturados escuchando la red, como se ve en la siguiente captura:

Ilustración 27: Captura de paquetes en un AP WEP

Para reducir el tiempo de espera se realizan inyecciones de paquetes, y para que un punto de acceso acepte cualquier paquete, la dirección MAC del cliente debe estar asociada, en caso contrario el AP ignorará los paquetes y enviará paquetes de desautenticación sin crear IVs, por ello primero se necesita tener una asociación satisfactoria, como se muestra a continuación:

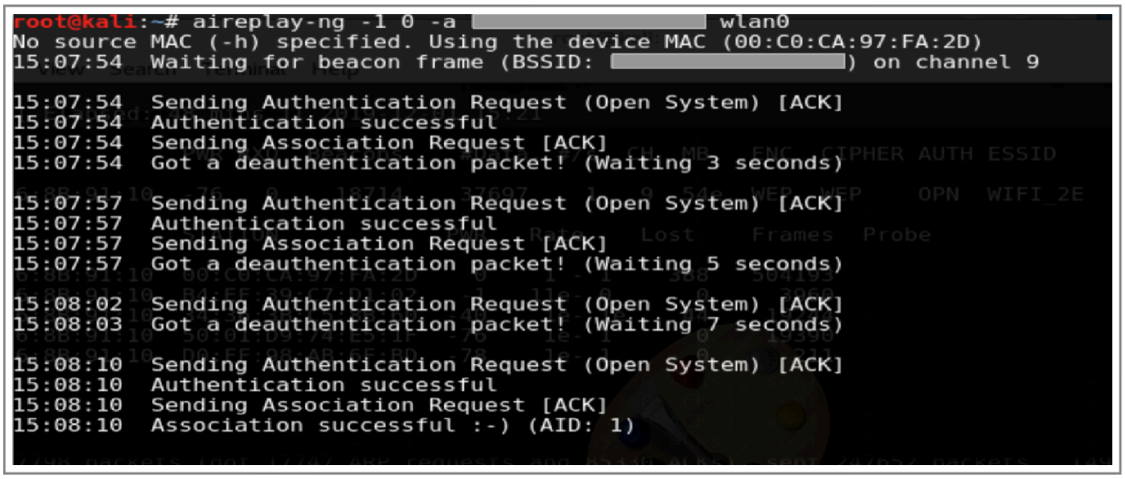


Ilustración 28: Asociación con el AP WEP

Tras recibir varios IVs, al utilizar RC4, la contraseña se puede desencriptar fácilmente, para esta prueba se utiliza airearck-ng (de Kali Linux), así se obtiene la clave en formato hexadecimal y ASCII. Finalmente, tras obtener 22.000 IVs se obtiene la clave, como se muestra en la siguiente figura:

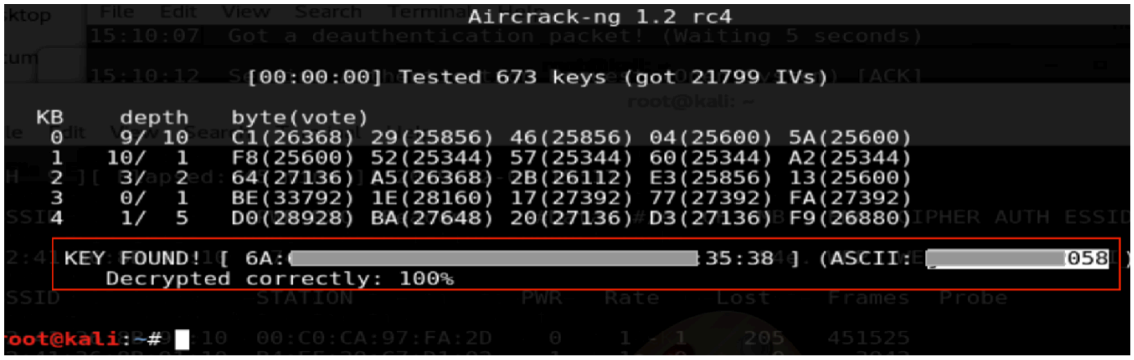


Ilustración 29: Obtención de la clave

Y con ella no solo obtener acceso a la red como se muestra a continuación:

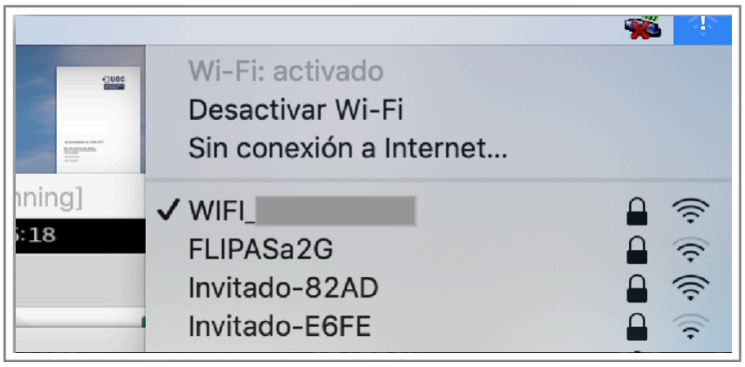


Ilustración 30: Acceso a la red

Sino también ver el tráfico que se ha guardado en la captura de paquetes para hacer el desencriptado:

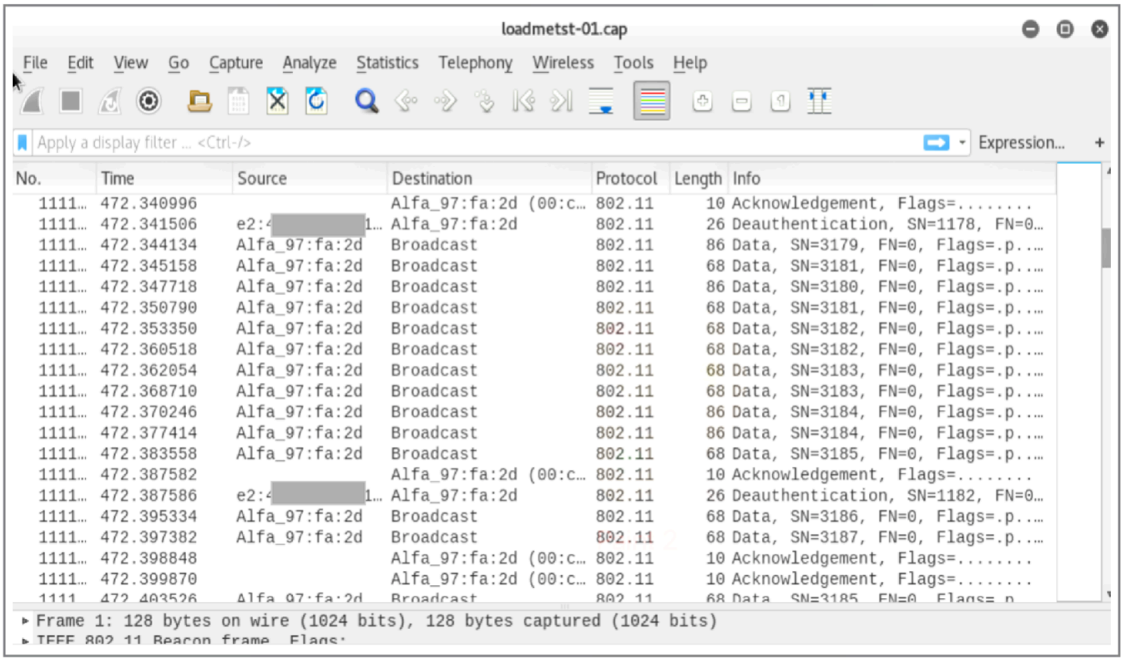


Ilustración 31: Captura de Wireshark del tráfico capturado

Que, aunque en esta prueba se trata de tráfico “falso” creado para ésta, en el caso de un AP real se vería el tráfico sin encriptar (con la clave obtenida) entre este punto de acceso y los clientes, además de el tráfico que se quiera capturar en un futuro, pudiendo obtener información importante de la víctima.

Tras esta demostración, se recomienda no utilizar el protocolo WEP en ninguna red wifi, debido a la débil encriptación, pudiendo quedar expuesto todo el tráfico de la red y haciéndolo “transparente” a atacantes con pocos conocimientos de redes.

4.4. Prueba 2: Contraseñas débiles

Una de las mayores “vulnerabilidades” de las redes Wifi, y que aplica tanto a WEP, como a WPA y a WPA2 son las contraseñas débiles que se vulneran a partir de ataques por diccionario.

Un gran porcentaje de usuarios no cambia la contraseña del router por defecto, y aunque estas contraseñas se consideran sólidas, existen diccionarios que a partir de la dirección MAC del punto de acceso y de la SSID pueden proveer la clave del punto de acceso por defecto. Esto ocurre porque los puntos de acceso están asociados a una contraseña generada por un algoritmo que, si se conoce, se puede conocer la clave de cifrado y así las contraseñas de aquellos routers en los que no se haya cambiado la contraseña por defecto.

Para evitar esto, se recomienda que nada más instalar un nuevo punto de acceso se cambie la contraseña por defecto. De hecho, al entrar por primera vez al router mediante su IP para editar la configuración, el propio operador advierte sobre esto, como se ve en la siguiente figura:

Ilustración 32: Configuración del Punto de acceso

El problema es que muchos usuarios nunca acceden a esta configuración. Simplemente habría que poner en el buscador la IP del router que tiene en la red interna e ingresar el usuario y contraseña.

El otro gran problema son las contraseñas débiles que ponen los usuarios. A continuación, se demostrará cómo una contraseña débil o común permite a un atacante obtener la contraseña del punto de acceso.

Para esto se utiliza Kali Linux en una máquina virtual para hacer escuchas en la red, obtener el handshake y para la comparación de la clave con diccionario, se utilizará un diccionario que contenga la contraseña, una antena Alfa Network AWUS036NH con un chipset Ralink RT3070 y un punto de acceso que utiliza el protocolo WPA2.

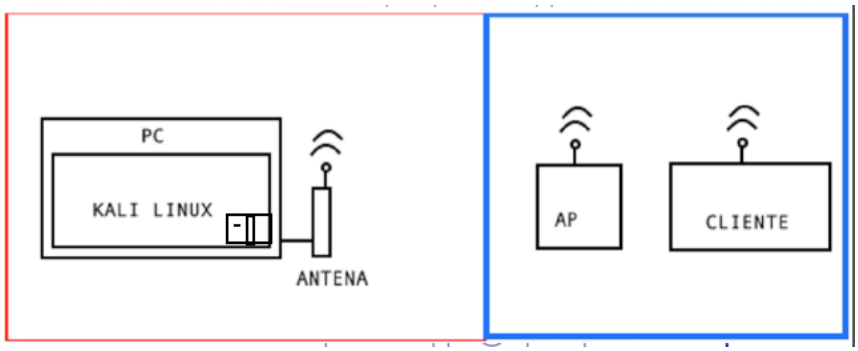


Ilustración 33: Esquema prueba 2

En primer lugar, se realiza un escaneo de los puntos de acceso que estén al alcance de la antena, como se ve a continuación:

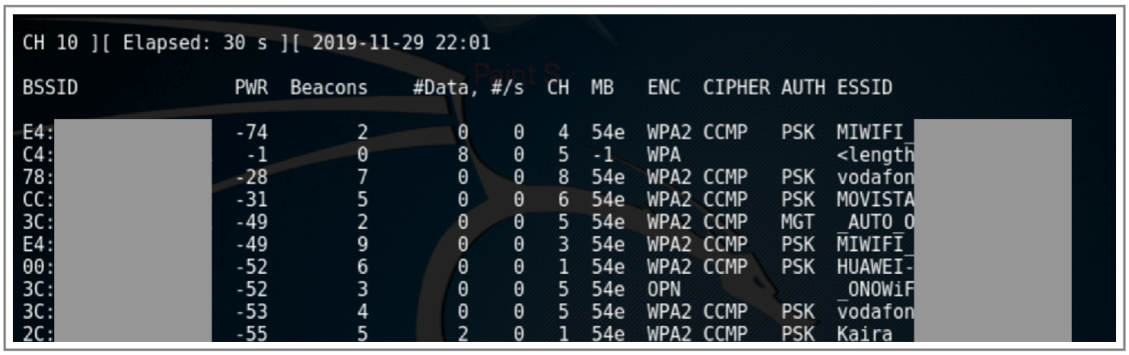


Ilustración 34: Escáner de redes

Simplemente con el escaneo se obtiene mucha información, como BSSID, proveedor del servicio o protocolo de seguridad que utiliza, por esto, se recomienda cambiar el BSSID que viene por defecto y el nombre del punto de acceso por defecto para evitar dar información adicional a posibles atacantes.

