UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

Identificación de vulnerabilidades en la red *wlcampus* mediante el ataque *Rogue Access Point*

TRABAJO DE TESIS
PARA OBTENER EL GRADO DE
INGENIERO EN REDES

PRESENTA
GUILLERMO ELEAZAR FUNES

DIRECTOR DE TESIS
MTI.VLADIMIR VENIAMIN CABAÑAS VICTORIA

ASESORES
DR. JAVIER VÁZQUEZ CASTILO
MSI. LAURA YÉSICA DÁVALOS CASTILLA
MSI. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE
DR. JAIME SILVERIO ORTEGÓN AGUILAR

CHETUMAL QUINTANA ROO, MÉXICO, MAYO DE 2016

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO DE TESIS ELABORADO BAJO SUPERVISIÓN DEL COMITÉ DE ASESORÍA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

Universidad de Quintana Roo
DCI DIVISIÓN DE CIENCIAS E INGENIERÍA

COMITÉ DE TRABAJO DE TESIS

DIRECTOR:

MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA

ASESOR:

DR. JAVIER VAZQUEZ CASTILLO

ASESORA:

MSI. LAURA YESICA DÁVALOS CASTILLA

CHETUMAL QUINTANA ROO, MÉXICO, MAYO DE 2016

Agradecimientos

A Dios por ser el creador de todo y por acompañarme en todo momento y darme todo lo necesario para perseverar en mis objetivos.

A mis padres Guillermo y Ofelia por su total apoyo, amor, compresión y ayuda que siempre me han brindado y por enseñarme a ser un hombre de bien.

A la Universidad de Quintana Roo por darme la oportunidad de estudiar y formar parte de esta gran familia universitaria.

A mi tutor y director de tesis MTI Vladimir Veniamín Cabañas por guiarme y apoyarme durante todo el transcurso de la carrera.

A la División de Ciencias e Ingenierías (DCI), en especial al Departamento de Ingeniería, por la formación académica que de ella he recibido y cuyo emblema me identificará como Universitario en cualquier lugar en que me encuentre.

A mis hermanos Obed, Jonathan y Zury quienes siempre me han apoyado y animado en todas las etapas de mi vida.

A mis compañeros y amigos de la carrera Ingeniería en Redes con quienes compartí inolvidables momentos dentro y fuera del salón de clases y a quienes aprecio no sólo por ser excelentes personas sino también por ser un gran apoyo durante la carrera. Ellos y ellas siempre formarán parte de esta importante etapa de mi vida.

A mí cuñada Vianie y mi sobrino Caleb quienes han traído mucha alegría a mi vida y quienes me han ayudado en todo lo que han podido.

A todos los que de una u otra forma colaboraron en mi formación. Este trabajo no habría sido posible sin la contribución de todas estas personas que de forma directa e indirecta ofrecieron su apoyo.

Dedicatoria

A:

México por su hospitalidad y por darme la oportunidad de realizar mis estudios en este agradable y hermoso país lleno de gente trabajadora, amable e inteligente.

Al Gobierno de México por becarme 5 años para lograr este objetivo. Este trabajo de investigación fue realizado con una beca de excelencia otorgada por el Gobierno de México, a través de la Secretaría de Relaciones Exteriores. Expreso mi profundo agradecimiento al Gobierno de México ya que sin la beca de excelencia que me fue otorgada no hubiera podido lograr este sueño.

Resumen

En el ámbito de las redes inalámbricas, los usuarios son capaces de acceder a un canal del espectro inalámbrico; esto permitiría que algún usuario explote esta característica haciéndose pasar por un usuario común, incluso podría establecer un punto de acceso que se haga pasar por uno legítimo, este usuario (atacante) está en posibilidades de interceptar la información de los demás usuarios (víctimas) conectadas a esta red ficticia.

El objetivo principal de esta investigación es la identificación de vulnerabilidades de la red inalámbrica '*wlcampus'* en la Universidad de Quintana Roo, campus Chetumal mediante un ataque inalámbrico llamado '*Rogue Access Point/Evil Twin*' o en otras palabras, ataque de punto de acceso falso.

Después de lanzar el ataque '*Rogue Access Point'*, el ataque se extiende a un ataque llamado '*Man In The Middle'* o ataque de hombre en medio que hace referencia a la parte donde se intercepta gran mayoría del tráfico de la red que se está atacando a través de diferentes herramientas como *urlsnarf*, *sslstrip* entre otras.

Para llevar a cabo los ataques mencionados anteriormente, se utiliza el dispositivo *Wifi Pineapple Mark V* (dispositivo exclusivamente para realizar auditorías de red). La finalidad es comprender de mejor manera las amenazas de seguridad, las vulnerabilidades y los riesgos de ataques a la que están expuestas las redes inalámbricas 802.11.

En el capítulo 1 se ponen de manifiesto las condiciones de la red inalámbrica que da servicio a los usuarios (*wlcampus)* en el campus Chetumal de la UQROO. Se justifica el motivo por el cual se llevó cabo esta investigación y se definen también los objetivos que se desean alcanzar. Se describe el alcance de la investigación y por último, se hace una descripción de la metodología que se utilizara para llevar a cabo la parte práctica de esta tesis que es la metodología de 'pentesting' o 'penetration testing'.

En el capítulo 2 se hace una descripción general de las redes inalámbricas basadas en el estándar 802.11, sus componentes o elementos principales, tipos de configuraciones de red del protocolo 802.11, descripción de bandas de frecuencia y canales, descripción de la capa física y capa de enlace de datos de la tecnología 802.11 y los mecanismos de seguridad que se pueden implementar para la tecnología WiFi. Se describe además el proceso de 'pentesting' y cómo los métodos y técnicas de ataques de red se pueden efectuar con la utilización de diversas herramientas de ataque de red como '*aircrack-ng'*, '*sslstrip'*, 'karma' etc.

En el capítulo 3 se expone el desarrollo de la parte práctica de la tesis donde se describe con detalle el procedimiento que se debe llevar a cabo para lanzar el ataque '*Rogue AP'* y posteriormente extenderlo a un ataque '*Man In The Middle'*. Se describe también el orden y la forma en la que se utilizaron las distintas herramientas de hardware y software (Wifi Pineapple Mark V, Adaptador de red Alfa AWUS036H, Antenna Alfa de 18 dbi, Laptop con Kali Linux 2.0, karma, urlsnarf, sslstrip, aircrack-ng) para llevar a cabo el proceso de 'pentesting' enfocándonos en el ataque de punto de acceso falso.

En el capítulo 4 describe la puesta en marcha de las cuatro etapas del procedimiento que son:

- la recopilación de información
- el establecimiento de un punto de acceso falso
- la adquisición de clientes
- intercepción de tráfico de red.

En este capítulo se analizan los resultados de cada una de las cuatro etapas que se llevó a cabo con la ayuda de las herramientas de hardware y software mencionadas anteriormente. En el análisis de cada una de las etapas expone lo exitoso que es llevar un proceso de 'pentesting' enfocándonos en el ataque 'Rogue Access Point' para atacar y vulnerar la red abierta inalámbrica 'wlcampus' y poder interceptar información de los usuarios que hayan sido víctimas de este ataque extendido un ataque de hombre en medio.

Finalmente se presentan las conclusiones derivadas de la investigación realizada y además se exponen posibles soluciones y las recomendaciones a las deficiencias y huecos de seguridad que se encontraron dejando claro que es necesario que se implementen mecanismos de seguridad de autenticación y autorización en la red wlcampus. Se hace evidente que se debe concientizar a la comunidad universitaria de tomar ciertas medidas de seguridad a la hora de utilizar alguna red inalámbrica abierta (Hotspot) tal como la utilización de una VPN y la actualización constante de las aplicaciones de sus equipos informáticos.

Contenido

Índice de figuras

Índice de tablas

Capítulo 1 Introducción

1.1 Introducción

La Universidad de Quintana Roo (UQROO), es un Instituto de educación superior que ofrece distintos tipos de servicios a la comunidad universitaria siendo el acceso a las tecnologías de la información una de las más importantes. El campus sede de la UQROO está ubicado en Chetumal, Quintana Roo en donde se encuentra implementada una red inalámbrica. La red inalámbrica consta de varios puntos de acceso distribuidos en distintos sitios estratégicos alrededor del campus y es administrado por separado de las otras redes cableadas existentes. La red inalámbrica conecta a cientos de usuarios como lo son estudiantes, maestros, personal administrativo y visitantes a través de cinco subredes inalámbricas (con los siguientes nombres**: wlcampus, uqroodigital, invitados, eventos y alumnos**) difundidas por los puntos de acceso que juntos conforman la red inalámbrica. Por lo tanto, una red inalámbrica que brinda servicio a cientos de usuarios a través de distintas subredes siempre presenta riegos en cuestión de seguridad de la información.

1.2 Definición del problema:

Para poder identificar y comprender los riesgos que suponen en el tema de seguridad de la información en las distintas subredes de la red inalámbrica es necesario conocer los esquemas de seguridad implementados y el tipo de información que generan los usuarios al conectarse diariamente a una red inalámbrica. Por ejemplo: la subred inalámbrica wlcampus implementa un esquema de seguridad abierta sin ningún tipo de autenticación y cifrado de información lo cual la deja expuesta y vulnerable a recibir ataques que fácilmente comprometerían la seguridad de la información de los usuarios y los equipos de red.

En relación a la falta de mecanismos de seguridad esenciales en la subred inalámbrica wlcampus, se mencionan los principales riesgos en seguridad de información que afronta:

I. Vulnerabilidad en cuanto al acceso externo a datos confidenciales, recursos de red y/o servicios.

II. Ambiente adecuado y oportuno para llevar a cabo ataques informáticos que culminen en robo de información, denegación de servicio, cuentas de correo comprometidas entre otras.
III. La propagación y ataque de malware.
IV. Inexistencia de políticas robustas de autenticación y procesamiento de usuarios.

Por lo tanto, las circunstancias y situaciones planteadas anteriormente son las responsables de la realización de un trabajo de investigación que evaluará la seguridad de la red inalámbrica wlcampus en la Universidad de Quintana Roo, campus Chetumal, cuya finalidad tiene como resultado trazar un plan de estrategias a seguir para mejorar la seguridad de la red inalámbrica, así como también fomentar y promover una cultura de seguridad informática en la Universidad de Quintana Roo.

1.3 Justificación:

La Universidad de Quintana Roo es una institución educativa de prestigio que ha adoptado las tecnologías de información y comunicación (TICs) para brindar un servicio de alta calidad a los estudiantes, maestros, personal administrativo y a toda la comunidad universitaria. Durante los últimos años, la UQROO ha mejorado y expandido su red de datos a través de la implementación de redes inalámbricas, impulsando el acceso a Internet y la conectividad a las diferentes aplicaciones institucionales.

La red inalámbrica que se encuentra establecida en el campus Chetumal, brinda los beneficios de la conectividad a los usuarios en lugares o sitios donde resulta inconveniente o imposible brindar servicio con una red cableada.

Sin embargo, el hecho de que cualquier persona logre captar la señal inalámbrica del punto de acceso e intente acceder a la red no significa un beneficio o una ventaja sin antes corroborar si dicha persona es un usuario legítimo. Debido a que la red inalámbrica se encuentra configurada para el libre acceso sin ningún tipo de seguridad que permite autenticar y procesar a los usuarios

que acceden a ella, un atacante puede ejecutar herramientas de red sofisticadas sin tener grandes conocimientos de redes informáticas para llevar a cabo ataques y comprometer la seguridad de la información que transita en la red y la seguridad de los equipos de red por medio del robo de información, denegación de servicios de red, la ejecución de malware para obtener privilegios de administrador entre otras.

Un punto de acceso inalámbrico abierto o mal configurado se convierte en una puerta que vulnera por completo la confiabilidad en la seguridad informática de la red inalámbrica, incrementado el riesgo de que posteriormente hasta la red cableada sea comprometida. Por consiguiente, ya que se tiene el planteamiento del problema y dada la falta de seguridad en la red inalámbrica wlcampus, dicha red no ha recibido la atención debida a pesar de la gravedad de la situación.

Cabe resaltar que es necesario la identificación, manejo adecuado y oportuno de los huecos o brechas de seguridad en relación a la red inalámbrica, así como el planteamiento de mecanismos de seguridad de red y recomendaciones para fortalecer el esquema de seguridad. Finalmente, a través de la realización de este proyecto de tesis, la Universidad de Quintana Roo se verá beneficiada a través de la formulación de mecanismos y políticas de seguridad que tengan la capacidad de mitigar posibles ataques internos o externos, o cualquier actividad en la red inalámbrica que pueda presentar una amenaza a la seguridad de la información en la red.

1.4 Objetivos

General:

Identificar las posibles vulnerabilidades por medio de la realización de un ataque de suplantación de red que permita analizar, evaluar y plantear posibles soluciones que contrarresten o mitiguen los riesgos que representan las vulnerabilidades que pueden ser explotadas.

Específicos:

i. Realizar un reconocimiento de la red inalámbrica wlcampus para el levantamiento de información con la finalidad de alcanzar la familiarización y conocimiento de la configuración de los puntos de acceso, el tipo y la cantidad de tráfico de red que generan los usuarios, cantidad de usuarios, el esquema de seguridad que se maneja internamente para los servicios que acceden los usuarios y la disponibilidad de la red inalámbrica.
ii. Analizar y evaluar cualquier tipo de vulnerabilidades en la red inalámbrica wlcampus previo a la realización del ataque de suplantación de red.
iii. Realizar un ataque de suplantación de red hacia la red inalámbrica wlcampus tomando en consideración los resultados del análisis y la evaluación de las vulnerabilidades detectadas.
iv. Analizar y evaluar los resultados del ataque de suplantación de red para determinar la gravedad de las vulnerabilidades explotadas en la red inalámbrica wlcampus.
v. Elaborar recomendaciones que den a conocer posibles mejoras a los mecanismos de seguridad de la red inalámbrica wlcampus y sugerir planes de acción para corregir los agujeros de seguridad que pueden ser explotados mediante ataques de red inalámbricos.

1.5 Alcance:

La trascendencia de esta investigación es descubrir, analizar y evaluar las vulnerabilidades en materia de seguridad informática en la red inalámbrica wlcampus para luego proponer recomendaciones y planes de acción que puedan mejorar y fortalecer los actuales mecanismos de seguridad de red. La investigación se centra en la red inalámbrica wlcampus ya que es la red que requiere de mayor atención por el hecho de ser una red inalámbrica abierta (HotSpot). Por lo tanto, el estudio realizado tuvo como propósito llevar a cabo un ataque de suplantación de red inalámbrica del tipo: *Rogue Access Point Attack* con la finalidad de probar su efectividad en la red wlcampus para luego observar brechas de seguridad de red y la magnitud de su impacto en general.

El ataque se llevará a cabo en el área de la Biblioteca, Edificio L, Edificio B, Cyber Jardin del campus sede de la Universidad de Quintana Roo. Las herramientas de software que se utilizarán para llevar a cabo la parte práctica de esta investigación son de software libre y software de privado.

Debo destacar que actualmente existen varios tipos de ataques a redes inalámbricas que se pueden utilizar para detectar y corregir amenazas y vulnerabilidades que pudieran presentarse en una red. Sin embargo, el objetivo de este proyecto es realizar únicamente el ataque de suplantación de una red inalámbrica para la identificación de vulnerabilidades que permitiría un enfoque más profundo al tema de seguridad de la información de los usuarios. La detección y mitigación de amenazas de red a tiempo para prevenir ataques y/o el acceso no autorizado a información en la red inalámbrica wlcampus es altamente esencial para la seguridad y control de la misma.

1.6 Metodología:

Para poder llevar a cabo el estudio de las vulnerabilidades y amenazas que presenta la red inalámbrica wlcampus, se utilizará la metodología de ‘pentesting’ o ‘penetration testing’ inalámbrica que está basada sobre estándares informáticos de alto nivel. La metodología de ‘pentesting’ cuenta con los siguientes pasos:

i. Reconocimiento (activo y pasivo)

ii. Ataques y penetración
iii. Acceso a la red
iv. Evaluación de vulnerabilidades
v. Explotación y post explotación de vulnerabilidades
vi. Reporte

La realización del estudio se enfocó en el ataque de suplantación de red inalámbrica y para el reporte se agregaron recomendaciones y planes de acción que corrija y fortalezca el esquema de seguridad de la red inalámbrica wlcampus.

Capítulo 2 Marco Teórico

2.1 Introducción a las Redes Inalámbricas

Las redes inalámbricas están diseñadas para operar en bandas de frecuencia para las que no se necesita licencia de uso (2.4 GHz y de 5GHz) y por lo tanto son de carácter libre. Esta tecnología se ha visto muy beneficiada y favorecida ya que los costos de uso son mucho menores que las redes basadas en sistemas celulares o redes cableadas; además, facilita mucho su implementación y el acceso a ella en lugares donde resulta costoso, difícil o inconveniente la instalación de una red cableada.

No obstante, presenta algunas desventajas: las bandas en las que opera también son utilizadas por otras tecnologías, lo cual puede representar problemas de interferencias otro punto muy importante son los problemas derivados de los esquemas de seguridad que se implementan en dichas redes.

Las redes inalámbricas pueden clasificarse de diferentes formas dependiendo del criterio establecido. Para este caso, se clasificaron los sistemas de comunicaciones inalámbricas, de acuerdo con su alcance. El alcance se conoce como la distancia máxima a la que pueden situarse las dos partes de la comunicación inalámbrica para operación. (Martín, enero 2015)

- Las redes inalámbricas de área personal (*Wireless Personal Area Network* (WPAN)) son aquellas que tienen un área de cobertura de unos pocos metros. El propósito de estas redes es la comunicación entre cualquier dispositivo personal (por ejemplo: una computadora portátil, un teléfono móvil, tableta electrónica, etc.) con otros dispositivos o periféricos. Las tecnologías como Bluetooth, DECT entre otras utilizan en este tipo de redes. (Martín, enero 2015)
- Las redes inalámbricas de área local (*Wireless Local Area Network* (WLAN)) son aquellas que pueden llegar a cubrir distancias de uno a varios cientos de metros. Estas redes se implementan para crear un entorno de red local entre computadoras o terminales limitadas a un área geográfica como un mismo edificio o grupo de edificios. Para este tipo de red inalámbrica, la más común y frecuentemente utilizada es la tecnología WiFi pero existen otras como HomeRF, HiperLAN y OpenAir. (Martín, enero 2015)

- Las redes inalámbricas de área metropolitana (*Wireless Metropolitan Area Network* (WMAN)) son aquellas redes que pueden cubrir el área de una ciudad o entorno metropolitano. Tienen una cobertura que se extiende desde cientos de metros hasta varios kilómetros. Las tecnologías WiMax (*Worldwide Interoperability for Microwave Access*) o LMDS (*Local Multipoint Distribution Service*) son las que ofrecen soluciones de este tipo. (Martín, enero 2015)

- Las redes inalámbricas de área global (*Wireless Wide Area Network* (WWAN)) son aquellas redes basados en la tecnología celular y tienen la capacidad de cubrir un país entero o un grupo de países. Este tipo de red inalámbrica tiene como objetivo mantener la comunicación independientemente del lugar donde uno se encuentre. Las tecnologías WWAN se conocen también como sistemas de segunda generación (2G), de tercera generación (3G) y la tecnología más actual de cuarta generación (4G) definidos como un estándar de la norma 3GPP. (Martín, enero 2015)

2.2 La Tecnología Inalámbrica WIFI

La IEEE 802.11 es la tecnología inalámbrica más desplegada y utilizada en la actualidad. A esta tecnología se le conoce como Wifi (*Wireless Fidelity*). WiFi es la tecnología inalámbrica usada a gran escala para la creación de redes inalámbricas de área local. Esta tecnología tuvo sus inicios en la década de 1970s con el proyecto de investigación ALOHA NET de la universidad de Hawái pero no fue hasta en 1991 que se aprobó el proyecto 802.11.

En 1997 se desarrolló la certificación de interoperabilidad aceptada por todos los fabricantes como sistema común a través de la creación de la asociación WECA (*Wireless Ethernet Compatibility Alliance*), actualmente conocida como WiFi Alliance. El objetivo de WiFI Alliance fue crear una tecnología común como una marca que permitiese fomentar la tecnología inalámbrica y asegurar la compatibilidad de equipos. Como resultado, el usuario tiene la garantía de que todos los equipos que tengan el sello WiFi pueden ser implementados para trabajar juntos sin problemas, independientemente de su correspondiente fabricante.

Los Estándares IEEE 802.11

La IEEE 802.11 conforma una familia de estándares que gobierna la comunicación de dispositivos, terminales o estaciones de trabajo a lo largo de una red inalámbrica. Esto consiste de diferentes esquemas que ayudan en la propagación de la señal inalámbrica en una red inalámbrica. Típicamente, los estándares inalámbricos de red operan en distintas bandas a lo largo del espectro inalámbrico y también especifica los tipos de datos que pueden ser enviados y transitar la red. Es importante mencionar que los estándares y las bandas funcionan de la mano en un ambiente de red inalámbrico. Por consiguiente, un grupo de estándares pueden operar entre uno o más bandas. Dentro del grupo de trabajo IEEE 802.11 se pueden encontrar diferentes estándares tales como: (Martín, enero 2015)

IEEE 802.11b

Este estándar fue creado por la IEEE como resultado de la expansión del estándar original 802.11 en 1999 y ganó una amplia aceptación en la industria. Opera a una velocidad máxima de transmisión de 11 Mbps en la banda de frecuencia de 2.4 GHz y utiliza el método de acceso definido en el estándar original CSMA/CA. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, la velocidad real de transmisión se reduce a 5.9 Mbps sobre TCP y 7.1 Mbps sobre UDP.

Ventajas:

- Bajo costo de implementación para vendedores
- Adoptado globalmente
- Las señales no son obstruidas fácilmente
- Excelente alcance de señal

Desventajas:

- Interferencia entre electrodomésticos por su banda de frecuencia no regulado
- Tasa de transmisión de datos muy lenta

IEEE 802.11a

La IEEE crea el estándar 802.11a en julio de 1999 aunque no llega a comercializarse hasta 2002. Sin embargo, no tuvo la aceptación y ni la adopción esperada comparado con el estándar 802.11b por su alto costo de implementación. Soporta velocidades de 54 Mbps en la regulada banda de frecuencia de 5.0 GHz e incluso puede alcanzar los 72 y 108 Mbps con versiones propietarias de esta tecnología. También, este estándar utiliza la técnica OFDM (Orthogonal Frequency-Division Multiplexing) con 52 subportadoras y tiene doce canales sin solapa, 8 para red inalámbrica y 4 para conexiones punto a punto. En un entorno práctico y real, es un estándar con velocidades reales de hasta 20 Mbps.

Ventajas:

- No hay interferencia de otros dispositivos por su banda de frecuencia regulada
- Tasa de transmisión de datos rápida

Desventajas:

- No hay interoperabilidad con equipos del estándar 802.11b excepto si los equipos implementan ambos estándares.
- Bajo alcance de señal por su mayor índice de absorción de sus ondas.
- Alto costo de implementación

IEEE 802.11g

En junio de 2003 fue creado el estándar 802.11g para dar soporte a los nuevos dispositivos de red inalámbricos ya que incorporaban componentes de hardware y software más avanzados que extienden sus capacidades. Este estándar tuvo una gran aceptación en el mercado y también es desplegado juntos con el estándar 802.11b ya que combina características de los estándares 802.11a y 802.11 b. Con la idea de aumentar la velocidad sin renunciar a las ventajas de la banda de los 2.4 GHz, este estándar alcanza velocidades de transmisión de datos de 54 Mbps. El estándar 802.11g ha tenido mucho éxito ya que es compatible con el protocolo 802.11b y puede trabajar con el protocolo 802.11a cambiando la configuración de los equipos.

Ventajas:

- Adoptado globalmente
- Tasa de transmisión de datos rápida

- Alto rango de frecuencia
- Compatibilidad con estándares anteriores (802.11b y 802.11a)

Desventajas:

- Alto costo de implementación en comparación con el estándar 802.11b
- Alta probabilidad de interferencia por su banda de frecuencia no regulado
- Velocidad de transmisión reducida con clientes que utilizan el estándar 802.11b

IEEE 802.11n

El estándar 802.11n fue implementado y ratificado en septiembre de 2009 para el mejoramiento de la cantidad de ancho de banda del estándar 802.11g utilizando múltiples señales inalámbricas y antenas. A través de la incorporación de varias antenas, el estándar funciona de tal manera que utiliza varios canales para enviar y recibir datos simultáneamente, mejorando de forma sustancial la señal recibida por el receptor y como consecuencia el ancho de banda utilizado se multiplica. A esta tecnología se le conoce como MIMO (Multiple Input Multiple Output). Este estándar puede alcanzar una tasa de transmisión de datos de 600 Mbps en las bandas de frecuencia de 2.4 GHz y 5.0 GHz.

