Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Aplicación de las políticas de seguridad del ENS en redes inalámbricas WiFi

Grado en Ingeniería Mecánica

ALUMNO: Jesús Muñoz Castaño

DIRECTORES: Belén Barragáns Martínez

Pablo Sendín Raña

CURSO ACADÉMICO: 2017-2018

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Aplicación de las políticas de seguridad del ENS en redes inalámbricas WiFi

Grado en Ingeniería Mecánica

Intensificación en Tecnología Naval

Infantería de Marina

Universidade Vigo

RESUMEN

Este Trabajo Fin de Grado se plantea estudiar la aplicación de las políticas de seguridad definidas en el Esquema Nacional de Seguridad a redes inalámbricas WiFi. Para ello, realiza un estudio preliminar de la situación actual del ciberentorno y la seguridad en redes inalámbricas, así como el marco en el que España se encuentra. Se hace referencia al Esquema Nacional de Seguridad, al Centro Criptológico Nacional y a las guías publicadas por este organismo. Basándose en la guía CCN-STIC-816 de seguridad en redes inalámbricas, se despliega una red WiFi en el cuartel de alumnos "Marqués de la Victoria" emulando una red que dará servicio al Centro Universitario de la Defensa.

Desplegada la red, se evalúa la categoría de seguridad necesaria para una red de estas características según la documentación de referencia. Acorde con la categoría de seguridad establecida, se implantan las medidas correspondientes haciendo uso de *software* libre.

Con objeto de validar las medidas de seguridad establecidas en la red, se realiza una comparativa entre las medidas que podríamos denominar domésticas y las que se han implementado, visualizando los objetivos de seguridad alcanzados con cada uno de ellas. Además, se llevan a cabo una serie de pruebas de *pentesting* para demostrar la efectividad de las medidas implantadas.

Al final de este documento, se recogen las conclusiones obtenidas durante el desarrollo del TFG, así como las líneas futuras a desarrollar siguiendo esta línea de investigación.

PALABRAS CLAVE

Seguridad, guía CCN-STIC-816, WiFi, ENS, WPA2.

AGRADECIMIENTOS

Comienzo agradeciendo a mis dos tutores, Belén Barragáns Martínez y Pablo Sendín Raña por guiarme a lo largo del proyecto. Al personal del CAI de la ENM, con una mención especial al STTE. Don Ramón Carpintero. Mencionar también al TTE. David Méndez por proporcionarme interesante información sobre seguridad de redes inalámbricas. Por ayudarme a traducir al inglés el resumen de este TFG y su apoyo a lo largo del mismo debo darle muchísimas gracias a Holly Sandler. No puedo olvidar tampoco a mi gran amigo Samu por sus sabios consejos para gestionar mi tiempo estos meses.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

En este primer capítulo se procederá a explicar la motivación que ha impulsado el planteamiento de este Trabajo Fin de Grado (TFG), los objetivos que se persiguen en el desarrollo del mismo, así como la forma en la que se ha estructurado la memoria.

1.1 Motivación del TFG

Debido a la facilidad que aporta el empleo de redes inalámbricas WiFi tanto en nuestros hogares, como en organizaciones públicas o privadas, unido al desarrollo del Internet de las cosas (en inglés *Internet of Things*, IoT [1] a partir de ahora) cada vez es más común desplegar este tipo de redes pasando a ser sustitutas de las tradicionales redes cableadas.

El empleo de redes WiFi ha permitido una transición en el entorno doméstico. De tener una conexión a Internet exclusivamente en un ordenador de sobremesa ahora podemos conectar una cantidad mayor de dispositivos que pueden ir desde *smartphones* y *tablets* a ordenadores portátiles, impresoras o vídeo consolas.

En el ámbito profesional, las organizaciones pueden dotar de forma sencilla de conexión a Internet y a la intranet de la organización a multitud de dispositivos, así como de movilidad a los usuarios dentro de la infraestructura de la organización. El uso de redes inalámbricas WiFi permite, además, un importante ahorro a la hora de desplegar la infraestructura de red. Se pasa de tener que tender cable a las distintas zonas de la organización a tener que tan solo desplegar un punto de acceso conectado a una toma con conexión a la red WAN.

Por otro lado, una de las principales tendencias en el pasado año 2017 fue el desarrollo del IoT que trae consigo una carencia importante de seguridad. Esta tendencia afecta tanto a usuarios domésticos como a grandes organizaciones. El IoT abarca desde encimeras que detectan qué alimentos se posan sobre ella, hasta ciudades completas (*Smart cities*) como es el caso de Songdo, en Corea del Sur [2]. IoT actualmente tiene asociado una falta de seguridad importante por parte de los fabricantes y falta de concienciación de los usuarios. IoT puede llegar a hacer vulnerable una red debidamente asegurada, pero desatendida en el aspecto de estos dispositivos.

A pesar de esta falta de concienciación de los dispositivos IoT, la tendencia actual es que la población cada vez se implique más en la seguridad tanto de redes, como de dispositivos o redes sociales. Es destacable el hecho de que la sensibilización por la seguridad en las redes está en aumento: a día de hoy muchas empresas tienen la ciberseguridad como una asignatura pendiente e invierten en mejorarla.

La concienciación gana un papel muy importante en la seguridad de las redes ya que el eslabón más vulnerable de una red son los usuarios. Por tanto, una red es tan segura como metódicos y confiables sean sus usuarios. Un sistema puede implementar las máximas medidas de seguridad técnicas posibles y, sin embargo, si uno de sus usuarios facilita el empleo de sus credenciales de acceso a terceros, estas medidas no sirven para nada. De hecho, organismos gubernamentales tales como el Centro Criptológico Nacional (CCN) [3] y el Instituto Nacional de Ciberseguridad (INCIBE) [4] ofrecen programas de formación tanto para administradores de red como para usuarios de ésta.

INCIBE proporciona desde un sencillo decálogo para el usuario de una red [5] hasta un kit de concienciación para empresas [6] que incorpora recursos gráficos, elementos interactivos y una programación detallada. Por su parte, el CCN publica una serie de guías de buenas prácticas, muchas de las cuales están orientadas a la implementación de seguridad que deben realizar usuarios y empresas [7].

Por otro lado, el CCN, en el ejercicio de sus competencias, elabora y difunde las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones en el marco de lo establecido en el Esquema Nacional de Seguridad (ENS) [8].

El ENS fue aprobado por el Real Decreto 3/2010, de 8 de enero, y la responsabilidad de su aplicación recae en el CCN. El ENS tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y está constituido por los principios básicos y requisitos mínimos que permiten una protección adecuada de la información [9]. Varios aspectos son contemplados en el ENS para el presente proyecto, debido a que define políticas relacionadas con las redes inalámbricas WiFi. En el capítulo 2 se desarrollará más en detalle el ENS.

En este contexto surge la motivación del presente TFG, con el objeto de comprobar la eficacia de las medidas que el ENS propone en el ámbito de la seguridad en redes inalámbricas WiFi.

Esta preocupación por la seguridad de la información no interesa sólo en el ámbito doméstico o empresarial. Afecta a otras organizaciones, como pueden ser las Fuerzas Armadas de un país. Esto es debido a que aumenta el interés en el desarrollo de tecnologías inalámbricas seguras para mejorar el Mando y Control de las unidades en el terreno, sin que ello suponga una fuga de información de interés para el enemigo.

El Ejército de Tierra de los Estados Unidos ya ha comenzado el despliegue de redes WLAN en los puestos de mando [10], conocidos por ellos como TOC (*Tactical Operations Center*). Esta implementación ha permitido que un mayor número de aplicaciones puedan conectarse a la red, así como una mayor velocidad a la hora de establecer el puesto de mando, frente a las horas que llevaba preparar una red cableada. El Ejército de Tierra de los Estados Unidos emplea en su estructura el estándar 802.11ac, el término acuñado como WiFi Gigabit, que permite mejorar las tasas de transferencia notablemente. Los puntos de acceso empleados presentan un cifrado aprobado por la NSA (*National Security Agency*) y forman parte de WIN-T (*Warfighter Network Tactical*) *Increment* 1, el sistema de mando y control del ejército estadounidense. Desde el punto de vista logístico, los medios que deben transportarse para establecer la red son mucho menores que en el antiguo sistema cableado.

La Infantería de Marina española está planteando la incorporación de elementos inalámbricos de ámbito local en sus puestos de mando, con el fin de ampliar la capacidad de acceso a Internet que se tiene por medio de satélite, ya sea a otros vehículos en el concepto SOTM (*Satcom On The Move*) o dentro del propio puesto de mando, SATQH (*Satcom At The Quick Halt*). La configuración original empleaba como medio de transmisión inalámbrica la radio SPEARNET que ofrecía una tasa de transferencia limitada. Actualmente se pretenden emplear routers adaptados para el ambiente de operaciones, pero no cuentan con una certificación de seguridad aprobada por el CCN y, por tanto, no pueden utilizarse.

1.2 Objetivos

Para realizar dicho estudio de las medidas que marca el ENS, en este TFG se establecen los siguientes objetivos, que se desarrollan a lo largo de la memoria:

- Instalación de una red inalámbrica WiFi simulando la red de una organización. En nuestro caso, se simula una red WiFi para el Centro Universitario de la Defensa (CUD).
- Estudio y clasificación de la seguridad necesaria para la red según el ENS.
- Revisión de *software* libre de gestión de redes inalámbricas.
- Configuración de la red WiFi e implementación de las medidas de seguridad que marca el ENS para la categoría de seguridad determinada previamente.
- Validación de la seguridad de la red establecida.

1.3 Organización de la memoria

La memoria se divide en cinco capítulos.

En esta primera parte se ha mostrado la motivación que ha llevado al desarrollo de este TFG. Después se han presentado los objetivos que se persiguen y el apartado ha concluido con la forma en la que se ha organizado la memoria.

En el segundo capítulo (Estado del arte) se presenta la información necesaria para la comprensión del problema tratado. En el caso particular de este proyecto se hablará de las redes de información en general, centrándonos en las redes inalámbricas WiFi y el estándar que las regula. Seguidamente, se revisarán las distintas opciones de *software* libre de gestión de redes inalámbricas. También se evaluarán las distintas amenazas más comunes para redes inalámbricas WiFi. Finalmente, se hablará de la función del CCN y del Esquema Nacional de Seguridad.

El tercer capítulo (Desarrollo del TFG) comienza describiendo todo el *software* y *hardware* empleado en el TFG, así como, el propósito de la red inalámbrica que se va a desplegar y la seguridad a implantar. Finalmente, se detallará el proceso de despliegue y configuración de la red según el ENS.

La Validación del TFG, que conforma el cuarto capítulo de la memoria, recoge las ventajas que supone para la red la aplicación de las medidas de seguridad del ENS, y de qué forma se solucionan, de manera implícita, las amenazas referidas en el apartado 2.4. Además, se incluye un apartado de pruebas de *pentesting* que trata de medir la eficacia de las medidas implementadas.

Con el capítulo de Conclusiones y líneas futuras se cerrará el contenido de la memoria, resumiendo las principales conclusiones obtenidas durante el desarrollo del TFG y se propondrán futuras líneas de trabajo relacionadas con el tema del presente trabajo.

2 ESTADO DEL ARTE

En el presente capítulo se revisa el estado del arte de las redes de comunicaciones y, en particular, de las redes inalámbricas, del *software* libre de gestión de redes WiFi, y de aspectos relacionados con la ciberseguridad en redes WiFi, que se particularizarán en el último apartado, centrándose en el órgano encargado de la ciberseguridad en España, así como el marco legal en el que se encuadra.

2.1 Redes de comunicaciones

Desde la creación del primer enlace en la primera red de área extensa del mundo hasta el día de hoy hemos podido observar una vertiginosa evolución de las tecnologías relacionadas con las redes de comunicaciones. Esto ha provocado, además, que hayan surgido nuevos servicios, retos y problemas [11].

En la actualidad nos encontramos inmersos en el mundo de las redes de comunicaciones, ya sea en casa o en el trabajo, como fuente de ocio o forma de relación con otras personas. A través de las redes se mueven grandes flujos de información de un lugar a otro del planeta, de forma rápida y preferiblemente segura. Las redes, o esa gran red conocida como Internet, constituyen el medio en el que nos movemos en el mundo globalizado en el que vivimos.

Teniendo en cuenta la distancia entre los dispositivos que consideremos conectados, podemos clasificar las redes en cinco tipos [12], de menor a mayor escala:

- Redes PAN (*Personal Area Network*): Son redes de área personal, es decir, redes que comunican los dispositivos cercanos a una persona como puede ser un monitor, el teclado o un ratón. Estas conexiones pueden ser vía cable o inalámbricas, y usan tecnologías como Bluetooth o ZigBee.
- Redes LAN (*Local Area Network*): Hablamos en este caso de redes que engloban desde un cuarto hasta un conjunto de edificios. El objetivo de estas redes es la compartición de recursos entre equipos de la red LAN, por ejemplo, intercambio de información sin salir de dicha red o uso común de una impresora y también, interconectar diferentes dispositivos a otro que les proporcione conexión con el exterior. Igual que en el caso anterior, estas redes pueden ser cableadas o inalámbricas. Las redes cableadas usan el estándar IEEE 802.3 o Ethernet. En el caso de ser inalámbricas, se usa el estándar IEEE 802.11, también conocido como WiFi.
- Redes MAN (*Metropolitan Area Network*): Cubren toda una ciudad, son redes de área metropolitana. Originalmente aparecieron con el fin de dar cobertura de TV dentro de las ciudades, ya que en ese momento la transmisión por aire de TV era de inferior calidad. Con el desarrollo de Internet, los operadores de televisión se dieron cuenta de la necesidad de

implementar una red MAN que proporcionara Internet a los hogares. Actualmente existe la tecnología WiMAX, estándar IEEE 802.16, que permite la creación de redes de área metropolitana de forma inalámbrica.

- Redes WAN (*Wide Area Network*): Añaden una extensa cobertura en un área geográfica, por ejemplo, un país o continente. Dichas redes podríamos verlas como una red LAN de gran tamaño, aunque presenta sus particularidades. En estas redes debemos diferenciar a los hosts, usuarios que quieren comunicarse con otro host en otra parte del país, y las subredes, que son las encargadas de poner en contacto a esos hosts que se encuentran en redes LAN distintas. Los encargados de gestionar las subredes suelen ser las operadoras telefónicas, conocidas como ISP (*Internet Service Provider*), ya que a las organizaciones que usan las redes WAN no les interesa mantener ni gestionar la arquitectura de la subred, que suele ser un entramado cableado que usa, obviamente, tecnología diferente a la de una red LAN. Las conexiones en red WAN también pueden ser inalámbricas, como una conexión satélite o la red de telefonía móvil. Como ejemplo de red WAN en el ámbito de la Armada tenemos la WAN-PG, una red WAN de Propósito General.
- Interredes: Se conoce como interred o internet a un conjunto de redes conectadas. El ejemplo más conocido y utilizado de interred es Internet.

En la Tabla 2-1 se muestra la forma de clasificar las redes según su escala.

Distancia entre procesadores	Procesadores ubicados en el mismo	Tipo de red
1 m	Metro cuadrado	PAN
10 m	Cuarto	LAN
100 m	Edificio	LAN
1 km	Campus	LAN
10 km	Ciudad	MAN
100 km	País	WAN
1000 km	Continente	WAN
10000 km	Planeta	Internet

Tabla 2-1 Tabla resumen de las distintas clasificaciones de red según escala

Como ya se ha visto, además de la clasificación según su escala, podemos clasificarlas en redes cableadas o inalámbricas. En nuestro caso nos centraremos en las redes inalámbricas, más concretamente en las redes de área local inalámbricas o WLAN (*Wireless Local Area Network*), basadas en el estándar IEEE 802.11 [13].

2.2 Las redes inalámbricas WiFi

En el presente apartado se presentan los distintos estándares que regulan el empleo y desarrollo de las redes inalámbricas WiFi, haciendo especial hincapié en los estándares recogidos en la guía CCN-STIC-816 Seguridad en Redes Inalámbricas en el ENS [14].

Pero antes de presentar los estándares, debemos comentar las funciones del IEEE [15] (*Institute of Electrical and Electronics Engineers*).

El IEEE se define como la mayor organización, técnica y profesional, del mundo dedicada al avance de la tecnología en beneficio de la humanidad. Su misión es fomentar la innovación y excelencia tecnológica en beneficio de la humanidad.

De forma más tangible, el IEEE se encarga, entre otras cosas, de la creación de estándares, una serie de normas y reglas en diversos ámbitos de la tecnología, desde la energía nuclear hasta la nanotecnología. El ámbito que nos atañe es el de tecnologías cableadas e inalámbricas. Estos estándares se encuentran en constante evolución debido a la dedicación de los grupos de trabajo encargados de cada uno de ellos.

La Tabla 2-2, Tabla 2-3, Tabla 2-4 muestran, respectivamente, los grupos de trabajo y estudios activos, en suspensión y disueltos de los grupos de trabajo según su estándar en el ámbito LAN y MAN.

Estándar	Tema del estándar
802.1	*Higher Layer LAN Protocols Working Group*
802.3	*Ethernet Working Group*
802.11	*Wireless LAN Working Group*
802.15	*Wireless Personal Area Network (WPAN) Working Group*
802.16	*Broadband Wireless Access Working Group*
802.18	*Radio Regulatory TAG*
802.19	*Wireless Coexistence Working Group*
802.21	*Media Independent Handover Services Working Group*
802.22	*Wireless Regional Area Networks*

Tabla 2-2 Grupos de trabajo y estudio activos (tomada de [15])

Estándar	Tema del estándar
802.17	*Resilient Packet Ring Working Group*
802.20	*Mobile Broadband Wireless Access (MBWA) Working Group*

Tabla 2-3 Grupos de trabajo y estudio en suspensión (tomada de [15])

Estándar	Tema del estándar
802.2	*Logical Link Control Working Group*
802.4	*Token Bus Working Group*
802.5	*Token Ring Working Group*
802.6	*Metropolitan Area Network Working Group*
802.7	*Broadband TAG*
802.8	*Fiber Optic TAG*
802.9	*Integrated Services LAN Working Group*
802.10	*Security Working Group*
802.12	*Demand Priority Working Group*
802.14	*Cable Modem Working Group*
802.23	*Emergency Services Working Group*

Tabla 2-4 Grupos de trabajo y estudio disueltos (tomada de [15])

De los estándares anteriormente citados, nos centramos en el 802.11, que define las redes WLAN. Este estándar ha ido evolucionando desde su primera versión, en 1997, hasta nuestros días, con diferentes estándares, los últimos, el 802.11ah y el 802.11ai [13]. Aunque estos últimos sean los estándares más recientes no son necesariamente utilizados a nivel global, ya que la implantación puede depender de que la tecnología de los dispositivos que utilizamos tenga la capacidad de soportar las características definidas, como pueden ser los métodos de codificación que utilizan, el ancho de banda que ofrecen o las mejoras de rendimiento.

Para el desarrollo de este TFG nos interesan los protocolos a los que se refiere el Centro Criptológico Nacional, a partir de ahora CCN [16], en la guía CCN-STIC-816 Seguridad en Redes Inalámbricas en el ENS [14]. Estos son el IEEE 802.11i [17] y el IEEE 802.11w [18]. Aunque ajeno al estándar 802.11, la guía también contempla el uso del IEEE 802.1x [19], modelo que rige el control de puertos. Se exponen, a continuación, breves descripciones de los estándares anteriormente nombrados:

- IEEE 802.11i: es una revisión del estándar original en el que se modificaron el mecanismo de seguridad original, que se trataba de WEP (*Wired Equivalent Privacy*). El motivo de este cambio fue la detección de vulnerabilidades de WEP, probando no ser adecuado para dar seguridad a redes inalámbricas. Esto fue lo que IEEE 802.11i corrigió, pasando a crear mecanismos más robustos que WEP, como fueron WPA (*WiFi Protected Access*) y WPA2, que es el que se utiliza actualmente.

  Estos dos últimos estándares, WPA y WPA2, utilizan los protocolos criptográficos *Temporal Key Integration Protocol* (TKIP, a partir de ahora) y *Counter-mode/CBC-MAC Protocol* (CCMP), respectivamente. CCMP utiliza el modo de operación *Counter with CBC-MAC* (CCM), también conocido como *Advanced Encryption Standard* (AES), usando una clave de 128-bits y un tamaño de bloque de 128-bit. Para incrementar la confidencialidad y la integridad de los datos, CCMP combina diversos métodos para mejorar las prestaciones de TKIP y WEP.

- IEEE 802.1x: Se definen dos modos de implementación (*Personal* y *Enterprise*) para WPA y WPA2. El modo *Enterprise* utiliza el mecanismo de autenticación 802.1x en el que se

utiliza un Servidor de Autenticación (*Authentication Server*, AS) para autorizar las peticiones de conexión entrante que se dirigen a la red.

La combinación de ambos estándares nos permite la creación del concepto englobado en el IEEE 802.11i, las redes RSA (*Robust Security Networks*), que son aquellas que únicamente permiten la creación de asociaciones RSNA (*Robust Security Network Associations*). Para garantizar la seguridad robusta de una red, todos los dispositivos deben utilizar RSNA. Para establecer RSNA se distinguen 5 fases:

1. Descubrimiento y asociación: en el que el dispositivo cliente solicita el acceso al AP (*Access Point*) con el fin de unirse a la red inalámbrica.
2. Autenticación y distribución de claves raíz: una vez realizada la asociación entre cliente y AP, se inicia el proceso de autenticación y entrega de las claves raíz. Ambos dispositivos se autentican mutuamente, el cliente para mostrarse como un usuario legítimo y autorizado para conectarse a la red y ésta para demostrar que es una red legítima y no nos conectamos a una red falsa. La entrega de claves raíz también se realiza y éstas se usan para generar las demás claves criptográficas.
   El primer proceso de autenticación se puede llevar a cabo mediante:
   - El modelo de control de acceso basado en puerto, definido en el estándar IEEE 802.1x y empleando el protocolo EAP (*Extensible Authentication Protocol*).
   - El método de claves pre-compartidas PSK (*Pre-shared keys*), en el que se supone que la posesión de la clave pre-compartida entre cliente y AP sirve como prueba de autenticación.

   En el primer caso, para el uso del método EAP, se lleva a cabo una transferencia de datos entre el suplicante o cliente y el servidor de autenticación, usando como puente del enlace al AP para el encapsulamiento y transmisión de los mensajes entre cliente y AS. La autenticación en sí se puede realizar mediante diversos mecanismos: contraseñas estáticas, dinámicas, o certificados.

   El estándar 802.1x añade el término de puertos controlados y puertos no controlados. El tráfico de autenticación EAP es conducido por los puertos no controlados. El resto del tráfico se conduce por los puertos controlados, que no se podrán utilizar hasta que la autenticación finalice con éxito y, además, se haya generado y distribuido el material de claves criptográficas con el fin de proteger la comunicación. Se genera la clave raíz AAAK (*Authentication, Authorization and Accounting Key*), también llamada MSK (*Master Session Key*), y se distribuye al dispositivo suplicante.
3. Generación y distribución de las claves criptográficas: una vez obtenidas las claves raíz, se obtiene el material de claves necesario para proteger la comunicación.
   En el proceso de generación y distribución de claves se emplean dos tipos de negociación: la negociación en 4 etapas o *4-way handshake*, y la negociación de grupo. Ambas negociaciones emplean mecanismos de cifrado y de protección de integridad para el material criptográfico distribuido.
   Al finalizar esta fase, consideramos completada la autenticación mutua, y los puertos controlados son desbloqueados para permitir el tráfico de datos de usuario.
4. Transferencia de datos protegidos: es la fase propia de transferencia de datos. La protección de la información se realizará a través de los algoritmos criptográficos de la suite criptográfica negociada y acordada en la primera fase, descubrimiento y

asociación. Los algoritmos utilizarán las claves criptográficas generadas en la fase 3.

5. Fin de la conexión: en esta fase se elimina la asociación entre el AP y el dispositivo cliente. El AP desautentica al cliente, se eliminan las claves empleadas y el puerto controlado 802.1x pasa de nuevo a estado bloqueado, impidiendo el tráfico de usuarios.

- IEEE 802.11w: supone una mejora al estándar 802.11i, porque añade seguridad al tráfico de gestión durante la conexión. Proporciona protección de confidencialidad, integridad, autenticidad y protección anti-reenvíos para las tramas de gestión.

Para la aplicación de estos estándares hemos visto que intervienen tres elementos de *hardware*: el cliente, el Punto de Acceso y el Servidor de Autenticación:

- Cliente: cualquier dispositivo de usuario que solicita un acceso a la red inalámbrica para realizar la transferencia de datos de usuario. Pueden ser, por ejemplo, ordenadores portátiles, *smartphones*, videoconsolas, etc.
- Puntos de Acceso (AP): son parte de los equipos que forman la infraestructura inalámbrica, y se encargan de conectar los dispositivos cliente entre sí, o con la infraestructura cableada de la organización.
- Servidor de Autenticación (AS): son equipos encargados de gestionar el acceso de clientes a la red y de expedición de certificados. Son capaces de mantener una base de datos con cada usuario y otorgarle a cada uno una clave distinta para acceder a la red WiFi.

Esto será así si empleamos una distribución en modo Infraestructura (Figura 2-1), ya que si empleamos una distribución Ad Hoc (Figura 2-2) no existirían los puntos de acceso ni los servidores de autenticación y los dispositivos clientes se comunicarían entre sí directamente. Para el desarrollo del presente proyecto emplearemos el modo Infraestructura.

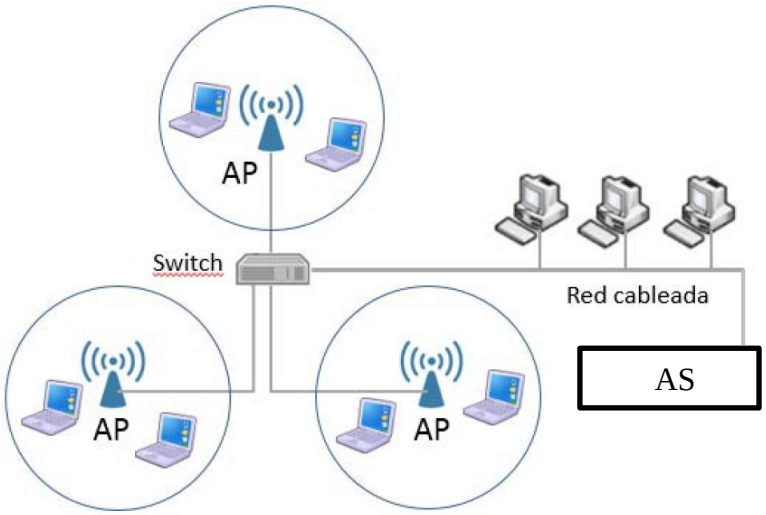


Figura 2-1 Diagrama de una red inalámbrica en modo Infraestructura

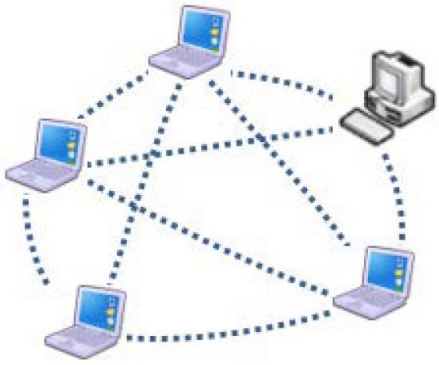


Figura 2-2 Diagrama de una red inalámbrica en modo Ad Hoc

2.3 Revisión de software libre de gestión de redes inalámbricas

Para la gestión y configuración de los routers se emplea *firmware*, generalmente desarrollado por el fabricante. Estos *firmware* suelen presentar ciertas limitaciones tanto a nivel de configuración como de seguridad y pueden llegar a quedarse obsoletos. Un ejemplo de ello es la empresa UNIFI [20], que a partir de septiembre de 2018 deja de dar soporte a un modelo de punto de acceso.

Una solución a este problema puede ser el empleo de *software* libre de gestión de redes inalámbricas, que nos aporta una mayor seguridad, personalización y opciones de configuración. Estos paquetes de *software*, soportados por la comunidad de usuarios de *software* libre, se encuentran en constante actualización dando soporte a los routers por un tiempo más prolongado.

En 2002, la compañía Linksys lanzó una línea de routers (los modelos WRT54G) con un *software* basado en Linux. Desde su lanzamiento varias compañías han seguido sus pasos y se han desarrollado diferentes programas de gestión como son DD-WRT [21], Tomato [22] y OpenWrt [23].

El *firmware* libre presenta una serie de ventajas genéricas comunes a todos:

- El código del *firmware* está visible para toda la comunidad.
- Mejora de la interfaz de usuario y funcionalidades en distintas marcas y modelos.
- Integración VPN.
- Mejorada estabilidad de las redes y la información de estado de éstas.
- Modos inalámbricos avanzados: punto de acceso, cliente puente inalámbrico y modo repetidor.
- Soporte a redes inalámbricas virtuales (VLAN, *Virtual Local Area Network*).
- Acceso a tablas IP.
- Soporte de IPv6.
- Autenticación RADIUS.
- Soporte Telnet/SSH.
- Integración de *Hotspots WiFi*.
- Soporte NAT (*Network Address Translation*).

Más allá de estas ventajas, cada *firmware* presenta particularidades que puede hacerlo más apto para unos usuarios u otros [24].

En el caso de DD-WRT, podemos decir que se trata de uno de los más populares debido a su facilidad de instalación. Además, presenta una gran variedad de características y el soporte de la comunidad es muy activo y eficaz. Su principal limitación radica en lo complicado de su configuración.

El *firmware* Tomato es el más sencillo de emplear de los tres. La interfaz gráfica es muy intuitiva e incluye una herramienta de monitorización de la red de serie. Sin embargo, este *firmware* puede no ser el más adecuado para implementarse en un router antiguo debido a la baja compatibilidad que tiene con routers actuales. Tomato presenta varias versiones como Tomato Shibby y AdvancedTomato. Este *firmware* tiene una mejor estabilidad y rendimiento que DD-WRT.

OpenWrt estaba originalmente basado en línea de comandos y requería de conocimientos avanzados para su configuración, pero actualmente se han desarrollado diversas interfaces gráficas de gestión del router como son LuCI o Gargoyle. OpenWrt presenta una gran cantidad de *firmware* para cada uno de los modelos de router que soporta y previamente se debe elegir el adecuado para nuestro router. OpenWrt es altamente personalizable y puede añadir gran cantidad de funciones adicionales integradas en un solo *firmware*.

Se puede decir que OpenWrt nos ofrece todo lo que nos ofrecen los otros *firmware*, añadiendo, además, su alta personalización y una mayor estabilidad que su principal competidor DD-WRT. Su principal desventaja, la complejidad de configuración, se mitiga con el empleo de interfaces gráficas.

2.4 Amenazas de seguridad en redes inalámbricas WiFi

La Unión Internacional de Telecomunicaciones define la ciberseguridad como [25]:

> *El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios del ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: Disponibilidad, integridad que puede incluir la autenticidad y el no repudio y confidencialidad.*

Entendemos el ciberentorno como el conjunto de usuarios, redes, dispositivos, *software*, que están conectados directa o indirectamente a las redes. Para un adecuado funcionamiento del ciberentorno se deben mantener íntegras ciertas propiedades.

A continuación, se exponen las propiedades de seguridad [14]:

- Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: Propiedad o característica consistente en que el archivo de información no ha sido alterado de manera no autorizada.
- Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- Autenticidad: Propiedad o característica que garantiza la fuente de la que proceden los datos.
- Trazabilidad: Propiedad o característica que nos permite comprobar a posteriori quién ha accedido, o modificado, una cierta información.

Estas propiedades pueden verse afectadas por distintas actividades maliciosas por parte de atacantes e impedir el correcto funcionamiento de una red.

Las redes inalámbricas se ven amenazadas por los mismos riesgos que las cableadas añadiendo además riesgos específicos del ámbito inalámbrico. En la siguiente lista se incluyen algunos de los más representativos [14].

- *Eavesdropping*. Cuando un individuo no autorizado utiliza alguna herramienta (generalmente antenas de gran alcance) para capturar de forma pasiva el tráfico inalámbrico. Este tráfico le sirve para espiar información (en caso de que no vaya cifrada) y para detectar patrones de comportamiento.
- Denegación del Servicio (*Denial of Service*). Cuando la infraestructura inalámbrica queda incapacitada para ofrecer el servicio, por ejemplo, cuando un individuo no autorizado inyecta peticiones masivas de asociación a los AP dejándolos incapacitados para responder a las peticiones de los clientes legítimos.
- *Man-in-the-middle*. Cuando un individuo no autorizado se coloca en medio de la comunicación inalámbrica entre emisor y receptor, suplantando a una de las partes y haciendo creer a la otra que está hablando con el comunicante legítimo. Desde ese punto, se pueden ejecutar multitud de ataques posteriores (captura de credenciales, de tráfico, etc.).
- *MAC Spoofing*. Los AP pueden tener configurada una lista de direcciones MAC (*Media Access Control*) permitidas. A pesar de ello, un individuo no autorizado puede suplantar una dirección MAC autorizada para lograr el acceso.
- Acceso de dispositivos no autorizados que están conectados al dispositivo cliente autorizado y que a través de él pueden lograr acceso a la red inalámbrica y por tanto a la red cableada de la organización pudiendo introducir *software* dañino.

Merece una mención especial una amenaza reciente para la seguridad que puso en jaque a todos los fabricantes de dispositivos de redes inalámbricas WiFi, los ataques KRACK.

Actualmente la seguridad en las redes WiFi está basada en el protocolo WPA2, protocolo creado en 2003 y que ha sido válido hasta finales de 2017. En esa fecha Mathy Vanhoef descubrió una vulnerabilidad que él llamó KRACK [26], *Key Reinstallation Attacks*. Estos ataques consisten en romper WPA2 forzando la reutilización de *nonces* o paquetes de incremento de número transmitido.

KRACK funciona de la siguiente manera. Cuando un cliente se une a la red, se ejecuta un *4-way handshake* para negociar la nueva clave de encriptación que se utilizará en toda la comunicación posterior. Se instalará esta clave después de recibir el tercer mensaje del *4-way handshake*. Una vez que la clave está instalada, será utilizada para cifrar los bloques de datos usando un protocolo de cifrado. Sin embargo, como los mensajes pueden perderse, el AP retransmitirá el tercer mensaje si no recibe el pertinente mensaje de recibido por parte del solicitante. El resultado es que el cliente puede recibir el tercer mensaje varias veces. Cada vez que recibe el mensaje, se reinstalará la misma clave de encriptación, y de este modo se resetea el paquete de incremento de número transmitido. Un atacante puede forzar esos reinicios *nonce* compilando y retransmitiendo el tercer mensaje del *4-way handshake*. De esta forma, forzando la reutilización de *nonce,* el protocolo de encriptación puede ser atacado, por ejemplo, replicando paquetes o desencriptándolos.

Esta técnica permite al atacante realizar uno de los ataques más comunes en redes WiFi abiertas, inyectar paquetes maliciosos en conexiones HTTP (*Hipertext Transfer* Protocol) sin cifrar. Por ejemplo, un atacante puede inyectar ransomware o malware en las páginas que la víctima está visitando.

Si la víctima usa WPA-TKIP o *Galois Counter Mode Protocol* (GCMP) en lugar de AES-CCMP, las consecuencias pueden ser catastróficas. En estos protocolos la reutilización de *nonce* permite al adversario desencriptar, inyectar o falsificar paquetes. GCMP está siendo implantado bajo el nombre de *Wireless Gigabit* (WiGig) y se espera que sea adoptado en un alto porcentaje en los próximos años.

Los ataques KRACK no permiten recuperar las contraseñas de las redes WiFi. Actualmente los fabricantes tanto de dispositivos clientes como de AP´s están actualizando WPA2 para evitar estos ataques. La organización *WiFi Alliance* anunció que en 2018 lanzaría un nuevo protocolo de seguridad, el WPA3, con sustanciales mejoras [27].

2.5 CCN y el Esquema Nacional de Seguridad

Dado el peso que ha ganado en los últimos años la ciberseguridad y el aumento de los ciberataques a nivel mundial, se han creado organismos en muchos países para combatir el cibercrimen. Ejemplo de ello es la Organización Europea de Ciberseguridad ECSO (*European Cyber Security Organisation*) [28], y, a nivel español, el ya mencionado INCIBE [29] o el MCCD, Mando Conjunto de Ciberdefensa [30]. Además de INCIBE en España existe el Centro Criptológico Nacional (CCN).

El CCN es el organismo responsable de coordinar la acción de los diferentes organismos de la Administración pública que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

El CCN fue creado en el año 2004, a través del Real Decreto 421/2004 [31], adscrito al Centro Nacional de Inteligencia (CNI). De hecho, en la Ley 11/2002, de 6 de mayo [32], reguladora del CNI, se encomienda a dicho centro el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que se confiere a su Secretario de Estado la responsabilidad de dirigir el Centro Criptológico Nacional. Por ello, el CCN comparte con el CNI medios, procedimientos, normativa y recursos [3].

El CCN cuenta con un órgano, el CCN-CERT, que le dota de capacidad de respuesta a incidentes en el ámbito de la ciberseguridad. CERT es un término que proviene del inglés *Computer Emergency Response Team*, y define a un equipo de personas dedicado a la implantación y gestión de medidas preventivas, reactivas y de gestión de seguridad con el objetivo de mitigar el riesgo a los ataques contra las redes y sistemas de la comunidad a la que se proporciona el servicio [33].

En el caso particular del CCN-CERT se fija su actividad en los sistemas de las distintas administraciones (general, autonómica y local) para, posteriormente, ampliar esta responsabilidad a los ciberataques sobre sistemas de empresas pertenecientes a sectores de interés estratégico para la seguridad nacional y para el conjunto de la economía del país.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional, cooperar y ayudar a responder de forma rápida y eficiente a los ciberataques y afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

El CCN se rige por el Esquema Nacional de Seguridad. El ENS tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. La Ley 11/2007, de 22 de junio [34], de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el ENS, que fue aprobado mediante Real Decreto 3/2010, de 8 de enero [35]. En 2015 se publicó la modificación del Esquema Nacional de Seguridad a través del Real Decreto 951/2015, de 23 de octubre [36], en respuesta a la evolución de la normativa, en especial de la Unión Europea, de las tecnologías de la información y de la experiencia de la implantación del ENS.

Los sistemas debieron adecuarse a lo dispuesto en la citada modificación en un plazo de veinticuatro meses.

El ENS estipula lo siguiente en diversos artículos [37]:

- Artículo 11, la gestión continuada de la seguridad como un aspecto clave que ha de acompañar a los servicios disponibles por medios electrónicos.
- Artículo 15, la exigencia, de manera objetiva y no discriminatoria, de profesionales cualificados a las organizaciones que presten servicios de seguridad a las Administraciones Públicas.
- Artículo 18, la utilización, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, de aquellos productos que tengan certificada la funcionalidad, de seguridad relacionada con el objeto de su adquisición.
- Artículo 24, el despliegue de procedimientos de gestión de incidentes de seguridad, y de debilidades detectadas en los elementos del sistema de información.
- Artículo 27, la formalización de las medidas de seguridad en un documento denominado "declaración de aplicabilidad" y la posibilidad de reemplazar medidas de seguridad por otras compensatorias cuando se justifique documentalmente.
- Artículo 29, la figura de las "Instrucciones técnicas de seguridad" que regularán aspectos tales como el informe del estado de la seguridad, la auditoría de la seguridad, la conformidad con el ENS, la notificación de incidentes de seguridad, la adquisición de productos de seguridad, la criptología empleada en el ámbito del ENS y los requisitos de seguridad en entornos externalizados, entre otras.
- Artículo 34, señala que los sistemas de información a los que se refiere el real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del presente Esquema Nacional de Seguridad.
- Artículo 36, la notificación al CCN de aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados.

Uno de los métodos que utiliza el CCN para cumplir sus cometidos y adecuarse al ENS es la publicación de una serie de documentos CCN-STIC (Servicio de las Tecnologías de la Información y las Comunicaciones). Éstos proporcionan un marco de referencia en esta materia para que sirva de apoyo para el personal de las administraciones públicas que lleve a cabo la tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Para este TFG se han empleado las siguientes guías CCN-STIC:

- CCN-STIC-803 Valoración de los sistemas [38]
- CCN-STIC-804 Medidas de implantación del ENS [39]
- CCN-STIC-816 Seguridad en Redes Inalámbricas en el ENS [40]
- CCN-STIC-406 Seguridad en Redes Inalámbricas [41]
- CCN-STIC-803 Anexo I universidades [42]

Como se puede intuir por los títulos de estas guías, es la serie 800 la que regula lo relacionado con el Esquema Nacional de Seguridad.

Además, el CCN-CERT emite una serie de informes ciberentorno actual, como, por ejemplo, el informe CCN-CERT-IA 16-17 Ciberamenazas y Tendencias 2017. Se incluyen, entre la información generada, recomendaciones y buenas prácticas, como, por ejemplo, el CCN-CERT BP-05-16 Dispositivos IoT.

También se ha tenido en cuenta en este TFG el RFC (*Request for Comments*) 4017 [43], del IETF (*Internet Engineering Task Force*), referenciado en la guía CCN-STIC-816. El RFC 4017 es un documento que define los requerimientos para los métodos de autenticación EAP usado en el estándar IEEE 802.11. El material del documento ha sido aprobado por el IEEE 802.11.

3 DESARROLLO DEL TFG

En este capítulo se expondrá el proceso completo de instalación y configuración de una red inalámbrica WiFi siguiendo las directrices del ENS. Se partirá de cuatro routers de uso doméstico con configuración de serie y se establecerá finalmente una red inalámbrica capaz de dar cobertura a un área equivalente al pasillo de despachos del Centro Universitario de la Defensa. Esta red presenta todas las medidas de seguridad que una red de su clasificación necesita según el ENS. Todo ello se realizará empleando *software* libre, desde el *firmware* de los routers hasta servidores de autenticación.