Una vez realizado el escaneo, se elige a la víctima del ataque, que en este caso será un punto de acceso de prueba que se está escuchando en el canal 8 del proveedor Vodafone, cuyo BSSID comienza por 78.

Una vez escogida la víctima, el atacante queda a la escucha para ver los posibles clientes que estén conectados a la red si los hay:

Ilustración 35: Escucha de posibles clientes de la red

En esta prueba hay un usuario conectado a la red. Ahora el atacante necesita conseguir el handshake de la conexión, que como se comenta en el capítulo anterior, en WPA2 se utiliza el 4-way-handshake en el proceso de autenticación, y una vez el cliente es autenticado se inicia el proceso de compartición de información en el canal cifrado, por tanto, el atacante debe esperar a que un usuario realice este proceso de autenticación. Como este proceso puede durar mucho tiempo, se puede reducir el tiempo de espera simplemente desautenticando al cliente para forzarle a volver a autenticarse.

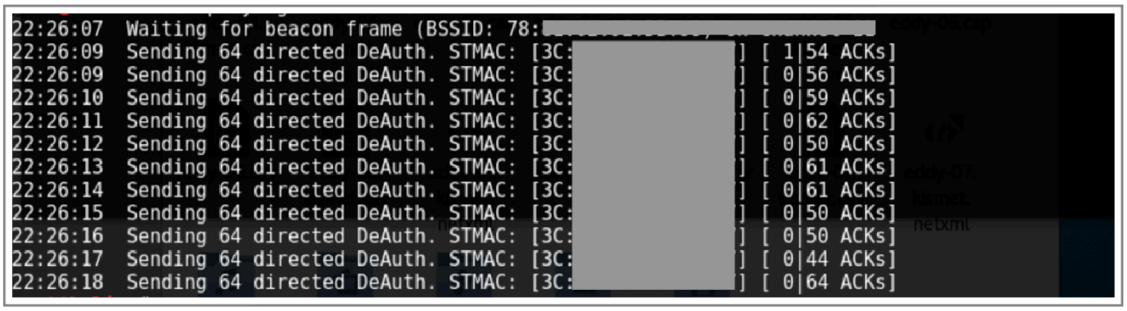


Ilustración 36: Desautenticación del cliente

Tras la desautenticación del cliente, y en menos de dos minutos se consigue el handshake, como se observa en la siguiente ilustración:

Ilustración 37: Obtención del handshake

Aquí es cuando viene el problema de las contraseñas débiles, y aunque el protocolo WPA2 cuenta con el 4-way handshake, y aun siendo uno de los protocolos más seguros, es fácil obtener la contraseña de un punto de

acceso si la contraseña es débil o común. Esto es porque hay diccionarios ya creados por otros usuarios donde se comparan con el handshake de manera automática hasta averiguar la contraseña, es decir, un atacante no tiene que probar una a una las contraseñas más comunes, sino que simplemente se puede hacer una comparación con librerías con millones de contraseñas con las que en unos minutos o en unas horas puede dar con estas contraseñas.

A continuación, se muestra que en un tiempo aproximado de 6 horas y media se pueden probar las millones de claves que hay en el fichero “rockyou.txt”, un diccionario de claves conocido.

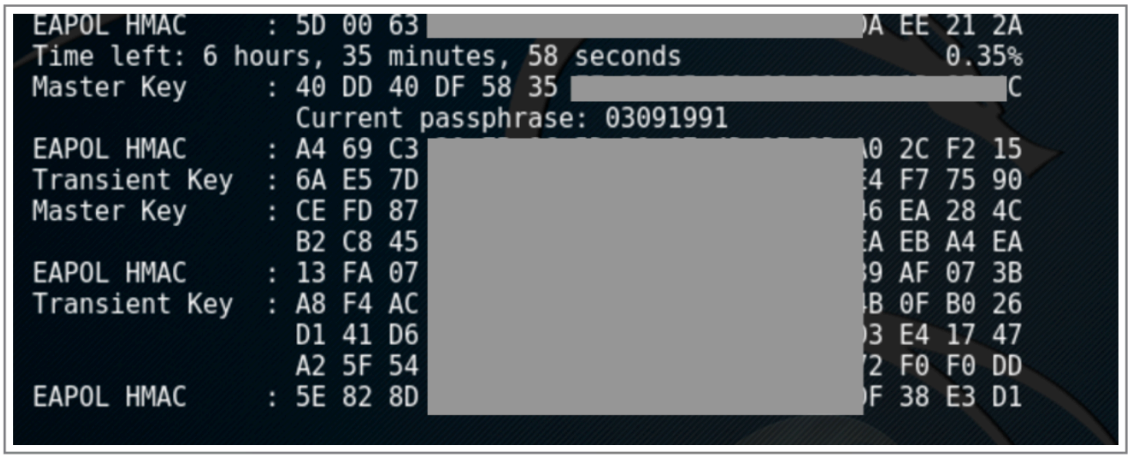


Ilustración 38: Comparación con el diccionario "rockyou"

En este documento se recomienda no utilizar contraseñas comunes, nombres, secuencias en las que únicamente haya números o secuencias que puedan tener algún sentido para la víctima. Se recomienda una secuencia aleatoria de números y letras utilizando mayúsculas y minúsculas, y comprobar que esta contraseña no sea parte de los diccionarios comunes. En este caso, utilizando el diccionario “rockyou.txt”, se ven algunos ejemplos de las contraseñas más comunes utilizadas por los usuarios en diferentes idiomas, aunque también hay diccionarios específicos para un idioma seleccionado. A continuación, se muestran algunas de estas contraseñas:

```
li123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
```

Ilustración 39: Ejemplos de contraseñas débiles

Estas contraseñas podrían parecer demasiado obvias, pero realmente muchos usuarios las utilizan. Y en aproximadamente seis horas se podrían testear millones de posibles contraseñas, algunas no tan obvias como por ejemplo 03091991, (lo que parece una fecha de nacimiento).

Como en esta prueba la contraseña del punto de acceso al que se está atacando es conocida, y es una combinación aleatoria que no está dentro de este diccionario, se ha creado un nuevo diccionario con 5 palabras (para no tener que esperar demasiado tiempo), y donde la cuarta es la contraseña actual, y el resultado es el siguiente:

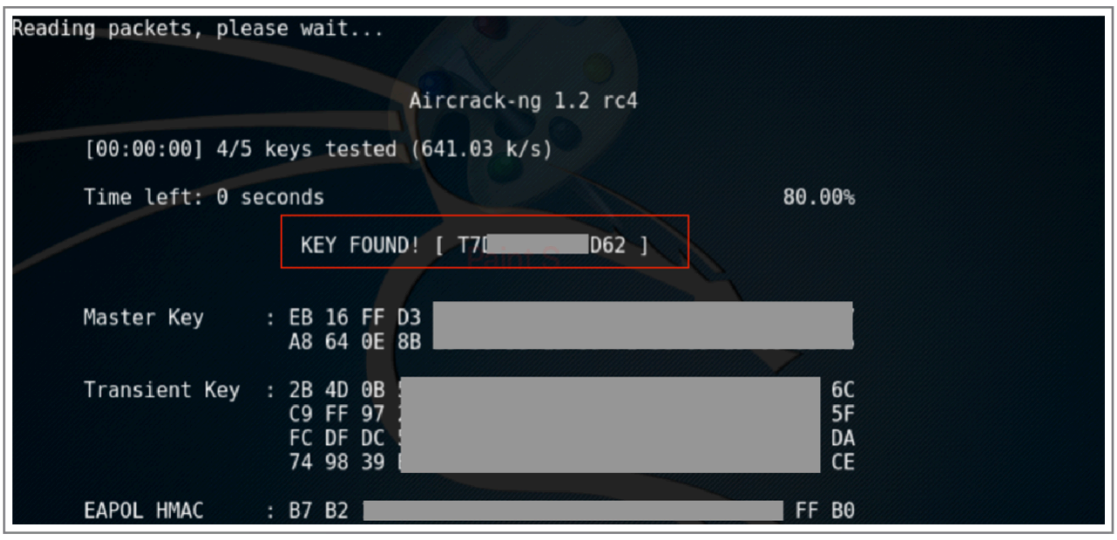


Ilustración 40:Obtención de la clave de acceso

Comparando el handshake con el diccionario creado que tiene entre ellas la contraseña del punto de acceso, la contraseña ha sido encontrada por el atacante.

4.5. Prueba 3: Uso de WPS

Aunque el estándar WPS permite una configuración rápida y sencilla en los diferentes modos estudiados, y puede resultar atractiva para un usuario, este estándar es muy vulnerable a ataques de fuerza bruta, ya que se puede acceder al punto de acceso con tan solo conocer el PIN de 8 dígitos, lo que se consideraría algo moderadamente seguro en un ataque de fuerza bruta con un delay de 1 segundo por cada prueba, ya que se necesitarían 1.000.000.000 segundos, equivalente a más de 31 años. Pero realmente no se necesita todo este tiempo para realizar un ataque de fuerza bruta en WPS, ya que utiliza un esquema que lo hace más vulnerable, y que es el siguiente:

Se utilizan 8 mensajes llamados M1, M2, M3, M4, M5, M6, M7 y M8 que serán las peticiones y respuestas entre el enrollee y el registrar:

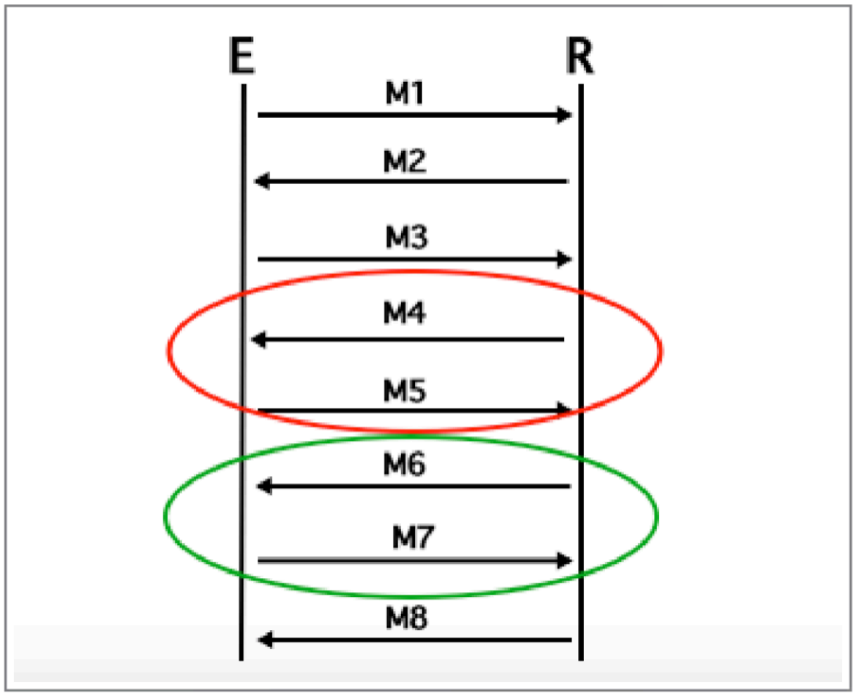


Ilustración 41: Intercambio de mensajes entre enrollee y registrar

Lo importante de este esquema son los mensajes M4 y M5. En el mensaje M4, el registrar (o cliente) envía los 4 primeros dígitos del pin al enrollee (o Punto de Acceso), y el mensaje M5 se recibe si estos 4 primeros dígitos son correctos. Entonces, con este esquema de envío de mensajes, se pueden tener los 4 primeros dígitos con un total de 10.000 combinaciones, que si se hace una consulta cada segundo, se podría obtener en 10.000 segundos, es decir, en menos de 3 horas.

Una vez obtenidos los 4 primeros dígitos simplemente habría que obtener los cuatro últimos, pero teniendo en cuenta que el último dígito de estos ocho es un checksum de los anteriores, solo quedarían por probar 3 dígitos (y añadir como último el checksum de los anteriores). En los mensajes M6 y M7 el registrar manda los 4 últimos dígitos al Enrollee, y este confirma si son válidos.

En total, para probar todas las combinaciones en un ataque de fuerza bruta se necesitan 10.000 + 1.000 = 11.000 intentos, que a intento por segundo serían poco más de 3 horas, un tiempo de espera muy bajo para conseguir realizar con éxito un ataque de fuerza bruta.