Ventajas:

- Alta velocidad de transmisión de datos
- Mejoramiento esencial en la intensidad de la señal
- Resistente a interferencias de otros dispositivos
- Utiliza los esquemas de seguridad más nuevos y robustos
- Excelente alcance de señal
- Compatibilidad con estándares anteriores (802.11b, 802.11a y 802.11g)

Desventajas:

- Alto costo de implementación en comparación con los otros estándares
- Alta probabilidad de interferencia a dispositivos que utilizan los estándares 802.11a/b/g.

IEEE 802.11ac

La IEEE 802.11ac es el estándar más reciente desarrollado entre 2011 y 2013 y fue implementado en el 2014. Es una mejora del protocolo 802.11n y actualmente la industria ya ha comenzado a trabajar y comercializar nuevos protocolos y dispositivos basados en el estándar 802.11ac. Este

estándar opera en la banda de 5.0 GHz con una velocidad de transmisión de datos de hasta 3.5 Gbps y utiliza la tecnología MIMO.

Ventajas:

- Velocidad más alta de transmisión de datos que cualquiera de los otros estándares
- Compatibilidad con estándares anteriores (802.11b, 802.11a, 802.11g y 802.11n)
- Tiene el mejor alcance de señal que cualquiera de los otros estándares (hasta un máximo de 90-100 metros mediante el uso de tres antenas internas)
- Utiliza los esquemas de seguridad más nuevos y robustos
- Altamente resistente a interferencias
- Optimización de la intensidad y rango de la señal a través de la tecnología MIMO

Desventajas:

- Alto costo de implementación en comparación con los otros estándares
- Alta probabilidad de interferencia a dispositivos que utilizan los estándares 802.11a/b/g/n.

Otras Versiones IEEE 802.11

Versión del Estándar 802.11	Descripción
802.11 c	Estándar que define las características que necesitan los puntos de acceso para actuar como puentes (bridges). Utilizado para la comunicación de dos redes distintas a través de una conexión inalámbrica.
802.11 d	Estándar que permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo móvil.
802.11 e	Estándar inalámbrico que permite interoperar entre entornos públicos, empresariales y usuarios residenciales. Añade características de QoS (calidad de servicio) y de soporte multimedia, manteniendo la compatibilidad con el estándar 802.11b y 802.11a.
802.11 f	Este estándar permite a un usuario se cambie de un punto de acceso a otro mientras está en movimiento sin importar los fabricantes de los puntos de acceso siendo utilizados en la infraestructura de red. También se conoce a esta propiedad simplemente como itinerancia (*Roaming*).
802.11 h	Estándar que proporciona al 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia como la potencia de transmisión.
802.11 i	Estándar que define el cifrado y la autentificación para complementar, completar y mejorar WEP. Es un estándar que mejora la seguridad de las comunicaciones mediante el uso de WPA a corto plazo y WPA2 a largo plazo.
802.11 k	Estándar que permite a los conmutadores (switches) y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red WLAN para incrementar su eficiencia. Está diseñado para ser implementado en software y así el equipamiento WLAN sólo requiera de actualizaciones.
802.11 m	Estándar Propuesto para el mantenimiento de redes inalámbricas.

802.11 r	Este estándar también es conocido como '*Fast Basic Service Set Transition'* y su principal característica es permitir a la red que establezca los protocolos de seguridad que identifiquen a un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él. Esta función permite transferencias rápidas, de forma que se mantenga una comunicación sin que haya cortes perceptibles.
802.11 s	Es la especificación desarrollada por el IEEE Task Group (TGs) para redes WiFi malladas. También son conocidas como redes Mesh. Se trata de una topología de red donde cada nodo está conectado a uno o varios nodos dando lugar a diferentes caminos para transmitir la información de un nodo a otro.

Tabla 1: Otras versiones del estándar IEEE 802.11

2.3 Elementos Básicos de Una Red Inalámbrica 802.11

En las redes inalámbricas existen una serie de elementos básicos que son indispensables y es importante conocerlos.

El punto de acceso (Access Point, (AP))

Es categorizado como el centro de las comunicaciones de la mayoría de las redes inalámbricas. El punto de acceso, además de ser el medio de intercomunicación de todos los terminales inalámbricos, también es el puente de interconexión con la red fija e Internet. Un punto de Acceso está compuesto por un equipo radio, antenas exteriores o interiores, un software de gestión de comunicaciones y puertos para conectar el punto de acceso a Internet o a la red cableada. A través de ondas de radio frecuencia (RF) recibe información de diferentes dispositivos llamados clientes y la transmite a través de la red cableada o viceversa. Como consecuencia de lo antes mencionado, es importante tener en cuenta aspectos como: (Martín, enero 2015)

- Comprobar las características de enrutamiento del punto de acceso tales como DHCP, NAT o propiedades firewall que facilitan la configuración y manejo de las comunicaciones con Internet o con otras redes.
- Comprobar que el AP sea compatible con el protocolo de red cableada con el que se va a conectar.
- La existencia de ciertos tipos de incompatibilidad. Los puntos de acceso WiFi funcionan sin problema con los adaptadores de red de cualquier fabricante. Sin embargo, existe cierta incompatibilidad cuando se crea una red con varios puntos de acceso de distintos fabricantes ya que estándar 802.11 es bastante ambiguo y no define con claridad todas las funciones que debería realizar un Punto de Acceso. Los diferentes

fabricantes diseñan los puntos de acceso según su criterio. Esto da lugar a que existan en el mercado puntos de acceso con características y funcionalidades muy dispares.

- Es recomendable que los puntos de acceso en un sistema distribuido sean del mismo fabricante para evitar cortes de comunicación cuando los clientes inalámbricos pasan de un AP al otro. Esto se debe a la falta de entendimiento que suele aparecer a la hora de mantener en servicio una comunicación cuando un usuario pasa del área de cobertura de un punto de acceso a otro (a esto se le llama itinerancia o *roaming*).

Los adaptadores inalámbricos de red son unas estaciones de radio con el objetivo de comunicarse con otros adaptadores en modo 'ad hoc' o con un punto de acceso en 'modo infraestructura' y permitir a los dispositivos que están conectados dentro de la red inalámbrica acceder a recursos en la red. A estos equipos también se les conoce como tarjetas de red, interfaces de red o NIC (Network Interface Cards) y cumplen con el estándar 802.11.

También existen otros elementos interesantes como los amplificadores y las antenas que se pueden agregar a una red inalámbrica 802.11 y sirven para direccionar y mejorar las señales de Radio Frecuencia (RF) transmitidas.

La mayoría de los dispositivos y computadoras tienen integrado el adaptador de red inalámbrico. Cabe mencionar que es importante la compatibilidad del adaptador WiFi con el router o punto de acceso.

2.4 Tipos de Configuraciones de Red 802.11

Los dos tipos de configuraciones que se pueden llevar a cabo en una red inalámbrica 802.11 desde el punto de vista del tipo de equipamiento son las siguientes: (Martín, enero 2015)

2.4.1 Modo Ad hoc.

Este modo de configuración se pone en marcha cuando sólo se necesita disponer de tarjetas de red o dispositivos inalámbricos WiFi que se puedan conectar entre si y formen una red. La red se le denomina ad hoc porque no depende de una infraestructura pre-existente, como puntos de accesos en redes inalámbricas administradas o de routers en redes

cableadas. En lugar de ello, cada nodo participa en el enrutamiento mediante el reenvío de datos hacia otros nodos.

La determinación que toman estos nodos al momento de la transmisión de información se hace dinámicamente sobre en base a la conectividad de la red. Este tipo de configuración de red facilita en gran medida la agregación de nuevos dispositivos con el solo hecho de estar en el rango de alcance de un nodo ya perteneciente a la red establecida. Por otra parte, el principal inconveniente de este tipo de configuración de red radica en el número de saltos que debe recorrer la información transmitida antes de llegar a su destino. Para este caso, cada nodo que retransmite la información significa un salto. Por lo tanto, cuanto más saltos existan entre el origen y destino de la información, mayor es el tiempo que tarda en llegar a su destino y además, la probabilidad de que la información se corrompa con cada salto aumenta.

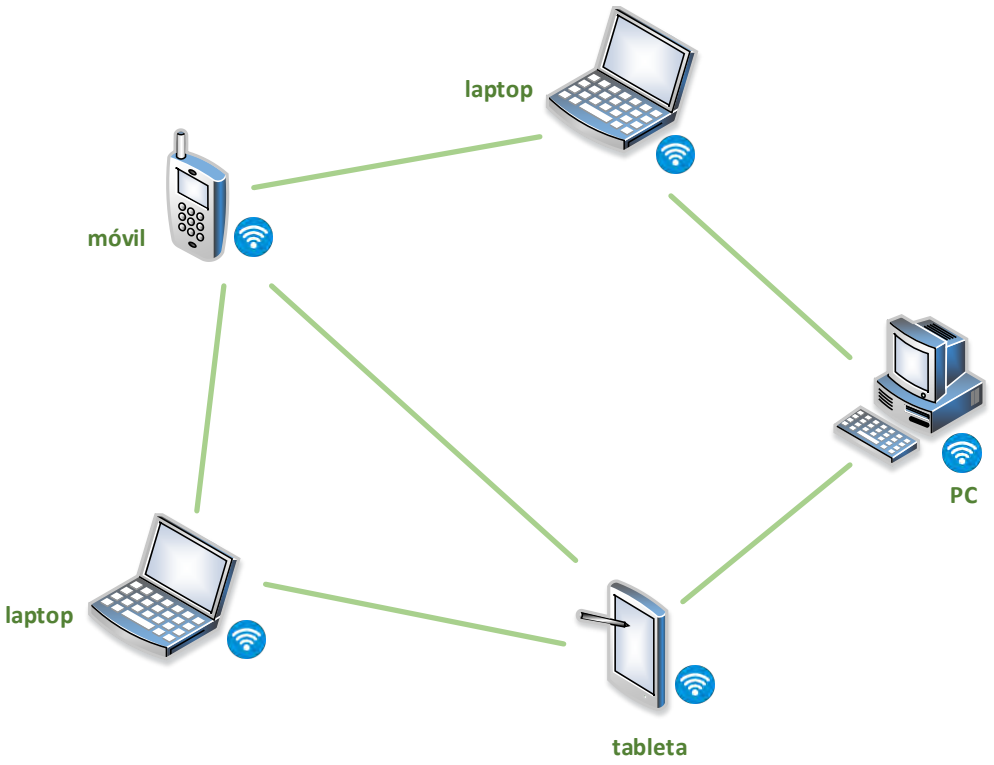

Ilustración 1: Topología de modo de configuración Ad hoc

2.4.2 Modo infraestructura. Para este tipo de configuración, se necesita disponer de un equipo conocido como Punto de Acceso (AP) además de las tarjetas de red WiFi. Para este escenario,

los clientes inalámbricos se conectan a un punto de acceso a través de un enlace inalámbrico. El entorno creado por el punto de acceso y los clientes inalámbricos ubicados dentro del área de cobertura del punto de acceso se le conoce como conjunto de servicio básico (*Basic Service Set* (BSS)). En un ambiente inalámbrico, se pueden tener más de un BSS y cada BSS se identifica a través de un BSSID que corresponde a la dirección MAC del punto de acceso.

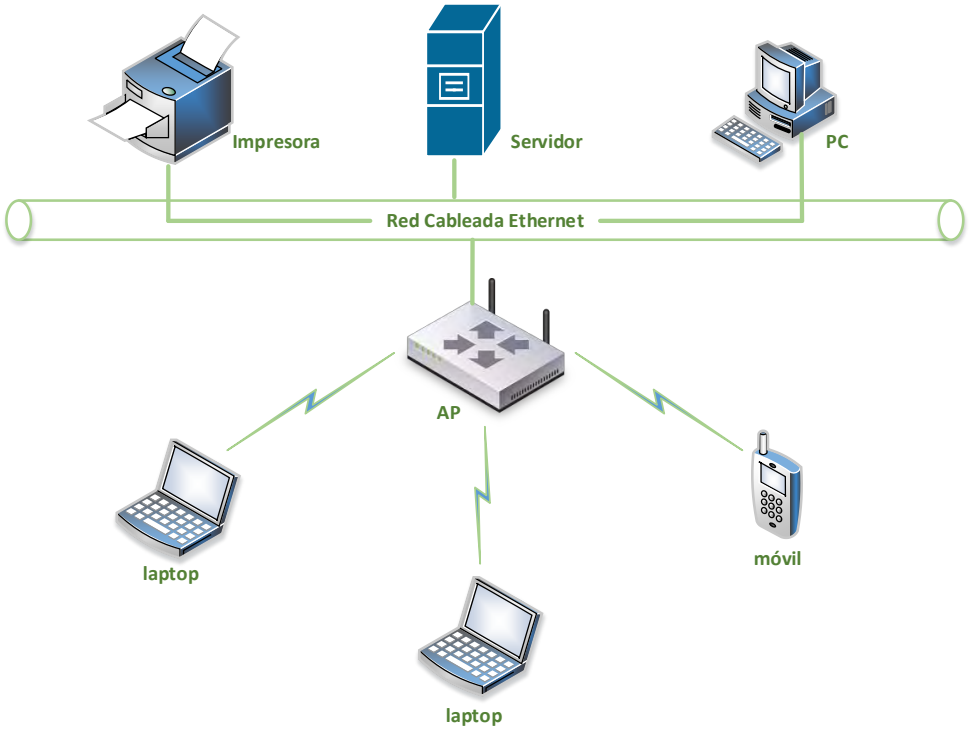

Ilustración 2: Topología de modo de configuración Infraestructura

Al momento de vincular varios BSS o varios puntos de acceso, se necesita establecer una conexión llamada sistema de distribución (SD) para formar un conjunto de servicio extendido (*Extended Service Set* (ESS)). Un ESS se identifica a través de un identificador del conjunto de servicio extendido (*Extended Service Set Identifier* (ESSID)). Cabe mencionar que un ESSID también se puede abreviar como un SSID, ya que una estación debe saber el SSID o dirección MAC de uno de los puntos de acceso del sistema distribuido para conectarse a la red extendida. Esto de alguna manera representa una medida de seguridad de primer nivel.

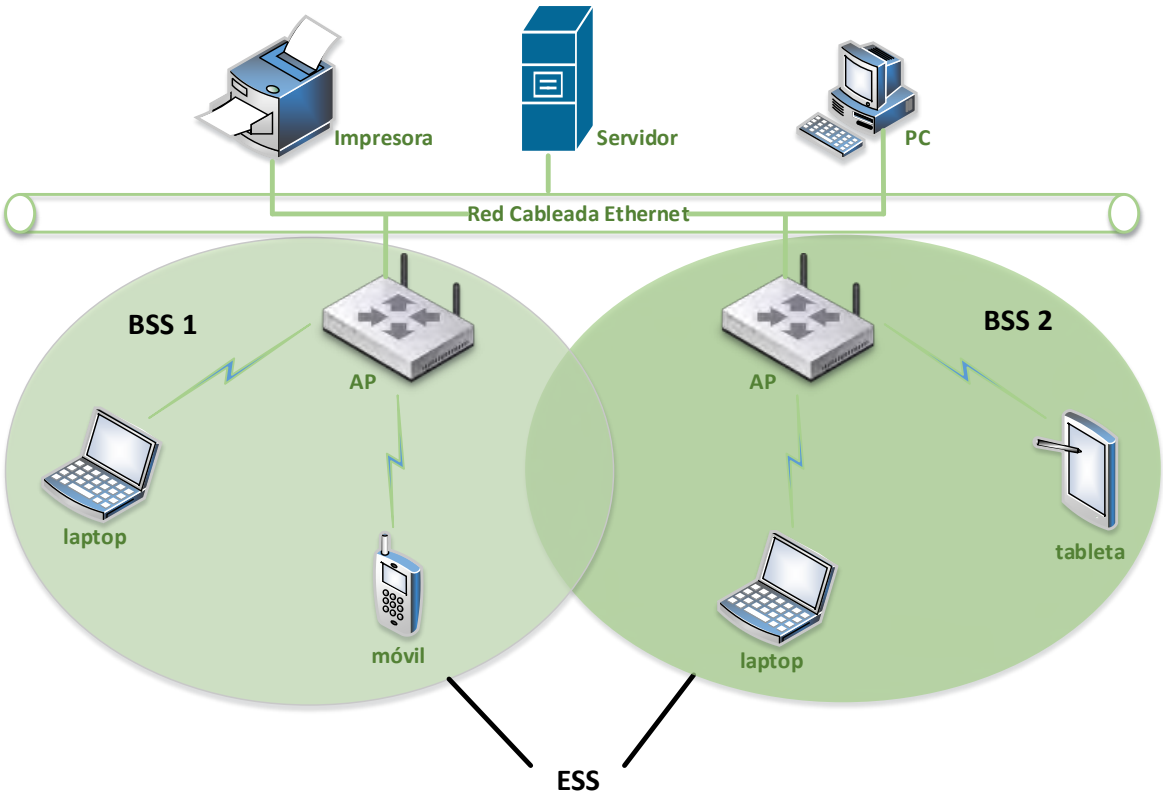

Ilustración 3: Topología de modo de configuración ESS

El modo infraestructura es el más adecuado para crear redes permanentes. Las ventajas del modo infraestructura sobre la modalidad Ad-hoc son: (Martín, enero 2015)

- Ofrece un mayor alcance que la modalidad ad hoc ya que os terminales no tienen por qué estar dentro del área de cobertura el uno del otro y pueden duplicar su distancia al tener un punto de acceso de intermedio.
- El punto de acceso permite compartir el acceso a Internet entre todos sus terminales y también permite compartir un acceso de banda ancha (ADSL o cable) entre todos los terminales que forman la red.
- El punto de acceso permite crear redes con un mayor número de clientes inalámbricos.
- El punto de acceso permite la gestión centralizada de la comunicación, algo que no ofrece el modo ad hoc.
- Los recursos de los terminales que forman la red como lo son archivos, impresoras entre otras, son compartidos a través del punto de acceso.

No obstante, las comunicaciones ad hoc son muy fáciles de configurar y resultan muy interesantes cuando se necesita establecer una comunicación temporal entre dos equipos.

2.5 Bandas de frecuencias y Canales

Las dos bandas de frecuencias que las redes WiFi utilizan para operar son las siguientes:

- Banda de 2.4 GHz
- Banda de 5 GHz

Estas dos bandas de frecuencias no requieren de licencia para su utilización pero están sujetas a la regulación de un organismo que controla y regula su uso en cada país y zona geográfica. Es importante mencionar que ambas bandas están designadas para aplicaciones ISM (*Industry, Science and Medical*) ó ICM (Industrial, Científica y Médica). (Martín, enero 2015)

Número de Canal	Europa (ETSI)	Norte America (FCC)	Japan
1	✓	✓	✓
2	✓	✓	✓
3	✓	✓	✓
4	✓	✓	✓
5	✓	✓	✓
6	✓	✓	✓
7	✓	✓	✓
8	✓	✓	✓
9	✓	✓	✓
10	✓	✓	✓
11	✓	✓	✓
12	✓	No	✓
13	✓	No	✓
14	No	No	Solo 802.11b

Tabla 2: Canales autorizados por ETSI, FCC y Japón

2.5.1 Banda 2.4 GHz:

La banda de 2.4 GHz para las redes WiFi consta de un rango de frecuencias que va desde 2.4 GHz a 2.4835 GHz. Existen un total de 14 canales disponibles, sin embargo, cada país y zona geográfica aplica sus propias restricciones en cuanto al número de canales disponibles. El ancho de banda por canal es de 22 MHz en la banda de 2.4 GHz y la separación entre cada canal es de 5MHz excepto para los canales 13 y 14 que tiene una separación de 12 MHz. Debido a una corta separación entre los anchos de banda de los 14 canales, esto hace que se produzca un solapamiento de todos los canales con sus adyacentes. El término de solapamiento está definido como la superposición o solapamiento del rango de frecuencia entre dos canales que pueden generar interferencias entre ellas. (Martín, enero 2015)

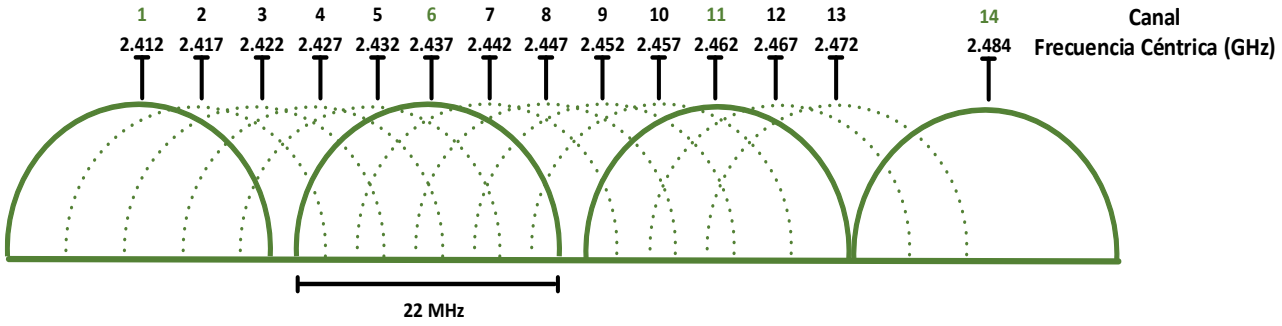

Ilustración 4: Canales y sus respectivas frecuencias céntricas para la banda de 2.4 GHz

De acuerdo a la figura, el canal 1 se superpone con los canales 2, 3 ,4 y 5, y como consecuencia, los dispositivos que emitan la señal inalámbrica en ese rango de frecuencias pueden provocar interferencias entre sí. Lo mismo sucede con el canal 6 y los canales 7, 8, 9 y 10, y también con el canal 11 y los canales 12 y 13. Esto quiere decir que para obtener un rendimiento óptimo en cuanto a la señal emitida a través de los distintos canales de la red inalámbrica WiFi, los dispositivos conocidos como puntos de acceso (Access Points (AP)) deben ser configurados en los canales que no se traslapan con otros canales, bien sea el canal 1, el canal 6 o el canal 11, dependiendo del nivel de saturación de la zona de cobertura. Cabe mencionar que solo se puede tener un máximo de 4 canales sin solapamiento en el orden siguiente: canal 1, 6, 11 y 14. (Martín, enero 2015)

2.5.2 Banda 5 GHz.

La banda de 5 GHz opera a tasas máximas de transferencia de datos y dispone de un mayor ancho de banda que la banda de frecuencia de 2.4 GHz. También presenta un menor nivel de interferencias ya que existen menos servicios que los que se pueden encontrar en la banda ICM. Por otra parte, esta banda presenta otros problemas ya que el uso de mayores frecuencias implica mayor atenuación en las transmisiones y en cuanto a las bandas existe poca armonía. Los canales cuentan con un ancho de banda de 16.6 MHz y están separados por 20 MHz. El rango de los canales empieza del canal 36 (5.15 GHz) hasta el canal 165 (5.82 GHz) en el espectro. Las bandas de frecuencia indicadas por los distintos canales podrán ser utilizadas por el servicio móvil en sistemas y redes de área local de altas prestaciones. Una gran ventaja que tiene esta banda de frecuencia es que el espectro de ningún canal solapa con algún otro canal por lo que pueden ser utilizados todos al mismo tiempo. En el año 2003, la banda de 5 GHz fue aprobada para uso común aunque sigue siendo regulada debido a su importancia y las interferencias con distintos equipos como lo son radares climáticos y otras aplicaciones militares. Ante la presión de entidades influyentes en el ámbito de las telecomunicaciones, la IEEE creó un requerimiento llamado selección de frecuencias dinámicas (*Dynamic Frequency Selection* (DFS)) en donde dispositivos sin licencia que cumplan con el requerimiento puedan utilizar y operar en la banda de 5 GHz. DFS es un mecanismo que permite a los dispositivos sin licencia poder utilizar el espectro de 5 GHz sin causar interferencias con los sistemas de radar. (Martín, enero 2015)

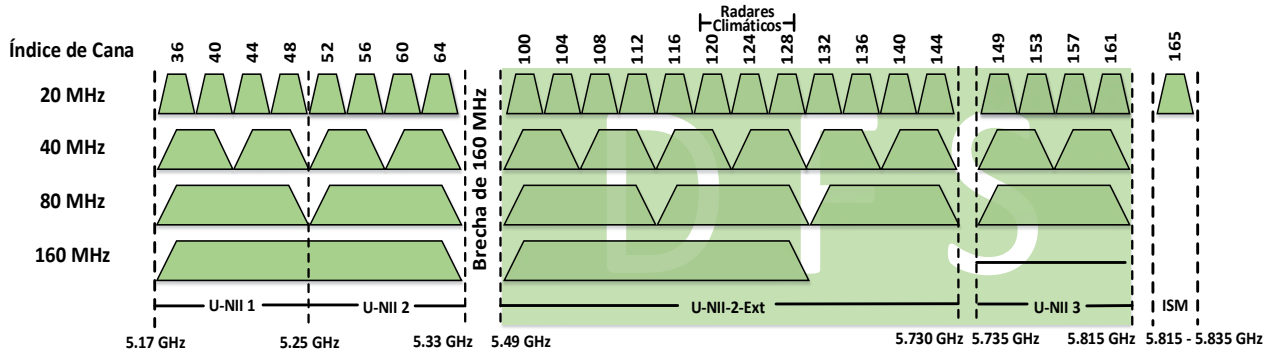

Ilustración 5: Canales y sus respectivas frecuencias para la banda de 5.0 GHz

2.6 Capa Física y Capa de Enlace

La organización IEEE diseñó y desarrolló el primer estándar para redes LAN inalámbricas (IEEE 802.11) para que pudiera sustituir a las capas física y enlace de datos (MAC) de la tecnología IEEE 802.3 mejor conocido como Ethernet. La diferencia de estos estándares o normas es la forma en que las computadoras y terminales acceden a la red ya que el resto es similar. Las nuevas versiones creadas a raíz de un mismo estándar se consiguen simplemente con modificar una de las capas, ya sea la capa física o la capa de enlace de datos. Por consiguiente, el proceso de crear nuevas versiones a raíz de un mismo estándar facilita no sólo la evolución de los estándares, sino que también la compatibilidad de un mismo equipo con distintas versiones de un estándar. Un claro ejemplo sería la tecnología IEEE 802.11b que sólo se diferencia de la tecnología IEEE 802.11 en que su capa física permite transmitir datos a una velocidad mucho más alta. (Martín, enero 2015)

La tecnología IEEE 802.11 está basada en la arquitectura IEEE 802 creada para las redes LAN. Las dos primeras capas del modelo OSI (capa física y capa de enlace de datos) son las que define el estándar IEEE 802. La capa física del estándar 802.11 corresponde totalmente con la capa física del modelo OSI y la capa de enlace se divide en dos subcapas (Control de acceso al medio (MAC) y Control de enlace lógico (LLC)) para el estándar 802.11 al igual que en todos los estándares IEEE 802. Por lo tanto, la arquitectura de las capas queda de la siguiente manera: (Martín, enero 2015)

- PHY (Physical Layer, Capa física)
- DLL (Data Link Layer, 'Capa de enlace de datos')
  - MAC (Medium Access Control, 'Control de acceso al medio')
  - LLC (Logical Link Control, 'Control de enlace lógico')

Como se ya se había mencionado anterior, las capas restantes para el estándar IEEE 802.11 son idénticas a las empleadas en las redes locales cableadas e Internet y se le conoce como un conjunto de protocolos IP (Internet Protocol).