3.1 *Software* y *hardware* empleados en este TFG

En esta parte, nos centraremos en el *hardware* y *software* empleado para los puntos de acceso, que son la parte principal del TFG.

3.1.1 Hardware, AP

El router de banda ancha Wireless-G Linksys WRT54GL es el modelo utilizado para desplegar la red inalámbrica sobre la que implementaremos las medidas recogidas en la guía CCN-STIC-816. El router cuenta con su propio sistema operativo para su configuración, proporcionándonos una interfaz gráfica. Pero, además, nos permite la instalación de un entorno Linux que nos proporciona una mayor libertad a la hora de configurarlo, ya sea mediante interfaz gráfica o mediante la terminal.

El router nos presenta información sobre su estado mediante una serie de LEDs situados en la cara frontal del mismo (ver Figura 3-1):

1. *Power*: nos proporciona información sobre si el router está conectado a la red eléctrica. Puede proporcionarnos información adicional en caso de mal funcionamiento del router.
2. DMZ (*DeMilitarized Zone*): indica que está habilitada la opción DMZ en la que hay algún equipo que se encuentra fuera de la zona de seguridad, por la propia configuración del router. También nos permite saber cuándo debemos resetear el router para acceder al modo *Failsafe*.
3. WLAN: nos indica si está activa la red de área local inalámbrica.
4. Ethernet: son cuatro LEDs que nos indican qué conexiones Ethernet se encuentran en funcionamiento, es decir, cuántos cables están conectados a la parte trasera del router (ver Figura 3-2).
5. Internet: situado en el extremo derecha nos indica si está conectado el cable que proporciona el acceso a Internet.

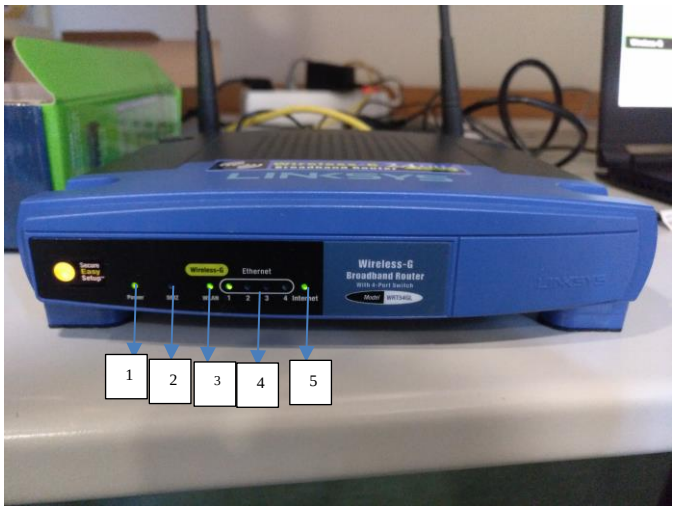


Figura 3-1 Router Linksys WRT54GL

Figura 3-2 Router Linksys WRT54GL parte trasera (tomado de [44])

Respecto a las especificaciones técnicas, destacamos las mostradas en la Tabla 3-1 [45]:

Banda de Frecuencia	2.4 GHz
Algoritmos de encriptación	128-bit WEP, 64-bit WEP, WPA, WPA2
Fabricante	Cisco
Protocolos de enlace de datos	*Ethernet*, *Fast Ethernet*, IEEE 802.11b, IEEE 802.11g
Características	Soporte DHCP, puerto DMZ, filtro de direcciones MAC, SPI (*Stateful Packet Inspector*), soporte de WiFi Multimedia, asignación de IP dinámicas, protección firewall, actualización de *firmware*
Estándares	IEEE 802.11b, IEEE 802.11g, IEEE 802.3, IEEE 802.3u, UPnP, WiFi-Certified
Velocidad de transferencia de datos	54 Mbps
Memoria	13388 kB

Tabla 3-1 Especificaciones técnicas estándar (tomado de [45])

De las características anteriormente nombradas destacamos la memoria del router. Ésta ha supuesto una limitación considerable a la hora de desarrollar este TFG y condicionó ciertas decisiones como la instalación de FreeRADIUS o cargar las librerías que permiten el acceso vía web seguro mediante HTTPS.

3.1.2 Software, AP

El propio router trae un CD de instalación que nos permite hacer una configuración del router con ayuda del asistente. Sin embargo, trabajaremos con un *software* libre basado en Linux, empleando OpenWrt frente a Tomato y DD-WRT.

Se decide emplear OpenWrt porque es soportado por una gran variedad de routers, y permite un gran abanico de personalización gracias a un elevado número de utilidades y extensiones. El desarrollo de interfaces gráficas para su configuración mitigó su principal desventaja, que era la complejidad en la configuración.

OpenWrt es un *software* basado en Linux con el objetivo de crear un *firmware* 100% personalizable por parte de sus usuarios, proporcionando un completo sistema de archivos con un gestor de paquetes. Para los desarrolladores, OpenWrt es el marco en el que construir una aplicación sin tener que construir un *firmware* completo para esa aplicación.

La versión más actualizada es Chaos Calmer 15.05-r,c3 publicada en 2015, que añade una serie de mejoras respecto a versiones anteriores que no son objeto de este trabajo. En los routers empleados en este trabajo se ha utilizado la versión Backfire 10.03.1, la versión más moderna compatible con nuestro router.

OpenWrt nos permite configurar el router por medio de una interfaz gráfica vía web para facilitar la configuración al usuario. Existen varias interfaces, para este trabajo hemos utilizado LuCi. También tenemos la opción de configurar el router mediante comandos empleando la terminal. Debido a que está basado en Linux, los comandos son los mismos que en plataformas más conocidas como Ubuntu. El empleo de la terminal presenta ciertas ventajas al usuario ya que, aunque la presentación es menos

clara, es más rápido y consume menos recursos de la memoria del router. OpenWrt permite el acceso a la interfaz gráfica mediante HTTP, y HTTPS en routers con capacidad para almacenar las librerías HTTPS. El router empleado no tiene la capacidad de memoria necesaria para soportar HTTPS.

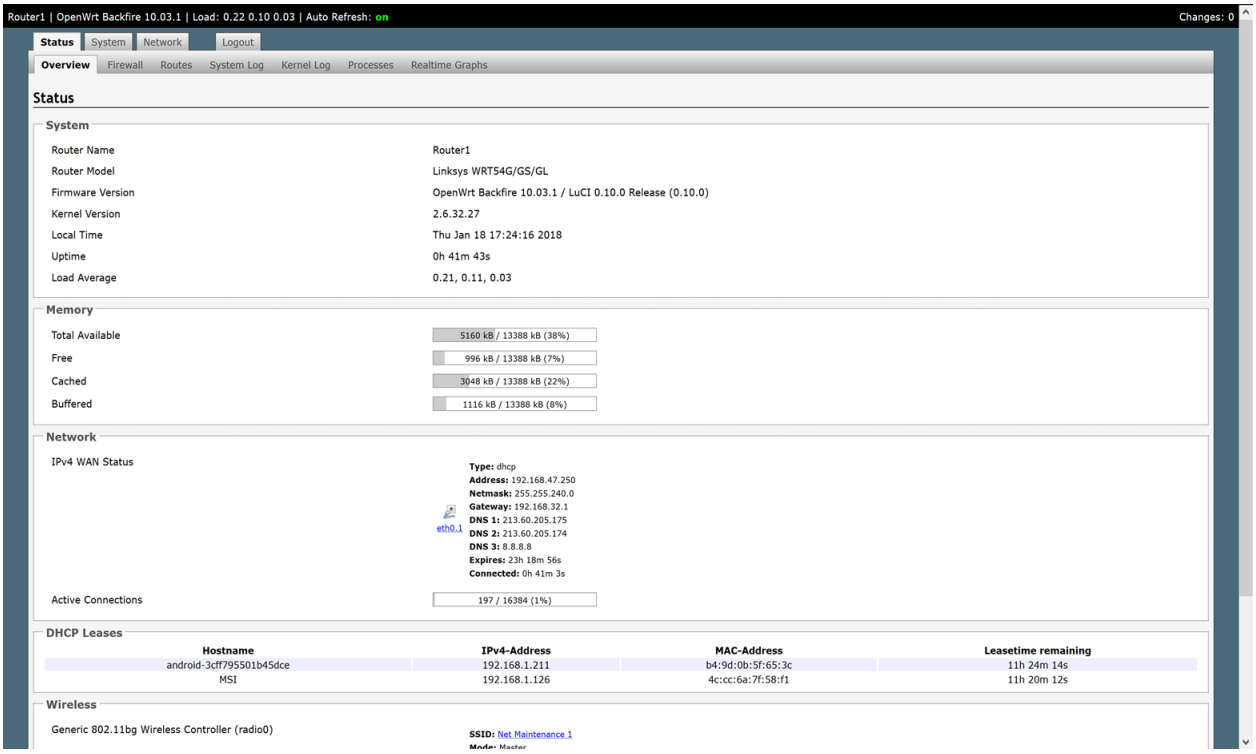


Figura 3-3 Interfaz gráfica LuCi

En la Figura 3-3 podemos ver cómo se presenta la información con la interfaz gráfica para la configuración del router. Las modificaciones que realizamos en esta página se pueden hacer mediante la terminal con un editor de texto modificando los distintos archivos de configuración. Este modo de proceder presenta la desventaja de que cualquier error de sintaxis puede provocar errores en el router.

En nuestro caso particular, al tener que realizar una configuración segura siguiendo la guía CCN-STIC-816, y no poder acceder a la web de configuración vía HTTPS, accederemos a los routers empleando el *software* PuTTY. Éste nos permite acceder a los routers utilizando dos métodos distintos, la terminal y un túnel SSH para acceder a la web. A continuación, se explicará cómo es el acceso a los routers mediante PuTTY.

En la Figura 3-4 se muestra la ventana principal de PuTTY tras haber configurado el acceso a los cuatro routers y haber creado un túnel SSH (*OpenWrt Luci Tunnel*) para conectar a la web LuCI de forma segura. El último de los métodos de acceso no se empleará debido a que necesitamos desactivar el acceso HTTP, no seguro, a la interfaz gráfica. Desactivar la interfaz web hace inservible el túnel SSH.

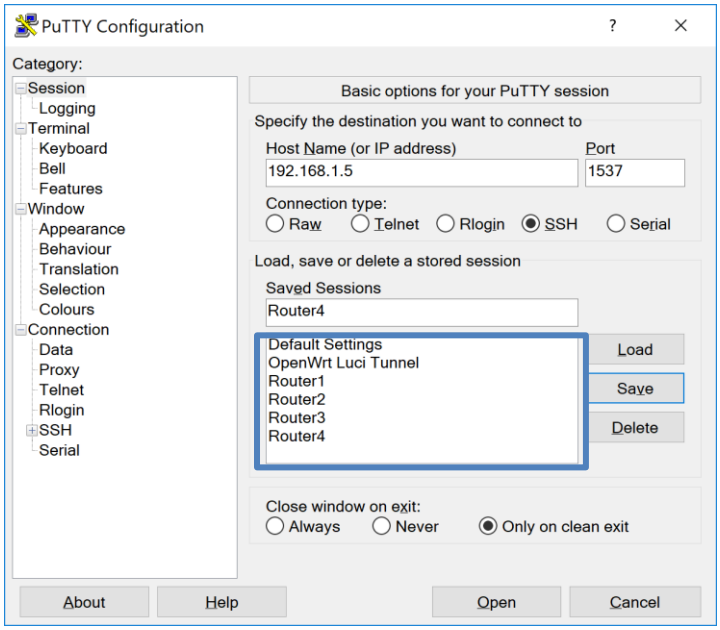


Figura 3-4 Ventana principal PuTTY

Seguidamente, se explicará cómo se debe configurar PuTTY para acceder a los routers. En la Figura 3-5 se muestra cómo se accedería al Router 1.

- *Host Name (or IP address)*, introducimos la dirección IP del Router 1 (192.168.1.2) o el nombre del router (Router1).
- *Port*, indica el puerto por el que nos conectaremos al router, 1537. No se emplea el puerto tradicional 22 ya que se cambió en el router el puerto de acceso mediante SSH.
- *Connection type*, de las cinco opciones que se presentan se han empleado dos para acceder a los routers SSH y Telnet. Telnet se emplea la primera vez que se accede al router, cuando aún no se establecido una contraseña de acceso. SSH se emplea a partir del establecimiento de una contraseña.

Para evitar tener que introducir continuamente los datos para acceder a los routers, podemos guardarlos en la aplicación. Para ello introduciremos un nombre en *Saved Sessions* y haremos click en *Save*.

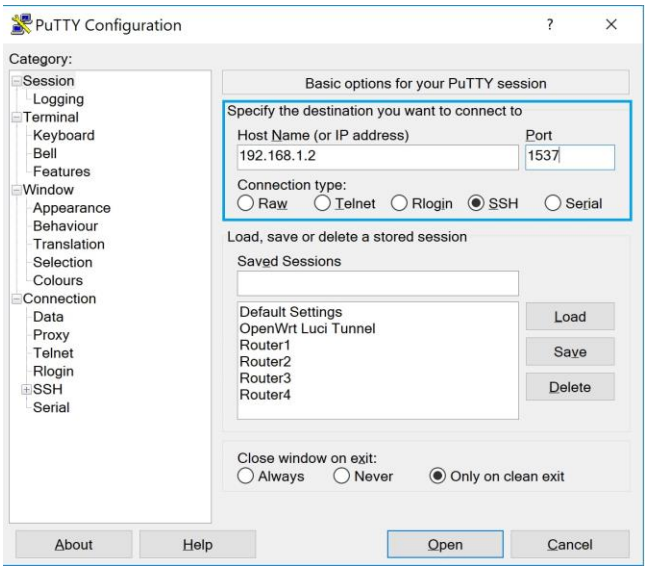


Figura 3-5 Acceso a Router 1 vía PuTTY

Una vez guardados los routers para acceder a ellos, los seleccionamos en la lista y hacemos click en *Open*. De esta forma entraremos en la terminal de OpenWrt. Primero nos pedirá usuario (*root*) y contraseña (ver Figura 3-6).

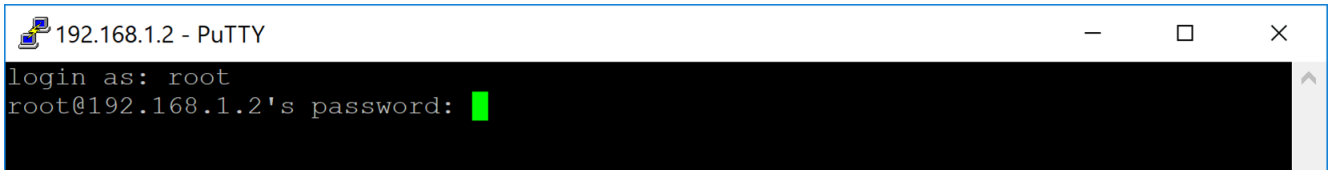


Figura 3-6 Autenticación para acceder a Router1

Una vez introducidos usuario y contraseña, pulsaremos *Enter* y aparecerá la ventana inicial del OpenWrt y la opción de introducir comandos (*root@Router1: ~#*) como se muestra en la Figura 3-7.

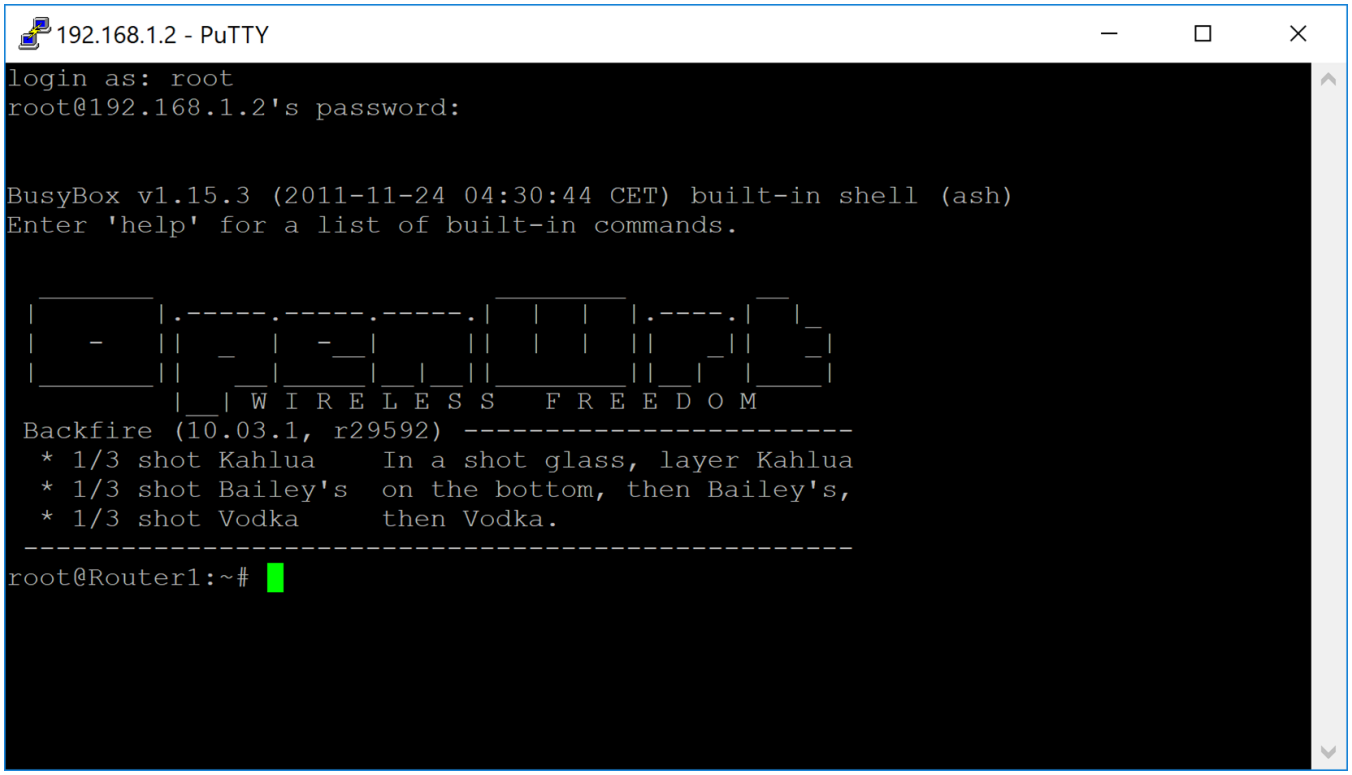


Figura 3-7 Ventana principal de la terminal OpenWrt

Como ya se ha mencionado, además del acceso a la terminal de los routers para su configuración, podemos emplear PuTTY para acceder a la web de forma segura creando un túnel SSH. Con la siguiente configuración se conducirá el tráfico desde el puerto 8000 de la dirección 127.0.0.1 de la máquina local al puerto 80 del router que tiene una dirección local 127.0.0.1. A continuación se muestra el proceso de configuración [46].

1. Navegar hasta *Connections -> SSH -> Tunnels* (Figura 3-8).

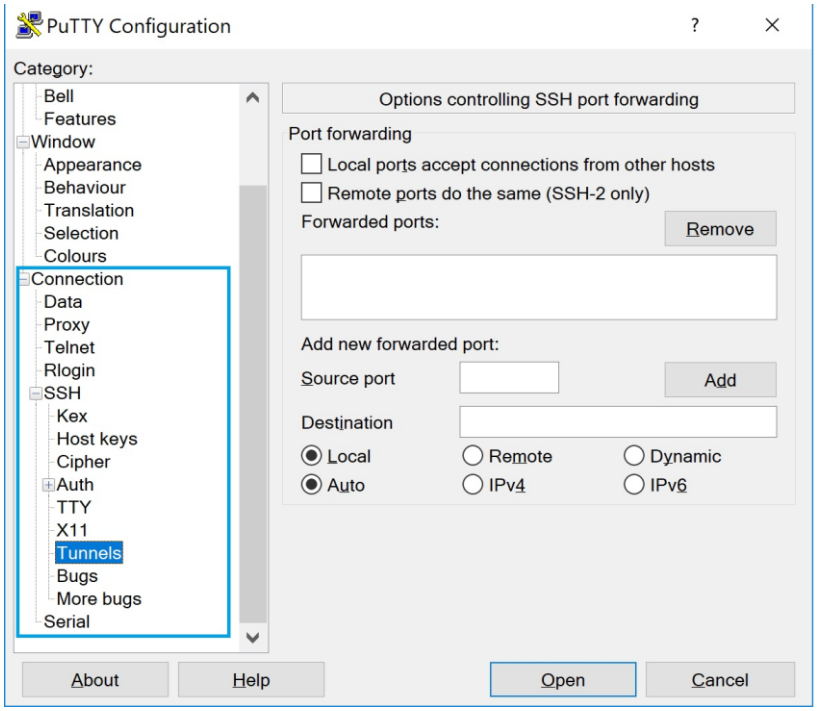


Figura 3-8 Configuración túnel SSH, paso 1

2. Añadir 8000 en el campo *Source port* y 127.0.0.1:80 en *Destination field* (Figura 3-9).

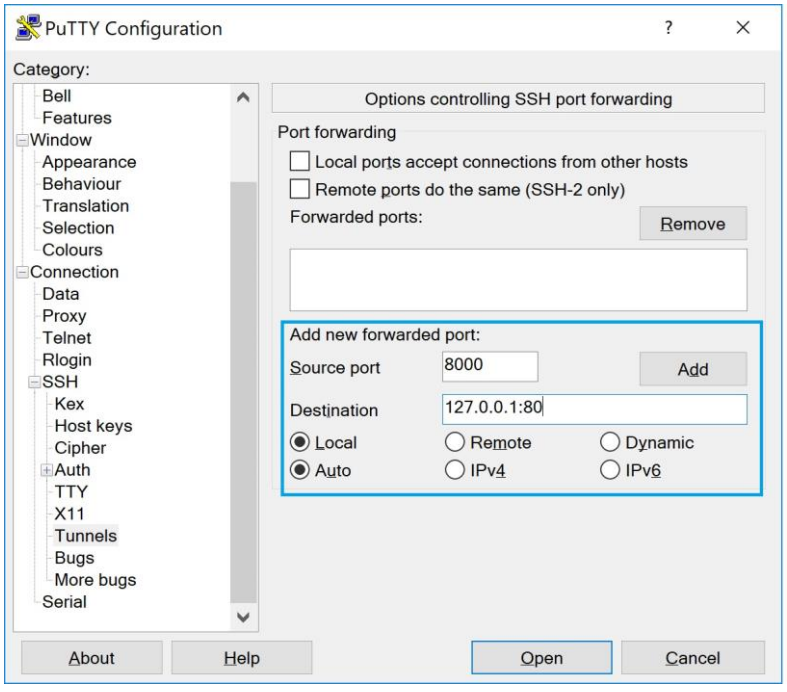


Figura 3-9 Configuración túnel SSH, paso 2

3. Hacemos click en *Add* y veremos cómo aparece en la sección *Forwarded ports* L8000 127.0.0.1:80 (Figura 3-10).

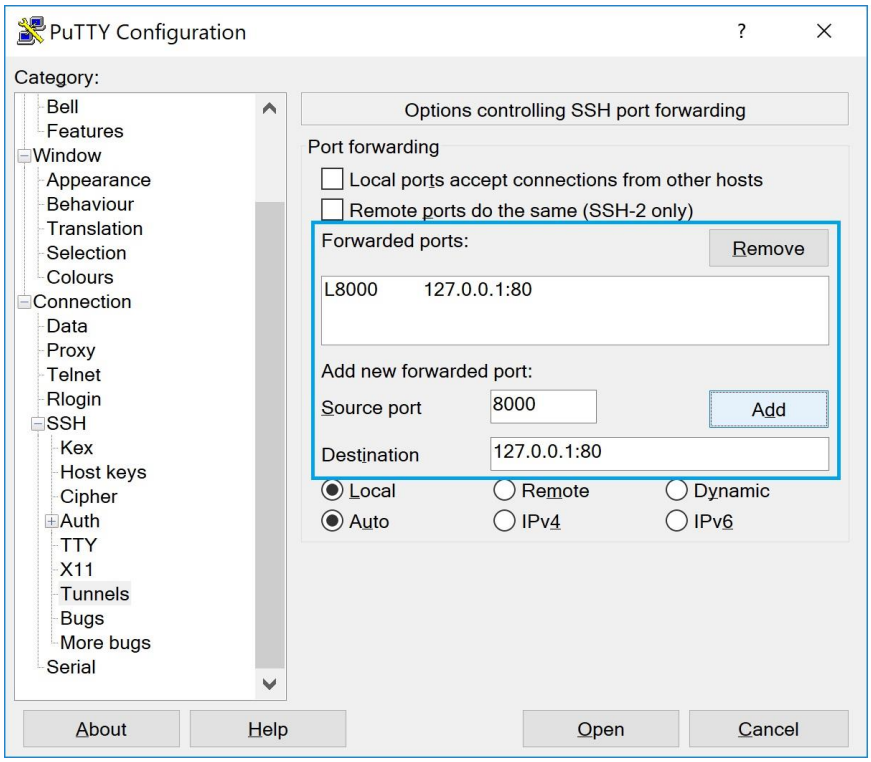


Figura 3-10 Configuración túnel SSH, paso 3

4. Navegaremos hasta *Session*. Añadiremos *root@Router1* en *Host Name* y 1537 en *Port* (Figura 3-11).

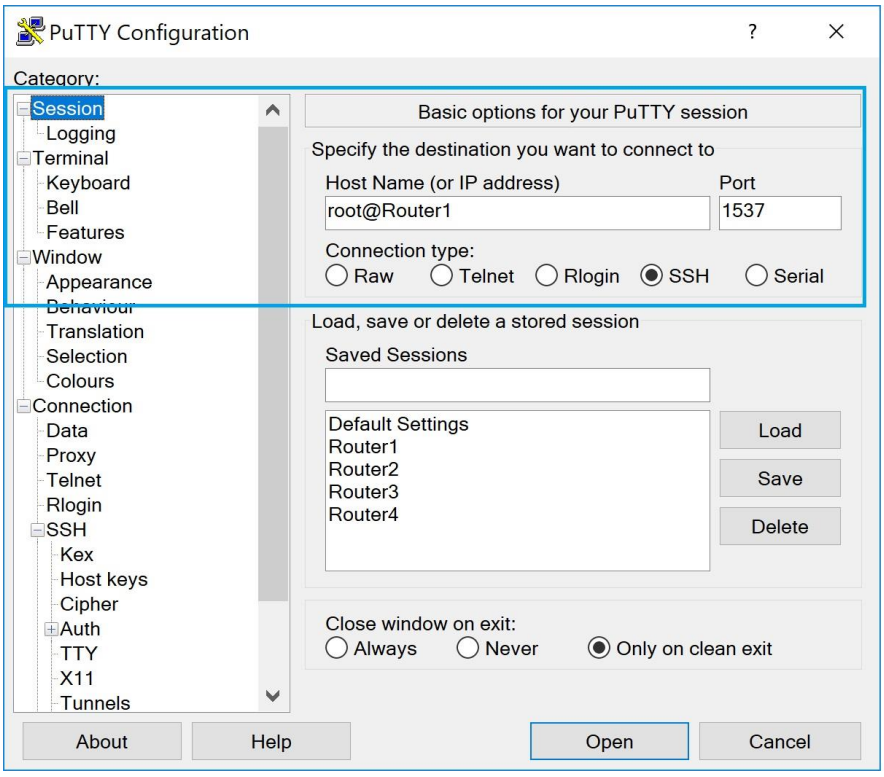


Figura 3-11 Configuración túnel SSH, paso 4

5. Añadimos *OpenWrt Luci Tunnel* en el campo *Saved Sessions* y hacemos click en *Save*.
6. Iniciaremos sesión seleccionando *OpenWrt Luci Tunnel* y pulsando *Open*.
7. En la terminal introduciremos el usuario y contraseña del router.

8. Manteniendo abierta la terminal, usando nuestro navegador web con la dirección *127.0.0.1:8000* accederemos a la interfaz gráfica (Figura 3-12).

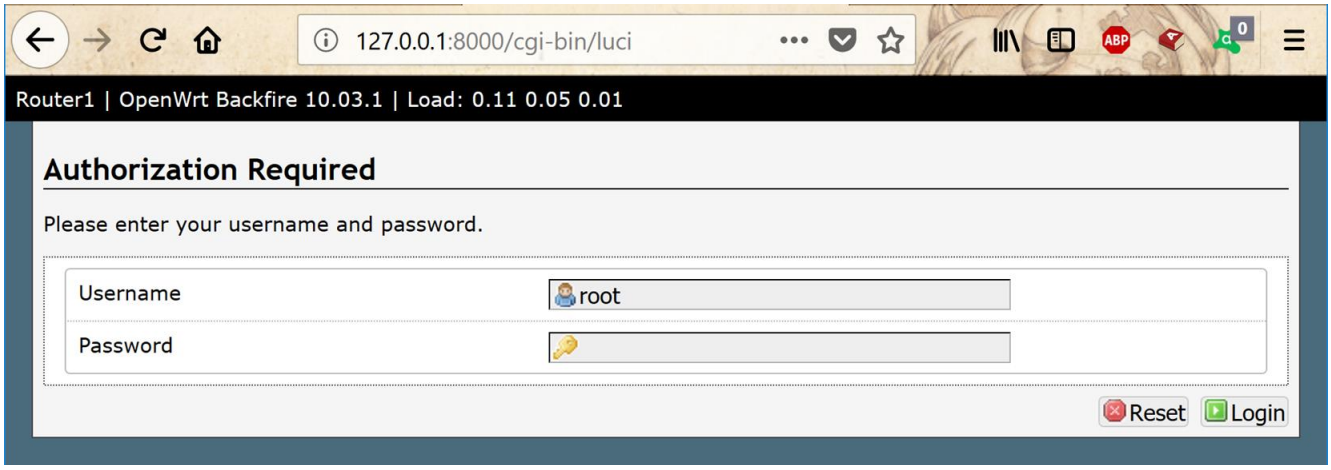


Figura 3-12 Acceso a LuCI con túnel activado

Más adelante, en el capítulo de validación de la red, se verá cómo esta medida nos permite acceder a la web sin filtraciones de seguridad.

OpenWrt tiene un gestor de paquetes, como se dijo anteriormente, que nos permite descargar aplicaciones para aumentar o complementar las capacidades de nuestro router, como pueden ser las librerías para HTTPS, la posibilidad de añadir un Servidor de Autenticación como FreeRADIUS o simplemente activar la opción UPnP (*Universal Plug and Play*). Estos paquetes enriquecen el *firmware* OpenWrt y empleando el *firmware* original del fabricante no podríamos utilizarlos.

Parte de estos paquetes están orientados a la implementación de seguridad en nuestros routers y en nuestras redes, faceta sobre la que cada vez se tiene una mayor concienciación.

3.2 Propósito de la red inalámbrica planteada y establecimiento del nivel de seguridad

En este apartado se analiza qué tipo de red inalámbrica se simula (una red WiFi para su empleo en el Centro Universitario de la Defensa) y el nivel de seguridad en el que se categoriza la red según el ENS.

Para la configuración de la red tendremos en cuenta que, aunque la red no llegue a instalarse de forma funcional, se trataría de una red WiFi de uso en el Centro Universitario de la Defensa. La configuración se realizará en base al Esquema Nacional de Seguridad, adoptando las medidas que se determinan para una red de categoría MEDIA. En los siguientes párrafos se expondrán y desarrollarán los motivos por los que se valora la red en esta categoría.

Para determinar la categoría de una red inalámbrica como sistema de información dentro del ENS, habrá que considerar la criticidad de los recursos y servicios de la organización con los que se establece la comunicación a través de ella, y la criticidad de la información que fluye a través de sus conexiones.

Esta criticidad se basa en la medición de una serie de criterios, aplicable a cada una de las propiedades de seguridad citadas anteriormente en el apartado 2.4: integridad [I], confidencialidad [C], autenticidad [A], trazabilidad [T] y disponibilidad [D].

Es la valoración de las consecuencias de un impacto negativo sobre la seguridad que afecte a las dimensiones de seguridad de estos servicios, recursos e información lo que determinará la categoría de la red inalámbrica, pudiendo ser de categoría BÁSICA, MEDIA o ALTA.

Se estudiarán las propiedades de seguridad de forma independiente y atendiendo a los criterios de valoración de la Guía CCN-STIC-803, valoración de los sistemas [38], y se particularizará el estudio en el ambiente universitario, basándose en el Anexo I de dicha guía, que se refiere a redes inalámbricas de área local en el ámbito universitario [42]. Cada propiedad se clasificará en BAJA, MEDIA o ALTA y la clasificación global del sistema será la más alta presente entre las cinco propiedades. Se muestra en la Tabla 3-2 la categorización de las distintas características de seguridad para una selección de tipos de información y servicios que la red del CUD maneja.

	I	**C**	**A**	**T**	**D**
Información - Expedientes administrativos	BAJA	BAJA	BAJA	BAJA	BAJA
Información - Expedientes académicos	MEDIA	MEDIA	MEDIA	MEDIA	MEDIA
Servicio - Plataforma de Docencia Virtual	-	-	-	-	BAJA
Clasificación sistema global			MEDIA		

Tabla 3-2 Tabla resumen de la clasificación del nivel de seguridad

En el caso de los expedientes administrativos y académicos la valoración de los distintos criterios coincide con lo que marca el Anexo I de la guía CCN-STIC-803. Sin embargo, en el del servicio de Docencia Virtual, se difiere con lo que refleja la guía, ya que ésta le da una clasificación en disponibilidad MEDIA. En el caso del CUD se determina que la criticidad es BAJA debido a que las clases de los alumnos son presenciales, por tanto, la pérdida de la plataforma en un momento puntual no es tan grave como si las clases se impartieran a través de ese medio.

La categorización del sistema da lugar a una serie de medidas que se deben aplicar para alcanzar el nivel de seguridad definido.

La primera medida a tomar, según la guía CCN-STIC-816 [14] es la de crear una Política de seguridad de la red inalámbrica, que junto a las decisiones que tome la organización para forzar su cumplimiento, será la base para todas las medidas de seguridad. Se tendrá en cuenta que en este proyecto se simula una red de trabajo en el entorno del CUD, así que, la normativa se orientará a esa aplicación.

Los siguientes apartados representarían la política de seguridad de la red inalámbrica, sin embargo, en nuestro caso, en lugar de ser un documento de requerimientos, también incluye cómo se instaurarán en nuestra red.

3.2.1 Uso aceptable de la red inalámbrica

Se considerará la red como una red de trabajo, por lo que cada usuario será responsable del uso que dé a dicha red. El uso aceptable incluye el uso de recursos compartidos del propio Centro Universitario de la Defensa, así como el acceso a páginas web de entorno académico y de investigación. En caso del incumplimiento de las directrices anteriores se puede llegar a retirar el acceso a la red inalámbrica durante un período a determinar por el administrador acorde con la infracción cometida.

Cada usuario que quiera acceder a la red deberá ser dado de alta previamente, indicando cuántos dispositivos quiere utilizar y proporcionando la dirección MAC de cada dispositivo. Una vez registrados los dispositivos, se le asignará un nombre de usuario y contraseña para el acceso a la red. Los dispositivos clientes deben disponer de soporte del protocolo IEEE 802.1x/EAP para poder acceder a la red en las condiciones de seguridad establecidas.

Se recomienda a la organización la distribución de equipos corporativos debidamente configurados para el uso seguro de la red.

3.2.2 Requisitos de seguridad de la infraestructura inalámbrica

Para establecer una red inalámbrica que sigue los requisitos del ENS se tomaron diversas medidas a distintos niveles.

REQUISITO 1: ARQUITECTURA DE SEGURIDAD

Para la cual se tienen en cuenta dos parámetros.

- Cobertura de los puntos de acceso, limitando la radiación de estos fuera del perímetro controlado por la organización. En nuestro caso se limita al Hall y al ala Este del cuartel de alumnos Marqués de la Victoria (a partir de ahora, MdV). En la Figura 3-13 se muestra la zona que se cubre. Para ello combinamos la ubicación física de los routers con la dirección y potencia de radiación, lo que nos da la cobertura final de la red inalámbrica.
- La red inalámbrica se constituyó en modo infraestructura, lo que nos permite configurar y estandarizar la seguridad a desplegar en los AP. Se tomó esta opción frente a la distribución ad-hoc, que presenta una configuración más difícil de controlar y con una mayor vulnerabilidad a los ataques.

Figura 3-13 Zona de cobertura MdV

REQUISITO 2: MÉTODO DE AUTENTICACIÓN

En este apartado se decide qué tipo y mecanismo de autenticación se va a usar, así como el método EAP. Todas estas decisiones se basan en que la red objeto tiene una clasificación de seguridad MEDIA.

- **Tipo de autenticación**: se empleará el basado en el estándar 802.1x/EAP, que nos permite un proceso explícito de autenticación mutua, en el que cada cliente dispondrá de sus propias credenciales de acceso, proporcionando trazabilidad. Es un método más seguro que el empleo de una clave precompartida. Este método es utilizado por WPA y WPA2 en su versión *Enterprise*.
- **Mecanismo de autenticación**: debemos emplear la autenticación de doble factor, que en nuestro caso serán contraseñas y usuarios concertados. Estas contraseñas tendrán un nivel de seguridad que cumplirá los siguientes requisitos: longitud mínima de 16 caracteres, empleo de mayúsculas y minúsculas, al menos un número y un signo ortográfico. Las

contraseñas serán expedidas por el administrador, deberán renovarse de forma cuatrimestral, intentando hacerlo coincidir con cambios de cuatrimestre académicos.

- **Método EAP**: la guía determina que los únicos métodos que soportan los requisitos obligatorios para redes inalámbricas indicados en la RFC 4017 son los EAP basados en TLS. En nuestra configuración emplearemos PEAP (*Protected Extensible Authentication Protocol*).

REQUISITO 3: ACCESO AL ROUTER

El acceso local para los administradores de los puntos de acceso se realizará por medio de SSH debido a la clasificación MEDIA de la red y a que los routers empleados no soportan las librerías para SSL/TLS (que permitirían el acceso por HTTPS) debido a las limitaciones de memoria que presentan. Como medida adicional, se deshabilitará cualquier otro protocolo de gestión inseguro que, en nuestro caso, es la interfaz gráfica web, solo accesible por HTTP.

Solo los administradores tendrán acceso a la administración del AP. Los accesos, así como las actividades realizadas durante los mismos, deben quedar registrados.

Otra medida que se debe tomar es cambiar el puerto de acceso mediante SSH al router, no dejar el puerto 22 que viene por defecto.

REQUISITO 4: DISPOSITIVOS CLIENTE

Respecto a los dispositivos cliente, atenderán a las consideraciones mencionadas en párrafos anteriores teniendo en cuenta, además, que:

- debe evitarse que los dispositivos establezcan conexiones duales ya que puede suponer una vulnerabilidad para la red inalámbrica (un *software* malicioso podría acceder por la otra conexión al dispositivo cliente).
- Se recomienda además que, en los equipos no corporativos, se empleen cortafuegos personales, ya que ayudan a evitar que otros usuarios de la misma red consigan acceso no autorizado al dispositivo.
- Se debe desactivar la conexión de red de forma automática para evitar conexiones a puntos de acceso falsos (*Rogue AP*).
- Es necesario el empleo del método EAP empleado por la arquitectura de autenticación.

REQUISITO 5: MÍNIMA FUNCIONALIDAD

Cambiando de ámbito y atendiendo al principio de mínima funcionalidad, deberán deshabilitarse todos los servicios y funciones del AP que no sean estrictamente necesarios. También debemos minimizar la superficie de exposición de la red para asegurar una mayor seguridad. Con respecto a las interfaces de gestión no seguras de las que pueda disponer el AP, es especialmente importante que sean deshabilitadas como se dijo anteriormente.

Dado que empleamos CCMP, se han deshabilitado las funciones de seguridad que no deben usarse (WEP y TKIP) para prevenir su uso.

REQUISITO 6: MODIFICACIÓN PARÁMETROS POR DEFECTO

Los parámetros por defecto de los routers deberán ser modificados, asignándose el valor apropiado en campos como dirección IP de acceso al router, usuario y contraseña de administración. Se establecerá un SSID a la red WiFi que no aporte información de la organización (por ejemplo, Red TFG). Se deben revisar las configuraciones de los AP después de cierto tipo de reinicios, porque se puede establecer de nuevo la configuración por defecto.

REQUISITO 7: OCULTAR SSID

De forma disuasoria, podemos ocultar la emisión del SSID por parte del AP para que solo se puedan conectar a la red inalámbrica si el SSID ha sido especificado explícitamente. Aún así podría ser detectada con escáneres de red como, por ejemplo, Kismet.

REQUISITO 8: FILTRADO MAC

Se creará una lista de direcciones MAC, de forma que solo los dispositivos cuya dirección MAC se encuentre en la lista autorizada pueda acceder a la red inalámbrica. Esta medida no evita que un potencial atacante pueda suplantar una de las direcciones MAC autorizadas (MAC *Spoofing*).

REQUISITO 9: HORARIO OPERATIVO

Se establecerá un horario operativo en el que los AP estarán encendidos, para evitar que en horario no laborable puedan ser atacados. En nuestro caso particular debería evaluarse esta opción en detalle. Debido a la idiosincrasia del CUD, y la flexibilidad de horario del profesorado, el apagar los routers a una hora determinada y dejar sin servicio a algún profesor puede ser más perjudicial que el riesgo de un ataque fuera de horario.

Se limita el tiempo de sesión a seis horas, considerando ésta la duración máxima del periodo de la mañana, que será el periodo de conexión ininterrumpido más prolongado. Sobrepasado el tiempo máximo de sesión, la asociación será disuelta por el AP y el cliente deberá reautenticarse.