Siempre que se publican nuevas vulnerabilidades, las actualizaciones de firmare de los puntos de acceso tratan de mitigarlas, y aunque actualmente la mayoría de puntos de acceso comerciales nuevos llevan la función WPS activada por defecto, como se ve en la figura 42, gran parte de ellos tratan de impedir este tipo de ataques al aumentar el tiempo entre requests de PINs, o añadiendo una funcionalidad en la que al hacer más de tres peticiones de PINs fallidas, estas se bloquean hasta que se hace un reinicio del punto de acceso (como se muestra en la figura 44) , pero hay muchos puntos de acceso que o bien sí son vulnerables a este ataque o bien utilizan uno de los pines por defecto conocidos.

Ilustración 42: Configuración del punto de acceso

Con un rápido escaneo de la red se ven qué puntos de acceso tienen WPS activo y cuáles no son vulnerables a un ataque de fuerza bruta

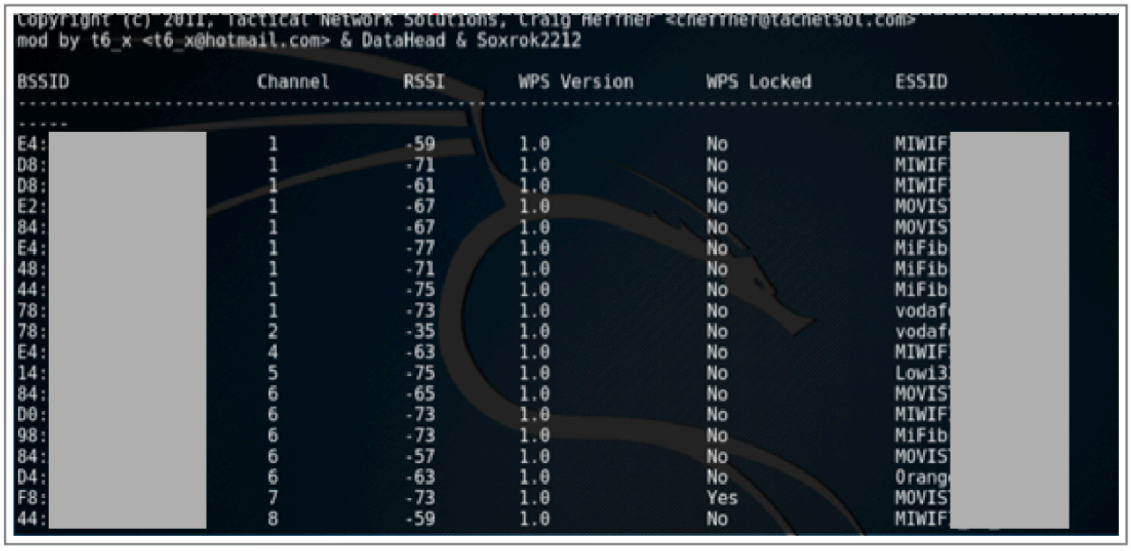


Ilustración 43: Escáner de la red

En un punto de acceso nuevo que se pone a prueba en este escenario, aunque tiene por defecto WPS activado, no es vulnerable ya que se bloquea después de tres intentos fallidos.

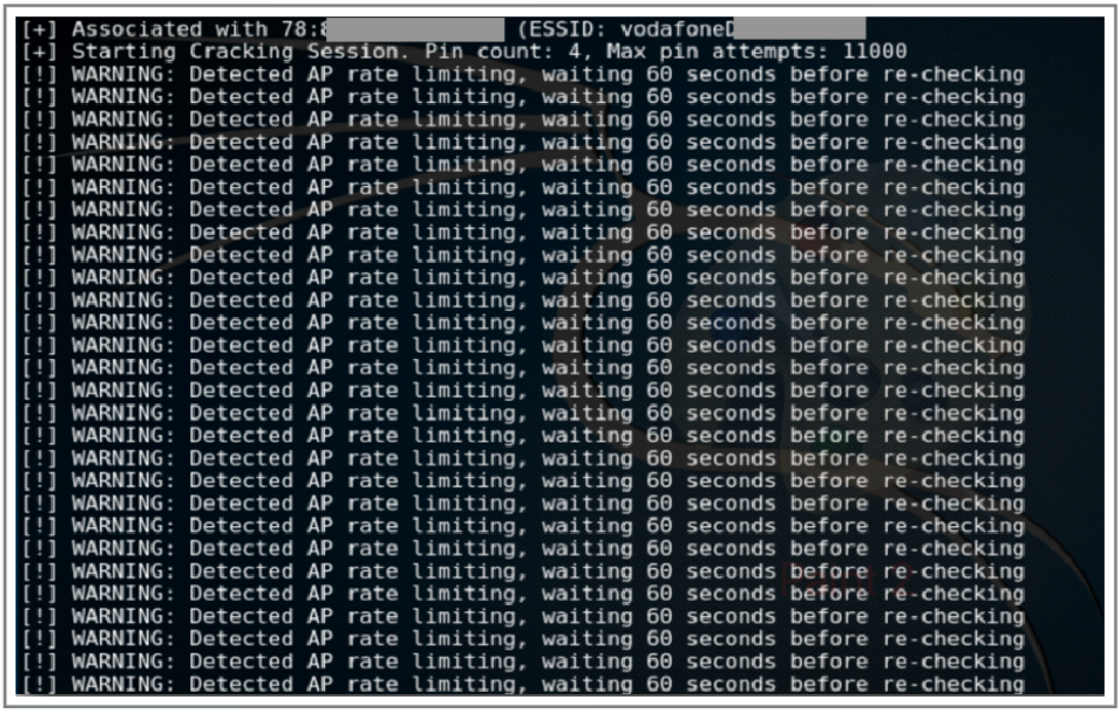


Ilustración 44: Bloqueo de petición de PIN después de tres intentos fallidos

Pero sí se ha conseguido obtener el PIN de un punto de acceso no actualizado con el PIN por defecto. Al ser este PIN el que primero prueba, se obtiene el pin al momento, pero normalmente el proceso puede durar unas horas.

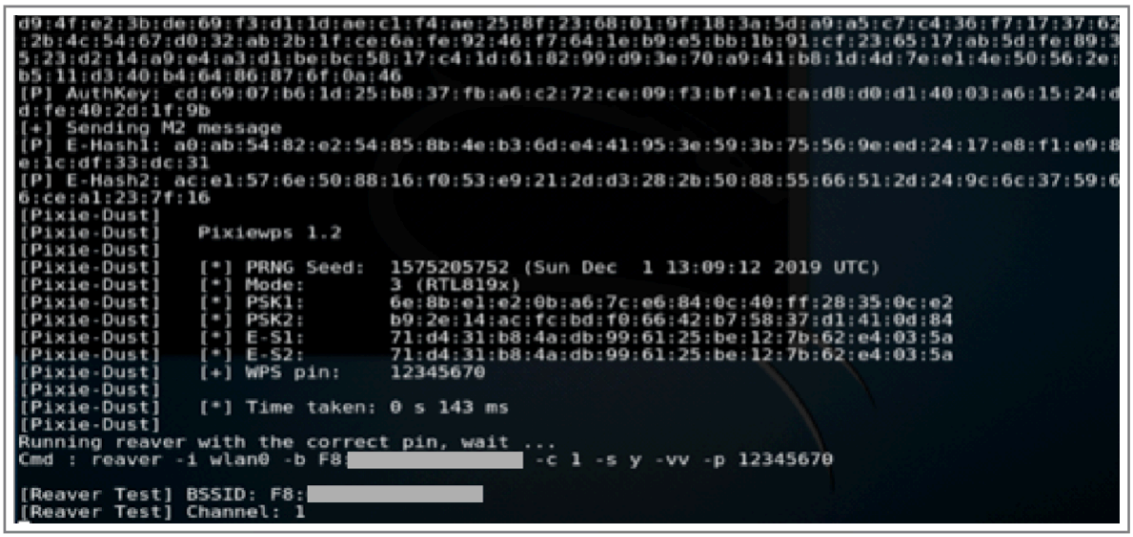


Ilustración 45: Obtención del PIN WPS

En la bibliografía se deja un enlace para que el lector pueda comprobar si su punto de acceso está entre la lista de puntos de acceso vulnerables y de los puntos de acceso con PINs por defecto. (Lista1, 2019) (Lista2, 2019).

Por tanto, se han hecho pruebas en dos escenarios, uno con un AP no vulnerable que cuenta con bloqueo tras tres PINs incorrectos, y otro con un AP vulnerable a este ataque. El esquema de las pruebas es el siguiente:

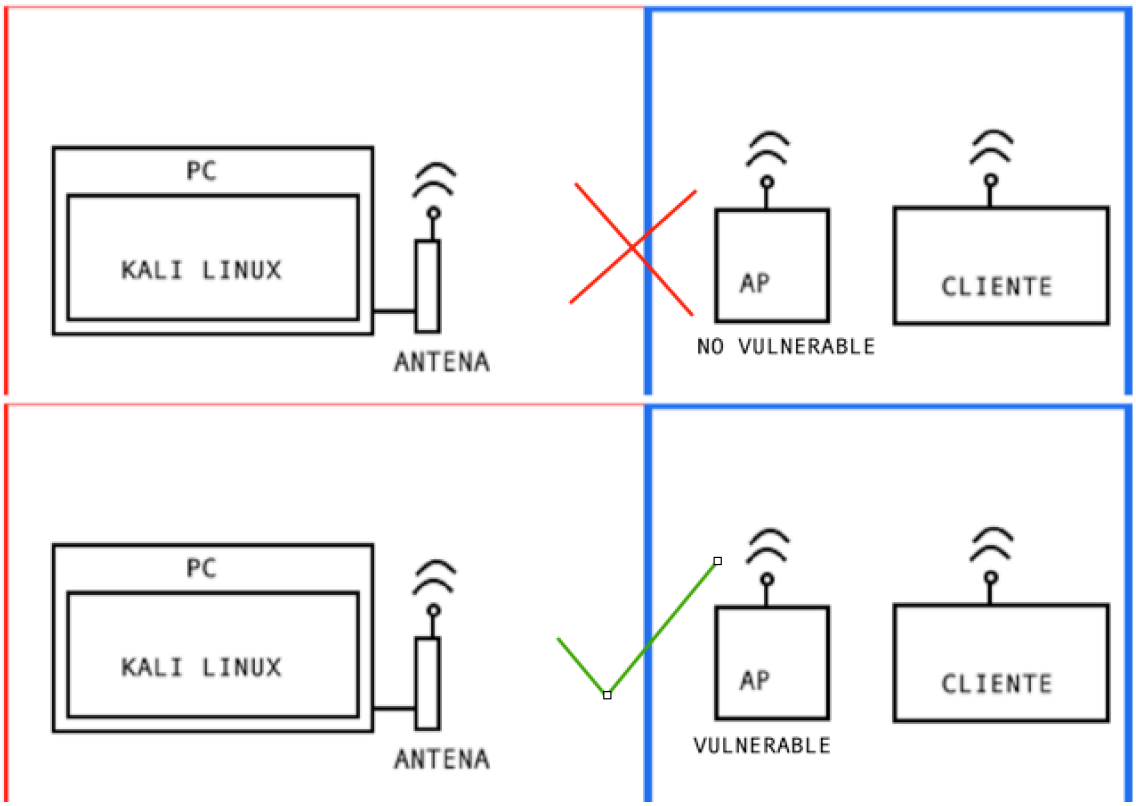


Ilustración 46: Escenario de pruebas

Aun así, se recomienda no utilizar la funcionalidad WPS, además de deshabilitar la opción de WPS. Otras recomendaciones para evitar este tipo de ataques son, por un lado, proteger de manera física el punto de acceso, para evitar un acceso no deseado en el modo NFC y en el PBC, y por otro lado filtrar por MAC el acceso de clientes al punto de acceso, restringiendo el acceso a todos los dispositivos, excluyendo los dispositivos cuyas direcciones MAC se indiquen, que serán las direcciones MAC de los dispositivos permitidos en la red.

4.6. Prueba 4: Importancia de las actualizaciones: ataque KRACK

Las redes WPA2 se habían considerado muy seguras hasta que en 2017 se publicó la primera vulnerabilidad, descubierta por Mathy Vanhoef llamada Key Reinstallation Attack o KRACK. Mediante este ataque, el atacante puede ver el tráfico de una red WPA2 con el tráfico desencriptado, lo que supone que todos los paquetes, que pueden contener emails, fotos, contraseñas, números de tarjetas de crédito, etc, queden expuestos a terceros.