2.6.1 La Capa Física

La capa física es la que define las características mecánicas, eléctricas y funcionales del canal de comunicación y lo hace Intercambiando tramas entre la capa física (PHY) y la primera subcapa (MAC) de la capa de enlace de datos (DLL). La capa física utiliza los mecanismos de la portadora de señal y modulación de espectro aumentado para transmitir tramas a través del medio y proveer a la subcapa MAC de un indicador de detección de portadora para señalizar actividad en el medio. También, la capa física es la responsable de definir los métodos por los que se difunde la señal y para lograr esto en el estándar 802.11, dicha capa se divide en dos subcapas: PLCP (*Physical Layer Convergence Procedure*, 'Procedimiento de convergencia de la capa física') la cual se encarga de convertir los datos a un formato compatible con el medio físico y PMD (*Physical Medium Dependent*, 'Dependiente del Medio físico') la cual permite la difusión de la señal. (Martín, enero 2015)

Subcapa PMD (*Physical Medium Dependent*)

La subcapa PMD tiene como objetivo la gestión de las características particulares del medio inalámbrico y también define los métodos para transmitir y recibir datos en el medio. Es importante mencionar que la tecnología básica para el funcionamiento de los sistemas inalámbricos es el sistema conocido como espectro expandido. Esta tecnología implementa una técnica de modulación empleada en telecomunicaciones para la transmisión de datos digitales y transmisión por radiofrecuencia. Esta técnica de modulación consigue que el ancho de banda real utilizado en la transmisión sea superior a la que necesita estrictamente y esto hace que el sistema sea muy resistente a las interferencias de otras fuentes de radio. Por lo tanto, la implementación de este sistema puede coexistir con otros sistemas de radiofrecuencia sin verse afectado. (Martín, enero 2015)

En la siguiente tabla se muestran las técnicas de difusión utilizadas por los diferentes estándares 802.11 que posibilitan el envío de tramas MAC de una estación a otra, dependiendo de la velocidad a la que se vayan a transmitir los datos. (Martín, enero 2015)

Estándar	Técnicas de difusión
802.11	IR, FHSS, DSSS
802.11a	OFDM
802.11b	DSSS
802.11g	DSSS Y OFDM
802.11n	MIMO-OFDM

Tabla 3: Técnicas de difusión que se aplican en las versiones a,b,g,n del estándar IEEE 802.11

Infrarrojos (*Infrared* (IR)) es un medio de transmisión que fue utilizado en las primeras versiones de la tecnología 802.11. Esta técnica de difusión utiliza la luz infrarroja que es un tipo de radiación electromagnética invisible para el ojo humano. Los sistemas de comunicaciones con infrarrojo

funcionan en base a la emisión y recepción de haces de luz infrarroja y estos sistemas de comunicaciones pueden ser divididos en dos categorías: (Martín, enero 2015)

- Infrarrojo de haz directo: Para que se produzca la comunicación, se necesita una visibilidad directa sin obstáculos entre ambos terminales.
- Infrarrojo de haz difuso: Los terminales involucrados en la comunicación tienen suficiente potencia como para alcanzar el destino mediante múltiples reflexiones en los obstáculos intermedios y no se necesita visibilidad directa entre los terminales.

El espectro infrarrojo para los sistemas de comunicación está comprendido entre los 850 y 950 nanómetros (nm) y alcanzando velocidades de 1 y 2 Mbps, usando modulación PMM. Por otra parte, las ventajas que ofrecen las comunicaciones de infrarrojo es que no están reguladas, son resistentes a las interferencias de los sistemas de radio de alta frecuencia y son de bajo coste. Sin embargo, sus desventajas son su corto alcance, su deficiencia a la hora de traspasar objetos y su limitación a entornos cerrados ya que no son utilizables en el exterior debido a que agentes naturales como la lluvia o la niebla les producen grandes interferencias. No obstante, cuando se habla de sistemas de comunicaciones punto a punto para corta distancia los sistemas infrarrojos son de los más eficaces. (Martín, enero 2015)

Espectro expandido por salto de frecuencia (*Frequency Hopping Spread Spectrum* (FHHS)) es un mecanismo que consiste en dividir la banda de frecuencias en un conjunto o serie de canales e ir transmitiendo la información dando saltos de un canal a otro siguiendo un patrón de saltos (*Hopping code*). El patrón u orden de los saltos en frecuencia está determinada por una secuencia pseudoaleatoria almacenada en unas tablas. Esta tabla tiene que ser conocido tanto por el emisor como por el receptor y el tiempo máximo que se debe permanecer en cada frecuencia es de 400 ms. Cuando se haya pasado ese tiempo, se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. Esta técnica utiliza el rango de frecuencia de 2.4 GHz y se encuentra organizada en 79 canales con un ancho de banda de 1 MHz por cada canal. Cabe mencionar que la técnica FHHS es equivalente a una multiplexación en frecuencia. (Martín, enero 2015)

Espectro ensanchado por secuencia directa (*Direct-Sequence Spread Spectrum* (DSSS)) es una técnica que tiene como objetivo generar un patrón de bits redundante por cada uno de los bits que componen la señal. Mediante esta técnica de difusión de señal inalámbrica, se sustituye cada bit de información por una secuencia de bits conocida como código de chips (chipping code). El propósito de estos códigos de chips es permitir a los receptores filtrar las señales y eliminar cualquier señal que no utiliza la misma secuencia de bits como por ejemplo, el ruido y las interferencias en el ambiente. Cabe mencionar que cuanto mayor sea este patrón de bits, mayor será la resistencia de la señal a las interferencias. Para el estándar IEEE 802.11, se recomienda que el tamaño de la señal sea de 11 bits aunque el óptimo es de 100 bits. Por otra parte, la secuencia de bits utilizada para modular los bits de la señal se conoce como la secuencia de Barker. Cuando se implementa esta técnica, solo los receptores a los que el emisor haya enviado previamente la secuencia, pueden descifrar los datos y reconstruir la señal original. (Martín, enero 2015)

Multiplexación por división de frecuencias ortogonales (*Orthogonal Frequency Division Multiplexing* (OFDM)) es un mecanismo de multiplexación que crea una combinación de dos o más canales de información en un solo medio de transmisión. Esto es posible mediante la emisión de un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información. Dicho de otra manera más detallada, OFDM divide el ancho de banda en subcanales más pequeños que operan en paralelo consiguiendo velocidades de transmisión de hasta 54 Mbps. La técnica OFDM está basada en la transformada rápida de Fourier (*Fast Fourier Transform* (FFT)) y su objetivo primordial es dividir la frecuencia portadora en 52 subportadoras solapadas donde 48 de estas subportadoras son utilizadas para transmitir datos y las otras cuatro para poder alinear las frecuencias en el receptor y establecer la comunicación. La ortogonalidad de las portadoras es el concepto principal de las señales OFDM debido a que permite la transmisión simultánea en un ajustado rango de frecuencias, reduciendo notablemente el ancho de banda y sin que se produzcan interferencias entre ellas. A través de la multiplexación OFDM, se puede transmitir datos a distintas velocidades, utilizando diferentes técnicas de modulación en cada una de ellas. Las velocidades normalizadas para la transmisión de datos utilizando OFDM son 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. (Martín, enero 2015)

En el siguiente esquema se muestra el ahorro de ancho de banda que supone la técnica OFDM con respecto a una técnica multiportadora convencional. (Martín, enero 2015)

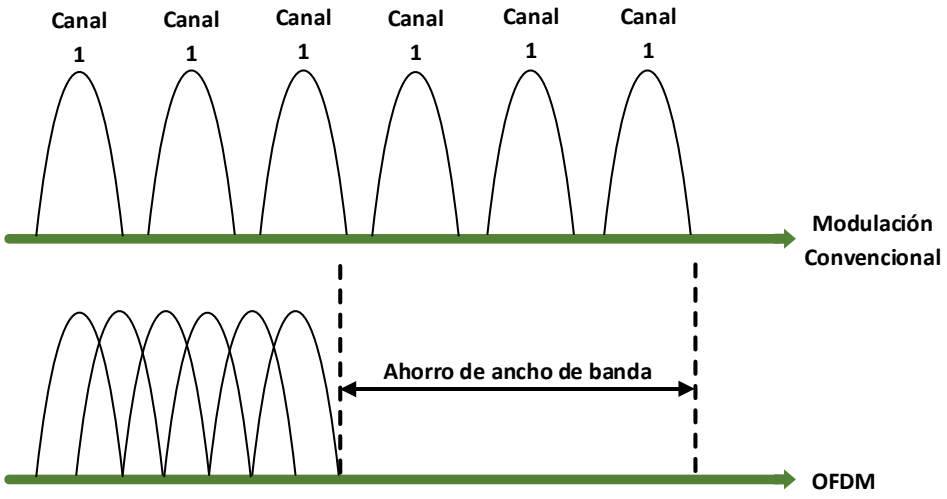

Ilustración 6: Comparación de la técnica de Modulación Convencional y OFDM

Múltiple entrada múltiple salida (*Multiple Input Multiple Output* (MIMO)) es una tecnología que implementa el uso de múltiples antenas transmisoras y receptoras con el propósito de mejorar el desempeño del sistema al poder manejar más información que cuando se utiliza una sola antena. Esta tecnología es posible gracias al desfase de la señal, que a su vez hace que la señal rebote o sea reflejada. Sin embargo, en lugar que la señal rebotada o reflejada sea destructiva, la hace constructiva y como consecuencia se produce una mayor velocidad. El concepto principal de MIMO se basa que al haber menor pérdida de datos, se necesitan menos retransmisiones y por lo tanto se logran velocidades mayores. Es decir, la tecnología MIMO aprovecha fenómenos físicos como

la propagación multitrayecto para incrementar la tasa de transmisión y reducir la tasa de error. Otra funcionalidad de MIMO es el Multiplexado de División Espacial (SDM) que multiplexa espacialmente flujos de datos independientes, transportados simultáneamente con un canal de frecuencia o canal de ancho de banda. SDM aumenta la eficiencia espectral de un sistema de comunicación inalámbrica y es un factor clave de la tecnología MIMO. Por otra parte, el estándar IEEE 802.11n utiliza la tecnología MIMO para lograr un rendimiento de aproximadamente unos 300 Mbps ya que MIMO permite incrementar significativamente el área de cobertura y hasta más de seis veces la velocidad de las actuales redes IEEE 802.11g. Igualmente, MIMO una de las primeras tecnologías para las comunicaciones inalámbricas que ha innovado el tratamiento de la propagación multidireccional como una característica esencial en los ambientes inalámbricos. (Martín, enero 2015)

Subcapa PLPC

La subcapa de la capa física llamado procedimiento de convergencia de la capa física (*Physical Layer Convergence Procedure* (PLCP)), tiene como objetivo principal convertir los datos a un formato compatible con el medio físico. PLCP es la subcapa superior de la capa física que aplica un procedimiento de convergencia al convertir MPDUs (*Media Access Control Protocol Data Unit*) en PPDUs (PLCP *Protocol Data Unit*) y viceversa. Durante la transmisión, se le adiciona, a la MPDU, un preámbulo y una cabecera para crear la PPDU. Durante la recepción, se procesa el preámbulo y la cabecera y luego se expide la MPDU. (Martín, enero 2015)

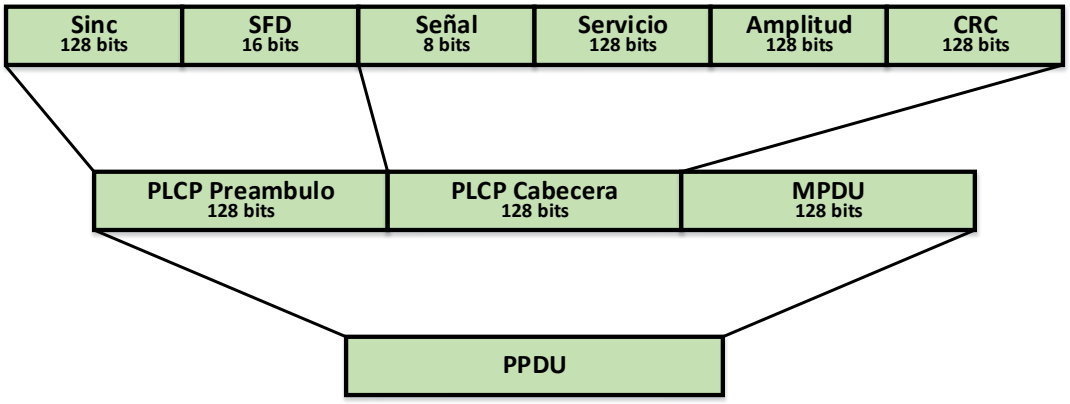

Ilustración 7: Trama PLCP

De acuerdo a la figura, la trama PLCP está compuesta de los siguientes tres campos: (Martín, enero 2015)

- Preámbulo: El receptor utiliza este campo para adquirir la señal entrante y sincronizarlo con el demodulador. Indica el inicio de una trama y contiene los campos de sincronización (SYNC) y delimitador del inicio de trama (SFD).
- Cabecera PLCP: Este campo contiene información acerca de la trama de dirección física (MAC) transmitido, al igual que la duración o la velocidad de transmisión utilizada. Además, contiene los campos de señalización IEEE 802.11 que indica la modulación

que será utilizada para la transmisión y recepción (SEÑAL), el servicio IEEE 802.11 (SERVICIO), Longitud (AMPLITUD) que indica el número de microsegundos requeridos para transmitir la MPDU y CRC que protege a los campos SEÑAL, SERVICIO y AMPLITUD.

- Payload: Este campo hace referencia a la PDU-PLCP que son los datos o la trama entregada por la MAC.

El conjunto de estos tres campos crean y dan el formato general de una trama PLCP y también conforman a lo que se le conoce por PPDU.

2.6.2 Capa de Enlace de Datos

De acuerdo con el modelo OSI, la capa de enlace de datos se divide en dos niveles o subcapas, Control de Acceso al Medio (Medium Access Control (MAC)) y Control del enlace lógico (*Logical Link Control* (LLC)). Sin embargo, cuando se hace referencia al estándar 802.11, la subcapa más importante es el control de acceso al medio (MAC). Esta subcapa se encarga de definir los procedimientos que permiten a los distintos dispositivos compartir el uso del espectro radioeléctrico. Cabe mencionar se encuentran distintas versiones del estándar 802.11 y estas utilizan diferentes mecanismos para difundir su señal ya la capa física es distinta. No obstante, la subcapa MAC es la misma para todas ellas. (Martín, enero 2015)

Para la subcapa MAC, sus diversas funciones se mencionan a continuación: (Martín, enero 2015)

- Exploración/Búsqueda: Esta funcionalidad se refiere al proceso por el cual una determinada estación logra identificar la existencia de una determinada red inalámbrica. Durante este proceso, se envían señales que identifican la estación a través de los SSID (*Service Set Identifiers*) y los ESSID (*Extended SSID*) con una longitud máxima de 32 caracteres.
- Autenticación: Esta función establece la identidad de las estaciones y autoriza la asociación entre las estaciones y terminales que quieran comunicarse en una red. Para el estándar 802.11, la autenticación se da de dos formas: Autenticación de sistema abierto o Autenticación de Clave compartida.
    - Autenticación de sistema abierto: La autenticación de sistema abierto simplemente consta de dos procesos en cuanto a la comunicación. La primera es una solicitud de autenticación por el cliente que contiene el ID de estación (por lo general, la dirección MAC). Esto es seguido de una respuesta de autenticación desde el punto de acceso o enrutador que contiene un mensaje de resultado correcto o incorrecto. Un ejemplo de cuándo puede producirse un fallo es si dirección MAC del cliente se excluye explícitamente en la configuración del punto de acceso o enrutador.

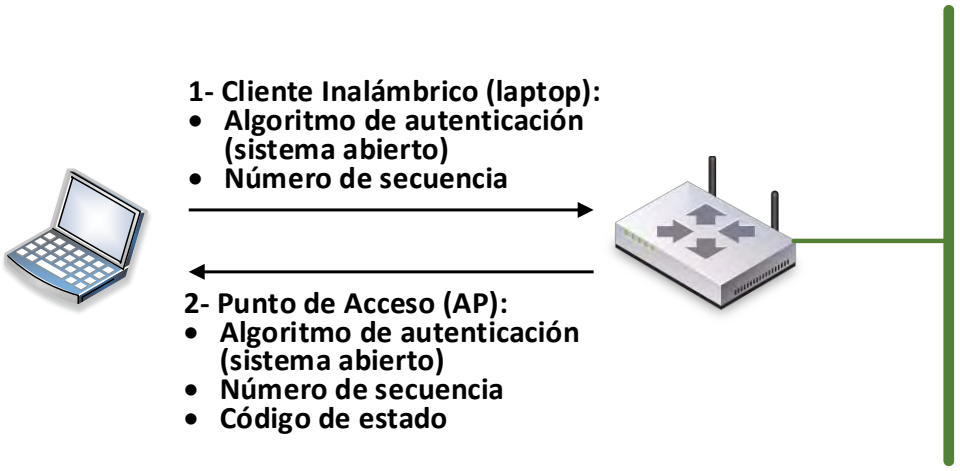

Ilustración 8: Autenticación Sistema Abierto

Para este tipo de autenticación, el cliente envía una solicitud de autenticación con su SSID a un punto de acceso (*Access Point* (AP)), el cual autorizará o no la asociación entre ambas. Primero, la estación que requiere el acceso envía una primera trama donde se especifica el identificador del algoritmo de autenticación, y el número de secuencia de transacción de la autenticación. Por otra parte, la identificación de una estación con el estándar 802.11 se hace por medio de la transmisión de la dirección MAC de esa estación. Sin embargo, el punto de acceso es el responsable de dar respuesta al requerimiento de autenticación y lo hace enviando en una trama que contiene el identificador del algoritmo de autenticación, el número de secuencia de transacción de autenticación y el código de estado indicando el resultado del requerimiento. Cabe mencionar que esta es la única autenticación obligatoria para el estándar 802.11. (Martín, enero 2015)

- Autenticación de clave compartida: La autenticación de clave compartida se basa en el hecho de que ambas estaciones que participan en el proceso de autenticación tengan la misma clave o frase de contraseña. La clave compartida se establece manualmente en la estación cliente como en el punto de acceso o enrutador. Los tres tipos de autenticación de clave compartida en entornos de WLAN disponibles hoy para el hogar o una oficina son privacidad equivalente a cable (*Wired Equivalente Privacy* (WEP)), acceso protegido a WiFi (*WiFi Protected Access* (WPA)) y acceso protegido a WiFi versión 2 (*WiFi Protected Access* (WPA2)).

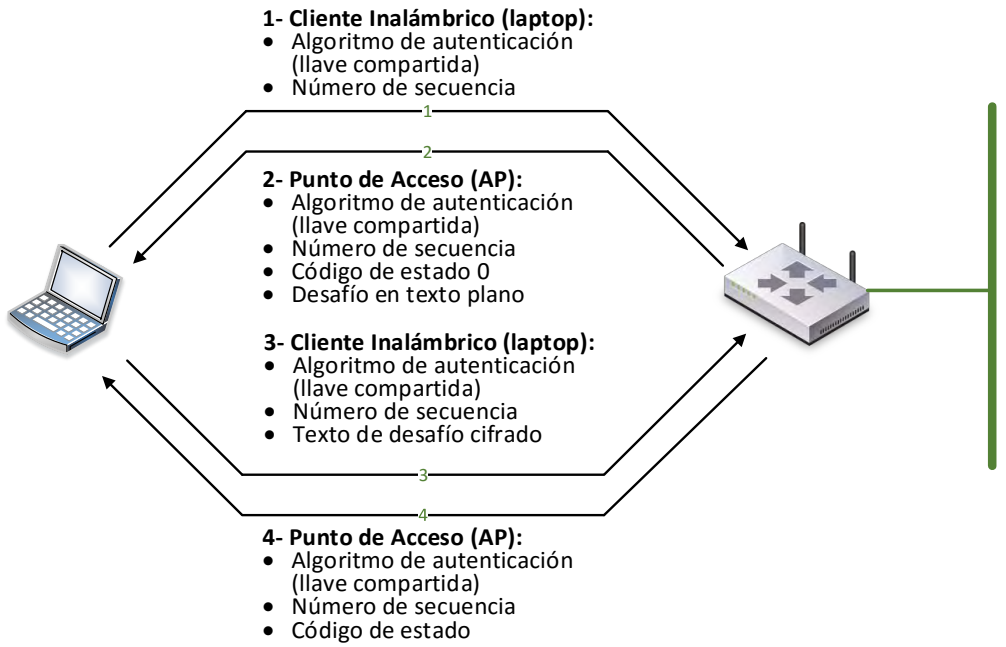

Ilustración 9: Autenticación Clave Compartida

- Asociación:
  Esta funcionalidad se refiere al proceso que le dará al cliente acceso a la red y solo puede ser llevado a cabo una vez realizada la autenticación.
- Seguridad:
  Esta funcionalidad define mecanismo de seguridad para la autenticación y cifrado de los datos cuando se tenga acceso a la red. Los tres mecanismos de seguridad que se utilizan con mayor frecuencia son WEP, WPA y WPA2. WEP es un protocolo se cifra solo los datos pero no los encabezados. Los protocolos WPA y WPA2 son los protocolos de seguridad que se prefieren para las redes WLAN y se especificarán más adelante.
- Señales de control RTS/CTS:
  Esta funcionalidad permite el intercambio de señales que gestionan el canal y que define el tamaño de trama (para el estándar 802.11, el tamaño está entre 256 y 2312 bytes)
- Gestión de potencia:
  Debido a la cantidad de potencia necesaria para transmitir y el consumo de energía que esto implica, el ahorro de potencia es una necesidad importante en comunicaciones. Los puntos de acceso pueden comprender que la estación está en modo de ahorro de energía y como consecuencia, colocan en su buffer las tramas de dichas estaciones.
- Fragmentación:
  La fragmentación se define como la capacidad que tiene un AP para dividir la información en tramas más pequeñas y así garantizar su recepción.

