Estudio de los riesgos relacionados con las redes Wi-Fi

Alejandro González Martínez
Grado de Tecnologías de Telecomunicaciones

Antoni Morell Pérez

12 de Junio de 2016

Agradecimientos

A mi mujer Yaiza y mi hija Valentina que me han apoyado todos estos años.
A mi padre, sin él no podría haber continuado estudiando.
Carlos, contigo el camino se hizo menos duro.

A) Creative Commons:

B) GNU Free Documentation License (GNU FDL)

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	Estudio de los riesgos relacionados con las redes Wi-Fi
Nombre del autor:	Alejandro González Martínez
Nombre del consultor:	Antoni Morell Pérez
Fecha de entrega (mm/aaaa):	06/2016
Área del Trabajo Final:	Integración de redes telemáticas
Titulación:	*Grado de Tecnologías de Telecomunicaciones*

Resumen del Trabajo (máximo 250 palabras):

En este trabajo fin de grado se pretende realizar un estudio de los riesgos y amenazas a las que están expuestas las redes Wi-Fi.

Primeramente se realizará una introducción a la seguridad en las redes Wi-Fi, en el que se describirá brevemente una serie de conceptos básicos sobre esta tecnología. También se plasmará una descripción teórica de los protocolos de encriptación (WEP, WPA, WPA2, EAP, TKIP y WPS) disponibles en los puntos de acceso, indicando sus virtudes y vulnerabilidades. Y se analizarán cada uno los diferentes ataques más comunes que se pueden realizar a las redes inalámbricas.

Una vez definida las medidas que existen para securizar una red Wi-Fi, se pondrán en práctica, en un laboratorio, las diferentes técnicas que permiten saltarse la seguridad de los protocolos anteriormente definidos, analizando a nivel teórico qué vulnerabilidad es explotada en cada uno de los ataques.

Demostrado que las medidas de seguridad ofrecidas por routers y/o puntos de acceso presentan carencias, se implementará un servidor RADIUS para que gestione la autenticación, autorización y registro de los usuarios de una red inalámbrica.

Para concluir se resumirán las políticas, elementos y soluciones de seguridad inalámbrica que se deberán tener en cuenta a la hora de implementar una red Wi-Fi, tanto en el ámbito doméstico como en el empresarial.

Abstract (in English, 250 words or less):

The aim of this is to conduct a study of the risks and threats WIFI networks are exposed to.

The starting point would be an introduction to Wi-Fi network security. First with a brief description of this technology's basics and second with a theoretical description about encryption protocols (WEP, WPA, WPA2, AES, TKIP and WPS), which are available in access points, showing their strengths and vulnerabilities. Apart from that, each of the most common attacks on wireless networks will be briefly analyzed.

After this definition of/After defining Wi-Fi security measures, a laboratory will be set up in order to put bypassing techniques into practice. From this practical part, a demonstration of these protocols exposure will be shown followed by a consistent analysis of the vulnerability addressed/treated/considered/evaluated in each attack.

Once shown that security measures offered by routers and/or access points are insufficient, a RADIUS server will be implemented to manage authentication, authorization and user registration of a wireless network.

To conclude this thesis, a summary of policies, elements and safety solutions will be presented, which have to be taken into account when implementing a WI-FI network, domestic and business environment.

Palabras clave (entre 4 y 8):

Wi-Fi seguridad ataques RADIUS vulnerabilidades 802.11

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del trabajo

Cualquier empresa, por pequeña que sea, dispone de una red Wi-Fi donde los trabajadores y clientes conectan múltiples dispositivos para acceder a internet y a la información alojada en recursos de red.

Suele ser habitual que una vez el instalador configura el router, la contraseña de la Wi-Fi se distribuya a cualquier persona que la solicite. En ningún momento se tiene en cuenta las repercusiones que esto puede tener y mucho menos se tiene presente realizar modificaciones adicionales.

Este desconocimiento puede implicar:

- Reducción del ancho de banda debido a un uso indiscriminado por parte del atacante.
- Robo, eliminación o secuestro de información.
- Infección de dispositivo con malware permitiendo que el atacante lo controle de forma remota.

Según el informe Symantec Internet Security Threat Report Volumen 21 [1] (ISTR) los ataques contra las pequeñas empresas han crecido en 9 puntos porcentuales respecto al informe realizado en 2011 (ISTR Volumen 17) [2] donde se recogía que el 40% de los ataques originados a principios de 2010 han tenido como objetivo empresas con menos de 500 trabajadores, frente a sólo el 28% de ciberataques a las grandes empresas.

La planificación y ejecución de un intento de penetración contra una organización normalmente requiere entre 1 y 24 horas. Un retraso de cinco horas en la realización de un ataque exitoso disuade el 13% de los ataques, mientras que un retraso de 20 horas, disuade el 36% de los ataques. A raíz de los resultados de este estudio se llega a la conclusión de que al invertir en seguridad se está colocando una barrera que conseguirá bloquear intentos de acceso no autorizados o, al menos, disuadir a la inmensa mayoría de atacantes.

Si una red es vulnerada, los atacantes se ponen en contacto con la empresa

para solicitarle un rescate, ya sea para recuperar los datos cifrados o las estaciones de trabajo infectadas por software malicioso. Si bien los organismos de seguridad recomiendan no pagar nunca el rescate, ya que esto no asegura la recuperación de los datos, los precios exigidos pueden variar desde los 400 $ hasta los 3,7 millones de $ que han solicitado al Hollywood Presbyterian Medical Center. Estas cifras son estimativas ya que las empresas que pagan los rescates no hacen público este tipo de datos, pero según se recoge en el informe de ChekPoint Inside Nuclear's Core : Analyzing the Nuclear Exploit Kit Infrastructure – Part I [3], los desarrolladores del ransomware Nuclear generan unos ingresos mensuales que rondan los 90.000 €.

A fin de evitar lo anteriormente descrito, es necesario implantar una solución basada en WPA2 Enterprise o RADIUS que ofrece una protección adecuada para las empresas y garantiza totalmente la seguridad de una red Wi-Fi.

Valoración económica

Nombre	Descripción	Importe
HP ProLiant ML310e	Intel Xeon E5-2620, 4GB RAM, Ethernet 1 Gb, HD 1TB.	**695€**
Linksys Business AC1200	La cantidad de dispositivos puede varias en función de las dimensiones del recinto y número de conexiones.	**126 €**
Ubuntu Server	Sistema Operativo	**0 €**
FreeRADIUS	Servicio RADIUS	**0 €**
OpenLDAP	Servicio de directorio de usuarios	**0 €**
Servicios Ingeniero Técnico de Sistemas	Instalación, configuración y puesta en marca. 12 horas de trabajo (52,5 € hora)	**632,06 €**
	TOTAL	**1453,06 €**

1.2 Objetivos del trabajo

La intención de este proyecto es la de realizar un estudio completo de la seguridad en las redes inalámbricas implementadas con Wi-Fi. Se pondrán de manifiesto los problemas, más comunes, presenta en el campo de la seguridad. Este proyecto se podría usar como una guía en la que se mostrarán las diferentes técnicas, de las que hacen uso los atacantes, parar infiltrarse en una red, pero también se darán una serie de soluciones y recomendaciones que obstaculicen lo máximo posible esos intentos de acceso no autorizados.

Los objetivos que se pretenden alcanzar con el trabajo fin de grado son los siguientes:

1. Conocer la tecnología que permite la conexión de dispositivos electrónicos de forma inalámbrica.
2. Qué fiabilidad y seguridad ofrecen las conexiones Wi-Fi.
3. Identificación y análisis de riesgos en las redes inalámbricas.
4. Conocer las medidas que permiten securizar las conexiones Wi-Fi.

1.3 Enfoque y método seguido

El enfoque y método seguido para la realización del presente proyecto ha consistido en la división en cuatro fases. La primera de ellas ha servido para la obtención del conocimiento y así poder abordar las tres fases siguientes.

En la primera fase se ha realizado un estudio del estándar 802.11x, de las formas de securizar una red Wi-Fi y las vulnerabilidades que presenta.

La segunda fase pondrá en práctica diferentes ataques contra redes Wi-Fi en un entorno de laboratorio, para valorar por un lado si son efectivos y la complicación que implica la realización de los mismos.

Posteriormente se implementará la tercera fase en la que se usará un servidor RADIUS para gestionar la autorización, autenticación y gestión de acceso de los usuarios a la red inalámbrica.

Una vez obtenidos los resultados de las anteriores fases ya se estará en posición de realizar la cuarta fase, que consiste en dar recomendaciones de seguridad para fortificar una red Wi-Fi.

1.4 Planificación del trabajo

La realización completa del proyecto está compuesta por una serie de entregables parciales, los cuales tienen una fecha de entrega límite.

En el siguiente diagrama de Gantt se puede observar cada una de estas entregas parciales (Pruebas de Evaluación Continua - PEC) y a su vez cada PEC está compuesta por varias subtareas que se deben completar para alcanzar la fecha objetivo.

Nombre de tarea	Duración	Comienzo	Fin
TFG - Estudio de los riesgos relacionados con las redes Wi-Fi	**89 días**	**mié 24/02/16**	**vie 24/06/16**
Decisión del proyecto y comunicación al consultor	6 días	mié 24/02/16	mié 02/03/16
PEC1 - Planificación del proyecto	**6 días**	**mié 02/03/16**	**mié 09/03/16**
Recolección de información bibliográfica	2 días	mié 02/03/16	jue 03/03/16
Elaboración de la PEC1	3 días	vie 04/03/16	mar 08/03/16
Entrega de la PEC1	0 días	mié 09/03/16	mié 09/03/16
PEC 2 - Primera entrega del proyecto	**31 días**	**jue 10/03/16**	**mié 20/04/16**
Recopilación de información sobre tecnologías inalámbricas	2 días	jue 10/03/16	vie 11/03/16
Recopilación de información sobre el estándar IEEE 802.xx	2 días	lun 14/03/16	mar 15/03/16
Recopilación de información sobre ataques a redes Wi-Fi	2 días	mié 16/03/16	jue 17/03/16
Elaboración de la memoria	15 días	vie 18/03/16	jue 07/04/16
Instalación y configuración del laboratorio	1 día	vie 08/04/16	vie 08/04/16
Realización práctica de ataques a redes Wi-Fi en laboratorio	3 días	sáb 09/04/16	mar 12/04/16
Redacción de los resultados obtenidos	4 días	mié 13/04/16	lun 18/04/16
Revisión de la memoria	1 día	mar 19/04/16	mar 19/04/16
Entrega de la PEC2	1 día	mié 20/04/16	mié 20/04/16
PEC 3 - Segunda entrega del proyecto	**25 días**	**jue 21/04/16**	**mié 25/05/16**
Instalación y configuración de la maqueta del servidor RADIUS	13 días	jue 21/04/16	lun 09/05/16
Redacción de los pasos seguidor y resultados	3 días	mar 10/05/16	jue 12/05/16
Recopilación de información sobre vulnerabilidades WEP,WPA y WPS	3 días	vie 13/05/16	mar 17/05/16
Completar y revisar de la memoria	5 días	mié 18/05/16	mar 24/05/16
Entrega de la PEC3	1 día	mié 25/05/16	mié 25/05/16
Finalización del FTG	**22 días**	**jue 26/05/16**	**vie 24/06/16**
Entrega de la memoria final	13 días	jue 26/05/16	dom 12/06/16
Entrega de la presentación y del código	7 días	lun 13/06/16	mar 21/06/16
Tribunal	3 días	mié 22/06/16	vie 24/06/16

Ilustración 1 División de tareas

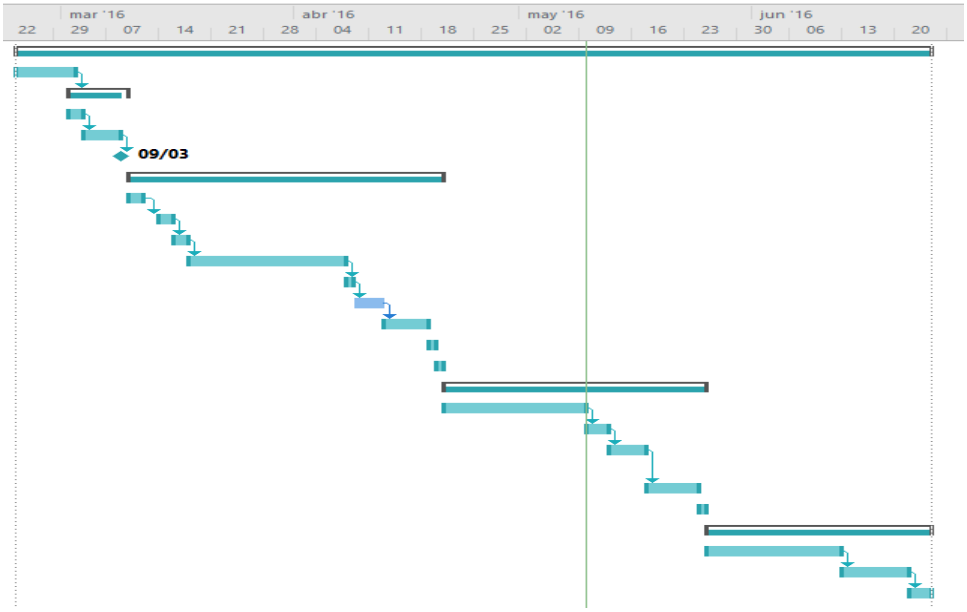

Ilustración 2 Diagrama de Gantt

En la siguiente tabla se recoge, a modo de resumen, las fechas más importantes:

Entregable	Fecha límite
Decisión del proyecto y comunicación al consultor	2 de Marzo del 2016
PEC 1 - Entrega de la planificación del trabajo	9 de Marzo del 2016
PEC 2 - Primera entrega del proyecto	20 de Abril del 2016
PEC 3 - Segunda entrega del proyecto	25 de Mayo del 2016
Entrega de la memoria final	12 de Junio del 2016
Entrega de la presentación y del código	19 de Junio del 2016
Inicio del tribunal	20 de Junio del 2016
Final del tribunal	24 de Junio del 2016

1.5 Breve sumario de productos obtenidos

El resultado final es un manual que servirá para que el lector conozca qué y cómo funcionan los elementos de seguridad existentes en la electrónica de red Wi-Fi y los riesgos derivados de las vulnerabilidades que posee esta tecnología.

A nivel práctico se pone en relieve que las redes Wi-Fi son vulnerables y que no es necesario tener unos conocimientos muy avanzados para poder penetrar en una red en la que no se haya tenido la precaución de aplicar unos parámetros de seguridad más allá de los que se establecen por defecto por parte del fabricante del dispositivo.

Con los resultados obtenidos del análisis anterior se han podido confeccionar una serie de recomendaciones que ayudan al lector a mejorar la seguridad en una red inalámbrica basada en el estándar 802.11.

Por último, se ha podido elaborar una guía que permite instalar y configurar una plataforma de autenticación RADIUS que a nivel empresarial proporciona un mayor grado de seguridad.

1.6 Breve descripción de los otros capítulos de la memoria

Capítulo 2: se detallan los conceptos básicos del estándar IEEE 801.11, el mecanismo de seguridad que implementa y los diferentes tipos de ataques que normalmente se aplican a éstos. Este capítulo sienta las bases de los conceptos que serán tratados en capítulos posteriores.

Capítulo 3: se ponen en práctica diversos ataques sobre los protocolos WEP, WPA y WPS para poner en evidencia que son vulnerables. Junto con cada demostración práctica se acompaña una explicación de la vulnerabilidad que es usada por la herramienta para llevar a cabo la intrusión.

Capítulo 4: en este capítulo se implementa una solución WPA2 Enterprise, la cual a día de hoy es la que mayores garantías de seguridad ofrece.

Capítulo 5: se recogen las mejores prácticas que se pueden aplicar para elevar el nivel de seguridad de una red Wi-Fi.

2. La seguridad en redes Wi-Fi

Las redes inalámbricas se han popularizado fuertemente en los últimos años, tanto en el ámbito del hogar como en el corporativo y espacios públicos. Éstas proporcionan flexibilidad y movilidad, debido a que las ondas de radio tienen una propagación radial que se da en tres dimensiones, dentro de un rango relativamente amplio. Es por esto que es muy difícil mantener las transmisiones dentro de un área limitada y las ondas pueden pasar de una planta a otra de un edificio. La principal consecuencia de esta propagación es que personas no autorizadas pueden realizar escuchas de la red, sin tener que estar físicamente dentro del edificio donde reside la red inalámbrica, este hecho podría causar problemas de diversa índole como el robo de archivos personales, contraseñas de acceso a bancos, redes sociales u otros servicios y distintos tipos de incidentes de seguridad.

2.1 Conceptos básicos

Wi-Fi (Wireless Fidelity) es el nombre con el que se bautizó al estándar que describe los productos WLAN basados en los estándares 802.11. Esta tecnología es utilizada para la comunicación de datos entre equipos situados dentro de una misma área de cobertura. Dicho modelo fue desarrollado por un grupo de las principales empresas del sector de las comunicaciones denominado WECA (Wireless Ethernet Compability Aliance). WECA cambió de nombre en 2002, pasando a denominarse Wi-Fi Alliance.

Ilustración 3 Logotipo Wi-Fi

El estándar 802.11 fue publicado en 1997 y se caracteriza por ofrecer velocidades de 1 y 2 Mbps (Megabits por segundo), un sistema de cifrado sencillo llamado WEP (Wired Equivelent Privacy) y opera en la banda de frecuencia de 2.4 GHz (Gigahercio). En 1999 aparecen las primeras variantes denominadas 802.11a y 802.11b que ofrecen velocidades de 54 y 11 Mbps respectivamente.

A nivel de seguridad el estándar IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) 802.11 propone tres servicios:

1. Autenticación: provee servicios de seguridad para verificar la identidad entre las estaciones clientes. Establece un control de acceso a la red denegando la entrada a los equipos clientes que no pueden ser autentificados.
2. Confidencialidad: provee de la privacidad lograda en una red cableada. El objetivo es prevenir que la información quede comprometida debido a un ataque pasivo.
3. Integridad: este servicio asegura que los mensajes no son modificados en el camino entre los clientes inalámbricos y el punto de acceso en un ataque activo.

No pasaría mucho tiempo hasta que se puso de manifiesto que el estándar tenía carencias a nivel de seguridad.

A continuación se procede a realizar un breve resumen de las diferentes versiones que se han publicado del estándar:

- 802.11a: fue aprobada en 1999 y es el primer estándar inalámbrico con velocidades máximas variables de 54 Mbps. Opera dentro del rango de los 5 Ghz.
- 802.11b: esta revisión fue ratificada en 1999. Soporta velocidades de hasta 11 Mbps comparable con una ethernet tradicional. Funciona en la banda de 2.4.
- 802.11g: lanzado al mercado en 2003. Utiliza la banda de 2.4 Ghz pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a.
- 802.11n: es el desarrollo de la nueva generación del estándar para redes inalámbricas. El estándar 802.11n trabaja tanto en la banda de 2.4GHz como en la de 5 GHz y es mucho más estable y seguro. La velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps.
- 802. 11ac: lanzada al mercado en enero de 2014. Es conocida como Wi-

Fi 5G o Wi-Fi Gigabit. Mejora las tasas de transferencia hasta 433 Mbit/s por flujo de datos, consiguiendo tasas de 1.3 Gbit/s empleando 3 antenas.

2.1.1 Modos de operaciones.

El estándar 802.11 define dos modos operativos: modo ad-hoc y modo infraestructura.

El modo ad-hoc se denota como Conjunto de Servicios Básicos Independientes (Independent Basic Service Set - IBSS), aunque también puede ser denominado como punto a punto. En este método de operación, los clientes inalámbricos pueden establecer una comunicación directa entre sí. Cada estación de una red ad-hoc debería configurar su adaptador inalámbrico en modo ad-hoc y usar los mismos service set identifier (SSID) y número de canal de la red.

Normalmente está conformada por un pequeño grupo de dispositivos dispuestos cerca unos de otros.

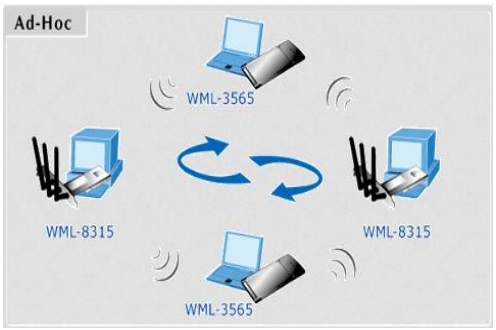

Ilustración 4 Modo Ad-Hoc

En este modo de operación el rendimiento es menor a medida que el número de nodos crece. Para conectar una red ad-hoc a una red de área local cableada o a Internet es necesario el uso de una pasarela (gateway).

El modo de infraestructura es conocido como Conjunto de Servicios Básicos (Basic Service Set - BSS). Al contrario de como sucedía con el modo ad-hoc, donde no hay un elemento central, en el modo de infraestructura hay un componente central conocido como un punto de acceso o estación base que tiene la función de coordinar. Si el punto de acceso se conecta a una red cableada, los clientes inalámbricos pueden acceder a la red fija a través de él.