El ataque KRACK consiste en 10 vulnerabilidades que pueden explotarse de manera independiente y que deben mitigarse, y según la parte de comunicación que se ve afectada, se han dividido en diferentes CVEs (Common Vulnerabilities and Exposures):

- CVE-2017-13077 afecta al cliente, y se describe de la siguiente manera: *"El acceso protegido Wi-Fi (WPA y WPA2) permite la reinstalación de la clave temporal (TK) de la clave transitoria por pares (PTK) durante el 4-way handshake, lo que permite que un atacante dentro del alcance de la radio reproduzca, descifre o falsifique paquetes."* (NVD-13077, s.f.)

- CVE-2017-13078 afecta al cliente, y se define como: *"El acceso protegido Wi-Fi (WPA y WPA2) permite la reinstalación de la clave temporal grupal (GTK) durante el 4-way handshake, lo que permite a un atacante dentro del alcance de la radio reproducir fotogramas desde los puntos de acceso a los clientes."* (NVD-13078, s.f.)

- CVE-2017-13079 afecta al cliente, y se define como: *"El acceso protegido Wi-Fi (WPA y WPA2) que admite IEEE 802.11w permite la reinstalación de la clave temporal de grupo de integridad (IGTK) durante el protocolo de enlace de cuatro vías, lo que permite a un atacante dentro del alcance de la radio falsificar paquetes desde los puntos de acceso a los clientes."* (NVD-13079, s.f.)

- CVE-2017-13080 describe la siguiente vulnerabilidad: *"El acceso protegido Wi-Fi (WPA y WPA2) permite la reinstalación de la clave temporal grupal (GTK) durante handshake de la clave de grupo, lo que permite que un atacante dentro del alcance de la radio reproduzca paquetes desde los puntos de acceso a los clientes."* (NVD-13080, s.f.)

- CVE-2017-13081 afecta al cliente, y enuncia lo siguiente: *"El acceso protegido a Wi-Fi (WPA y WPA2) que admite IEEE 802.11w permite la reinstalación de la clave temporal de grupo de integridad (IGTK) durante el handshake de la clave de grupo, lo que permite a un atacante dentro del alcance de la radio falsificar marcos desde puntos de acceso a clientes*." (NVD-13081, s.f.)

- CVE-2017-13082 afecta al punto de acceso y se describe como: *"El acceso protegido Wi-Fi (WPA y WPA2) que admite IEEE 802.11r permite la reinstalación de la clave temporal (TK) de clave transitoria por pares (PTK) durante el handshake, lo que permite que un atacante dentro del alcance de radio replique o desencripte paquetes."* (NVD-13082, s.f.)

- CVE-2017-13084 afecta al cliente con lo siguiente: "*El acceso protegido Wi-Fi (WPA y WPA2) permite la reinstalación de la clave transitoria de estación a estación (STSL) durante el protocolo de enlace PeerKey, lo que permite a un atacante dentro del alcance de la radio reproducir, descifrar o falsificar paquetes."* (NVD-13084, s.f.)

- CVE-2017-13086 afecta al cliente de la siguiente manera: *"El acceso protegido Wi-Fi (WPA y WPA2) permite la reinstalación de la clave de igual (TPK) Tunneled Direct-Link Setup (TDLS) durante el protocolo de enlace TDLS, lo que permite que un atacante dentro del alcance del punto de acceso descifre o falsifique paquetes."* (NVD-13086, s.f.)

- CVE-2017-13087 afecta al cliente de este modo: *"El acceso protegido a Wi-Fi (WPA y WPA2) que admite 802.11v permite la reinstalación de la clave temporal grupal (GTK) al procesar un paquete de respuesta de modo de suspensión de gestión de red inalámbrica (WNM), lo que permite a un atacante dentro del alcance del punto de acceso reproducir tramas desde puntos de acceso a los clientes"* (NVD-13087, s.f.)

- CVE-2017-13088 afecta al cliente y en este se describe la siguiente vulnerabilidad: *"El acceso protegido a Wi-Fi (WPA y WPA2) que admite 802.11v permite la reinstalación de la clave temporal de grupo de integridad (IGTK) cuando se procesa un paquete de respuesta de modo inactivo de gestión de red inalámbrica (WNM), lo que permite a un atacante dentro del alcance de radio reproducir paquetes del acceso."* (NVD-13088, s.f.)

Estas vulnerabilidades permiten a un atacante ver el tráfico desencriptado o incluso inyectar malware en la red, y es que el eje principal vector del ataque se centra en 4-way handshake de WPA2, que comprueba las credenciales del usuario como se vio en el estándar de autenticación 802.1X. Durante el 4-way handshake se generan nuevas claves de cifrado que se instalan tras recibir los mensajes M3 y M4. Lo que se consigue mediante el ataque KRACK es manipular o repetir el M3 (mensaje 3) para conseguir reinstalar la clave que ya se ha utilizado.

El proceso del ataque es el siguiente:

En primer lugar un atacante pide acceso a una red iniciándose un 4-way handshake donde en el mensaje 3 se negocia una nueva clave de cifrado, pero en este caso, el cliente atacante no envía un OK indicando que ha recibido este mensaje, lo que deriva en que el punto de acceso debe retransmitir el mensaje 3 una y otra vez, haciéndose que se resetee el campo nonce de la trama EAPOL, que se encarga de contar los paquetes retransmitidos. Aquí, el atacante puede forzar reseteos nonce guardándolos y retransmitiendo los mensajes. Reutilizando los nonce es posible descifrar los paquetes y retransmitirlos, ya que utiliza la misma clave de descifrado que se utiliza con valores nonce. Así se puede analizar el tráfico que existe en esta red entre otros clientes y el punto de acceso o incluso inyectar malware a la red. A continuación, en el siguiente esquema se ve el mensaje recalcando el mensaje M3, en el que se hace el ataque KRACK:

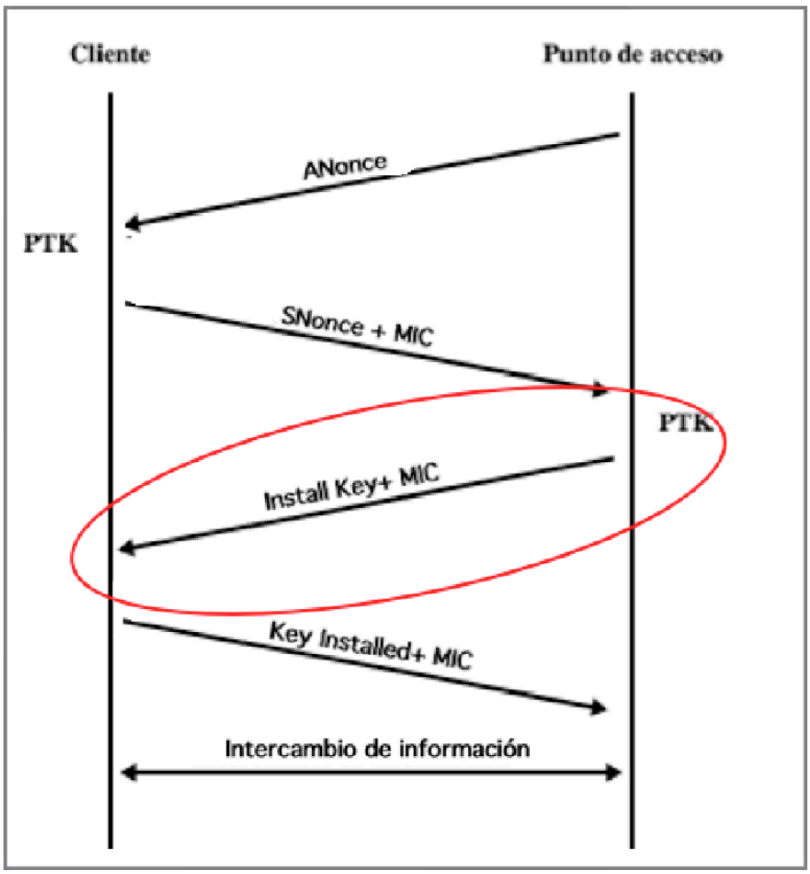


Ilustración 47: Esquema 4-way-handshake resaltando el mensaje 3

En esta parte práctica se ha querido verificar si varios clientes son vulnerables a este ataque. En el anexo se dejan detallados los pasos seguidos y los problemas resueltos que se han encontrado al hacer este ataque. Este es el único punto que se hará paso a paso ya que en internet no hay demasiada información, no está demasiado clara y no hay muchos posts con los problemas que se pueden encontrar al hacer este ataque (al contrario que en los otros ataques que se han hecho en este documento), por lo que se cree que puede servir de ayuda al lector. En este caso se han probado un Macbook Pro utilizando macOS Mojave Versión 10.14.6 y un Iphone con una versión de software 12.4.1, y los resultados obtenidos concluyen que no son vulnerables y están parcheados.

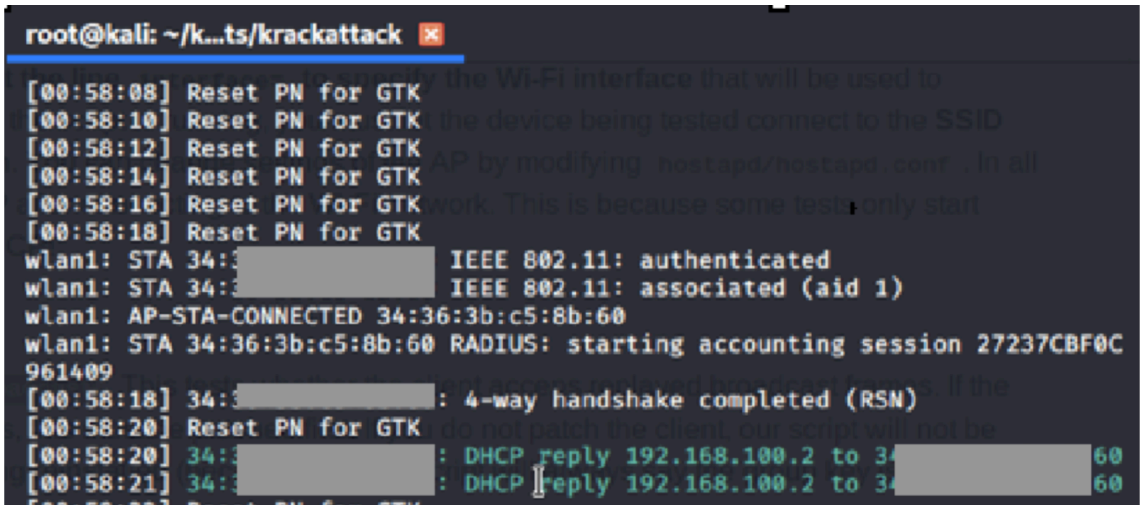


Ilustración 48: Cliente no vulnerable

Se explica el proceso para poder probar esto en la parte del anexo. Si se encuentra que un cliente es vulnerable habiendo hecho las actualizaciones de software, se recomienda contactar con el proveedor para alertar de esta vulnerabilidad.

Hoy en día la vulnerabilidad KRACK, o Key Registraron Attack es una de las más sonadas en el último año, y de la que todavía no hay demasiada documentación. Muchas alarmas saltaron cuando se publicó esta vulnerabilidad, pero realmente hoy en día, y como se ha visto en las pruebas, se han creado parches para mitigarla, y estos parches son compatibles con versiones anteriores, por lo que si un punto de acceso está parcheado puede seguir comunicándose con un cliente y viceversa. Este parche asegura que una clave solo se instale una vez, evitando el ataque, por lo que si se parchean no debería haber ningún problema en utilizar WPA2, a priori.

Se recomienda actualizar el firmware del punto de acceso y realizar actualizaciones de software en los dispositivos cliente. Esto, además de proteger frente a ataques Wireless también protegerá ante otro tipo de ataques cuyas vulnerabilidades sean conocidas, y es que las actualizaciones de software no solo añaden nuevas funcionalidades a los dispositivos, sino que parchean vulnerabilidades que pueda haber, es por esto por lo que realmente es importante tener los dispositivos siempre actualizados, de hecho, es el gran problema de los ataques más relevantes de los últimos años, como el ataque de 2017 a Telefónica, a hospitales o a centros educativos ente otros:

Ilustración 49: Noticia sobre el ataque a varias empresas (elperiodico, 2017)

O el reciente ataque a grandes empresas como Cadena Ser o Everis:

Ilustración 50: Noticia sobre el ataque a varias empresas (adslZone, 2019)

Podrían haber sido prevenidos con actualizaciones de software de los ordenadores Windows, ya que las vulnerabilidades explotadas en ambos casos habían sido anteriormente descubiertas y Microsoft había informado de esta vulnerabilidad que ya estaba solucionada en sus nuevas publicaciones.