- Sincronización, direccionamiento, comprobación de errores y los servicios de gestión de 'roaming' dentro de un ESS se consideran también como otras de las funciones principales de la subcapa MAC.

La subcapa MAC utiliza la técnica conocida como Acceso múltiple por detección de portadora (*Carrier Sense Multiple Access* (CSMA)) en conjunto con la tecnología CA (*Collision Avoidance*, 'Evitación de la Colisión'). Una colisión se produce cuando dos terminales intentan hacer uso del medio físico simultáneamente. La tecnología CA dispone de procedimientos para evitar que se produzcan colisiones. En contraste, el estándar Ethernet también utiliza la técnica CSMA pero en conjunto con la tecnología CD (*Collision Detection*, 'Detección de Colisión'), mientras que la versión inalámbrica utiliza la tecnología CA. La tecnología CD detecta que se ha producido una colisión y retransmite los datos. (Martín, enero 2015)

La subcapa MAC implementa la técnica CA que tiene como objetivo evitar colisiones ya que en el medio radioeléctrico un terminal no puede transmitir y recibir al mismo tiempo por el mismo canal. Esto haría que la transmisión dejará opaca a la recepción. Entre la capa MAC y la capa física se intercambian tres tipos de tramas: de control, de gestión y de información. La arquitectura MAC del estándar 802.11 coordina la transferencia de datos a través de dos funciones de coordinación. Estas dos funciones de coordinación determinan, dentro de un conjunto básico de servicios (Basic Service Set (BSS)), cuándo una estación puede transmitir y/o recibir unidades de datos de protocolo a nivel MAC a través del medio inalámbrico. Las dos funciones son: (Martín, enero 2015)

- Función de coordinación distribuida (*Distributed Coordination Function* (DCF)): Esta función se encuentra en el nivel inferior de la subcapa MAC y su manera de operar se basa en técnicas de acceso aleatorias de contienda por el medio. El tráfico que se transmite bajo esta funcionalidad es de carácter asíncrono. La función DCF permite que todas las estaciones compiten por el acceso al canal simultáneamente y para ello facilita un mecanismo para compartir el medio físico entre todas las estaciones de la red. CSMA/CA con RTS/CTS son mecanismos para el estándar 802.11 que le permiten a las estaciones negociar el acceso al medio físico, así como asegurar la entrega de los datos a las estaciones. El algoritmo CSMA/CA consiste en realizar pruebas en el medio o canal inalámbrico antes de transmitir para determinar su estado ya sea que esté libre u ocupado. La función DCF contempla un mecanismo físico conocido como CCA (Clear Channel Assessment, 'Valoración de la disponibilidad del canal' que comprueba si el medio está siendo utilizado antes de transmitir:
- Función de coordinación del punto (*Point Coordination Function* (PCF)): Esta función se encuentra situada por encima de la funcionalidad DCF. El tráfico que se transmite bajo esta funcionalidad es de carácter síncrono que utilizan técnicas de acceso deterministas ya que no toleran retardos aleatorios en el acceso al medio. A la estación que hace uso de esta función se le llama coordinadora del punto (*Point Coordinator* (PC)) y generalmente se trata de un punto de acceso. El PC emite una señal guía con la duración del periodo de tiempo que necesita

disponer del medio. Las estaciones que reciben esta señal no emiten durante ese tiempo. La función PCF es totalmente compatible con DCF y pueden operar conjuntamente dentro de un mismo entorno o un conjunto básico de servicios

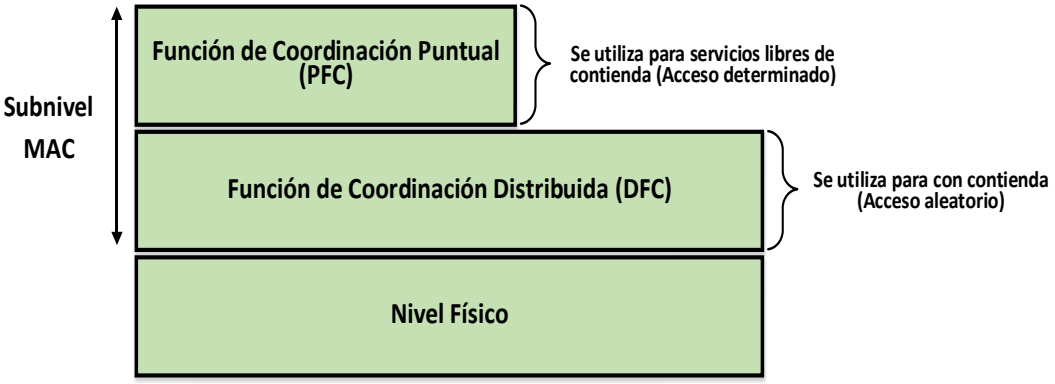

Ilustración 10: Funciones de coordinación MAC

Encabezados y Tramas

Cada trama enviada en una red inalámbrica, tiene encabezados que contienen distinta información. Una típica trama de MAC del estándar 802.11 consiste de los siguientes campos: (Gast, 2005)

- Control de trama (*Frame Control*)
- Duración / Identificador (*Duration* / ID)
- Dirección 1 (*Address* 1)
- Dirección 2 (*Address* 2)
- Dirección 3 (*Address* 3)
- Control de Secuencia (*Sequence Control*)
- Dirección 4 (*Address* 4)
- Cuerpo de la trama (*Frame Body*)
- Secuencia de verificación de trama (*Frame Check Sequence* (FCS))

Todas las tramas 802.11 tienen los campos de control de trama, dirección 1 y FCS pero otros campos pueden estar presentes dependiendo del tipo/subtipo de la trama en sí. (Gast, 2005)

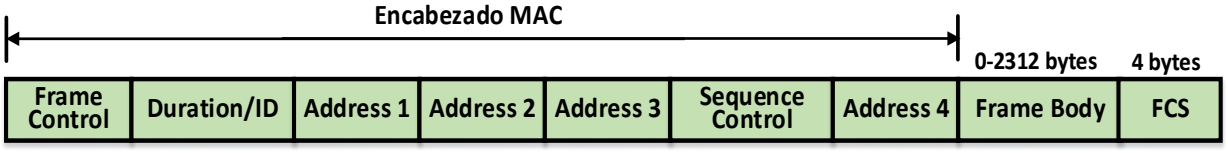

Ilustración 11: Encabezado de trama 802.11

Cada campo en el encabezado MAC 802.11 se encuentra dividido en distintos subcampos. La siguiente figura demuestra los campos y sus respectivos subcampos. (Gast, 2005)

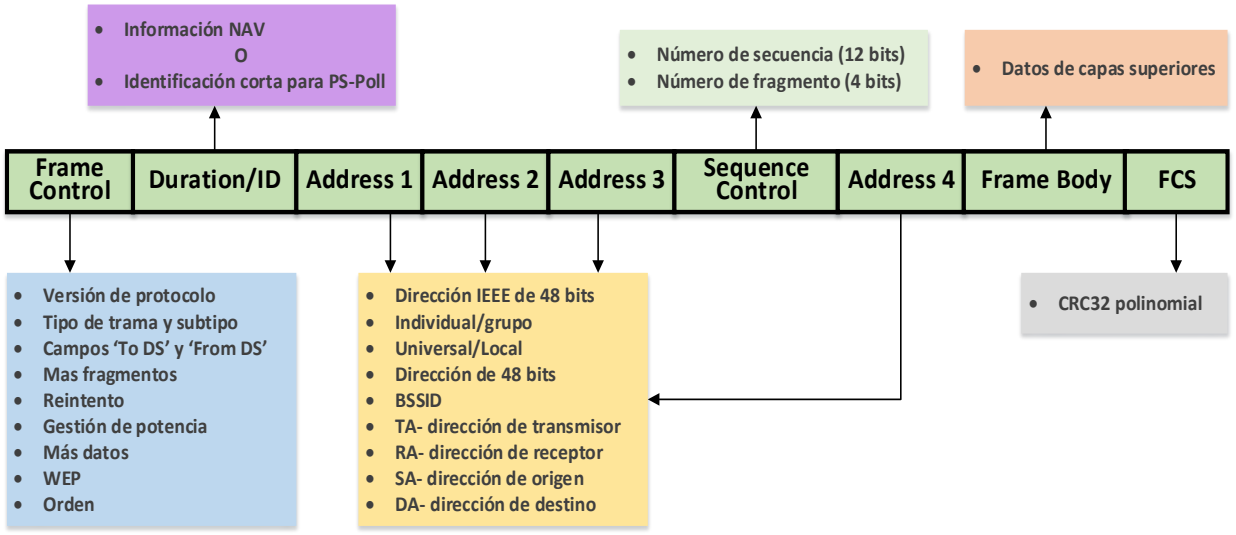

Ilustración 12: Campos y subcampos de una trama 802.11

Control de trama (*Frame Control* (FC)): Este campo tiene un tamaño de 2 bytes y contiene diferentes subcampos que todos juntos conforma los 16 bits. Los siguientes subcampos son: (Gast, 2005)

- Versión de Protocolo (*Protocol versión*). Su tamaño es de 2 bits y un valor por defecto de 0. El valor no cambia excepto si se da una revisión de incompatibilidad con otra versión previa.
- Tipo de trama (*Frame type*). Su tamaño es de 2 bits e indica el tipo de trama. Los tipos de trama de MAC 802.11 son gestión, control y dato (Management, Control and Data).
- Subtipo (*Subtype*). Su tamaño es de 4 bits y contiene los diferentes subtipos de tramas que han sido enviados en la red.
- Hacia un Sistema de distribución (*To DS (Distribution System*)). Su tamaño es de 1 bit y especifica si una trama está entrando en un sistema de distribución. Un ejemplo sería cuando un cliente inalámbrico envía una trama al punto de acceso con destino hacia internet.
- De un Sistema de Distribución (*From DS (Dsitribution System*)). Su tamaño es de 1 bit y especifica que una trama está saliendo de un sistema de distribución. Un ejemplo sería cuando un punto de acceso envía una trama hacia un cliente inalámbrico.
- Mas fragmentos (*More fragments*). Su tamaño es de 1 bit e indica si más fragmentos de una determinada trama necesitan ser enviados especialmente cuando una trama es demasiado grande para transitar en la red como una solo unidad. Este subcampo se aplica en tramas de tipo dato o gestión.
- *Retry* (Reintento). Su tamaño es de un 1 bit e indica si la trama es el paquete original o si es una trama retransmitida. El valor 0 indica un trama original y el

valor 1 indica una trama retransmitido. Este subcampo se aplica en tramas de tipo dato o gestión.

- Gestión de Potencia (*Power Management*). Su tamaño es de 1 bit e indica si la estación se encuentra en modo ahorro de energía o en modo activo.
- Más datos (*More data*). Su tamaño es de 1 bit e le indica a la estación (en modo ahorro de energía) que más datos están en camino y que se encuentran almacenadas en el buffer del punto de acceso.
- Trama protegida/WEP (*WEP/protected frame*). Su tamaño es de 1 bit e indica si el campo '*frame body*' está cifrada o no. Este subcampo se aplica en tramas de tipo dato o gestión.
- Orden (*Order*). Su tamaño es de 1 bit e indica el orden en que las tramas son recibidas y de acuerdo a dicho orden son procesadas.

Duración / Identificador (*Duration/ID*): Este campo está compuesto por 2 bytes y es utilizado para definir el vector de asignación de la red (*Network Allocation Vector* (NAV)). El NAV se refiere a la mínima cantidad de tiempo que una estación necesita esperar antes transmitir. También, este campo a veces se utiliza para definir un identificador en las tramas que gestionan el ahorro de energía en un punto de acceso.

Dirección1/2/3/4 (*Address* 1/2/3/4): Estos campos están compuestos por 6 bytes cada uno. La presencia de estos campos de dirección en una trama depende del tipo y sub-tipo de la trama. Estos campos consisten de los siguientes subcampos: (Gast, 2005)

- BSSID (*Basic Service Set Identifier*)- se refiere a la dirección MAC del punto de acceso
- Dirección del transmisor (*Transmitter Address*)- se refiere a la dirección MAC del dispositivo que transmite una trama.
- Dirección del receptor (*Receiver Address*)- se refiere a la dirección MAC del dispositivo que recibe una trama.
- Dirección de origen (*Source Address*)- se refiere a la dirección MAC del del transmisor de una trama.
- Dirección de destino (*Destination Address*)- se refiere a la dirección MAC de una estación que una trama tiene como destino.

Control de secuencia (*Sequence Control*): El tamaño de este campo es de 2 bytes y consiste de los siguientes subcampos: (Gast, 2005)

- Número de secuencia (*Sequence Number*)- indica el número de secuencia de la trama transmitida por una entidad inalámbrica.
- Número de fragmento (*Fragment Number*)- indica el número específico del fragmento en cuestión.

Cuerpo de trama (*Frame Body/Data*): El tamaño de este campo varía de 0 a 2312 bytes, dependiendo de la cantidad de información a transmitir. Este campo contiene los detalles de una trama de gestión o los datos reales y por ese motivo es vital en cualquier trama del estándar 802.11.

Secuencia de verificación de trama (*Frame Check Sequence* (FCS)): El tamaño de este campo es de 4 bytes e indica el '*checksum'*, a lo que se le conoce como una técnica de verificación de errores en una trama, llevado a cabo en todo el encabezado MAC y el cuerpo de trama utilizando un procedimiento llamado verificación de redundancia cíclica (*Cyclic Redundancy Check* (CRC)).

Por otro parte, las tramas son un conjunto de información enviados para establecer la comunicación entre los adaptadores de red inalámbricos (*radio network interface cards* (NIC)) y las estaciones inalámbricas. Todas las tramas contienen un campo de control (*control field*) que representa la versión del protocolo 802.11, tipo de trama y otros indicadores. Estos indicadores indican por ejemplo, si WEP está habilitado, si la gestión de potencia se encuentra activa etc. También, todas las tramas contienen direcciones MAC de origen, de destino y de los puntos de acceso, número de secuencia de trama, cuerpo de trama y secuencia de verificación de trama (FCS). Hay tres tipos de tramas MAC que son transmitidos en una red inalámbrica y cada uno se divide en distintos subtipos. Las tramas son esenciales para la búsqueda y resolución de problemas que se presentan en una red ya sea cableado o inalámbrica. Es fundamental aprender y entender los diferentes tipos de trama y sus respectivos sub-tipos. A continuación se tienen dos tablas los tipos de tramas y sus sub-tipos. (Gast, 2005)

Tipo de valor b3 b2	Tipo de trama	Valor de Sub-tipo b7 b6 b5 b4	Descripción de Subtipo
00	Gestión	0000	Solicitud de asociación
00	Gestión	0001	Respuesta de asociación
00	Gestión	0010	Solicitud de re-asociación
00	Gestión	0011	Respuesta de re-asociación
00	Gestión	0100	Solicitud de sondeo (*Probe request*)
00	Gestión	0101	Respuesta de sondeo (*Probe response*)
00	Gestión	0110-0111	Reservado
00	Gestión	1000	*Beacon*
00	Gestión	1001	ATM
00	Gestión	1010	Des-asociación
00	Gestión	1011	Autenticación
00	Gestión	1100	De-autenticación
00	Gestión	1101	Acción
00	Gestión	1110-1111	Reservado
01	Control	0000-0111	Reservado
01	Control	1000	Bloqueo de solicitud ACK (*BlockAckReq*)
01	Control	1001	Bloqueo ACK (*BlockAck*)
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF-End

01	Control	1111	CF-End + CF-Ack

Tabla 4: Tipos de tramas y sus combinaciones de subtipos

Tipo de valor b3 b2	Tipo de trama	Valor de Sub-tipo b7 b6 b5 b4	Descripción de Subtipo
10	Dato	0000	Datos
10	Dato	0001	Datos + CF-Ack
10	Dato	0010	Datos + CF-Poll
10	Dato	0011	Datos + CF-Ack + CF-Poll
10	Dato	0100	Null (nulo, sin datos)
10	Dato	0101	CF-Ack (sin datos)
10	Dato	0110	CF-Poll (sin datos)
10	Dato	0111	CF-Ack + CF-Poll (sin datos)
10	Dato	1000	Datos de Calidad de Servicio (QoS Data)
10	Dato	1001	QoS Data + CF-Ack
10	Dato	1010	QoS Data + CF-Poll
10	Dato	1011	QoS Data + CF-Ack + CF-Poll
10	Dato	1100	QoS Null (sin datos)
10	Dato	1101	Reservado
10	Dato	1110	QoS CF-Poll (sin datos)
10	Dato	1111	QoS CF-Ack + CF-Poll (sin datos)
10	Dato	0000-1111	Reservado

Tabla 5: Tipos de tramas y sus combinaciones de subtipos (Continuación)

Trama de Gestión (*Management Frame*)

Como su nombre lo implica, las tramas de gestión son tramas diseñadas y dedicas a la administración de los enlaces inalámbricos en una red inalámbrica. Este tipo de tramas son generados por las siguientes tareas: (Gast, 2005)

- Solicitud de asociación y des-asociación de cliente a punto de acceso
- Respuesta de prueba
- Tramas de de-autenticación generados por el punto de acceso

El encabezado MAC es la misma para todas las tramas de gestión y no depende de los subtipos de la trama. Este tipo de trama tiene un encabezado MAC estándar de 24 bytes con los siguientes campos: (Gast, 2005)

- *Frame control*
- *Duration/ID*
- *Destination Address*
- *Source Address*
- *BSSID*
- *Sequence Control*
- *Frame Check Sequence*

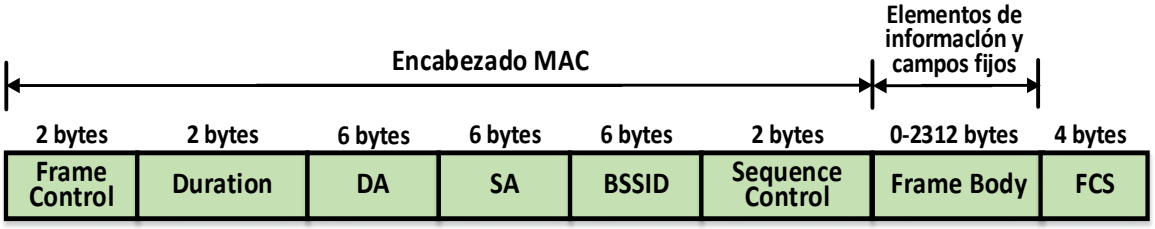

Ilustración 13: Encabezado de trama de Administración (Management) típico

La trama de gestión también se divide en los siguientes sub-tipos: (Gast, 2005)

Trama Beacon se refiere a tramas o mensajes transmitidos periódicamente por las estaciones inalámbricas con el objetivo te anunciar y difundir su presencia a clientes inalámbricos en un entorno inalámbrico. Los puntos de acceso son los responsables de transmitir las tramas 'beacon' en un tipo de configuración inalámbrica llamado una red inalámbrica de infraestructura bajo un área definida de servicio básico. Las estaciones pueden obtener una lista de puntos de acceso disponibles buscando tramas '*beacon'* continuamente en todos los canales establecidos para el estándar 802.11. Las tramas '*beacon'* contienen la información necesaria para identificar las características de la red y poderse conectar con el punto de acceso deseado.

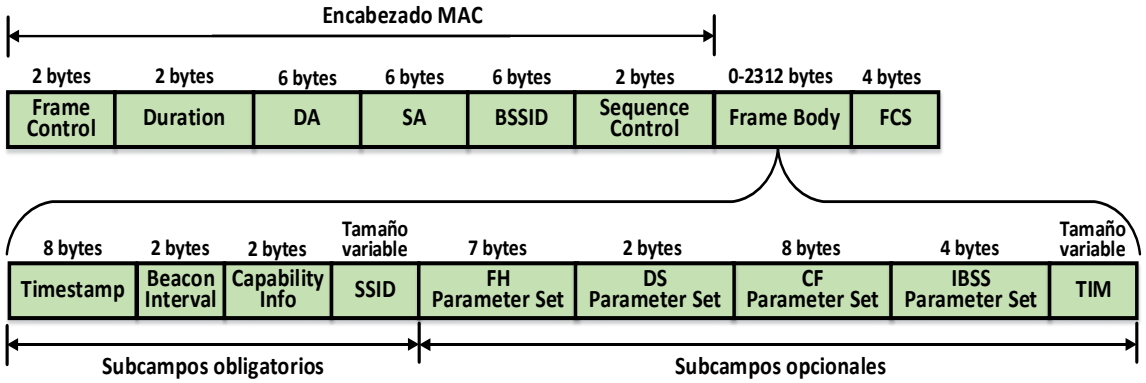

Ilustración 14: Encabezado de trama 'Beacon' típico

Trama de Solicitud de Prueba. Las estaciones utilizan tramas de solicitud de prueba cuando necesitan obtener información de otra estación, por ejemplo obtener una lista de puntos de acceso disponibles. Este tipo de trama es transmitida por clientes inalámbricos para escanear un área y determinar la existencia de una red 802.11 existente. El cliente inalámbrico debe de soportar la tasa de transmisión de datos requerido por la red antes de que se le permita conectarse a la red.

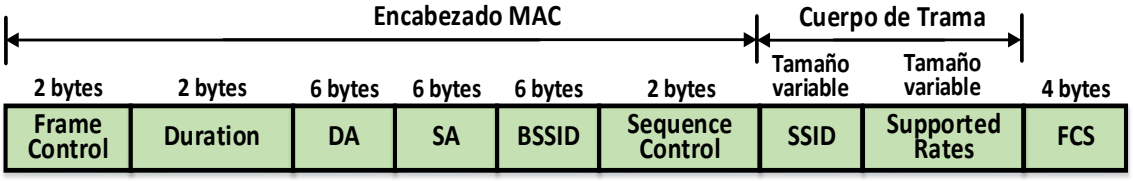

Ilustración 15: Encabezado de trama de solicitud de prueba

Trama de Respuesta de Prueba. Esta trama es la respuesta de una estación a una solicitud de prueba de un cliente. Esta trama contiene la información necesaria como por ejemplo las tasas de transmisión y otros requerimientos que el cliente debe cumplir antes de conectarse a la red.

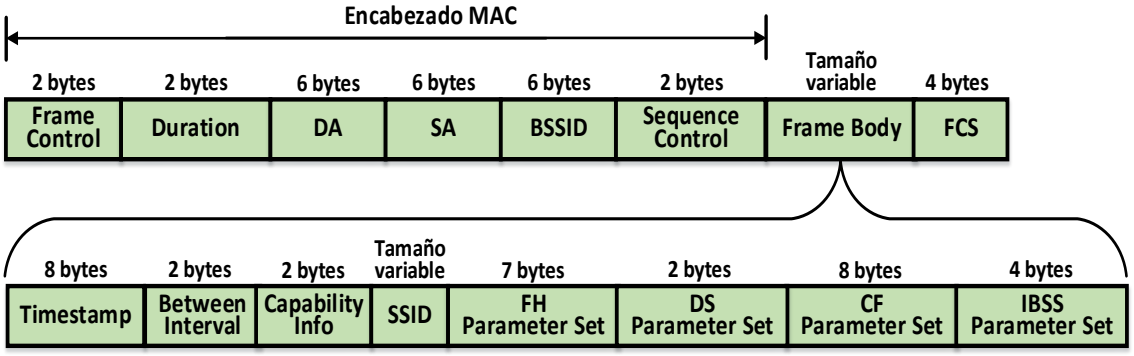

Ilustración 16: Encabezado de trama de respuesta de prueba

Trama de autenticación (*Authentication Frame*). Esta trama se transmite entre el punto de acceso y el cliente inalámbrico para la autenticación. La autenticación es el proceso para comprobar la identidad de un adaptador en la red para aceptarlo o rechazarlo. El adaptador cliente inicia el proceso enviando al punto de acceso una trama de autenticación que contiene su identidad en el campo de datos. El diálogo que se establece con las tramas de autenticación depende del sistema de autenticación que use el punto de acceso, sea abierto o con clave compartida. Cuando se trata de sistemas abiertos, el cliente sólo envía la trama de autenticación y el punto de acceso responde con otra trama de autenticación que indica si acepta o rechaza la conexión. Sin embargo, en el caso de la autenticación de clave compartida, el punto de acceso tiene que comprobar que la estación tiene la llave correcta por lo que se generan dos tramas de autenticación más en el diálogo, una que envía el punto de acceso con un texto para que lo cifre la estación con su clave y otra de respuesta por parte del cliente con el desafío cifrado.