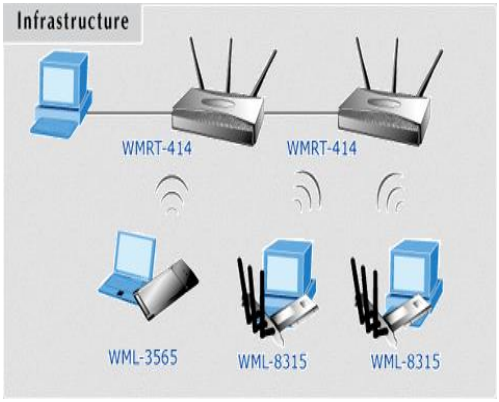

Ilustración 5 Modo Infraestructura

Para interconectar muchos puntos de acceso y clientes inalámbricos, todos deben configurarse con el mismo SSID.

2.1.2 Control de acceso al medio

El estándar 802.11 define en su capa de Control de Acceso al Medio (Medium Access Control - MAC) una serie de funciones para realizar las operaciones propias de las redes inalámbricas. Esta capa se encarga de gestionar y mantener las comunicaciones entre estaciones 802.11. También tiene que coordinar el acceso a un canal de radio compartido, utilizar su capa física para detectar la portadora y realizar tanto la transmisión como la recepción de tramas.

El proceso de acceso al medio por parte de un cliente inalámbrico implica tres etapas: exploración activa / pasiva de los servicios inalámbricos, la autenticación y asociación.

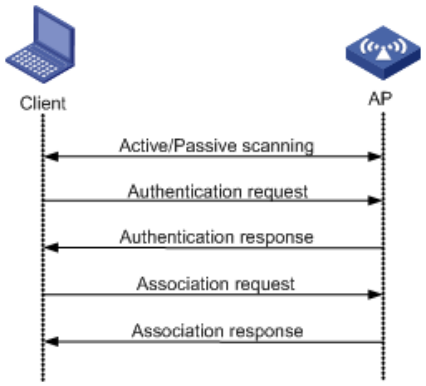

Ilustración 6 Establecer acceso de un cliente

Búsqueda (Scanning): el estándar 802.11 define tanto la búsqueda activa como pasiva, esto es utilizado por un adaptador de red para localizar puntos de acceso. La búsqueda pasiva es obligatoria, cada adaptador de red busca canales individuales para encontrar la mejor señal del punto de acceso. Periódicamente,

cada punto de acceso difunde señales y el adaptador recibe estas señales denominadas beacon.

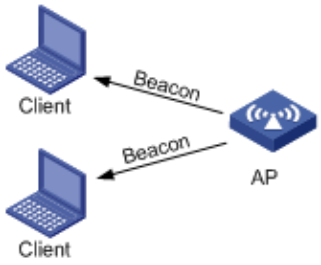

Ilustración 7 Exploración pasiva

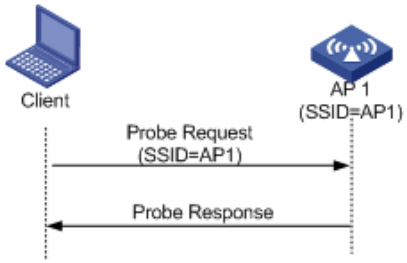

Ilustración 8 Exploración activa

Estas beacon (señales de faro) contienen datos sobre el punto de acceso incluyendo el SSID y las tasas de transmisión. El adaptador de red puede usar esta información para compararla y determinar junto con otras características, como la fuerza de la señal, qué punto de acceso debe utilizar.

La búsqueda activa es similar, salvo que la propia tarjeta inicia el proceso difundiendo una trama de prueba a la que responden todos los puntos de acceso que estén al alcance con otra trama de prueba.

En la búsqueda activa se permite que un adaptador de red reciba respuesta inmediata del punto de acceso sin necesidad de esperar a una transmisión beacon.

Autenticación (Authentication): la autenticación es el proceso para comprobar la identidad de un adaptador en la red para aceptarlo o rechazarlo. En el estándar 802.11 se especifican dos formas de autenticación: el sistema abierto y el sistema basado en una clave compartida.

El sistema abierto es obligatorio y consta de dos pasos:

1. El adaptador de red inicia el proceso enviando una trama de solicitud de autenticación al punto de acceso.
2. El punto de acceso responde con una trama de autenticación que indica si acepta o rechaza la autenticación utilizando el campo de código de estado de la trama.

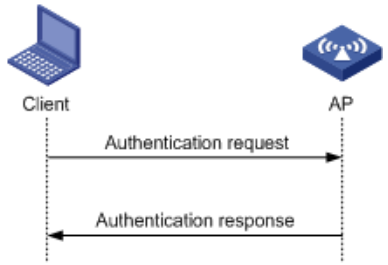

Ilustración 9 Proceso de autenticación de sistema abierto

La autenticación de clave compartida es opcional y básicamente comprueba si la clave es la correcta. El hecho de ser opcional para el protocolo no impide que esté en la práctica totalidad de los adaptadores y puntos de acceso.

Este proceso consta de cuatro pasos:

1. El cliente envía una solicitud de autenticación al AP.
2. El AP genera aleatoriamente un desafío y lo envía al cliente.
3. El cliente utiliza la clave compartida para cifrar el desafío y la envía al AP.
4. El AP utiliza la clave compartida para cifrar el desafío y compara el resultado con la recibida desde el cliente. Si son idénticos, el cliente pasa la autenticación de enlace. Si no, la autenticación de enlace falla.

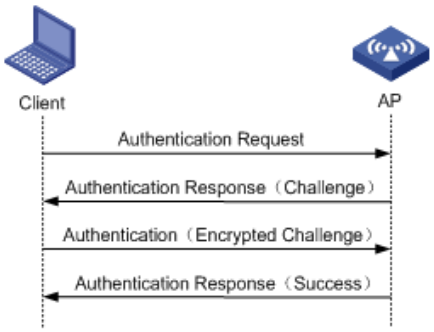

Ilustración 10 Proceso de autenticación de clave compartida

Asociación (Association): la asociación es un proceso por el cual el punto de acceso reserva recursos y sincroniza con una estación cliente.

Una vez que el adaptador de red se ha autenticado, también tiene que asociarse al punto de acceso antes de poder transmitir tramas de datos. La asociación es importante para sincronizar a ambos elementos con información importante, como por ejemplo, las tasas de transmisión admitidas.

El adaptador que inicia la asociación envía una trama de solicitud de asociación que contiene elementos como el SSID y tasas de transferencia admitidas. El

punto de acceso reserva memoria para ese cliente, le asigna un ID de asociación y le responde con una trama de respuesta de asociación que contiene el ID de asociación junto con otra información referente al punto de acceso. Una vez que el adaptador de red y el punto de acceso han completado el proceso de asociación pueden comenzar a transmitir tramas de datos entre ellos, es decir el cliente puede utilizar el punto de acceso para comunicar con otros clientes de la red.

2.2 Mecanismos de seguridad

2.2.1 Listas de control de acceso basadas en MAC

Fue la primera medida de seguridad implantada en las redes Wi-Fi y sigue siendo utilizado a día de hoy. Es un mecanismo que se activa en los puntos de acceso permitiendo que únicamente accedan a la red a aquellos dispositivos cuya dirección física MAC esté especificada en la lista de acceso. Esta medida se puede utilizar como control adicional; pero es fácilmente vulnerable aplicando un clonado de la MAC a suplantar.

2.2.2 WEP (Wired Equivalent Privacy)

El protocolo WEP fue el primer mecanismo que impedía la obtención de la información que se intercambiada entre los terminales y punto de acceso ofreciendo así una solución a los problemas generados por las redes abiertas. Tiene como objetivo principal el de proporcionar confidencialidad, autenticación y control de acceso. Este sistema emplea un algoritmo RC4 para el cifrado de las llaves que pueden ser de 40 o 104 bits y una vez añadido los 24 bits para el vector de iniciación ocupan un total de 64 o 128 bits. Un vector de iniciación es un contador que va cambiando de valor a medida que se generan tramas de forma que, al añadirlo a la clave, se aumenta el número de claves posibles a emplear.

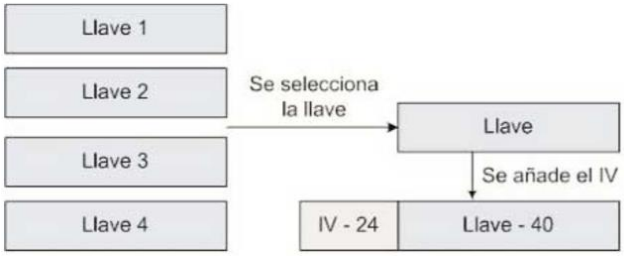

Ilustración 11 Se añade el IV a la clave seleccionada

Las llaves se generan a partir de una clave que ha de ser conocida por todos los dispositivos involucrados en la comunicación y este hecho provoca que las claves sean sencillas y que permanezcan siempre estáticas. A partir de esta clave se generan 4 llaves de 40 bits, de las cuales se empleará una diferente cada vez para realizar el cifrado WEP

Inicialmente se creía que se trataba de un cifrado muy seguro, pero pronto se descubrió que no era así, demostrando que ofrece muchas debilidades.

Entre las principales debilidades de este sistema se encuentran que las claves permanecen siempre estáticas y por otro lado los 24 bits del vector de inicialización son insuficientes, además de transmitirse sin cifrar.

2.2.3 WPA (Wi-Fi Protected Access)

Este sistema de cifrado surgió para solucionar los problemas de seguridad que ofrecía el sistema WEP. WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado.

WPA soluciona la debilidad del vector de inicialización de WEP, mediante la introducción de vectores del doble de longitud (48 bits), permitiendo un total de 2^{48} combinaciones de claves posibles, muy por encima de los 16 millones que permitía WEP, aunque sigue utilizando el algoritmo RC4 como sistema de cifrado. Se implementa el protocolo de gestión de claves dinámicas (TKP – Temporal Key Integrity Protocolo) que permite utilizar una clave diferente para cada trama transmitida. La clave es generada a partir de la clave base, la dirección MAC del dispositivo emisor y del número de serie del paquete. Estos paquetes que se transmiten incluyen un número de serie único de 48 bits que se incrementa en cada trama, para asegurar claves distintas. También se ha eliminado el CRC-32 y se ha incluido un nuevo código denominado MIC (Message Integrity Code) o Michael, código que verifica la integridad de las tramas.

WPA puede admitir diferentes sistemas de control de acceso incluyendo la validación de usuario-contraseña, certificado digital o simplemente utilizar una contraseña compartida para identificarse.

La implementación de estos nuevos mecanismos de autenticación y cifrado es posible mediante una actualización de software en la mayoría de dispositivos existentes en el mercado. En entornos empresariales WPA se utiliza junto con servidores de autenticación, como RADIUS, para proporcionar gestión centralizada de usuarios. RADIUS será explicado con más detalle en el punto 4.

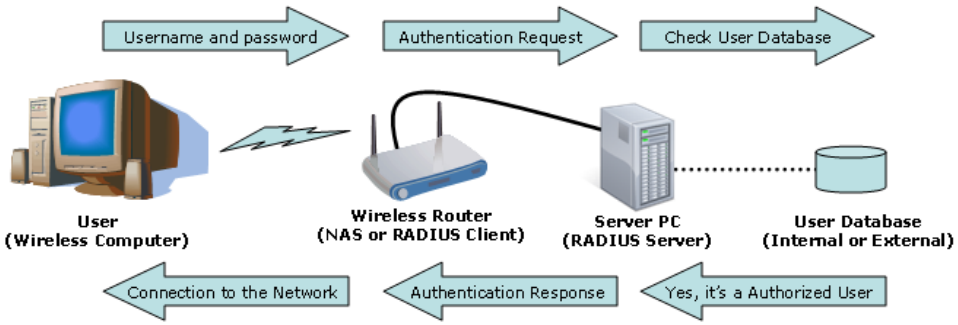

Ilustración 12 Autenticación RADIUS

En entornos domésticos o de pequeñas oficinas, donde no hay servidores de autenticación, WPA funciona en modo PKS (Pre-Shared Key), permitiendo a los usuarios configurar las claves manualmente en el punto de acceso y en los clientes.

2.2.4 WPA2 (Wi-Fi Protected Access 2)

WPA2 fue creado para corregir las vulnerabilidades detectadas en su antecesor, WPA. Este sistema cumple con todas las características del estándar IEEE 802.11i y en Junio de 2004 fue ratificada como la versión certificada del estándar 802.11i.

La principal ventaja de WPA2 respecto a WPA es que este primero utiliza el sistema de cifrado por bloques conocido como AES (Advanced Encryption Standard).

Otra ventaja de este sistema es que incluye el protocolo de encriptación CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), sustituyendo al TKIP. El uso del protocolo CCMP es obligatorio en el estándar WPA2, pero opcional en WPA.

CCMP emplea el algoritmo de seguridad AES. A diferencia de TKIP, la integridad de la clave de administración y mensaje es manejada por un único componente creado alrededor de AES utilizando una clave de 128 bits.

2.2.5 WPS (Wi-Fi Protected Setup)

El WPS es un mecanismo creado para facilitar la conexión de dispositivos wireless. Existen varios métodos a través de los cuales un dispositivo puede unirse a una red inalámbrica mediante WPS, pero el más extendido es el intercambio de PIN. El dispositivo debe transmitir un código numérico al router y a cambio este último le envía los datos para acceder a la red. Es decir simplemente se debe enviar un código PIN de 8 dígitos para que el router permita acceder a la red inalámbrica.

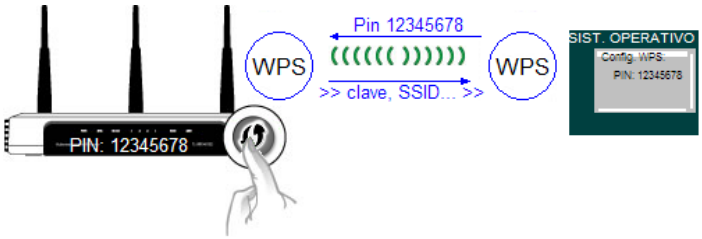

Ilustración 13 Acceso mediante WPS

WPS define una arquitectura con tres elementos con roles diferentes:

- Registrar (matriculador): dispositivo con la autoridad de generar o revocar las credenciales en la red. Tanto un AP como cualquier otra estación o PC de la red pueden tener este rol. Puede haber más de un Registrar en una red.
- Enrollee (matriculado): dispositivo que solicita el acceso a la red WLAN.
- Authenticator (autenticador): AP funcionando de proxy entre el Registrar y el Enrollee.

El inconveniente de esta funcionalidad es que el tiempo que un atacante necesita para averiguar un PIN de 8 dígitos es mucho menor que el que necesita para averiguar la contraseña WPA2 configurada en la red.

2.3 Clasificación y tipo de ataque a redes Wi-Fi.

Tal y como se ha comentado anteriormente, dado que el aire es el medio por el que se transmite la información, es muy sencillo escuchar esta información. Existe la práctica de realizar un mapa exacto de la ubicación de estos puntos de acceso con la ayuda de un sistema de posicionamiento global. Estos mapas pueden revelar las redes inalámbricas inseguras que están disponibles. A esto se conoce como Wardriving, el cual dio origen al Warchalking, que es un lenguaje

de símbolos escritos con tiza en las paredes y que informa a los posibles interesados de la existencia de una red inalámbrica en ese punto.

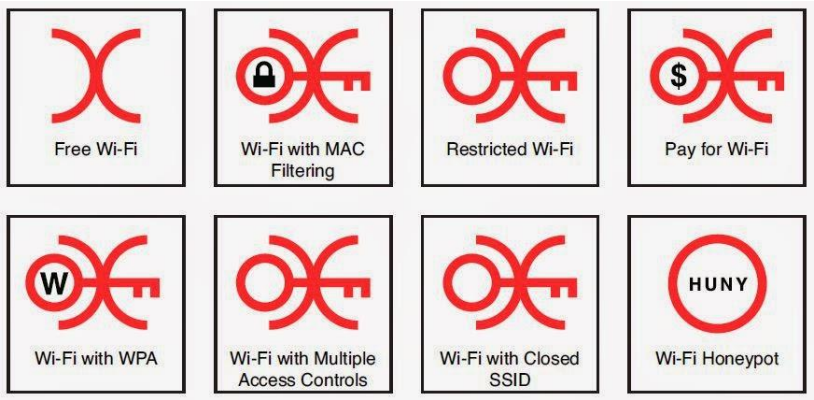

Ilustración 14 Símbolos Wardriving

Si bien el escaneo e identificación de puntos de acceso no es una actividad ilegal, el acceso a una red Wi-Fi sin la autorización de su propietario puede suponer un delito en muchos países, el cual puede estar penado con diferentes sanciones.

Cuando se hace referencia a un acceso sin autorización a una red, hablamos del concepto de ataque. Este ataque es un evento exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Los ataques a redes se pueden agrupar en dos categorías:

- Ataques pasivos: en los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, con el objetivo de interceptar los datos y obtener información que está siendo transmitida. Es una técnica sutil para obtener información de la comunicación. Cualquier ataque pasivo tiene los siguientes objetivos principales:
  - Intercepción de datos: consiste en el conocimiento de la información cuando existe una liberación de los contenidos del mensaje.
  - Análisis de tráfico: consiste en la observación de todo el tráfico que pasa por la red.

Las técnicas más conocidas dentro de los ataques pasivos son:

- Sniffing: consiste en capturar el tráfico de la red para obtener datos relevantes (usuarios, contraseñas, direcciones IP, etc...).

- Ataques al protocolo WEP: en este tipo de ataque se requiere capturar un gran volumen de paquetes de información con el objetivo de obtener la clave.
- Ataques al protocolo WPA/WPA2: consiste en capturar la secuencia de autenticación del protocolo WPA, por lo que es necesario que un cliente se conecte. Por último se utiliza un ataque de fuerza bruta para obtener la clave utilizada en el cifrado.
- Ataques de fuerza bruta: este tipo de ataque trata de obtener la clave de acceso probando todas las combinaciones posibles. La fuerza bruta suele combinarse con un ataque de diccionario. El ataque de diccionario es un método similar al de fuerza bruta pero prueba todas las palabras del diccionario.

❖ Ataques activos: estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

  - Suplantación: el intruso se hace pasar por una entidad diferente y se suele utilizar de forma conjunta con otro tipo de ataque activo.
    El ataque más representativo de suplantación es el ataque Man-in-the-Middle (MiTM). Este método sólo necesita que el atacante se sitúe entre las dos partes que intentan comunicarse interceptando los mensajes enviados e imitando al menos a una de ellas.
  - Reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
  - Modificación: una porción del mensaje legítimo es alterado, retardado o reordenado, para producir un efecto no autorizado. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.
  - Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Este tipo de ataque también es conocido como ataque DoS (siglas en inglés de Denial of Service) o DDoS (Distributed Denial of Service).

3. Análisis práctico de la seguridad en redes Wi-Fi

3.1 Introducción.

Una vez se han visto qué medidas existen para securizar una red Wi-Fi, en este capítulo se pondrán en práctica algunos ataques con el fin de acceder a una red de prueba.

Para poder llevar a cabo los ataques se ha creado un entorno de laboratorio que consta de un router inalámbrico Linksys WRT320N, un ordenador portátil ASUS N53SV y una suite de auditoría Wi-Fi.

Existen múltiples distribuciones que permiten hacer análisis de redes inalámbricas como:

- Kali Linux
- BackTrack
- Xiaopan OS
- Knoppix STD

Se ha elegido la distribución GNU/Linux Wifislax (basada en Slackware) ya que está especializada en la auditoría de redes inalámbricas y test de penetración. Tiene múltiples herramientas sencillas de utilizar tanto para personas que están iniciándose como para usuarios más experimentados. Dado que uno de los objetivos de este trabajo de fin de grado es poner en relieve cuanto de complicado resulta acceder a una red sin autorización y si es necesario tener conocimientos avanzados para realizarlo, la elección de esta distribución queda justificada.

Ilustración 15 Logo de la distribución de auditoría

Otra ventaja que ofrece Wifislax es que se puede usar como LiveCD o LiveUSB con lo que no es necesario instalarlo en el disco duro. Esta distribución tiene preinstalado el software aircrack-ng, que es una colección de programas que permiten auditar y atacar redes inalámbricas. Las herramientas que incluye aircrack son las siguientes:

- airmon-ng. Permite poner la tarjeta inalámbrica en modo monitor (sniffer).
- airodump-ng. Guarda las capturas del tráfico de red para ser procesado posteriormente con aircrack-ng.
- aircrack-ng. Permite romper el protocolo WEP y WPA para conseguir la clave de encriptación.
- aireplay-ng. Permite inyectar paquetes ARP-Request en una red inalámbrica para generar tráfico y de esta forma, que sea más fácil romper la clave con aircrack-ng.

A lo largo de este punto se realizarán varios intentos de intrusión usando diferentes procedimientos.

Con el primer punto se intentará determinar el nombre de la red que será objeto de la intrusión y posteriormente se ejecutará un ataque que permita saltarse la protección basada en control de acceso.

Los subsiguientes puntos se centrarán en las vulnerabilidades del protocolo WEP, WPA2 y WPS.

El router Linksys WRT320N permite implementar todas las medidas de seguridad citadas anteriormente.

Ilustración 16 Vista frontal del router

Ilustración 17 Vista trasera del router

Adicionalmente este router también permite el uso de WPA/WPA2-Enterprise con lo que también es válido para la implementación de un servidor RADIUS, el cual será abordado en el punto 4.