Así pues, tanto para la utilización de redes Wifi de manera segura como para la protección frente a otros tipos de ataques, se recomiendas utilizar las ultimas versiones de software en todos los dispositivos.

4.7. Prueba 5: Proporcionar la clave al atacante

Para hacer esta prueba se utiliza Wifislax, un software de análisis Wireless utilizado tanto en ámbitos profesionales como personales que permite conocer el nivel de seguridad de la red Wireless mediante sus diferentes herramientas. Está especializada en la auditoria de redes inalámbricas, pero también tiene herramientas de gestión.

Para esta prueba se utiliza un USB booteable con Wifislax, que es lo que recomienda en la página web oficial, para asegurar un buen funcionamiento.

Se trata de una herramienta muy fácil de utilizar, y que se recomienda utilizar, ya que posee scripts que automatizan los comandos que se escribirían en la terminal, y es muy fácil de utilizar incluso para aquellos que no tengan demasiados conocimientos en seguridad informática.

La herramienta que se utiliza para esta prueba es Linset, y lo que se hará será intentar “engañar” a un cliente para que él mismo proporcione la contraseña de su AP.

El esquema de la prueba sería el siguiente:

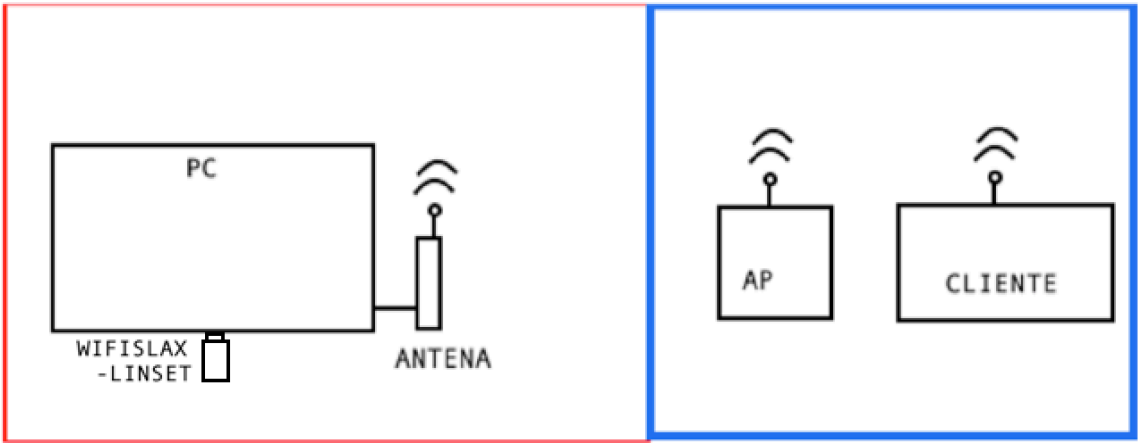


Ilustración 51: Esquema de la prueba

Se comienza fijando un AP que será la víctima, en este caso, la red se llama “wifi”. En la siguiente ilustración se muestra el escáner de las redes al alcance del PC atacante

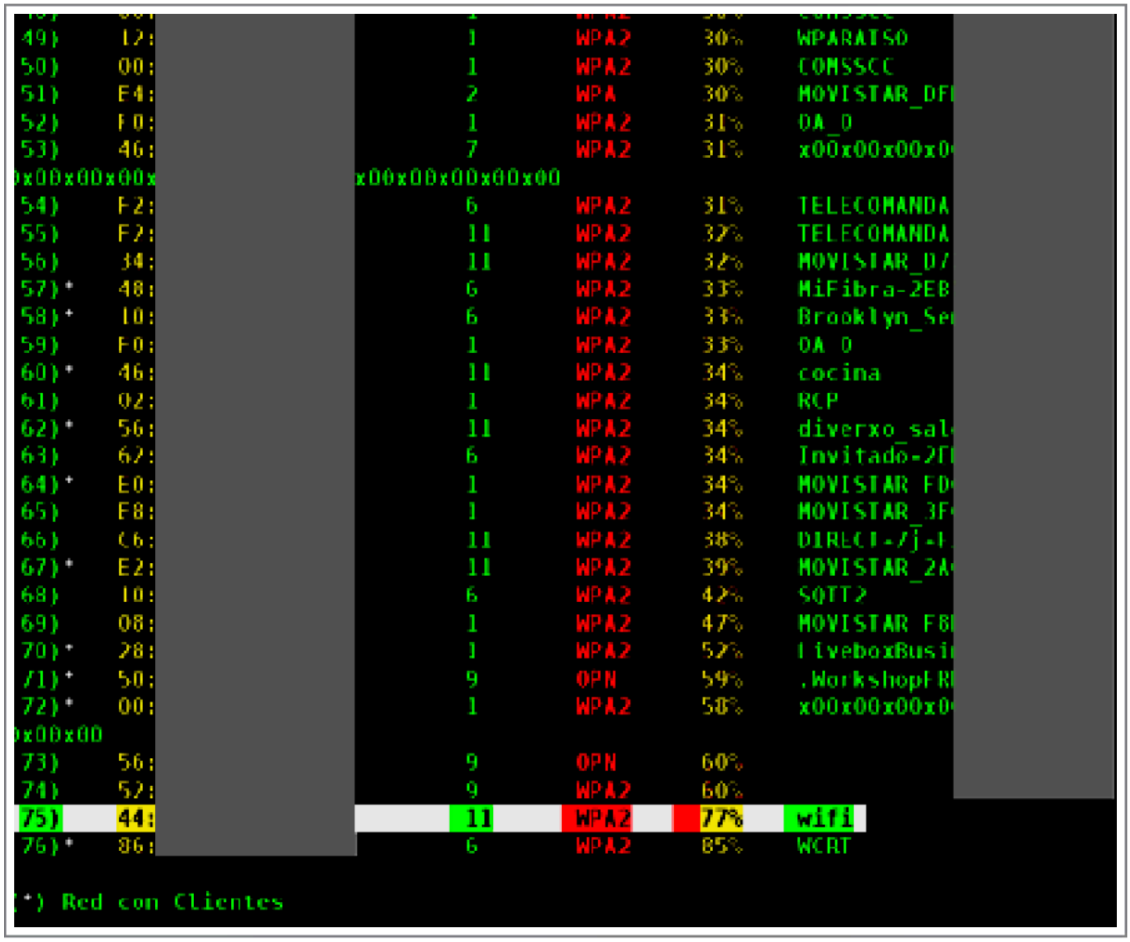


Ilustración 52: Escáner de las redes

Una vez seleccionado el objetivo, se elige en la herramienta en qué modo se realizará el punto de acceso falso (se utiliza Hostapd), y el modo en el que se intenta obtener el handshake (en este caso mediante desautenticación masiva al AP objetivo).
No es demasiado complicado realizar estos pasos mediante línea de comandos y cambiando la configuración de un fichero hostapd.conf (esto ya se ha hecho en el ataque KRACK y se deja en el anexo), aun así, con Wifislax simplemente hay que seleccionar entre tres opciones, e incluso recomiendan una, lo que hace pensar que cualquier persona, sin conocimientos de informática, podría atacar la red.

Una vez obtenido el handshake, y tras seleccionar el idioma en el cual le aparecerá el mensaje engañoso al cliente, las siguientes pantallas aparecerán:

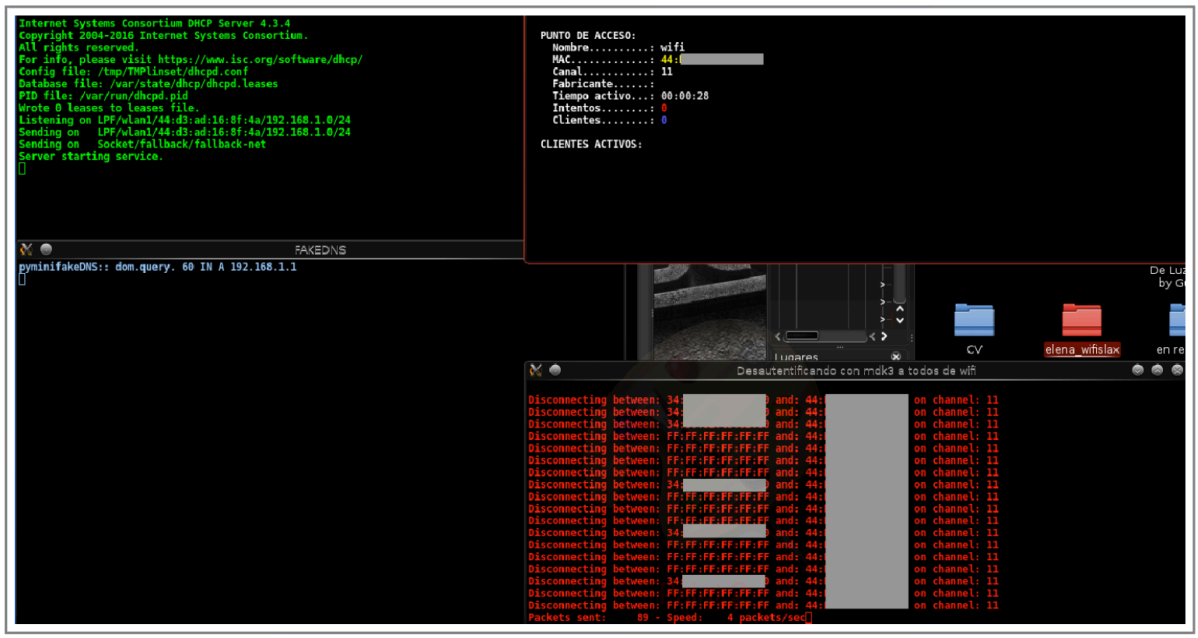


Ilustración 53: Pop Ups de Wifislax

Por un lado, se puede ver la información del punto de acceso replicado, que actualmente no tiene clientes y ninguno de los clientes ha hecho ningún intento de insertar una contraseña.

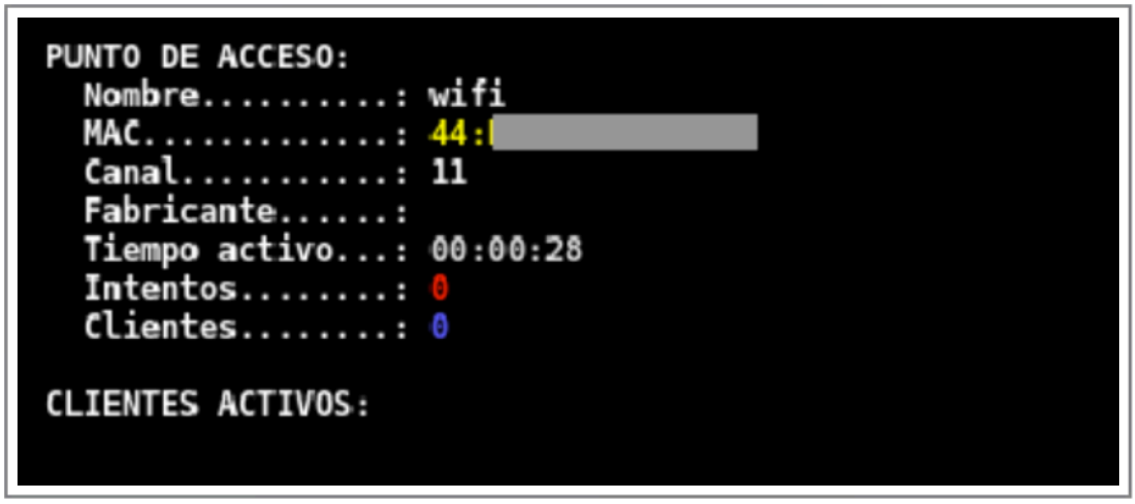


Ilustración 54: Punto de acceso replicado en Wifislax

Por otro lado, se están desautenticando a los clientes que estaban en el punto de acceso objetivo, por lo que los clientes se están desconectando de esta red.