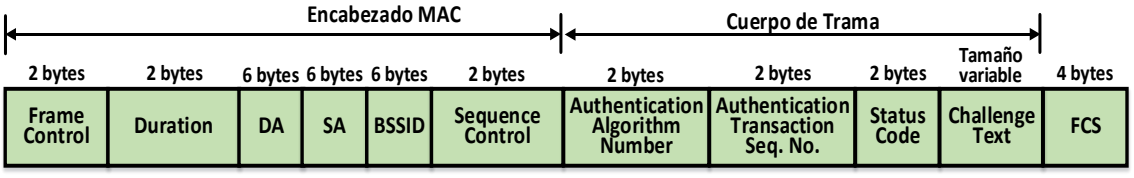

Ilustración 17: Encabezado de trama de autenticación

Trama de des-autenticación (*Deauthentication Frame*). Es una trama que envía ya sea una estación inalámbrica a un cliente o viceversa cuando una o ambas partes quiere terminar la comunicación. Además, esta tipo de trama incluye un campo fijo y sencillo llamado '*Reason Code*' en el cuerpo de trama.

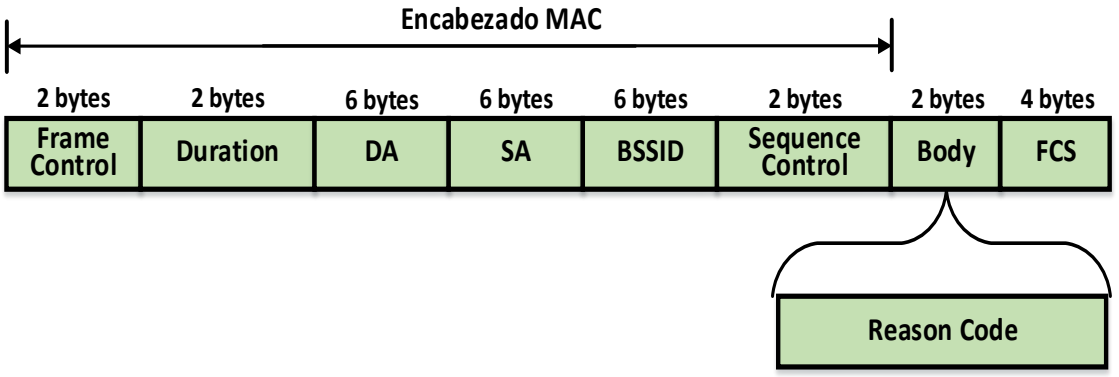

Ilustración 18: Encabezado de trama de des-autenticación

Trama de Solicitud de Asociación (*Association Request Frame*). La asociación es un proceso por el cual el punto de acceso reserva recursos y se sincroniza con una estación cliente. Por consiguiente, este tipo de trama la utiliza la estación cliente para iniciar el proceso de asociación con el punto de acceso. La asociación la inicia el cliente enviando una trama de solicitud de asociación al punto de acceso y el punto de acceso establece un ID de asociación para identificar al cliente y reservarle recursos como memoria. El proceso de asociación usualmente comienza después del proceso de autenticación.

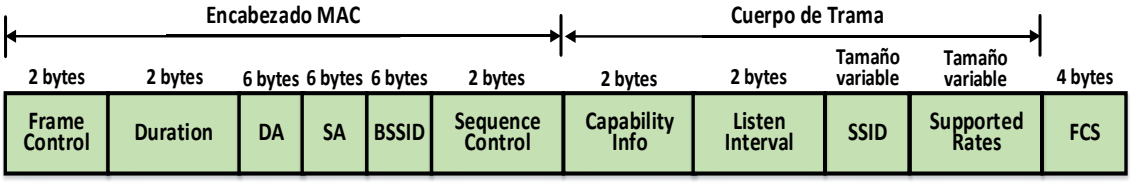

Ilustración 19: Encabezado de trama de solicitud de asociación

Trama de Respuesta de Asociación (*Association Response Frame*). Este tipo de trama la utilizan los puntos de acceso para responder a una solicitud de asociación de un determinado cliente. Esta trama le indica al cliente inalámbrico que licitud de asociación y también le indica si la acepta o la rechaza. Si se acepta la asociación, la trama también incluye el ID de asociación y las tasas de transferencia admitidas.

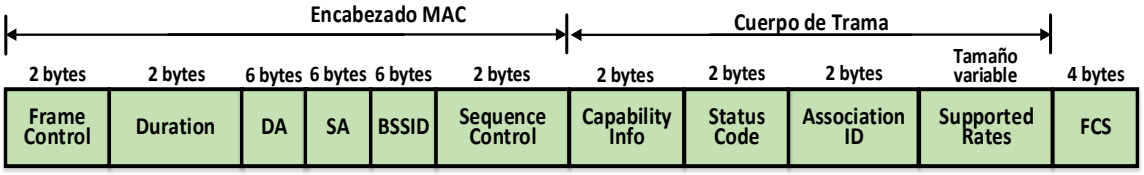

Ilustración 20: Encabezado de trama de respuesta de asociación

Trama de des-asociación (*Disassociation Frame*). Es una trama transmitida ya sea del cliente inalámbrico al punto de acceso o viceversa que indica la decisión de desasociarse de la red. Esta trama permite que el punto de acceso pueda liberar los recursos que se le asignaron al cliente durante el proceso de asociación. Además, esta tipo de trama incluye un campo fijo y sencillo llamado '*Reason Code*' en el cuerpo de trama.

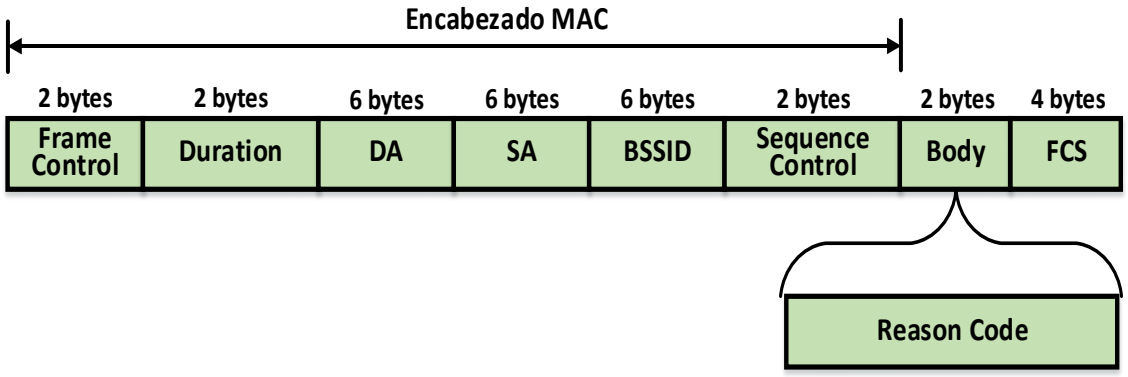

Ilustración 21: Encabezado de trama de desasociación

Trama de Solicitud de re-asociación (*Reassociation Request Frame*). Este tipo de trama es utilizado por el cliente inalámbrico y dirigido a las estaciones para que se pueda reconectar a la red inalámbrica que esta implementada como un sistema distribuido. Cuando un cliente asociado con un punto de acceso se desplaza al radio de cobertura de otro punto de acceso de la misma red con mejor señal o cuando temporalmente se sale del radio de cobertura del punto de acceso, intenta establecer una re-asociación.

La re-asociación implica que los puntos de acceso coordinen los búferes. Como era de suponerse, para establecer una re-asociación con un nuevo punto de acceso o el mismo, el cliente le envía una trama de re-asociación.

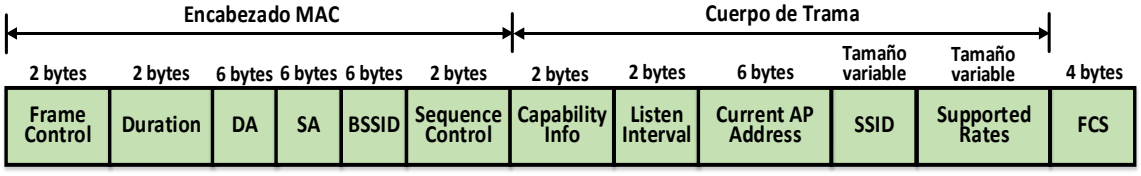

Ilustración 22: Encabezado de trama de solicitud de reasociación

Trama de Respuesta de re-asociación (*Reassociation Response Frame*). La trama de respuesta de re-asociación es similar a la trama de respuesta de asociación con la única diferencia de que este proceso se hace después de haberse dado un proceso de des-asociación.

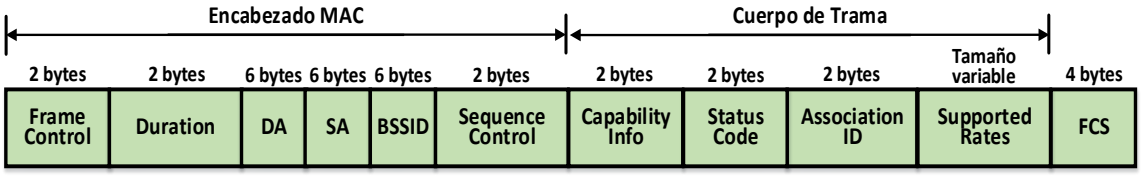

Ilustración 23: Encabezado de trama de respuesta de reasociación

Trama de Control (Control Frame). Las tramas de control se utilizan para colaborar en la entrega de tramas de datos entre estaciones en una red inalámbrica. Una típica trama de control tendrá los siguientes campos: control de trama, duración, dirección de receptor y FCS. También se encuentran otros campos dependiendo del tipo de control de trama en cuestión. A continuación una visión general de los tipos de control de trama y sus respectivos subcampos: (Gast, 2005)

Trama *Request to send* (*Request to send frame*). Este tipo de control de trama son tramas opcionales que se transmiten de un cliente inalámbrico a una estación inalámbrica para iniciar un dialogo de dos vías (*Two-way handshake*) que es necesario antes de transmitir tramas de datos. También, se utilizan para reducir las colisiones en el caso de dos estaciones asociadas a un mismo punto de acceso pero que se encuentran mutuamente fuera del rango de cobertura.

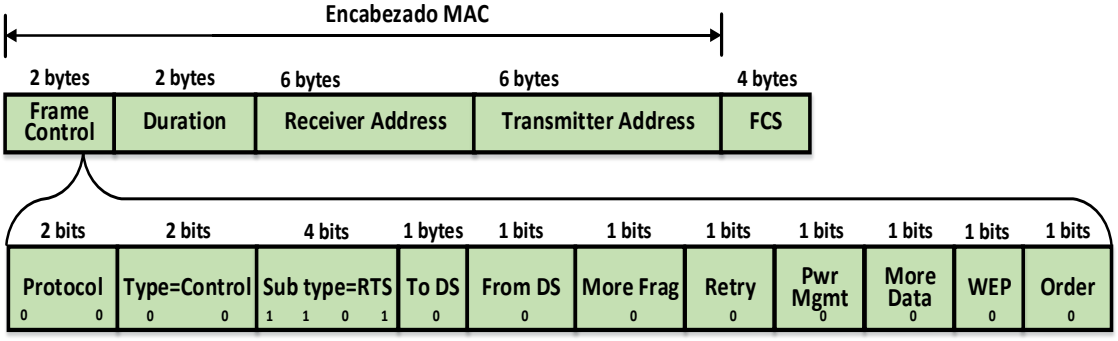

Ilustración 24: Encabezado de trama RTS

Trama Clear to send (*Clear to send frame*). La trama CTS es utilizada por las estaciones inalámbricas para responder a una trama RTS de un cliente inalámbrico y dejar el canal libre de transmisiones para que el cliente pueda transmitir tramas de datos. Las tramas CTS contienen un valor de tiempo durante el cual el resto de las estaciones dejan de transmitir hasta que transcurra el tiempo indicado.

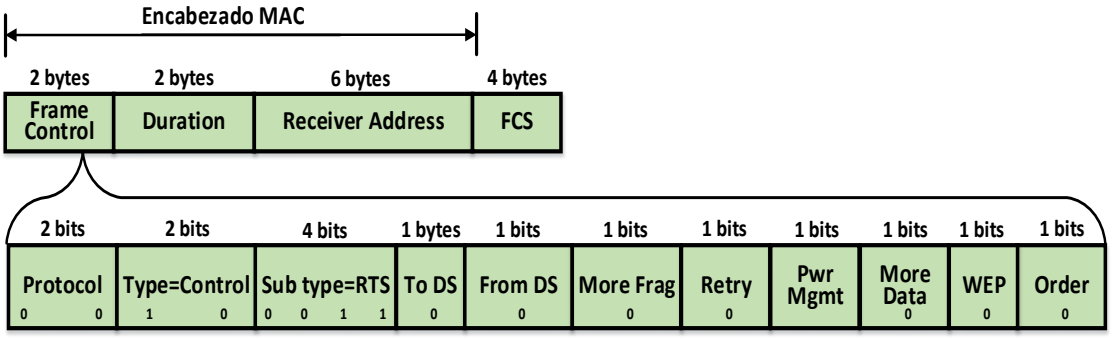

Ilustración 25: Encabezado de trama CTS

Trama *Acknowledgement* (*ACK frame*). Las tramas ACK tienen como objetivo confirmar la recepción de una trama. La estación receptora verifica las tramas para encontrar errores y si no las hay, envía una trama ACK. En caso de no llegar la trama ACK el emisor vuelve a enviar la trama de datos.

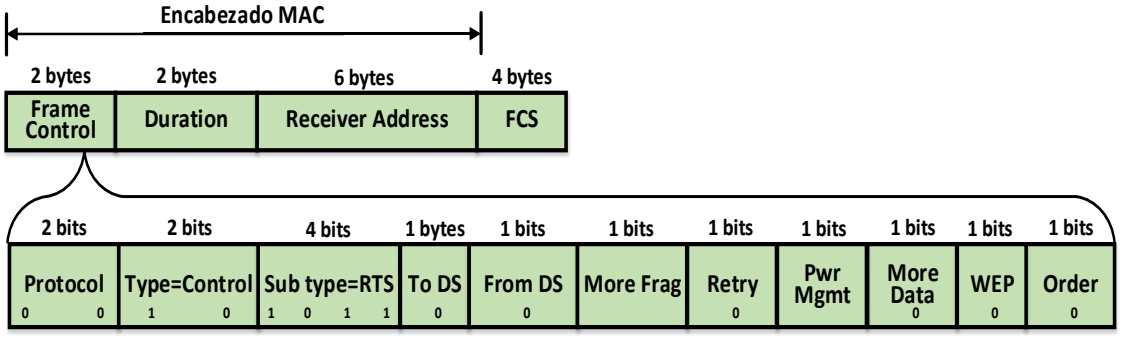

Ilustración 26: Encabezado de trama ACK

Trama de Datos (*Data Frame*). Este tipo de trama es la que se encarga de transportar la información de las capas superiores en una red inalámbrica. Estas tramas hacen referencia por ejemplo, a las solicitudes de los clientes inalámbricos vía la estación inalámbrica hacia internet. Una trama de datos típico tiene un encabezado MAC que consiste de los siguientes campos:

- *Frame control*
- *Duration*
- *Destination address*
- *BSSID*
- *Source Address*
- *Sequence control*
- *Frame Check Sequence*

Estos campos pueden llegar a estar presentes dependiendo del tipo de trama de dato siendo transmitido.

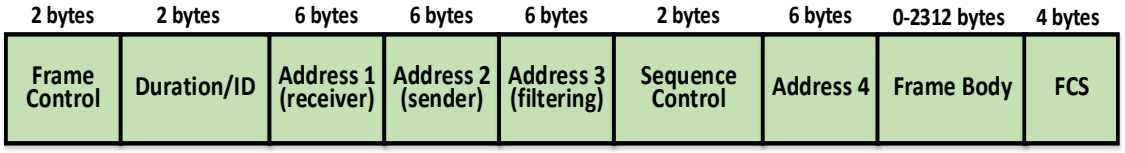

Ilustración 27: Encabezado de trama de datos genérico

El tipo de dato típico puede ser una trama de datos reales o una trama de datos nula. La trama de datos nula consiste de un encabezado MAC y el campo FCS. Este tipo de trama es transmitida por el cliente inalámbrico para informar al punto de acceso que se ha producido un cambio en el estado de ahorro de energía. Esto pasa cuando el cliente entra en modo inactivo (sleep) e indicarle al punto de acceso que inicie el almacenamiento en su buffer de las tramas destinados para el cliente.

2.7 Seguridad de Red Inalámbrica 802.11

La seguridad de la información es un aspecto fundamental e importante de las comunicaciones llevadas a cabo en sistemas informáticos. Por consiguiente, es necesario que la comunicación se realice de manera fiable y confidencial, ya que la inspección y/o alteración de la información transmitida por parte de terceras personas no autorizadas puede llegar a comprometer de manera severa la seguridad de información de las personas u organizaciones que hacen uso de las tecnologías de información. La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio en las redes inalámbricas ha producido beneficios pero también importantes riesgos de seguridad. El hecho de utilizar el aire como medio de transmisión hacen que las redes inalámbricas carezcan de barreras físicas y como consecuencia, cualquier persona con poco conocimiento de seguridad informática puede acceder a la red desde fuera de los límites físicos de una casa, empresa u organización. Esto hace que las redes inalámbricas sean susceptibles a múltiples tipos de ataques. (Martín, enero 2015)

Para que un sistema de seguridad en las redes de comunicaciones, particularmente en los entornos de red inalámbricos, esté completa y sea eficiente debe de proveer cinco pillares básicos de seguridad que son: (Martín, enero 2015)

- Confidencialidad: Consiste en garantizar la privacidad de la información y asegura que la información no pueda ser divulgada a dispositivos, procesos o personas no autorizadas.
- Integridad: Es un mecanismo de seguridad informática que garantiza que la información transmitida al usuario final no pueda ser alterada en su forma ni en su contenido en su trayecto desde el emisor hasta el receptor.

- Autenticación: Es un mecanismo de seguridad que establece la validez de una transmisión, mensaje o remitente, o un medio que verifique la autorización de un individuo para recibir información o acceder a información sensible (verificación de emisor). En otras palabras, la autenticación asegura que una entidad, quien dice ser, sea.
- Disponibilidad: Consiste en garantizar el acceso oportuno y confiable a datos y servicios de información para usuarios autorizados. La disponibilidad también hace referencia a la resistencia del sistema a ataques y su capacidad de recuperarse rápida y completamente después de estas.
- No repudio: Es una técnica que consiste en asegurar que el remitente de información es provisto de una prueba de envío y que el receptor es provisto de una prueba de la identidad del remitente, de manera que ninguna de las partes puede negar el proceso de dicha información.

La seguridad de las redes WiFi puede ser comprometida a través de dos de los pilares de seguridad informática que son autenticación y confidencialidad (cifrado). La autenticación se emplea para identificar un usuario inalámbrico ante un punto de acceso y viceversa. Por otra parte, los mecanismos implementados para garantizar la confidencialidad aseguran que no sea posible decodificar el tráfico de los usuarios. Por lo tanto, los protocolos de seguridad para redes 802.11, deben proteger estos dos puntos vulnerables ante posibles ataques. (Martín, enero 2015)

Fecha	**Hitos**
Septiembre 1997	Estándar IEEE 802.11 ratificado, incluyendo WEP.
Abril 2000	Lanzamiento del programa de certificación (WiFi CERTIFIED), con soporte para WEP.
Mayo 2001	Se crea el grupo de trabajo IEEE 802.11i
Abril 2003	Se introduce WPA con: ❖ Autenticación IEEE 802.11X ❖ Encriptación *Temporal Key Integrity Protocol* (TKIP) ❖ Compatible con *EAP-Transport Layer Security* (EAP-TLS)
Septiembre 2003	Obligatorio WPA para todos los equipos WiFi CERTIFIED
Junio 2004	Rectificación IEEE 802.11i ratificada
Septiembre 2004	Se introduce WPA2 con: ❖ Autenticación IEEE 802.11X ❖ Encriptación AES ❖ Compatible con EAP-TLS
Abril 2005	Apoyo a cuatro tipos EAP adicionales: ❖ *EAP Tunneled TLS Microsoft Challenge Handshake Authentication Protocol Version 2* (EAP-TTLS/MSCHAPv2) ❖ *Protected EAP Version 0* (PEAPv0)/EAP-MSCHAPv2 ❖ *Protected EAP Version 1* (PEAPv1)/EAP *Generic Token Card* (EAP-GTC) ❖ *EAP-Subscriber Identity Module* (EAP-SIM)
Marzo 2006	Obligatorio WPA2 para todos los equipos WiFi CERTIFIED

Enero 2007	Lanzamiento *WiFi Protected Setup (*WP S*)*
Noviembre 2007	Se crea el grupo de trabajo IEEE 802.11w
Mayo 2009	Apoyo para EAP-AKA y EAP-FAST añadido.

Tabla 6: Evolución de la seguridad del estándar IEEE 802.11

En la actualidad, existen otros mecanismos de seguridad del nivel de enlace que pueden ser utilizados en redes WiFi. Estos mecanismos son PPTP (*Point to Point Tunnelling Protocol*) y L2TP que es una extensión del protocolo PPTP. Sin embargo, estos mecanismos de seguridad no fueron desarrollados exclusivamente para las redes WiFi sino que también son aplicables en otro tipo de redes. El objetivo principal de estas tecnologías es la creación una Red Privada Virtual o mejor conocida como VPN (*Virtual Private Network*). Una VPN es una tecnología de red que se utiliza para realizar una extensión segura de la red LAN sobre una red pública o no controlada como Internet. Para realizar esta extensión segura, la tecnología VPN utiliza una técnica llamada *tunneling* donde los paquetes de datos son encaminados por la red pública, ya sea Internet o alguna otra red comercial, en un túnel privado que simula una conexión punto a punto. De allí el nombre de red privada virtual. Este mecanismo también permite la creación de muchos enlaces por medio de diferentes túneles virtuales utilizando la misma infraestructura. (Martín, enero 2015)

Se puede crear una VPN usando tecnologías de la capa 2 (enlace de datos) y de capa 3 (red) de acuerdo al modelo OSI. En la capa 2 se encuentran inmersos los protocolos PPTP y L2TP, y en la capa 2 se encuentra el protocolo IPsec. (Martín, enero 2015)

- El protocolo PPTP (*Point to Point Tunnelling Protocol*). Este protocolo es una extensión del protocolo base llamado *Point to Point protocol* (PPP) que fue desarrollado por Microsoft para permitir el tráfico seguro de datos desde un cliente a un servidor estableciendo una VPN basada en TCP/IP. Para asegurar la confidencialidad de la conexión, la información transmitida entre el emisor y receptor son cifrados por el protocolo PPP, un protocolo de acceso remoto, y posteriormente la información cifrada es enrutada sobre una conexión previa por un dispositivo PPTP. La principal ventaja de PPTP es que es fácil de implementar y no tiene un costo elevado.
- El protocolo L2TP (*Layer Two Tunneling Protocol*). Este protocolo también es una extensión del protocolo PPP que permite la creación VPNs a nivel de enlace de datos y no está basada en TCP/IP. La diferencia entre PPTP y L2TP es que L2TP reúne las mejores características de los protocolos PPTP de Microsoft y L2F de Cisco Systems y las combina en una sola tecnología.

PPTP y L2TP utiliza la funcionalidad de PPP para proveer acceso conmutado para luego ser tunelizado a través de Internet hacia un sitio destino. No obstante, el protocolo L2F integrado en L2TP no depende del protocolo IP (*Internet Protocol*) y por lo tanto es capaz de establecer túneles que trabajen directamente con otros medios, como *Frame Relay* o ATM. También, L2TP no depende de los mecanismos de cifrado específicos del fabricante para ofrecer una implementación completamente segura y correcta mientras que PPTP si depende de ellas. (Martín, enero 2015)

Es importante mencionar que un ataque realizado a nivel de capa 2 (enlace de datos) puede tener el control completo sobre todas las capas superiores si llegara a tener éxito. Por lo tanto, es sumamente importante estudiar y entender el funcionamiento de estas capas y poner énfasis en su seguridad. (Martín, enero 2015)

En la comunicación inalámbrica, los datos son transmitidos en un formato cifrado para evitar que terceras personas disimuladamente puedan escucharlas o leerlas mientras los datos viajan a través del medio de red. Una descripción de como los datos podrían ser manejados (el cifrado y el desciframiento) será necesaria. En los actuales sistemas informáticos, la información puede ser cifrada y descifrada a través de dos métodos criptográficos: (Martín, enero 2015)

- Clave Secreta que utiliza algoritmos simétricos.
- Clave Pública que utiliza algoritmos asimétricos.

2.7.1 Algoritmos de clave simétrica

Este tipo algoritmos están diseñados para cifrar un mensaje utilizando una única clave conocida por los participantes involucrados en la comunicación, de manera que la información cifrada sólo pueda descifrarse conociendo dicha clave secreta. Algunas de las características más destacadas de este tipo de algoritmos son las siguientes: (Ola, Otoño 2013)

- A partir del mensaje cifrado no se puede obtener el mensaje original ni la clave que se ha utilizado, aunque se conozcan todos los detalles del algoritmo criptográfico utilizado.
- Se utiliza la misma clave para cifrar el mensaje original que para descifrar el mensaje codificado.
- El emisor y receptor deben de acordar en usar una clave secreta por medio de un canal de comunicación confidencial antes de poder intercambiar información sensible.