3.2 Ocultación del SSID

Una de las medidas de seguridad que se implementan en los puntos de acceso, está basada en la ocultación el SSID, es decir, que cuando se haga un escaneo de las redes Wi-Fi no aparezca el nombre de la red. Que no figure en la búsqueda

no implica que no esté presente. El dispositivo que actúa como cliente Wi-Fi al intentar conectarse a una red o descubrir si esta red se encuentra al alcance, envía al punto de acceso un frame de tipo Probe Request con el fin de solicitarle cierta información al AP al mismo tiempo que le envía información propia. El punto de acceso responde al cliente mediante otro frame conocido como Probe Response (tipo=0x00, subtipo=0x05). El intercambio de estos mensajes da inicio al proceso de asociación de un cliente con el punto de acceso.

Parte de la información enviada a la red por el cliente es el nombre de la red Wi-Fi. Como este tipo de frames no van cifrados ni protegidos de ser vistos por otras personas, basta con monitorizar el tráfico de red con un sniffer hasta que se conecte un cliente legítimo para conocer el nombre de la red.

Mediante la interfaz de administración web del punto de acceso se configura el SSID UOC_LAB y se deshabilita la difusión del mismo:

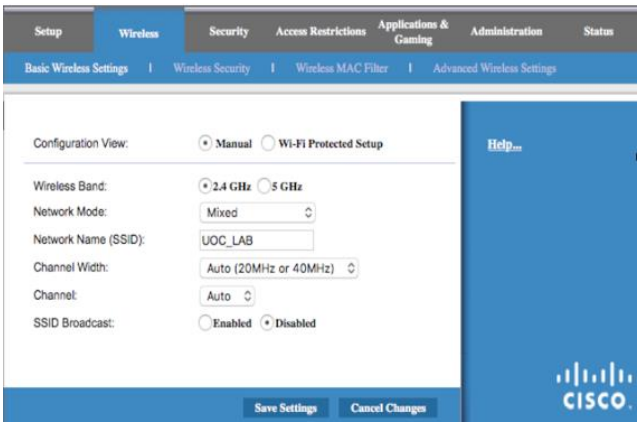

Ilustración 18 Ocultación del SSID

Primer paso: para buscar redes que tengan oculto el SSID se hará uso de la aplicación airoscript (incluida dentro de la distribución Wifislax). Una vez abierta, se debe elegir una interfaz inalámbrica. En este caso wlan0:

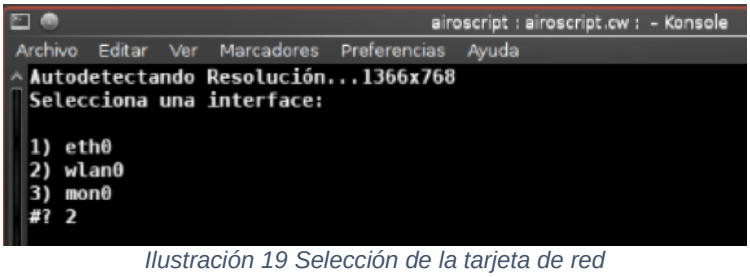

Ilustración 19 Selección de la tarjeta de red

El asistente preguntará si desea poner la tarjeta Wireless en modo monitor. Para activarlo se selecciona la opción 1:

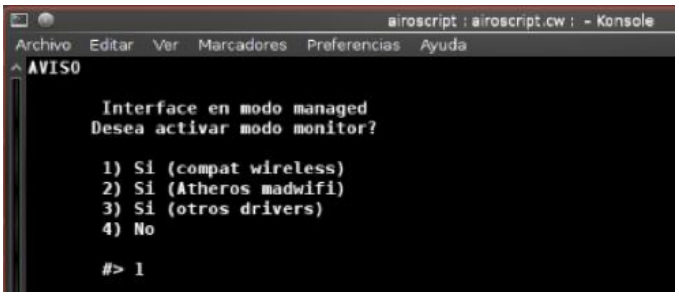

Ilustración 20 Activación del modo monitor

En la siguiente ventana seleccionamos la opción 1 para escanear la redes cercanas.

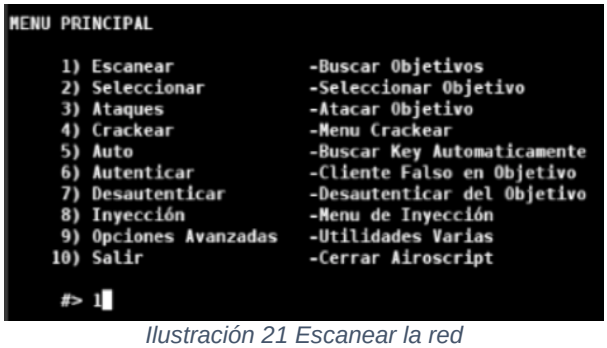

Ilustración 21 Escanear la red

Indicamos que la búsqueda sea sin filtros y en todos los canales:

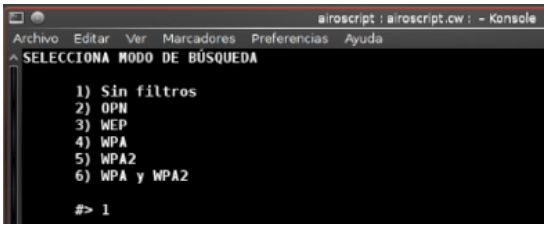

Ilustración 22 Búsqueda sin filtros

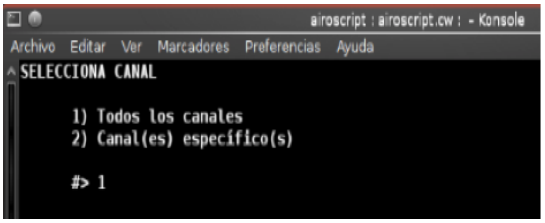

Ilustración 23 Búsqueda en todos los canales

La aplicación comenzará a mostrar información por pantalla:

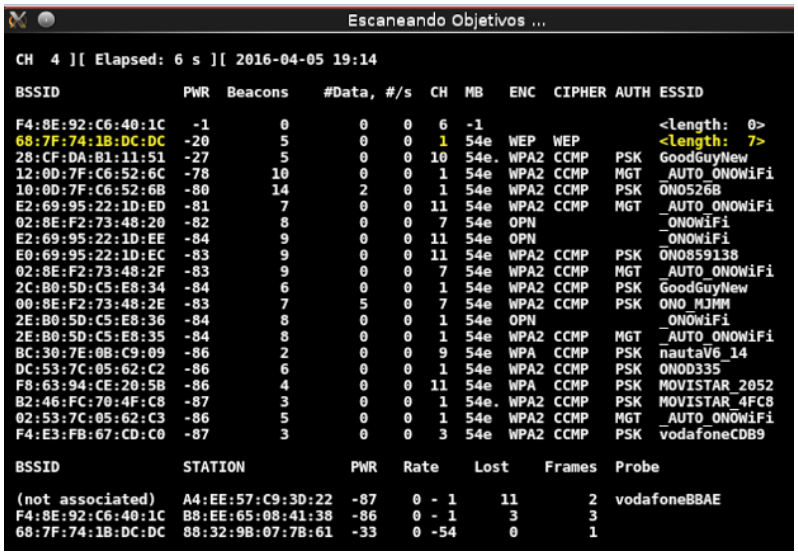

Ilustración 24 Resultado de la búsqueda

Las redes que ocultan el SSID son mostradas como <lenght: x>, donde la x representa un número. Una vez verificado que la dirección MAC (marcada en amarillo) corresponde al punto de acceso se procede a anotarla, al igual que el canal en el que transmite (canal 1).

Segundo paso: para determinar el SSID es necesario capturar el tráfico de red, para ello se hace uso de la utilidad Wireshark. Se vuelve a activar, de nuevo, el modo monitor de la tarjeta wireless con el fin de capturar todo el tráfico que circula por ella. Se ejecuta la herramienta airmon-ng incluida en la suite Aircrack.

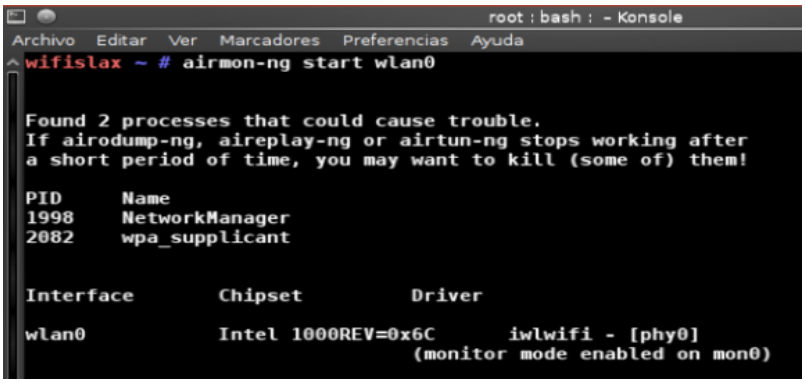

Ilustración 25 Activación del modo monitor

Al abrir el software de captura, éste muestra las redes cercanas que publican el nombre de red:

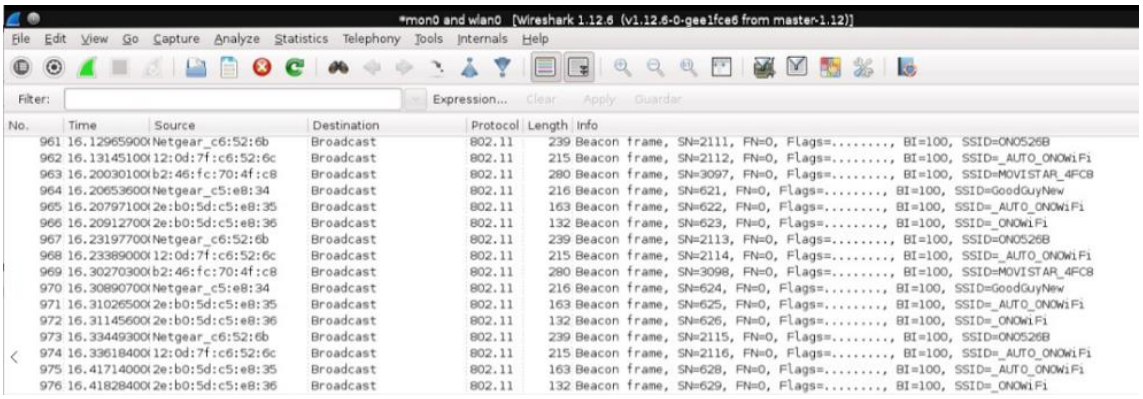

Ilustración 26 Captura Wireshark

Tercer paso: como ya se dispone de la MAC de punto de acceso y el canal de transmisión es posible obtener información adicional con el comando airodump-ng:

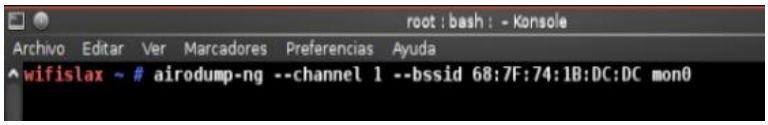

Ilustración 27 Ejecución de airodump-ng

En la siguiente imagen se puede ver el resultado de la ejecución de airodump-ng:

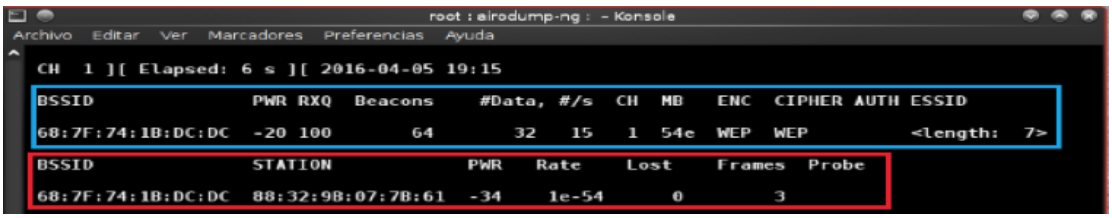

Ilustración 28 Resultado de la ejecución de airodump-ng

En el recuadro azul se puede ver la MAC del AP mientras que en el recuadro rojo se muestra la estación conectada.

Cuarto paso: el ataque de Deauthentication consiste en desautenticar a un dispositivo que hay en la red forzándolo a que se vuelva a conectar de forma automática. Para realizar las desautenticación del cliente se ejecuta la herramienta aireplay-ng tal y como sale en la siguiente imagen:

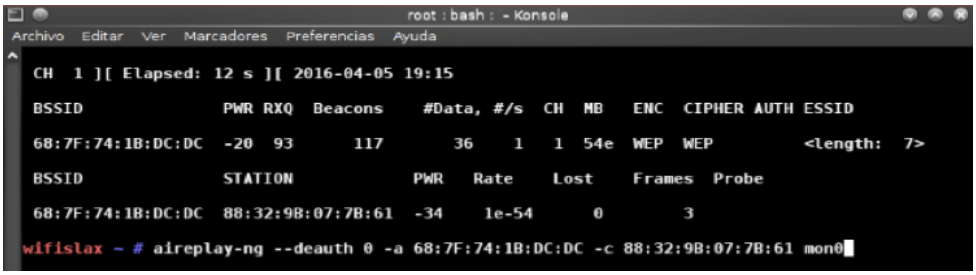

Ilustración 29 Ejecución de airoplay-ng

El parámetro -a indica el punto de acceso y -c el cliente:

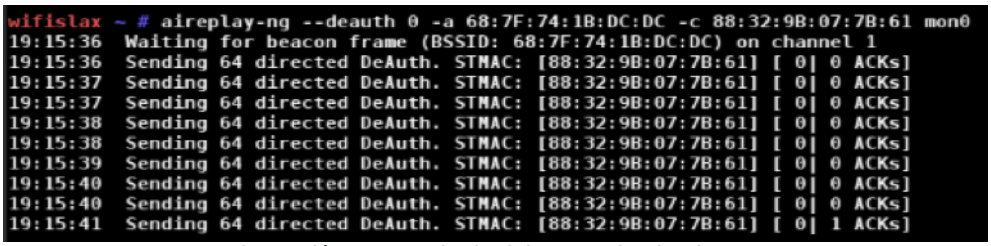

Ilustración 30 Resultado del comando aireplay-ng

Una vez conseguido que se generen los paquetes que nos interesan, debemos buscarlos en el Wireshark (tiene que estar capturando tráfico antes de la ejecución del ataque). Debido a la gran cantidad de paquetes que se obtienen, es recomendable aplicar un filtro de la MAC del AP en buscar de los paquetes de subtipo *Probe Response* que contienen la información que se precisa.

Antes de lanzar el ataque de Deauthentication vemos que el punto de acceso

no publica el SSID:

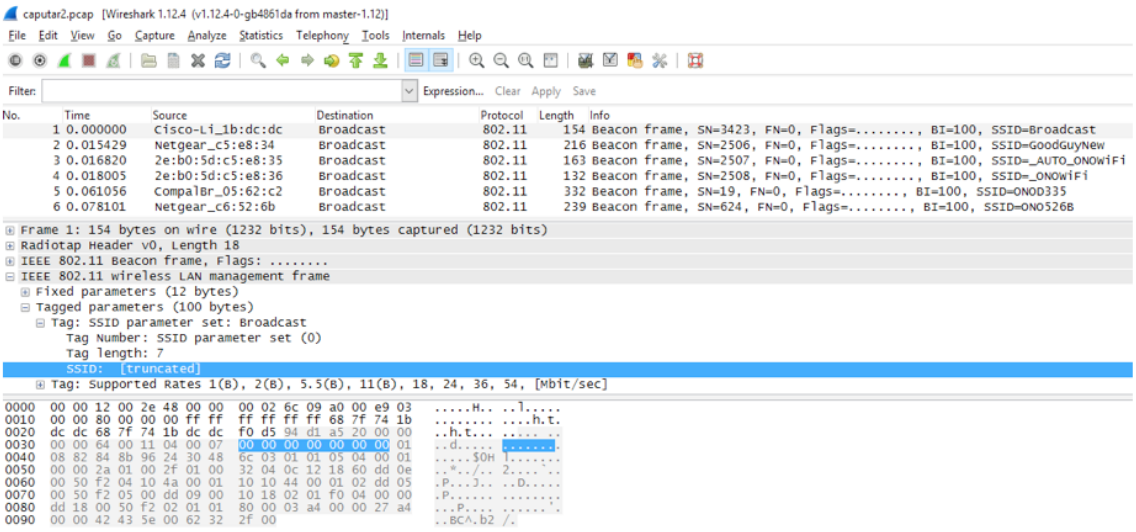

Ilustración 31 SSID oculto

Durante el envío de los paquetes Deauthentication en la captura ya aparece el SSID que anteriormente figuraba como oculto:

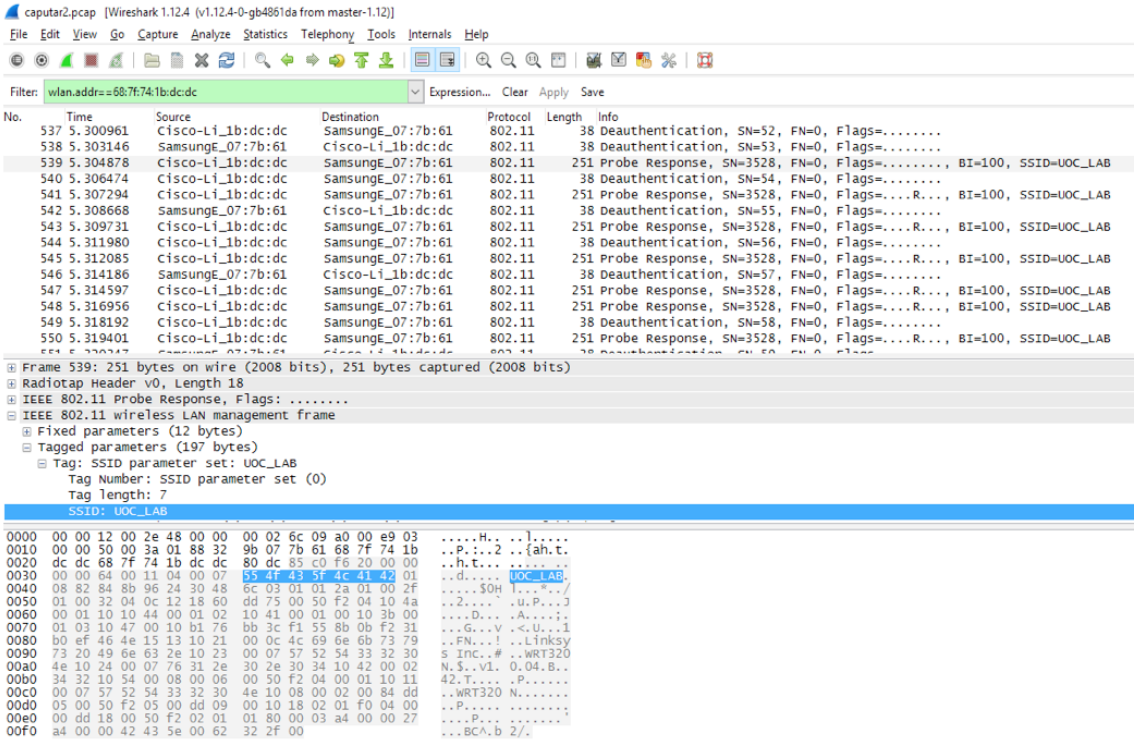

Ilustración 32 Identificación del SSID

3.3 Listas de control de acceso

En el punto de acceso se ha configurado que solo las direcciones MAC que figuran en el listado sean las permitidas para conectar a la red:

Ilustración 33 Activación filtrado MAC

Una vez obtenido el nombre de la red inalámbrica, se presupone que ésta estará habilitada en el filtrado MAC. Como ya se dispone de la dirección física de al menos un equipo conectado (ilustración 28) tan solo es necesario clonar la dirección en el equipo desde donde se está haciendo el ataque.

Primer paso: desde una consola del sistema se procede a parar la interfaz wireless mediante el comando: ifconfig wlan0 down.

Segundo paso: clonar la MAC con el uso del comando: ifconfig wlan0 hw ether 88:32:9B:07:7B:61

Tercer paso: desde una consola del sistema se procede a levantar la interfaz de red wireless mediante el comando: ifconfig wlan0 up:

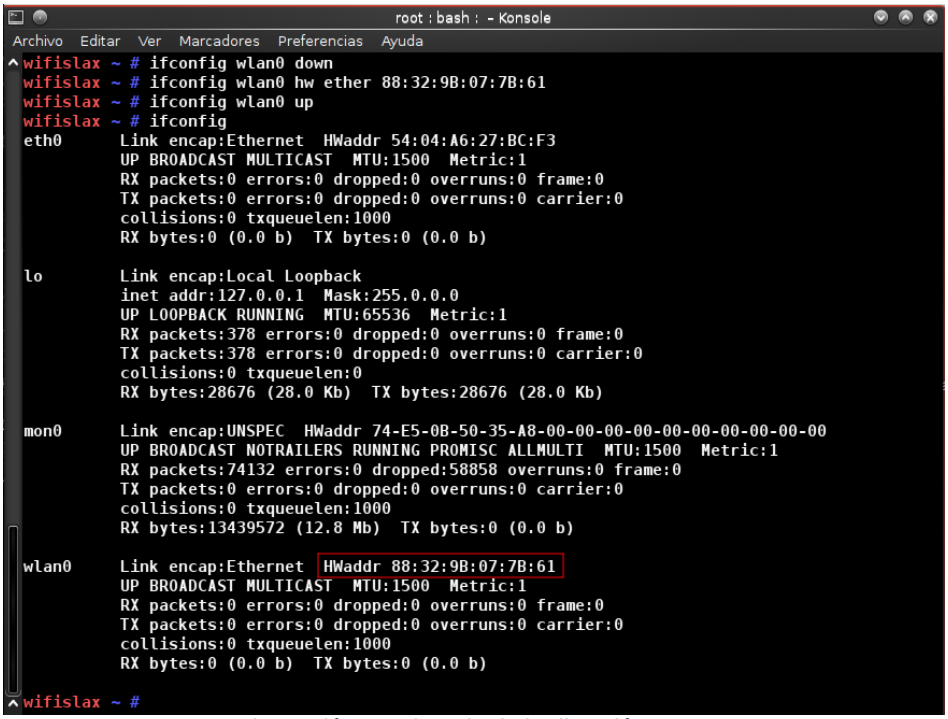

Ilustración 34 Clonado de la dirección MAC

En la imagen anterior se puede ver como el sistema operativo ha reemplazado la dirección física del portátil por la nueva.