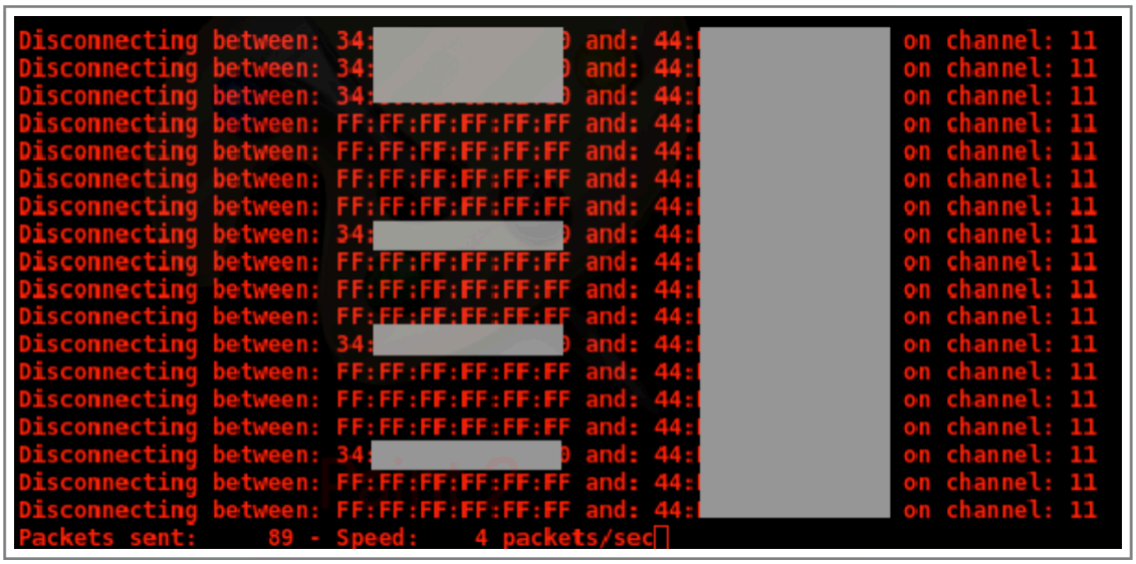


Ilustración 55: Desautenticación de clientes en Wifislax

Se manda la interfaz web a la víctima para que introduzca la contraseña del punto de acceso.

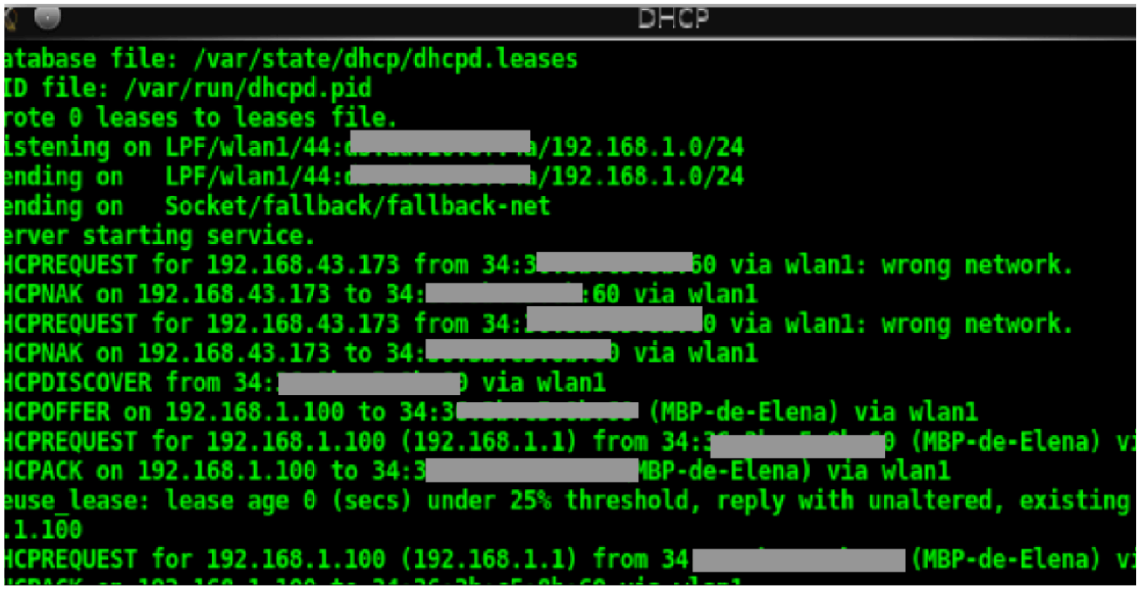


Ilustración 56: Interfaz web con mensaje engañoso

Además, en la siguiente terminal se ven las peticiones web a las que el cliente está queriendo acceder :

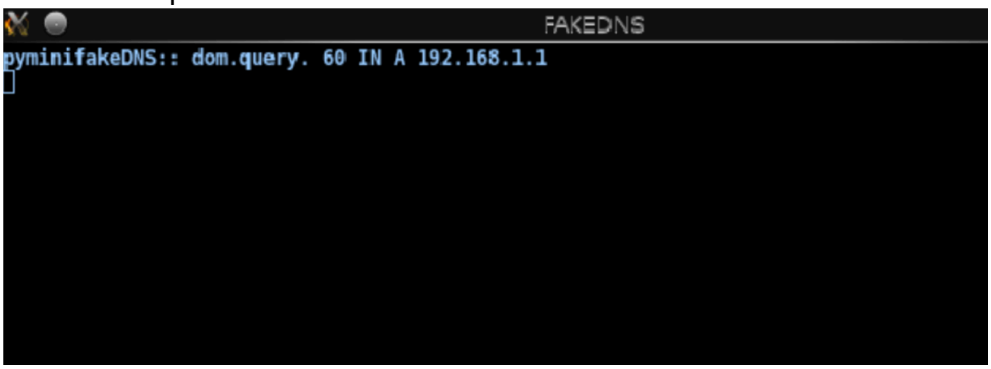


Ilustración 57: Peticiones Web

Una vez comenzado el ataque, el cliente deja de tener conexión con el punto de acceso, esto puede ocurrir en alguna ocasión real, por lo que el cliente puede no sospechar nada. Cuando el cliente busca su red para conectarse, no aparecerá su red, en cambio aparecerá el punto de acceso recreado, que tendrá el mismo nombre que el punto de acceso original, pero no aparecerá el símbolo del candado que aparece en las redes seguras. Este es el primer punto en el que se debe sospechar que se está produciendo un ataque en la red. Siempre hay que conectarse a un punto de acceso seguro, y normalmente esto se identifica con un candado al lado del nombre del punto de acceso, aun así, muchos clientes no suelen fijarse en esto.

Una vez el cliente selecciona conectarse al punto de acceso recreado (creyendo que es el suyo original), saldrá una interfaz web donde le indica que por razones de seguridad debe ingresar la contraseña del punto de acceso. Este mensaje puede ser modificado y personalizado, pudiendo averiguar que tipo de dispositivo utiliza el cliente para hacer que este mensaje parezca lo más real posible. En este punto, el cliente ingresa la contraseña del punto de acceso. En el supuesto en el que se inserte una contraseña incorrecta, el cliente recibirá el aviso de contraseña incorrecta y tendrá que volver a insertar una nueva hasta insertar la correcta.

En este caso, el atacante verá lo siguiente:

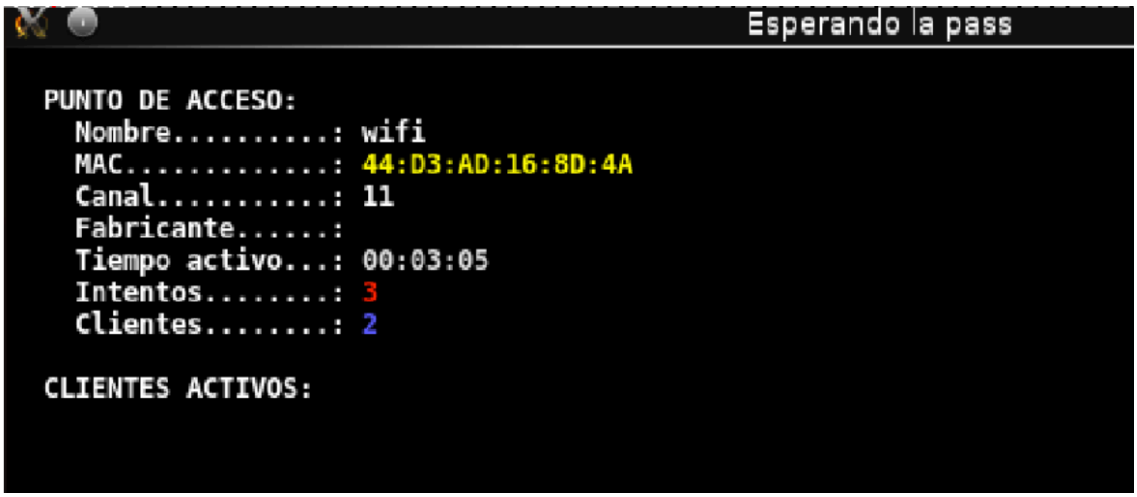


Ilustración 58: Inserción de contraseña incorrecta

Entonces el ataque continuará, mientras se chequea si la clave del punto de acceso es el correcto, y seguirá siendo así hasta que se compruebe que la contraseña permite acceder al punto de acceso. Si un usuario se encuentra en esta situación o tiene sospechas de estar siendo atacado por un ataque como este, la única solución será reiniciar el router, ya

que sino, estará siendo desautenticando de la red hasta que el atacante consiga la contraseña correcta.

En este caso, se ha intentado insertar la contraseña 3 veces de forma errónea, y sigue pidiendo que se necesita una contraseña correcta. Además, el atacante tiene la información de las páginas web a las que el cliente está intentando acceder, y la interfaz gráfica que se está enviando.

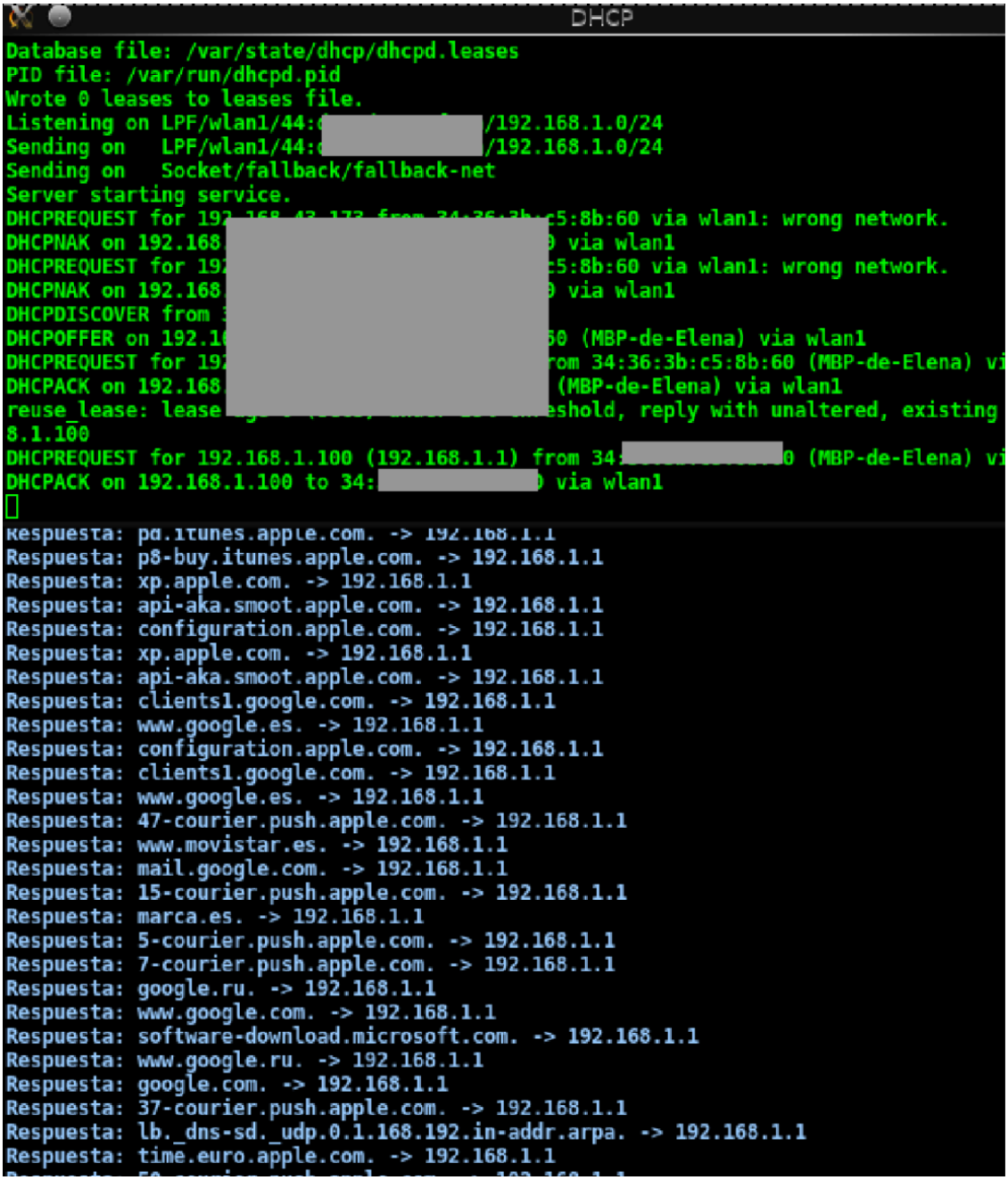


Ilustración 59: Interfaz y peticiones web

Una vez el cliente inserte la contraseña correcta, aparecerá la siguiente pantalla, donde se muestra la contraseña que permite acceder al punto de acceso, además de guardarse en un fichero .txt