El mensaje que será cifrado se le conoce como ‘texto plano’ mientras que el mensaje que será descifrado se le conoce como ‘texto cifrado’ o ‘texto codificado’. El método criptográfico de clave simétrica utiliza la técnica de cifrado por flujo (*stream cipher*) o cifrado por bloque (block cipher) para cifrar y descifrar los mensajes. Estas técnicas de cifrado sólo garantizan la privacidad pero no la integridad ni la autenticación sobre el mensaje. (Ola, Otoño 2013)

- Cifrado por flujo (*stream cipher*) cifra cada byte del mensaje uno por uno.
- Cifrado por bloques (*block cipher*) toma un número determinado de mensajes y los cifra como una unidad.

En la actualidad, los algoritmos simétricos más conocidos son: DES, 3DES, RC2, RC4, RC5, IDEA, Blowfish y AES.

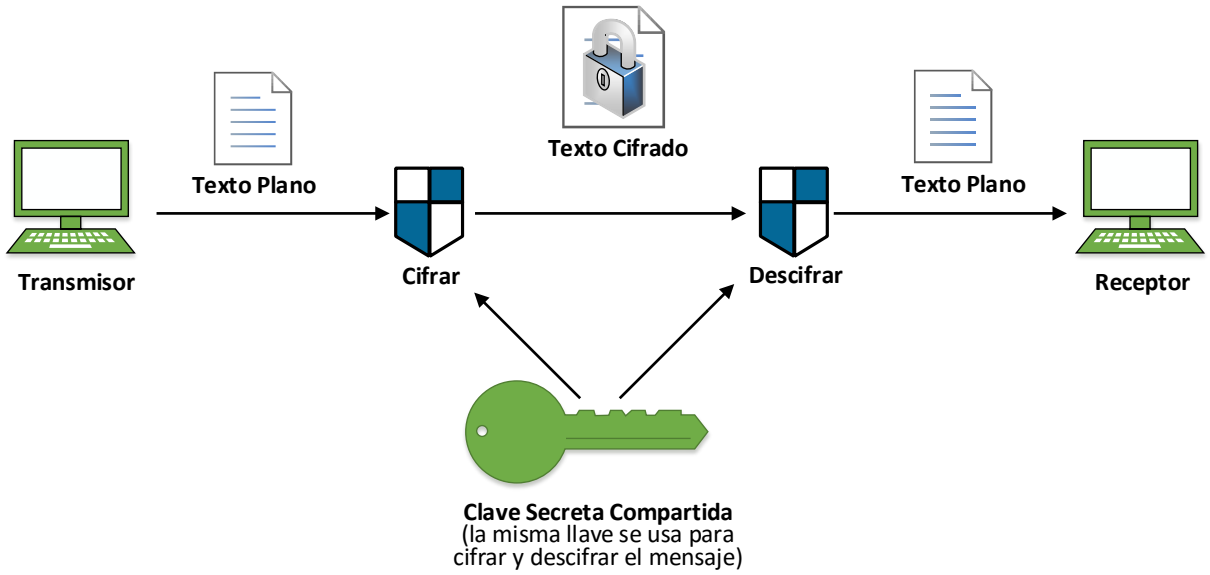

Ilustración 28: Algoritmo de clave simétrica

2.7.2 Algoritmos de Clave Pública (Asimétrica)

Estos son algoritmos criptográficos que utilizan dos claves distintas para cifrar y para descifrar el mensaje. Ambas claves tienen una relación matemática entre sí, pero la seguridad de esta técnica radica en que el conocimiento de una de las claves no permite descubrir cuál es la otra clave. Para este tipo de cifrado, cada usuario cuenta con una pareja de claves, una la mantiene en secreto (clave privada) y la clave pública que se puede distribuir libremente.

Para enviar un mensaje confidencial sólo hace falta conocer la clave pública del destinatario y cifrar el mensaje utilizando dicha clave con algún algoritmo asimétrico. Luego, el receptor usará su clave privada para descifrar el mensaje codificado y convertirlo otra vez en texto plano utilizando el mismo algoritmo. Los algoritmos asimétricos son los responsables de garantizar que el mensaje original sólo puede volver a recuperarse utilizando la clave privada del destinatario. Ya que la clave privada se mantiene en secreto, sólo el destinatario podrá descifrar el mensaje. Es importante mencionar que la clave pública se utiliza también para verificar un certificado digital mientras que la clave privada se utiliza para crear un certificado digital. (Ola, Otoño 2013)

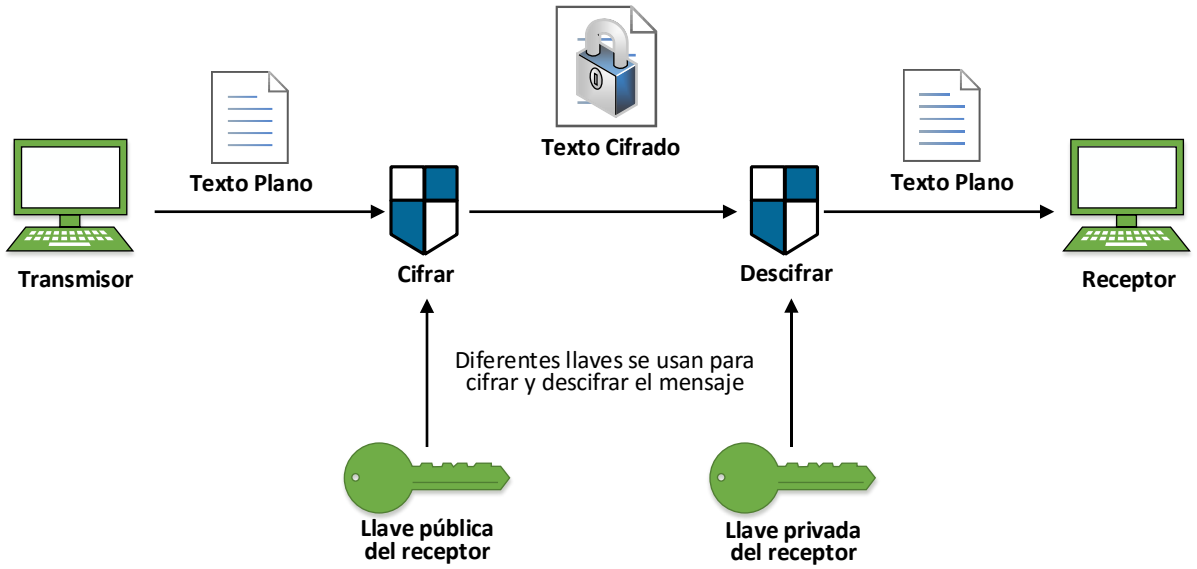

Ilustración 29: Algoritmo de clave pública

Algunas de las características de los algoritmos asimétricos son las siguientes: (Ola, Otoño 2013)

- Utilizan una pareja de claves denominadas clave pública y clave privada, y aunque las claves están relacionadas matemáticamente entre sí, en la práctica no es posible descubrir la clave privada a partir de la clave pública.
- Cuando se cifra un mensaje, no se puede obtener el mensaje original aunque se conozcan todos los detalles del algoritmo criptográfico utilizado y aunque se conozca la clave pública utilizada para cifrarlo.
- Emisor y receptor no requieren establecer ningún acuerdo sobre la clave a utilizar. El emisor se limita a obtener una copia de la clave pública del receptor a través de cualquier medio de comunicación, ya sea seguro o inseguro.

El algoritmo asimétrico ofrece una mayor confidencialidad que el algoritmo simétrico ya que los participantes de la comunicación no requieren llegar a un acuerdo sobre una clave secreta común para ser utilizado en el cifrado y la decodificación de la información. También, los algoritmos de clave pública proporcionan los tres pillares de la seguridad de información que son confidencialidad, integridad y autenticación. La única desventaja que tienen los algoritmos asimétricos es que no son lo suficientemente rápido como los algoritmos simétricos. (Ola, Otoño 2013)

La seguridad informática en la actualidad ha generado una preocupación cada vez mayor pero también ha despertado un gran interés a la hora de administrar los sistemas de comunicaciones informáticos. Debido a su cada vez más creciente popularidad, las redes inalámbricas 802.11 han sufrido un gran impacto en cuanto a la seguridad de información y esto es el foco principal de este trabajo de tesis. La implementación de mecanismos de seguridad en las redes inalámbricas ha sido una tarea incómoda, desde la invención del sistema inalámbrico. Esto se ha visto desde la aparición de diferentes parámetros de seguridad durante años, pero el sistema inalámbrico todavía

lucha con ciertas deficiencias y agujeros de seguridad que son difíciles de contra-arrestar. Muchas debilidades todavía existen en el sistema inalámbrico, y esto ha animado a hackers a realizar varias formas de ataques sobre una red inalámbrica. En la actualidad, es muy fácil tener acceso y comprometer una red Inalámbrica porque los atacantes no tienen que estar presentes sobre una red en particular para iniciar ataques. Los ataques pueden puede ser llevados a cabo a kilómetros de distancia usando un adaptador inalámbrico con antenas direccionales capaces de inyectar paquetes arbitrarios y husmear la red. Además, hoy en día existen herramientas informáticas sofisticadas que pueden ser utilizados por terceras personas con poco conocimiento de redes informáticas para lanzar ataques que comprometa la seguridad de la información en una red inalámbrica.

Los protocolos de seguridad que tienen la misión de proteger los dos puntos vulnerables (autenticación y cifrado) de las redes Wifi ante posibles ataques son WEP, WPA, WPA2.

2.7.3 *Wired Equivalency Protocol* (WEP)

WEP (Protocolo de equivalencia con red cableada) es un mecanismo de seguridad desarrollado junto en el estándar 802.11 en el año 1999 con el propósito de brindar la confidencialidad de información similar a la red cableada tradicional de Ethernet. WEP es el protocolo de cifrado incluido en el estándar 802.11 que permite cifrar la información que se transmite entre los usuarios y el punto de acceso utilizando el algoritmo de cifrado RC4. El algoritmo RC4 fue creado por Ron Rivest en el año 1987 y tiene como misión generar claves de cifrado arbitrarias empleando la función lógica XOR. La longitud de RC4 puede ser de 64 bits, donde la clave consiste de 40 bits sumado con un vector de inicialización (IV) de 24 bits, de 128 bits (104 bits para la clave con un vector de inicialización de 24 bits) o de 256 bits (232 bits para la clave con un vector de inicialización de 24 bits). El vector de inicialización es una técnica que hace que la clave varíe con el propósito de impedir que un posible atacante recopile suficiente información cifrada con una misma clave. También, el algoritmo RC4 utiliza un '*checksum'* (verificador de secuencia de paquetes) basado en CRC32 para prevenir que se inyecten tramas en el flujo de datos. (Martín, enero 2015)

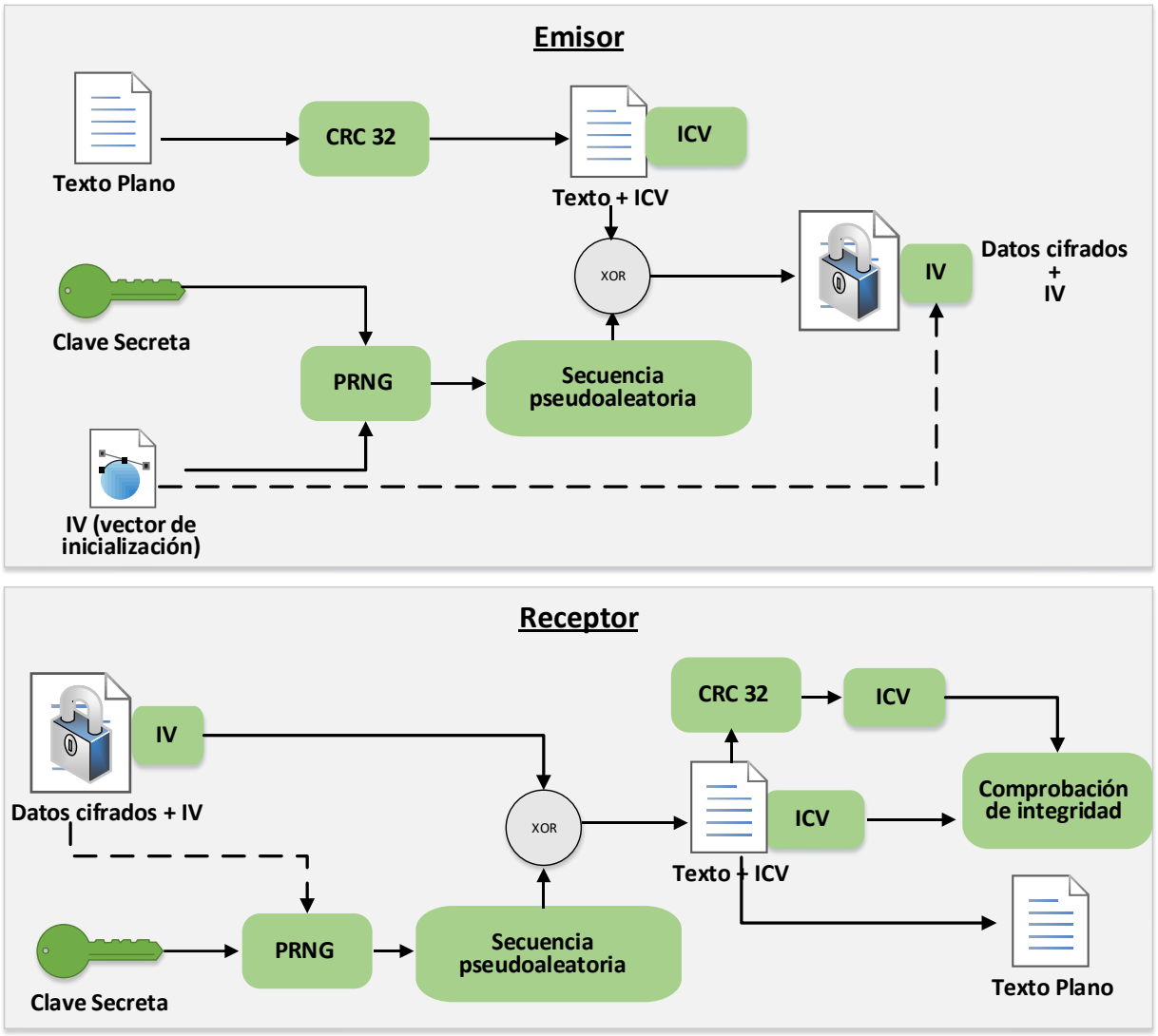

Ilustración 30: Proceso de cifrado y descifrado WEP

Proceso de cifrado RC4 en WEP: (Martín, enero 2015)

1. Se calcula el CRC32 del '*payload*' (información útil) de la trama que se quiere enviar.
2. Se añade a la trama como Valor de Chequeo de Integridad (ICV)
3. Se escoge una clave secreta. A la trama se concatena la clave secreta con un número aleatorio llamado Vector de inicialización (IV) de 24 bits al principio de la clave seleccionada.
4. A este conjunto se le conoce como *Keystream*. La clave será común para todos los paquetes cifrados y el vector de inicialización variará con cada paquete. Se utiliza el *Keystream* para cifrar la trama.
5. El cifrado se lleva a cabo mediante la utilización de la función XOR.

6. El resultado obtenido de este cifrado junto con el vector de inicialización usado durante el proceso y sin cifrar, conforman la trama cifrada que se enviará a través del medio.

Proceso de descifrado RC4 en WEP: (Martín, enero 2015)

1. Se utiliza el vector de inicialización y la llave para descifrar el *payload* e ICV.
2. Se vuelve a calcular el ICV y se compara con el original. Si no coincide indica que el texto ha sido modificado por el camino.

Este proceso de cifrado y descifrado tiene lugar para todo el tráfico intercambiado entre el punto de acceso y el cliente inalámbrico (dispositivo del usuario) en una red WLAN. Este proceso de cifrado y descifrado se compone de los siguientes pasos. (Martín, enero 2015)

1. El cliente envía una petición de autenticación al AP.
2. El AP genera un texto plano de 128 bytes aleatorio que envía al cliente con el fin de que 'resuelva el reto', esperando que el cliente cifre dicho texto utilizando la clave WEP.
3. El cliente recibe el 'reto' del AP y utiliza el algoritmo RC4, los IVs y la clave WEP para generar el texto cifrado que enviará posteriormente al AP.
4. El AP recibe el texto cifrado y posteriormente intenta descifrarlo con la clave WEP verificando que corresponde con el enviado anteriormente

En el caso que el proceso anterior se ejecute correctamente, el usuario se autenticará con el AP y en caso contrario un error se producirá y no será posible realizar la autenticación y posterior asociación. El cifrado basado en WEP no es fiable ni seguro dado que existen bastantes técnicas que se han empleado con éxito para romper las claves cifradas con RC4. WEP presenta las siguientes debilidades como las que se muestran a continuación: (Martín, enero 2015)

- Al tener una clave compartida, cualquier usuario o atacante que posea la clave es capaz de comprometer la integridad de los datos transmitidos.
- El vector de inicialización de WEP es enviado en texto plano sin ningún tipo de cifrado. Cuando se tiene una red con muchos usuarios, debido a la corta longitud del IV éste se repite cada cierto tiempo. Al capturar varios paquetes que contienen el mismo IV, un atacante puede descubrir la contraseña que le permita dar con la clave WEP y lograr el acceso a la red.
- Actualmente, existen muchas herramientas de penetración de red que son capaces de romper las claves cifradas en unos cuantos minutos.

Cabe mencionar que en la actualidad el protocolo WEP ha quedado obsoleto en materia de seguridad aunque todavía se sigue utilizando en hogares, empresas y organizaciones. Para neutralizar las deficiencias y debilidades de WEP, se desarrollaron mecanismos de seguridad como WPA y WPA2 que utilizan una tecnología de cifrado fuerte.

2.7.4 *WiFI Protected Access* (WPA)

WPA son las siglas de '*Wifi Protected Access'* y fue diseñada en 2003 por la alianza WiFI como reemplazo mucho más óptimo y confiable que cualquier implementación de WEP. WPA es un mecanismo de seguridad creado para corregir las deficiencias de WEP, incorporando un método de autenticación y mejoras significantes en cuanto al cifrado de información. WPA no ha sido diseñado para ser una solución a largo plazo, de hecho, se trata de una solución intermedia para realizar la transición entre WEP y WPA. Solamente WPA2 es una solución que se ha diseñado para cumplir completamente con el estándar 802.11i y se encuentra soportada por los dispositivos inalámbricos más recientes. Por este motivo, se decidió desarrollar dos soluciones. Una rápida y temporal que se denominó WPA y otra a largo plazo que se denominó WPA2. (Montoya, 2014)

WPA es una tecnología que opera a nivel MAC y está basado en el estándar IEEE 802.11i como una implementación casi completa ya que WPA tiene algunas carencias que WPA2, basado completamente en el estándar IEEE 802.11i, no tiene. WPA contrarresta las debilidades conocidas de WEP introduciendo una extensión del vector de inicialización que pasa de ser de 24 a 48 bits, minimizando así la reutilización de claves. También, WPA integra mecanismos nuevos de derivación y distribución de claves y un nuevo protocolo conocido como '*Temporal Key Integrity Protocol*' (TKIP) para la generación de claves por paquete. Este protocolo utiliza el algoritmo de cifrado RC4, al igual que WEP, pero elimina el problema de las claves estáticas compartidas. TKIP es el responsable de cambiar dicha clave cada cierto tiempo, ampliando la longitud de la clave de 40 a 128 bits. Como consecuencia, la clave pasa de ser única y estática a ser generada de forma dinámica para cada usuario y para cada paquete. TKIP cifra el vector de inicialización (IV), que suponía un problema de privacidad en WEP ya que el IV se enviaba por el aire en texto plano, para mitigar ataques que permitan revelar la clave. (Montoya, 2014)

Además, se incluye el Control de la Integridad del Mensaje (*Message Integrity Check, MIC*). Este procedimiento MIC, reemplaza el *Checksum* CRC32 utilizado en WEP y se encarga de verificar la integridad de los datos en las tramas. Esto previene que intrusos capturen paquetes, los alteren y los reenvíen en la red. MIC, que también lleva por sobrenombre Michael, provee una función matemática de alta fortaleza en la cual el transmisor y el receptor deben calcular y comparar si los datos coinciden o no. En caso de que no coincida, los datos se consideran corruptos y se descarta el paquete. De este modo, TKIP impide que un atacante pueda alterar los datos que se transmiten dentro de un paquete. (Montoya, 2014)

WPA y WPA2 tienen dos tipos distintos de ediciones, las cuales son '*Personal'* y '*Enterprise'*, que son simplemente para el uso personal en redes domésticas y para el uso empresarial en redes con un número de clientes mayor. En cuanto a la autenticación, el mecanismo usado emplea 802.X y EAP y en función del entorno de aplicación, en WPA es posible operar en las dos modalidades o ediciones previamente mencionadas que son: (Montoya, 2014)

- Modalidad o Edición Personal que utiliza WPA-PSK (Pre-Shared Key):

Para esta modalidad, se requiere introducir una contraseña compartida en el punto de acceso o modem ADSL, así como en cada uno de los dispositivos que desean conectarse a la red WiFi. Solamente podrán acceder al punto de acceso los dispositivos cuya contraseña coincida con la del punto de acceso. Esto evita ataques basados en husmeo de la red así como acceso de usuarios no autorizados. La contraseña provee una relación para establecer un acuerdo único entre el AP y el cliente inalámbrico y así poder generar el cifrado TKIP en la red. Por lo tanto, aunque la contraseña inicial es compartida por todos los dispositivos de la red, las claves de cifrado son diferentes para cada dispositivo. Cabe mencionar que en estos entornos no es posible contar con un servidor de autenticación centralizado o un marco EAP. (Montoya, 2014)

- Modalidad o Edición Empresarial

En este entorno WPA utiliza el estándar IEEE 802.11x y EAP para emplear un mecanismo de autenticación. EAP se utiliza como transporte extremo a extremo para los métodos de autenticación entre el cliente inalámbrico y los puntos de acceso. Mientras que el protocolo IEEE 802.1x se emplea para encapsular los mensajes EAP. La combinación de estos dos mecanismos junto con el esquema de cifrado forma una fuerte estructura de autenticación que utiliza un servidor de autenticación centralizado, como por ejemplo, un servidor RADIUS. (Montoya, 2014)

2.7.5 WPA2

WPA2 fue lazada en septiembre de 2004 por la WiFi Alliance y es la versión certificada que cumple completamente con el estándar 802.11i ratificado en junio de 2004. La seguridad es mucho más robusta que la que ofrece WPA ya que WPA2 refuerza el algoritmo de cifrado utilizando como protocolos de cifrado CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) basado en el algoritmo de cifrado AES (*Advanced Encryptation Standard*) de 128 bits. El componente que negocia dinámicamente los algoritmos de autentificación y de cifrado que se utilizarán para las comunicaciones entre los puntos de acceso y los usuarios inalámbricos es llama '*Robust Security Network*' (RSN). RSN utiliza AES, junto con IEEE 802.1x y EAP y el responsable de construir, sobre AES, el protocolo CCMP. Por consiguiente, WPA2 ofrece un mecanismo de autenticación de usuarios avanzado que superado por mucho a los estándares de seguridad como WEP y WPA. No obstante, tiene la gran desventaja de no ser compatible con versiones anteriores de software. (Montoya, 2014)

Además, WPA2 incluye soporte no sólo para el modo infraestructura BSS sino también para redes ad-hoc y permite la de-autenticación y des-asociación segura de la red, algo que no se puede encontrar en el estándar WPA. (Montoya, 2014)

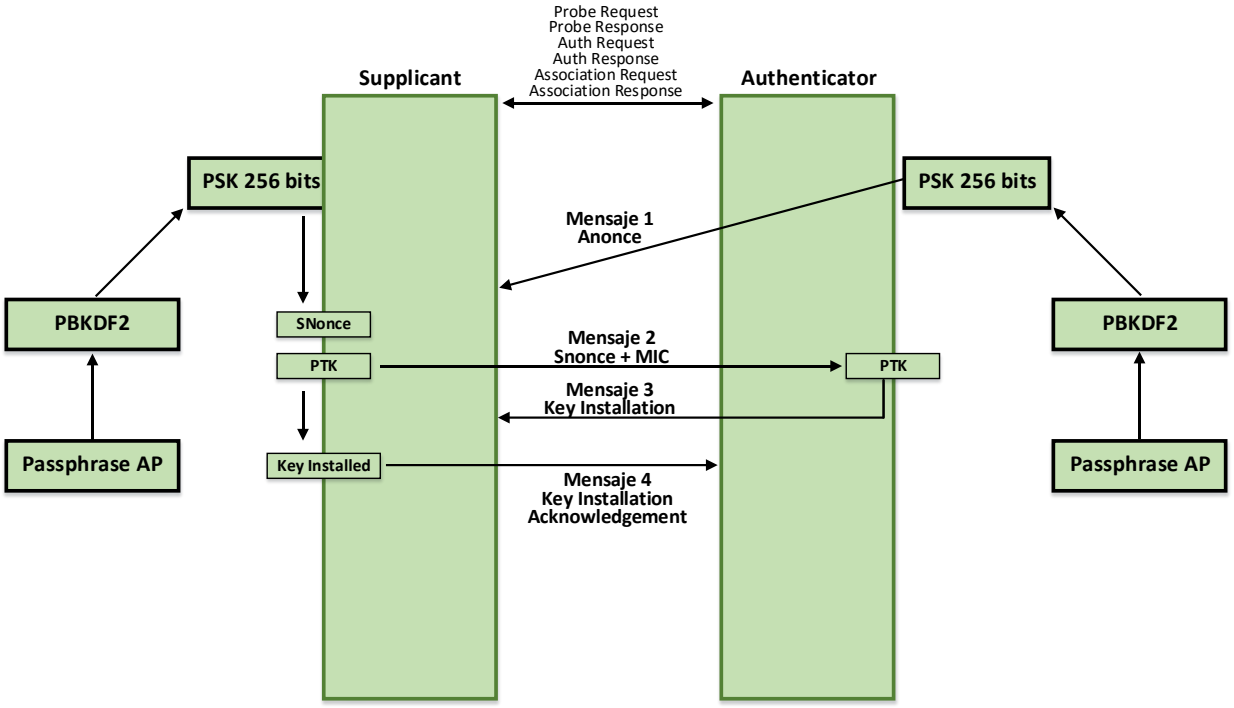

Ilustración 31: Proceso de autenticación WPA/WPA2

El proceso conocido como '*Four-Way Handshake'* se resume con los siguientes pasos: (Montoya, 2014)

1. El '*Authenticator*' envía un mensaje al '*supplicant'* con un valor generado aleatoriamente utilizando su clave PSK. Se trata simplemente de un valor arbitrario sin ningún tipo de significado especial, este mensaje es conocido como un '*Authenticated nonce*' o simplemente '*Anonce'* dado que contiene un campo llamado '*nonce'* cuyo valor es el texto generado aleatoriamente con la clave PSK del '*Authenticator'*.
2. Posteriormente, el '*Supplicant'* recibe dicho mensaje y genera otra llamada '*Snonce'* ('*Supplicant nonce'*) que es básicamente del mismo tipo que el '*Anonce'* enviado por el '*Authenticator'*, solamente que contiene un nonce distinto
3. Con la información suministrada, el 'Supplicant' procede a crear un par de claves llamadas '*Pairwise Transient* Key' (PSK). Este paso es sumamente importante y es justo donde el lector debe prestar mayor atención, principalmente porque es aquí donde está la magia de PSK y la generación dinámica de claves. Las PTK son las claves generadas en cada paquete intercambiado entre el '*Supplicant'* y el '*Authenticator'* y se generan utilizando la '*Pairwise Master Key'* (PMK) que es de la misma clave PSK generada en el paso uno. Cada PTK es dinámicamente generada con las PSK del '*Supplicant'* y el '*Authenticator'*.