3.4 Ataque WEP

Para obtener la clave WEP de la red UOC_LAB se hará uso de goyscript. Esta herramienta está basada en la suite Aircrack-ng para la explotación de vulnerabilidades en el cifrado WEP. En concreto realiza el ataque estadístico FMS (Flushrer, Mantin y Sharmir son los apellidos de los investigadores que descubrieron la vulnerabilidad) el cual está basado en las debilidades derivadas de la implementación específica del algoritmo RC4 en WEP, en concreto en el modo de operación de RC4 y sus módulos Key Scheduling Algorithm (KSA) y Pseudo-Random Generation Algorithm (PRGA).

La principal carencia existente en la encriptación WEP está motivada por la implementación del vector de inicialización. Este tiene un rango fijo de valores y si la clave WEP no es cambiada, los keystreams (clave generada por el usuario más un IV) también se repetirán. Por lo que se pude aplicar un enfoque matemático a la reutilización de los IV. Primero se capturan los paquetes hasta que se encuentren dos que tienen el mismo vector de inicialización (éste se envía en texto plano):

- M1=informacion1(x)keystream(clave web, IV) -> primer mensaje cifrado
- M2=informacion2(x)keystream(clave web, IV) -> segundo mensaje cifrado

Se aplica una operación xor entre ambos:

- M1(x)M2=informacion1(x)informacion2

Se observa que si los keystream son los mismos en ambos mensajes al realizar una operación xor entre ellos el keystream desaparece. Ahora si hacemos el xor entre un mensaje sin cifrar y el mismo cifrado, nos dará el keystream para ese IV. Conociendo el keystream asociado a un IV, podremos descifrar todas las tramas que usen el mismo IV.

Con lo que hemos descrito no podemos deducir la clave secreta, aunque sí es posible generar una tabla con los IVs de los que sabemos su keystream, la cual permitirá descifrar cualquier mensaje que tenga un IV contenido en esta tabla. Sin embargo, podemos llegar a deducir la clave secreta. La vulnerabilidad descrita por FMS dice que se puede conseguir la clave total conociendo parte de la clave (justamente, el IV que es conocido). Para ello necesitamos recopilar

suficientes IVs y sus keystreams asociados obtenidos por el procedimiento anterior.

Una vez señalada la base del ataque pasaremos a la ejecución del mismo en el laboratorio.

Durante el escaneo inicial de la red se obtuvieron datos como la MAC de la estación base, canal de transmisión y el cifrado utilizado:

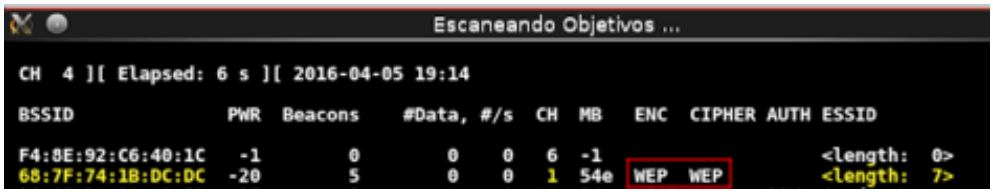

Ilustración 35 Red con cifrado WEP

Desde la web de administración del AP se puede ver la contraseña establecida:

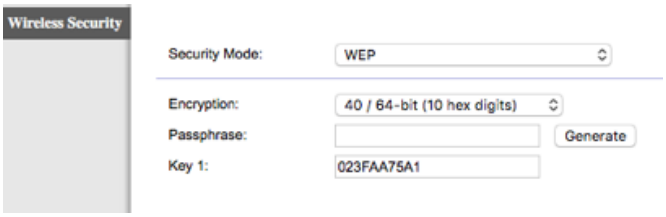

Ilustración 36 Contraseña WEP

Una vez ejecutada, la utilidad detecta la tarjeta de red y automáticamente comienza a explorar redes con cifrado WEP:

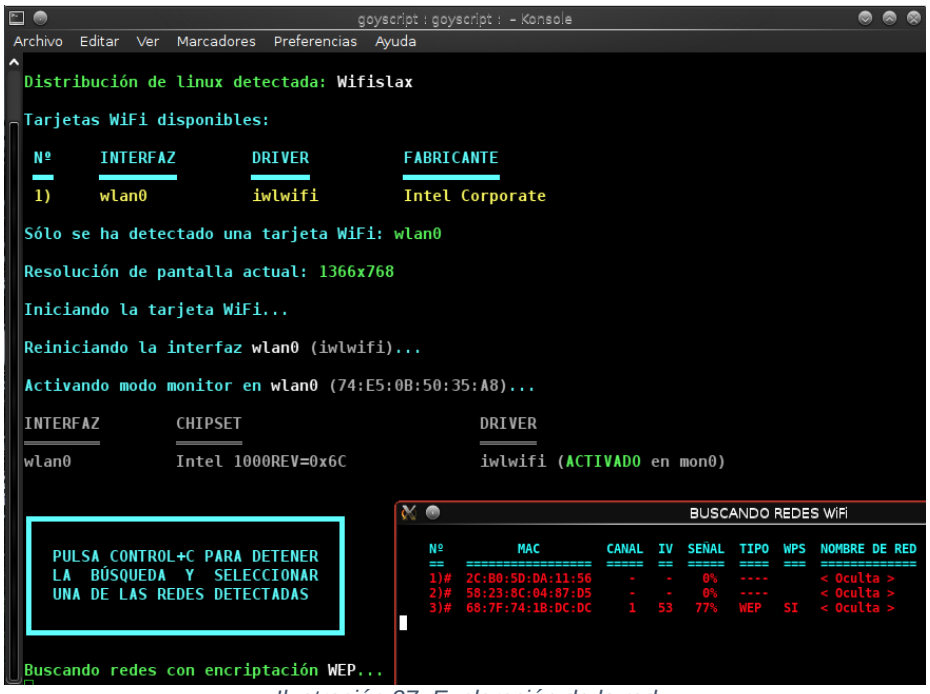

Ilustración 37 Exploración de la red

Una vez localizada la red a atacar se pulsa CONTROL + C para continuar con el asistente. Este requerirá que introduzca una de las redes detectadas:

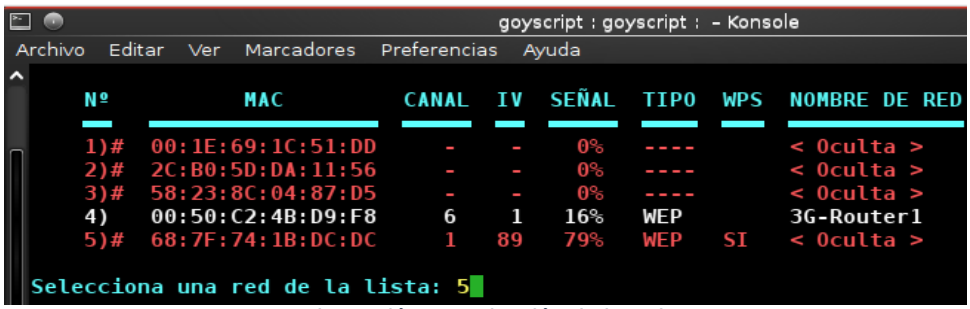

Ilustración 38 Selección de la red

Como la red seleccionada tiene oculto el SSID se debe introducir manualmente:

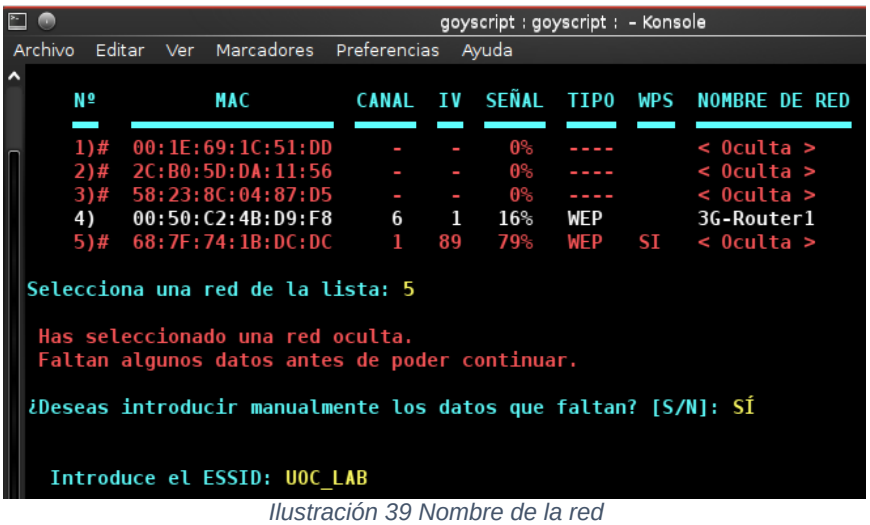

Ilustración 39 Nombre de la red

A partir de este momento goyscript comienza a lanzar el ataque:

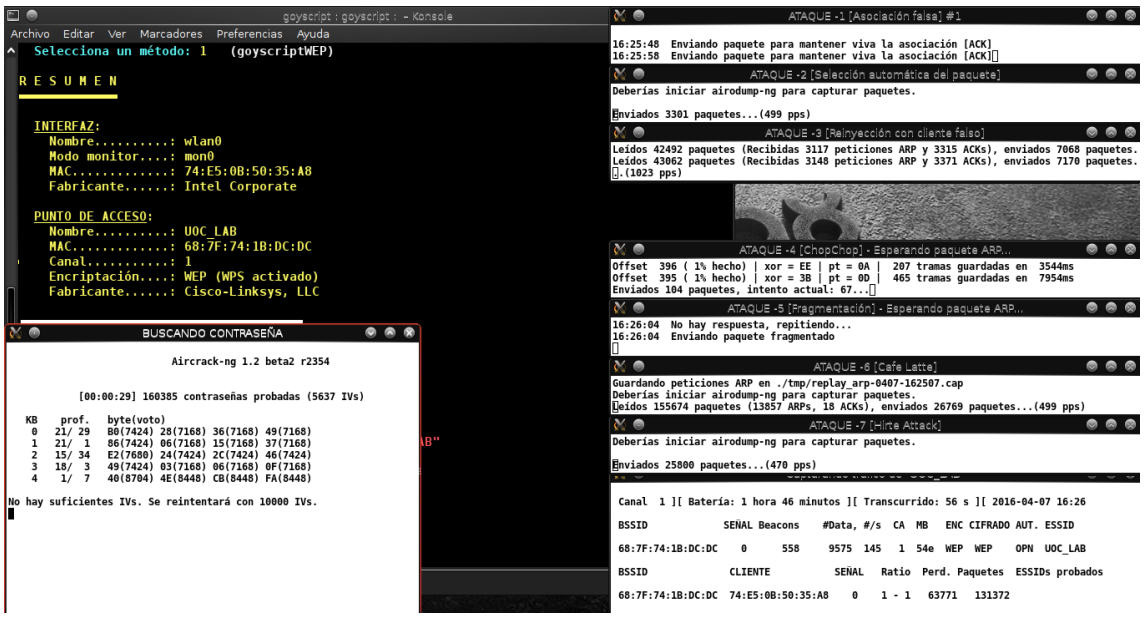

Ilustración 40 Ejecución de goyscript

Goyscript envía gran cantidad de paquetes de forma muy rápida ya que el IV tiene un tamaño fijo de 24 bits (16 millones de valores posibles), pero una vez se han utilizado todos estos valores comienzan a repetirse. Una vez se ha recolectado un número elevado de IVs (múltiplos de 5000) se puede descifrar la clave. Como se conoce el primer byte del keystream y los primeros m bytes de la clave, se puede derivar el byte m+1. El primer byte del plaintext es conocido porque corresponde a la cabecera SNAP (Subnetwork Access Protocol) de WEP. A partir de esta información se deberá capturar un IV de la forma (a+3, n-1, x) para el byte en el lugar “a” de la clave, espacio de valores “n” y cualquier “x”. Por ejemplo, primero necesitará IVs de la forma (3, 255, x). El algoritmo se aplica sucesivamente a todos los bytes para descifrar la clave [4].

La aplicación ha necesitado 1 minuto para dar con la clave WEP:

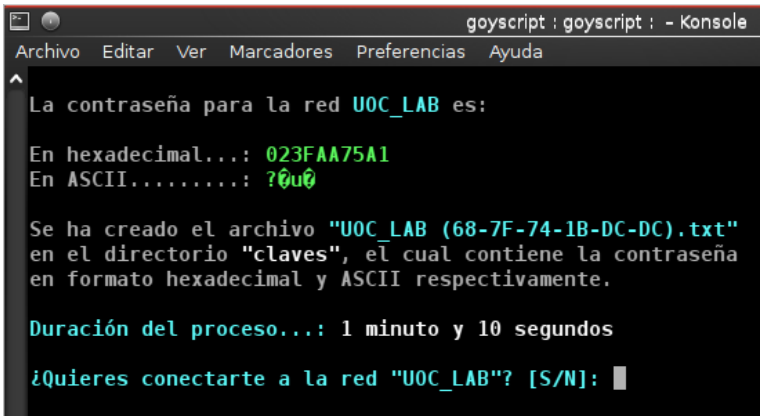

Ilustración 41 Clave WEP descifrada

Ahora procederemos a introducir la contraseña más segura que permite el AP (26 dígitos en hexadecimal y con una encriptación de 128 bits) y repetimos el ataque:

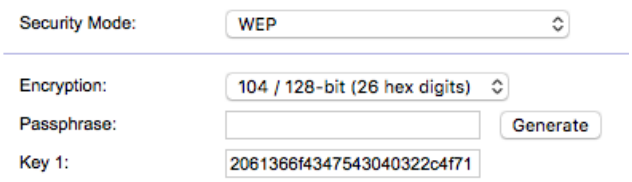

Ilustración 42 Contraseña WEP 128 bits

En este caso vemos que tan solo ha requerido de 10 minutos más para obtener la contraseña:

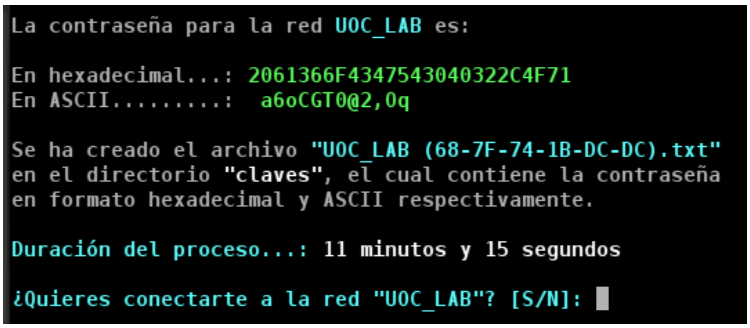

Ilustración 43 Clave WEP 128 bits descifrada

3.5 Ataque WPA2

Tanto WPA-PSK como WPA2-PSK padecen de vulnerabilidad y es posible atacar estas tecnologías con el objetivo de poder acceder a la red sin autorización. Para comprender la vulnerabilidad debemos fijarnos en el proceso de comunicación que se lleva a cabo entre un cliente (Supplicants) y un AP (Authenticator) que consiste en el intercambio de una serie de paquetes Probe Request (cliente), Probe Response (AP), Authentication Request (cliente), Authentication Response (AP), Association Request (cliente) y Association Response (AP). Hasta este punto un cliente se encontraría asociado con un AP y posteriormente vendría el intercambio de paquetes de datos. Para cifrar cualquier paquete de datos se emplea un mecanismo de generación de clave dinámica entre cliente y AP, esto simplemente significa que para cada sesión entre clientes y el AP, se utilizan un par de claves distintas a las de los demás clientes.

La forma de generar dinámicamente dichas claves es gracias al algoritmo PBKDF2 que permite la generación de lo que se conoce como Pre-Shared Key (PSK). Se trata de un algoritmo basado en una clave de entre 8 y 63 caracteres la cual es tomada como parámetro y finalmente con dicho valor se genera de forma aleatoria una nueva PSK. El algoritmo PBKDF2 en su implementación interna toma 5 parámetros que son: la clave del AP seleccionada por el administrador del router (passphrase), el SSID, la longitud del SSID, el número de veces que el passphrase será codificado (hashed) 4096 y la longitud de la clave PSK. Con estos parámetros el algoritmo genera una clave PSK de una longitud de 256 caracteres

Hasta este punto solamente se tienen un par de claves PSK que serán utilizadas

en el cliente y en el punto de acceso, ahora llega el momento de intercambiar paquetes de datos entre ambas entidades. En la fase de intercambio de claves entre el Supplicants y el Authenticator éstos utilizan la PSK para generar una clave llamada Pairwise Master Key. Con la PMK se genera otra clave de cifrado para cada proceso de autenticación de un cliente llamada PTK (Pairwise Transient Key), que se genera a partir de dos números aleatorios, uno de ellos generado por el cliente y el otro por el AP que intercambian para obtener ambos la misma clave PTK. A todo este proceso se le conoce como 4-way Handshake [5].

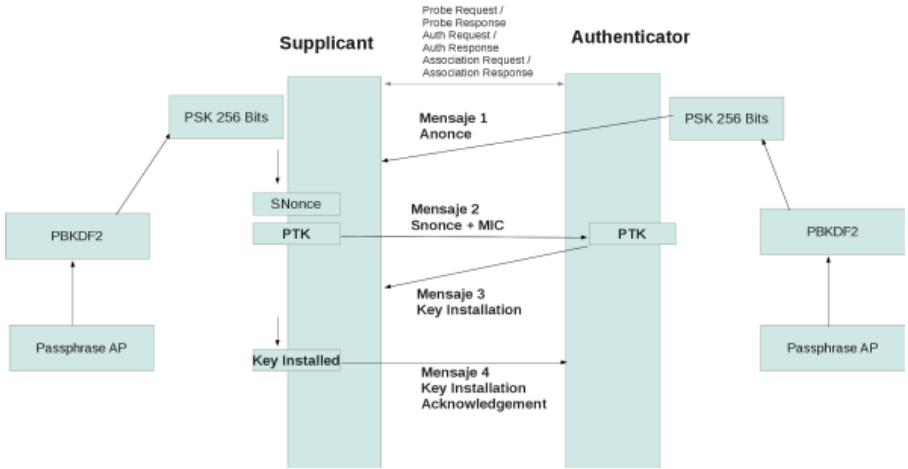

Ilustración 44 4-Way Handshake

El atacante interesado en atacar una red Wi-Fi estará interesado en capturar los paquetes que contengan los siguientes mensajes: Anonce, Snonce, MIC, MAC del cliente y MAC del AP. Los dos últimos campos son capturados fácilmente de cualquier paquete entre AP y Cliente, sin embargo los mensajes Anonce y Snonce solamente pueden ser capturados en el momento en el que se inicia el proceso de instalación de las claves PTK en el supplicant y el authenticator, por lo tanto, es necesario capturar todos los paquetes intercambiados entre un AP y sus correspondientes clientes con la finalidad de obtener el 4-way Handshake. Al conseguir el 4-way Handshake no se obtiene la clave Wi-Fi sino es un medio para poder compararla. Dado que el atacante tiene los mensajes necesarios para el 4-way Handshake (Anonce, Snonce, MIC, MAC del AP, MAC del Cliente) solamente necesita utilizar el algoritmo PBKDF2 para la generación de la clave PSK de 256 bits y posteriormente la generación de los mensajes correspondientes al 4-way Handshake, en este punto, los valores que se enviarán al algoritmo PBKDF2 son simplemente cada una de las palabras

contenidas en un diccionario de contraseñas. Para determinar si una de las palabras contenidas en el diccionario ha sido la que se ha usado para generar la clave PSK y la PTK, simplemente se compara el mensaje MIC (contenido en el mismo paquete que contiene el Snonce) y si coincide con el MIC del 4-way Handshake capturado anteriormente, se puede afirmar que se ha conseguido la clave correcta.