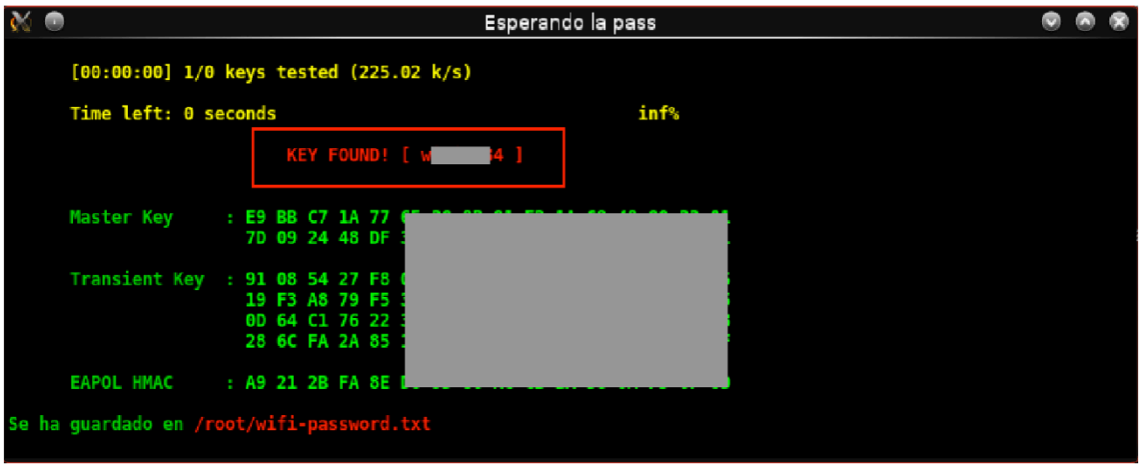


Ilustración 60: Contraseña encontrada

Una vez realizado el ataque de forma satisfactoria, se termina el ataque de forma automática, apareciendo la siguiente imagen:

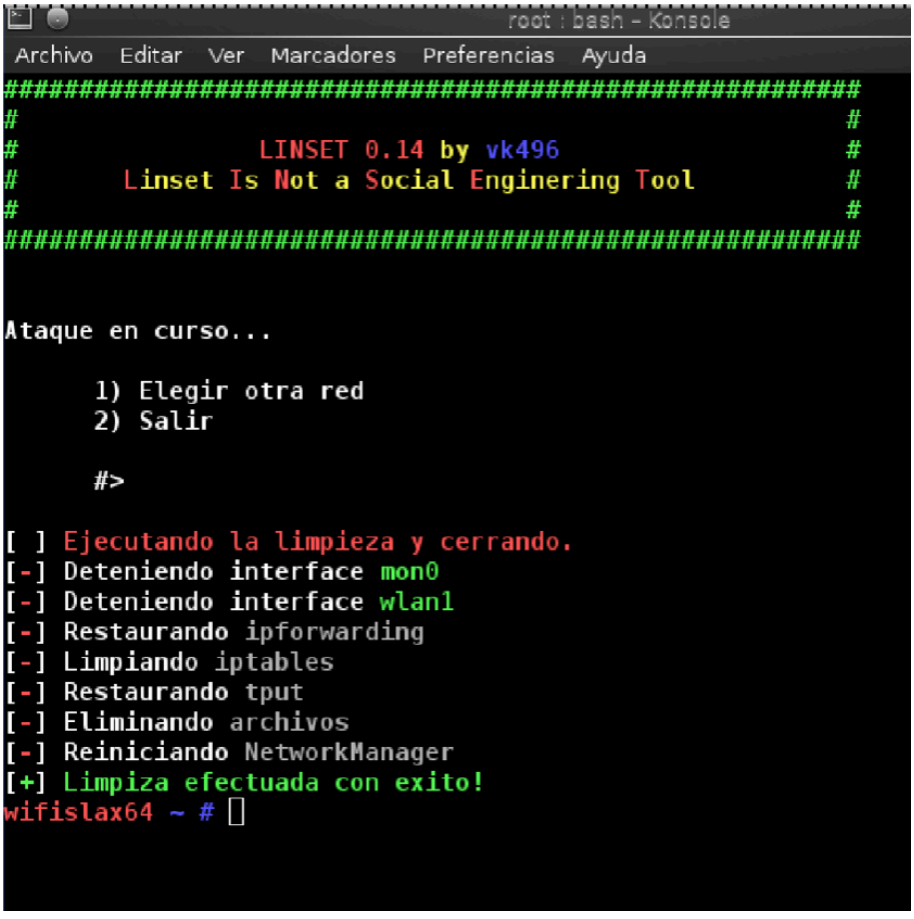


Ilustración 61: Ataque finalizado con éxito

En este momento, la red replicada desaparecerá y volverá a aparecer el punto de acceso original. En este punto, el cliente volverá a conectarse al punto de acceso ingresando la contraseña o si posee conexión automática al punto de acceso, habiendo guardado la contraseña (que es lo más común), simplemente se conectará automáticamente, por lo que el cliente no tendrá sospechas de haber sido atacado, ya que después de ingresar la contraseña, parecerá como si hubiera tenido éxito al hacerlo y se conectará a su red (aunque ambos sucesos no tienen relación realmente).

Una vez realizada esta prueba se enfatizan los dos puntos clave que hay que tener en cuenta: Primero, cuando el cliente queda desconectado de su red y se crea un punto de acceso replicado, este no dispone de candado. En este documento no se recomienda nunca la conexión a una red abierta o sin candado. Si la red tiene seguridad, aparecerá con candado, por lo tanto, un cliente no debe conectarse a una red sin candado y si aparece el nombre de la red sin candado se debe sospechar que está siendo atacada.
Segundo, si aparece un mensaje en una interfaz web pidiendo la contraseña del punto de acceso no se debe insertar. Las contraseñas de los puntos de acceso no se introducen por interfaces web a no ser que se esté accediendo a una red abierta de algunos establecimientos como cliente, aun así, tampoco se recomienda acceder a estas redes, ya que se estará totalmente expuesto. Además, si se piensa que se está siendo víctima de un ataque como este, se recomienda reiniciar el router.

5. Conclusiones

Durante el proyecto se estudian las redes wifi en el contexto de las redes en general, y se comprende que debido a su naturaleza es importante protegerlas de manera adecuada para evitar que personas no deseadas accedan a ésta, ya que no se tiene un control físico de estas redes a diferencia de las cableadas.

Se cumple con los objetivos del trabajo realizando un estudio de las redes wifi y de los diferentes protocolos en los capítulos 2 y 3, y haciendo pruebas de las vulnerabilidades más comunes en el capítulo 4, intercalando comentarios adicionales para que el lector pueda aumentar la seguridad de sus redes Wireless y evitar posibles ataques.

La planificación inicial se ha modificado añadiendo parte de la recreación del laboratorio de pruebas en la primera parte de la práctica para evitar posibles retrasos en las pruebas, ya que el correcto montaje ha sido decisivo para llevar a cabo las pruebas de manera satisfactoria. Además, se han incluido varios puntos frente a la planificación inicial: Se añade el estándar WPS y una introducción al protocolo WPA3 que no se había contemplado en la planificación inicial, y se añade el capítulo 2 para añadir contextualización al proyecto. Por otra parte, se planifican las pruebas para hacer llegar al lector los consejos de seguridad que se consideran más importantes tocando varios puntos, que como conclusión general del trabajo serían: La importancia de utilizar un cifrado fuerte, donde se recomienda el protocolo WPA2; la importancia de utilizar contraseñas fuertes recomendando la utilización de contraseñas con mayúsculas, minúsculas, letras, números y caracteres especiales de una manera aleatoria; evitar el uso del estándar WPS que hace la red más vulnerable por el acceso a través de un PIN débil con acceso remoto o por la conexión a través de PBC, NFC o USB si se consigue un acceso físico al dispositivo. También se resalta la importancia de las actualizaciones de software recomendando tener los dispositivos siempre actualizados, además de no ofrecer las contraseñas a través de interfaces o sitios web sospechosos. Como medida adicional se aconseja utilizar seguridad como filtrado por MAC en las redes o monitorización de redes.

En cuanto a las líneas futuras de estudio, en el mundo de la ciberseguridad todo está en constante evolución, y cuando parece que se han parcheado las vulnerabilidades conocidas se descubren otras nuevas, por tanto, la seguridad en las redes wifi es un tema de constante estudio y desarrollo. Además, el nuevo protocolo WPA3 se publicará en unos meses y también es interesante estudiar más sobre sus características y funcionamiento, ya que en este documento se ha presentado muy brevemente.

6. Bibliografía

adslZone. (04 de 11 de 2019). Obtenido de https://www.adslzone.net/2019/11/04/bluekeep-ransomware-cadena-ser/

Alliance, W.-F. (December 2006). *Wi-Fi Protected Setup Specification* (Vol. Version 1.0h).

bleepingcomputer. (s.f.). Recuperado el 12 de 2019, de https://www.bleepingcomputer.com/news/security/millions-of-amazon-echo-and-kindle-devices-affected-by-wifi-bug/

boxcryptor. (s.f.). Recuperado el 11 de 2019, de https://www.boxcryptor.com/es/encryption/

boxcryptor. (s.f.). *https://www.boxcryptor.com/es/encryption/*. Recuperado el 11 de 2019

Cisco. (s.f.). Recuperado el 11 de 2019, de https://www.cisco.com/c/en/us/products/wireless/access-points/index.html#~benefits

cissp. (s.f.). Recuperado el 11 de 2019, de https://www.oreilly.com/library/view/cissp-certification-training/9781771375320/video227227.html

citeseerx. (s.f.). Recuperado el 11 de 2019, de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.2.3663&rep=rep1&type=pdf

ConferenciaUPM. (s.f.). Recuperado el 10 de 2019, de https://youtu.be/Zvsc_OnMSS4, UPM TASSI 2012 Conferencia 3: Cómo asegurar las redes WiFi,.

ecured. (s.f.). Recuperado el 11 de 2019, de https://www.ecured.cu/Wired_Equivalent_Privacy_(WPE)#WEP2

elo, u. (s.f.). Recuperado el 10 de 2019, de http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf

elperiodico. (12 de 05 de 2017). Obtenido de https://www.elperiodico.com/es/sociedad/20170512/un-ataque-informatico-masivo-infecta-a-las-grandes-empresas-de-espana-6033534

Fluhrer, S., Mantin, I., & Shamir, A. (2001). *Weaknesses in the Key Scheduling Algorithm of RC4.*

grandmetric. (07 de 2018). Obtenido de https://www.grandmetric.com/2018/07/06/ended-wpa3-wi-fi-security-evolution/

grandmetric2. (2018). Obtenido de https://www.grandmetric.com/2018/07/06/ended-wpa3-wi-fi-security-evolution/

helpdeskgeek. (s.f.). Recuperado el 20 de 2019, de https://helpdeskgeek.com/networking/what-is-the-difference-between-wpa-and-wep-wireless-security-encryption

IEEE. (s.f.). Recuperado el 2019 de 11, de https://es.wikipedia.org/wiki/IEEE_802.11.

INCIBE. (s.f.). Recuperado el 2019 de 10, de https://www.incibe.es/sites/default/files/paginas/jornadas-incibe-espacios-ciberseguridad/estudiantes/seguridad_redes_wifi.pdf

INCIBE. (2018). *Seguridad en redes wifi: una guía de aproximación para el empresario*.