4. La PTK es generada por la PMK utilizando para ello una función de generación aleatoria de claves PTK que recibe una lista con los siguientes parámetros que pasan a ser descritos a continuación:
    - PMK- La PSK generada por ambas entidades (*Supplicant* y *Authenticator*) utilizando el algoritmo PBKDF2.
    - *Anonce*- Generado por el '*Authenticator'* que contiene un texto aleatorio cifrado con su clave PSK.
    - *Snonce*- Generado por el '*Supplicant'* que contiene un texto aleatorio cifrado con su clave PSK.
    - MAC del '*Authenticator'*
    - MAC del '*Supplicant'*
5. El '*Supplicant'* procede a enviar un paquete al '*Authenticator'* con el mensaje '*Snonce'* y un campo MIC; valor cifrado utilizando el mecanismo de cifrado 'Michael' que permite realizar el chequeo de integridad y consistencia del paquete. Este campo es generado por el '*Supplicant'* utilizando la PTK y la PMK.
6. Con el paquete enviado anteriormente por el '*Supplicant'*, el '*Authenticator'* ahora procede a derivar la clave PTK dado que ahora conoce los campos necesarios para hacer el cálculo: PMK (que se la misma para el '*Supplicant'* y el '*Authenticator'*), *Anonce*, *Snonce* y las direcciones MAC del '*Authenticator'* y el '*Supplicant'*.
7. Una vez el '*Authenticator'* ha podido generar el PTK con los campos recibidos del paquete anterior, intentará generar el campo MIC, dado que cuenta con la misma PTK y PSK que el '*Supplicant'*, el MIC generado por el '*Authenticator'* y el '*Supplicant'* deben de ser el mismo. En tal caso, envía un mensaje al '*Supplicant'* del tipo '*Key Installation'*. Este mensaje puede verse con la bandera ('flag') del tipo '*Install Flag'* la cual puede apreciarse en el tercer paquete intercambiado en el proceso de autenticación. En el caso que el chequeo del MIC falle debido a que el valor calculado por el '*Authenticator'* no corresponda con el valor enviado por el '*Supplicant'*, el '*Authenticator'* inmediatamente finaliza el proceso enviando un paquete '*DeAuthentication'*.
8. Finalmente el '*Supplicant'* envía un mensaje de '*Key Install Acknowledgement'* el cual es simplemente una confirmación que se envía al '*authenticator'* para que en esta sesión de intercambio de paquetes, se utilice la misma PTK generada en el cliente y el AP. Este paquete simplemente contiene un campo 'Key ACK' con un valor de 0 indicando que es el último mensaje enviado en el proceso de autenticación entre el '*Supplicant'* y el '*Authenticator'*.

WPA	WPA2
Solución intermedia que sirve de transición entre WEP y WPA	Solución definitiva (a largo plazo) que soporta completamente el estándar IEEE 802.11i.

No requiere ningún cambio en el hardware utilizado, ya que 'hereda' directamente de WEP. Esto quiere decir, que si un dispositivo ha utilizado WEP anteriormente, éste soportará WPA. Solamente será requerida la actualización del firmware correspondiente	Requiere un cambio en el dispositivo utilizado para que soporte WPA2 y las características del estándar IEEE 802.11i. Esto quiere decir que si un dispositivo ha utilizado WEP posiblemente no soportará WPA2 y es necesario utilizar una tarjeta de red más moderna.
Usa TKIP que se encuentra basado en WEP, pero implementa algunas características de seguridad adicionales que le hacen bastante difícil de craquear.	Usa CCMP el cual se encuentra basado en AES. Es bastante más seguro que cualquiera de las implementaciones basadas en WEP existentes.

Tabla 7: Comparación de WPA y WPA2

2.7.6 Autenticación y Gestión de Claves WPA y WPA2

IEEE 802.1X es un estándar para el control de acceso a red de capa 2 que complementa a la autenticación y la distribución de claves. El estándar traduce las tramas transmitidas por un algoritmo de autenticación en el formato necesario para que el sistema de autenticación que se encuentre implementado en la red pueda entenderlas. Por lo tanto, el estándar IEEE 802.1x debe emplearse de forma conjunta con protocolos de autenticación para llevar a cabo la verificación de las credenciales de usuario y la generación de las claves de cifrado aunque no es por sí mismo un método de autenticación. La IEEE 802.1x involucra la existencia de tres actores como lo son: (Montoya, 2014)

1. Solicitante: se refiere a un usuario inalámbrico que desea acceder a la red.
2. Autenticador: generalmente es un punto de acceso que recibe la conexión del solicitante y su función es forzar el proceso de autenticación y encaminar el tráfico hacia los diferentes usuarios y entidades de la red.
3. Servidor de autenticación: es un servidor que verifica las credenciales del solicitante. Generalmente se suele emplear como servidor de autenticación remota de servicios de usuario o mejor conocido como RADIUS (*Remote Authentication Dial In User Service*).

Los tres actores anteriores a través de EAP e IEEE802.1x trabajan de la siguiente manera: (Montoya, 2014)

1. Cuando el equipo del usuario quiere acceder a la red, este le envía una solicitud al punto de acceso que implementa EAP.
2. EAP a través el punto de acceso le envía una respuesta al usuario para que envíe sus credenciales de identificación.
3. El usuario le envía sus credenciales de identificación.
4. EAP a través del punto de acceso envía las credenciales de identificación del usuario ya traducidas con el protocolo 802.1x al servidor para que el servidor pueda entender la información.

5. El servidor comprueba el derecho de acceso del usuario y luego le envía un mensaje de respuesta al cliente a través del punto de acceso.
6. Si no hubo ningún problema con la autenticación, EAP a través del punto de acceso permite el acceso a la red al usuario de acuerdo con el mensaje de autorización del servidor.

La autenticación del cliente se lleva a cabo mediante el protocolo EAP y generalmente un servidor RADIUS.

EAP es un protocolo de autenticación para verificar la identidad de un cliente inalámbrico. Un punto de acceso que implementa la tecnología 802.1x sólo se comunica con los usuarios autentificados y antes de su autenticación sólo admite las comunicaciones con el protocolo EAP (*Extensible Authentication Protocol*). Específicamente hablando, EAP lleva a cabo tareas de AAA (*Authentication, Authorization, Accounting*) y fue diseñado originalmente como una extensión del protocolo PPP. El protocolo EAP tiene diferentes versiones y las más comunes son:

- EAP-MD5 (*Message Digest 5*)

  Para la autenticación utiliza un nombre de usuario y una contraseña que irá cifrada mediante el algoritmo MD5, mientras que el nombre de usuario se envía en texto plano. Este protocolo no utiliza ningún mecanismo de seguridad para autenticar el servidor y brinda un nivel de seguridad muy bajo por lo que no es recomendable utilizarlo como protocolo en redes inalámbricas.

- EAP-LEAP (*Lightweight EAP*)

  Es un protocolo propietario de Cisco en el que se utilizan las contraseñas como método de autenticación del servidor. Las credenciales de usuario se envían en texto plano. LEAP no soporta la utilización de *One Time Password* (OTP) y requiere de infraestructura CISCO para poder ser utilizado. Esta autenticación tiene la capacidad de prevenir ataques *Man-in- The-middle* y de secuestro de la sesión, aunque presenta el riesgo de exposición de la identidad y de ataques diccionario.

- EAP-TLS (*Transport Layer Security*)

  Este protocolo ofrece una autenticación mutua entre el cliente y el servidor y está considerado como una de las versiones más seguras de EAP. EAP-TLS utiliza certificados digitales para garantizar la identidad del cliente y del servidor lo que obliga a disponer de una infraestructura de clave pública para gestionar estos certificados.

- EAP-TTLS (*Tunnelled TLS*)

Es un protocolo que ofrece un mecanismo de autenticación fuerte mutua y sólo requiere certificados en el servidor ya que está orientado a trabajar con servidores RADIUS. Está integrado con una gran variedad de formatos de almacenamiento de contraseñas y sistemas de autenticación basados en contraseñas así como con múltiples bases de datos de seguridad. Una ventaja de EAP-TTLS es que elimina la necesidad de configurar certificados para cada usuario de la red inalámbrica. Su funcionamiento es la siguiente: primero se autentica al usuario en el sistema con las credenciales basadas en nombre de usuario y contraseñas. Luego, TTLS cifra las credenciales de usuario para garantizar la protección de la comunicación inalámbrica.

- PEAP (Protected EAP)

Es un protocolo desarrollado por Microsoft, Cisco y RSA Security, similar a EAP-TTLS, en el sentido de que solamente requiere certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP mediante el establecimiento de un túnel seguro TLS entre cliente y el autenticador.

- EAP-FAST (*Flexible Authentication via Secure Tunnelling*)

Este protocolo ofrece una autenticación mutua tunelada y no requiere que el servidor se identifique con un certificado digital. Es un protocolo diseñado por Cisco para reemplazar a LEAP ya que ofrece utilizar una clave secreta compartida conocida como PAC (Protected Access Credential, 'Credencial de acceso protegido').

- EAP-SIM (Subscriber Identity Module)

Es un protocolo que ofrece una autenticación mutua mediante la utilización de tarjetas SIM insertadas en el propio dispositivo inalámbrico o conectado a través del puerto USB.

2.8 *Pentesting*

2.8.1 Razones de llevar a cabo el proceso de *Pentesting*

Hay varios motivos por qué una organización debería de contratar los servicios de un profesional de seguridad informática para realizar una prueba de penetración. La razón principal es que los sistemas informáticos siempre tienden a padecer de agujeros o brechas de seguridad conforme la tecnología avanza y esto puede llegar a ser sumamente costoso para una organización sino se adapta a las reglas que rigen la seguridad de cualquier sistema informático. Un ataque acertado

puede conducir a pérdidas financieras, dañar la reputación de la organización, provocar multas, etc. Con una prueba de penetración apropiada es posible identificar vulnerabilidades de seguridad y luego tomar contramedidas antes de que un verdadero ataque ocurra.

Una prueba de penetración generalmente es realizada por gente experta en la materia y usualmente son externos a la organización del sistema bajo prueba. Por consiguiente, esta persona o grupo de personas que prueban la seguridad de un sistema o red informática, lo hacen basándose en un punto de vista diferente del que se tiene en la institución y pueden ser capaces de identificar las cuestiones que no eran fácilmente visibles a operadores, administradores o empleados internos. Otra razón de realizar pruebas de penetración es que esto puede ser un factor para forzar al operador y/o administrador del sistema a mantener el sistema actualizado en lo que concierne a las últimas vulnerabilidades. Nuevos 'bugs' o fallos y cuestiones de seguridad con frecuencia son descubiertos. Una violación de seguridad específica produce un cierto daño a la organización. Dependiendo la severidad de las cuestiones que son identificadas, es posible de manera apropiada planificar una estrategia de mitigación con un enfoque más fuerte sobre problemas más críticos. Ya que una prueba de penetración simula un verdadero ataque, esto es una posibilidad buena para evaluar la preparación del personal técnico de la organización en tales situaciones.

2.8.2 El Proceso de '*Pentesting'*

El objetivo de una prueba de penetración es la de evaluar el nivel de exposición del sistema bajo prueba y determinar el modo de comprometer el sistema. Para realizar correctamente una prueba valiosa y legítima, varios procedimientos tienen que ser realizados además de la fase de pruebas real, como descrito en esta sección. El proceso de una prueba de penetración profesional puede ser dividido en cuatro fases principales: iniciación, preparación, pruebas, y reportaje.

Iniciación

La fase de iniciación implica una discusión inicial con el cliente (el propietario del sistema bajo prueba) con el objetivo de establecer un acuerdo con el '*pentester'*, es decir, el responsable de realizar la prueba de penetración. En esta fase, las dos partes (el cliente y el '*pentester'*) definen el alcance de la prueba, la gente responsable de las diferentes tareas, las acciones que le son permitas tomar al '*pentester'*, y la planificación de prueba. Un equipo es formado e información de contacto es intercambiado.

Preparación

Antes del comienzo de las pruebas de penetración reales, una preparación ocurre según el acuerdo establecido durante la fase de iniciación. Si más de un '*pentester'* está implicado en las pruebas, entonces el trabajo es organizado y dividido dentro del equipo. Dependiendo de las tareas que tienen que ser ejecutadas, las herramientas, tanto software como hardware, son escogidos y configurados debidamente. Esta fase requiere que los '*pentesters'* tengan la integridad y la

estabilidad del sistema bajo prueba en cuenta. Esto es un aspecto crítico estableciendo las acciones que serán tomadas durante la prueba de penetración.

Prueba

Esta fase contiene las pruebas reales y estrechamente se parece al proceso llamado '*hacking process*'. Cada acción tomada durante la fase de pruebas debe ser registrada de modo que sea posible analizar la historia en caso de que situaciones inesperadas surjan. La comunicación con el cliente es también importante en situaciones específicas donde el '*pentester'* necesite la aprobación del propietario o administrador del sistema antes de tomar una acción. El proceso de pruebas implica varios pasos diferentes, descritos en las secciones siguientes. Algunos de estos pasos son repetidos con el tiempo cuando nuevos fragmentos de información son recogidos y analizados por el '*pentester'* como un rompe cabezas para luego explorar las nuevas áreas del sistema bajo prueba.

Identificación del objetivo

La identificación del objetivo consiste en la obtención de información sobre el sistema bajo prueba como dominios disponibles, direcciones IP, recursos internos, política de seguridad, etc. La importancia de la fase de identificación del objetivo depende de la cantidad de información disponible al equipo que realiza el '*pentesting'* al principio de la prueba. La identificación del objetivo es esencial, sobre todo en el contexto de una prueba de penetración externa por ejemplo cuando el '*pentester'* no tiene ningún acceso inicial a recursos internos (punto de acceso, un nodo ethernet etc.) La información útil puede ser descubierta con un número de técnicas diferentes, como una exploración exhaustiva de un sitio web, la información creciente de motores de búsqueda, o la realización de algún proceso de ingeniería social.

Escaneo

El escaneo es la primera parte del proceso de pruebas de penetración que implica una interacción pasiva o activa con el sistema bajo prueba. Esto consiste en explorar la red con el objetivo de encontrar que tipo y cuantos 'hosts' están presentes, que puertos están abiertos, y que servicios informáticos se encuentran activos. Un conjunto de herramientas por lo general es usado para realizar esta tarea.

Enumeración

Una vez que el '*pentester'* ha construido una descripción de los 'host' (dispositivos en la red) y los servicios activos en el sistema bajo prueba, es hora de identificar aquellos que con la mayor probabilidad son vulnerables. La enumeración consiste en la obtención de información sobre los servicios en el sistema además de los resultados de la exploración de puertos. Ejemplos de tal información son la versión de los servicios activos, vulnerabilidades conocidas, la política de cierre de contraseña para un servicio específico, etc. Este conocimiento permite al '*pentester'* identificar el punto o los puntos más débiles. La experiencia del '*pentester'* es un factor clave en esta fase, aunque hay herramientas que también facilitan en gran medida la realización de esta fase.

Penetración

La penetración es el acto de explotar una debilidad que ha sido identificada en el sistema bajo prueba. Un '*exploit'* o vulnerabilidad bien definida, es el medio por el cual un '*pentester'* o un atacante toma ventaja de un defecto dentro del sistema, causando un comportamiento anormal y contraproducente en el sistema. El objetivo de la explotación es de ganar el acceso a un cierto recurso, por ejemplo: obteniendo el acceso remoto para controlar una máquina sobre la red. Ejemplos de '*exploits'* comunes son desbordamientos de bitácoras ('*buffer overflow'*), inyecciones SQL, errores de configuración, etc.

Ya que los '*exploits'* tienen la capacidad de causar un daño temporal o permanente al sistema bajo prueba, es la responsabilidad del '*pentester'* de determinar si es aceptable usar una cierto '*exploit'*. Mantener una buena comunicación con el cliente por lo general ayuda al '*pentester'* realizar estas decisiones. Por lo general, no se le permite al '*pentester'* realizar acciones potencialmente peligrosas a la estabilidad y la integridad del sistema bajo prueba, de ahí el concepto de prueba de penetración y hackeo ético.

Escalación

Cuando una vulnerabilidad es explotada satisfactoriamente, el acceso ganado a un recurso a menudo es limitado. Por ejemplo, el '*pentester'* de penetración podría ganar el acceso a una cuenta de usuario con privilegios limitados, pero privilegios más altos son necesarios para realizar ciertas operaciones. La fase de escalación de privilegios consiste en una posterior explotación a un recurso del sistema para aumentar la influencia del '*pentester*' sobre la máquina o sistema comprometido.

Interacción

El hecho que un 'host' en el sistema bajo prueba sea comprometida no necesariamente significa que sea fácil controlarlo. El '*pentester*' necesita establecer un mecanismo de interacción para realizar operaciones sobre la máquina comprometida de la misma manera que un administrador lo haría. A veces, los 'exploits' directamente proveen al '*pentester*' de una interfaz interactiva por ejemplo una herramienta de acceso remoto ('remote shell') para controlar el sistema o recurso comprometido. Sin embargo, cuando esto no es posible, una fase adicional para ganar el acceso interactivo (gráfico o la línea de comando) es necesaria.

Explotación

El pillaje ocurre cuando se logra el acceso al sistema bajo prueba, y consiste en la recolección de información sobre el recurso comprometido y potencialmente otras entidades de red por ejemplo 'routers', 'switches' y 'hosts'. El objetivo de esta fase es la de ampliar la influencia del '*pentester*' sobre el sistema y posiblemente identificar vulnerabilidades adicionales sin la necesidad de explotarlos. Por ejemplo, el '*pentester*' podría extraer credenciales de bases de datos locales, leer las contraseñas de los usuarios en su forma 'hashed', analizar configuraciones de cortafuegos etc.

Limpiar

Un '*pentester*' profesional no debe dejar nada de lo que fue instalado sobre el sistema durante la prueba. Cada configuración cambiada o alterada también debe ser restaurada a su estado original. El objetivo de esta fase es evitar introducir vulnerabilidades adicionales en el sistema bajo prueba. El objetivo de esta fase es diferente de la perspectiva de un hacker. Un hacker está preocupado con eliminar y borrar todos los rastros de su presencia en el sistema objetivo para evitar ser descubierto e identificado. Sin embargo, un hacker podría estar interesado en la salida de una puerta trasera, por ejemplo un mecanismo que le permita más tarde recuperar el mismo nivel de acceso sin la necesidad de explotar el sistema otra vez.

Reportaje

La fase final de una prueba de penetración debe relatar los resultados de la prueba. El informe incluye una descripción de las vulnerabilidades que se encontraron durante la prueba, cómo fue posible su explotación y sugerencias sobre cómo corregir dichas vulnerabilidades y fallos del sistema probado. Desde la perspectiva del cliente, recibir una lista de cuestiones que fueron identificadas no proporciona mucho valor. Por lo tanto, a menudo es preferido organizar un taller donde el contenido del informe puede ser dialogado y los '*pentester*s' claramente pueden explicar al cliente de lo que realmente pasó durante la prueba de penetración. Otra ventaja de dicho taller consiste en que la severidad de las vulnerabilidades que fueron encontradas puede ser discutida y definida juntos con el cliente. La severidad indica el nivel de peligro de una vulnerabilidad y está basado en dos factores: la probabilidad que una vulnerabilidad sea explotada y el daño que una explotación posible puede tener sobre la organización o empresa.

2.8.3 Ataques Inalámbricos y Los Pasos de Pentesting

A continuación se presentan diferentes tipos de ataques y sus respectivos pasos de una prueba de penetración inalámbrica: (Johns, enero de 2015)

Reconocimiento:

- El escaneo inalámbrico de puntos de accesos
  - Encontrar el punto de acceso de nuestro objetivo
- Identificando SSID y dirección MAC
  - Nombre de difusión
  - Dirección MAC inalámbrica del AP
- Recolección de información sobre el cifrado y algoritmos de cifrado
  - WEP, WPA, WPA2
  - PSK, AES, TPK
- Husmear redes inalámbricas
  - Recolección de tráfico de red sobre Wi-Fi

- Manteniéndonos indetectables
  - Llevar a cabo la técnica de 'spoofing' de una dirección IP o conexión de retorno
  - Procurar pasar desapercibido para no levantar sospecha

Ataques y penetración:

- Sobrepasar o atacar las medidas de seguridad
  - Llevar a cabo el ataque de 'banner grabbing'
  - Acertar o craquear la contraseña
  - inyección SQL
  - Ganando acceso vía protocolos HTTP, HTTP, SSH, y Telnet
- 'Spoofing' de direcciones MAC
  - Utilización de herramientas como 'macchanger'
- Craqueo de algoritmos de cifrado inalámbricos
  - Utilizar herramientas como Aircrack-ng, Reaver etc.

Ataques a clientes:

- Ataques locales y remotos
  - Contraseñas comúnmente usadas
  - Tener acceso a archivos en las máquinas 'hosts' sin ningún tipo de autenticación.
  - Manipulación del sistema operativo para crear una puerta trasera
- Captura y craqueo de credenciales
  - Wireshark
  - Ettercap NG

Exploración de la red:

- Identificando a los 'hosts' del sistema
  - Comúnmente se utiliza la herramienta 'Nmap scanner'
- Determinando el tamaño de la red
  - Se puede llevar a cabo utilizando una herramienta llamado 'Zenmap scanner'

Evaluación de vulnerabilidad:

- Realización de escaneos de vulnerabilidad automatizados o manuales
  - La herramienta de escaneo de vulnerabilidades tal como Nessus
- Generación de reportes de vulnerabilidades
  - Exportación de informes vía Nessus

Explotación y captura de datos:

- Penetración
  - La explotación de 'routers' inalámbricos y APs para obtener acceso no autorizado a recursos de una red inalámbrica.