Para llevar a cabo este caso práctico se procede a cambiar el tipo de seguridad en el punto de acceso:

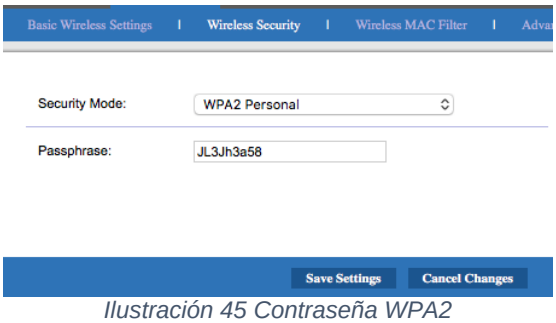

Ilustración 45 Contraseña WPA2

Primer paso: configurar la tarjeta de red wireless en modo monitor:

```
wifislax ~ # airmon-ng start wlan0


Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
1981    NetworkManager
2064    wpa_supplicant


Interface       Chipset         Driver

wlan0           Intel 1000REV=0x6C      iwlwifi - [phy0]
                                        (monitor mode enabled on mon0)
```

Ilustración 46 Modo monitor

Segundo paso: obtener información sobre el punto de acceso (MAC y canal de emisión):

```
CH  8 ][ Elapsed: 12 s ][ 2016-04-11 16:36

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

28:CF:DA:B1:11:51  -24        8       32   15  10  54e. WPA2 CCMP   PSK  GoodGuyNew
68:7F:74:1B:DC:DC  -28       10        0    0   6  54e  WPA2 CCMP   PSK  UOC_LAB
E2:69:95:22:1D:ED  -78       12        0    0  11  54e  WPA2 CCMP   MGT  _AUTO_ONOWiFi
E0:69:95:22:1D:EC  -78       15        0    0  11  54e  WPA2 CCMP   PSK  ONO859138
B2:46:FC:70:4F:C8  -80       12        0    0   1  54e. WPA2 CCMP   PSK  MOVISTAR_4FC8
12:0D:7F:C6:52:6C  -80       10        0    0   1  54e  WPA2 CCMP   MGT  _AUTO_ONOWiFi
10:0D:7F:C6:52:6B  -80       13        3    0   1  54e  WPA2 CCMP   PSK  ONO526B
02:8E:F2:73:48:2F  -80        9        0    0   7  54e  WPA2 CCMP   MGT  _AUTO_ONOWiFi
2E:B0:5D:C5:E8:35  -86       10        0    0   1  54e  WPA2 CCMP   MGT  _AUTO_ONOWiFi
2C:B0:5D:C5:E8:34  -86        7        2    0   1  54e  WPA2 CCMP   PSK  GoodGuyNew
F8:8E:85:5B:99:0E  -86        6        0    0  11  54e  WPA2 CCMP   PSK  JAZZTEL_990E
C2:3F:0E:F3:B7:72  -87        2        0    0   6  54e  WPA2 CCMP   MGT  _AUTO_ONOWiFi
DC:53:7C:05:62:C2  -87        8        0    0   1  54e  WPA2 CCMP   PSK  ONOD335
02:53:7C:05:62:C3  -88        2        0    0   1  54e  WPA2 CCMP   MGT  _AUTO_ONOWiFi

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

E0:69:95:22:1D:EC  14:2D:27:52:4B:31   -1    1e- 0      0        1
2C:B0:5D:C5:E8:34  88:32:9B:07:7B:9C  -76    0 -54      0        1
```

Ilustración 47 Obtención de MAC y Channel

Tercer paso: iniciar airodump-ng para capturar el handshake. Desde un terminal se ejecuta el comando:

airodump-ng -c 6 --bssid 68:7F:74:1B:DC:DC -w WPA2PSK mon0

El parámetro -a indica el punto de acceso, -c el cliente y -w nombre del fichero donde se guarda la captura del tráfico:

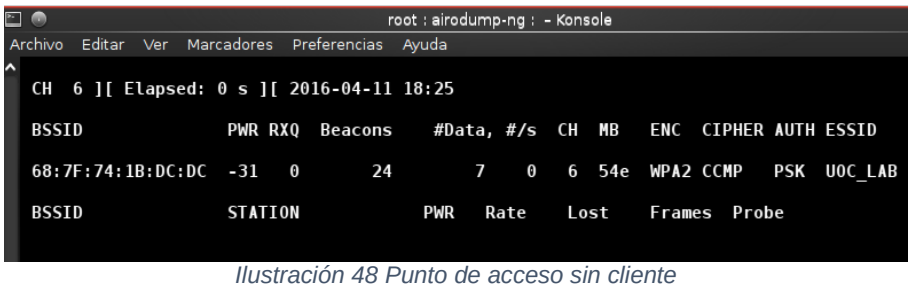

Ilustración 48 Punto de acceso sin cliente

Tras la conexión de una estación se puede ver como airodump ha capturado el handshake:

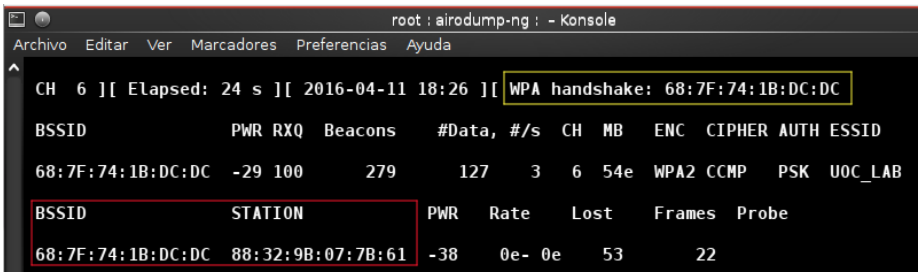

Ilustración 49 Punto de acceso con cliente

Cuarto Paso: usar aireplay-ng para desautentificar a un cliente conectado. Este paso es opcional y solo es necesario realizarlo si se quiere acelerar activamente todo el proceso. El requisito necesario es que se encuentre asociado un cliente con el AP en el momento del ataque:

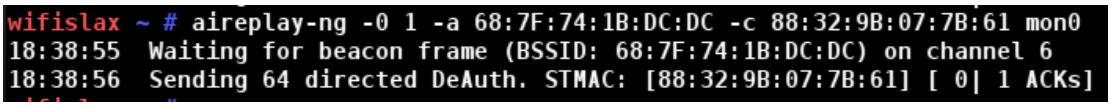

Ilustración 50 Desautenticación de cliente

El parámetro -a indica el punto de acceso y -c el cliente.

Quinto paso: ejecutar aircrack-ng para obtener la clave pre-compartida. Tal y como se ha comentado al inicio de este apartado, es necesario un diccionario para que la utilidad aircrack-ng pueda verificar si coincide la clave. Haciendo una búsqueda por internet se encuentran múltiples sites donde están disponibles

para su descarga. Para este caso se ha usado un diccionario con 4865841 entradas.

aircrack-ng -w diccionario.lst -b 68:7F:74:1B:DC:DC WPA2PSK.cap

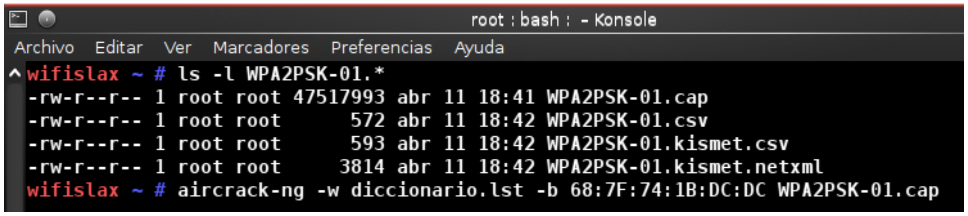

Ilustración 51 Ejecución de aircrack-ng

El parámetro -w indica el nombre del fichero que contiene el diccionario, -b el punto de acceso y WPA2PAS-01.cap es el nombre del fichero que contiene la captura del tráfico.

Desde el terminal se muestra el proceso:

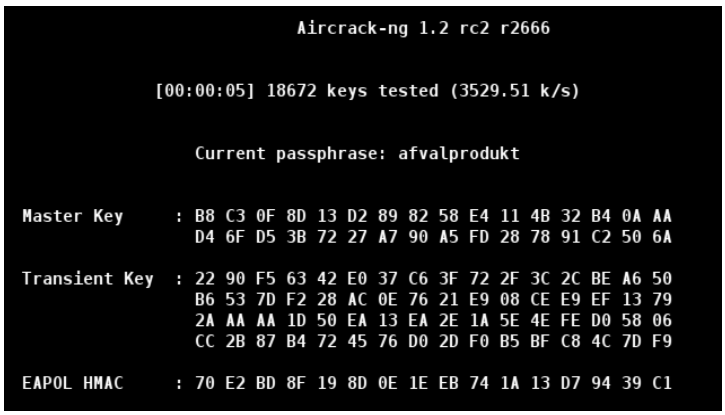

Ilustración 52 Inicio del proceso

Pasado unos minutos la aplicación muestra por pantalla la contraseña:

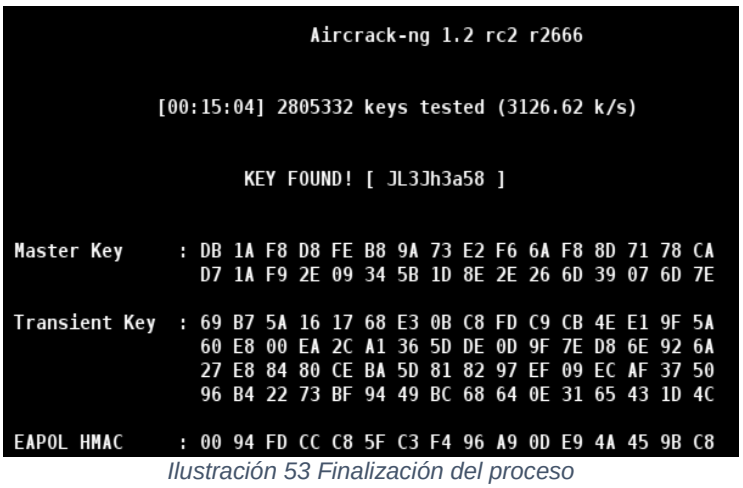

Ilustración 53 Finalización del proceso

A la vista del resultado anterior queda demostrado que la seguridad ofrecida por WPA2 no es del todo fiable, más aun si se hace uso de contraseñas poco seguras, ya que el éxito del ataque radica única y exclusivamente en la fortaleza de las contraseña que se haya utilizado. En este caso práctico se ha utilizado una contraseña alfanumérica muy simple.

También se debe evitar los nombres SSID comunes como: Home, Personal, Wifi, Default, etc.

Para generar una contraseña segura se deben seguir las siguientes recomendaciones:

- Debe tener ocho caracteres como mínimo.
- No debe contener el nombre de usuario, el nombre real o el nombre de la empresa. No debe contener una palabra completa.
- Debe ser significativamente diferente de otras contraseñas anteriores.
- Debe estar compuesta por caracteres de cada una de las siguientes cuatro categorías: minúsculas, mayúsculas, números y símbolos.

Dado que son muchos los factores a tener en cuenta, en Internet se encuentran generadores de claves que ayudan a conseguir una contraseña segura en pocos segundos como por ejemplo:

www.yellowpipe.com/yis/tools/WPA_key/index.php.

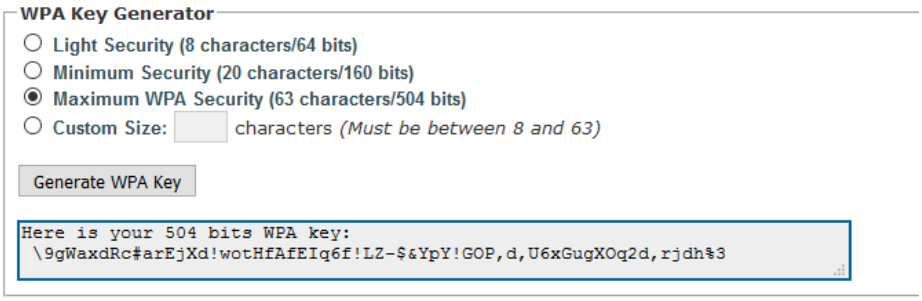

Ilustración 54 Generador WPA

Para determinar la fortaleza de una clave se puede recurrir a páginas como: www.passwordmeter.com.

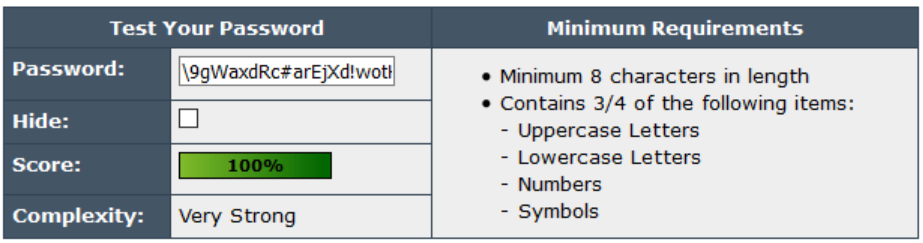

Ilustración 55 Verificación de fortaleza

3.6 Ataque WPS

El objetivo de este punto es usar la vulnerabilidad de WPS que fue descubierta en 2011 por Stefan Viehböck, el cual permite a un atacante obtener el PIN WPS de un punto de acceso y por ende la clave WPA/WPA2 mediante un ataque de fuerza bruta en un breve periodo de tiempo.

La vulnerabilidad se basa en los mensajes de registrar y el enrollee cuando se intenta validar un PIN. El protocolo de registro WPS establece una serie de mensajes de intercambio EAP (Extensible Authentication Protocol) de la siguiente forma:

```
Enrollee -> Registrar: M1 = Version || N1 || Description || PKE
Enrollee <- Registrar: M2 = Version || N1 || N2 || Description || PKR [ || ConfigData ] || HMAC_AuthKey(M1 || M2*)
Enrollee -> Registrar: M3 = Version || N2 || E-Hash1 || E-Hash2 || HMAC_AuthKey(M2 || M3*)
Enrollee <- Registrar: M4 = Version || N1 || R-Hash1 || R-Hash2 || ENC_KeyWrapKey(R-S1) || HMAC_AuthKey (M3 || M4*)
Enrollee -> Registrar: M5 = Version || N2 || ENC_KeyWrapKey(E-S1) || HMAC_AuthKey (M4 || M5*)
Enrollee <- Registrar: M6 = Version || N1 || ENC_KeyWrapKey(R-S2) || HMAC_AuthKey (M5 || M6*)
Enrollee -> Registrar: M7 = Version || N2 || ENC_KeyWrapKey(E-S2 [||ConfigData]) || HMAC_AuthKey (M6 || M7*)
Enrollee <- Registrar: M8 = Version || N1 || [ ENC_KeyWrapKey(ConfigData) ] || HMAC_AuthKey (M7 || M8*)
```

Ilustración 56 Mensajes WPS

La identificación del PIN WPS se articula alrededor de un juego de preguntas y respuestas llamadas Mx. Si el PIN empleado es correcto se usaran 8 mensajes M.

Todos los dispositivos WPS utilizan Pseudo Random Number Generator (PRNG) para generar claves públicas mediante la fórmula: g^{AB} mod p.

- g: es el generador.
- A: es un número privado usado por el "enrolle" (el punto de acceso).
- B: es un número privado usado por el "registrar" (el cliente).
- mod p: es un módulo primario tal y como se entiende en aritmética.

En los mensajes M1 y M2 se obtiene la siguiente información:

- N1 Enrollee Nonce.
- PKR Public Key (Registrar Nonce) (g^B mod p).
- PKE Public Key (Enrollee Nonce) (g^A mod p).

En el mensaje M3 se obtiene:

- E-Hash1= HMAC (E-S1, PSK1, PKE, PKR).
- E-Hash2= HMAC (E-S2, PSK2, PKE, PKR).

E-S1 y E-S2 son nonces (número arbitrario que sólo puede ser utilizado una vez) de 128 bits secretos generados justo después de que el punto de acceso genere su N1 Nonce.

Los E-Hash emplean la función de hash (algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija) HMAC para cifrar los datos que están entre paréntesis.

PSK1 (PIN1) y PSK2 (PIN2) son la primera y la segunda mitad de PIN del AP.

Reaver utiliza las siguientes debilidades que ocurren durante el proceso de registro:

1. Si el protocolo de registro falla en algún punto, el registrar enviará un mensaje NACK.

Si el atacante recibe un mensaje NACK después de enviar el M4, sabrá que la primera mitad del PIN es incorrecta (R-Hash1 comprueba que la primera mitad del PIN sea correcta, si recibimos un NACK es que el PIN no es correcto):

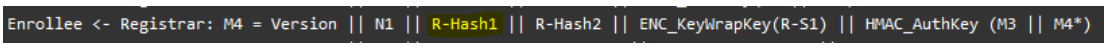

Ilustración 57 Mensaje M4

2. Si el atacante recibe un NACK después de enviar el mensaje M6, sabe que la segunda mitad del PIN es incorrecta (análogamente a lo que sucede con el mensaje M4).

Como el PIN1 está compuesto de cuatro dígitos y por tanto el número de combinaciones es de 10^4. El PIN2 varía dependiendo del fabricante, existe un caso donde el último dígito de este PIN (casuística muy común) se utiliza como checksum (tiene como propósito principal detectar cambios accidentales en una secuencia de datos para proteger la integridad de estos), por lo que el número de combinaciones desciende hasta 10^3. En el segundo caso el último dígito formaría parte de PIN, por lo que el número de combinaciones sería de 10^4. Nos enfrentamos a una tecnología que con un máximo de 20.000 combinaciones que se podría vulnerar, aunque normalmente son 11.000 combinaciones por usar el

último dígito como checksum.

Ilustración 58 PIN WPS

A través de la interfaz web se activa WPS:

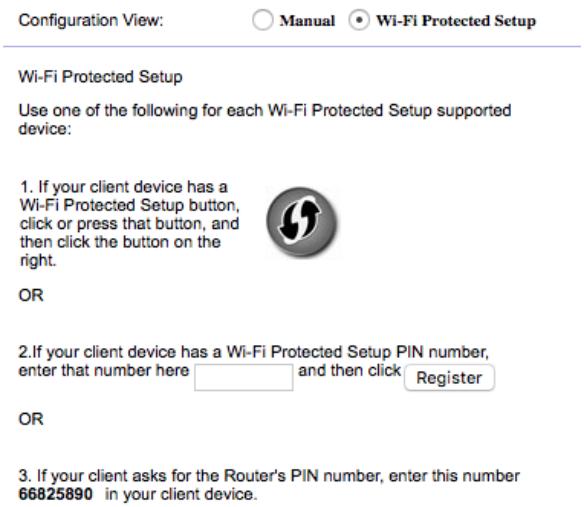

Ilustración 59 Activación de WPS

Primer paso: configurar la tarjeta de red wireless en modo monitor:

arimon-ng start wlan0

Para atacar redes con WPS se hará uso de Reaver; una herramienta que permite realizar ataques de fuerza bruta contra puntos de acceso.

Segundo paso: detectar puntos de acceso con WPS. Para obtener el listado de las redes se ejecutará:

#wash –i mon0 --ignore-fcs

Donde –ignore-fcs evita que salga por pantalla la información detallada:

```
wifislax ~ # wash -i mon0 --ignore-fcs

Wash v1.4-r119 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

BSSID               Channel    RSSI    Version    Locked    ESSID
--------------------------------------------------------------------------------
2C:B0:5D:C5:E8:34      1       -85      1.0        No      GoodGuyNew
DC:53:7C:05:A3:74      1       -90      1.0        No      ONOEFF1
DC:53:7C:05:62:C2      1       -88      1.0        No      ONOD335
DC:53:7C:3A:BC:DD      6       -89      1.0        No      ONOFB9B
68:7F:74:1B:DC:DC      7       -35      1.0        No      UOC LAB
```

Ilustración 60 Ejecución de wash

Tercer paso: ataque de fuerza bruta. Reaver ha sido desarrollado para realizar un ataque de fuerza bruta contra la primera mitad del PIN y una vez descubierto realizar otro ataque contra la segunda mitad.

Una vez localizada la red, se procederá a ejecutar reaver desde un terminal de consola:

```
wifislax ~ # reaver -i mon0 -b 68:7F:74:1B:DC:DC -c 7 -vv

Reaver v1.4-r119 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
```

Ilustración 61 Ejecución de reaver

Donde –b es la MAC del punto de acceso, -c es el canal de emisión y –vv el nivel de detalle de información que se quiere obtener.

Tras la ejecución, reaver comienza a generar contraseñas y prueba si son válidas:

```
[+] Switching mon0 to channel 7

[+] Waiting for beacon from 68:7F:74:1B:DC:DC
[+] Associated with 68:7F:74:1B:DC:DC (ESSID: UOC_LAB)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[!] WARNING: Receive timeout occurred
[+] Sending WSC NACK
[+] Trying pin 00005678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 11865674
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
```

Ilustración 62 Ataque de fuerza bruta

Pasadas unas horas se obtiene la contraseña y por pantalla se observa la contraseña del cifrado WPA:

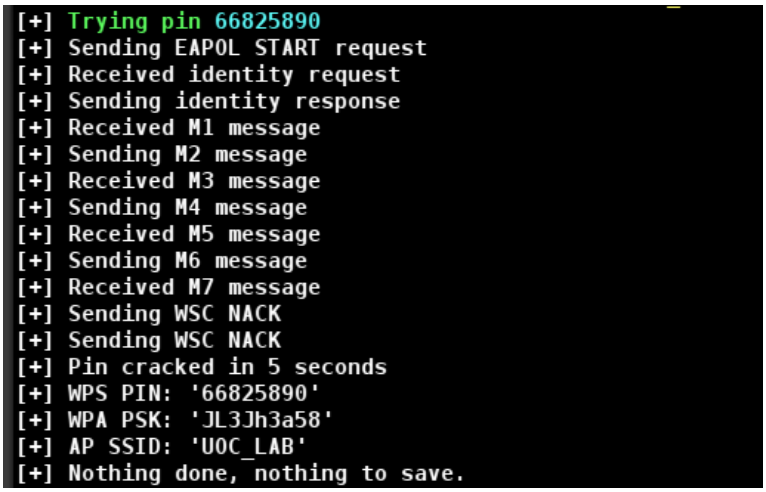

Ilustración 63 Obtención del PIN WPS

Tal y como funciona WPS una vez obtenido el PIN reaver transmite el código al router y a cambio este último le envía los datos para acceder a la red.