REQUISITO 10: SERVIDOR DE AUTENTICACIÓN

Debido a este nivel MEDIO es necesario el empleo de un servidor de autenticación. En nuestro caso utilizamos un ordenador portátil multipropósito. En caso de ser un servidor de autenticación real y dedicado, debería estar adecuadamente bastionado y protegido.

REQUISITO 11: REGISTRO DE ACTIVIDAD

En lo que respecta a la actividad de los usuarios en la red inalámbrica, en especial a la de los administradores, deberá ser registrada para posibles análisis posteriores. Como mínimo se requiere de un registro detallado de los intentos de conexión exitosos y fallidos. Este registro permite la trazabilidad de acciones y proporciona información que podrá ser revisada en caso de actividades maliciosas. Esta función estará habilitada en los AP y en el servidor de autenticación.

En nuestro caso, se realizarán revisiones de los registros de actividad con objeto de identificar problemas de seguridad y tomar las acciones correctivas cuanto antes en auditorías de seguridad. La periodicidad de estas revisiones quedará a criterio del administrador.

REQUISITO 12: ROUTER MASTER

Para la creación de la infraestructura se establecerán tres AP, de los cuales solo uno será *Master* y el resto serán esclavos. Será el AP *Master* el que gestione toda la información que proviene de los routers esclavos. La creación de dicha infraestructura se detallará más adelante en la memoria, siempre teniendo presente que se trata de una simulación de una red real.

REQUISITO 13: MONITORIZACIÓN DE LA RED

La monitorización de seguridad se llevará a cabo de forma automática a través de Sistemas de Detección Inalámbrica de Intrusos, WIDS (*Wireless Intrusion Detection Systems*). Nuestra red empleará el *software* Kismet [47], cuyo servidor y cliente se establecerá en el portátil multipropósito, y en el cuarto router se instalará un dron que enviará la información detectada al servidor.

REQUISITO 14: ASEGURAR EQUIPOS IoT

Aunque la guía no lo mencione, se debe tener en cuenta la vulnerabilidad de elementos conectados a la red para su uso compartido como, por ejemplo, una impresora. En el caso del CUD existe una

impresora conectada a la red a la que se ha desactivado la opción de acceder a ella de forma inalámbrica. Así se dificulta el acceso a posibles atacantes.

3.3 Configuración de la red

3.3.1 Instalación de la red WiFi

Para la implantación de la red se emplearán cuatro routers, de los cuales uno sirve como monitor WIDS. En primer lugar, se explicará la instalación de la red WiFi, exclusivamente.

La intención inicial de la instalación fue desplegar los routers desde la habitación F-3. Se hubiera dejado el router *Master* en dicha habitación y se hubieran desplegado los otros dos routers por el pasillo conectándolos sucesivamente uno a otro. Se hubiera cubierto la misma extensión que se pretende. Sin embargo, la limitación de cable de red disponible hizo que se planteara la opción que se empleó definitivamente.

El esquema de instalación que seguiremos será el mostrado en la Figura 3-14. En él podemos ver que contamos con un Router 1, que funciona en modo *Master*, siendo el encargado de servicios tales como *Firewall* y DHCP. Está conectado por cable a Internet y a dos routers (2 y 3) que trabajan en modo *Slave* (esclavo) dependiendo del Router 1. Los tres routers funcionan como puntos de acceso que permiten la conexión a la red inalámbrica denominada Red TFG.

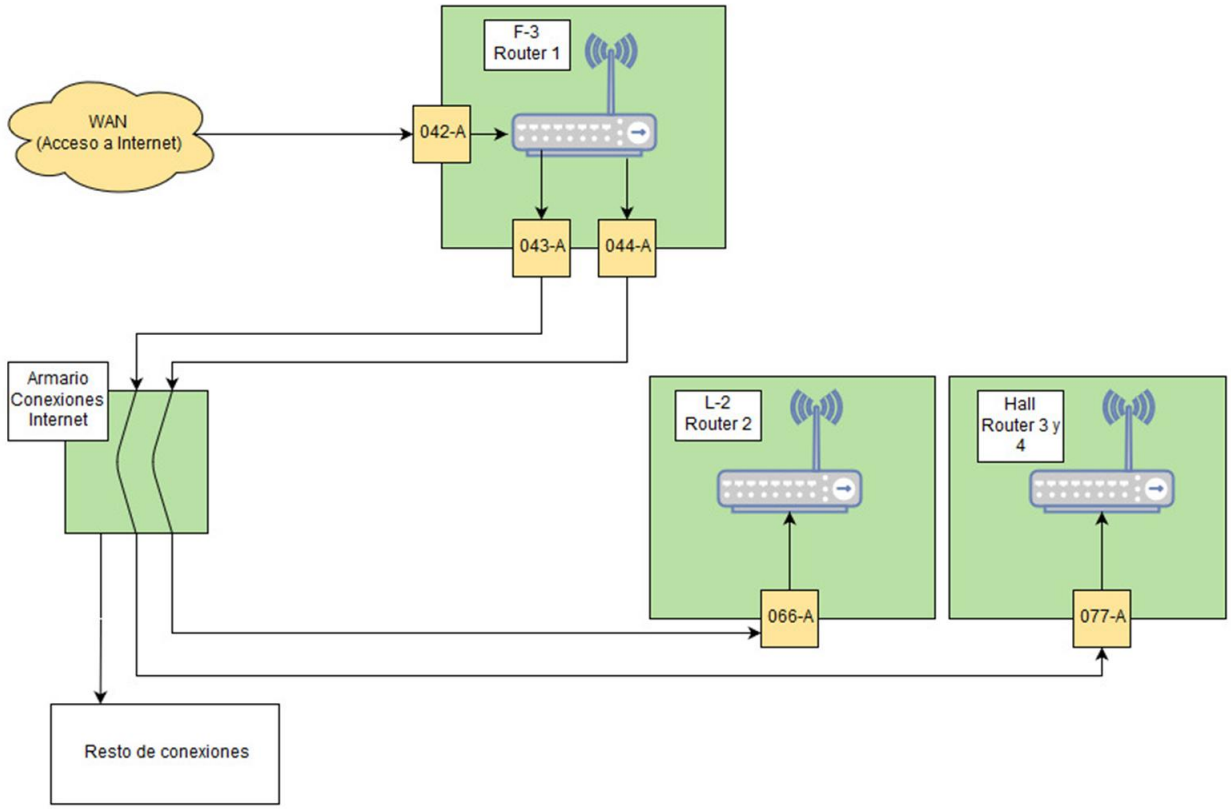


Figura 3-14 Esquema de configuración de red

Los routers se desplegaron de la siguiente manera: en la segunda planta del cuartel MdV, en la habitación F-3 (ver Figura 3-15) se situó el Router 1 que se conectó a la toma de red 042-A para acceso a Internet. Este router además actúa como *Master* para acceso de los otros routers esclavos conectados por las tomas de red 043-A y 044-A de la propia habitación.

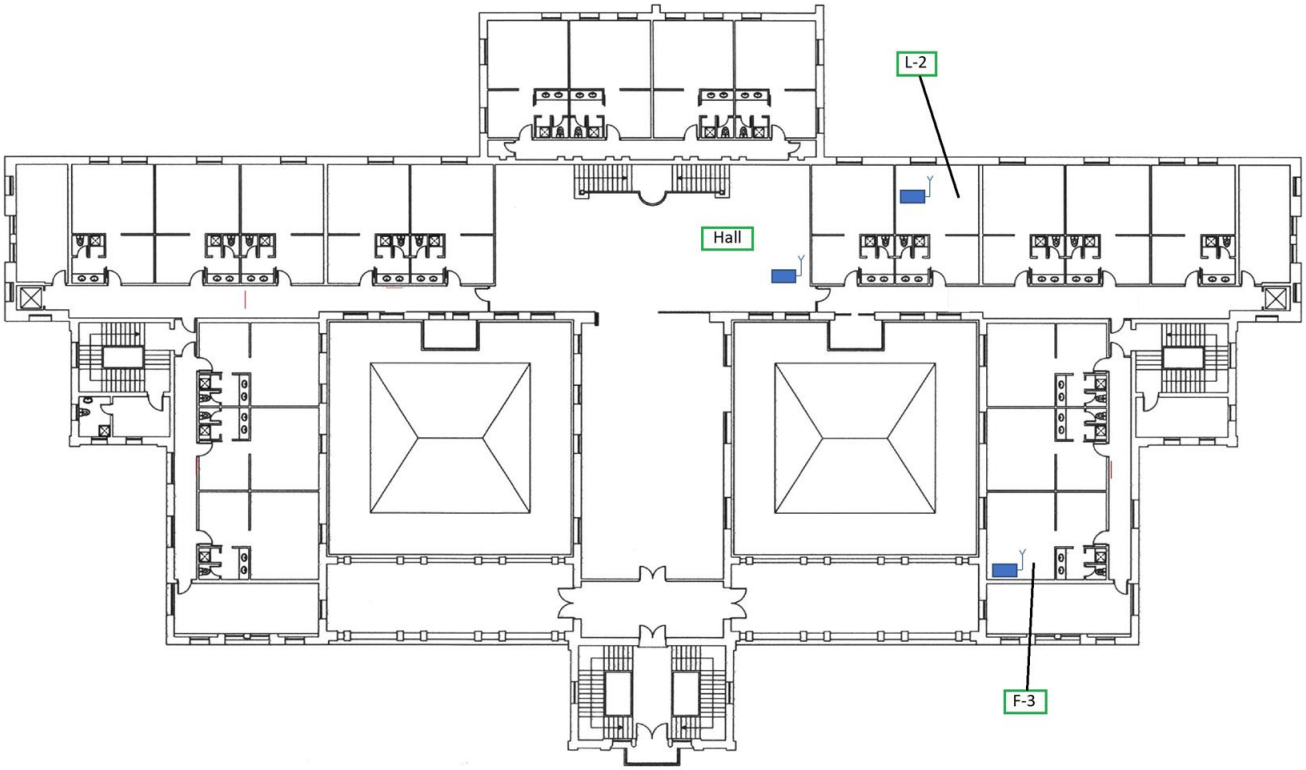


Figura 3-15 Distribución routers en MdV

Mediante un puente en el "Armario Conexiones Internet" se conectaron las tomas 043-A y 044-A a las tomas 077-A y 066-A, respectivamente, siendo el 077-A una toma ethernet situada en el Hall y 066-A la toma de la habitación L-2. De esta forma se aprovecha la red cableada del edificio para conectar los AP y dar cobertura WiFi al ala Este del MdV y al Hall en su totalidad (probablemente la cobertura sea mayor).

Sin contribuir a la cobertura de red propiamente dicha se instala un cuarto router que sirve como monitor de la red al completo. La instalación se realiza en la misma ubicación en la que se encuentra el router del Hall. La Tabla 3-3 resume emplazamiento de los routers y conexiones.

Router	Ubicación	Conecta con
Router 1	F-3	Routers 2 y 3
Router 2	L-2	Router 1
Router 3	Hall	Router 1
Router 4	Hall	Router 3

Tabla 3-3 Tabla resumen despliegue routers

A efectos de las conexiones propias de los routers, se sigue el esquema que se muestra a continuación (Figura 3-16), indicándose los puertos a los que va conectada cada toma de red anteriormente mencionada.

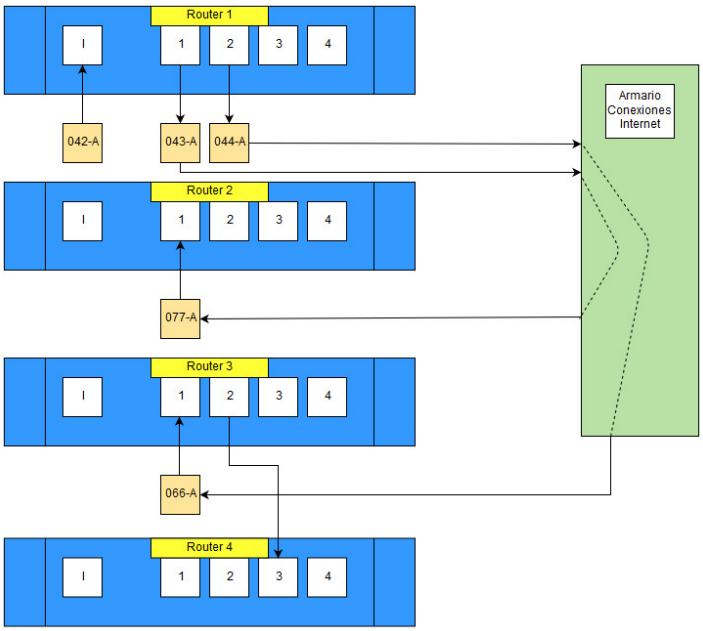


Figura 3-16 Conexiones routers

A continuación, se muestra dónde se realizó la instalación de cada router.

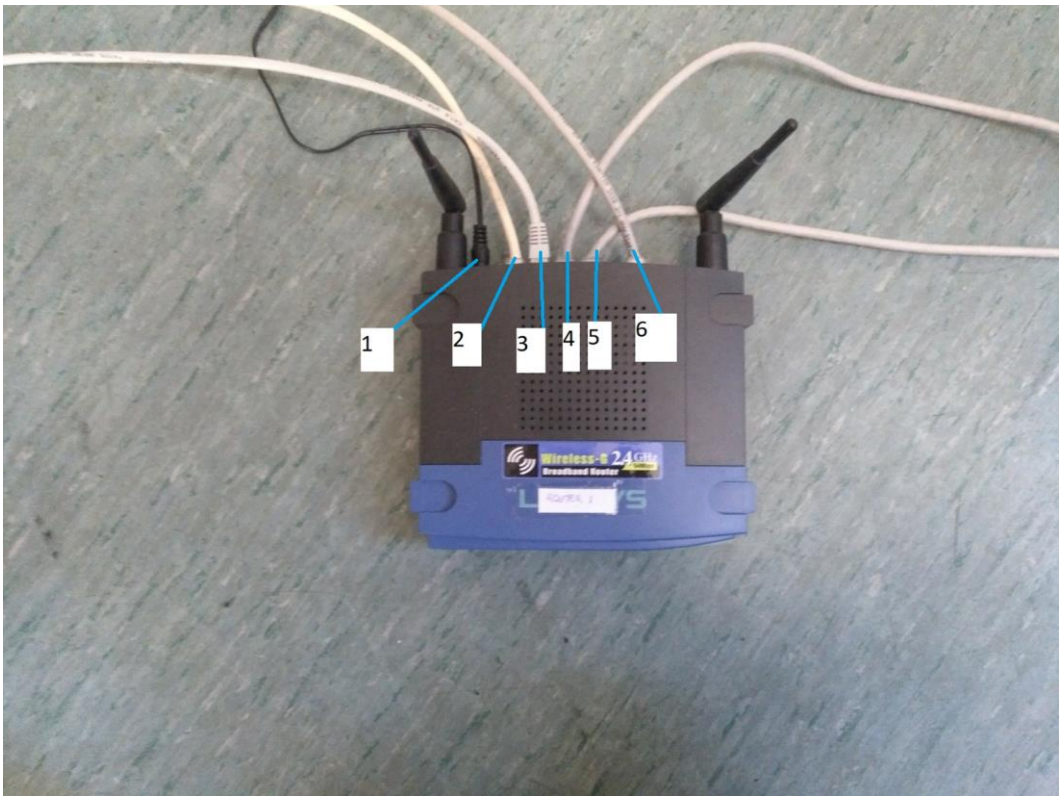


Figura 3-17 Detalle router F-3

La Figura 3-17 muestra el cableado del Router 1, en F-3:

1. Cable de alimentación.
2. Cable ethernet a portátil personal, desde el que se gestionan los routers.
3. Cable ethernet a portátil con Kali Linux, donde se encuentran instalados los diversos servidores.
4. Cable ethernet hasta la toma 044-A, que conecta con 066-A en la camareta L-2.

5. Cable ethernet hasta la toma 043-A, que conecta con 077-A en el Hall.
6. Cable ethernet hasta la toma 042-A, que conecta el router a la red WAN.

Se muestra en la Figura 3-18 y Figura 3-19 la ubicación en la habitación L-2 y en el Hall respectivamente. Los routers en el Hall sirven, uno como punto de acceso, y el otro como monitor de red para Kismet.

Figura 3-18 Router de L-2

Figura 3-19 Routers en el Hall

Tras instalar la red, se decide realizar un mapeado del área que cubren los routers para ver si dan servicio a la zona designada. También buscaremos posibles interferencias con la red *wificud*, que es la red desplegada en el cuartel MdV, para minimizarlas ajustando los canales de trabajo.

Para el mapeado se empleó el *software Ekahau HeatMapper* [48] y el resultado se puede ver en la Figura 3-20. Se puede observar que las habitaciones L-4 y L-5 son las que tienen una peor cobertura. Esto se podría solucionar situando el router de la habitación L-2 en la L-4. Fue por motivos ajenos a la instalación por lo que dejó en L-2. En la Tabla 3-4 se muestran los valores en dBm según los colores. La Tabla 3-5 muestra el nivel de calidad de una red WiFi según la señal recibida en dBm.

Una de las medidas de seguridad que propone la guía CCN-STIC-816 es limitar la superficie de exposición de la red WiFi. Por tanto, se procede a modificar la potencia de transmisión de los routers para ajustar la cobertura lo más posible al área designada.

Color	Nivel de señal en dBm
Rojo intenso	-95 a -88
Rojo	-88 a -80
Naranja	-80 a -72
Amarilla	-72 a -64
Verde	-64 a -56
Verde intenso	-56 a -48

Tabla 3-4 Leyenda de nivel de señal *Ekahau HeatMapper*

Nivel de calidad	Nivel de señal en dBm
Mínima aceptable	Mayor de -80
Normal-baja	-70 a -80
Bueno	-60 a -70
Idóneo	-40 a -60

Tabla 3-5 Nivel de calidad señal WiFi

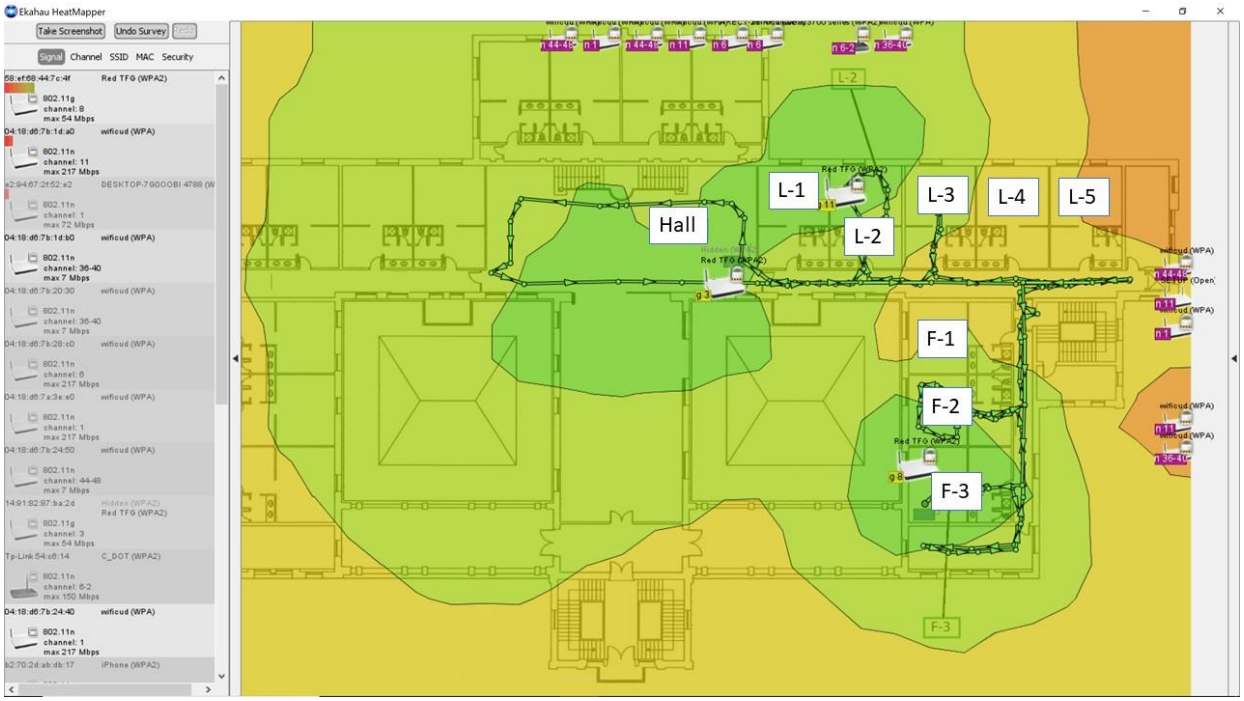


Figura 3-20 Mapa de calor de Red TFG (20 dBm)

Como vemos en la Figura 3-20, considerando buenas las zonas de color amarillo del esquema, la cobertura excede por mucho la zona que queremos cubrir. Nuestra intención es seguir ofreciendo una buena cobertura a nuestra zona, pero sin exponer tanto la superficie de la red.

Se procede a disminuir la potencia de los routers a la mitad y a volver a mapear la zona. En Figura 3-21 se puede ver cómo ha disminuido el área de cobertura de la red. Aunque la red siga cubriendo un área superior a la deseada, se decide no disminuir más la potencia para no privar de servicio WiFi a la habitación L-5, que se encuentra muy próxima a los límites de calidad asumibles.

De esta forma se llega a un compromiso entre QoS (*Quality of Service*) y seguridad.

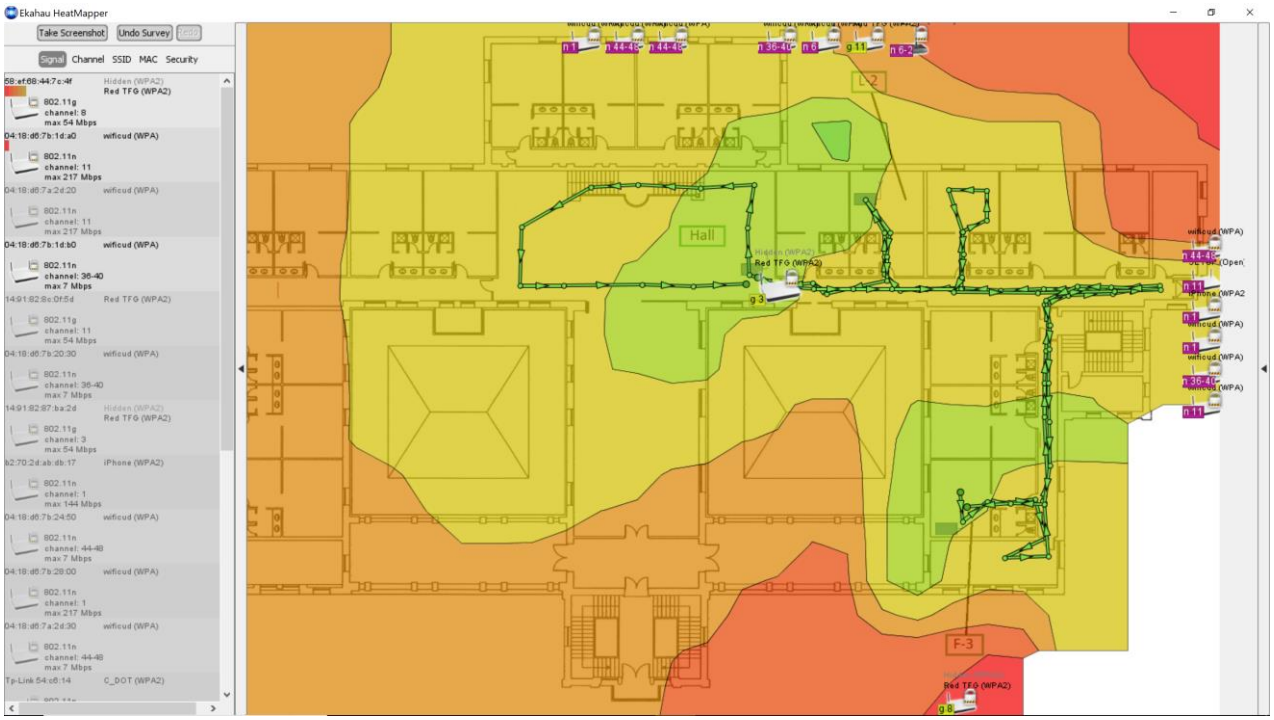


Figura 3-21 Mapa de calor de Red TFG (10 dBm)

En el mapeo de la red también se realiza un estudio de los canales. En base a ese estudio, se determinan los canales de los routers de la Red TFG para que no interfieran con la señal de los routers de *wificud*.

El criterio para la selección de los canales es dejar una diferencia de tres canales entre nuestro router y la red que más interfiera. Las redes interferentes son las segundas en la lista de cada router (ver Figura 3-22). Se puede ver que entre los routers de la Red TFG y los inmediatos en potencia de *wificud* hay, al menos, tres canales de diferencia.

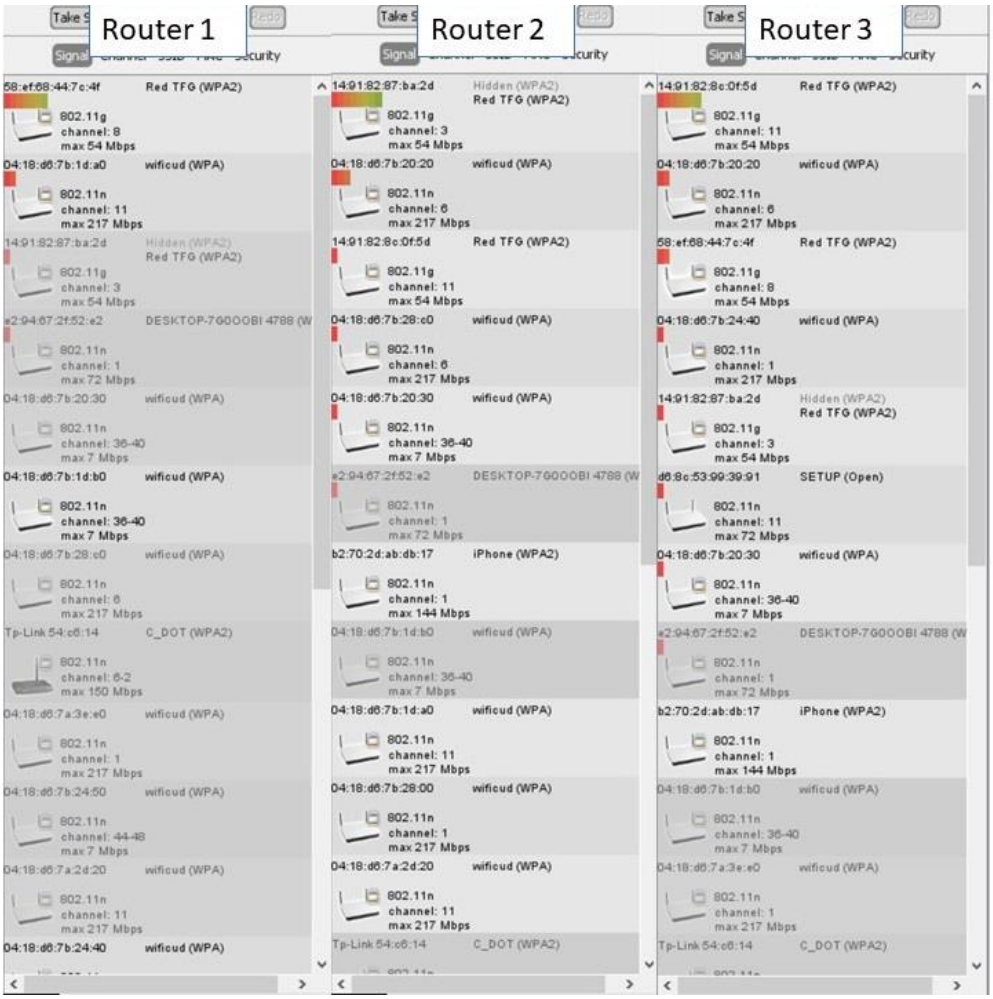


Figura 3-22 Canales de los routers obtenidos durante mapeo de la red

3.3.2 Securización de la red

Para configurar los parámetros de los routers se emplea el *software* PuTTY, mencionado en el apartado 3.1.2, para acceder a la terminal y configurar los routers. También hubiera sido posible el empleo del comando *ssh* en la terminal Linux. La configuración del router se realiza mediante la edición de ficheros de texto almacenados en el router. Se emplea el editor de texto *vim*, instalado de serie con el *firmware* OpenWrt.

A continuación, se presenta la configuración que se realiza para crear la red WiFi. Como medidas principales destacamos el cambio de los valores por defecto:

- Canal, aunque previamente se habló de ellos en la instalación, más adelante se explicará cómo modificarlos.
- SSID (*Service Set Identifier*).

- Añadir una contraseña mediante cifrado WPA2 y AES. El caso particular de nuestra red se empleará WPA2 *Enterprise*, en la que se otorga un nombre de usuario y contraseña a cada usuario.
- Se deshabilita WEP y TKIP.
- Se oculta la red a aquellos dispositivos que no tengan guardada la red.
- Se desactiva la interfaz gráfica LuCI, por no poder acceder vía HTTPS.
- Se añade filtrado por MAC.
- Cambio de puerto acceso a router de 22 a 1537.

La primera medida que realizaremos es cambiar el puerto de acceso al router modificando el archivo */etc/config/dropbear* y cambiando el puerto de 22 a 1537. Se muestra en la Figura 3-23 como queda el archivo de configuración.

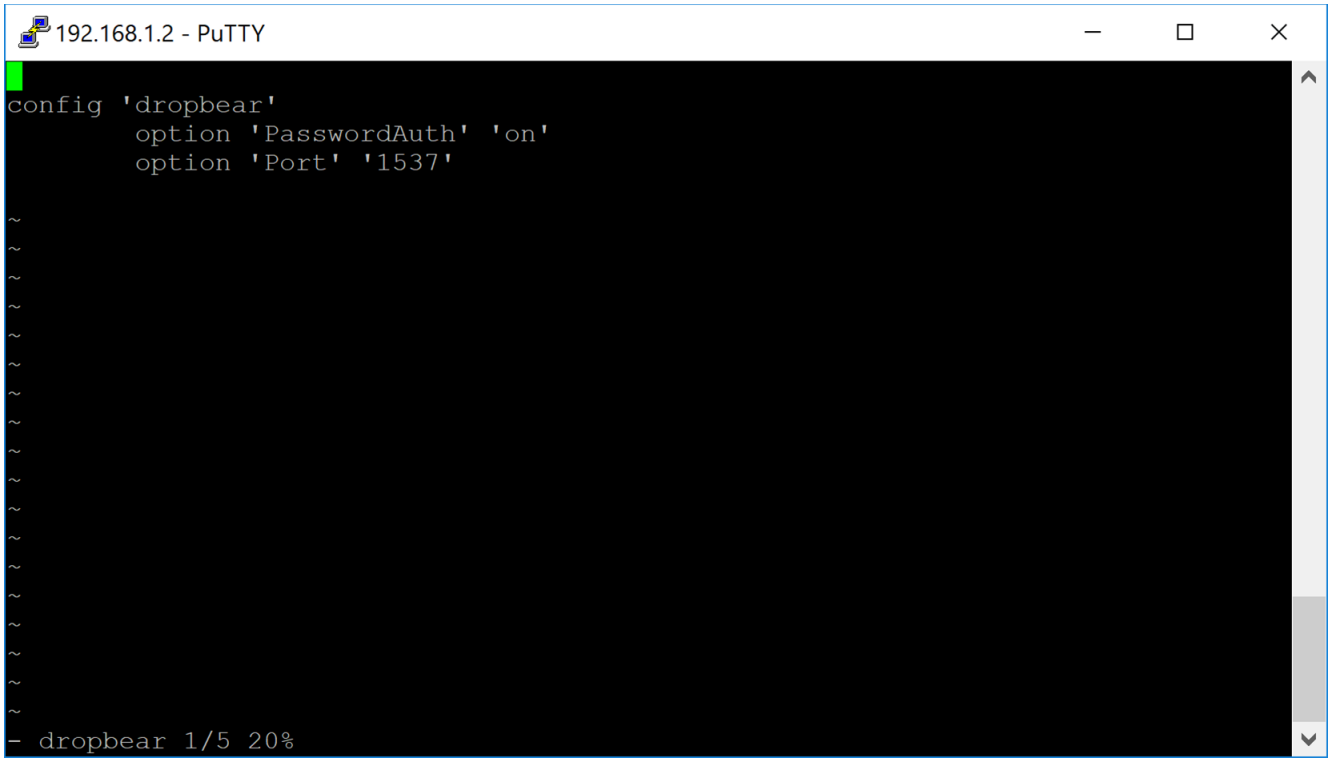


Figura 3-23 Configuración archivo *dropbear*

En la Figura 3-24 podemos ver cómo quedaría el archivo de configuración, el archivo */etc/config/wireless* de nuestro router.

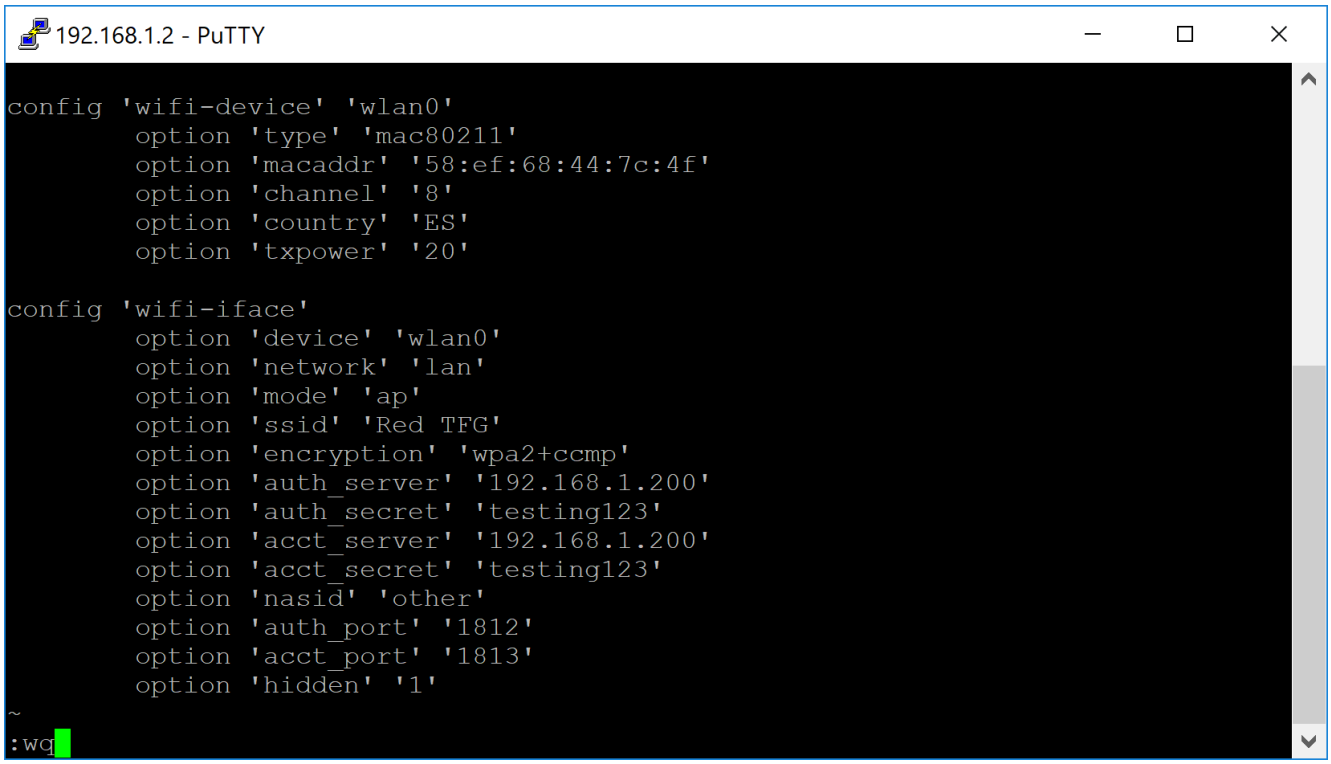


Figura 3-24 Configuración de la red WiFi

Con respecto a la configuración anterior, se procederá a explicar cada uno de los términos de configuración.

- *'wifi-device' 'wlan0'*, hace referencia al adaptador WiFi del router.
- *'type' 'mac80211'*, define el tipo de chipset [49] (*hardware* que actúa como placa base del centro de comunicaciones y control del tráfico del router).
- *'macaddr' '58:ef:68:44:7c:4f'*, define la dirección MAC del router.
- '*channel' '8'*, establece el canal de funcionamiento del router. Seleccionamos canal 8.
- *'country' 'ES'*, establece el país en que nos encontramos. ES indica que es España.
- *'txpower' '20'*, define el nivel de potencia del router en dBm. De momento se mantiene la potencia en 20 dBm (100 mW).
- *'wifi-iface'*, establece la interfaz de red del router.
- *'device' 'wlan0'* selecciona el adaptador WiFi anteriormente configurado.
- *'network' 'lan'* selecciona la interfaz de red a la que está conectado.
- *'mode' 'ap',* define el modo de operación del router. En nuestro caso, seleccionamos el modo punto de acceso (*Access point).* Existen otros modos de operación como modo cliente, ad-hoc, empleo de WDS, modo monitor y ofrece la posibilidad de configurar una red mesh.
- *'SSID' 'Red TFG'*, define el nombre de la red, Red TFG.
- *'hidden' '1'*, nos permite ocultar la emisión del SSID. Con valor 1 lo oculta y con 0 o eliminando la opción, la red vuelve a ser visible.

El resto de las opciones serán tratadas en el apartado 3.3.5 cuando se hable de FreeRADIUS.

Para añadir el filtrado MAC se añadiría la siguiente opción (ver Figura 3-25)

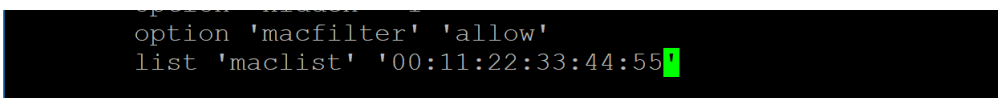


Figura 3-25 Filtrado MAC

Con *option 'macfilter' 'allow'* activamos el filtro MAC, autorizando a conectarse exclusivamente a las direcciones en la lista. Con '*list 'maclist' '00:11:22:33:44:55'*", se añaden las direcciones de los distintos equipos.

Con el comando '*# /etc/init.d/uhttpd disable'* se desactiva el acceso vía web al router (ver Figura 3-26).

```
root@Router1:~# /etc/init.d/uhttpd disable
```

Figura 3-26 Desactivación interfaz web

3.3.3 Dumb APs

Una vez configurado el router principal, debemos configurar los routers *Dumb*, que proporcionarán cobertura WiFi, pero a través del router principal sin enrutar o realizar otra función. Estos routers serán los routers 2 y 3 situados en el Hall y L-2, respectivamente.

Debemos conectarnos al punto de acceso mediante SSH. Configuraremos los AP 2 y 3 definiéndolos como un *Dumb* AP, es decir, estableceremos un modo "esclavo". Para ello accederemos al fichero de configuración de red y veremos los valores por defecto (Figura 3-27) [50].

```
config 'switch' 'eth0'
        option 'enable' '1'

config 'switch_vlan' 'eth0_0'
        option 'device' 'eth0'
        option 'vlan' '0'
        option 'ports' '0 1 2 3 5'

config 'switch_vlan' 'eth0_1'
        option 'device' 'eth0'
        option 'vlan' '1'
        option 'ports' '4 5'

config 'interface' 'loopback'
        option 'ifname' 'lo'
        option 'proto' 'static'
        option 'ipaddr' '127.0.0.1'
        option 'netmask' '255.0.0.0'

config 'interface' 'lan'
        option 'type' 'bridge'
        option 'ifname' 'eth0.0'
        option 'proto' 'static'
        option 'netmask' '255.255.255.0'
        option 'ipaddr' '192.168.1.3'

config 'interface' 'wan'
        option 'ifname' 'eth0.1'
```

Figura 3-27 Estado de configuración inicial de la red

Una vez abierto, modificaremos los parámetros, quedando la configuración como se muestra en la Figura 3-28.

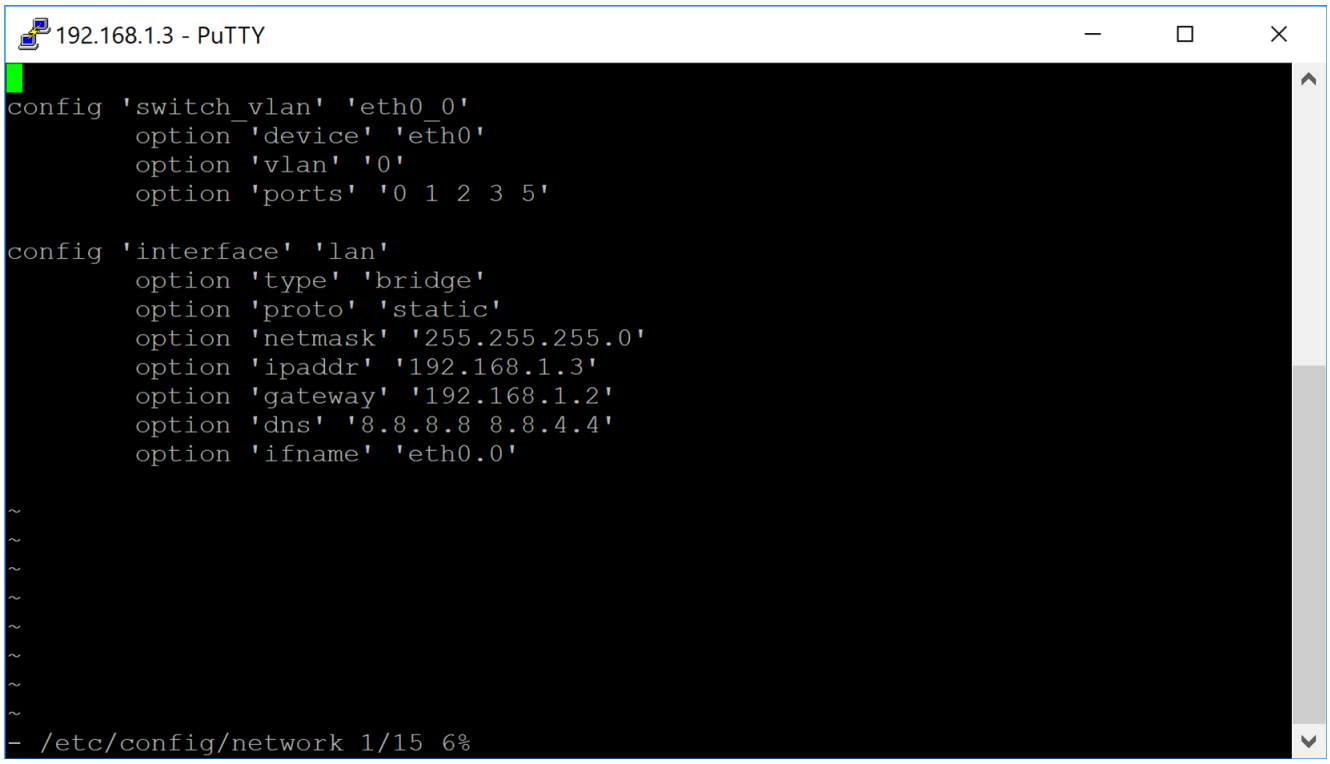


Figura 3-28 Configuración de red modificada

Con esta nueva configuración conseguimos transformar los routers *dumb* en un *switch* virtual junto con los puertos del router *Master*. Para ello se indica como *gateway*, puerta de enlace, la dirección del router *Master*. Al router se le añade una IP estática (192.168.1.3).