INCIBE. (10 de 1 de 2019). Obtenido de https://www.incibe.es/protege-tu-empresa/blog/wpa3-mayor-actualizacion-redes-wi-fi-ultima-decada

Lammle, T. (2013). *CCNA Routing and switching Study guide, SYBEX*.

Lista1. (2019). *Lista de APs con vulnerabilidad WPS*. Obtenido de https://docs.google.com/spreadsheets/d/1uJE5YYSP-wHUu5-smIMTmJNu84XAviw-yyTmHyVGmT0/edit#gid=0

Lista2. (2019). *Lista de APS con vulnerabilidad WPS, pines por defecto*. Obtenido de https://www.atotclic.es/category/redes/

microsoft. (2019). Obtenido de https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-drmnd/6dadc7ac-df68-4649-b5f2-ef34c5da5449

NVD-13077. (s.f.). Recuperado el 11 de 2019, de https://nvd.nist.gov/vuln/detail/CVE-2017-13077

NVD-13078. (s.f.). Recuperado el 11 de 2019, de https://nvd.nist.gov/vuln/detail/CVE-2017-13078

NVD-13079. (s.f.). Recuperado el 11 de 2019, de https://nvd.nist.gov/vuln/detail/CVE-2017-13079

NVD-13080. (s.f.). *NIST*. Recuperado el 11 de 2019, de https://nvd.nist.gov/vuln/detail/CVE-2017-13080

NVD-13081. (s.f.). *NIST*. Recuperado el 11 de 2019, de https://nvd.nist.gov/vuln/detail/CVE-2017-13081

NVD-13082. (s.f.). *NIST*. Recuperado el 11 de 2019, de https://nvd.nist.gov/vuln/detail/CVE-2017-13082

NVD-13084. (s.f.). *NIST*. Recuperado el 11 de 2019, de https://nvd.nist.gov/vuln/detail/CVE-2017-13084

NVD-13086. (s.f.). *NIST*. Recuperado el 11 de 2019, de https://nvd.nist.gov/vuln/detail/CVE-2017-13086

NVD-13087. (s.f.). *NIST*. Recuperado el 11 de 2019, de https://nvd.nist.gov/vuln/detail/CVE-2017-13087

NVD-13088. (s.f.). *NIST*. Recuperado el 11 de 2019, de https://nvd.nist.gov/vuln/detail/CVE-2017-13088

PEARSON. (2012). *Redes de computadoras, quinta edición, TaNeNbaum, WetheRall, Mexico*.

Prieto, D. G. (s.f.). Recuperado el 10 de 2019, de https://repositorio.unican.es/xmlui/bitstream/handle/10902/5944/Diego%20Garcia%20Prieto01.pdf?sequence=5&isAllowed=y

Rotger, L. H. (2017). *“Criptografía avanzada, apartado elementos de criptografía”, por Llorenç Huguet Rotger Josep Rifà Coma, Juan Gabriel Tena Ayuso*.

RovingNotes. (s.f.). Recuperado el 11 de 2019, de http://ww1.microchip.com/downloads/en/AppNotes/WPS-App-note.pdf.

Ruz Maluenda, J., Riveros Vasquez, B., & Varas Escobar. (s.f.). *Redes WPA/WPA2*. Obtenido de http://profesores.elo.utfsm.cl/~agv/elo322/1s12/project/reports/RuzRiverosVaras.pdf

tech-faq. (s.f.). *http://www.tech-faq.com/rc4.html*. Recuperado el 10 de 2019

TestdeVelocidad. (s.f.). Recuperado el 11 de 2019, de https://www.testdevelocidad.es/2016/08/11/conoce-cuales-todos-los-estandares-wi-fi-existen/

UPC. (s.f.). Recuperado el 2019 de 10, de https://upcommons.upc.edu/bitstream/handle/2099.1/7865/memoria.pdf?sequence=1&isAllowed=y

utsfm. (s.f.). Recuperado el 2019 de 10, de http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf

vanhoefm, h. (s.f.). Obtenido de https://github.com/vanhoefm/krackattacks-scripts

WEP. (s.f.). Recuperado el 10 de 2019, de https://es.wikipedia.org/wiki/Wired_Equivalent_Privacy

7. Anexos

Anexo de la prueba 4: Importancia de las actualizaciones: Ataque KRACK

Para comprobar si un dispositivo es vulnerable al ataque KRACK se pueden utilizar los scripts publicados por el usuario vanhoefm de GitHub, perteneciente al descubridor de esta vulnerabilidad en el protocolo WPA2 y cuyo repositorio se deja en las referencias (vanhoefm, s.f.).

Para realizar estas pruebas se necesita un USB con Kali Linux persistente, y no se pueden realizar con Kali Linux en una máquina virtual.

En primer lugar, se descarga el repositorio en local con el siguiente comando:

```
root@kali:~# git clone https://github.com/vanhoefm/krackattacks-scripts.git
```

Además, se instalan las siguientes dependencias de Linux:

```
root@kali:~# apt-get install libnl-3-dev libnl-genl-3-dev pkg-config
libssl-dev net-tools git sysfsutils python-scapy python-pycryptodome
```

Y se deshabilita la encriptación hardware, dando permisos de lectura, escritura y ejecución. Un error que se ha cometido y por el que la primera vez se han tenido problemas es por no dar los permisos correctos, pero con el siguiente script se ha conseguido que funcione correctamente:

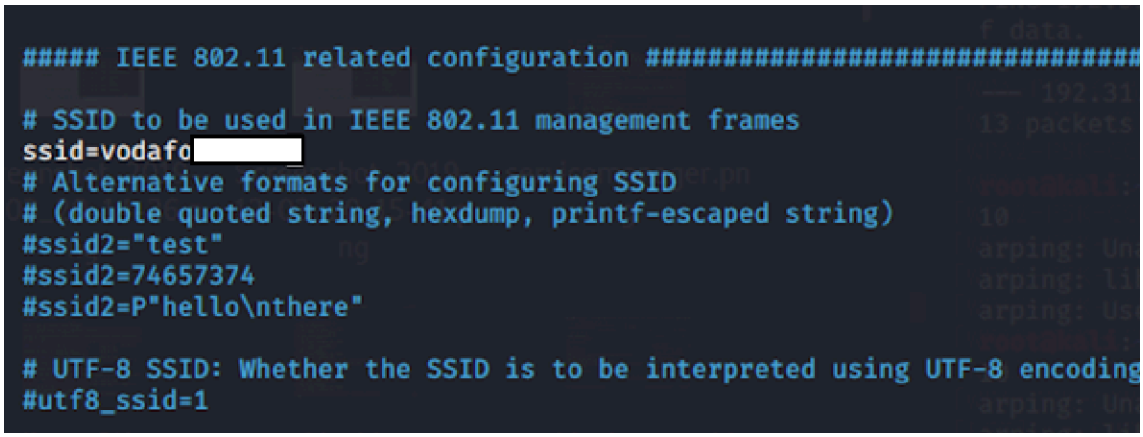
```
root@kali:~# cd krackattacks-scripts
root@kali:~/krackattacks-scripts# cd hostapd
root@kali:~/krackattacks-scripts/hostapd# chmod 777 disable-hwcrypto.sh
```

Después de esto hay que reiniciar, y es por ello por lo que se ha necesitado un USB persistente. Al realizar la prueba se ha intentado fallidamente en varias ocasiones hacer un reinicio con máquina virtual en modo persistente, pero en las pruebas realizadas ha resultado fallido, y la única forma que se ha encontrado para que funcione de manera correcta es utilizando USB persistente.

Una vez reiniciado, se compila la instancia hostapd:

```
root@kali:~/krackattacks-scripts# cd hostapd
root@kali:~/krackattacks-scripts/hostapd# cp defconfig .config
root@kali:~/krackattacks-scripts/hostapd# make -j 2
```

Cambiando la configuración según el nombre de la interfaz que se quiera utilizar para esta prueba, en este caso wlan1, y con el SSID que se quiera probar.



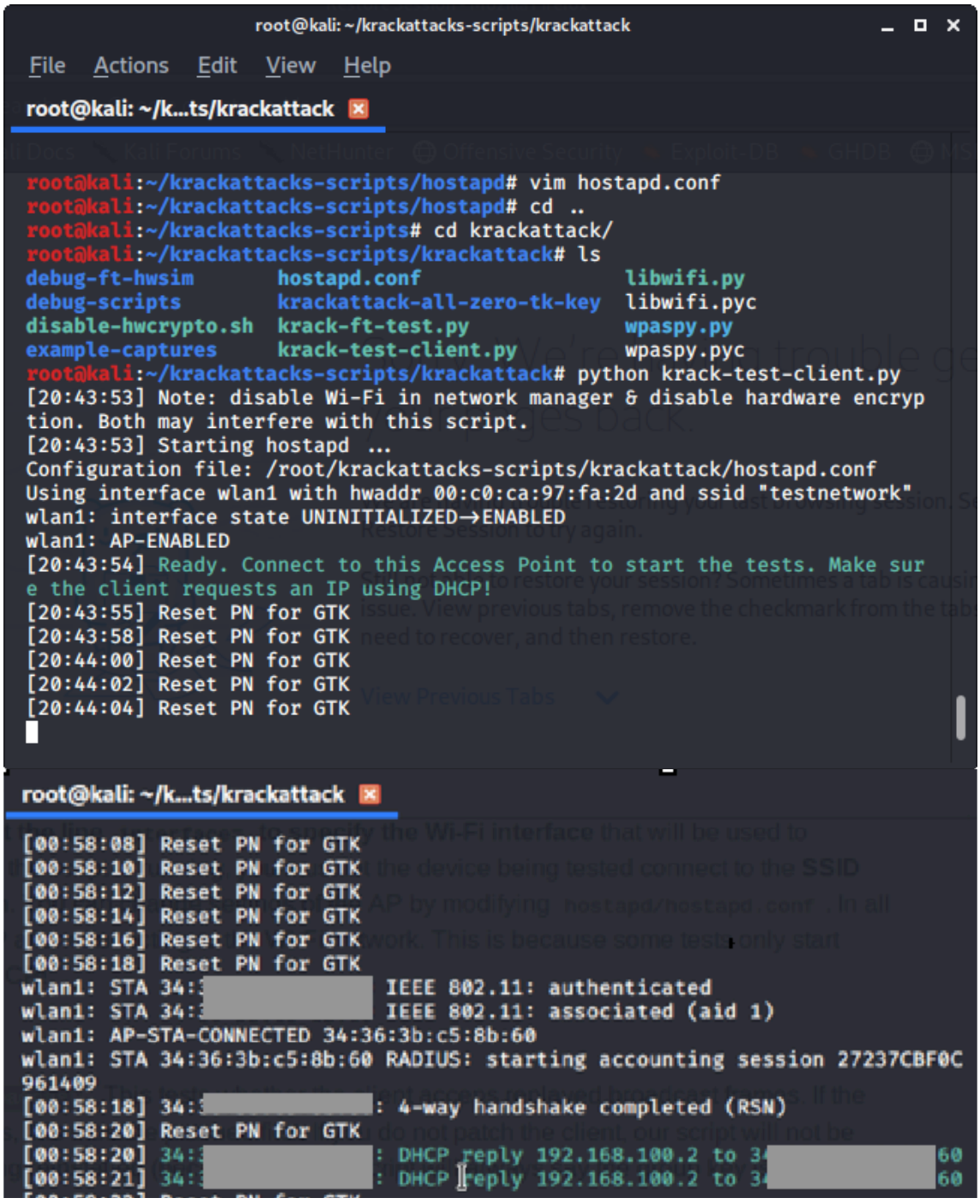
Se desabilita el network manager

```
root@kali:~/krackattacks-scripts/krackattack# service network-manager stop
```

y se ejecuta el siguiente script para que los scripts que se van a utilizar puedan seguir utilizando Wifi:

```
root@kali:~/krackattacks-scripts/hostapd# rfkill unblock wifi
```

Una vez realizados estos pasos previos, el sistema está preparado para comenzar a testear un dispositivo, para ello se ejecuta el script de prueba del cliente:



Los clientes probados están parcheados ante esta vulnerabilidad, y han sido un Macbook Pro utilizando macOS Mojave Versión 10.14.6 y un Iphone con una versión de software 12.4.1, En este caso la prueba no ha resultado satisfactoria, pero se anima al lector a hacer esta prueba con sus dispositivos. Si el sidpositivo fuera vulnerable debería aparecer el siguiente mensaje que se ve en amarillo “client reinstalls the key”

Ilustración 62: Cliente vulnerable a KRACK (bleepingcomputer, s.f.)