En el resumen de la configuración del punto de acceso se verifica que los datos obtenidos por reaver son correctos:

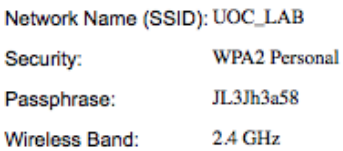

Ilustración 64 Clave WPA2

Ha quedado demostrado que aunque se disponga de un protocolo de WPA2-PSK con una contraseña con cierta complejidad, al configurar una red Wi-Fi con tecnología WPS se abre una puerta trasera que deja al descubierto la seguridad de la red.

3.7 Conclusiones

Acceder a una red Wi-Fi sin tener los datos de acceso es una tarea de una dificultad media y solo será necesario dedicarle unas horas.

No es obligatorio tener conocimientos avanzados de informática o programación para vulnerar una red. Si se poseen éstos, ayudarán, pero si no se tienen, bastará con ser un usuario audaz, ya que existen muchos programas preparados para realizar ataques a redes sin necesidad de extensos conocimientos.

Lo más habitual es que el atacante con un perfil bajo, que está iniciándose, siga un tutorial y consiga el acceso a redes con unos niveles de seguridad básicos. Pero no hay que olvidar que existen usuarios que se dedican de manera profesional y pasan largas horas aprendiendo el uso de las herramientas a un nivel más profundo, dado que las redes objetivos del ataque implementan una seguridad más compleja.

4. Autenticación en redes inalámbricas con RADIUS

4.1 Introducción

Actualmente la forma más efectiva de securizar una red Wi-Fi es mediante WPA/WPA2-Enterprise. El modo Enterprise, modo 802.1X o RADIUS ofrece una protección adecuada para las empresas ya que no solo es quien valida la identidad de quien accede a la red (a través de un método EAP) si no que es quien fuerza, con cierta frecuencia, la generación de una nueva clave de cifrado para la conexión establecida, haciendo que la probabilidad de que un ataque identifique la clave de cifrado sea mínima.

En el presente capítulo se procederá a explicar cómo implementar una plataforma que soporte WPA/WPA2-Enterprise haciendo uso de herramientas Open Source. Para ello se montará, en el laboratorio, un servidor FreeRADIUS y OpenLDAP con el objetivo de que los usuarios de la red inalámbrica usen como método de autenticación EAP-TTLS y con el protocolo de autenticación PAP.

4.2 WPA2-Enterprise

En entornos empresariales es necesario usar mecanismos de control de acceso versátiles y fáciles de mantener, como por ejemplo, identificación por medio de usuario/contraseña o la posesión de un certificado digital. Indudablemente el hardware de un punto de acceso no tiene la capacidad para almacenar y procesar toda esta información por lo que es necesario recurrir a un servidor que confirme las credenciales. Ahora bien, parece complicado que un cliente se pueda validar ante un componente de la red por cable si todavía no tiene acceso a la red y es en este punto donde entra en juego el IEEE 802.1X que permite el tráfico de validación entre un cliente y un equipo de la red local (RADIUS). Una

vez que se ha validado a un cliente es cuando WPA inicia TKIP para utilizar claves dinámicas o AES en el caso de WPA2.

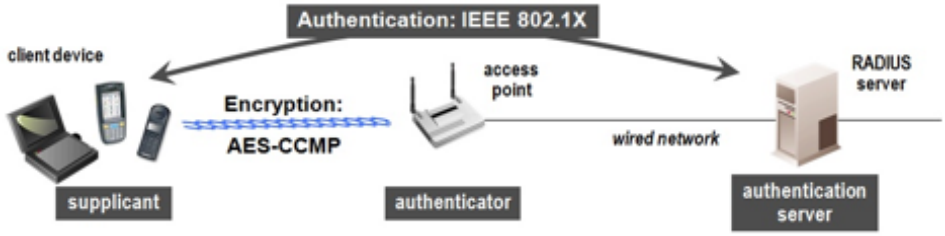

Ilustración 65 Validación IEEE 802.1X

Los clientes WPA/WPA2 tienen que estar configurados para utilizar un sistema concreto de validación que es completamente independiente del punto de acceso. Los sistemas de validación pueden ser:

- EAP-TLS: es un método de autenticación mutua, lo que significa que tanto el cliente como el servidor deben demostrar sus identidades uno a otro. Durante el proceso de autenticación, el cliente de acceso remoto envía su certificado de usuario y el servidor de acceso remoto envía su certificado de equipo. Si el certificado no se envía o no es válido, se termina la conexión.
- EAP-TTLs: método de autenticación basado en una identificación de usuario y contraseña que se transmiten cifrados mediante TLS, creando un túnel para transmitir las credenciales. La diferencia que presenta frente a EAP-TLS es que EAP-TTLs solo necesita certificado de servidor.
- PEAP: el protocolo de autenticación extensible protegido es un nuevo miembro de la familia de protocolos de EAP. Se utiliza seguridad de nivel de transporte (TLS) para crear un canal cifrado entre un cliente de autenticación PEAP y un autenticador PEAP. Este proceso tiene lugar en dos etapas: en la primera etapa se configura un canal seguro entre el cliente y el servidor de autenticación. En la segunda se proporciona la autenticación EAP entre el cliente y el autenticador EAP.

El estándar 802.1X utiliza EAP (Extensible Authentication Protocol, Protocolo de Autenticación Extensible) para la autenticación de usuarios. En realidad EAP actúa como intermediario entre un solicitante y un motor de validación (RADIUS) permitiendo la comunicación entre ambos.

El proceso de validación está conformado por tres elementos, un solicitante que

quiere ser validado mediante unas credenciales, un punto de acceso y un sistema de validación situado en la parte cableada de la red. Para conectarse a la red, el solicitante se identifica mediante unas credenciales, junto con las credenciales, el cliente solicitante tiene que añadir también qué sistema de validación tiene que utilizar. En general EAP recibe una solicitud de validación y la remite a otro sistema que sepa cómo resolverla y que formará parte de la red cableada. De esta forma vemos como el sistema EAP permite un cierto tráfico de datos con la red local para permitir la validación de un solicitante. El punto de acceso rechaza todas las tramas que no estén validadas, que provengan de un cliente que no se ha identificado, salvo aquéllas que sean una solicitud de validación. Estos paquetes EAP que circulan por la red local se denominan EAPOL (EAP over LAN). Una vez validado, el punto de acceso admite todo el tráfico del cliente.

El sistema de autenticación será un servidor RADIUS situado en la red local. El proceso de autenticación 802.1X consta de los siguientes pasos:

- El cliente envía un mensaje de inicio EAP que inicia un intercambio de mensajes para permitir autenticar al cliente.
- El punto de acceso responde con un mensaje de solicitud de identidad EAP para solicitar las credenciales del cliente.
- El cliente envía un paquete respuesta EAP que contiene las credenciales de validación y que es remitido al servidor de validación ajeno al punto de acceso.
- El servidor de validación analiza las credenciales y el sistema de validación solicitado y determina si autoriza o no el acceso. En este punto tendrán que coincidir las configuraciones del cliente y del servidor, las credenciales tienen que coincidir con el tipo de datos que espera el servidor.
- El servidor pude aceptar o rechazar la validación y le envía la respuesta al punto de acceso.
- El punto de acceso devuelve un paquete EAP de acceso o de rechazo al cliente.

- Si el servidor de autenticación acepta al cliente, el punto de acceso modifica el estado del puerto de ese cliente como autorizado para permitir las comunicaciones.

4.3 Modelado de la solución, recursos hardware y software.

La infraestructura que se va a instalar depende principalmente de las siguientes soluciones de software libre:

- Ubuntu Server 14.04.4 LTS: Ubuntu es un sistema operativo basado en GNU/Linux y que se distribuye como software libre. La edición Ubuntu Server es una variante de Ubuntu y está enfocada especialmente para su uso en servidores (un servidor es una máquina que nos proporciona algún servicio)**.** El uso de Ubuntu como servidor se ha extendido mucho en los últimos años tanto a nivel particular como profesional.

  El servidor será desplegado en un entorno virtual y en éste se instalarán el resto de componentes.
- FreeRADIUS 2.2.9: RADIUS es un protocolo de seguridad que sigue un modelo cliente/servidor, donde el papel de servidor es desempeñado por RADIUS que contiene o conoce donde está la información de los usuarios y un elemento de red designado como NAS (Network Access Server). NAS se encarga de retransmitir las solicitudes de conexión, autenticación de usuarios y en general toda la información necesaria para el usuario. Los elementos característicos que posee RADIUS le han permitido guardar un alto grado de compatibilidad con la arquitectura dispuesta por las redes inalámbricas IEEE 802.11, según la norma RFC3580 éste es el servidor recomendado para prestar los servicios de autenticación en redes inalámbricas.
- OpenLDAP 2.1. LDAP (Lightweight Directory Access Protocol): este protocolo organiza la información en un modo jerárquico usando directorios que almacenan una gran variedad de información. LDAP soporta la capa de conexión segura (SSL) y la seguridad de la capa de transporte (TLS), por lo que los datos confidenciales se pueden

proteger.

Es un sistema cliente/servidor, donde el servidor puede usar una variedad de bases de datos para guardar un directorio, cada uno optimizado para operaciones de lectura rápida y en gran volumen. Cuando una aplicación cliente LDAP se conecta a un servidor LDAP puede, o bien consultar un directorio, o intentar modificarlo. En el evento de una consulta, el servidor, puede contestarla localmente o puede dirigir la consulta a un servidor LDAP que tenga la respuesta. Si la aplicación cliente está intentando modificar información en un directorio LDAP, el servidor verifica que el usuario tiene permiso para efectuar el cambio y después añade o actualiza la información. Cabe destacar que LDAP define el método para acceder a datos en el servidor a nivel cliente pero no la manera en la que se almacena la información.

Los tres elementos anteriores permitirán implementar una configuración EAP-TTLS la cual resulta más equitativa en relación infraestructura-seguridad:

- Todo el tráfico circula totalmente cifrado, de manera que nos proporciona un sistema seguro de acceso a la red.
- Es un método de autenticación que implementa un sistema de dos túneles de seguridad: uno para el intercambio de credenciales y otro para el traspaso de la clave de cifrado de sesión con la que los puntos de acceso cifran el tráfico con el cliente que se conecta.
- La autenticación se realiza solo con certificados de servidor y no es necesario generar certificados para cada cliente nuevo que desee conectarse a la red.
- A diferencia de otros tipos de EAP, tiene la capacidad de soportar una amplia variedad de métodos de autenticación interna como: Active Directory, Token Systems, SQL y LDAP.
- EAP-TTLS no es vulnerable actualmente a ataques MiTM ni de diccionarios.

Independientemente de los métodos de autenticación que hemos visto en el punto anterior, para la comunicación interna de los servicios es posible usar diferentes protocolos de autenticación: PAP (Protocolo simple de autenticación),

CHAP (Protocolo de autenticación por desafío mutuo) o MSCHAP/MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol).

En la plataforma que se va a implementar debemos usar PAP debido a la compatibilidad que posee con los algoritmos de cifrado de las contraseñas de LDAP [6]. No es recomendable usarlo independiente, pero no existen inconvenientes al usarlo de forma conjunta con EAP-TTLS ya que éste cifra toda la comunicación cliente-servidor haciendo uso de túneles.

Para la virtualización del servidor será necesario un equipo que tenga recursos suficientes para cubrir los requerimientos tanto del sistema anfitrión como los requisitos mínimos del sistema operativo huésped que vayamos a virtualizar. En este caso en particular se hará uso de un Apple iMac 21.5-inch, Mid 2011 que consta de:

- Procesador: 2.5GHz quad-core Intel Core i5
- Memoria: 16GB DDR3.
- Disco Duro: Fusion Drive 750 GB.
- Sistema Operativo: OS X El Capitan.
- Sistema de virtualización: Parallels Desktop 11.

El servidor virtual tendrá los siguientes requisitos hardware:

- Memoria: 2 GB.
- 2 vCPU.
- Disco Duro: 15 GB.
- Sistema Operativo: Ubuntu Server 14.04.4 TLS.
- 1 tarjeta de red.

4.4 Instalación FreeRADIUS

Durante las primeras pruebas de concepto del laboratorio encontré varios bugs que afectaban a la versión que instala por defecto Ubuntu Server 14.04.4. Uno de los más graves era que una vez parado el servicio, éste arrancaba automáticamente bloqueando los puertos de conexión. Por este motivo se han añadido fuentes de actualización al sistema operativo, que permiten actualizar los binarios a una versión más reciente.

Para tener la última versión estable de FreeRADIUS es necesario añadir un repositorio adicional. Debemos editar el fichero /etc/apt/sources.list y agregar las siguientes líneas al final del fichero:

```
## FreeRadius Repository
deb http://ppa.launchpad.net/freeradius/stable/ubuntu trusty main
deb-src http://ppa.launchpad.net/freeradius/stable/ubuntu trusty main
```

Ilustración 66 Repositorios FreeRADIUS

Ahora procedemos a actualizar los repositorios mediante el comando:

sudo apt-get update

Una vez finalizado ejecutamos la instalación de FreeRADIUS:

sudo apt-get install freeRADIUS freeRADIUS-ldap

```
root@SerVer:/home/aglez# sudo apt-get install freeradius freeradius-ldap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  freeradius-common freeradius-utils libdbi-perl libfreeradius2 ssl-cert
Paquetes sugeridos:
  freeradius-postgresql freeradius-mysql freeradius-krb5 libclone-perl
  libmldbm-perl libnet-daemon-perl libplrpc-perl libsql-statement-perl
  openssl-blacklist
Se instalarán los siguientes paquetes NUEVOS:
  freeradius freeradius-common freeradius-ldap freeradius-utils libdbi-perl
  libfreeradius2 ssl-cert
0 actualizados, 7 se instalarán, 0 para eliminar y 2 no actualizados.
Necesito descargar 2.806 kB de archivos.
Se utilizarán 6.998 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Ilustración 67 Instalación de FreeRADIUS

Una vez concluida la instalación el sistema arranca el servicio.

4.5 Instalación OpenLDAP

Para lanzar la instalación del servicio debemos ejecutar el comando:

sudo apt-get install install slapd ldap-utils

```
aglez@SerVer:~$ sudo apt-get install slapd ldap-utils
[sudo] password for aglez:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  libltdl7 libodbc1 libperl5.18 libslp1
Paquetes sugeridos:
  libmyodbc odbc-postgresql tdsodbc unixodbc-bin slpd openslp-doc
Se instalarán los siguientes paquetes NUEVOS:
  ldap-utils libltdl7 libodbc1 libperl5.18 libslp1 slapd
0 actualizados, 6 se instalarán, 0 para eliminar y 0 no actualizados.
Necesito descargar 1.690 kB de archivos.
Se utilizarán 6.073 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Ilustración 68 Instalación de OpenLDAP

El sistema solicitará la contraseña del administrador de LDAP y su correspondiente verificación:

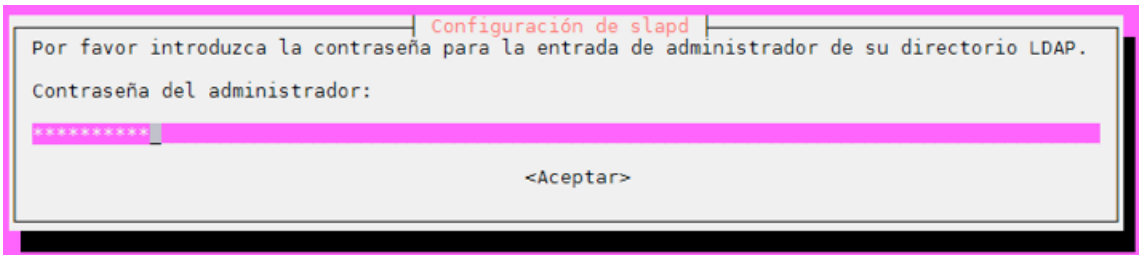

Ilustración 69 Contraseña de administrador

4.6 Configuración FreeRADIUS

Los archivos de configuración se encuentran en el directorio /etc/freeRADIUS/ y dentro es éste hay múltiples ficheros y subdirectorios. A continuación se nombrarán solo aquellos que serán necesarios modificar. Como medida preventiva se hará copia de seguridad de los ficheros originales para poder recuperar el estado inicial en caso de que hubiera algún tipo de error durante la edición de las nuevas versiones:

```
root@SerVer:/etc/freeradius# cp eap.conf eap.conf.BKP
root@SerVer:/etc/freeradius# cp clients.conf clients.conf.BKP
root@SerVer:/etc/freeradius# cp radiusd.conf radiusd.conf.BKP
root@SerVer:/etc/freeradius# cp modules/ldap modules/ldap.BKP
root@SerVer:/etc/freeradius#
```

Ilustración 70 Copia de seguridad

4.6.1 RADIUS.conf:

Este fichero es el principal del servicio y es aquí donde encontraremos muchas especificaciones y directivas del servidor.

Se modificarán las siguientes líneas:

auth = no → yes

auth_badpass = no → yes

auth_goodpass = no → yes

proxy_request = yes → no

$INCLUDE proxy.conf → Se comenta la línea añadiendo "#"

El fichero completo figura en el anexo 1.

4.6.2 Eap.conf

Se utiliza para configurar el tipo de EAP (Extensible Authentication Protocol) a emplear. Se deben definir donde se encuentran los certificados del servidor y de la autoridad de certificación (CA). Pero antes de definirlos es necesario crearlos, para ello se hará uso de un método automatizado, que provee FreeRADIUS, para obtener los certificados necesarios.

El primer paso es ubicarse en la ruta /usr/share/doc/freeRADIUS/examples/certs que es donde se encuentran los siguientes archivos:

```
root@SerVer:/usr/share/doc/freeradius/examples/certs# ls
bootstrap  ca.cnf  client.cnf  Makefile  README  server.cnf  xpextensions
root@SerVer:/usr/share/doc/freeradius/examples/certs#
```

Ilustración 71 Configuración de la CA

Editamos los siguientes campos del fichero ca.cnf para configurar la entidad certificadora:

```
[certificate_authority]
countryName             = ES
stateOrProvinceName     = CANARIAS
localityName            = Tenerife
organizationName        = my-lab
emailAddress            = admin@uoc.lab
commonName              = "Certificate Authority"
```

Ilustración 72 Entidad certificadora

Es recomendable cambiar la contraseña que viene por defecto:

```
[ req ]
prompt                  = no
distinguished_name      = certificate_authority
default_bits            = 2048
input_password          = whatever
output_password         = whatever
x509_extensions         = v3_ca
```

Ilustración 73 Contraseña de la CA

Ahora editamos solo los campos que salen en la imagen del fichero server.cnf para configurar los parámetros del certificado del servidor:

```
[server]
countryName             = ES
stateOrProvinceName     = CANARIAS
localityName            = TENERIFE
organizationName        = my-lab
emailAddress            = admin@uoc.lab
commonName              = "Server Certificate"
```

Ilustración 74 Certificado de servidor

En el caso de querer generar certificados de cliente, se debe editar el fichero client.cnf. Cabe destacar que esta parte es opcional y que en el caso que nos ocupa no serán necesarios.

Para crear los certificados ejecutamos el script bootstrap:

./bootstrap

```
Generating a 2048 bit RSA private key
.....................................................................
.....................+++
writing new private key to 'ca.key'
-----
Using configuration from ./server.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Apr 26 21:56:25 2016 GMT
            Not After : Apr 26 21:56:25 2017 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = CANARIAS
            organizationName          = my-lab
            commonName                = Server Certificate
            emailAddress              = admin@uoc.lab
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://www.example.com/example_ca.crl

Certificate is to be certified until Apr 26 21:56:25 2017 GMT (365 days)
```

Ilustración 75 Generación del certificado

En la siguiente imagen se ven los ficheros que se han generado:

```
root@SerVer:/usr/share/doc/freeradius/examples/certs# ls
01.pem     ca.cnf  ca.pem      client.csr  index.txt          index.txt.old  README      server.cnf  server.key  xpextensions
02.pem     ca.der  client.cnf  client.key  index.txt.attr     Makefile       serial      server.crt  server.p12
bootstrap  ca.key  client.crt  dh          index.txt.attr.old  random         serial.old  server.csr  server.pem
root@SerVer:/usr/share/doc/freeradius/examples/certs#
```

Ilustración 76 Certificados necesarios

Nos cambiamos a la carpeta /etc/freeRADIUS/certs y eliminamos los enlaces simbólicos que hay en este directorio:

```
root@SerVer:/etc/freeradius/certs# ls -l
total 4
lrwxrwxrwx 1 root freerad  34 abr 26 21:55 ca.pem -> /etc/ssl/certs/ca-certificates.crt
-rw-r--r-- 1 root freerad 245 abr 26 21:55 dh
lrwxrwxrwx 1 root freerad  38 abr 26 21:55 server.key -> /etc/ssl/private/ssl-cert-snakeoil.key
lrwxrwxrwx 1 root freerad  36 abr 26 21:55 server.pem -> /etc/ssl/certs/ssl-cert-snakeoil.pem
root@SerVer:/etc/freeradius/certs# rm ca.pem
root@SerVer:/etc/freeradius/certs# rm dh server.*
```

Ilustración 77 Certificados por defecto

Copiamos los certificados que se acaban de generar:

```
root@SerVer:/etc/freeradius/certs# cp /usr/share/doc/freeradius/examples/certs/ca.pem .
root@SerVer:/etc/freeradius/certs# cp /usr/share/doc/freeradius/examples/certs/dh .
root@SerVer:/etc/freeradius/certs# cp /usr/share/doc/freeradius/examples/certs/random .
root@SerVer:/etc/freeradius/certs# cp /usr/share/doc/freeradius/examples/certs/server.pem .
root@SerVer:/etc/freeradius/certs# cp /usr/share/doc/freeradius/examples/certs/server.key .
root@SerVer:/etc/freeradius/certs# ls -l
total 24
-rw-r----- 1 root freerad 1684 abr 26 23:00 ca.pem
-rw-r----- 1 root freerad  245 abr 26 23:00 dh
-rw-r----- 1 root freerad 5120 abr 26 23:00 random
-rw-r----- 1 root freerad 1834 abr 26 23:00 server.key
-rw-r----- 1 root freerad 3581 abr 26 23:00 server.pem
```

Ilustración 78 Certificados definitivos

Ya estamos en disposición de editar el fichero eap.conf para añadir las rutas de los certificados:

certdir = /etc/freeRADIUS/certs

cadir = /etc/freeRADIUS/certs/random

private_key_password = misecreto

private_key_file = /etc/freeRADIUS/certs/server.key

certificate_file = /etc/freeRADIUS/certs/server.pem

CA_file = /etc/freeRADIUS/certs/ca.pem

dh_file = /etc/freeRADIUS/certs/dh

random_file = /etc/freeRADIUS/certs/random

El fichero completo figura en el anexo 2.