Una vez configurada la red cableada, procedemos a modificar la red *wireless* como se muestra en la Figura 3-29.

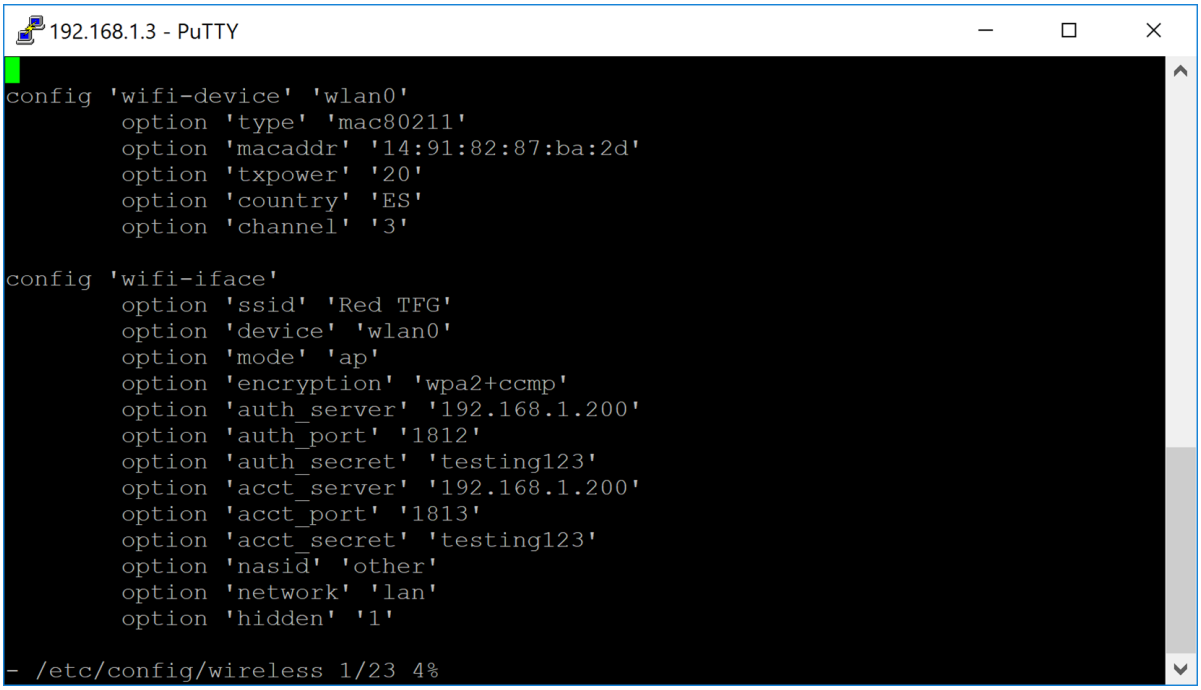


Figura 3-29 Configuración red *wireless*

Desactivaremos la función DHCP modificando el archivo *dhcp* en la carpeta */etc/config* (Figura 3-30). Se modifica en la sección *config dhcp wan* la opción *ignore* cambiando 0 por un 1.

```
config dnsmasq
        option domainneeded     1
        option boguspriv        1
        option filterwin2k      0  # enable for dial on demand
        option localise_queries 1
        option rebind_protection 1  # disable if upstream must serve RFC1918 addresses
        option rebind_localhost 1  # enable for RBL checking and similar services
        #list rebind_domain example.lan  # whitelist RFC1918 responses for domains
        option local    '/lan/'
        option domain   'lan'
        option expandhosts      1
        option nonegcache       0
        option authoritative    1
        option readethers       1
        option leasefile        '/tmp/dhcp.leases'
        option resolvfile       '/tmp/resolv.conf.auto'
        #list server            '/mycompany.local/1.2.3.4'
        #option nonwildcard     1
        #list interface         br-lan
        #list notinterface      lo
        #list bogusnxdomain     '64.94.110.11'

config dhcp lan
        option interface        lan
        option start    100
        option limit    150
        option leasetime        12h
        option disable

config dhcp wan
        option interface        wan
        option ignore   1
~
```

Figura 3-30 Desactivando DHCP

Posteriormente desactivaremos el *Firewall* del router como se ilustra en la Figura 3-31.

```
root@Router2:/etc/init.d# /etc/init.d/firewall disable
root@Router2:/etc/init.d# /etc/init.d/firewall stop
root@Router2:/etc/init.d#
```

```
root@Router2:/etc/init.d# /etc/init.d/network reload
```

Figura 3-31 Desactivando Firewall

3.3.4 Programación de tareas

Podemos programar una serie de tareas que el router puede realizar de forma periódica gracias al comando de Linux *cron* [51]. En nuestro caso, y siguiendo las directrices de la guía CCN-STIC 816, procederemos a programar el encendido y apagado de la red WiFi del router para evitar su uso fuera del horario establecido. Como se comentó en el apartado 3.2, para el CUD esta medida puede ser contraproducente. El ejemplo a continuación demuestra la posibilidad de establecer el horario con OpenWrt. Para ello realizamos la siguiente secuencia:

```
>#  crontab -e        #Abrimos la tabla para programar cron#
```

Como vemos en la Figura 3-32, se configura el router para apagar y encender la red WiFi a las 23:59 y 06:45, respectivamente, los días laborables y de 23:59 a 08:00 los fines de semana.

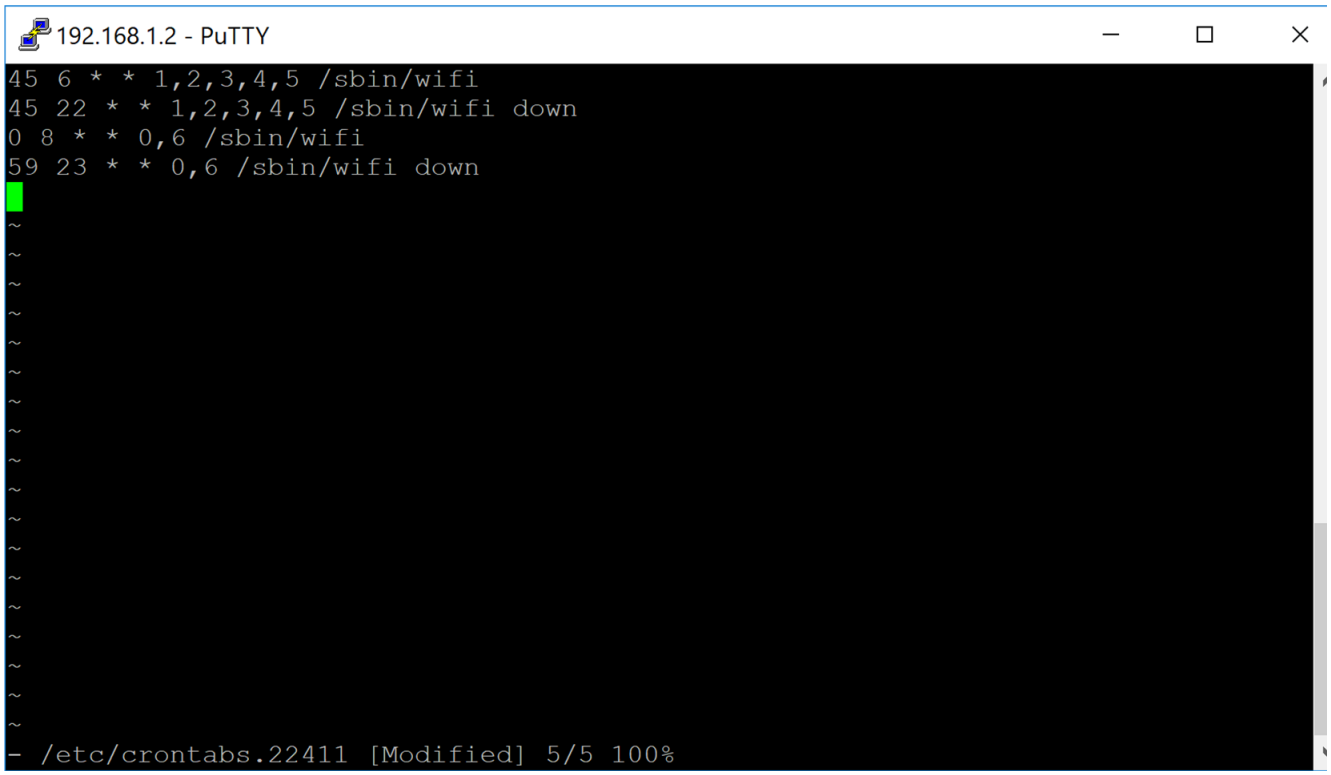


Figura 3-32 Tabla programación *cron*

La configuración de la tabla *cron* sigue la siguiente estructura y los valores que puede tomar cada columna (Tabla 3-6).

Minutos	Hora	Día del mes	Mes	Día de la semana	Comando a ejecutar
0-59	0-23	1-31	1-12	0-6	Comando Linux

Tabla 3-6 Estructura tabla *cron*

Cada línea de la tabla ejecuta un comando en un momento determinado. En cada línea, las columnas se separan por espacios y si queremos seleccionar varios momentos temporales distintos, por ejemplo, los días se separan mediante comas. Un asterisco en una columna indica que se realiza en todo el ámbito de tiempo que recoge. Por ejemplo, un asterisco en la columna día de la semana implica que se ejecuta todos los días.

Nuestra configuración indica lo siguiente,

- *45 6 * * 1,2,3,4,5 /sbin/wifi*: Indica que a las 6:45 (45 6) los lunes, martes, miércoles, jueves y viernes (1,2,3,4,5), todos los días del mes (*), todos los meses del año (*) se encienda la interfaz WiFi.
- *45 22 * * 1,2,3,4,5 /sbin/wifi down*: Indica que a las 22:45 (45 22) los lunes, martes, miércoles, jueves y viernes (1,2,3,4,5), todos los días del mes (*), todos los meses del año (*) se apague la interfaz WiFi.
- *0 8 * * 6,0 /sbin/wifi*: Indica que a las 08:00 (0 8) los sábados y domingos (0,6), todos los días del mes (*), todos los días del año (*) se encienda la interfaz WiFi.
- *59 23 * * 6,0 /sbin/wifi down*: Indica que a las 23:59 (59 23) los sábados y domingos (0,6), todos los días del mes (*), todos los días del año (*) se apague la interfaz WiFi.

Con las líneas anteriores hemos programado el encendido y apagado del router los días de diario y fin de semana.

Destacar la importancia de que el router tenga la hora acorde con nuestra zona horaria. Para ello debemos configurar el archivo */etc/config/system* como se muestra en la Figura 3-33, para que se sincronice correctamente con un servidor (o varios) NTP (*Network Time Protocol*).

Las opciones para *zonename* y *timezone* están recogidas en la página oficial de OpenWrt [52], y cada *zonename* tiene su correspondiente código *timezone.*

Se debe indicar que los routers empleados para este TFG no tienen capacidad de apagado y encendido. Para apagarlos se debe desconectar la alimentación. El mecanismo utilizado para evitar el uso de la red inalámbrica es desactivando la interfaz WiFi.

```
config 'system'
        option 'hostname' 'Router4'
        option 'zonename' 'Europe/Madrid'
        option 'timezone' 'CET-1CEST,M3.5.0,M10.5.0/3'
        option 'conloglevel' '8'
        option 'cronloglevel' '8'

config 'timeserver' 'ntp'
        list 'server' '0.openwrt.pool.ntp.org'
        list 'server' '1.openwrt.pool.ntp.org'
        list 'server' '2.openwrt.pool.ntp.org'
        list 'server' '3.openwrt.pool.ntp.org'

~
~
~
~
```

Figura 3-33 Configuración de hora y zona horaria

3.3.5 FreeRADIUS

FreeRADIUS [53] es un servidor de autenticación libre, que emplearemos para dotar a nuestra red de un servidor que gestione las conexiones de los usuarios a la red. En nuestro caso se hará mediante un nombre de usuario y contraseña por dispositivo.

RADIUS, que es el acrónimo de *Remote Authentication Dial In User Service* [54], es un protocolo de red que permite la autenticación y monitorización (en inglés, *accounting*). El protocolo realiza tres funciones primarias.

- Autentica a los usuarios o dispositivos antes de permitirles acceder a la red.
- Autoriza a aquellos usuarios o dispositivos el acceso a servicios de red específicos.
- Monitorización (*accounting*), permite el seguimiento del uso que hace cada usuario de esos servicios.

3.3.5.1 Instalación de FreeRADIUS

Antes de comenzar con la instalación debemos explicar la diferencia entre servidor, usuario y cliente en el ámbito de RADIUS. Para RADIUS el servidor es el lugar donde se procesan las solicitudes de acceso. El servidor comunica con el cliente, que es el router al que se le solicita acceso en primer lugar. El acceso lo solicitan los usuarios (dispositivos tipo móvil, portátil,…) a los clientes (routers).

Para implementar la medida de autenticación mediante servidor (IEEE 802.1x) procederemos a instalar el servidor FreeRADIUS en un portátil con sistema operativo Kali Linux. Para ello instalaremos mediante la terminal el paquete básico de FreeRADIUS. Se emplea Kali Linux por motivos ajenos a FreeRADIUS, pues podría instalarse en cualquier otra distribución Linux.

```
$ sudo apt-get install FreeRADIUS
```

FreeRADIUS puede ampliarse mediante módulos que permiten aumentar sus capacidades, aunque de momento trabajaremos con el módulo básico.

A continuación, procederemos a verificar la instalación del servidor con el comando *sudo freeradius -X*, como se ilustra en la Figura 3-34.

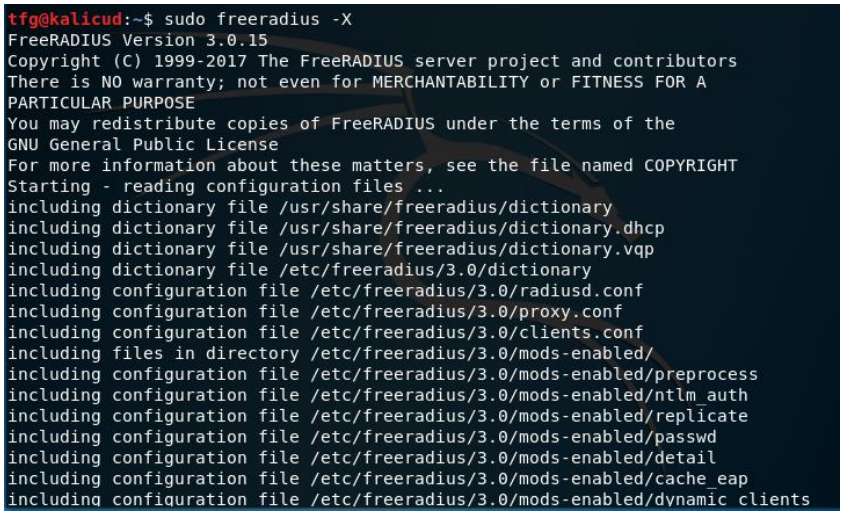


Figura 3-34 Verificando FreeRADIUS

El resultado mostrado, *Ready to process requests*, (Figura 3-35) nos indica que el servidor se instaló correctamente.

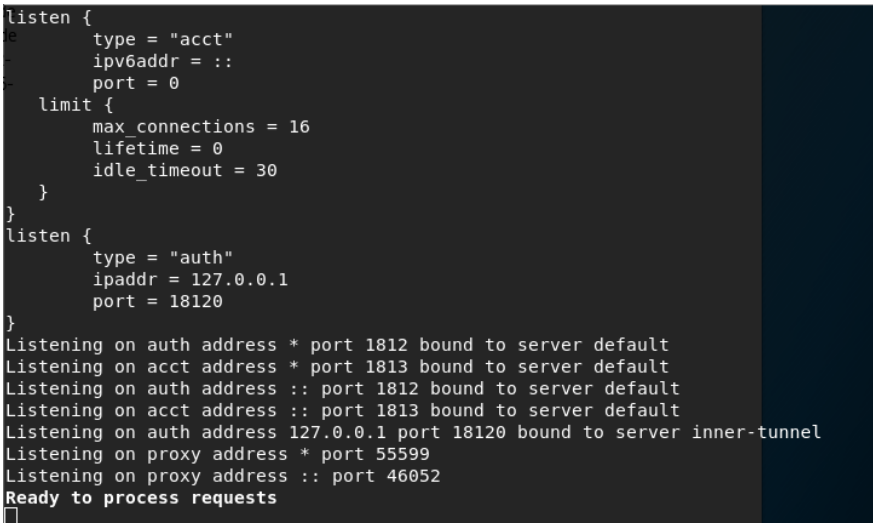


Figura 3-35 Verificación correcta FreeRADIUS

3.3.5.2 Configuración de FreeRADIUS

Para configurar el servidor existen varios archivos que podemos editar acorde al funcionamiento que deseemos por parte del servidor:

- *radius.conf*, que define los parámetros de configuración para el servidor RADIUS. Incluye referencia al resto de archivos de configuración.
- *clients.conf*, define la información necesaria para configurar el cliente RADIUS, incluyendo las direcciones IP y los secretos compartidos. Este archivo está referenciado en el fichero *radius.conf*.
- *dictionary*, define los atributos locales del servidor RADIUS. Este fichero referencia los archivos de diccionarios por defecto. Los archivos diccionario por defecto incluyen cientos de definiciones de atributos para más de cien vendedores de clientes.
- *proxy.conf*, define *upstream home servers* (define el servidor principal que da servicio a otros servidores secundarios), incluyendo la información de direcciones IP y secretos compartidos. El fichero *radius.conf* referencia el archivo *proxy.conf*.
- *sites-enabled/default.* Éste es el servidor virtual por defecto. Este archivo maneja las peticiones de autenticación y contabilización. Contiene una configuración designada a trabajar con el mayor número de protocolos de autenticación. El fichero *radius.conf* referencia el archivo *sites-enabled/default*.
- *sites-enabled/inner-tunnel*. Este servidor virtual maneja los métodos de autenticación que son transportados mediante un túnel TLS (*Transport Layer Security*), como parte de las autenticaciones PEAP (*Protected Extensible Authenticacion Protocol*) o EAP-TTLS. El archivo *radius.conf* referencia al archivo *sites-enabled/inner-tunnel*.
- *users*, archivo de configuración de los usuarios de RADIUS.

La configuración por defecto debería cubrir las necesidades que se pueden solicitar al servidor. Por tanto, solo modificaremos los valores imprescindibles, que son:

- La configuración del cliente mediante la edición del archivo *clients.conf*, añadiendo el nuevo cliente que será el Router 1. Como podemos ver en la Figura 3-36, el cliente se define con su dirección IP y su secreto, que es el código que debemos introducir en la propia configuración del router cliente.
- El siguiente archivo que modificaremos, *users*, nos permitirá asignar un nombre de usuario y clave para cada uno de los dispositivos que se van a conectar a la red, lo que nos permite fácilmente eliminar dispositivos de la red sin tener que modificar parámetros que afecten al resto de los usuarios. En la Figura 3-37 se muestran los tres usuarios que se han autorizado a conectarse. Estos usuarios están definidos por un nombre de usuario, al inicio de la línea, y una contraseña, en color rosa.

Además, podemos añadir una serie de modificadores a los usuarios para limitar el número de conexiones simultaneas o el tiempo máximo de conexión. Como nuestro router ya nos permite limitar ese tiempo de conexión máximo, solo incluiremos el límite de conexiones simultáneas, como se muestra en la ver Figura 3-38.

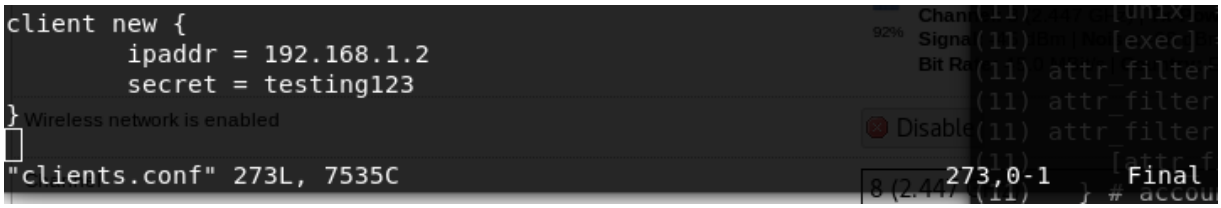


Figura 3-36 Añadiendo nuevo cliente

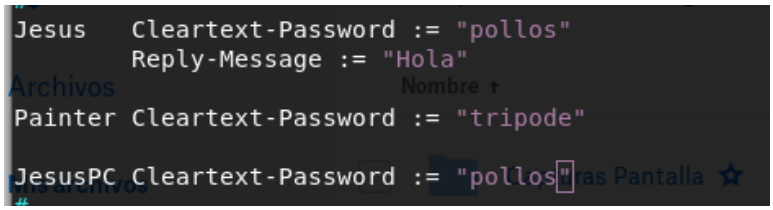


Figura 3-37 Añadiendo nuevos usarios

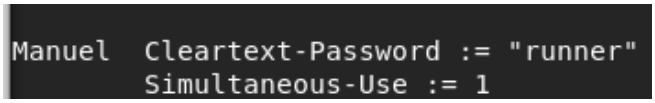


Figura 3-38 Limitando conexiones simultáneas

Una vez configurado el servidor, procedemos a configurar el cliente. OpenWrt no cuenta con soporte WPA2 *Enterprise* de forma predefinida. Para añadirlo, debemos previamente desactivar el módulo *wpad-mini* y posteriormente instalar su versión completa *wpad*, que añade soporte a WPA2 *Enterprise*.

Una vez añadido WPA2 *Enterprise*, configuramos el archivo *wireless* como se muestra en la Figura 3-39.

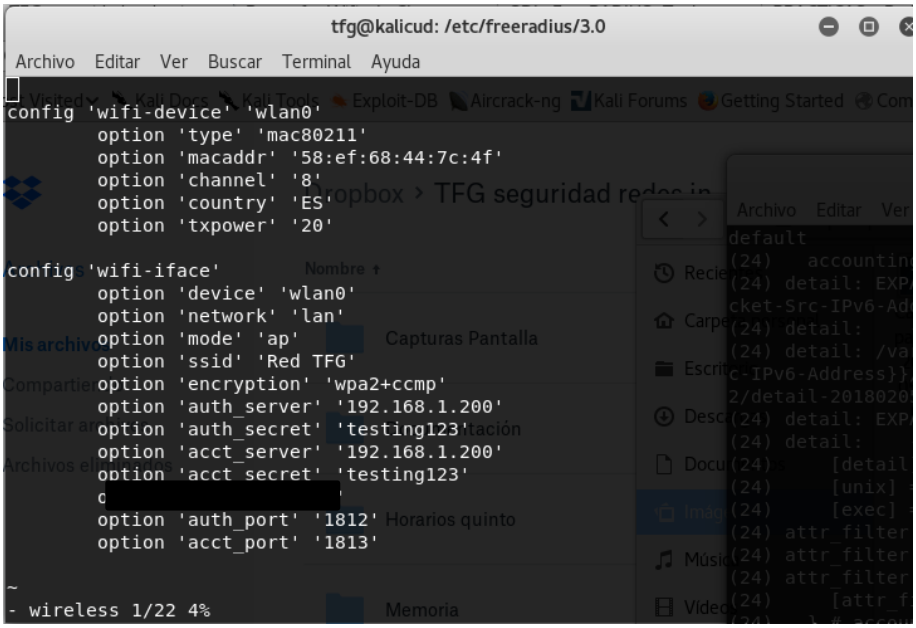


Figura 3-39 Configurando WPA2 *Enterprise*

Nos centraremos en la configuración de *'wifi-iface'*.

- *encryption*, aquí seleccionamos el método de encriptación, *wpa2+ccmp*. De esta forma forzamos a que se emplee WPA2 con CCMP, sin permitir el uso de TKIP.
- *auth_server*, seleccionamos la IP donde se encuentra el servidor para autorización, en nuestro caso, la dirección IP del equipo empleado como servidor.
- *auth_secret*, introducimos el secreto que comparten el servidor para autenticación con los clientes.
- *acct_server*, seleccionamos la IP donde se encuentra el servidor para monitorización de usuarios, que es la misma que en *auth_server* ya que el servidor se encuentra en el mismo equipo.
- *acct_secret*, análogo a *auth_secret*.

- *auth_port*, establecemos el puerto de enlace 1812 como puerto de comunicación para autenticación con FreeRADIUS.
- *acct_port*, establecemos el puerto de enlace 1813 como puerto de comunicación para contabilización con FreeRADIUS.

3.3.6 Base de datos MySQL

El empleo de la base de datos MySQL nos permite una gestión de los usuarios mucho más sencilla e intuitiva. La base de datos remplazará los archivos *users* y *clients.conf*.

Para instalar MySQL [55], se descarga el paquete *mysql-apt-config_0.8.9-1_all.deb*, que contiene los archivos que debemos cargar en el repositorio APT, como se muestra en la Figura 3-40.

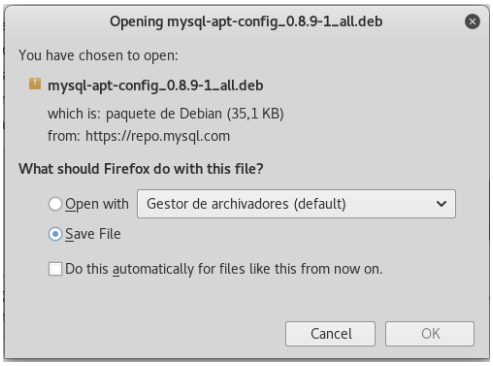


Figura 3-40 Descarga paquete *mysql-apt-config_0.8.9-1_all.deb*

A continuación, instalamos el paquete descargado mediante:

```
$ sudo dpkg -i ~/Descargas/mysql-apt-config_0.8.9-1_all.deb
```

Posteriormente procedemos a actualizar la información del repositorio y a instalar el servidor MySQL (Figura 3-41).

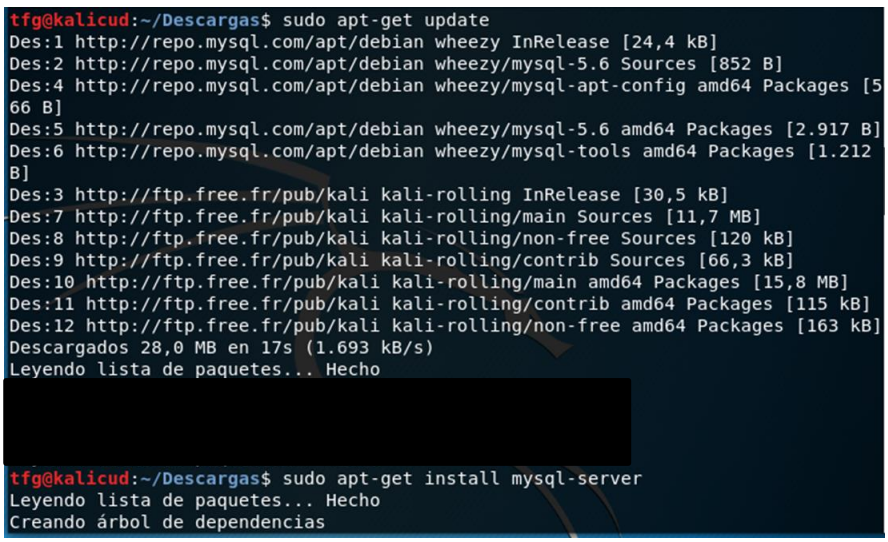


Figura 3-41 Actualizando repositorio e instalando servidor MySQL

Una vez instalado MySQL, se procede a configurarlo para su empleo con FreeRADIUS, creando una base de datos en MySQL. Para la configuración es importante usar la versión más actualizada de FreeRADIUS mediante el comando:

```
sudo apt-get upgrade freeradius
```

En primer lugar, se debe lanzar el servidor MySQL (ver Figura 3-42). Con el primer comando, *sudo service mysql status* se comprueba el estado del servidor. Como se muestra en el apartado *Active: inactive (dead)*, el servidor está apagado. Con el segundo comando *sudo service mysql start*, se inicia el servidor. Procedemos a comprobar su estado después de la activación. Vemos que el servidor está activo y el grupo fecha y hora de activación.

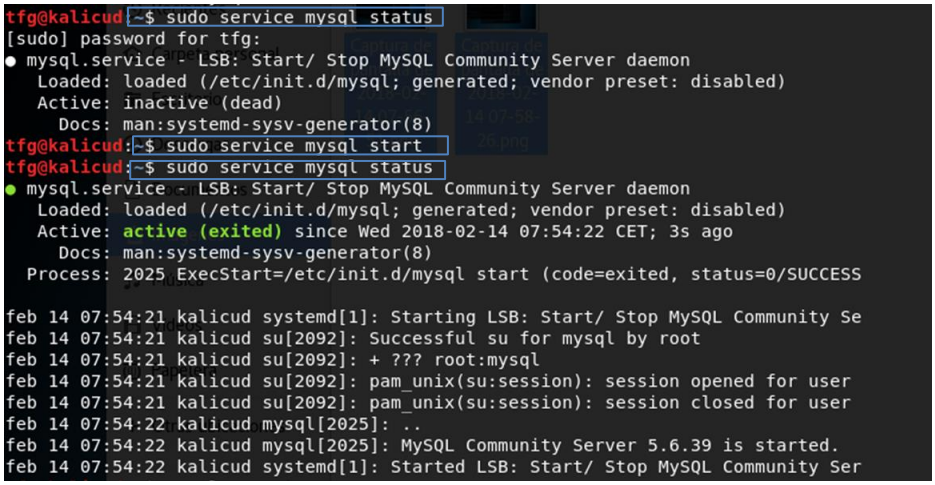


Figura 3-42 Lanzamiento del servidor

Una vez lanzado el servidor, accederemos a configurarlo, accediendo a él mediante el comando *$ mysql -uroot -p* (nos conectamos al motor de MySQL con el usuario root, y nos solicita su contraseña). El establecimiento de la conexión se ilustra en la Figura 3-43.

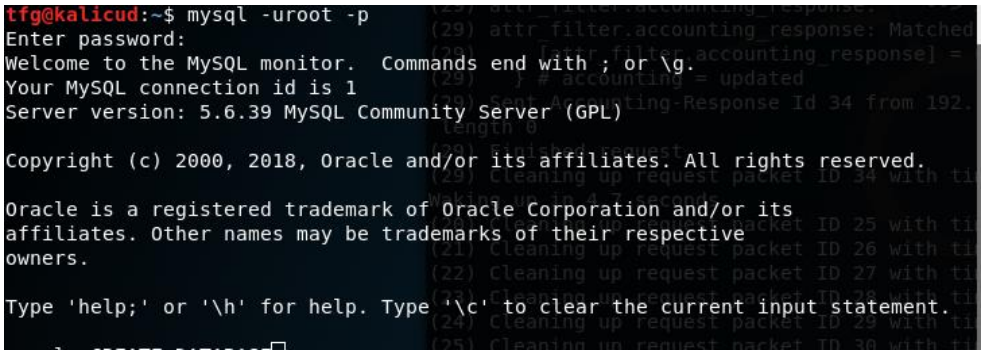


Figura 3-43 Conectándose a MySQL

El siguiente paso es crear una base de datos a la que llamaremos “radius” mediante la ejecución del comando SQL:

```
mysql > CREATE DATABASE radius
```

Posteriormente se importan las estructuras de tablas y contenidos que trae FreeRADIUS preestablecidos para el uso en MySQL. Para ello establecemos la base de datos con la que vamos a trabajar, “radius”, con *mysql> use radius*, e importamos del directorio de FreeRADIUS el archivo *schema.sql* con el comando *source*.

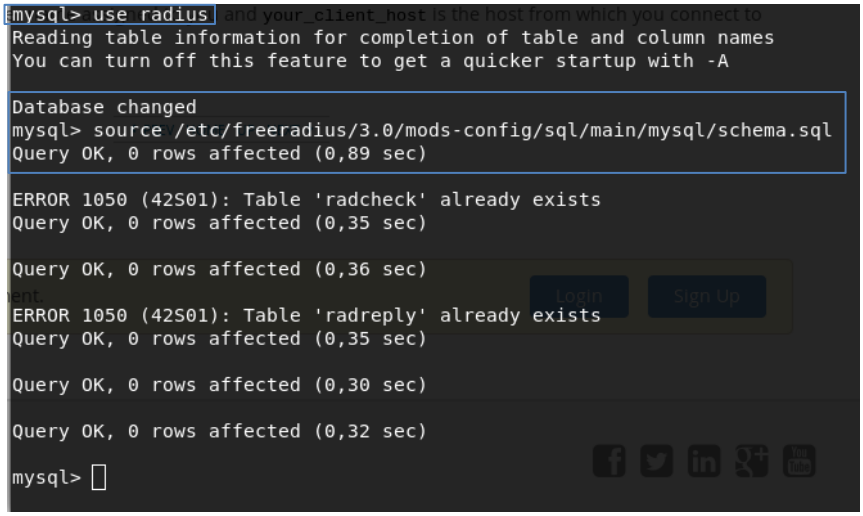


Figura 3-44 Importando tablas FreeRADIUS

En la Figura 3-45 se muestran las tablas que se han creado en la base de datos “radius”, importadas del archivo *schema.sql* de FreeRADIUS. Como se verá a continuación, las tablas tienen una estructura definida, pero no tendrán datos en ellas.

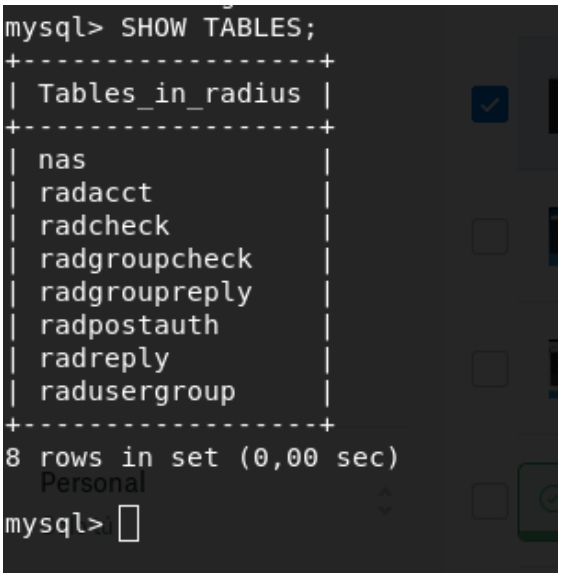
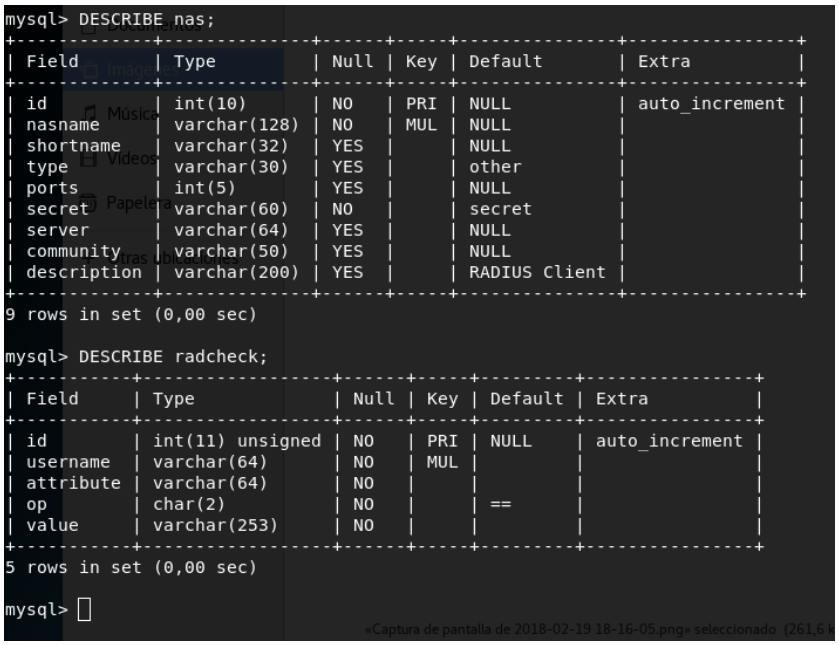


Figura 3-45 Tablas FreeRADIUS importadas

De las tablas anteriormente mostradas, emplearemos la tabla *nas* y *radcheck*, que recogen la información de los clientes conectados al servidor FreeRADIUS y los usuarios que pueden acceder al mismo, respectivamente (ver Figura 3-46). Para el funcionamiento del servidor, debemos poblar estas tablas como se muestra en la Figura 3-47.

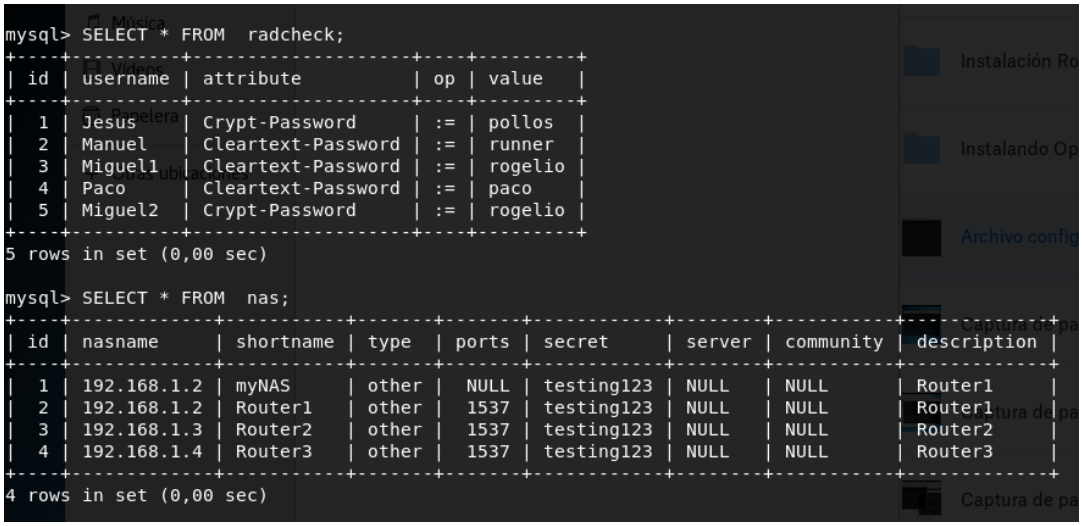


```
mysql> DESCRIBE nas;
+-------------+--------------+------+-----+---------------+----------------+
| Field       | Type         | Null | Key | Default       | Extra          |
+-------------+--------------+------+-----+---------------+----------------+
| id          | int(10)      | NO   | PRI | NULL          | auto_increment |
| nasname     | varchar(128) | NO   | MUL | NULL          |                |
| shortname   | varchar(32)  | YES  |     | NULL          |                |
| type        | varchar(30)  | YES  |     | other         |                |
| ports       | int(5)       | YES  |     | NULL          |                |
| secret      | varchar(60)  | NO   |     | secret        |                |
| server      | varchar(64)  | YES  |     | NULL          |                |
| community   | varchar(50)  | YES  |     | NULL          |                |
| description | varchar(200) | YES  |     | RADIUS Client |                |
+-------------+--------------+------+-----+---------------+----------------+
9 rows in set (0,00 sec)

mysql> DESCRIBE radcheck;
+-----------+------------------+------+-----+---------+----------------+
| Field     | Type             | Null | Key | Default | Extra          |
+-----------+------------------+------+-----+---------+----------------+
| id        | int(11) unsigned | NO   | PRI | NULL    | auto_increment |
| username  | varchar(64)      | NO   | MUL |         |                |
| attribute | varchar(64)      | NO   |     |         |                |
| op        | char(2)          | NO   |     | ==      |                |
| value     | varchar(253)     | NO   |     |         |                |
+-----------+------------------+------+-----+---------+----------------+
5 rows in set (0,00 sec)

mysql>
```

Figura 3-46 Formato tablas *nas* y *radcheck*

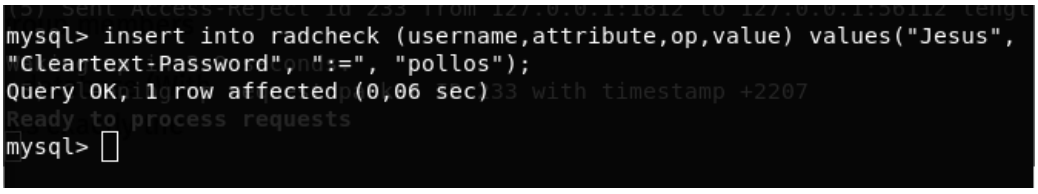


```
mysql> SELECT * FROM  radcheck;
+----+----------+--------------------+----+---------+
| id | username | attribute          | op | value   |
+----+----------+--------------------+----+---------+
|  1 | Jesus    | Crypt-Password     | := | pollos  |
|  2 | Manuel   | Cleartext-Password | := | runner  |
|  3 | Miguel1  | Cleartext-Password | := | rogelio |
|  4 | Paco     | Cleartext-Password | := | paco    |
|  5 | Miguel2  | Crypt-Password     | := | rogelio |
+----+----------+--------------------+----+---------+
5 rows in set (0,00 sec)

mysql> SELECT * FROM  nas;
+----+-------------+-----------+-------+-------+------------+--------+-----------+-------------+
| id | nasname     | shortname | type  | ports | secret     | server | community | description |
+----+-------------+-----------+-------+-------+------------+--------+-----------+-------------+
|  1 | 192.168.1.2 | myNAS     | other |  NULL | testing123 | NULL   | NULL      | Router1     |
|  2 | 192.168.1.2 | Router1   | other |  1537 | testing123 | NULL   | NULL      | Router1     |
|  3 | 192.168.1.3 | Router2   | other |  1537 | testing123 | NULL   | NULL      | Router2     |
|  4 | 192.168.1.4 | Router3   | other |  1537 | testing123 | NULL   | NULL      | Router3     |
+----+-------------+-----------+-------+-------+------------+--------+-----------+-------------+
4 rows in set (0,00 sec)
```

Figura 3-47 Contenido tablas *nas y radcheck*

Para poblar las tablas, se emplea el comando *INSERT INTO nombre_tabla (valores)*. En el ejemplo, se añade el usuario Jesus a la tabla *radcheck* incluyendo la contraseña que empleará para conectar al servidor RADIUS. Como se ve en la Figura 3-48, en el primer paréntesis se indica en qué columna de la tabla *radcheck* va a ir la información que se muestra en el segundo paréntesis. De esta forma se pueblan las tablas *nas* y *radcheck.*



```
mysql> insert into radcheck (username,attribute,op,value) values("Jesus",
"Cleartext-Password",":=", "pollos");
Query OK, 1 row affected (0,06 sec)

mysql>
```

Figura 3-48 Añadiendo usuario Jesus a *radcheck*

Una vez configurado MySQL se procederá a configurar FreeRADIUS para que, en lugar de emplear los archivos *users* y *clients.conf*, emplee la base de datos.