4.6.3 Clients.conf

Este fichero contiene la lista de clientes que están autorizados para usar los servicios de AAA (Authentication, Authorization and Accounting). En este fichero introduciremos el punto de acceso y el propio servidor RADIUS de esta forma podremos hacer una comprobación del servicio:

client 192.168.1.250 { # Direccion IP del cliente

secret = 12345678Ab # Contraseña compartida entre cliente y servidor

shortname = APCiscoLAB # Nombre identificatico }

El fichero completo figura en el anexo 3.

4.6.4 Módulos LDAP

En el directorio modules se encuentran los diferentes módulos que puede usar este servidor. Solo será necesario modificar el fichero ldap.

La conexión entre el servicio de RADIUS y LDAP puede ser tanto cifrada como sin cifrar, en este caso se ha implementado sin cifrar ya que la comunicación no sale del servidor, pero en caso de usar un servicio de directorio ubicado en otro servidor sí que debe ir cifrada.

Editamos los siguientes campos del fichero ldap:

Server = debe ir la direccion IP o el nombre de dominio del servidor.

Identity = Usuario con privilegios en el LDAP y dominio de busqueda.

Password = Password de este usuario (de conexion al LDAP).

Basedn = Definimos la rama base de busquedas (donde buscar en el LDAP).

Filter = Se define la busqueda LDAP. De esta forma solo los usuario con la objectclass RADIUSprofile podrán conectarse a la Wi-Fi.

El fichero completo figura en el anexo 4.

4.6.5 Sites-available y sites-enabled

Para concluir nos centraremos en las rutas sites-available y sites-enabled. El primer directorio es donde se encuentran los sitios habilitados, también denominados servidores virtuales, mientras que el segundo es donde estarán los

enlaces a los sitios que están activos o dicho de otra forma los sites que darán servicios.

En la primera ruta nos encontraremos con el sitio denominado “default” (servidor que viene por defecto) el cual usaremos de plantilla para crear un nuevo servidor virtual al que llamaremos UOC.

cp /etc/freeRADIUS/sites-availables/default /etc/freeRADIUS/sites-availables/UOC

Editamos el fichero para establecer la configuración que aparece en el anexo 5.

vi /etc/freeRADIUS/sitesavailables/UOC

Para activar el servidor que queremos tener en uso (UOC), tendremos que situarnos en la segunda ruta indicada anteriormente (/etc/freeRADIUS/sites-enabled/) y crear un enlace.

ln -s /etc/freeRADIUS/sites-availables/UOC /etc/freeRADIUS/sites-enabled/UOC

Dado que solo vamos a tener un servidor activo, borraremos el resto de enlaces que figuran el sites-enabled:

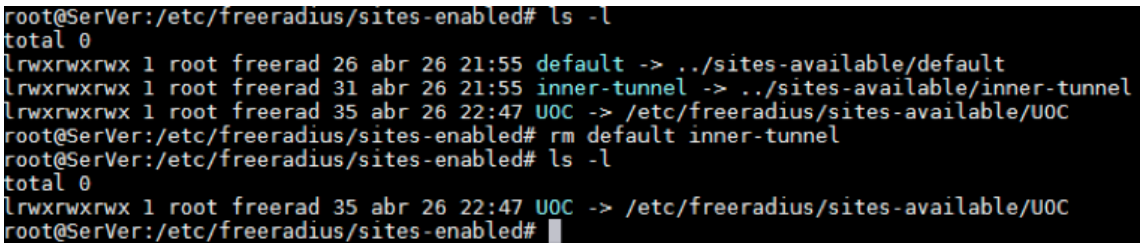

Ilustración 79 Sites activos

4.7 Configuración OpenLDAP

Para empezar configuramos LDAP, introduciendo el siguiente comando:

#dpkg-reconfigure slapd:

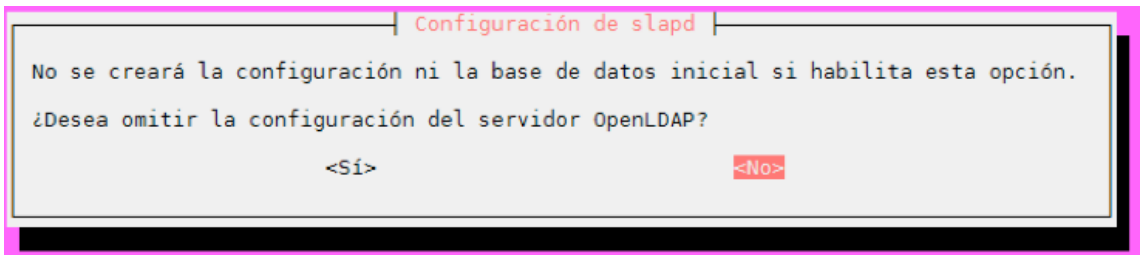

Ilustración 80 Omitir configuración

Seleccionamos que *No* queremos omitir la configuración como vemos en la captura superior:

Le indicamos nombre del dominio: uoc.lab:

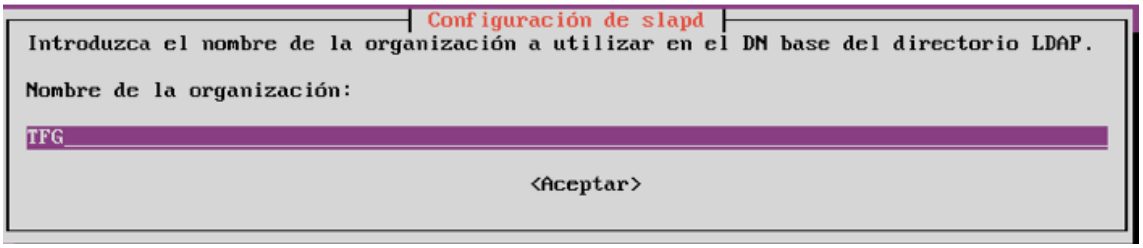

Ilustración 81 Nombre de la organización

Le indicamos el nombre de la organización (TFG) y le facilitamos la contraseña de administrador de LDAP junto con la verificación.

Seleccionamos el motor de base de datos BDB:

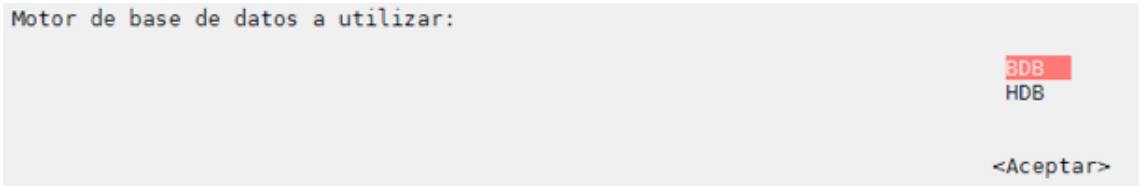

Ilustración 82 Motor de la base de datos

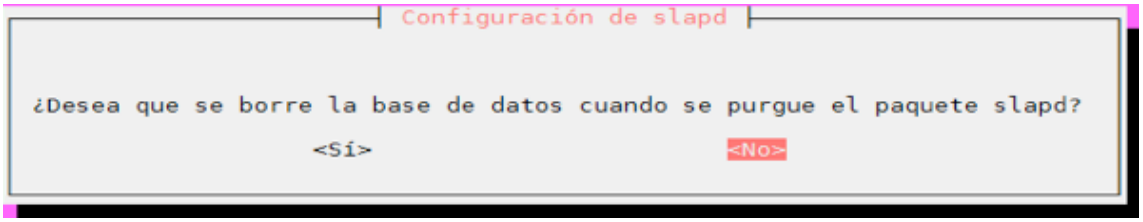

Ilustración 83 Borrado de la base de datos

Seleccionamos que *No* borre la base de datos si se purga el paquete slapd, que *Si* mueva los ficheros ya creados y elegimos que no deseamos ldapv2.

El proceso de configuración realiza los cambios y reinicia el servicio:

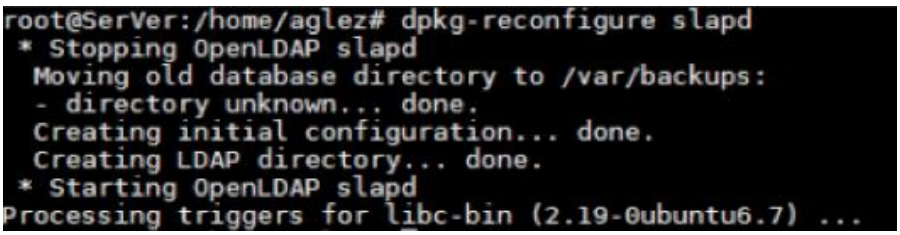

Ilustración 84 Finalización de la reconfiguración

4.7.1 Ampliación del esquema.

Es necesario ampliar el esquema del LDAP (contiene la definición de los objetos que pueden formar parte del directorio) para que el servicio OpenLDAP reconozca los atributos dialupAccess y RADIUSGroupName con su correspondiente objectclass RADIUSprofile.

Para disponer del esquema, tenemos que copiar el fichero openldap.schema ubicado en la ruta /usr/share/doc/freeRADIUS/examples/ a la carpeta /etc/ldap/schema/ con el nombre RADIUS.schema:

```
aglez# cp /usr/share/doc/freeradius/examples/openldap.schema /etc/ldap/schema/radius.schema
aglez# ls -l /etc/ldap/schema/ | grep radius
root 14694 abr 26 22:22 radius.schema
```

Ilustración 85 Copia del esquema

Ahora creamos el archivo schema.conf con el siguiente contenido:

```
root@SerVer:/home/aglez# vi schema.conf
root@SerVer:/home/aglez# cat schema.conf
include /etc/ldap/schema/radius.schema
```

Ilustración 86 schema.conf

Lo siguiente a realizar es la creación de un directorio (denominado salida) y ejecutamos el comando:

slapcat -f schema.conf -F salida -n0 –H ldap:///cn={0}RADIUS,cn=schema,cn=config -l cn=RADIUS.ldif

Obtendremos la salida que se ven en la siguiente imagen:

```
aglez# slapcat -f schema.conf -F salida -n0 -H ldap:///cn={0}radius,cn=schema,cn=config -l cn=radius.ldif
aglez# ls
blar.ldif  salida  schema.conf
aglez# ls -l salida/

root 4096 abr 26 22:26 cn=config
root  928 abr 26 22:26 cn=config.ldif
```

Ilustración 87 Salida del comando slapcat

Editamos el fichero cn=RADIUS.ldif y modificando las siguientes líneas:

dn: cn={0}RADIUS,cn=schema,cn=config

objectClass: olcSchemaConfig

cn: {0}RADIUS

Para que queden de la siguiente forma:

dn: cn=RADIUS,cn=schema,cn=config

objectClass: olcSchemaConfig

cn: RADIUS

Para concluir, con la modificación de este fichero, eliminamos las siguientes líneas:

```
structuralObjectClass: olcSchemaConfig
entryUUID: 490bbfac-a041-1035-90a1-3957da24be65
creatorsName: cn=config
createTimestamp: 20160426212629Z
entryCSN: 20160426212629.948039Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20160426212629Z
```

Ilustración 88 Líneas a eliminar

Por último cargamos el esquema en el sistema con el comando:

ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn\=RADIUS.ldif

Con la siguiente búsqueda en el LDAP se verifica que ya está disponible la nueva objectclass:

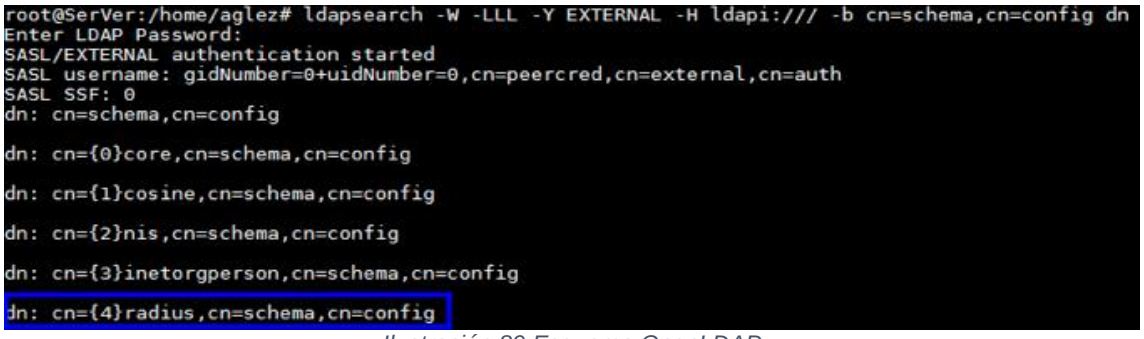

Ilustración 89 Esquema OpenLDAP

Aunque la documentación de OpenLDAP no lo indica, hasta que no se reinician los servicios no es posible añadir el RADIUSProfile a los usuarios:

service slapd restart

También se reinicia el servicio RADIUS para aplicar los cambios hechos en el punto anterior:

service freeRADIUS restart

4.8 Alta de usuarios.

Una vez tenemos nuestro directorio creado y configurado es necesario dar de alta los usuarios que podrán conectar a la red Wi-Fi. Aunque esta tarea se puede hacer de forma manual, se ha creado el fichero poblar.dif (anexo 6) el cual crea una estructura compuesta de 3 grupos, 2 unidades organizativas (OU) y 2 usuarios. Cabe destacar que bastaría con crear solo los usuario y una OU para tener un directorio jerarquizando.

Ejecutamos el siguiente comando:

ldapadd -x -D cn=admin,dc=uoc,dc=lab -W -f base.ldif”

Donde:

- x: desconecta la autenticación con SASL (capa de seguridad y autenticación simple).
- D: indica el usuario que llama a la operación.
- W: evita tener que introducir la contraseña en la línea de comando (en texto no cifrado) y activa un indicador de contraseña aparte.
- f: nombre del archivo a importar.

Una vez introducida la contraseña, el sistema muestra por pantalla que se han añadido las entradas correctamente:

```
root@SerVer:/home/aglez# ldapadd -x -D "cn=admin,dc=uoc,dc=lab" -W -f poblar.ldif
Enter LDAP Password:
adding new entry "ou=UsuariosWiFi,dc=uoc,dc=lab"

adding new entry "ou=Grupos,dc=uoc,dc=lab"

adding new entry "ou=Equipos,dc=uoc,dc=lab"

adding new entry "cn=empleados,ou=Grupos,dc=uoc,dc=lab"

adding new entry "cn=directivos,ou=Grupos,dc=uoc,dc=lab"

adding new entry "uid=alejandro,ou=UsuariosWiFi,dc=uoc,dc=lab"

adding new entry "uid=alfonso,ou=UsuariosWiFi,dc=uoc,dc=lab"
```

Ilustración 90 Alta de usuarios

Con el uso de una herramienta gráfica se puede ver de forma más amigable el resultado del comando anterior:

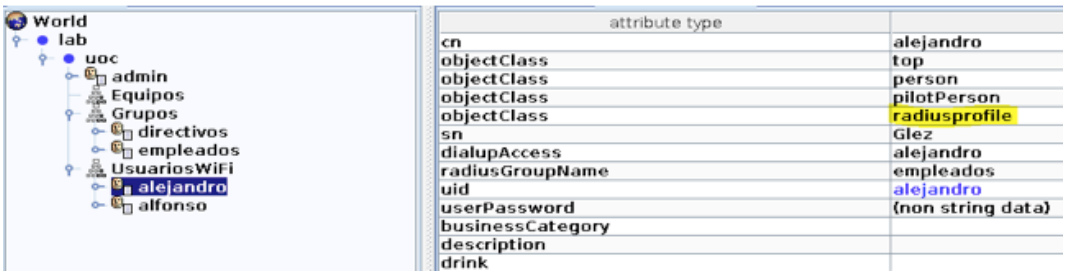

Ilustración 91 JXplorer

4.9 Verificación de los servicios

Dado que se trabaja con muchos ficheros en FreeRADIUS se puede dar el caso de que el servicio no arranque. Para detectar el error o errores que lo causan es posible arrancar el servicio en modo depuración (debug) con el comando freeRADIUS -X.

Si en la pantalla de depuración del servidor aparece *Ready to process requests*, esto indica que está ejecutándose adecuadamente:

```
radiusd: #### Opening IP addresses and Ports ####
listen {
        type = "auth"
        ipaddr = *
        port = 0
}
listen {
        type = "acct"
        ipaddr = *
        port = 0
}
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Ready to process requests.
```

Ilustración 92 Debug

Para verificar el funcionamiento del servicio se emplea el comando radtest*:*

radtest alejandro 123456 localhost 0 aglez

- alejandro: nombre del usuario
- 123456: contraseña
- localhost: IP o nombre del servidor

- 0: Nas-Port. Según la documentación no es importante lo que se ponga aquí.
- aglez: password compartido entre RADIUS y punto de acceso que se ha configurado en el fichero clients.conf.

Si los datos introducidos son correctos el sistema muestra lo siguiente:

```
aglez@SerVer:~$ radtest alejandro 123456 localhost 0 aglez
Sending Access-Request of id 188 to 127.0.0.1 port 1812
        User-Name = "alejandro"
        User-Password = "123456"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=188, length=20
```

Ilustración 93 Test correcto

En caso contrario se retornará:

```
rad_recv: Access-Request packet from host 127.0.0.1 port 55214, id=35, length=79
Received packet from 127.0.0.1 with invalid Message-Authenticator!  (Shared secret is incorrect.)
```

Ilustración 94 Test fallido

4.10 Configuración del punto de acceso

Para configurar WPA2 Enterprise, será necesario acceder a la sección de seguridad del router y cambiar el modo de seguridad:

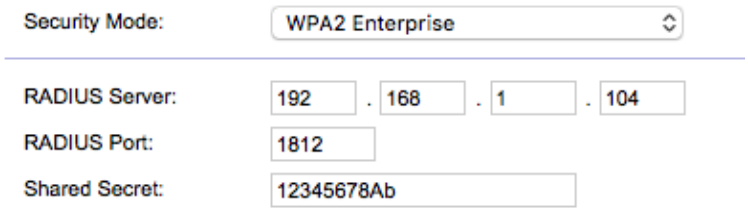

Ilustración 95 Configuración del AP

Debemos introducir la IP del servidor RADIUS, el puerto de conexión (por defecto 1812) y la contraseña que se ha establecido en el fichero clients.conf.

4.11 Configuración de cliente

EAP-TTLS/PAP está soportado de forma nativa por todos los sistemas operativos excepto por Windows 7 y versiones inferiores, el cual requeriría de un software cliente que le habilite establecer la conexión con este modo de autenticación. SecureW2 es uno de los más extendidos.

A modo de ejemplo se va a proceder a configurar un dispositivo Android. Una vez seleccionada la red (UOC_LAB) el termina mostrará los diferente métodos EAP. Rellenamos los campos y se establece la conexión:

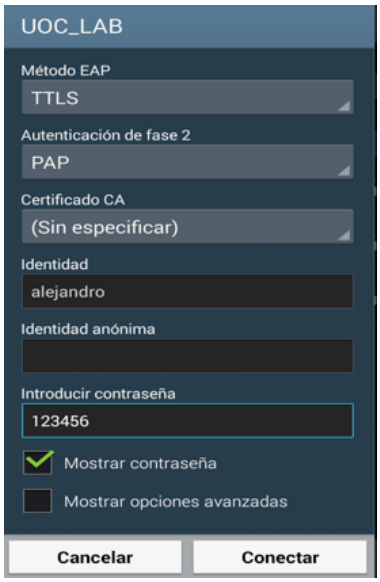

Ilustración 96 Configuración Android

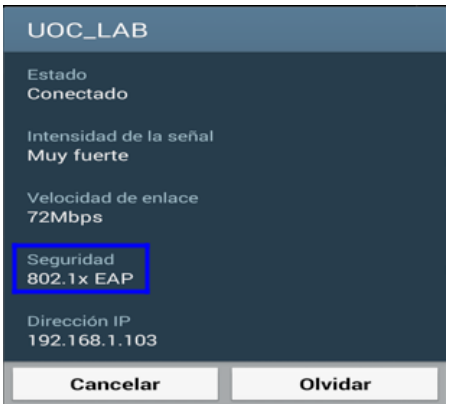

Ilustración 97 Detalle de la conexión

Accedemos al log de RADIUS para ver cómo una vez se ha validado el usuario y contraseña se concede el acceso:

```
Mon May  2 09:44:23 2016 : Auth: Login OK: [alejandro/123456] (from client APCiscoLAB port 0 via TLS
 tunnel)
Mon May  2 09:44:23 2016 : Auth: Login OK: [alejandro/<via Auth-Type = EAP>] (from client APCiscoLAB
 port 29 cli 88329b077b61)
```

Ilustración 98 Log RADIUS

4.12 Conexión cifrada

Una vez montada la infraestructura se ha de confirmar que efectivamente toda la comunicación está cifrada. Para ello se ha analizado la red con la ayuda de un sniffer.

La IP origen (192.168.1.250) corresponde al punto de acceso y la IP destino (192.168.1.104) al servidor FreeRADIUS. RADIUS establece un túnel cifrado por el que viajan todas las contraseñas. Observamos que el único dato que circula sin cifrar es el nombre de usuario *alejandro*:

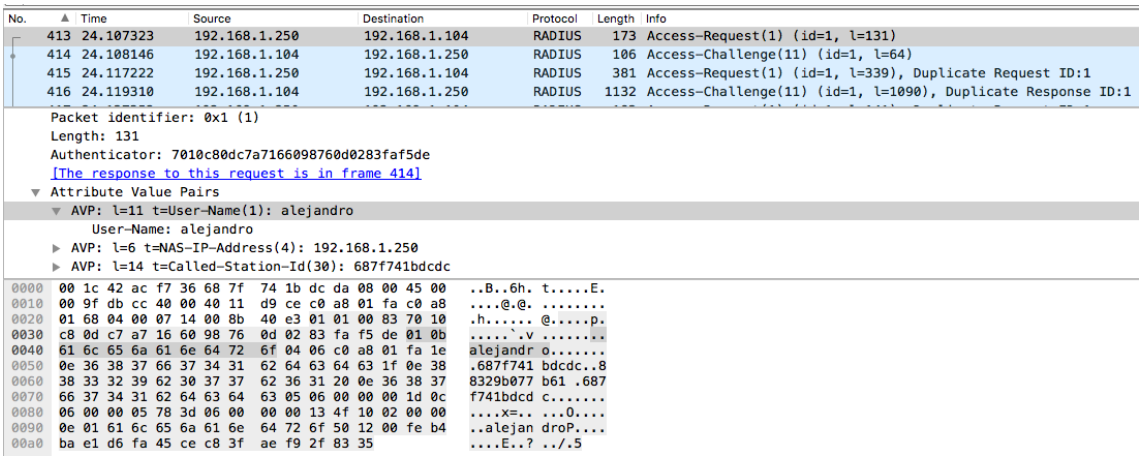

Ilustración 99 Tráfico de red RADIUS

De esta forma se verifica que aunque el método de autenticación que usa internamente sea PAP (sin cifrar) no afecta debido a que FreeRADIUS establece túneles cifrados entre cliente y servidor gracias al método EAP-TTLS aportando a la red un alto nivel de seguridad.

El mensaje *Access-Accept* indica que la autenticación ha sido realizada correctamente:

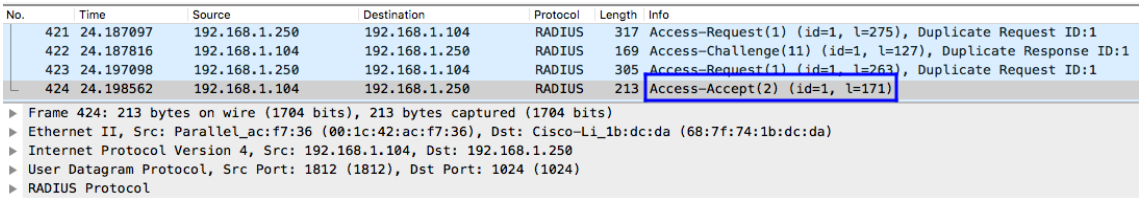

Ilustración 100 Captura de red del proceso de conexión WPA2

La siguiente imagen es simplemente para ejemplificar lo que se produce cuando se inicia la comunicación entre el dispositivo ANDROID y el AP. Se puede observar el *Client Hello*, el *Server Hello* y el intercambio de claves. Toda esa comunicación va en claro, pero en cuanto empiezan a enviarse los datos, éstos son cifrados mediante TLS:

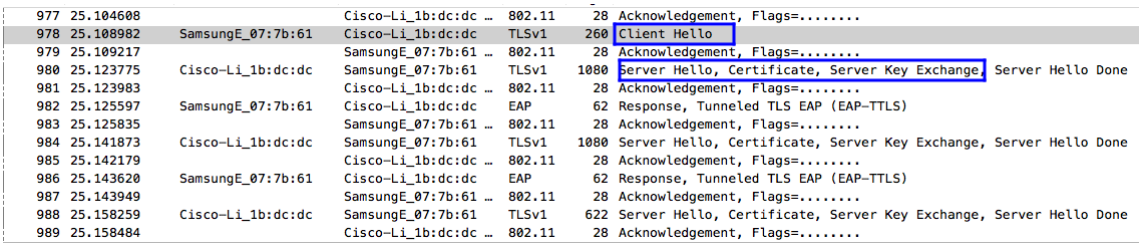

Ilustración 101 Establecimiento de conexión

4.13 Conclusiones

A la vista de los puntos anteriores queda de manifiesto que asegurar una red

inalámbrica no es algo trivial, es un proceso que implica la utilización de software y hardware que tiene que ser instalado y configurado por personal cualificado. Debido a esto, la implementación de esta solución se debe hacer cuando se desea tener una red Wi-Fi totalmente segura sabiendo en cada momento qué usuarios tienen acceso.

5. Recomendaciones de seguridad

En este capítulo se darán una serie de consejos que ayudarán al lector a proteger una red inalámbrica con un alto grado de seguridad, si bien puede resultar un poco engorroso y conlleva una revisión periódica, no hay que olvidar que de la misma forma que se contratan sistemas de alarmas para evitar o incluso disuadir a posibles intrusos ocurre exactamente lo mismo con las redes Wi-Fi.

5.1 Seguridad en la configuración de tu router WiFi

- Actualiza el firmware de tu AP: de la misma forma que ocurre con los sistemas operativos, los router y puntos de acceso también tienen disponibles actualizaciones que corrigen errores y/o añaden nuevas funcionalidades. Se debe buscar en la web del fabricante y poner el último firmware que haya disponible el dispositivo.
- Credenciales de acceso: las contraseñas por defecto son un grave problema en estos dispositivos, por lo que es necesario cambiarla cuanto antes. Es recomendable implementar para mayor seguridad una contraseña alfanumérica.

5.2 Seguridad en la configuración de la Wi-Fi

- Activa el filtrado de direcciones MAC. Activa en el AP el filtrado de direcciones MAC de los dispositivos Wi-Fi que actualmente están funcionando. Al activar el filtrado MAC dejarás que sólo los dispositivos con las direcciones MAC especificadas se conecten a la red wireless.
- Establece el número máximo de dispositivos que pueden conectarse.
- Cambia el SSID por defecto. Es recomendable no llamar la atención de un posible observador para aumentar las probabilidades de que éste no

intente entrar en la red. En vez de denominarlo como "MiAP", "Casa" o el nombre de la empresa, es preferible escoger algo menos atractivo como puede ser "Broken", "Down" o "Desconectado". El cambio periódico del nombre de la red evita que la red puede figurar en base de datos wardriving.

- Oculta el SSID: Al ocultar el SSID de la red, el punto de acceso Wi-Fi no emite los beacon frames con el nombre de la red. Ocultarlo hace que el atacante tenga más trabajo a la hora de descubrir los Probe de los clientes que se conectan.

- Establece cifrado WPA/WPA2 – PSK. Es el sistema más robusto que hay hoy en día, aunque ya ha quedado patente en el punto 4 que no es ni mucho menos infalible ya que existen formas de atacar una red con WPA/WPA2-PSK, pero en la actualidad es la mejor opción, a nivel doméstico, que se puede utilizar.

- Cambia la clave periódicamente. El cifrado WPA/WPA2 - PSK también puede ser atacado una vez descubierto los algoritmos que usaron los fabricantes para establecer claves por defecto.

- No usar cifrado WEP. No debes usar WEP para proteger una red inalámbrica si existe alternativa. Su protección es demasiado débil ya que se puede obtener la clave en pocos minutos usando las herramientas que no requieren de conocimientos avanzados.
  En caso de solo disponer de cifrado WEP se deben generar las contraseña de 128 o 256 bits y cambiarla regularmente.

- Desactivar WPS. Esta característica permite que un equipo se conecte a la una red Wi-Fi utilizando un código temporal que simplifica todo el proceso de enrollment de un nuevo equipo. Dado que muchas de las implementaciones en los routers no detectan los ataques de fuerza bruta, en unos minutos la red queda expuesta.

5.3 Monitorización de la red Wi-Fi.

- Con el fin de descubrir posibles intrusos en la red, se deben revisar los logs del router o punto de acceso Wi-Fi. En los logs aparecerán las

direcciones MAC y las direcciones IP de conexión a la red, la cuales pueden revelar (si está activado filtrado de MAC) si existen varios equipos con distinta dirección IP sobre la misma dirección MAC. Si no está activo el filtrado, el atacante usará una dirección MAC falsa y tendrá otra dirección IP para no generar alertas de seguridad, pero será más fácil darse cuenta de que hay un nuevo equipo en la red.

- El uso de herramientas como Satori, realizan un escaneo pasivo de la red y detecta los equipos que hay en ella por medio de las direcciones IPv4, IPv6 y direcciones físicas MAC que se usan en la red. Escanea el tráfico periódicamente de forma silenciosa con el objetivo de detectar algún dispositivo no deseado.

6. Conclusiones

Tal y como se ha visto en este proyecto las redes inalámbricas Wi-Fi no pueden ser consideradas totalmente seguras. Si bien, esta tecnología permite modificar las configuraciones de seguridad, su mayor problema reside en que todos sus protocolos presentan debilidades que son explotadas por parte de hackers para intentar vulnerarlas.

Al elegir este proyecto mi objetivo, desde el principio, fue el de verificar por mí mismo si realmente era complicado o no acceder a una red Wi-Fi sin permiso. Realmente me ha sorprendido mucho comprobar que no ha sido complicado, si bien en la planificación inicial del proyecto se establecieron entre 8 y 10 días para realizar los diferentes tipos de ataques, esto tan solo me llevó la mitad del tiempo programado.

Por otro lado me ha resultado muy interesante entender los fundamentos teóricos que hay debajo de las herramientas que se han usado para llevar a cabo el ataque y como lo investigadores han encontrado dichas debilidades tras realizar estudios muy detallados del protocolo de seguridad.

En la segunda parte del proyecto he planteado la instalación de un servidor RADIUS, un componente que dota a la seguridad Wi-Fi, a día de hoy, de una fiabilidad del cien por cien. Y es en este punto donde más dificultad he

encontrado. Por un lado el software FreeRADIUS posee multitud de ficheros de configuración y por otro me he tenido que familiarizar con OpenLDAP que al igual que ocurre con el software anterior tiene muchos parámetros de configuración y aparte usa un lenguaje específico para añadir y modificar valores. Aun así tan solo fue necesario invertir 1 día más de lo planificado.

Finalmente se han conseguido todos los objetivos que se habían planteado. Aunque en un principio solo se iba a realizar la parte práctica aportando los resultados, tal y como se ha comentado al principio, se ha añadido el fundamento técnico que está detrás de la herramienta, aportado mayor valor al documento. Una vez más fue necesario adaptar la programación, para ello se utilizó el tiempo que se había ganado al terminar antes de tiempo el punto 3.

Las líneas futuras del estudio pasarían por la implementación de un portal cautivo. Un portal cautivo es un software que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página web especial si quieren navegar por Internet de forma normal. Dicho programa intercepta todo el tráfico de navegación hasta que el usuario se autentifica. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo. Adicionalmente puede empezar a controlar el ancho de banda usado por cada cliente.

7. Glosario

AES	Advanced Encryption Standard
AP	Access Point
BSS	Bassic Service Set
CA	Certificate Authority
CHAP	Challenge Handshake Authentication Protocol
DdoS	Distributed Denial of Service
DoS	Denial of Service
EAP	Extensible Authentication Protocol
ESSID	Extended Service Set Identifier
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IV	Initialization Vector

KSA	Key Scheduling Algorithm
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MIC	Message Integrity Code
MiTM	Man-in-The-Middle
MSCHAP	Challenge-Handshake Authentication Protocol
NACK	Negative-acknowledge
PAP	Password Authentication Protocol
PBKDF2	Password-Based Key Derivation Function 2
PEAP	Protected Extensible Authentication Protocol
PMK	Pairwise Master Key
PRGA	Pseudo Random Generation Algorithm
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
RADIUS	Remote Authentication Dial-In User Service
SASL	Simple Authentication and Security Layer
SNAP	Subnetwork Access Protocol
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WIFI	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

8. Bibliografía

8.1 Libros

Miller, Stewart. (2003). Wi-Fi Security. McGraw-Hill Professional

Reid, Neil P. (2003). Manual de redes inalámbricas. McGraw-Hill

Arboledas Brihuega, David. (2013) Backtrack 5. Hacking de redes inalámbricas. RA-MA

8.2 Páginas web

Wikipedia (02/03/2016) https://es.wikipedia.org/wiki/IEEE_802.11

Wikipedia (05/05/2016) https://es.wikipedia.org/wiki/Wifi

Alonso, Chema (01/08/2008) http://www.elladodelmal.com/2008/08/atacar-wpawpa2-psk-parte-i-de-iv.html

Ellingwood, Justin (1/10/2013) https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-a-basic-ldap-server-on-an-ubuntu-12-04-vps

Hruska, Thomas (07/04/2013) http://cubicspot.blogspot.com.es/2013/04/setting-up-wpa2-enterprise-aes-with.html

wifislax (02/08/2013) http://www.wifislax.com/guia-basica/

Panda Software Internacional (2005) https://www.scribd.com/doc/40278796/Seguridad-en-Redes-Inalambricas

Reaver Open Source (23/01/2012) https://code.google.com/archive/p/reaver-wps/wikis/README.wiki

López, Roberto (24/08/2013) http://highsec.es/hacking-wifi-tutorial/

[6] DeKok, Alan T. (2014) http://deployingradius.com/documents/protocols/oracles.html

8.3 Artículos

[1] Symantec, Symantec Internet Security Threat Report Volume 21. (04/2016). https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[2] Symantec, Symantec Internet Security Threat Report Volume 17. (04/2012). http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

[3] Checkpoint, ChekPoint Inside Nuclear's Core : Analyzing the Nuclear Exploit Kit Infrastructure – Part I. (20/04/2016). http://blog.checkpoint.com/wp-content/uploads/2016/04/Inside-Nuclear-1-2.pdf

[4] Fluhrer, S., Mantin, I., and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", Selected Areas of Cryptography: SAC 2001

[5] Paul Arana, Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2). (10/2006). http://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf

9. Anexos

9.1 Anexo1 - radiusd.conf

```
##  RADIUS.conf
prefix = /usr
exec_prefix = /usr
sysconfdir = /etc
localstatedir = /var
sbindir = ${exec_prefix}/sbin
logdir = /var/log/freeRADIUS
raddbdir = /etc/freeRADIUS
radacctdir = ${logdir}/radacct
on.
name = freeRADIUS
confdir = ${raddbdir}
run_dir = ${localstatedir}/run/${name}
db_dir = ${raddbdir}
libdir = /usr/lib/freeRADIUS
pidfile = ${run_dir}/${name}.pid
user = freerad
group = freerad
max_request_time = 30
cleanup_delay = 5
max_requests = 1024

listen {

        type = auth
        ipaddr = *
        port = 0
        clients = per_socket_clients
}

listen {
        ipaddr = *

        port = 0
        type = acct
}

hostname_lookups = no
allow_core_dumps = no
regular_expressions    = yes
extended_expressions= yes
log {

        destination = files
        file = ${logdir}/radius.log
        syslog_facility = daemon
```

```
        stripped_names = no
        auth = yes
        auth_badpass = yes
        auth_goodpass = yes
        msg_badpass = ""
}

checkrad = ${sbindir}/checkra

security {
        max_attributes = 200
        reject_delay = 1
        status_server = yes
}

proxy_requests  = no

$INCLUDE clients.conf
thread pool {

        start_servers = 5
        max_servers = 32
        min_spare_servers = 3
        max_spare_servers = 10
        max_requests_per_server = 0
}

modules {

        $INCLUDE ${confdir}/mods-enabled/
        $INCLUDE eap.conf
}


instantiate {

        exec
        expr
        expiration
        logintime
}

$INCLUDE policy.conf
$INCLUDE sites-enabled/
```

9.2 Anexo 2 - eap.conf

```
## eap.conf
eap {

                default_eap_type = ttls
```

```
        timer_expire     = 60
        ignore_unknown_eap_types = no
        max_sessions = ${max_requests}
        tls {

                certdir = /etc/freeRADIUS/certs
                cadir = /etc/freeRADIUS/certs/random
                private_key_password = misecreto
                private_key_file = /etc/freeRADIUS/certs/server.key
                certificate_file = /etc/freeRADIUS/certs/server.pem
                CA_file = /etc/freeRADIUS/certs/ca.pem
                dh_file = /etc/freeRADIUS/certs/dh
                random_file = /etc/freeRADIUS/certs/random
                cipher_list = "DEFAULT"
                cache {

                    enable = no
                    lifetime = 24 # hours
                    max_entries = 255
                }
        }


        ttls {

                default_eap_type = tls
                copy_request_to_tunnel = no
                use_tunneled_reply = no
                include_length = yes
        }


}
```

9.3 Anexo 3 - clients.conf

```
## clients.conf
client localhost {
        ipaddr = 127.0.0.1
        secret = aglez
        require_message_authenticator = no
        nastype     = other      # localhost isn't usually a NAS...
}


client 192.168.1.250 {
        secret          = 12345678Ab
        shortname       = APCiscoLAB
}
```

9.4 Anexo 4 - ldap

```
ldap {

        server = "localhost"
        identity = "cn=admin,dc=uoc,dc=lab"
        password = 1q2w3e4r5T
        basedn = "ou=empleados,dc=uoc,dc=lab"
        filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
        base_filter = "(objectclass=RADIUSprofile)"
        ldap_connections_number = 5
        max_uses = 0
        timeout = 4
        timelimit = 3
        net_timeout = 1

        tls {

                start_tls = no
        }

        dictionary_mapping = ${confdir}/ldap.attrmap
        edir_account_policy_check = no
        keepalive {

                idle = 60
                probes = 3
                interval = 3
        }
}
```

9.5 Anexo 5 - UOC

```
authorize {
        preprocess
        auth_log
        chap
        mschap
        digest
        suffix
        eap {
                ok = return
        }
        files
        ldap
        expiration
        logintime
        pap
}
```

```
        authenticate {
                Auth-Type LDAP {
                ldap
                }
        eap
        }


        preacct {
                preprocess
                acct_unique
                suffix
                files
        }


        accounting {
                detail
                unix
                radutmp
                attr_filter.accounting_response
        }


        session {
                radutmp
        }


        post-auth {
                exec
                Post-Auth-Type REJECT {
                        attr_filter.access_reject
                }
        }

        pre-proxy {
        }

        post-proxy {
        }
```

9.6 Anexo 6 - poblar.ldif

```
#poblar.ldif
dn: ou=Usuarios,dc=uoc,dc=lab
ou: Usuarios
objectclass: top
```

```
objectClass: organizationalUnit

dn: ou=Grupos,dc=uoc,dc=lab
ou: Grupos
objectclass: top
objectClass: organizationalUnit

dn: ou=Equipos,dc=uoc,dc=lab
ou: Equipos
objectclass: top
objectClass: organizationalUnit

dn: cn=empleados,ou=Grupos,dc=uoc,dc=lab
objectClass: posixGroup
objectClass: top
cn: empleados
gidNumber: 2000

dn: cn=directivos,ou=Grupos,dc=uoc,dc=lab
objectClass: posixGroup
objectClass: top
cn: directivos
gidNumber: 3000

dn: uid=alejandro,ou=empleados,dc=uoc,dc=lab
uid: alejandro
sn: Glez
cn: alejandro
objectClass: top
objectClass: person
objectClass: pilotPerson
objectClass: RADIUSprofile
userPassword: 123456
dialupAccess: alejandro
RADIUSGroupName: empleados

dn: uid=alfonso,ou=empleados,dc=uoc,dc=lab
uid: alfonso
sn: Glez
cn: alfonso
objectClass: top
objectClass: person
objectClass: pilotPerson
objectClass: RADIUSprofile
userPassword: 654321
dialupAccess: alfonso
RADIUSGroupName: directivos
```