En primer lugar, debemos modificar el fichero *radiusd.conf* y debemos añadir *$INCLUDE mods-enabled/* en *modules* y *$INCLUDE sites-enabled/* en *policy* como se muestra en la Figura 3-49.

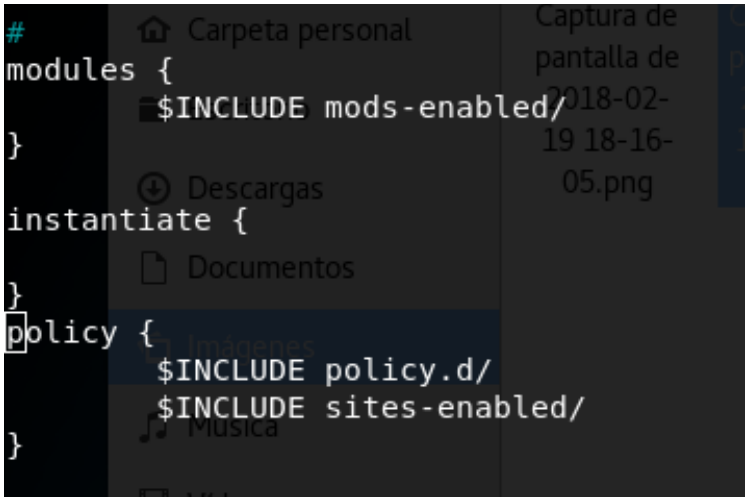


Figura 3-49 Configurando *radiusd.conf*

Seguidamente debemos modificar el archivo *default* en la carpeta *sites-available* y debemos activar *sql* en todos los apartados (como se muestra en Figura 3-50). En este archivo tenemos la opción de añadir un guión delante de la opción *sql* para indicar que debe usarse si está configurado. En nuestro caso, lo eliminamos para forzar el empleo de MySQL.

```
authorize {
…
sql
…
}
accounting {
…
sql
…
}
session {
…
sql
…
}
post-auth {
…
sql
…
}
Post-Auth-Type REJECT {
sql
}
```

Figura 3-50 Configurando *sites-available*

En tercer lugar cambiaremos los parámetros de conexión a la base de datos en la carpeta *../mods-available/* modificando el archivo *sql*. Los parámetros mostrados en la Figura 3-51 determinan, en orden de aparición:

1. *Driver*: base de datos *sql* que empleamos, en nuestro caso, *mysql*.

2. *Dialect*: debe coincidir con el *sql* que queremos usar.
3. *Server*: indica la dirección IP en la que se encuentra el servidor, en nuestro caso, la dirección es la propia del ordenador.
4. *Port*: puerto al que se debe conectar.
5. *Login*: usuario con el que accede a la base de datos, en nuestro caso es *root*, que cuenta con permisos de administración.
6. *Password*: contraseña para el usuario root, en claro.
7. *Radius_db*: indica qué base de datos dentro de MySQL debe emplear, en nuestro caso, *radius.*

En este archivo además añadimos *read_clients=yes*, para leer los clientes de la base de datos, y *client_table=”nas”* para indicar qué tabla debe leer para seleccionar los clientes.

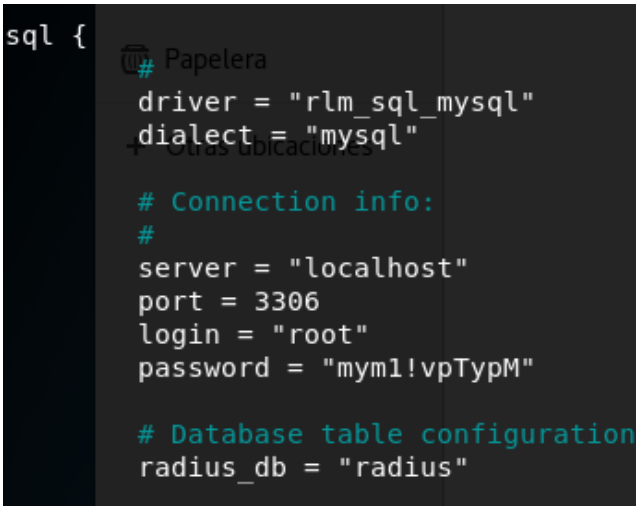


Figura 3-51 Configurando parámetros de conexión a base de datos

Con esto hemos configurado FreeRADIUS para el uso de MySQL. Ahora solo queda activarlo. FreeRADIUS almacena todas las extensiones disponibles en la carpeta *mods-available*, y para emplearlos debemos copiarlos en la carpeta *mods-enabled.* En la Figura 3-52 se muestra el proceso de creación de un enlace a la carpeta *mods-available*.

Se comprueba que la configuración se realizó correctamente con el comando $ *sudo freeradius -XC* que nos devuelve el siguiente mensaje *configuration appears to be OK*. En la Figura 3-53 se realiza la comprobación del usuario Miguel2, que devuelve *Received Access-Accept* (pantalla izquierda). En la pantalla de la derecha, se muestra la salida en modo *debug* del servidor FreeRADIUS, que acepta al usuario y devuelve *Ready to process request*.

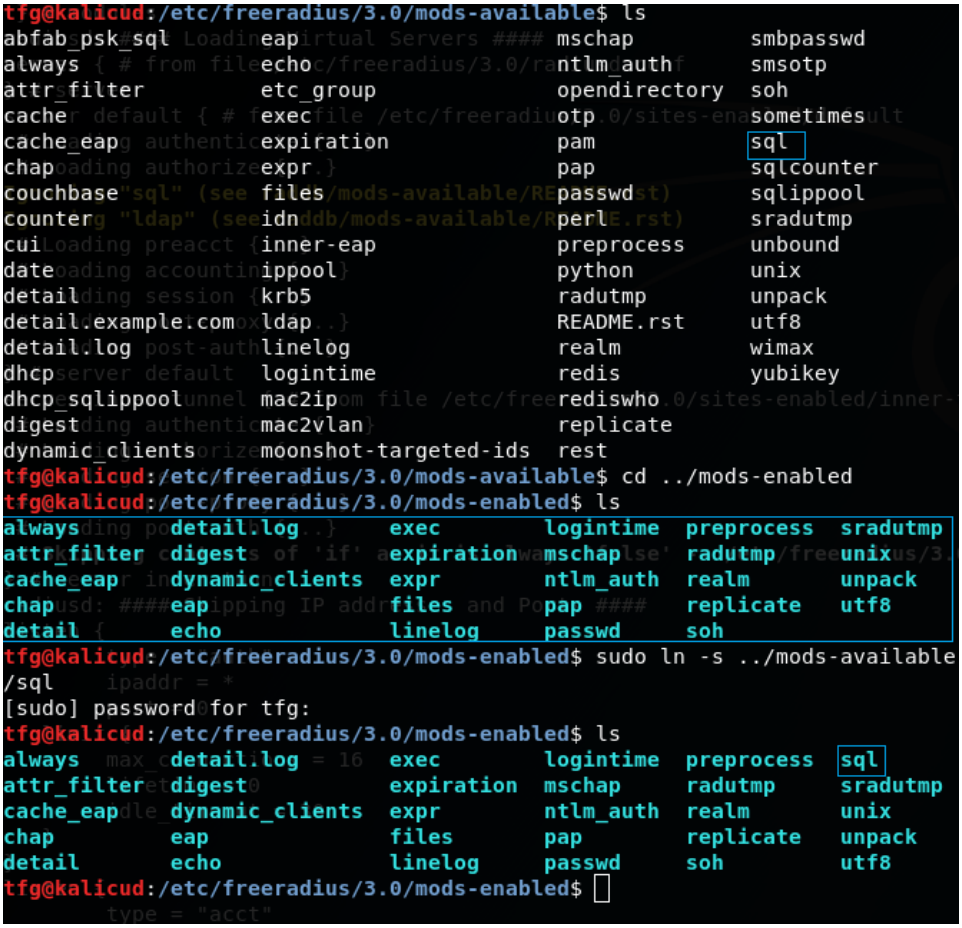


Figura 3-52 Activando MySQL en FreeRADIUS

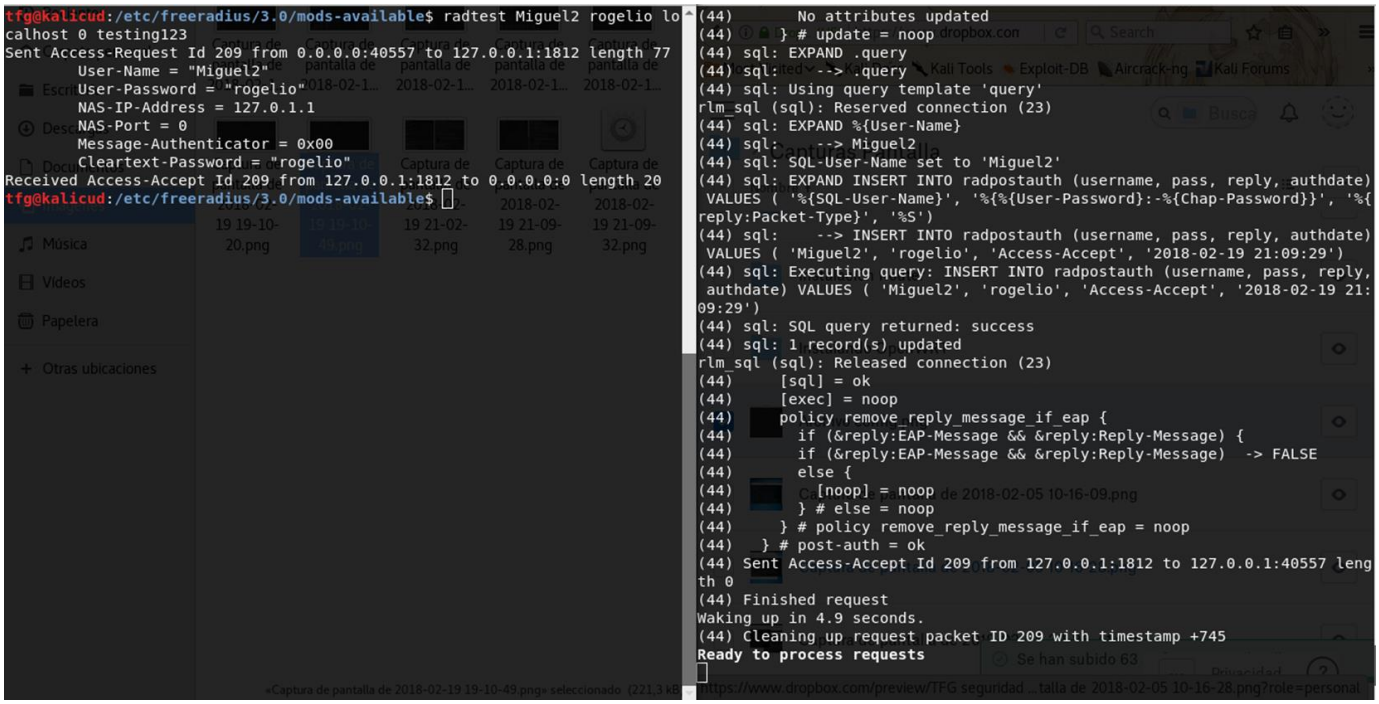


Figura 3-53 Test usuario Miguel2

3.3.6.1 MySQL Workbench

Para simplificar la gestión de las tablas y bases de datos instalamos *MySQL Workbench* (véase Figura 3-54).

```
tfg@kalicud:~/Descargas/mysql-workbench-community-6.3.10-src/wb-build$ sudo apt-get install mysql-workbench
```

Figura 3-54 Instalando *MySQL Workbench*

Una vez instalado, la aplicación estará disponible en el escritorio del ordenador. Cuando abrimos la aplicación, se muestra la pantalla de la Figura 3-55. En ella se muestran los distintos servidores MySQL a los que podemos acceder. En nuestro caso, solo tenemos el servidor local del ordenador con el usuario root. En la Figura 3-56 se introdujo la contraseña que empleábamos para acceder a MySQL con *mysql -uroot -p*.

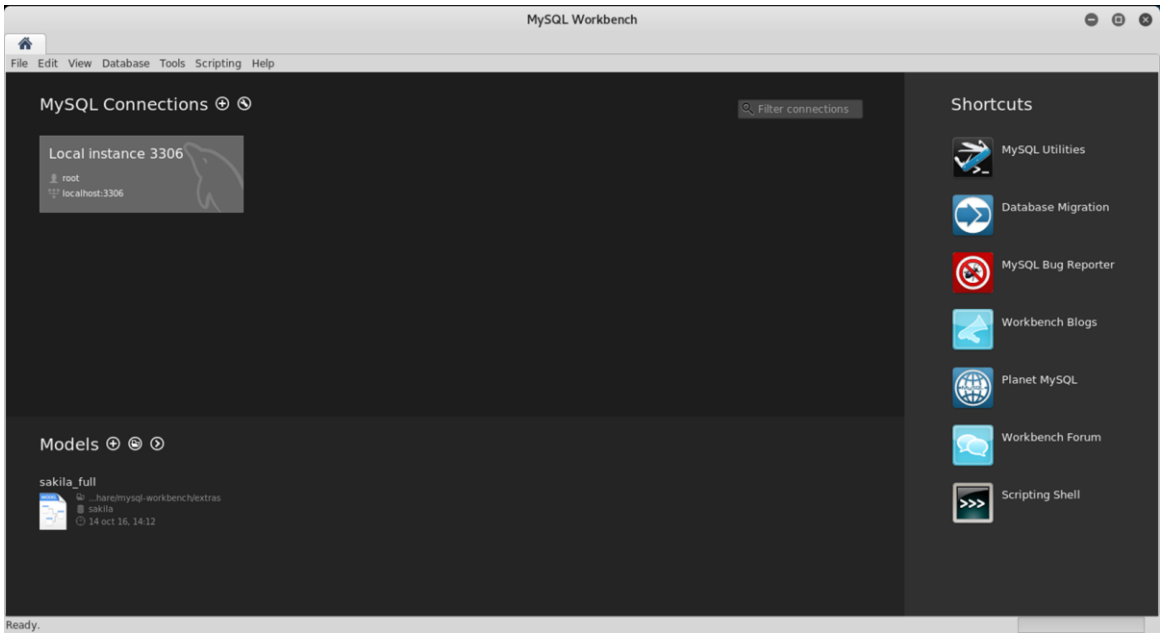


Figura 3-55 Pantalla inicial *MySQL Workbench*

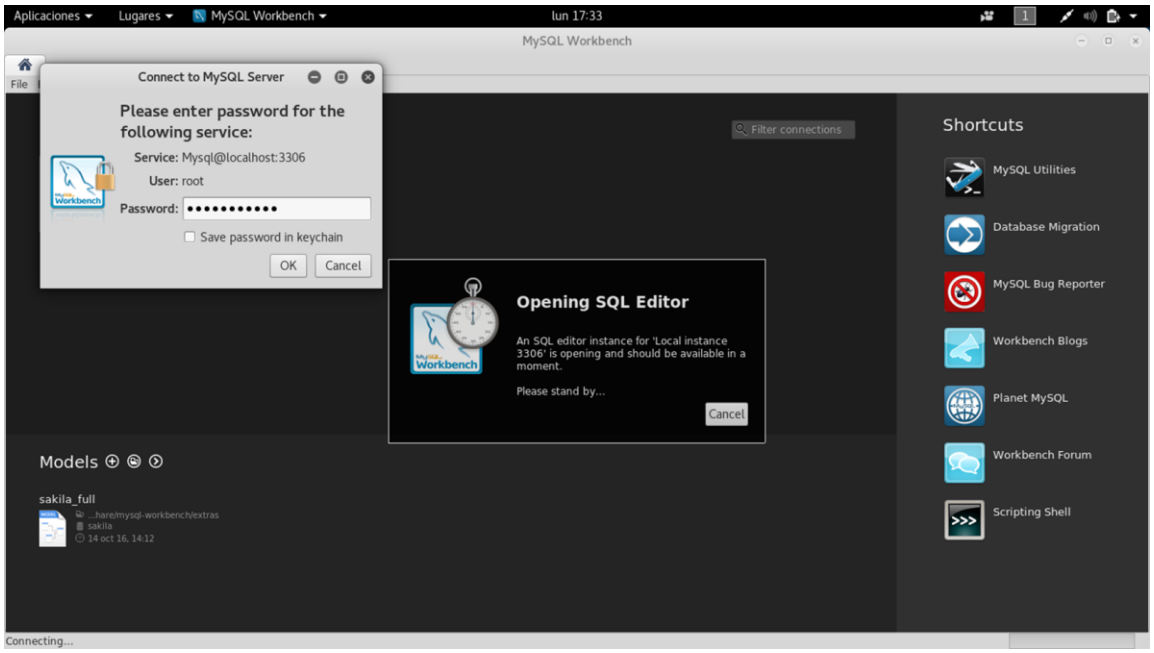


Figura 3-56 Ventana de acceso al servidor

En la Figura 3-57 se muestra la interfaz desde la que podemos acceder a la base de datos *radius*. Una vez abierto el menú desplegable, podemos acceder a las distintas tablas. Se selecciona *radcheck* (Figura 3-58) sobre la que podemos hacer los cambios simplemente haciendo click en el campo que nos interese.

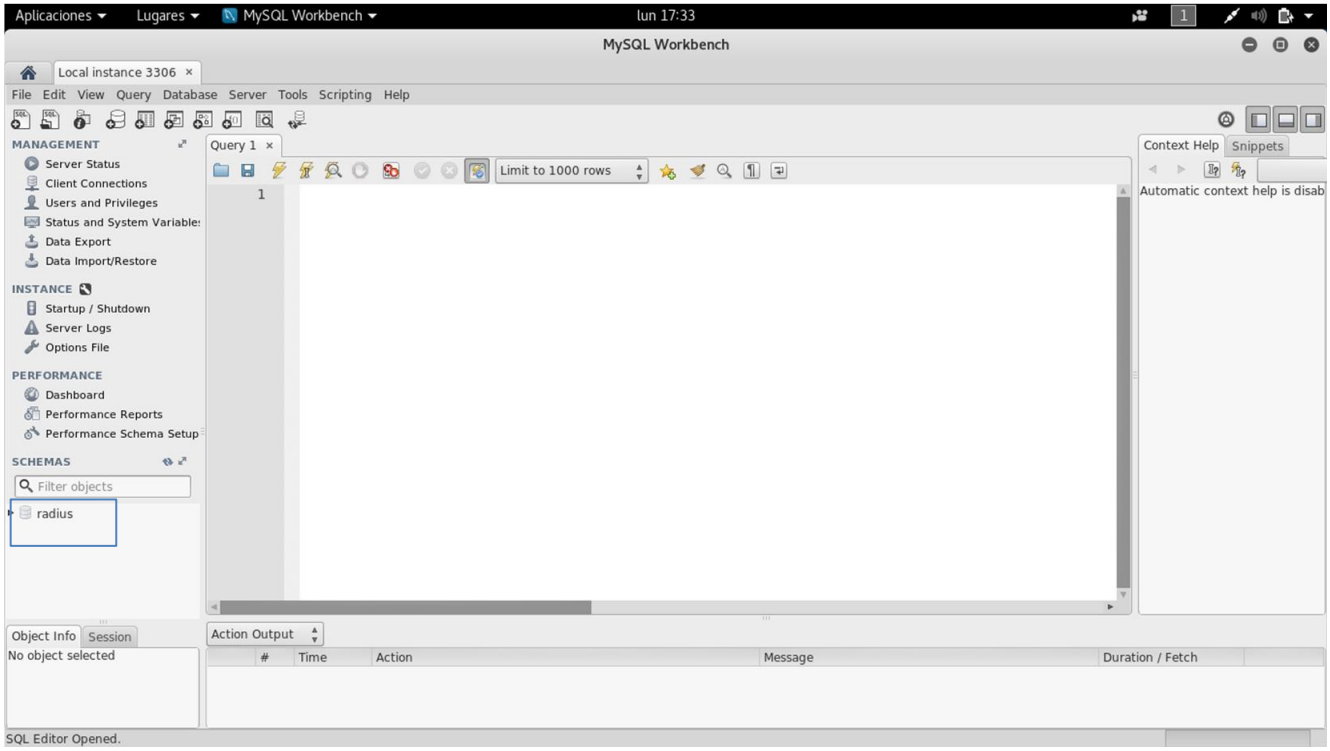


Figura 3-57 Interfaz de trabajo principal

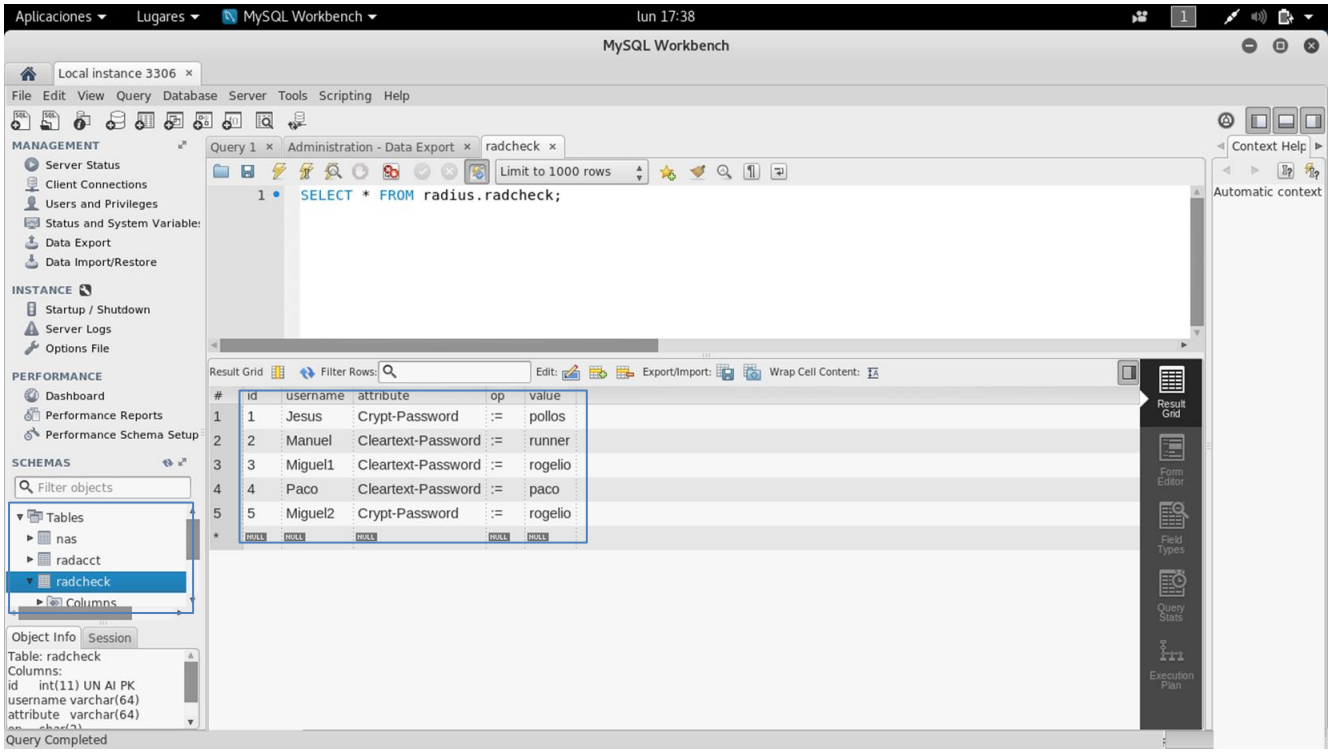


Figura 3-58 Editando tabla *radcheck*

La Figura 3-59 muestra cómo *MySQL Workbench* trabaja. A pesar de la interfaz, al modificar las tablas nos solicita confirmar los cambios, que se traducen al código que utilizaríamos con la interfaz en la terminal.

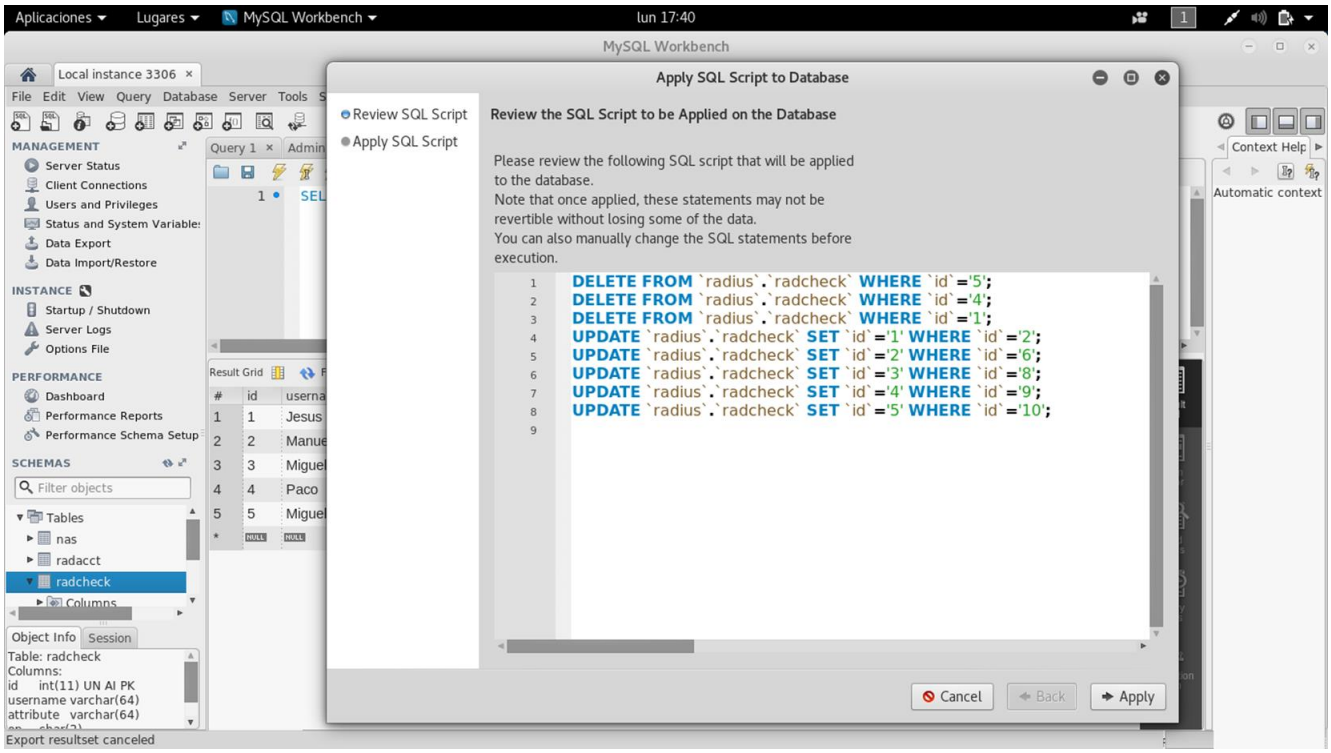


Figura 3-59 Muestra de funcionamiento *MySQL Workbench*

3.3.7 Kismet

Para completar uno de los requerimientos que recomienda la guía, que es tener un Sistema de Detección de Intrusión Inalámbrica o WIDS (*Wireless Intrusion Detection System*), emplearemos el *software* Kismet [47]. Instalaremos un servidor y cliente Kismet en nuestro equipo y un dron Kismet en un router que emplearemos exclusivamente para monitorizar la red.

Un Sistema de Detección de Intrusiones (IDS) es capaz de detectar los accesos no autorizados a una red o a un equipo informático. Pueden estar compuestos por los siguientes elementos [14]:

- Sensores: dispositivos que monitorizan y capturan la actividad de la red.
- Servidores de Administración: equipos que analizan la información enviada por los sensores.
- Servidores de Base de Datos: equipos que almacenan los eventos generados por los servidores de administración, tras su análisis.
- Consola: interfaz de gestión y control del sistema.

Los sensores WIDS pueden ser de varios tipos:

- Dedicados: son dispositivos independientes y dedicados únicamente a esta función de sensor. Los sensores están conectados a la red cableada y pueden ser fijos o móviles. Los sensores fijos se instalan en una localización fija donde pueden disponer de alimentación, conexión a la red cableada, etc. Los sensores móviles están diseñados para ser portables y poder usarse en distintas localizaciones o incluso en movimiento.
- No dedicados: el sensor no es un dispositivo, sino una función integrada en otros dispositivos de la red inalámbrica, como AP o conmutadores.

- Sensores *software* en dispositivo cliente: son unidades *software* que se instalan en los dispositivos cliente y tienen la función de detectar ataques en su rango de frecuencias, o vulnerabilidades dentro de los dispositivos cliente y enviar esta información a los Servidores de Administración.

En nuestro caso particular, el sistema lo componen un sensor no dedicado compuesto por uno de los routers con el *software* Kismet *drone* instalado. Los servidores de administración y base de datos son el servidor Kismet instalado en nuestro ordenador portátil. La consola la aporta el cliente Kismet, igualmente instalado en el portátil.

Aunque hablemos de un sensor no dedicado, el router que se emplea solo tiene esa función. Debido a su limitada capacidad de memoria interna, el router no puede tener instalado el dron Kismet y el *software* necesario para soportar la autenticación mediante FreeRADIUS de forma simultánea.

A continuación, se pasa a mostrar el proceso de instalación y configuración de Kismet, tanto en el portátil como en el router.

Primero instalaremos Kismet en el portátil. Esta versión de Kali Linux trae previamente instalado la versión de Kismet más reciente (2016.07.R1-1). La instalación se ejecuta de forma continua, sólo con una pausa para registrar a los usuarios que añadiremos al grupo de "usuarios con privilegios" de administración. Esto permite a los usuarios lanzar Kismet sin necesidad de usar *sudo*.

Con esto ya tendremos instalado en el ordenador el servidor y el cliente Kismet necesario para monitorizar una red. El emplear Kismet para monitorizar una red implica emplear la tarjeta WiFi del dispositivo de forma exclusiva para este fin. Debido a eso se decide emplear uno de los routers para realizar estas tareas de monitorización. Debido al despliegue de la red, emplear el router como monitor nos da mayor rango de cobertura, ya que podemos situarlo en la camareta central L-2 para cubrir la zona de emisión de los routers en F-3 y el hall.

Una vez justificado el empleo de un dron Kismet para monitorizar la Red TFG, procedemos a explicar su instalación en el router y la configuración para conectar al servidor Kismet. En la Figura 3-60 y Figura 3-61 se muestran los comandos para la instalación.

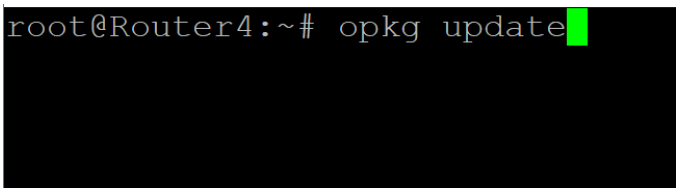


Figura 3-60 Actualizando repositorio *opkg*

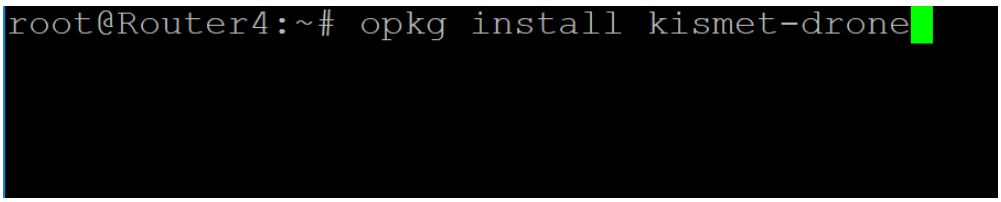


Figura 3-61 Instalación de dron de Kismet

En la Figura 3-62 se muestra cómo ahora en la carpeta */etc* aparece la carpeta *kismet*.

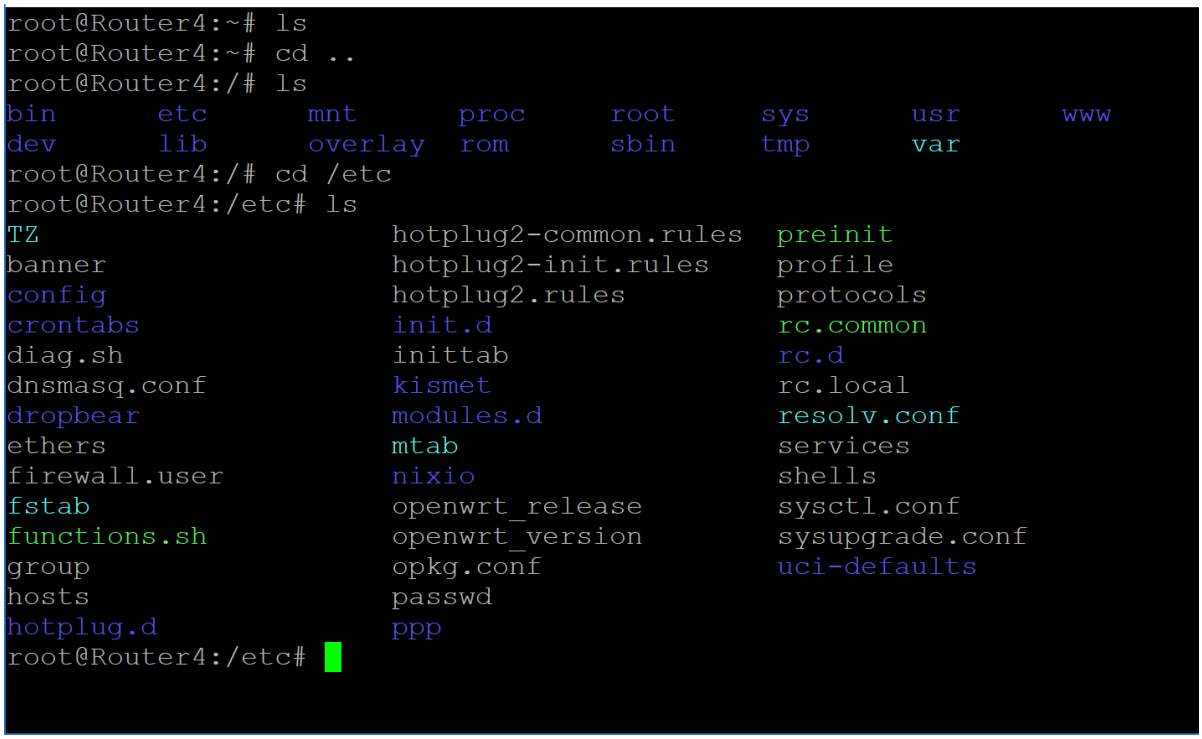


Figura 3-62 Contenido carpeta */etc* del router que actúa como dron

Dentro de ese directorio (ver Figura 3-63), se muestra el fichero */etc/kismet/kismet_drone.conf*.

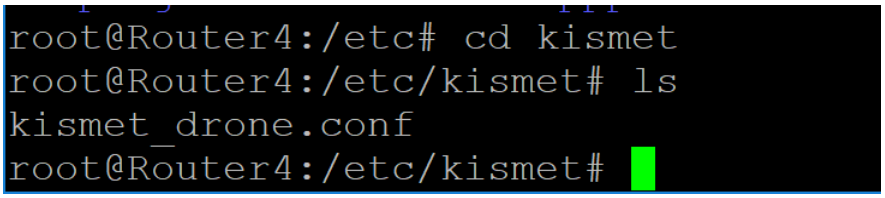
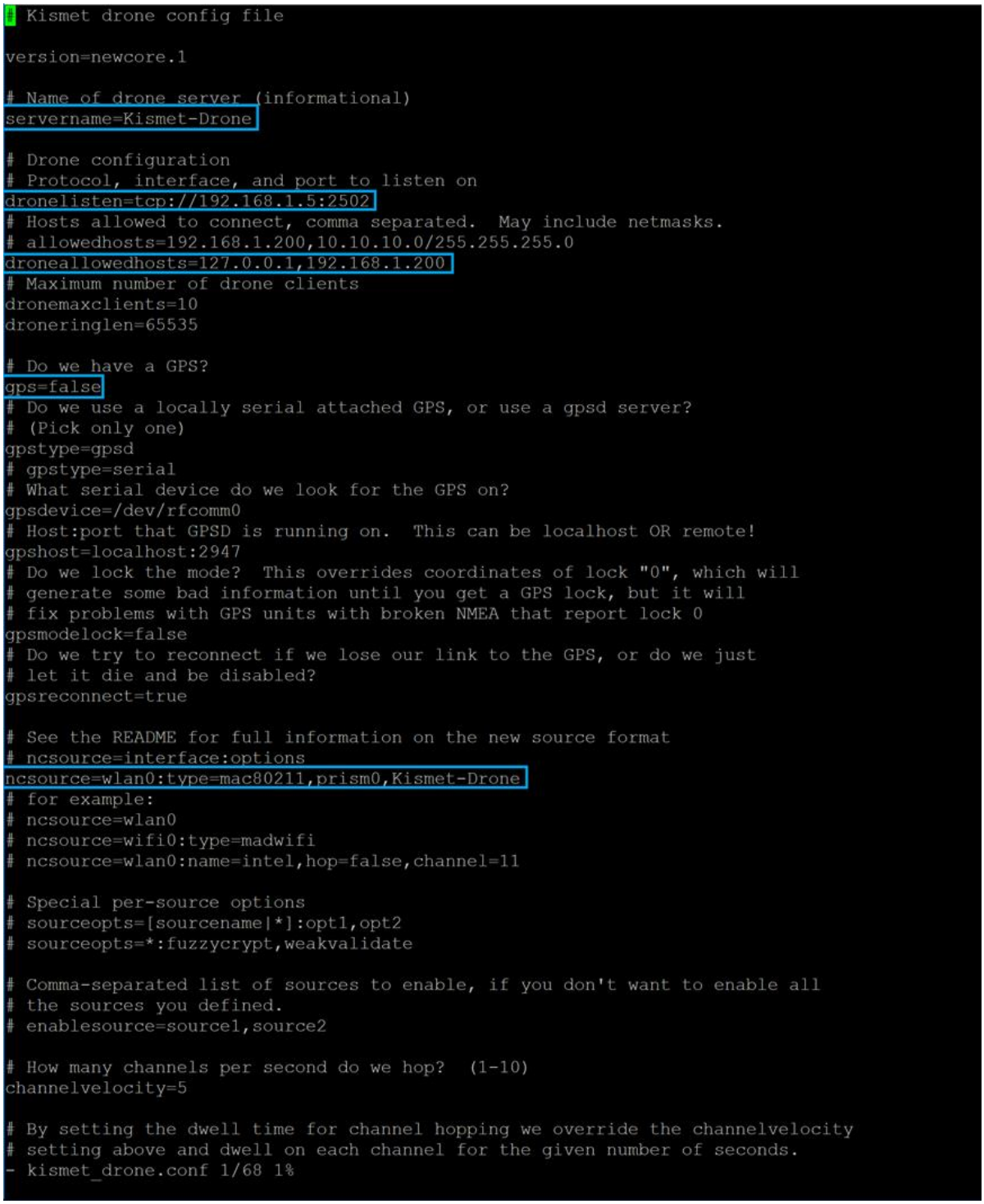


Figura 3-63 Fichero *kismet_drone.conf*

En la Figura 3-64 se muestra el contenido del fichero *kismet_drone.conf*. En él añadimos el nombre al servidor *kismet-Drone*. Con la opción *dronelisten=tcp://192.168.1.5:2502* indicamos al dron la dirección IP del dispositivo que tiene que monitorizar, que es la propia dirección del router, y el puerto de escucha, que Kismet determina 2502. La línea *droneallowedhost=127.0.0.1,192.168.1.200* autoriza a las IP añadidas a acceder al dron. En nuestro caso, se añade la IP 192.168.1.200, que es la IP del portátil en el que se encuentra el servidor Kismet.

Dado que nuestro router no tiene GPS incorporado se desactiva la opción asociada con *gps=false*. La última línea señalada indica qué interfaz debe monitorizar. Le indicamos que monitorice la interfaz *wlan0* del router, y también especificamos qué tipo de interfaz.



```
# Kismet drone config file

version=newcore.1

# Name of drone server (informational)
servername=Kismet-Drone

# Drone configuration
# Protocol, interface, and port to listen on
dronelisten=tcp://192.168.1.5:2502
# Hosts allowed to connect, comma separated.  May include netmasks.
# allowedhosts=192.168.1.200,10.10.10.0/255.255.255.0
droneallowedhosts=127.0.0.1,192.168.1.200
# Maximum number of drone clients
dronemaxclients=10
droneringlen=65535

# Do we have a GPS?
gps=false
# Do we use a locally serial attached GPS, or use a gpsd server?
# (Pick only one)
gpstype=gpsd
# gpstype=serial
# What serial device do we look for the GPS on?
gpsdevice=/dev/rfcomm0
# Host:port that GPSD is running on.  This can be localhost OR remote!
gpshost=localhost:2947
# Do we lock the mode?  This overrides coordinates of lock "0", which will
# generate some bad information until you get a GPS lock, but it will
# fix problems with GPS units with broken NMEA that report lock 0
gpsmodelock=false
# Do we try to reconnect if we lose our link to the GPS, or do we just
# let it die and be disabled?
gpsreconnect=true

# See the README for full information on the new source format
# ncsource=interface:options
ncsource=wlan0:type=mac80211,prism0,Kismet-Drone
# for example:
# ncsource=wlan0
# ncsource=wifi0:type=madwifi
# ncsource=wlan0:name=intel,hop=false,channel=11

# Special per-source options
# sourceopts=[sourcename|*]:opt1,opt2
# sourceopts=*:fuzzycrypt,weakvalidate

# Comma-separated list of sources to enable, if you don't want to enable all
# the sources you defined.
# enablesource=source1,source2

# How many channels per second do we hop?  (1-10)
channelvelocity=5

# By setting the dwell time for channel hopping we override the channelvelocity
# setting above and dwell on each channel for the given number of seconds.
- kismet_drone.conf 1/68 1%
```

Figura 3-64 Configuración del dron Kismet

Las últimas líneas del fichero de configuración definen los canales a cubrir durante la monitorización. Se dejan los valores por defecto.

Para monitorizar la interfaz *wlan0*, previamente hay que configurarla como se muestra en la Figura 3-65. Remarcar que la diferencia con respecto a los ficheros *wireless* de los routers que actúan como AP es que el modo de trabajo de la interfaz es *monitor*.

Figura 3-65 Configurando interfaz para monitorización

Ahora que se ha configurado el dron, debemos configurar el servidor Kismet para indicarle que monitorice el dron Kismet. Para ello accederemos a la carpeta *kismet* (*/etc/kismet*) del servidor y modificaremos el archivo *kismet.conf* (Figura 3-66).

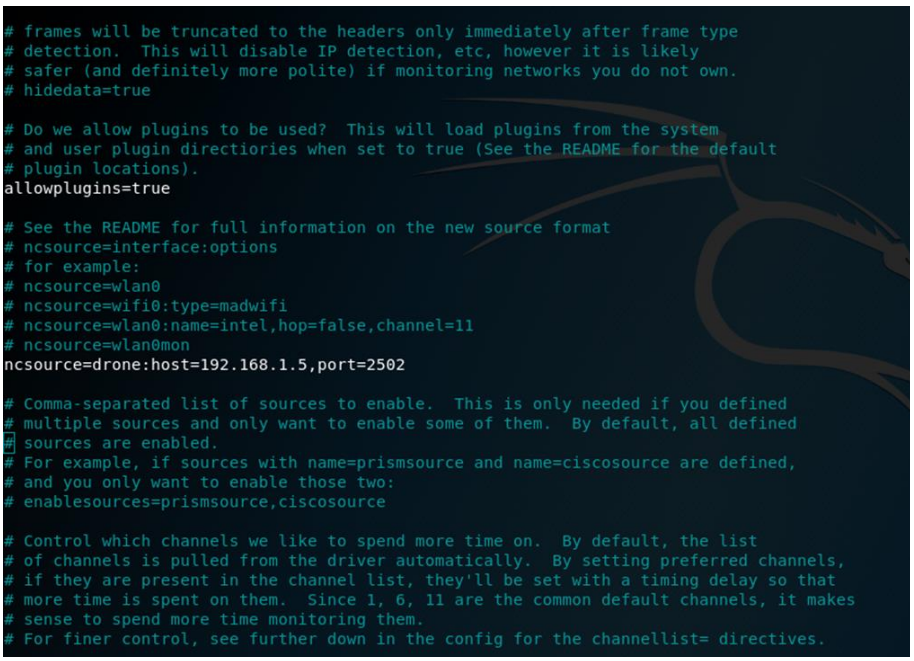


Figura 3-66 Configuración fichero *kismet.conf* en el servidor Kismet

El archivo de configuración es similar al del dron. Sólo añadiremos la fuente, en la que indicamos qué interfaz debe monitorizar. En nuestro caso, con *ncsource=drone:host=192.169.1.5, port=2502*, le estamos indicando que la interfaz es un dron, cuya IP y puerto son los del router en el que lo hemos instalado.

De esta forma quedaría el sistema Kismet configurado.

Para comenzar a monitorizar la red debemos lanzar, por un lado, el proceso *kismet_drone* y, por otro, el servidor y el cliente. Para lanzarlo desde el router, emplearemos el *software* PuTTY, entrando en la terminal del router y lanzándolo con el comando *kismet_drone* (Figura 3-67). En el portátil lo lanzaremos desde la terminal con el comando *sudo kismet*, y como resultado nos mostrará la interfaz cliente como ilustra la Figura 3-68, en la que nos pregunta si queremos lanzar el servidor.

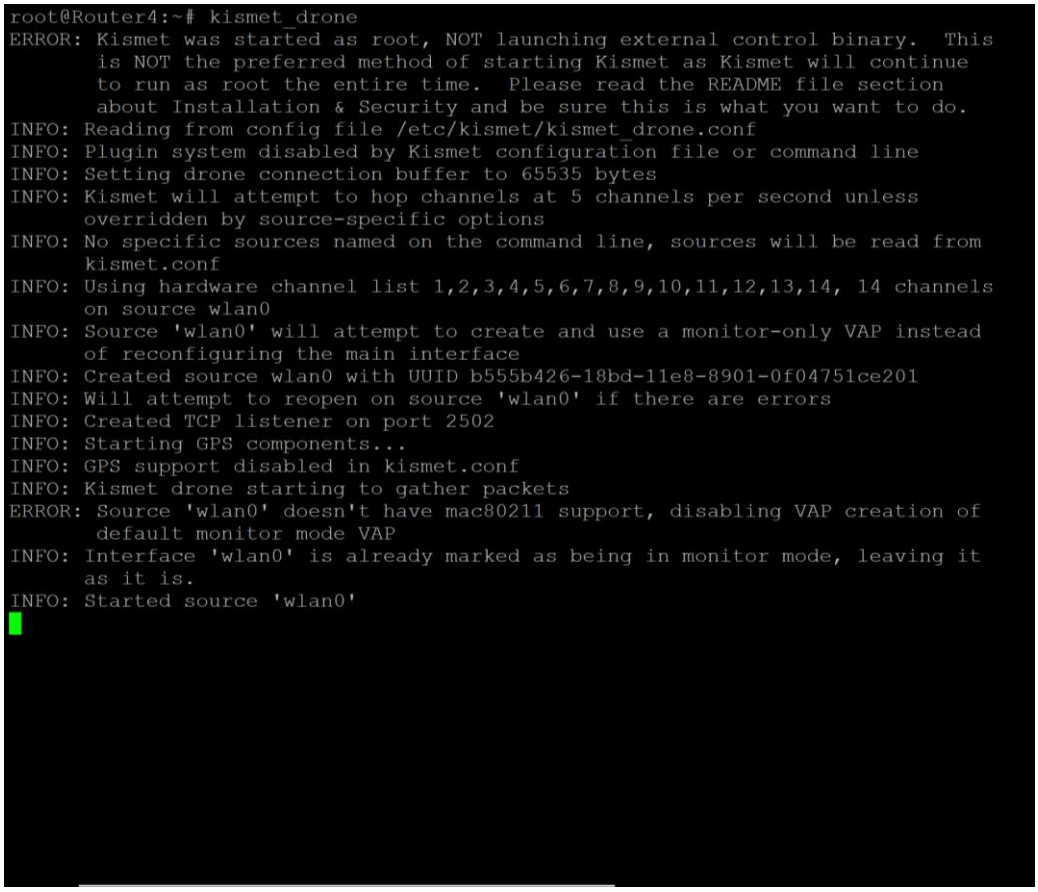


Figura 3-67 Lanzando *kismet_drone*

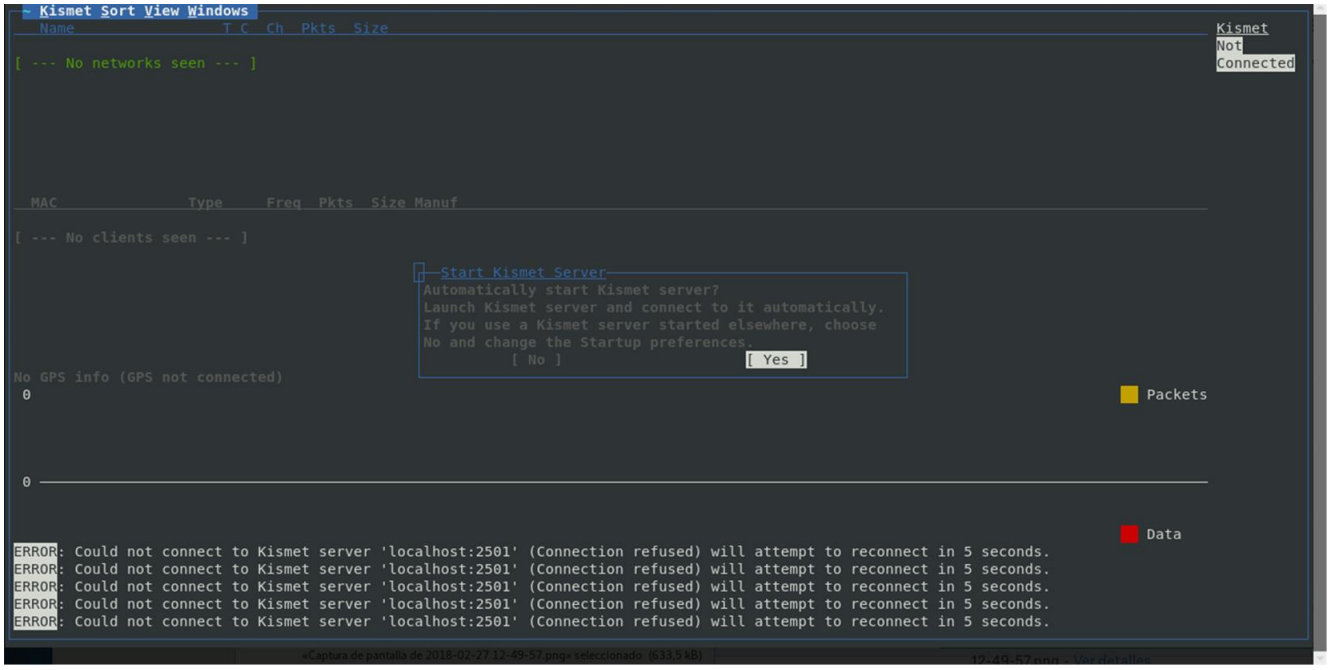


Figura 3-68 Interfaz cliente Kismet

Cuando pulsamos *Yes* se lanza el servidor y nos presenta en pantalla información de los AP´s detectados (Figura 3-69). Seleccionaremos la opción *Close Console window* para volver a la interfaz cliente inicial.

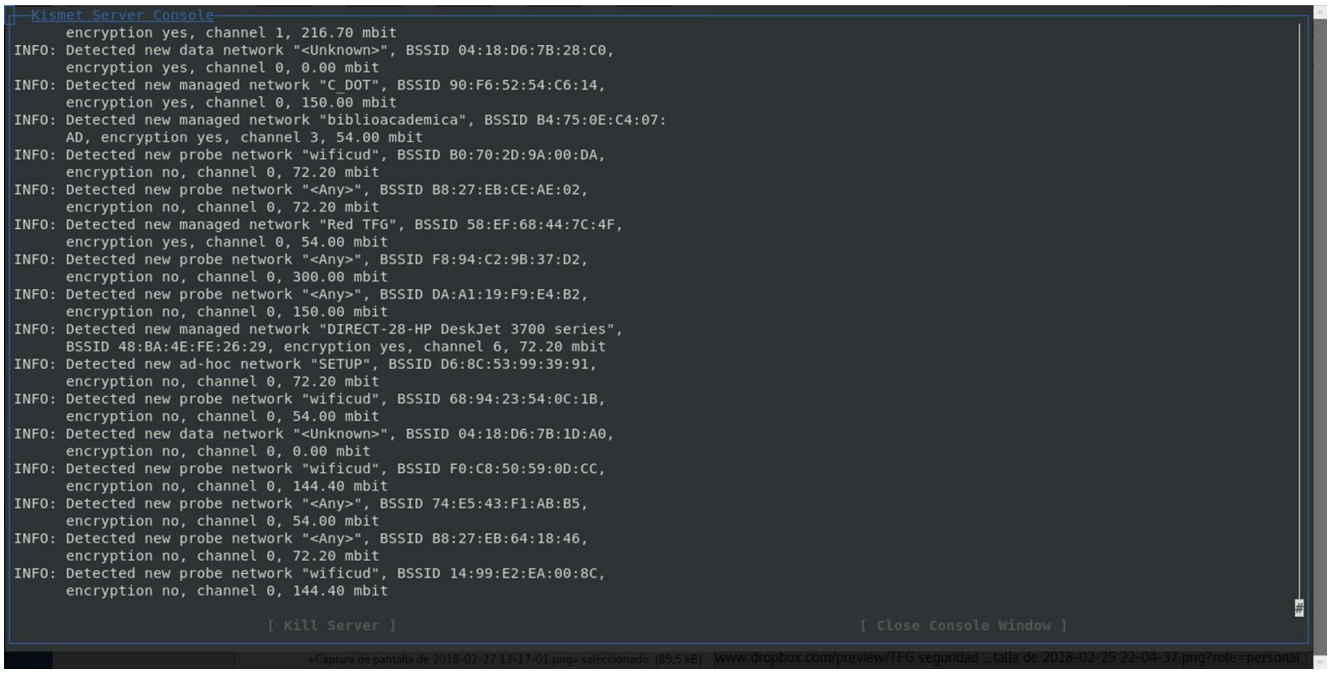


Figura 3-69 Captura de la consola del servidor Kismet

Seguidamente se presenta la pantalla principal que se divide en cuatro partes (ver Figura 3-70):

1. Se muestran todas las redes detectadas por el dron en su rango de cobertura. Muestra incluso las redes ocultas de Red TFG. Además, si se selecciona cada red, muestra información adicional, como la dirección MAC del router, o el tipo de cifrado de seguridad de la red. La información de las columnas puede tomar los siguientes valores:
    - *Name*: nombre de la red WiFi.
    - T: puede tomar los siguientes valores.
        - P, *probe request*, sin conexión asociada.
        - A, *Access point*, conexión inalámbrica estándar.
        - H, *Ad-hoc*, red inalámbrica punto a punto.
        - T, *Turbocell*, empleo de un router Karlnet o Lucent.
        - G, *Group*, grupo de redes inalámbricas.
        - D, *Data*, una red datos sin control de paquetes.
    - C: cifrado empleado en la red.
        - N, no emplea cifrado.
        - Y, emplea cifrado WEP.
        - O, emplea otro tipo de cifrado.
    - Ch: indica el canal de la red.
    - *Pkts*: indica el número de paquetes capturados.
    - *Size*: muestra el tamaño de los paquetes capturados.

2. Muestra las direcciones MAC de los dispositivos conectados a la red, y la forma a la que están conectados. Además, da información de los paquetes asociados a cada cliente. Esta información es valiosa para monitorizar que los usuarios conectados a la red sean legítimos (asumiendo la vulnerabilidad provocada por *MAC Spoofing*) y detectar actividad inusual por parte de algún usuario.
3. Este apartado muestra de forma gráfica el total de paquetes y datos monitorizados por Kismet.

4. En el margen derecho se muestra el tiempo que se lleva ejecutando Kismet (*Elapsed*), la lista de redes inalámbricas (*Networks*) que no coincide con la lista de redes del apartado 1. *Packets* muestra los paquetes totales monitorizados. *Pkt/Sec* indica los paquetes analizados cada segundo.

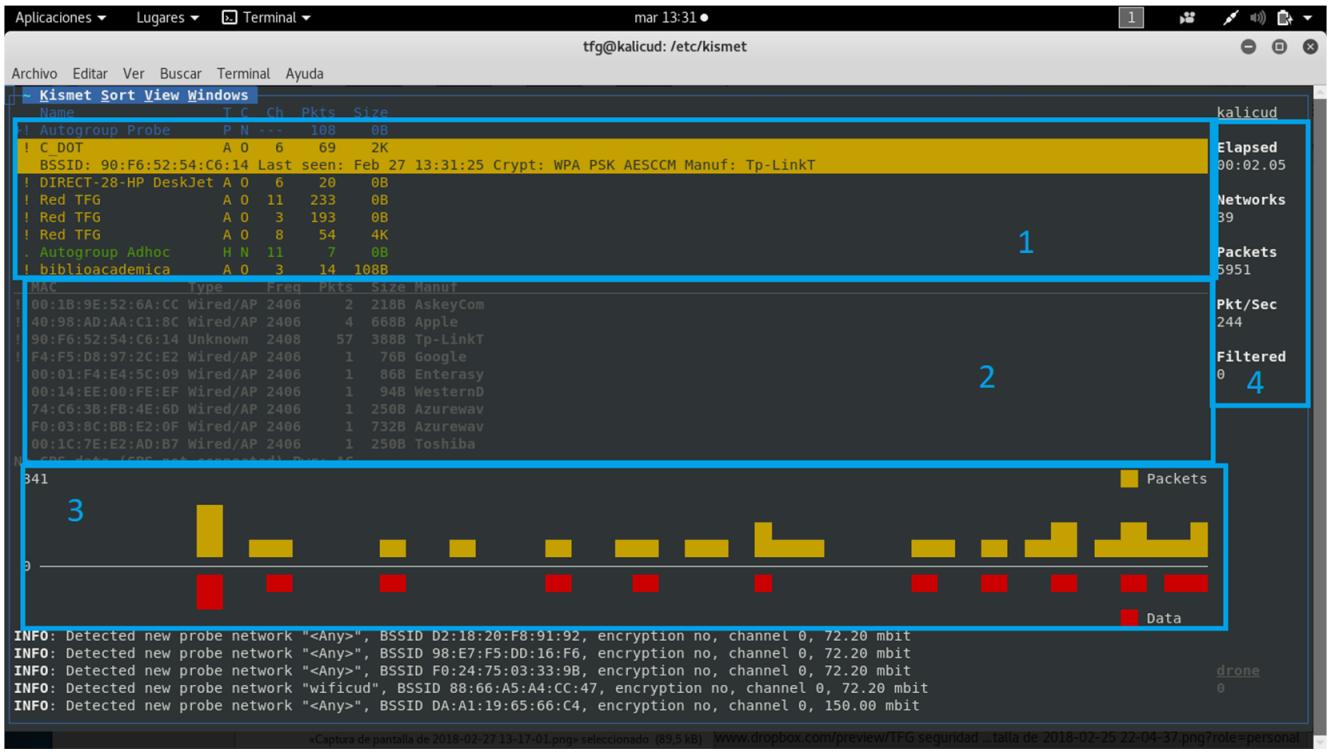


Figura 3-70 Pantalla principal cliente Kismet

Si seleccionamos una red, por ejemplo, Red TFG, y pulsamos *Enter*, podemos ver más información de esa red, como se muestra en la Figura 3-71. Un dato adicional que aporta esta ventana es *Seen By: drone (drone)*, que nos indica de dónde proviene la información de esta red. Esto es útil si tenemos varios drones funcionando de forma simultánea o el propio dispositivo dónde instalamos Kismet. La zona de *Packet Rate* muestra el tráfico de paquetes de la red en tiempo real.

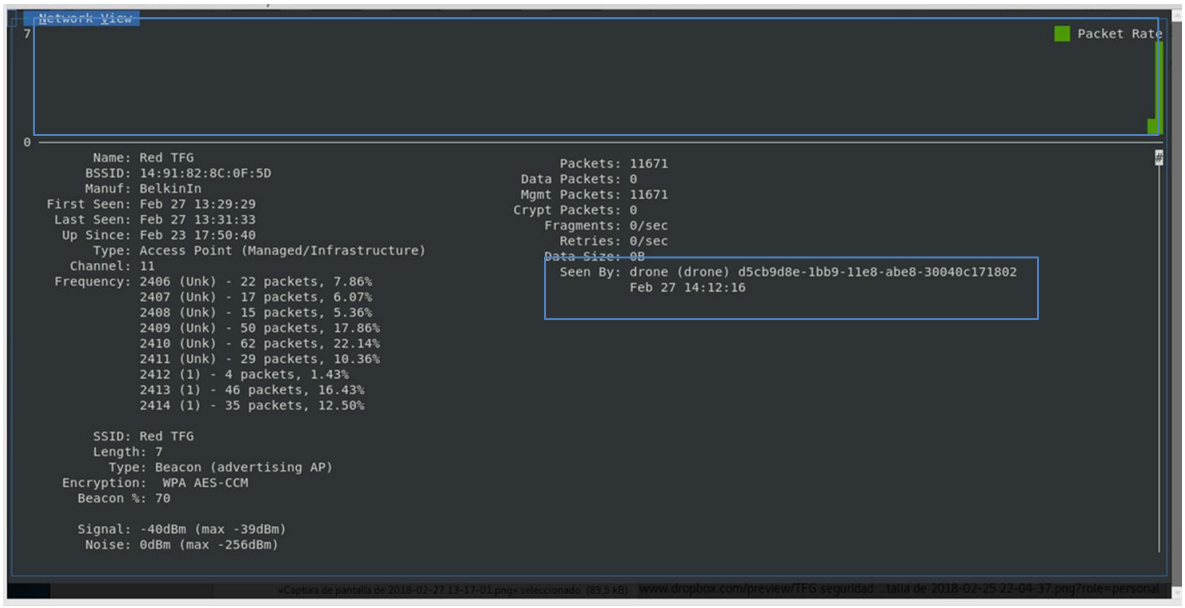


Figura 3-71 Detalle de Red TFG, desde el cliente Kismet

Con Kismet vienen una serie de alertas programadas por defecto. En este caso, interesa *APSPOOF*, que nos permite detectar *Rogue AP*, emitiendo una alarma cuando aparece una red inalámbrica que parte de un punto de acceso no incluido en la lista de direcciones MAC autorizadas de Kismet (Figura 3-72).

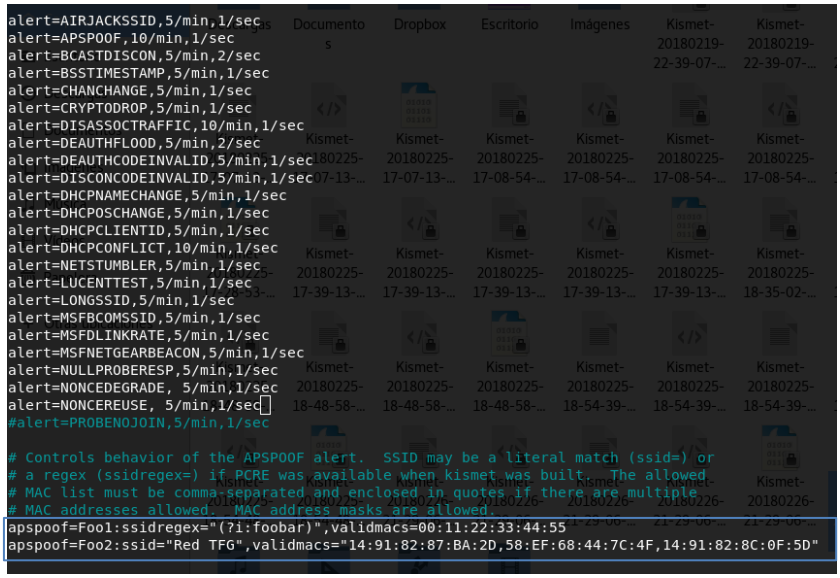


Figura 3-72 Alertas Kismet y MACs autorizadas para Red TFG

Se procede a comprobar la funcionalidad de esta alerta creando un punto de acceso para la Red TFG desde un dispositivo Android (ver Figura 3-73). Se comprueba que Kismet detecta el punto de acceso no autorizado, creado por el dispositivo Android y genera una alerta (Figura 3-74).

Figura 3-73 Red TFG, punto de acceso en dispositivo Android

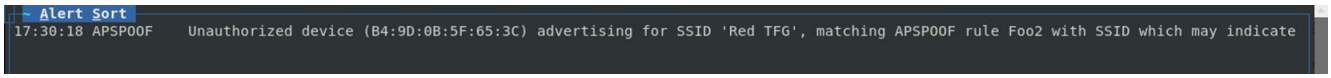


Figura 3-74 Alerta APSPOOF por *Rogue AP* Android

Con esto concluiría la configuración necesaria que requiere una red inalámbrica WiFi según el ENS.

Además, podemos utilizar Kismet para detectar ataques KRACK, vulnerabilidad no contemplada por la guía CCN-STIC-816, y configuración no recogida en el ENS:

- Para realizar un ataque KRACK, se debe clonar la dirección MAC de un punto de acceso, pero en diferente canal. Kismet generará una alerta CHANCHANGE (para el cambio de canal) o BSSTIMESTAMP si detecta dos puntos de acceso en conflicto. Éste es un buen indicio para saber si se está iniciando un ataque, sin embargo, en un futuro esto puede ser menos obvio.
- La mayoría de los ataques KRACK retransmiten un valor *nounce* previamente empleado, tanto en el primer como en el tercer *handshake*. Kismet monitoriza los 128 *nonce* previos vistos y si es detectado un *nonce* repetido, lanza la alerta NONCEREUSE.

4 VALIDACIÓN DEL TFG

En este capítulo se expondrá cómo las medidas implementadas contribuyen a aumentar el nivel de seguridad de la red. Así, en un primer apartado, se presentará una comparativa inicial con una red con seguridad doméstica y las amenazas que mitigan las medidas tomadas. En el segundo apartado, se realizarán una serie de pruebas para mostrar la eficacia de las medidas implantadas.

4.1 Medidas implementadas y objetivos de seguridad alcanzados

En las tablas que comprenden de la 4-1 a la 4-13 se recogen las medidas que añade la guía CCN-STIC-816, adoptadas en la red WiFi desplegada en este TFG.

Medida doméstica	**Medida CCN-STIC-816**
Claves WPA2 con PSK	Claves WPA2 con Servidor RADIUS
Soluciona	
Evitamos una única clave conocida por todos los usuarios de la red. Cada usuario tiene su *login* y contraseña para conectarse a la red, pudiendo limitar el número de accesos simultáneos por cuenta, y el tiempo de conexión de cada usuario. Además, permite dar de alta o de baja a usuarios sin perturbar al resto de usuarios. El tener un *login* y contraseña por usuario implica el paso a autenticación de doble factor, debiendo el atacante de conseguir ambos parámetros. El empleo de RADIUS ya implica uso de EAP, PAP, CHAP, etc.	

Tabla 4-1 Medida 1

Medida doméstica	**Medida CCN-STIC-816**
Claves WPA2 con TKIP	Claves WPA2 con CCMP
Soluciona	
A pesar de la vulnerabilidad actual de ambos WPA2, TKIP presenta serias vulnerabilidades ya conocidas, mientras que CCMP solventa estas vulnerabilidades. Mencionar que KRACK no ha sido aún liberado por su creador al público.	

Tabla 4-2 Medida 2

Medida doméstica	Medida CCN-STIC-816
Claves WEP	Claves WPA2
Soluciona	
Claves WEP quedan totalmente descartadas	

Tabla 4-3 Medida 3

Medida doméstica	Medida CCN-STIC-816
No filtrado MAC	Filtrado MAC
Soluciona	
Esta medida no deja de ser una medida disuasoria ya que las técnicas MAC *Spoofing* permiten a un usuario cambiar la dirección MAC de su dispositivo, y un atacante podría cambiarla por una que se encuentre en la lista de MAC´s autorizadas. No deja de ser una primera barrera para atacantes inexpertos.	

Tabla 4-4 Medida 4

Medida doméstica	Medida CCN-STIC-816
Parámetros predefinidos	Parámetros modificados
Soluciona	
El empleo de parámetros por defecto hace la red vulnerable a ataques de diccionario. Los parámetros a modificar son: dirección IP de acceso al router, puerto de acceso SSH, SSID, contraseña (en el caso de OpenWrt, la red hay que configurarla de cero, pero routers de ISP traen la red configurada por defecto).	

Tabla 4-5 Medida 5

Medida doméstica	Medida CCN-STIC-816
Contraseñas de red de baja seguridad	Contraseñas de red de alta seguridad
Soluciona	
El evitar emplear contraseñas de alta seguridad nos da una mayor protección frente ataques de diccionario. Se deben emplear contraseñas con un mínimo de longitud, que combinen mayúsculas, minúsculas, símbolos y números.	

Tabla 4-6 Medida 6

Medida doméstica	Medida CCN-STIC-816
Emisión del SSID	Ocultar SSID
Soluciona	
Anular el *broadcast* del SSID nos permite evitar mostrar la existencia de la red WiFi a personas no pertenecientes a la organización. Sirve como una primera medida disuasoria para posibles atacantes.	

Tabla 4-7 Medida 7

Medida doméstica	Medida CCN-STIC-816
AP funcionando siempre	AP apagado en horario no laborable
Soluciona	
Mitiga el riesgo de ser atacado, apagando los puntos de acceso en horario no laborable. Nuestros routers no se pueden apagar y volver a encender, así que lo que hacen es apagar la interfaz WiFi en el periodo establecido.	

Tabla 4-8 Medida 8

Medida doméstica	Medida CCN-STIC-816
Canales aleatorios	Selección de canales
Soluciona	
En el entorno doméstico el solape de canales puede ser un problema. En el entorno de la organización una buena gestión de los canales nos permite evitar interferencia entre los distintos AP.	

Tabla 4-9 Medida 9

Medida doméstica	Medida CCN-STIC-816
Contraseña administrador router predeterminada	Contraseña administrador router alta seguridad
Soluciona	
Los routers comerciales suelen presentar usuario y contraseña "admin" o usuario "admin" y contraseña "1234", permitiendo a cualquier atacante acceder a los parámetros de configuración del router y obtener acceso total a la red.	

Tabla 4-10 Medida 10

Medida doméstica	Medida CCN-STIC-816
Diversas opciones de gestión del AP	Deshabilitar accesos a AP inseguros
Soluciona	
Nuestro router nos permite configurarlo vía telnet, vía SSH, por HTTP, o HTTPS. En nuestro caso, se desactiva la opción de configurar por medio de HTTP, por no ser segura, y al no soportar HTTPS, será SSH el método de configuración de los routers.	

Tabla 4-11 Medida 11

Medida doméstica	Medida CCN-STIC-816
WPS activo	WPS desactivado
Soluciona	
WPS es un protocolo diseñado para facilitar la gestión de redes inalámbricas en entornos domésticos en los que se usan claves precompartidas. WPS se basa en la utilización de un código PIN, que se obtiene del punto de acceso. Este PIN está compuesto por ocho cifras divididas en dos bloques de cuatro cifras. La obtención del PIN es sencilla y puede arruinar la seguridad de la red aunque el resto de ella haya sido debidamente securizada.	

Tabla 4-12 Medida 12

Medida doméstica	Medida CCN-STIC-816
Puerto de acceso router: 22	Puerto de acceso router: 1537
Soluciona	
Modificar el puerto de acceso mediante SSH al router es una capa de seguridad más que añadimos al acceso al router. Para acceder a la configuración del router no sólo hace falta usuario y contraseña, si no que ahora es necesario saber el puerto.	

Tabla 4-13 Medida 13

4.2 Pruebas de *pentesting*

En este apartado se procede a mostrar cómo ciertas vulnerabilidades de seguridad son corregidas siguiendo las medidas reflejadas en la guía CCN-STIC-816.

PRUEBA 0: FILTRADO MAC Y SSID OCULTO

Esta primera prueba se destina a una serie de medidas que, aunque no puedan ser consideradas configuraciones de seguridad como tal, aportan una pequeña capa de seguridad, que evitarla ya implica una serie de conocimientos técnicos básicos. Estas medidas son el filtrado MAC y el SSID oculto.

En este apartado se procederá a mostrar cómo se puede eludir esta primera capa de defensa.

En primer lugar, se va a eludir el filtrado MAC. Se empleará un filtro MAC que permite la conexión de un único equipo con MAC B4:9D:0B:5F:65:3C (véase Figura 4-1).

Figura 4-1 Filtrado MAC de Red TFG

Para obtener el acceso a la red, la monitorizaremos con *airodump-ng*, *software* que se detallará más adelante. En la Figura 4-2 se pueden ver los equipos conectados a la Red TFG. En el apartado STATION vemos conectado al equipo con MAC B4:9D:0B:5F:65:3C. Ya sabemos qué dirección MAC queremos conseguir.

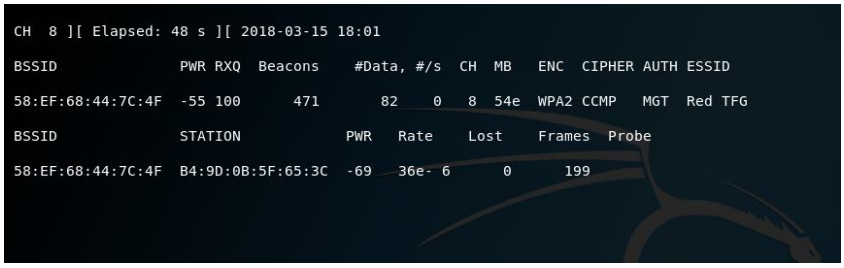


Figura 4-2 Monitorización de Red TFG

Para cambiar la dirección MAC del equipo con el que queremos acceder a la red empleamos el comando *sudo macchanger mac= B4:9D:0B:5F:65:3C wlan0*, la secuencia de comandos se puede ver en la Figura 4-3.

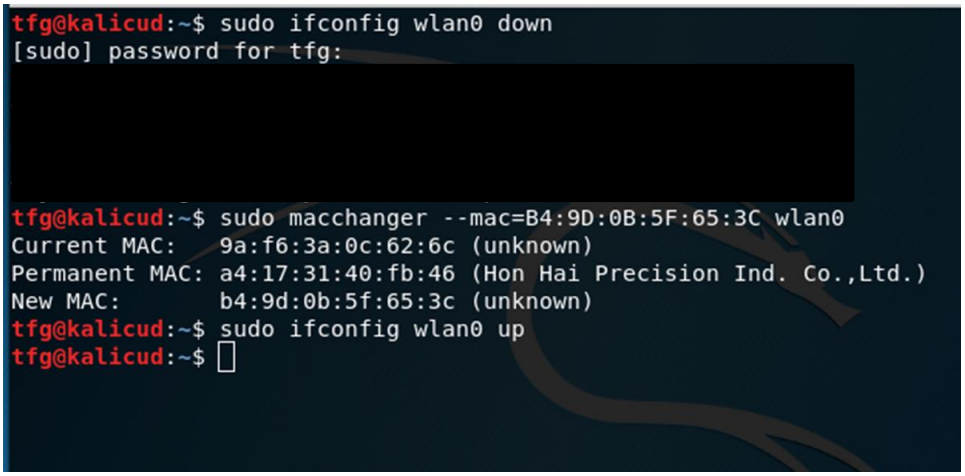


Figura 4-3 Cambio de dirección MAC

A continuación, abordaremos la medida de SSID oculto. Empleando un *software* como Kismet, mencionado en el capítulo 3 las redes ocultas muestran su nombre directamente en la interfaz. En este apartado se debe mencionar que, aunque la guía CCN-STIC-816 recomiende esta medida para incrementar la seguridad, otras fuentes consideran insegura esta medida debido a los ataques KARMA [56].

Los ataques KARMA aprovechan los mensajes *probe request* que algunos dispositivos WiFi envían para detectar la presencia de redes WiFi conocidas. En este caso, en lugar de ser el router quien informa de su presencia y el usuario el que confirma el acceso a la red, es el dispositivo el que busca la red (emite) para conectarse a ella. De esta forma, conociendo cualquiera de las redes guardadas en el dispositivo se puede crear un *Rogue AP* al que el dispositivo se conectaría.

La mayoría de los dispositivos actuales eliminaron el envío de estos mensajes *probe request*, sin embargo, si se guarda el SSID de una red oculta, la única forma de volver a conectarse a él es mediante el envío de mensajes *probe request*. Por tanto, aunque nuestro dispositivo no sea vulnerable a ataques KARMA, el tener una red con el SSID oculto guardada en el equipo nos hace vulnerables de nuevo.

PRUEBA 1: INTERFAZ WEB INSEGURA CON HTTP

En primer lugar, se demuestra cómo la interfaz LuCI es insegura en su versión HTTP.

El empleo de HTTP implica que la transferencia de paquetes se hace sin cifrado. Se emplea Wireshark para monitorizar la WiFi Red TFG. Se accede a la interfaz web LuCI desde el navegador web, introduciendo en la barra de dirección 192.168.1.2 (Figura 4-4). Esta dirección abre la herramienta de configuración del router *Master*. En la Figura 4-5 se introducen las credenciales de

acceso a la web, nótese que ya el navegador nos avisa en la barra de direcciones del no cifrado de la página.

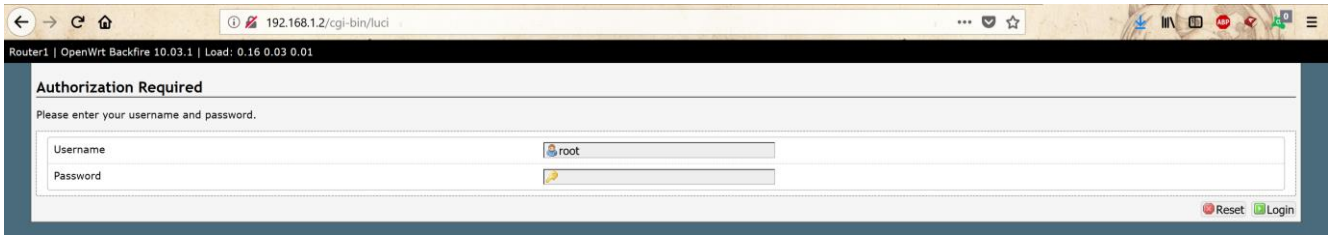


Figura 4-4 Acceso a configuración del router vía LuCI

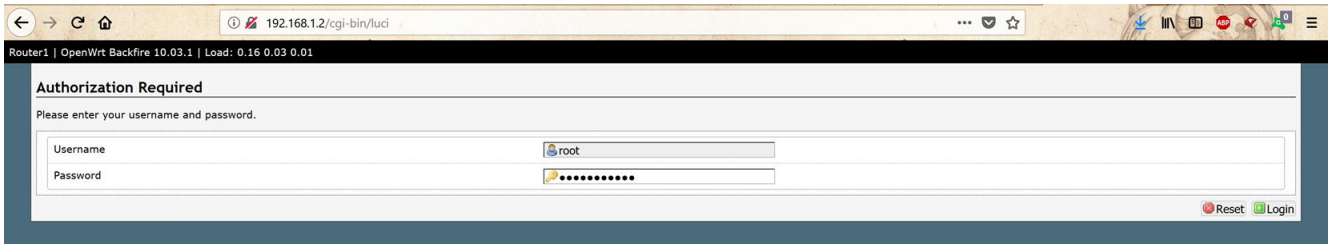


Figura 4-5 *Login* en web LuCI

Como se ve en la Figura 4-6, cualquiera con el *software* Wireshark y un ordenador conectado a la red podría obtener las credenciales de acceso al router *Master* y cambiar la configuración. Incluso dejando al administrador sin acceso al router, cambiando esas credenciales.

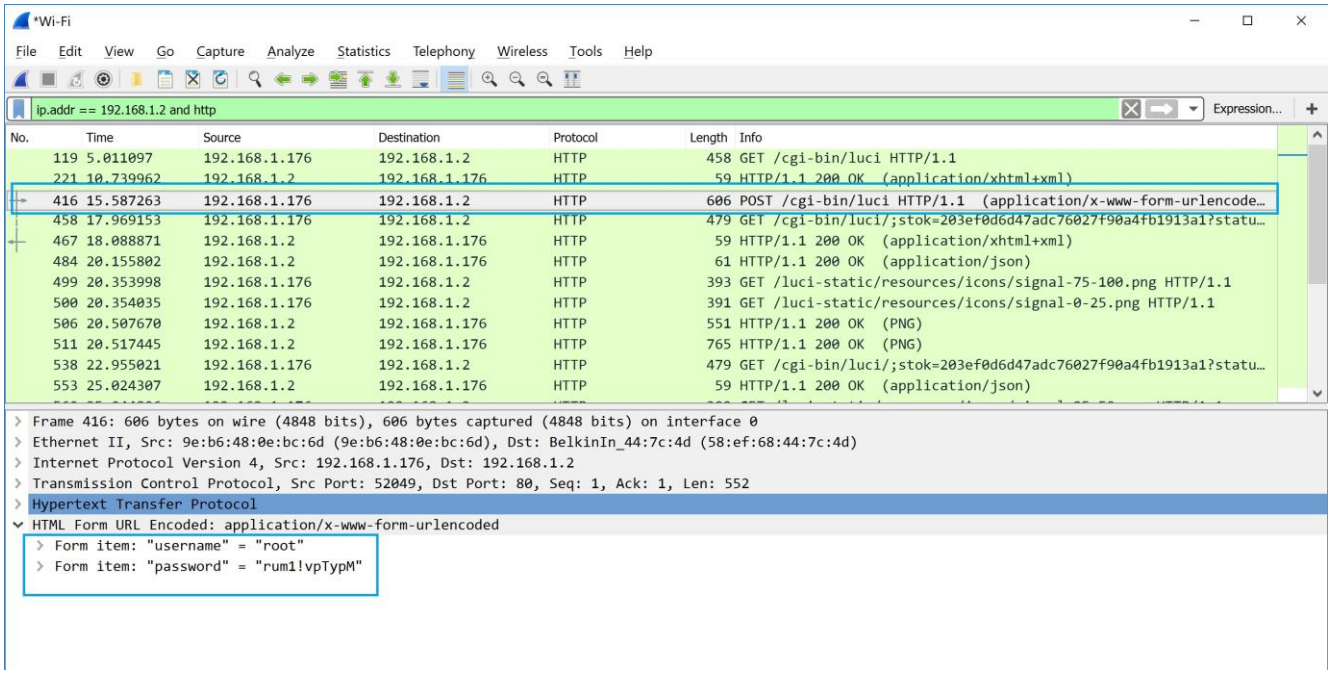


Figura 4-6 Captura paquete HTTP con la contraseña de acceso al router Master

PRUEBA 2: INTERFAZ WEB SEGURA CON TÚNEL SSH

La siguiente prueba que se realiza es acceder a la interfaz LuCI activando previamente el túnel SSH que se creó en el capítulo 3. Se accederá empleando el mismo navegador que en el caso anterior. Se accede a través de la dirección 127.0.0.1:8000.

Previamente se lanza desde PuTTY el túnel, véase Figura 4-7.

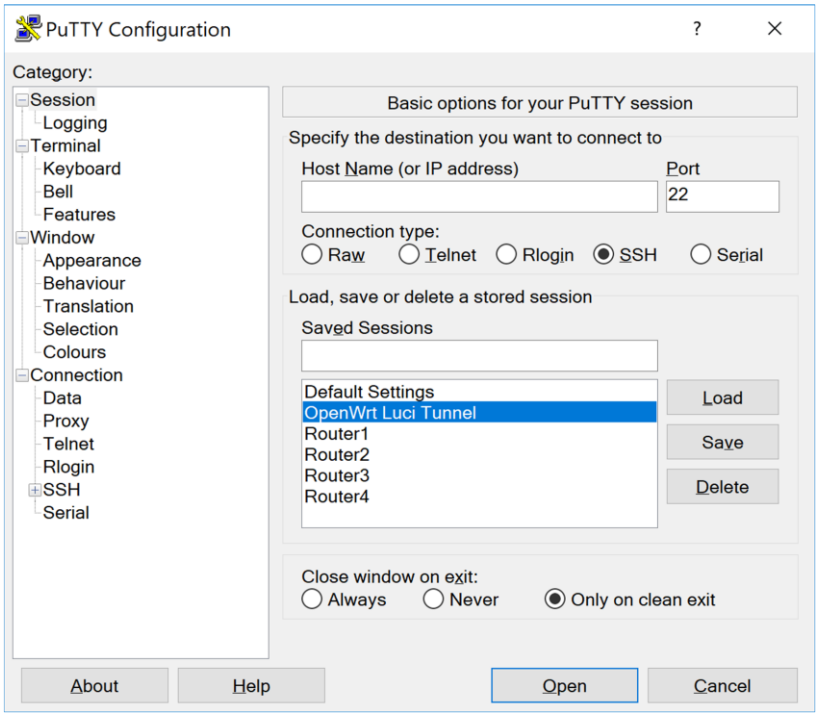


Figura 4-7 Lanzamiento *OpenWrt Luci Tunnel*

La Figura 4-8 muestra cómo se accede a la misma página a través del túnel.

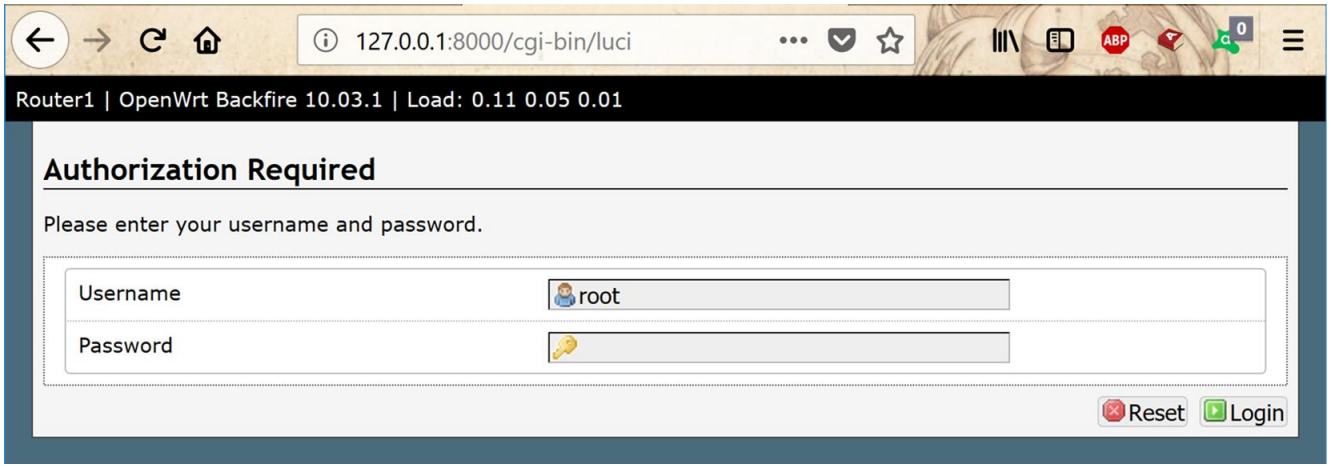


Figura 4-8 Acceso LuCI a través de túnel SSL

Como se puede ver en la Figura 4-9, todos los paquetes de protocolo HTTP desaparecen y las credenciales de acceso no se muestran en ningún paquete.

Lo mismo ocurre cuando se emplea PuTTY para acceder a configurar los routers mediante la terminal. La información de los paquetes no es visible.

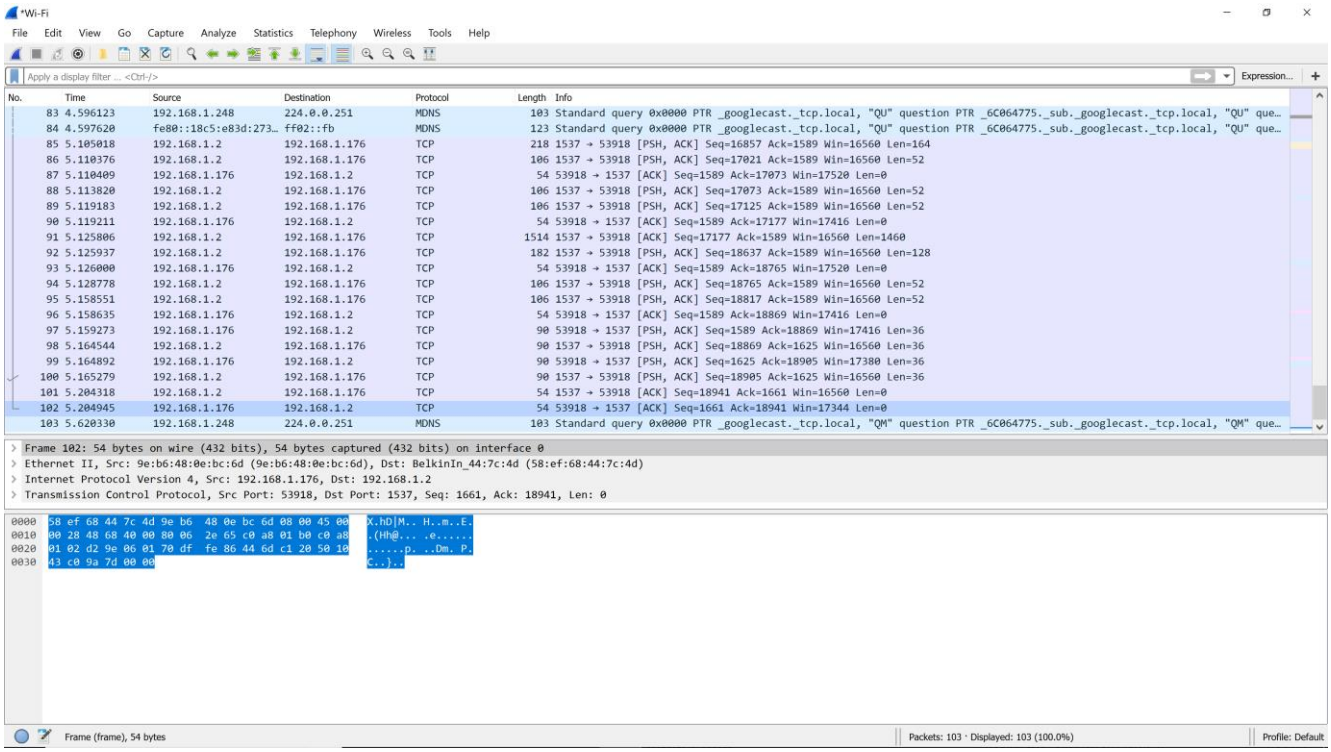


Figura 4-9 Captura paquetes TCP tras activar túnel SSH

PRUEBA 3: OBTENCIÓN DE CREDENCIALES FREERADIUS NO ROBUSTAS

Se decide comprobar la seguridad del sistema FreeRADIUS para el acceso a Internet. Se realiza una primera prueba con el usuario Jesús y la contraseña pollos. Emplearemos el *software hostapd-wpe* para la comprobación.

Hostapd-wpe simula un punto de acceso (*Rogue AP*) al que los usuarios se conectarán y recoge sus credenciales de acceso, su usuario y contraseña cifrada.

Después de instalarlo (Figura 4-10), configuramos el *software*.

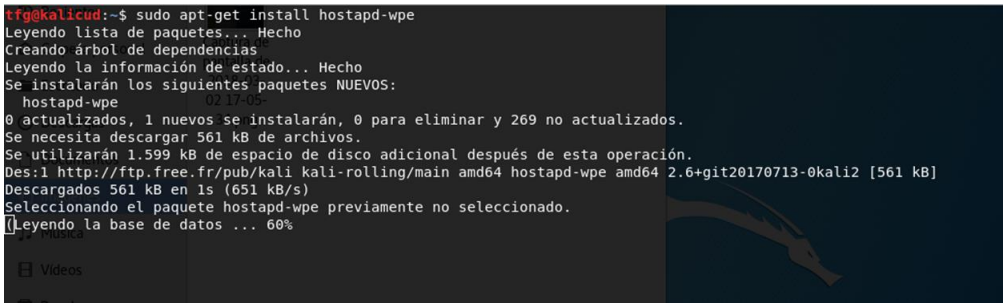


Figura 4-10 Instalación *hostapd-wpe*

La configuración permite editar un elevado número de parámetros para hacer más semejante el *Rogue AP* al AP original. Entre los parámetros podemos modificar el método EAP empleado, los certificados de autenticación a emplear, el SSID o el canal. Cuantas más características compartan, más sencillo es conseguir que un usuario se conecte de forma inconsciente al *Rogue AP*.

En nuestro caso, se realiza una configuración sencilla en la que sólo se modifica el SSID. En la Figura 4-11 se muestra el cambio del SSID *hostapd-wpe* a Red TFG, emulando la red del presente proyecto.

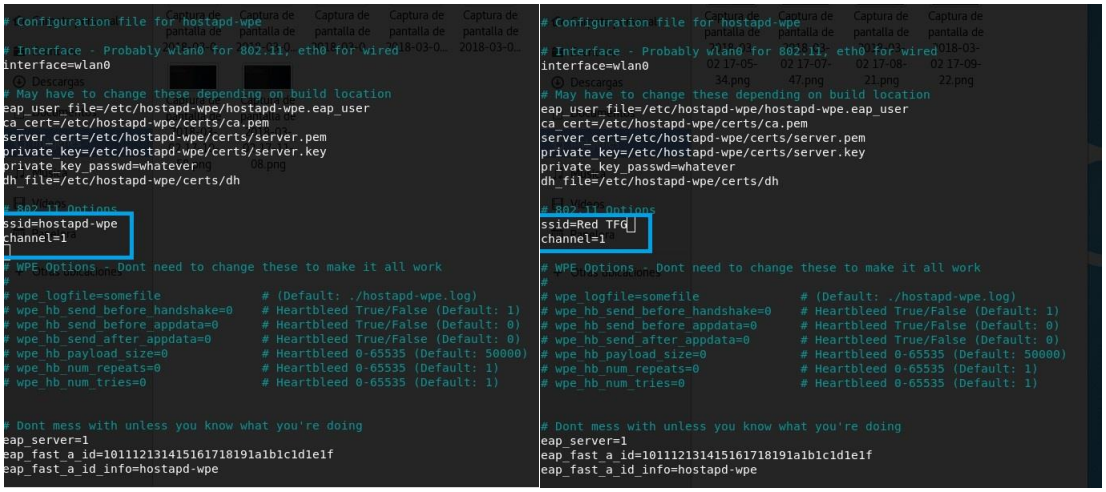


Figura 4-11 Cambio de SSID para *hostapd-wpe*

Como se muestra en la Figura 4-12 se emplea el comando:

```
sudo hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
```

Con el que se lanza *hostapd-wpe* cargando la configuración que hemos establecido previamente. Las primeras líneas de la interfaz son las que indican que se ha lanzado el *Rogue AP* y que un usuario se está intentando conectar a la red.

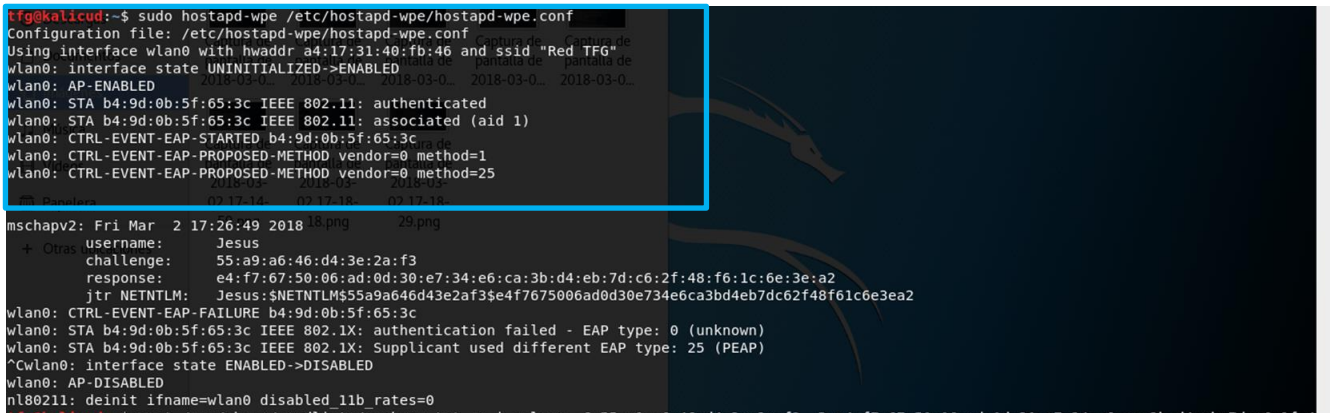


Figura 4-12 Lanzamiento *hostapd-wpe*

En la Figura 4-13 se muestra cómo, tras un intento de conexión con un móvil Android al *Rogue AP*, creado por *hostapd-wpe*, se capturan las credenciales del usuario, usuario en claro y la contraseña cifrada.

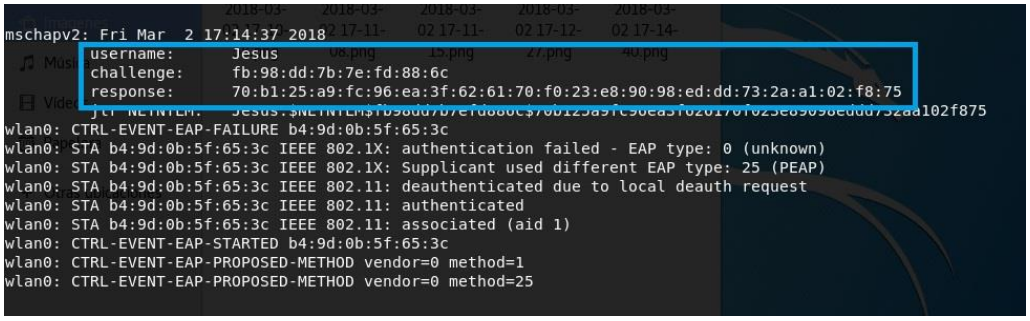


Figura 4-13 Obtención credenciales usuario Jesus

A continuación, se realiza un ataque de diccionario (se utiliza el fichero *rockyou.txt*) para obtener la contraseña en claro. Los datos a introducir son el *challenge* y *response* (Figura 4-14).

Figura 4-14 Empleo diccionario para descifrado de clave

En la Figura 4-15 se muestra la contraseña del usuario en claro (pollos).

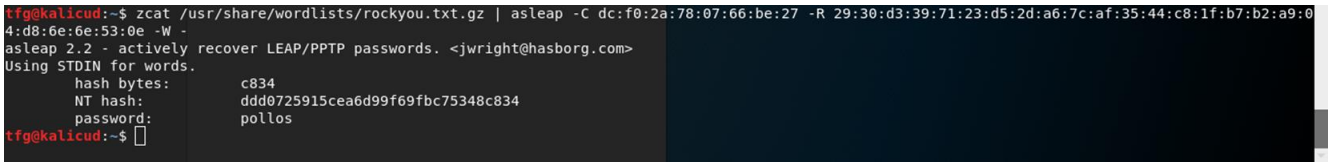


Figura 4-15 Contraseña del usuario Jesus descifrada

PRUEBA 4: OBTENCIÓN DE CREDENCIALES FREERADIUS ROBUSTAS

Seguidamente se repite el proceso empleando una contraseña más segura que sigue el patrón mencionado en el capítulo 3. La contraseña es 'tsm1!vpTypM1537'. El resultado es negativo (*I´ve given up. Sorry it didn´t work out*), como se puede ver en la Figura 4-16 con esto se demuestra la importancia del empleo de unas claves robustas por los usuarios de la red.

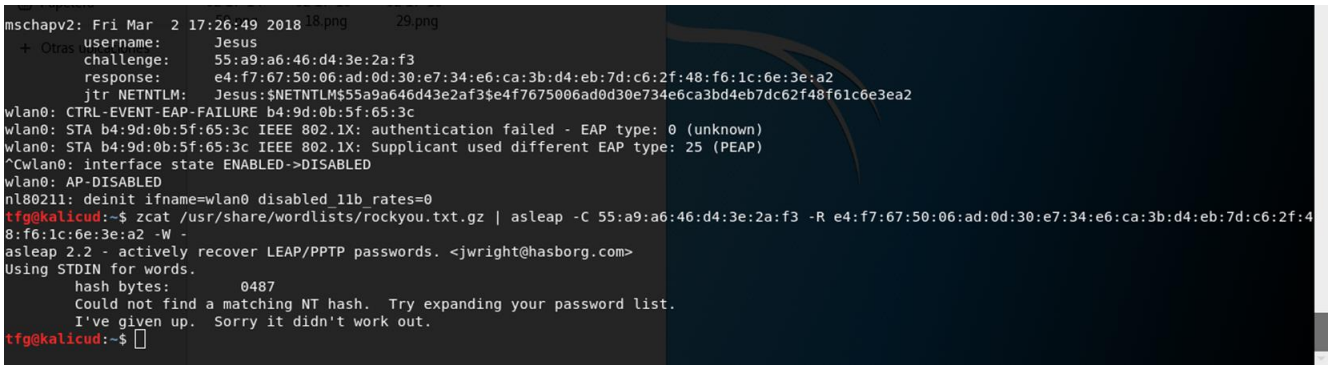


Figura 4-16 Intento fallido de obtención de contraseña

Hostapd-wpe además genera un archivo log con el registro de los distintos intentos de conexión con su correspondiente *username*, *challenge* y *response* para acceder a ellos posteriormente.

La conclusión que sacamos de las pruebas 3 y 4 es la siguiente, la elección de una contraseña robusta es importante. Sin embargo, si los usuarios toman ciertas medidas para evitar la conexión a redes falsas directamente se ataja el problema de que nos puedan sustraer la contraseña o ser víctimas de otro tipo de ataque. Para ello se debe concienciar a los usuarios de la red y se les debe educar en buenas prácticas como pueden ser, por ejemplo: no tener la búsqueda de WiFi permanentemente conectada o en caso de que el dispositivo lo permita guardar la BSSID del AP además de su ESSID.

PRUEBA 5: CRACKEO CONTRASEÑA WPA2 PERSONAL

En esta prueba se demostrará que los ataques realizados con el *software aircrack-ng* [57], una *suite* que recoge una amplia variedad de herramientas, no funcionan frente a una configuración de red WPA2 *Enterprise*. Primero, se realiza una prueba en una red WPA2 *Personal*. Se empleará la red la antigua red *wificud*, que a partir de ahora se llamará *wcud_cuartel* (el cambio de ESSID es ajeno a la realización de este proyecto).

El objetivo de esta prueba es *crackear* la clave empleada para acceder a una red objetivo (*wcud_cuartel*).

La prueba constará de seis pasos:

1. Activar interfaz de red Wireless en modo monitor con *airmon-ng*.
2. Monitorización de las distintas redes con *airodump-ng*.
3. Selección de la red objetivo a monitorizar.

4. Monitorización de la red objetivo con *airodump-ng*.
5. Capturar mensajes *handshake* durante autenticación de un usuario (se empleará *aireplay-ng*).
6. Ataque de diccionario para obtener la contraseña con *aircrack-ng*.

Para la realización de la prueba se emplea un adaptador de red *wireless* modelo *SMCWUSBS-N3* (véase Figura 4-17) conectado al portátil con Kali Linux. El adaptador se muestra en el ordenador creando la interfaz WiFi *wlan1*.

Figura 4-17 Adaptador *wireless* USB *SMCWUSBS-N3*

Para ver las interfaces WiFi disponibles, emplearemos el comando *sudo iwconfig* como se muestra en Figura 4-18.

```
tfg@kalicud:~$ sudo iwconfig
eth0      no wireless extensions.

wlan1     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Figura 4-18 Interfaces WiFi disponibles en portátil

Se pueden ver dos interfaces con extensión WiFi, *wlan0* y *wlan1*. El adaptador del portátil es *wlan0* y el del adaptador USB es *wlan1*. Ambos se encuentran actualmente en modo *Managed*, cumpliendo las funciones de conexión a la red.

A continuación, se emplea el comando *sudo airmon-ng start wlan1*, que cambia el modo de funcionamiento de la interfaz *wlan1* a monitor (Figura 4-19). La interfaz se renombra a *wlan1mon*. En la Figura 4-20 se muestra que *wlan1* ya no está listada y ahora se muestra *wlan1mon*, que se encuentra en modo monitor.

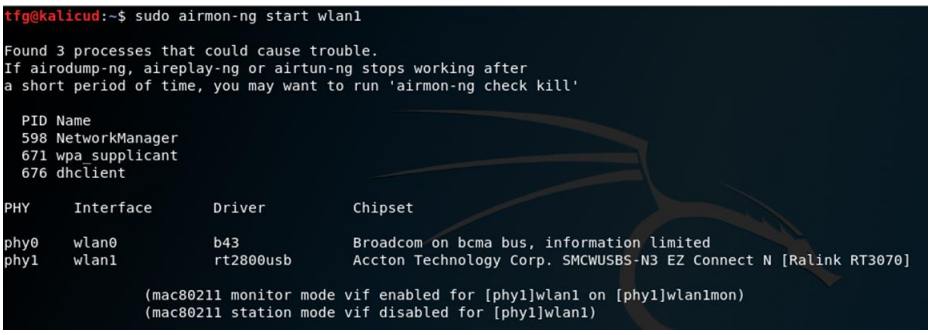


Figura 4-19 Cambio de modo de trabajo de *wlan1*

Figura 4-20 Lista de interfaces *wireless* tras lanzar *airmon-ng*

Una vez establecida la interfaz en modo monitor, procedemos a escanear el entorno para detectar redes WiFi. Para ello empleamos el comando:

```
sudo airodump-ng wlan1mon
```

Se lanzará la pantalla de monitorización que muestra la distribución de la Figura 4-21.

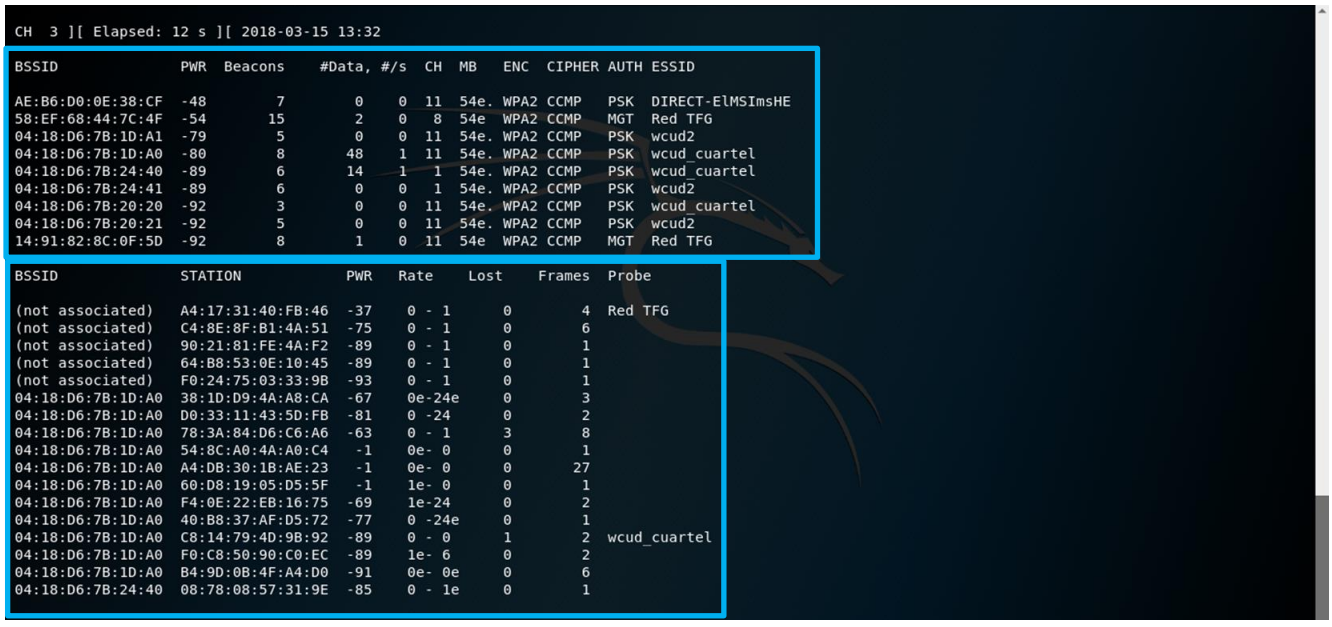


Figura 4-21 Pantalla de monitorización de *airodump-ng*

La pantalla se divide en dos bloques, superior e inferior. En el bloque superior aparecen las redes WiFi que se detectan desde la posición del ordenador.

De este bloque nos interesan los siguientes parámetros:

- BSSID: dirección MAC de los AP´s.
- CH: canal de trabajo de los AP´s.
- ENC: encriptación empleada, que puede ser: OPN (abierta), WEP, WPA o WPA2.
- CIPHER: cifrado empleado, puede ser TKIP o CCMP.
- AUTH: método de autenticación, puede ser PSK o MGT (indica el empleo de un servidor RADIUS).
- ESSID: nombre de la red.

El bloque inferior muestra todos los usuarios detectados en las distintas redes. Nos interesan dos parámetros: BSSID (dirección MAC del AP al que está conectado) y STATION (dirección MAC del dispositivo usuario).

En este punto seleccionaremos qué red es la objetivo. Elegimos la cuarta red que aparece en la Figura 4-21, *wcud_cuartel* con BSSID 04:18:D6:7B:1D:A0; la red trabaja en canal 11. Seguidamente, se procederá a monitorizar esta red. Empleamos el siguiente comando:

```
sudo airodump-ng -c 11 -bssid BSSID 04:18:D6:7B:1D:A0 wlan1mon -w ~/Descargas
```

Con `-w ~/Descargas`, *airodump-ng* crea un archivo de registro de la monitorización, necesario para el proceso.

El objetivo de monitorizar la red es capturar los paquetes de autenticación (*handshake*) de un usuario que se conecta. Se presentan dos opciones para esto, esperar hasta que un usuario se conecte a la red o forzar la expulsión y conexión de un usuario que ya esté conectado. Para la segunda opción se emplea *aireplay-ng*.

De forma paralela a la monitorización de la red lanzaremos *aireplay-ng* con el siguiente comando:

```
sudo aireplay-ng -0 2 -c 78:34:84:D6:C6:A6 -a 04:18:D6:7B:1D:A0 wlan1mon
```

Siendo:

- *-0*: el método de ataque a realizar, 0 es desautenticación.
- *2*: el número de veces que se repite el proceso.
- *-c*: la dirección MAC del cliente.
- *-a*: la dirección MAC del AP.
- *wlan1mon*: la interfaz que monitoriza.

Con este proceso se fuerza la captura del *handshake*. Se muestra en la Figura 4-22 la pantalla de monitorización de la red y el aviso de captura del *handshake*.

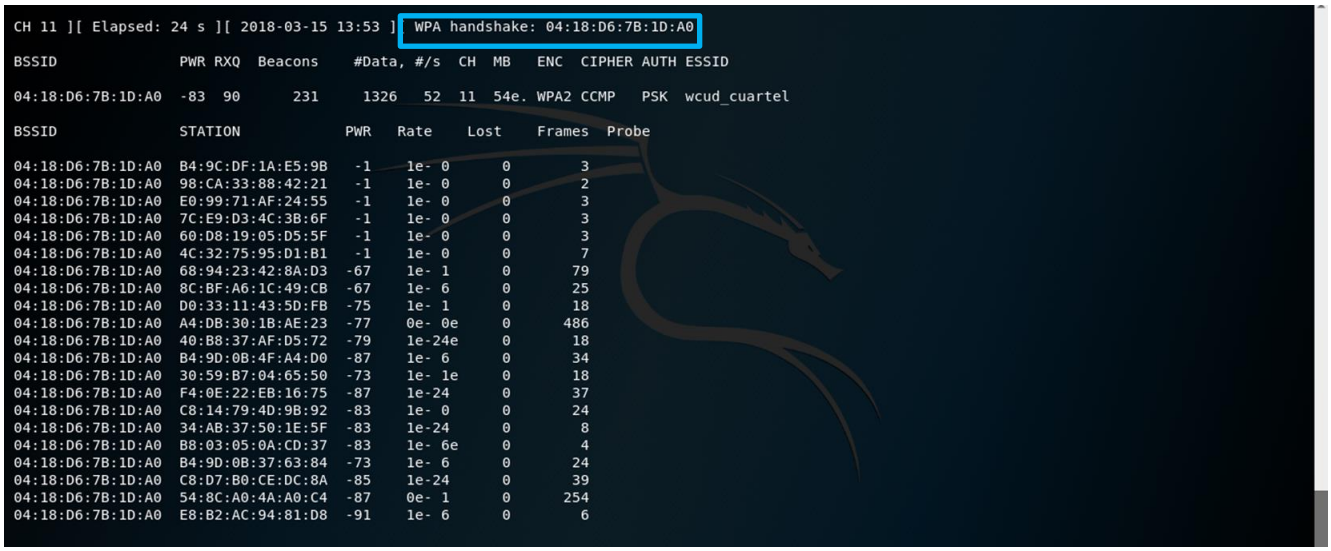


Figura 4-22 Monitorización de red *wcud_cuartel*

La estructura de la pantalla es la misma que para monitorizar todas las redes, con la particularidad de que cuando detecta el *handshake* aparece el aviso recuadrado en la figura.

Capturado el *handshake*, éste se guarda en un archivo con extensión *.cap*, en nuestro caso el fichero se llama *Descargas-01.cap*. Será este fichero del que obtendremos la contraseña de la red *wcud_cuartel*.

En la Figura 4-23 se introduce el comando para lanzar *aircrack-ng*. En él indica la dirección MAC del AP (04:18:D6:7B:1D:A0), la dirección del diccionario a emplear (*-w ~/Descargas/pass.txt*) y a continuación la ruta del archivo que guarda el *handshake* (*~/Descargas-01.cap*).

Figura 4-23 Comando *aircrack-ng*

El diccionario empleado (Figura 4-24) es un diccionario ad-hoc, que incluye la contraseña de la red *wcud_cuartel* y la del usuario Jesús para la siguiente prueba.

Figura 4-24 Diccionario empleado con *aircrack-ng*

El resultado del ataque de diccionario es el que se muestra en la Figura 4-25. Podemos ver en el apartado *KEY FOUND! [escuelanaval]* la contraseña de la red.

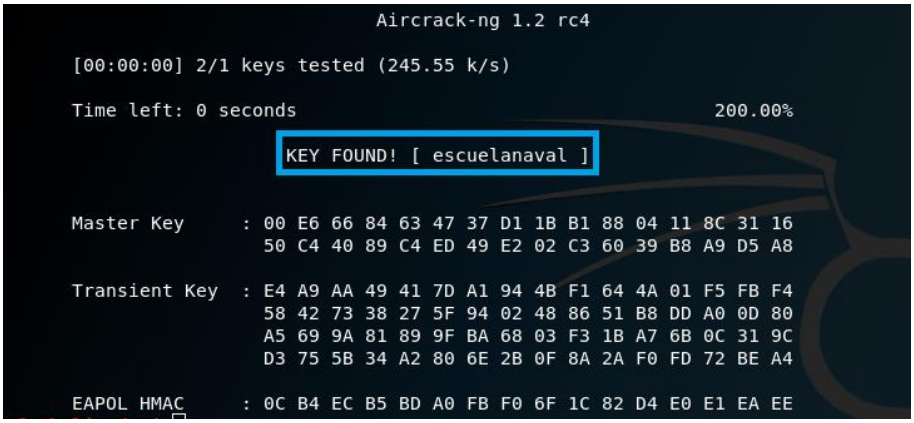


Figura 4-25 Interfaz de *aircrack-ng*

Para el *crackeo* de la clave se pueden emplear otros *software* como *cowpatty* o *pyrit* para realizar ataques de diccionario o *hashcat* que permite ejecutar ataques de fuerza bruta.

PRUEBA 6: CRACKEO CONTRASEÑA WPA2 ENTERPRISE

El objeto de esta prueba es emplear *aircrack-ng* en la Red TFG, que trabaja con servidor RADIUS, para demostrar que *aircrack-ng* no funciona como en la prueba 5. Se repite el proceso deteniéndonos solo en los detalles en los que diverge el proceso.

En la Figura 4-26 se vuelven a monitorizar las redes, y en este caso seleccionaremos la Red TFG (véase Figura 4-27).

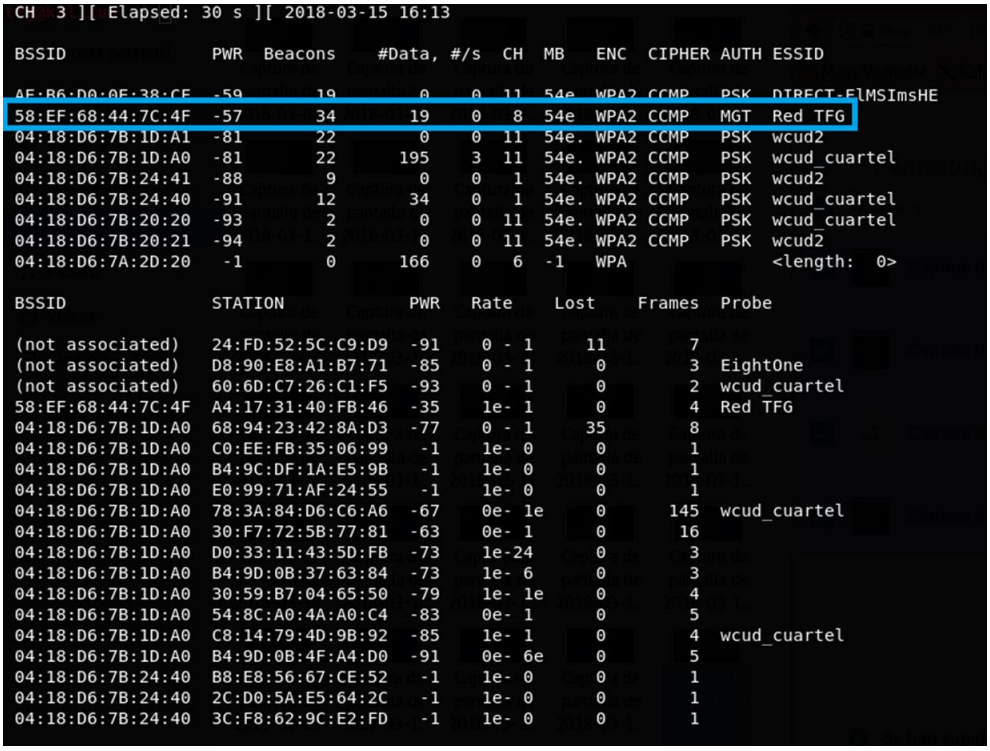


Figura 4-26 *airodump-ng wlan1mon*

Figura 4-27 Comando para monitorización de Red TFG

A continuación, en la Figura 4-28 vemos a los clientes conectados a la red. De los dos clientes conectados, utilizaremos *aireplay-ng* en el segundo (STATION: B4:9D:0B:5F:65:3C).

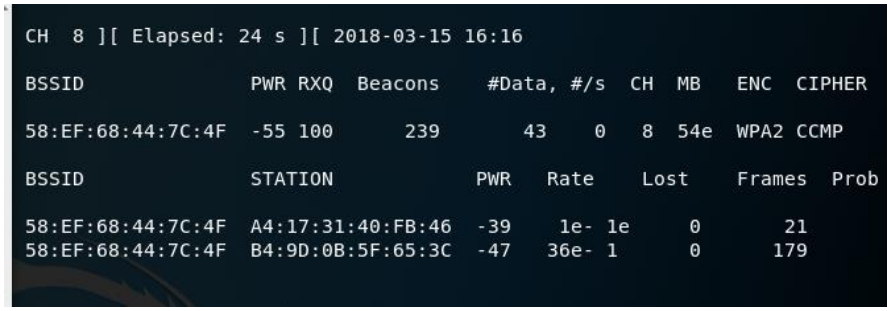


Figura 4-28 Interfaz de monitorización Red TFG

La Figura 4-28 muestra la situación antes de emplear *aireplay-ng* en el dispositivo seleccionado. Véase en la ventana de la derecha que no aparece el mensaje de captura del *handshake*. En la ventana de la izquierda se lanzará el comando:

```
sudo aireplay-ng -0 2 -a 58:EF:68:44:7C:4F -c B4:9D:0B:5F:65:3C wlan1mon
```

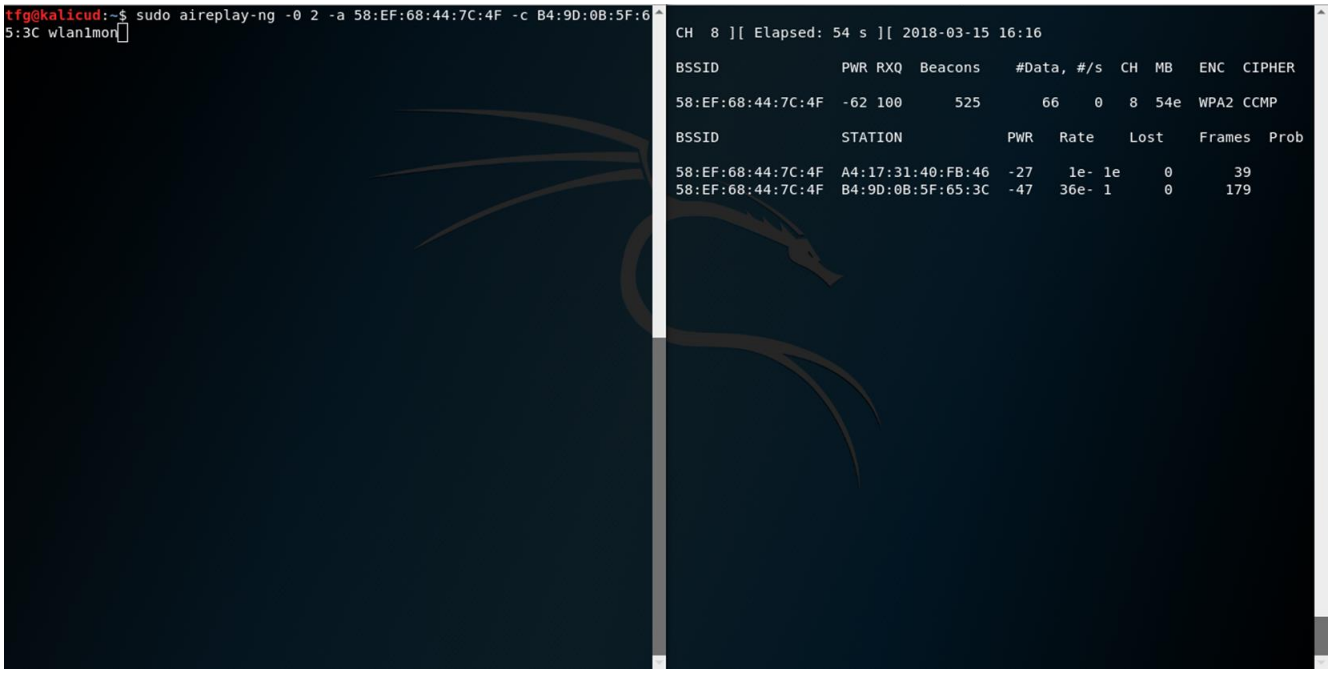


Figura 4-29 *aireplay-ng* ejecutándose junto con *airodump-ng*

Tras introducir el comando anteriormente mencionado, se produce la desautenticación del cliente, que se vuelve a conectar y hace que se capture el mensaje del *handshake* (véase Figura 4-30).

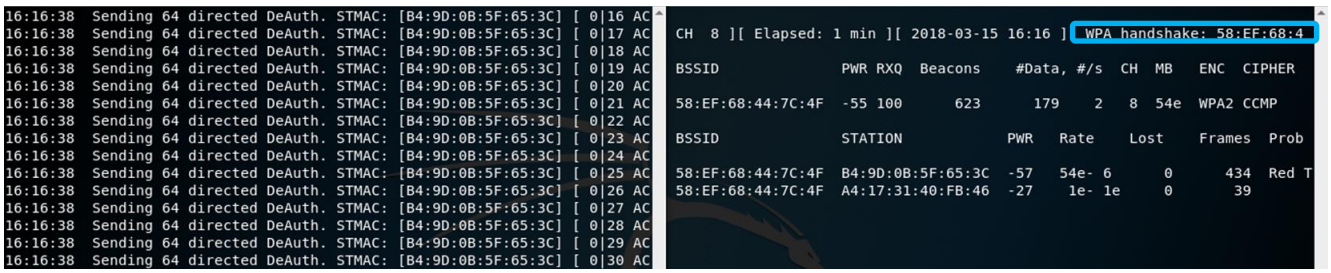


Figura 4-30 Captura del paquete *handshake*

Fruto de lo anterior, ahora tenemos el archivo necesario para emplear *aircrack-ng*, *~/Descargas-03.cap*. Lanzaremos *aircrack-ng* con el comando mostrado en la Figura 4-31.

Figura 4-31 Comando *aircrack-ng*

El resultado de la prueba demuestra que los ataques realizados con *aircrack-ng* en redes en las que se aplica el estándar IEEE 802.1x son infructuosos. Para la prueba se emplea el diccionario que contiene la contraseña del usuario que se conecta a la red y *aircrack-ng* no es capaz de descifrarla (ver Figura 4-32).

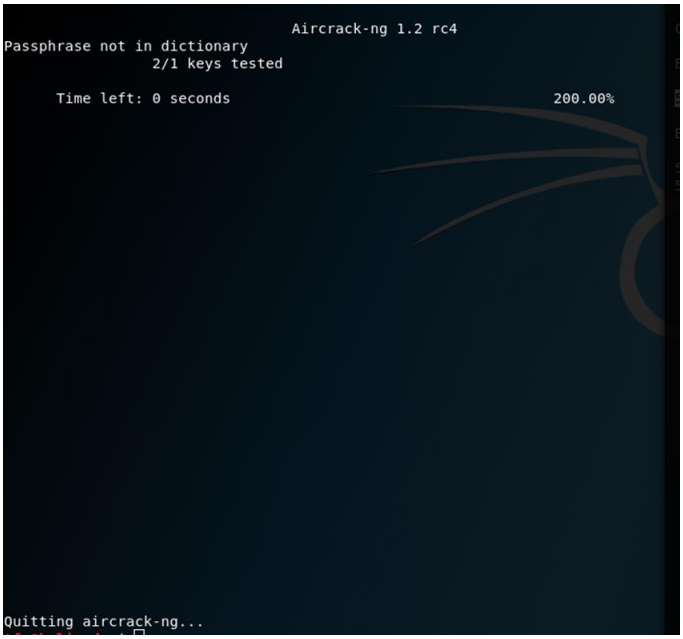


Figura 4-32 Proceso de crackeo *aircrack-ng*

PRUEBA 7: OBTENCIÓN DE CREDENCIALES MEDIANTE WIFIPHISHER

La siguiente prueba se orientará a vulnerabilidades de red que provienen de los usuarios de la misma. Esta prueba se puede ver de dos formas, o como un ataque *Evil Twin* o un ataque KARMA. La diferencia entre ellos es que, en *Evil Twin*, el *Rogue AP* debe ser creado en el entorno del usuario objetivo, desplegando una red de mayor potencia cerca de él.

Los ataques KARMA, como se comentó en la prueba 0, explotan los mensajes *probe request* enviados por los usuarios. Esto nos permite conocer qué redes guardadas tiene el dispositivo y nos permite crear un AP falso lejos del AP real que estamos copiando y asegurarnos de que el dispositivo se conectará.

El núcleo de la prueba es el mismo, pero se debe estudiar la situación para ejecutar un ataque lo más convincente posible.

En esta prueba emplearemos el *software wifiphisher* [58] que nos permite crear un *Rogue AP* "confiable" y establecer un portal web para capturar datos introducidos por el usuario. Para hacer más efectivo el empleo de la ingeniería social, el portal creado debe ser creíble. En nuestro caso se empleará uno de los portales predefinidos de la aplicación, que solicita usuario y contraseña de *Facebook*. Se podría configurar un portal más convincente que solicitara las credenciales de acceso a la Red TFG, por ejemplo, un logo del CUD con un aviso de un problema en la red; téngase en cuenta que la red simula una red para el CUD.

A continuación, se procede a indicar el proceso de instalación, configuración y empleo de *wifiphisher*.

Primero se instalará la aplicación (Figura 4-33).

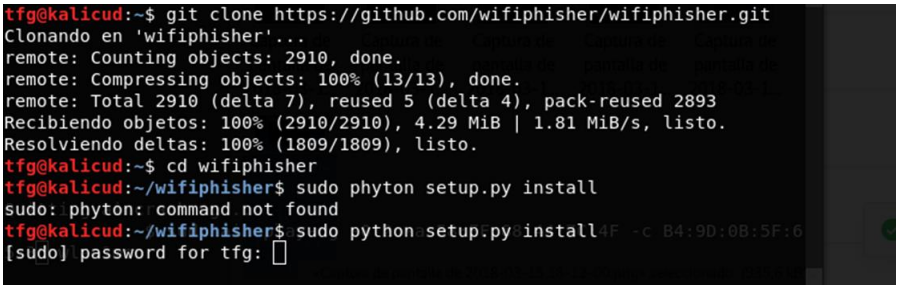


Figura 4-33 Instalación de *wifiphisher*

Al terminar la instalación nos aparecerá el siguiente logo (Figura 4-34).

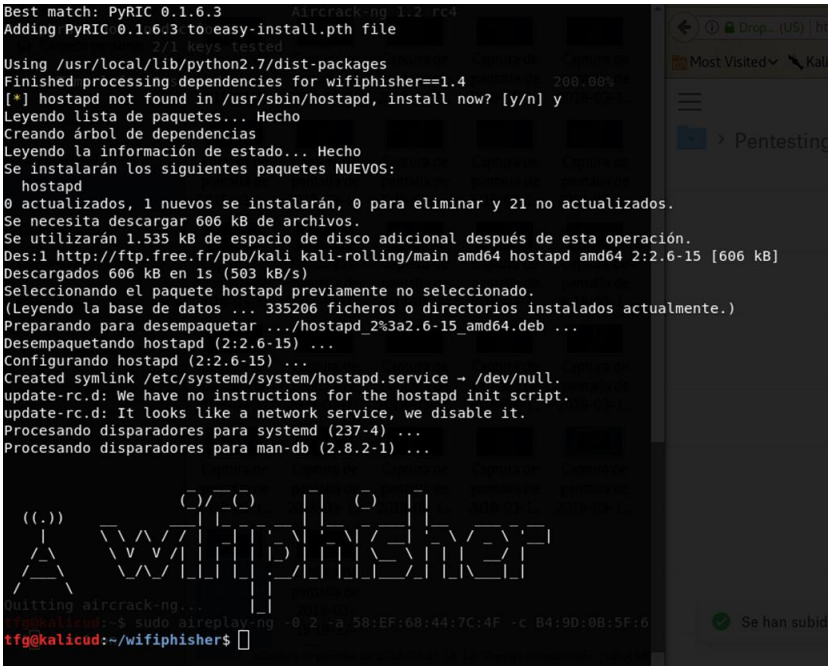


Figura 4-34 *wifiphisher* instalado

Una vez instalado ya podemos crear el falso AP. Para ello utilizaremos el siguiente comando:

```
sudo wifiphisher –essid “Red TFG” -p oauth-login -pK painter1537 -qS
```

Con este comando se define lo siguiente:

- *--essid “Red TFG”*, nombre de la red.
- *-p oauth-login*, carga uno de los escenarios precargados del programa, es decir, la interfaz web que se muestra cuando el usuario en el AP intenta acceder a Internet.
- *-pK painter1537*, establece una contraseña WPA2 para la red.
- *-qS*, establece que, una vez obtenidas las credenciales buscadas, se cierre el AP.

Tras introducir el comando, Figura 4-35, se abrirá la interfaz del AP, Figura 4-36. La interfaz aún no muestra ningún cliente pero muestra datos como el nombre de la red, canal de trabajo e interfaz que está empleando para generar el AP.

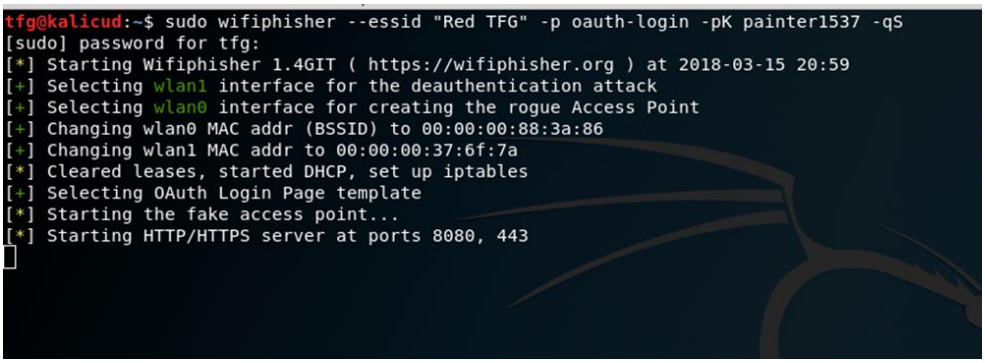


Figura 4-35 Comando *wifiphisher*

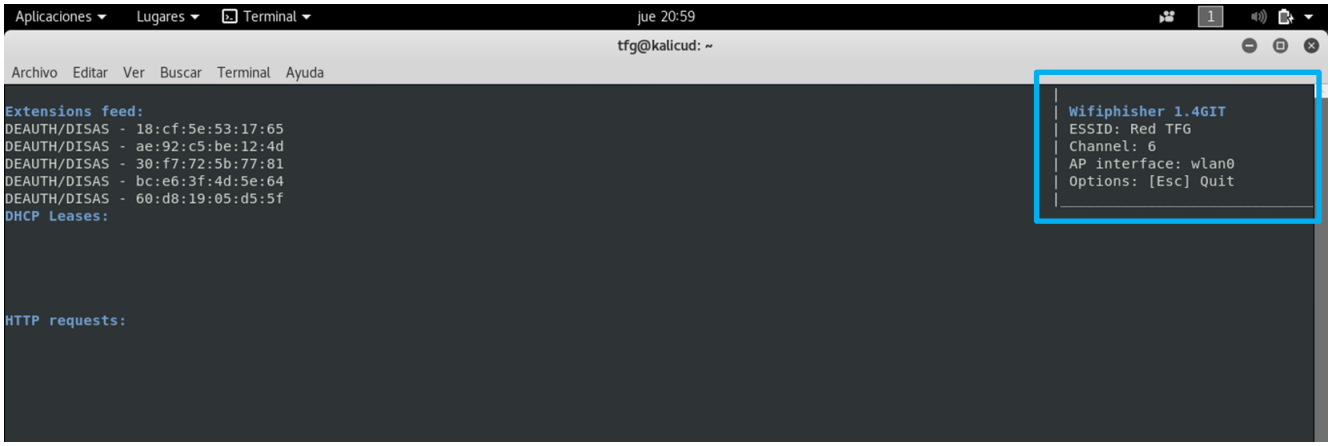


Figura 4-36 Interfaz *wifiphisher*

Activado *wifiphisher*, se procederá a conectar un equipo a dicha red, que, tras intentar acceder a Internet, accede a la web que emplearemos para obtener sus credenciales (véase Figura 4-37). La interfaz es editable y nos permitiría darle un aspecto más personalizado (*spear phishing*).

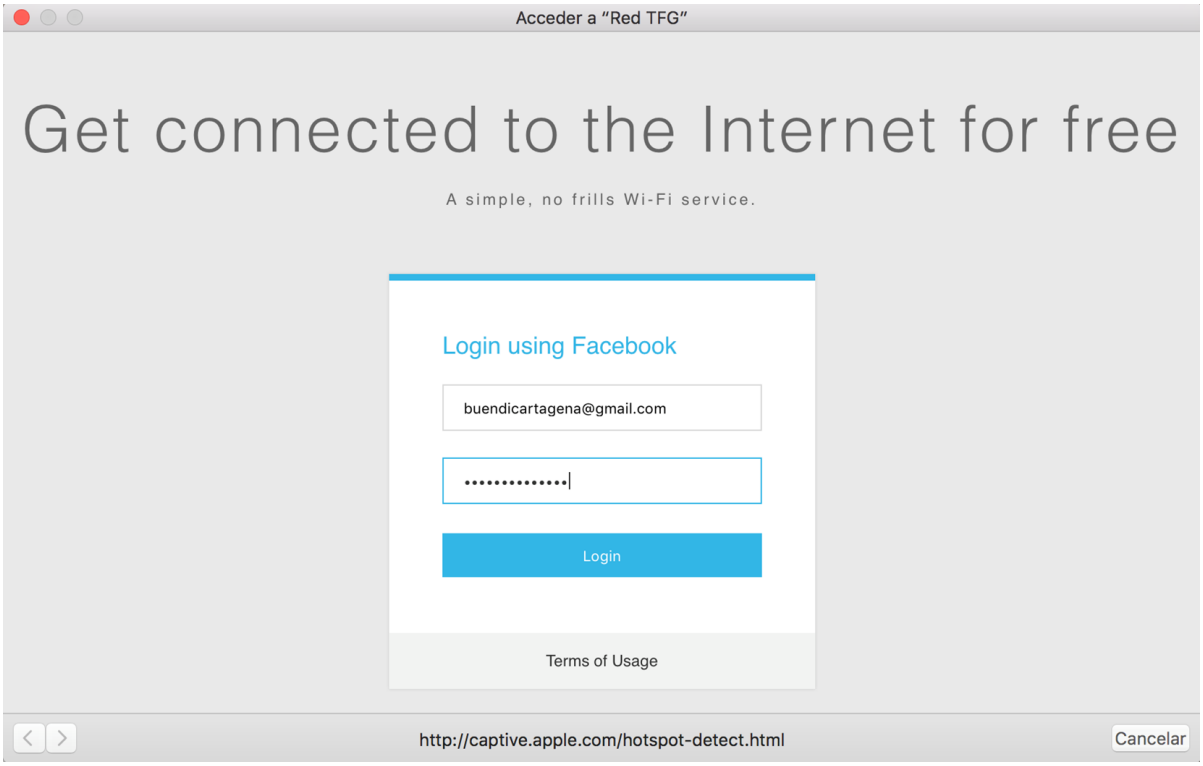


Figura 4-37 Portal de captura de credenciales

Una vez introducidas las credenciales y hecho *click* en *Login*, se mostrará la imagen de la Figura 4-38. En ese momento se capturan las credenciales del usuario y se desconecta el *Rogue AP*.

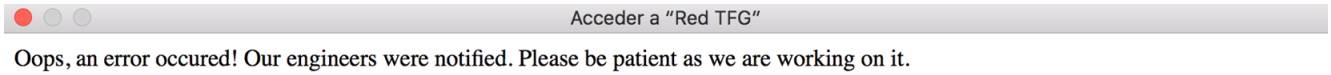


Figura 4-38 Mensaje de aviso de portal falso

Paralelamente, en el portátil del atacante aparece el usuario una vez conectado a la red (ver Figura 4-39).

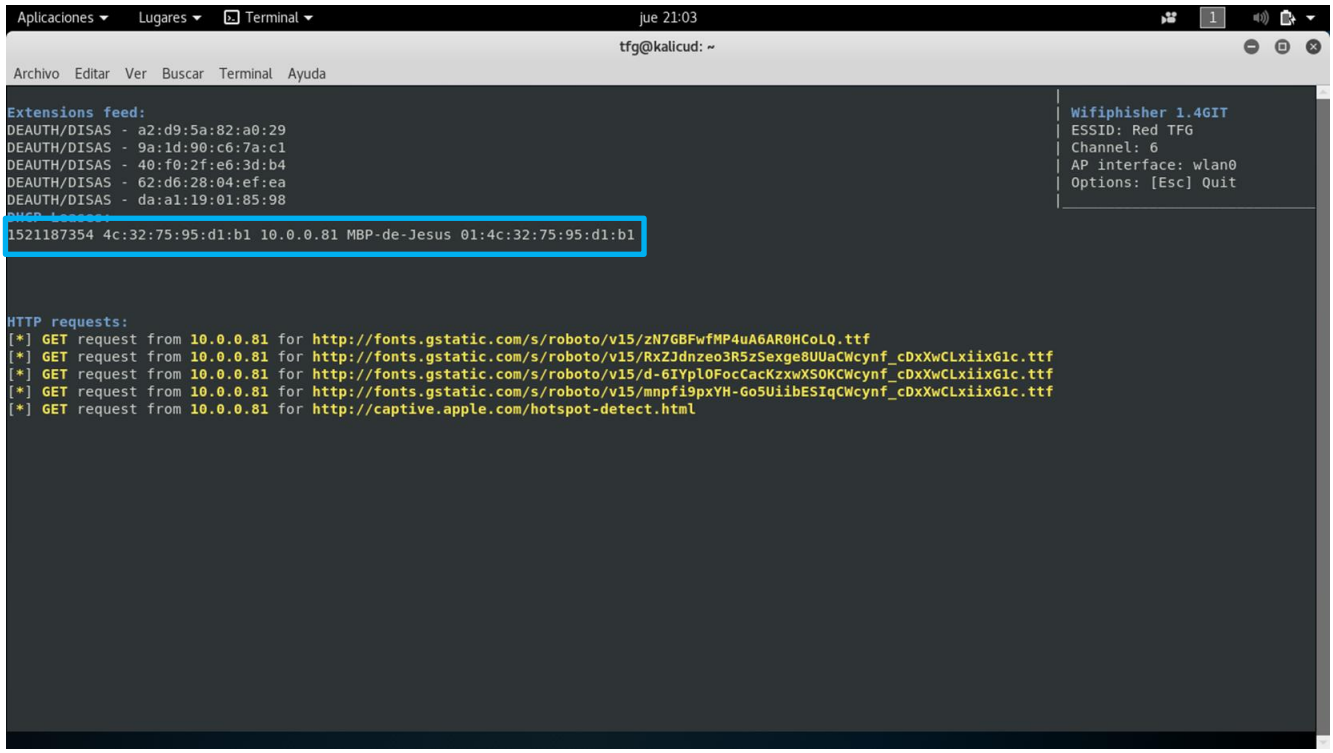


Figura 4-39 Interfaz *wifiphisher* con usuario conectado

Una vez realizado el *login* en el portátil del usuario del que queremos obtener las credenciales, se abandonará la interfaz y se volverá a la terminal que mostrará las credenciales del usuario:

- Usuario: buendicartagena@gmail.com
- Contraseña: calimeroseguro

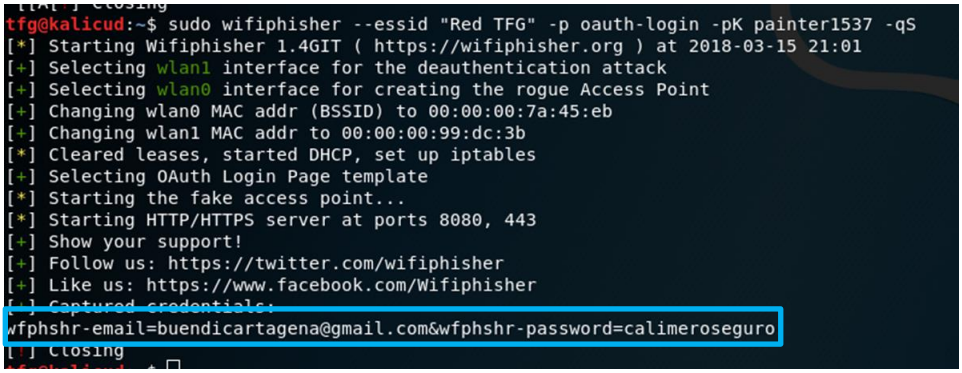


Figura 4-40 Credenciales del usuario atacado

Los ataques realizados con este programa sólo son compatibles para redes sin cifrado o con WPA2 *Personal*. Podríamos decir que empleando WPA2 *Enterprise* no existe amenaza de este tipo, sin embargo, si los usuarios de la red no están debidamente formados podrían ser víctima de un ataque de este tipo y proporcionar las credenciales de acceso a la red.

En el caso de una organización como el CUD, en la que el *e-mail* de los profesores está disponible en Internet, se podría orquestar un ataque *spear phishing* en el que se informara de un cambio en la contraseña de la red que se emplea. Se facilitaría la contraseña que deberían introducir para acceder al *Rogue AP*, y en un portal similar al empleado en esta prueba, solicitar las antiguas credenciales de acceso a la red con RADIUS. Obtenidas las credenciales se podría acceder a la red original por parte del atacante.

En la guía se menciona que es recomendable el empleo de equipos corporativos. Esta sería otra forma de evitar ataques de este tipo ya que se podrían limitar las opciones de configuración de los equipos para que solo el administrador de la red pueda realizar cambios. Se evitaría que algún usuario de la red pudiera ser engañado.

Una vez realizadas las pruebas podemos concluir que sólo con el empleo del estándar 802.1x se limitan las opciones que tiene el atacante para acceder a nuestra red. Si se configuran correctamente los mecanismos de transmisión de datos entre usuario, cliente y servidor, se impide el empleo de ataques que explotan fallos en SSL (*heartbleeding*). La principal forma de conseguir credenciales en la red es con el empleo de *hostapd-wpe*, lo que implica que con equipos bien configurados y usuarios concienciados se puede considerar segura la red.

Se ha visto también la importancia del empleo de contraseñas robustas en WPA2 ya sea en la versión *Personal* o *Enterprise*. Se demostró en la prueba 4 que empleando contraseñas robustas no se pueden descifrar las contraseñas, aunque el ataque previo con *hostapd-wpe* haya tenido éxito.

Las medidas menores como el filtrado MAC o la no emisión del SSID establecen una pequeña capa de seguridad que, aunque no vayan a detener a un atacante con conocimientos, sirven como medida deceptiva para personal no técnico.

5 CONCLUSIONES Y LÍNEAS FUTURAS

En este capítulo se procede a exponer las conclusiones obtenidas tras la realización del presente TFG así como las posibles líneas futuras a desarrollar por parte de otro alumno que quiera continuar por esta línea de investigación.

5.1 Conclusiones

El objetivo general de este TFG es comprobar si las medidas publicadas por el CCN-CERT, en el marco del ENS, en la guía CCN-STIC-816 Seguridad en Redes Inalámbricas solucionan los principales problemas relacionados con la seguridad en redes inalámbricas.

Para ello se desplegó una red en el cuartel de alumnos Marqués de la Victoria, empleando tres routers domésticos a modo de AP, uno para monitorizar la red y software libre. La red simulaba una posible red en los pasillos del CUD. Debido a limitaciones de material, eminentemente cables, se tuvo que adaptar el despliegue a éstas. El resultado final fue satisfactorio, con una red desplegada que cubría un área equivalente a los pasillos del CUD y que era incluso capaz de cubrir una zona más amplia.

Respecto al estudio y clasificación de la red, el proyecto se apoyó completamente en el empleo de las guías publicadas por CCN-CERT, tanto para aplicar las medidas de seguridad, como para clasificar la red. La decisión de categorización de la red se puede tomar basándose en los criterios de la guía CCN-STIC-816, sin embargo, para este proyecto se tuvieron en cuenta otras guías de carácter más amplio, como la guía CCN-STIC-803 de clasificación de los sistemas y, más concretamente, como el anexo I de la guía CCN-STIC-803 que definía la clasificación de las universidades. Finalmente se decidió que la red debía tener una categorización de seguridad MEDIA.

Antes de implementar las medidas que propone la guía CCN-STIC-816, se debió revisar el *software* libre que se emplearía para el establecimiento de las mismas. Se decidió el empleo del *firmware* OpenWrt, basado en Linux. También se estudió qué *software* se emplearía como servidor RADIUS (*freeRADIUS*), base de datos (*MySQL)* o sistema WIDS (*Kismet*). El *software* libre ofreció un gran abanico de posibilidades, que se vieron limitadas debido al *hardware* empleado ya que poseía escasa memoria. Esto último determinó que la instalación del *software* a emplear se hiciera de forma descentralizada, quedando las aplicaciones repartidas entre distintos routers o el ordenador portátil empleado para este TFG. Sin embargo, aún no siendo lo deseado, la elección del *software* e instalación sirvió para nuestros propósitos.

Una vez realizados los pasos previos, red desplegada, categoría de seguridad determinada y *software* a emplear seleccionado, se procedió a implementar las medidas del ENS que propone la guía CCN-STIC-816. Para un usuario sin conocimientos sobre configuración de redes puede resultar

confusa al principio. La guía incluye un estado del arte en el que desarrolla los conceptos que se deben conocer para aplicar las posteriores medidas. Durante el planteamiento de las medidas no se recomienda ningún *software* específico, quedando la decisión de cual usar en el administrador de la red.

Sobre las medidas propuestas para una categoría de red MEDIA, se implantaron todas menos el uso de certificados, una medida opcional. Tampoco se tuvieron en cuenta aspectos relativos a la eliminación de routers o equipos relacionados con la red. Se debe mencionar que se aplicaron medidas de protección extras como las alertas de Kismet que permiten detectar un ataque KRACK, ataque no contemplado en la guía CCN-STIC-816.

En el capítulo de validación de la red se comprobó la eficacia de las medidas propuestas por el ENS e implantadas en la red. Se realizaron un total de ocho pruebas empleando algunos de los principales programas de *pentesting*. Se demostró que el empleo del cifrado WPA2 *Enterprise* es más seguro que WPA2 *Personal* y permite un menor número de herramientas para intentar penetrar en la red. Se destaca el ataque a usuarios de la red como la principal amenaza para una red que cumple el ENS. Se ha demostrado que el empleo de medidas deceptivas puede llegar a poner en riesgo la red debido a la captura de credenciales.

En resumen, se puede hablar de que se han cumplido los objetivos marcados por este TFG y se puede concluir que la aplicación de las medidas propuestas por la guía CCN-STIC-816 incrementa notablemente la seguridad de una red, al menos, en el nivel MEDIO.

5.2 Líneas futuras

En este apartado se proponen las posibles opciones que permiten continuar o ampliar el trabajo realizado en este proyecto:

- Considerando que la mayor limitación para el desarrollo de este TFG han sido las características de memoria de los routers, se propone la implantación de las mismas medidas en un modelo de router pensado para despliegues profesionales, ya que estos tienen fundamentalmente un uso doméstico. Incluso, conociéndose las necesidades de una red de capacidad MEDIA, decidir qué router sería necesario para implantar todo el *software* de red (servidor RADIUS, bases de datos, cifrado de interfaz web,…) adecuadamente en los routers.
- Implantar las medidas de la categoría de seguridad ALTA y validar el funcionamiento de la red. La posibilidad de aumentar la categoría de seguridad existe dado que el futuro laboratorio de investigación del CUD puede llevar a cabo estudios en ámbitos militares cuya filtración pueda suponer un perjuicio para la reputación de la organización. Según la guía CCN-STIC-803 de valoración de redes, se considera la reputación como un criterio común evaluable para las redes [38] que de alcanzar nivel alto daría lugar a la categorización ALTA.
- Este TFG ha focalizado la validación principalmente en la captura de credenciales; con el empleo de routers de mayor capacidad, se podría intentar realizar ataques de otro tipo como puede ser denegación de servicio (*DoS, Denial of Service*). En nuestro caso, los routers no presentan capacidad para afrontar un ataque *DoS*.
- Una vez elegido el nivel de seguridad a implantar y con la red desplegada, poblar la red para detectar posibles fallos que hayan podido pasar desapercibidos debido al uso limitado de la red de este TFG.
- Estudiar la integración de la red inalámbrica según la guía CCN-STIC-816 con una red cableada y estudiar el nivel de seguridad conjunto del sistema. Implantar también las medidas de seguridad pertinentes.
- Seguimiento de la evolución de la guía CCN-STIC-816 debido a la posibilidad del lanzamiento de WPA3 a lo largo de 2018 [59] o liberación de los ataques KRACK.

- Centrar los esfuerzos de *pentesting* en acceder al router ya sea vía cableada o inalámbrica.
- Plantear y estudiar el establecimiento de una red WiFi segura para el empleo táctico de las tecnologías inalámbricas WiFi en teatro de operaciones. Empezando por unas pruebas iniciales de aplicación en la compañía de alumnos de Infantería de Marina, creando un Puesto de Mando y probando el alcance eficaz máximo que podría tener la red.
- Estudiar la viabilidad de incorporar una red WiFi inalámbrica segura a EDUROAM, un servicio mundial de movilidad segura desarrollado para la comunidad académica y de investigación, en el que un usuario con las credenciales adecuadas puede conectarse a la red de una universidad desde cualquier parte de la topología de la red.

6 BIBLIOGRAFÍA

[1] CCN-CERT, «Ciberamenazas y Tendencias Edición 2017» Junio 2017. [En línea]. Available: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2224-ccn-cert-ia-16-17-ciberamenzas-y-tendencias-edicion-2017/file.html. [Último acceso: 23 2 2018].

[2] CCN-CERT, «Buenas Prácticas CCN-CERT BP-05/16 - Internet de las Cosas» Junio 2017. [En línea]. Available: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2261-ccn-cert-bp-05-16-internet-de-las-cosas-1/file.html. [Último acceso: 23 2 2018].

[3] CCN, «Página de presentación CCN» [En línea]. Available: https://www.ccn.cni.es/index.php?option=com_content&view=article&id=1&Itemid=3&lang=es. [Último acceso: 26 2 2018].

[4] INCIBE, «Página principal INCIBE» [En línea]. Available: https://incibe.es/. [Último acceso: 4 3 2018].

[5] INCIBE, «Decálogo de la concienciación en ciberseguridad en la empresa» 11 8 2014. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/infografia-concienciacion-ciberseguridad. [Último acceso: 23 2 2018].

[6] INCIBE, «Kit de concienciación INCIBE» [En línea]. Available: https://www.incibe.es/protege-tu-empresa/kit-concienciacion. [Último acceso: 23 2 2018].

[7] CCN-CERT, «Listado de Guías CCN-STIC» 2 2 2018. [En línea]. Available: https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html. [Último acceso: 23 2 2018].

[8] BOE, «Real Decreto 3/2010, de 8 de enero - Aprobación del ENS» 29 1 2010. [En línea]. Available: https://www.ccn-cert.cni.es/publico/ens/BOE-A-2010-1330.pdf. [Último acceso: 24 2 2018].

[9] CCN-CERT, «Esquema Nacional de Seguridad, CCN-CERT» [En línea]. Available: https://www.ccn-cert.cni.es/ens.html. [Último acceso: 24 2 2018].

[10] Aruba, «Aruba, WiFi seguro para el Ejército americano» [En línea]. Available: http://www.arubanetworks.com/resources/us-army/. [Último acceso: 1 2 2018].

[11] B. M. Leiner, V. G. Cerf, D. D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, D. L. G. Roberts y S. Wolff, «Artículo sobre la historia de Internet» 1997. [En línea]. Available: https://www.internetsociety.org/es/breve-historia-de-internet/. [Último acceso: 16 1 2018].

[12] A. S. Tanenbaum y D. J. Wetherall, Redes de computadores, Editorial Pearson, 2012.

[13] IEEE, «IEEE 802.11 Timeline» 14 11 2017. [En línea]. Available: http://www.ieee802.org/11/Reports/802.11_Timelines.htm. [Último acceso: 17 1 2018].

[14] Centro Criptológico Nacional, «Guía CCN-STIC 816» 7 2017. [En línea]. Available: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2317-ccn-stic-816-seguridad-en-redes-inalambricas-en-el-ens/file.html. [Último acceso: 17 1 2018].

[15] IEEE, «IEEE website» [En línea]. Available: http://grouper.ieee.org/. [Último acceso: 17 1 2018].

[16] Centro Criptológico Nacional, «Web Centro Criptológico Nacional» [En línea]. Available: https://www.ccn.cni.es/. [Último acceso: 23 1 2018].

[17] IEEE, «Estándar 802.11i» 2004. [En línea]. Available: https://standards.ieee.org/findstds/standard/802.11i-2004.html. [Último acceso: 12 3 2018].

[18] IEEE, «Estándar 802.11w» 2009. [En línea]. Available: https://standards.ieee.org/findstds/standard/802.11w-2009.html. [Último acceso: 12 3 2018].

[19] IEEE, «Estándar 802.1x» 2010. [En línea]. Available: https://standards.ieee.org/findstds/standard/802.1X-2010.html. [Último acceso: 12 3 2018].

[20] UNIFI, «UNIFI website» [En línea]. Available: https://unifi-sdn.ubnt.com/. [Último acceso: 12 3 2018].

[21] DD-WRT, «Página oficial DD-WRT» [En línea]. Available: https://www.dd-wrt.com/site/index. [Último acceso: 4 3 2018].

[22] Tomato, «Página oficial de Tomato» [En línea]. Available: http://tomato.groov.pl/?page_id=81. [Último acceso: 4 3 2018].

[23] Flashrouters, «Ventajas del empleo de firmware libre» [En línea]. Available: https://www.flashrouters.com/learn/router-basics/benefits-of-open-source-firmware. [Último acceso: 25 2 2018].

[24] Best wireless routers now, «Comparativa firmwares libres» [En línea]. Available: http://bestwirelessroutersnow.com/dd-wrt-vs-tomato-vs-openwrt/#tab-con-2. [Último acceso: 26 2 2018].

[25] ITU, «Definición ciberseguridad, Unión Internacional de Telecomunicaciones» 18 4 2008. [En línea]. Available: https://www.itu.int/rec/T-REC-X.1205-200804-I/es. [Último acceso: 21 1 2018].

[26] M. Vanhoef, «Web Ataques KRACK» [En línea]. Available: https://www.krackattacks.com/. [Último acceso: 21 1 2018].

[27] Wi-Fi Alliance, «Protocolo de seguridad WPA3» 8 1 2018. [En línea]. Available: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-

enhancements. [Último acceso: 21 1 2018].

[28] ECSO, «*European Cyber Security Organisation website*» [En línea]. Available: https://www.ecs-org.eu/. [Último acceso: 12 3 2018].

[29] IT User, «Artículo sobre la creación de ECSO» 6 7 2016. [En línea]. Available: http://www.ituser.es/seguridad/2016/07/nace-la-organizacion-europea-de-ciberseguridad. [Último acceso: 26 2 2018].

[30] MCCD, «Mando Conjunto de Ciberdefensa website» [En línea]. Available: http://www.emad.mde.es/CIBERDEFENSA/. [Último acceso: 12 3 2018].

[31] Agencia Estatal Boletín Oficial del Estado, «Real Decreto 421/2004» 12 3 2004. [En línea]. Available: https://www.boe.es/boe/dias/2004/03/19/pdfs/A12203-12204.pdf. [Último acceso: 12 3 2018].

[32] Agencia Estatal Boletín Oficial del Estado, «Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia» 6 5 2002. [En línea]. Available: https://www.boe.es/buscar/act.php?id=BOE-A-2002-8628. [Último acceso: 12 3 2018].

[33] CCN-CERT, «Preguntas Frecuentes y Respuestas CCN-CERT» [En línea]. Available: https://www.ccn-cert.cni.es/sobre-nosotros/faq.html. [Último acceso: 26 2 2018].

[34] Agencia Estatal Boletín Oficial del Estado, «Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos» 22 6 2007. [En línea]. Available: https://www.boe.es/buscar/act.php?id=BOE-A-2007-12352. [Último acceso: 12 3 2018].

[35] Agencia Estatal Boletín Oficial del Estado, «Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica» 8 1 2010. [En línea]. Available: https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330. [Último acceso: 12 3 2018].

[36] Agencia Estatal Boletín Oficial del Estado, «Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica» 23 10 2015. [En línea]. Available: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-11881. [Último acceso: 12 3 2018].

[37] CCN-CERT, «Página CCN-CERT - ENS» [En línea]. Available: https://www.ccn-cert.cni.es/ens.html. [Último acceso: 26 2 2018].

[38] CCN, «Guía CCN-STIC-803 Valoración de los sistemas» 11 2017. [En línea]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html. [Último acceso: 30 1 2018].

[39] CCN-CERT, «CCN-STIC-804 Medidas de implantación del ENS» 6 2017. [En línea]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html. [Último acceso: 12 3 2018].

[40] CCN-CERT, «CCN-STIC-816 Seguridad en Redes Inalámbricas en el ENS» 6 2017. [En línea]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2317-ccn-stic-816-seguridad-en-redes-inalambricas-en-el-ens/file.html. [Último acceso: 12 3 2018].

[41] CCN-CERT, «CCN-STIC-406 Seguridad en Redes Inalámbricas» 31 7 2017. [En línea]. Available: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4846-seguridad-en-redes-inalambricas-basadas-en-estandar-802-11.html. [Último acceso: 12 3 2018].

[42] CCN, «CCN-STIC-803, Anexo I: Valoración de los sistemas en Universidades» 11 2017. [En línea]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2509-ccn-stic-803-valoracion-de-sistemas-en-el-ens-anexo-i-universidades/file.html. [Último acceso: 30 1 2018].

[43] IETF, «RFC 4017» 3 2005. [En línea]. Available: https://www.ietf.org/rfc/rfc4017.txt. [Último acceso: 12 3 2018].

[44] Linksys, «Características router WRT54GL» [En línea]. Available: https://www.linksys.com/es/p/P-WRT54GL/#product-features. [Último acceso: 17 1 2018].

[45] «C|net características router WRT54GL» [En línea]. Available: https://www.cnet.com/products/linksys-wrt54gl-wireless-g-broadband-router/specs/. [Último acceso: 18 1 2018].

[46] OpenWrt, «Configuración de un túnel SSH» [En línea]. Available: https://wiki.openwrt.org/doc/howto/secure.access. [Último acceso: 1 3 2018].

[47] Kismet, «Página oficial de Kismet» [En línea]. Available: https://www.kismetwireless.net/. [Último acceso: 20 2 2018].

[48] Ekahau, «*Ekahau HeatMapper website*» [En línea]. Available: https://www.ekahau.com/products/heatmapper/overview/. [Último acceso: 12 3 2018].

[49] Flashrouters, «Artículo sobre chipsets de un router» [En línea]. Available: https://www.flashrouters.com/blog/2018/01/22/understanding-router-chipsets/. [Último acceso: 28 2 2018].

[50] OpenWrt, «Configuración Dumb AP» [En línea]. Available: https://wiki.openwrt.org/doc/recipes/dumbap. [Último acceso: 1 3 2018].

[51] «Crontab, página manual de Linux» [En línea]. Available: https://linux.die.net/man/5/crontab. [Último acceso: 23 1 2018].

[52] OpenWRT, «Tabla de zonas horarias OpenWRT» [En línea]. Available: https://wiki.openwrt.org/doc/uci/system#time_zones. [Último acceso: 20 2 2018].

[53] FreeRADIUS, «FreeRadius website» [En línea]. Available: https://freeradius.org/. [Último acceso: 12 3 2018].

[54] FreeRadius, «Guía técnica de FreeRadius» [En línea]. Available: http://networkradius.com/doc/FreeRADIUS%20Technical%20Guide.pdf. [Último acceso: 5 2 2018].

[55] MySQL, «Librería descarga MySQL» [En línea]. Available: https://dev.mysql.com/downloads/repo/apt/. [Último acceso: 13 2 2018].

[56] Carnegie Mellon University, «Artículo sobre ataques KARMA» 11 8 2015. [En línea]. Available: https://insights.sei.cmu.edu/cert/2015/08/instant-karma-might-still-get-you.html. [Último acceso: 15 3 2018].

[57] Aircrack-ng, «Aircrack-ng website» [En línea]. Available: http://www.aircrack-ng.org/. [Último acceso: 15 3 2018].

[58] Wifiphisher, «Wifiphisher website» [En línea]. Available: https://wifiphisher.org/. [Último acceso: 15 3 2018].

[59] Universidad de Alcalá, «Temario auditoría en redes inalámbricas» [En línea]. [Último acceso: 15 3 2018].

[60] Comunidad OpenWrt, «Web de OpenWrt» [En línea]. Available: https://openwrt.org/. [Último acceso: 18 1 2018].

[61] IEEE, «IEEE website» [En línea]. Available: https://www.ieee.org/about/vision_mission.html. [Último acceso: 17 1 2018].

[62] OpenWrt, «Configuración cliente puente» [En línea]. Available: https://wiki.openwrt.org/doc/recipes/bridgedclient. [Último acceso: 29 1 2018].