- Comprometiendo
  - Obteniendo derechos de administrador completos a terminales y servidores
- Análisis de Datos
- Reportaje

La metodología llevada a cabo en una prueba de penetración inalámbrica da una visualización desde la fase reconocimiento hasta el reportaje.

2.9 Métodos y Técnicas de Ataques Inalámbricos

2.9.1 Ataques de Control de Acceso

Los ataques de control de acceso intentan penetrar una red utilizando medidas de evasión o medidas inalámbricas de control de acceso WLAN tales como filtros para direcciones MAC de APs y control de acceso de puertos 802.11. Las siguientes secciones muestran algunos ataques de control de acceso. (Johns, enero de 2015)

War Driving

El término 'war driving' se refiere a un tipo de ataque pasivo donde se lleva a cabo el monitoreo de una red inalámbrica para capturar información sensible por ejemplo, la dirección MAC o IP origen y destino, identificadores de usuario, contraseñas, clave WEP, etc. En esta técnica de ataque, individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar en coche, o algún otro medio de transporte, puntos de acceso inalámbricos. Los instrumentos como Airmon-ng, DStumbler, KisMAC, y NetStumbler pueden realizar este ataque. El 'war driving' por lo general es realizada por dos personas, alguien conduciendo el coche y la otra persona escanea, descubre y monitorea redes inalámbricas en el área. Con el software correcto y su correcta implementación, los individuos llevando acabo el 'war driving' pueden establecer ajustes de GPS para localizar estas posiciones o ubicaciones Wi-Fi y almacenarlos para futuros ataques inalámbricos. (Johns, enero de 2015)

Puntos de acceso no autorizados (Rogue AP)

Para este tipo de ataque, se implementa un AP o varios APs que se conectan sin autorización a una red existente. Estos puntos de acceso no son gestionados por los administradores de la red y es posible que no se ajuste a las políticas de seguridad de la red. De esta forma se tiene una alta capacidad para llevar a cabo muchos tipos de ataques indeseados, puesto que permite a cliente con un terminal WiFi conectarse a la red, y vulnera todos los mecanismos que se basan en el cifrado de información entre extremos (WEP, WEP2, WPA, etc.) Se recomienda evitar conectarse a puntos de acceso en modo de configuración abierta aunque utilizando un servicio de VPN, cualquier dispositivo conectado a cualquier red de Wi-Fi abierta o pública aumenta en gran medida la seguridad de su información que es enviada en la red. (Johns, enero de 2015)

Asociaciones ad hoc

Las asociaciones ad hoc se conectan directamente a un AP en modo abierto para vulnerar la seguridad del AP o atacar otro AP. El atacante se conecta al AP y cambia las configuraciones de seguridad del AP o también puede cambiar las contraseñas para bloquear el acceso a ella por parte del propietario. (Johns, enero de 2015)

MAC spoofing

El 'MAC spoofing' es un término usado cuando el atacante reconfigura su propia dirección MAC para hacerse pasar por un AP o un cliente legítimo. Esto da al atacante el acceso completo a la red a través del AP como si fuera un AP o cliente genuino. Este ataque comúnmente es utilizado en áreas WiFi de pago como hoteles, aeropuertos, cafeterías, y otras ubicaciones de acceso a internet de pago. (Johns, enero de 2015)

Craqueo 802.11 de RADIUS

Este tipo de ataque no es muy popular pero es un asunto importante que se debe mencionar. Este ataque consiste en que el atacante recupera una clave RADIUS ('Remote Authentication Dial In User Service') a través de la técnica de craqueo llamado fuerza bruta de una solicitud de acceso para acceder a la red. Cualquier herramienta de captura de paquetes en una red LAN entre el AP y un servidor RADIUS funcionaría para obtener una clave RADIUS. Esta técnica de ataque resulta ser muy peligrosa ya que muchos APs, servidores, e incluso servicios de software pueden requerir una cuenta RADIUS para acceder a la red. Si el sistema RADIUS es comprometido, el atacante puede obtener el acceso de cualquier servicio o dispositivo que utilice RADIUS para autorizar el acceso a la red. (Johns, enero de 2015)

2.9.2 Ataques de Confidencialidad

Estos ataques intentan interceptar información privada enviada sobre redes inalámbricas, no importando si es enviada en texto plano o cifrado por el estándar 802.11 o protocolos de capas superiores. Las secciones siguientes describen algunos ataques confidencialidad. (Johns, enero de 2015)

Escucha disimulada (Sniffing)

La escucha disimulada respecto a la seguridad informática es donde se capturan datos, se descifra, y luego se obtiene la información potencialmente sensible. Esto se parece exactamente a la escucha disimulada de una llamada telefónica ('wire tapping'). Un atacante escucha, registra, y luego posiblemente consigue la información sensible de la conversación. Las escuchas se consideran un paso previo a los ataques posteriores que suponen una importante fisura en cuanto a seguridad. Para que un dispositivo tenga la capacidad de llevar a cabo escuchas en una red WiFi, debe tener instalada o integrada una tarjeta WLAN que actúa en modo monitor o en modo promiscuo. Estos modos de operación permiten recibir todo el tráfico que circula por la red. Adicionalmente es necesario un software especial que monitorice toda la información que viaja a

través de la red. Herramientas como Ettercap, Hado, y Wireshark son algunas de muchas herramientas que facilitan realizar este tipo de ataque. (Johns, enero de 2015)

Craqueo de clave WEP

Este tipo de ataque se basa en la captura de datos para la recuperación de una clave WEP. Para realizar este tipo de ataque se utiliza métodos pasivos o activos. Con el avance tecnológico en cuanto al software y hardware, el cifrado WEP puede ser descifrado o craqueado fácilmente en menos de 5 minutos. El cifrado WEP sólo debería ser usado en casos donde se encuentran hardware obsoletos que siguen funcionando y operando en una organización, empresa u hogar. De otra manera, se recomienda usar el cifrado WPA2. Las herramientas tales como Aircrack-ng, AirSnort, Airoway, chopchop, y dwepcrack pueden realizar estos ataques. (Johns, enero de 2015)

Evil Twin AP

Un 'Evil Twin' AP se parece a un punto de acceso no autorizado (Rogue AP). El atacante crea un AP falso para atraer a usuarios pensando que es la red inalámbrica genuina a la que ellos/ellas se quieren conectar. Es decir, el ataque se basa en el hecho de que pueden existir dos APs con el mismo SSID en la misma área para luego volverse en un ataque de hombre en medio ('man in the middle'). El atacante amplifica la señal y el radio de cobertura del AP falso para que el cliente automáticamente se conecte al AP falso ya que las tramas 'Beacon' se difunden con más frecuencia y establecen comunicación rápidamente con el AP falso. Las herramientas tales como Honeypot, CqureAP, D-Link G200, HermesAP, Rogue Squadron, WifiBSD y Pineapple Wifi (Karma y Dogma) pueden realizar estos ataques. (Johns, enero de 2015)

AP Phishing

El atacante ejecuta un portal web falso o servidor web a través de un AP falso para 'pescar' (phish), es decir, obtener credenciales, cuentas bancarias, y números de tarjeta de crédito entre otras. Este tipo de ataque, por mucho, es uno de los más peligrosos y aterradores de ser víctima ya que un usuario común y corriente no se percataría del ataque. Los usuarios comunes creerían que es el verdadero sitio web cuando de hecho el atacante solamente espera para que accedan a su cuenta y luego recolectar información sensible al otro lado de la conexión. Las herramientas tales como Airpwn, Airsnarf, Hotspotter, Karma, y RGLUEAP pueden realizar estos ataques. (Johns, enero de 2015)

El ataque 'Man In The Middle'

Un ataque 'Man In The Middle' consiste en el hecho de que un atacante intercepta el tráfico de red entre un usuario y otro objetivo. Dicho de otra manera, el atacante adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante podría usar este ataque sobre una red cableada (Ethernet) o inalámbrica para obtener nombres de usuarios, contraseñas, correos electrónicos, ver las sesiones HTTP de sitios web, y mucho más. Las herramientas tales como dsniff, Ettercap-NG, y sshmitm pueden realizar estos ataques. (Johns, enero de 2015)

2.9.3 Ataques de obtención de credenciales

Un ataque de obtención de credenciales se relaciona con la adquisición de credenciales de conexión robadas por un atacante. Esto puede ser hecho por un servidor web o a través de un software llamado 'Social Engineering Toolkit (SET)'. El atacante puede clonar un sitio web, haciendo el sitio web parecer auténtico y bastante legítimo para engañar al usuario en acceder a ella con su cuenta de usuario. Las víctimas suelen pasar desapercibidas de que les hayan robado sus credenciales de algún sitio web o servicio web. En las secciones siguientes se mencionan ataques de recolección de credenciales y métodos de ataque 'phishing'. (Johns, enero de 2015)

Recolección de Credenciales ('Credential harvester')

Este ataque ejecuta un servidor apache sobre el sistema del atacante para clonar un sitio web que se parezca al sitio web legítimo. El atacante podría unir un punto de acceso y peticiones HTTP 'DNS-spoof' hacia el sitio web falso. El sitio web parecerá idéntico al sitio web legítimo donde el usuario intentará conectarse como normalmente lo hace. En el extremo donde el atacante se encuentra conectado, el atacante tendrá la capacidad de ver el nombre de usuario y la contraseña del usuario así como la dirección IP de su máquina. Luego, el atacante podría seguir recolectando cuentas de usuario para luego almacenarlos en un informe generado por algún software. Es esencial realizar ataques de ingeniería sociales en contra del personal de una organización para probar si ellos siguen las políticas y procedimientos de seguridad de la organización. (Johns, enero de 2015)

Phishing

'Phishing' es una prueba fraudulenta de recolectar información sensible como nombres de usuarios, contraseñas, números de seguro social, números de teléfono, y números de tarjetas de crédito. Estos ataques comúnmente son identificados a través de los correos electrónicos enviados directamente a un usuario para incitarlo a visitar un sitio web que lo engaña en cuanto a una actualización de su información, el cambio de contraseña, o la verificación de su información. La mejor manera de protegerse de un ataque 'phishing' es de aprender como los atacantes trabajan. Un correo electrónico pidiendo una contraseña o el cambio de contraseña de un remitente desconocido tiene una alta probabilidad de que sea un correo falso. Estos correos electrónicos tienen que ser bloqueados o señalados como correo basura (spam). Si uno cree que es víctima de este tipo de ataque, es imperativo cambiar las contraseñas y preguntas de seguridad para prevenir cualquier daño o pérdida de información en su cuenta en línea. (Johns, enero de 2015)

2.9.4 Ataques de autenticación

Los atacantes usan ataques de autenticación para el robo de cuentas y credenciales de usuarios legítimos y luego acceder a servicios y redes privadas. Las secciones siguientes explican algunos ataques de autenticación. (Johns, enero de 2015)

Adivinación/predicción de clave compartida

El atacante intenta adivinar una clave compartida de autenticación utilizando credenciales por defecto de fabricantes o proveedores o a través de generadores claves compartidas. Todas las llaves compartidas por defecto deberían de ser inmediatamente cambiadas a la hora de instalación y configuración de un dispositivo de red. Cualquier herramienta de craqueo tal como Aircrack-ng puede realizar este ataque. (Johns, enero de 2015)

Craqueo PSK

Este tipo de ataques tratan de descubrir la contraseña que un usuario utiliza para acceder al sistema o descubrir claves de cifrado de la información, generalmente, tras llevar a cabo una escucha y recopilación del tráfico cifrado durante cierto tiempo. Para elegir las posibles contraseñas se utilizan principalmente dos métodos: ataques de fuerza bruta y ataques de diccionario. El ataque de craqueo de PSK recupera una clave PSK WPA/WPA2 a través de la captura de tramas del inicio de la comunicación entre un usuario y un AP para luego ejecutar un ataque de diccionario o de fuerza bruta y recuperar así la clave PSK. Este ataque depende de la robustez de cifrado de la llave WPA/WPA2. Si la llave es realmente fuerte, esto podría tomar semanas para craquearla, algo que es demasiado inconveniente para un atacante. Siempre tenga una mezcla de letras, números, y símbolos alfanuméricos al crear sus propias contraseñas. Las herramientas tales como coWPAtty, genpmk, KisMAC, y wpa_crack pueden realizar este ataque. (Johns, enero de 2015)

Escuchas (Sniffing) de credenciales de aplicación

Para las escuchas de credenciales de aplicación, el atacante captura credenciales de usuario como direcciones de correo electrónico y contraseñas de protocolos de aplicación en texto plano. Ahora que más sitios web usan HTTPs, esto raramente se encuentra en sitios web populares. Sin embargo, cuando un usuario accede con credenciales a un router o AP, por lo general HTTP es utilizado por lo que la información viaja en texto plano. Si se ingresa con credenciales a través del protocolo HTTP, el atacante fácilmente puede ver el nombre de usuario y contraseña. Las herramientas tales como Ace Password Sniffer, dsniff, PHoss, y Win Sniffer pueden realizar este ataque. (Johns, enero de 2015)

Craqueo de cuentas de dominio

En ataques de craqueo de cuentas de dominio, el atacante recupera las credenciales del usuario como su cuenta de acceso al sistema operativo Windows y su contraseña a través del craqueo de los ‘hashes’ de contraseña NetBIOS utilizando ya sea la técnica de fuerza bruta o ataque de diccionario. Hay también algunas herramientas y aplicaciones disponibles que requerirán contraseñas guardadas en navegadores como Internet Explorer, Firefox, y Chrome de Google. Una vez que un atacante consigue estas credenciales de los navegadores, se podría acceder a una red, intercambiar correos electrónicos y tal vez aún comprometer el dominio entero si la cuenta resulta tener derechos administrativos. Las herramientas tales como John the Ripper, L0phtCrack, y Caín pueden realizar este ataque. (Johns, enero de 2015)

Craqueo de credenciales VPN

En este ataque, el atacante recupera las credenciales de un usuario como PPTP o contraseñas IPSEC ejecutando un ataque de fuerza bruta sobre los protocolos de autenticación de VPN. Se recomienda verificar y asegurarse que la contraseña y la llave pre-compartida secreta sean diferentes el uno del otro y sean fuertes. Contraseñas o números fáciles de adivinar fácilmente pueden comprometer el sistema informático de una organización entera y esto puede conducir al robo de información. Herramientas tales como -scan, IKECrack, anger y THC-pptp-bruter pueden realizar este tipo de ataque. (Johns, enero de 2015)

2.9.5 Robo de identidad 802.11

En un ataque de robo de identidad 802.11, el atacante captura perfiles de usuario en texto plano en una red 802.11. El cifrado es la clave para asegurarse que la información no sea comprometida. La utilización de HTTPS y protocolos VPN puede ayudar a proteger a los usuarios de este tipo de ataque. Herramientas de captura de datos como Wireshark o Ettercap-NG pueden realizar este tipo de ataque. (Johns, enero de 2015)

Adivinación de contraseñas 802.11

En un ataque de adivinación de contraseñas 802.11, el atacante utiliza un nombre de usuario capturado para continuamente intentar de adivinar o predecir la contraseña para la autenticación 802.11. El atacante comúnmente intentará dar con la contraseña probando contraseñas comunes, contraseñas por defecto, cumpleaños, nombres, números telefónicos entre otras hasta obtener la contraseña y acceder a la red inalámbrica. Si el atacante tiene un diccionario de contraseñas bastante creativo, entonces podría ejecutar un ataque de diccionario para dar con la contraseña en unas cuantas horas. Herramientas como John the Ripper y THC Hydra puede llevar a cabo este tipo de ataque. (Johns, enero de 2015)

Craqueo LEAP 802.11

En un ataque de craqueo LEAP 802.11, el atacante recupera las credenciales de usuario de paquetes LEAP 802.11 capturados utilizando una herramienta de ataque de diccionario para descifrar el hash de la contraseña NT. Esto depende de la fortaleza de la contraseña, si es muy buena, es poco probable que sea craqueada. Esa es la razón por la que es muy importante de contar con una combinación de letras, números y símbolos alfanuméricos para prevenir estos ataques de diccionario. Herramientas como Anwrap, Asleep, y THC - LEAPcracker pueden realizar este tipo de ataques. (Johns, enero de 2015)

Ataque '802.11 EAP downgrade'

El estándar 802.11 requiere EAP para enviar mensajes entre el usuario que se conecta y el mecanismo de autenticación. Si un atacante puede posicionarse entre el cliente y el proceso de autenticación, entonces el usuario que quiere conectarse se conecta a la red. El atacante obliga a un dispositivo o servidor inalámbrico ofrecer un tipo de autenticación débil mediante una respuesta EAP o un paquete NAK alterado. Dado que la autenticación es tan débil, que sólo toma unos pocos minutos para que el atacante obtenga acceso a la red. Herramientas como File2air y libradiate pueden realizar estos ataques. (Johns, enero de 2015)

Cuestiones con redes inalámbricas

Con la tecnología de hoy que avanza tan rápido, el Internet padece de muchos tipos de nuevas amenazas cada día. Los criminales utilizan malware sofisticados y ataques de ingeniería social que tiene como objetivos usuarios y organizaciones que se encuentra débiles en cuanto a conocimiento y políticas de seguridad informática. Los usuarios finales se conectan a una red WiFi normalmente para tener acceso a Internet y navegar en ella utilizando un navegador web. La sección siguiente describe uno de los ataques más comunes dirigidos en el nivel de usuario. (Johns, enero de 2015)

Descarga

La descarga es una de las razones más grande de tener acceso a Internet. Un usuario rápidamente puede descargar música, vídeos, libros etc. Si un usuario descarga de fuentes desconocidas, esto podría crear una amenaza seria, no solo a la máquina del usuario sino que a la red entera. La descarga es peligrosa porque muchas de las descargas no requieren del permiso del usuario. Esto es donde el malware entra y logra infectar al 'host' y posteriormente a muchos 'host' más. Si un usuario abre su correo electrónico y le da clic a un hiperenlace, esto por lo general le indica al navegador web que muestre el contenido; sin embargo, si el hiperenlace es una redirección hacia un malware, esto al instante lo descargaría y lo ejecutaría en la computadora. Se debe consultar la fuente antes de realizar descargas. (Johns, enero de 2015)

2.10 Herramientas de Pentesting

2.10.1 Software

Kali Linux

Kali Linux es la nueva generación de la conocida distribución Linux BackTrack, la cual se utiliza para realizar Auditorías de Seguridad y Pruebas de Penetración. Kali Linux es una plataforma basada en GNU/Linux Debian y es una reconstrucción completa de BackTrack, la cual contiene una gran cantidad de herramientas para capturar información, identificar vulnerabilidades, explotarlas, escalar privilegios y cubrir las huellas.

La siguientes herramientas se encuentran inmersas en Kali Linux y se utilizaron para llevar a cabo una auditoria inalambrica de la red WiFi 'wlcampus'.

Suite Aircrack-ng

Hablar de la suite Aircrack-ng es hablar de la mejor herramienta para craquear contraseñas WEP y WPA de los routers inalámbricos o APs, pero no sólo eso sino que gracias a las herramientas incorporadas en su suite, podremos realizar diversos tipos de ataques en la red inalámbrica. Las principales herramientas de las que consta la suite Aircrack-ng son las siguientes:

- Airmon-ng: es la herramienta encargada de poner en modo monitor o modo promiscuo a nuestra tarjeta de red inalámbrica, con la finalidad de poder capturar los paquetes.
- Airodump-ng: siempre se emplea inmediatamente después de airmon-ng, y justo antes que aircrack-ng y es fundamental para que la auditoría tenga éxito. Airodump-ng se encarga de capturar todos los paquetes cuando tenemos la tarjeta en modo monitor, de esta forma podremos capturar los IVs si tenemos una clave WEP o el handshake si tenemos WPA/WPA2 para posteriormente romper la contraseña con Aircrack-ng.
- Aircrack-ng: esta herramienta es la encargada de crackear por diccionario o por fuerza bruta las contraseñas de las redes inalámbricas, ya sea con cifrado WEP, WPA o WPA2.
- Aireplay-ng: esta herramienta se encarga de de-autenticar a los clientes legítimos con la finalidad de capturar el 'handshake' en redes WPA/WPA2, o generar un gran tráfico de datos en redes WEP. Incluso se puede utilizar para lanzar un ataque de denegación de servicio (DOS) a uno o varios puntos de acceso.
- Airbase-ng: esta herramienta permite configurar un punto de acceso falso para que el objetivo se conecte a él con la finalidad de poder lanzar un ataque MITM para robar la contraseña real de acceso.

Ethercap

Esta herramienta es una herramienta de sniffing y seguridad de redes para ataques 'Man In the Middle' en LAN, se ejecuta en varios sistemas operativos de tipo Unix como GNU/Linux, Mac OS X y Solaris y en Microsoft Windows. Es capaz de interceptar tráfico en un segmento de red, la captura de claves, y la realización de escucha activa contra una serie de protocolos comunes (stack de TCP/IP).

SSLstrip

SSLstrip es un proxy que tiene como objetivo eliminar el cifrado del contenido de las páginas web que implementan HTTPS como mecanismo de seguridad. Esta herramienta fue diseñada para hacer que las sesiones HTTP sin cifrar se vean como sesiones HTTPS. Convierte enlaces HTTPS a HTTP o HTTPS con una clave privada conocida. Incluso proporciona un icono de candado para generar la ilusión de un canal seguro. Muchos sitios HTTPS son normalmente accesibles desde una redirección HTTP en una página, y muchos usuarios no se dan cuenta cuando su conexión no se actualiza y su información que viaja en la red puede ser interceptada en texto plano.

URLsnarf

La herramienta urlsnarf es una herramienta que escucha sigilosamente peticiones HTTP en formato común de registro (Common Log Format). Urlsnarf muestra todas las solicitudes de URLs interceptadas en un formato de registro común ideal para un análisis fuera de línea con alguna

herramienta de análisis de registros web. Urlsnarf permite realizar capturas de URLs es decir capturas de nombres de páginas o direcciones de páginas web que nuestra victima este visitando en el momento que se esté llevando un ataque de 'Sniffing' o 'Man In the Middle'. Gracias a esta herramienta se puede conocer información importante de la página que están visitando así como hacer un perfil de nuestra victima en base a lo que está observando. Otro punto importante de mencionar es que también nos brinda información sobre el buscador que se está utilizando.

Wifipineapple Mark V

Básicamente este dispositivo se considera como un 'honeypot' para WiFi que permite a los usuarios llevar a cabo ataques 'man-in-the-middle'. El tráfico de los clientes conectados pasa por el atacante y esto le permite ejecutar otras herramientas de ataques como SSLstrip, tcpdump, session hijack entre otras para ampliar y garantizar la efectividad del ataque man-in-the-middle. Está equipado con 2 adaptadores de red (AR9331 and RTL8187) que puede trabajar en modo cliente lo que significa que puede aprovecharse de una red WiFi cercana y forzar conexiones automáticas y sigilosas del equipo de la víctima.

Ilustración 32: Dispositivo de auditoría de red llamado Wifi Pineapple Mark V.

PineAP

Es un conjunto de herramientas que se utiliza para crear y personalizar un punto de acceso falso de manera automática y efectiva. Está compuesta de las siguientes herramientas: MK5 Karma, Dogma, Beacon Response, Auto Harvester, Recon Mode (Site_Survey).

Beacon Response

De manera similar a la forma en que MK5 Karma responde a las peticiones 'probe' de clientes, el módulo Beacon Response responde al cliente potencial con tramas 'beacon' debidamente diseñadas dirigidas exclusivamente a ellos. Esto refuerza la legitimidad de la red falsa sin causar

la difusión de tramas 'beacon' que de otro modo podrían ser captadas por otros dispositivos. A diferencia de Dogma que está configurado por defecto en un estado de difusión, la respuesta beacon sólo responde al cliente potencial, y sólo cuando ese cliente realiza una solicitud 'probe'.

MK5 Karma

Desde el lanzamiento del primero dispositivo WiFi Pineapple, Karma ha jugado un papel muy importante en ataques a clientes en entornos WiFi. Karma toma este papel para lanzar ataques a clientes con la ayuda de otras herramientas como Dogma, Auto Harvester y Recon Mode para crear y establecer puntos de accesos no legítimos o honeypots. Su característica más esencial es la de engañar a los clientes de un determinado punto de acceso legitimo al dar respuestas a las solicitudes 'Probe' de los clientes a través de respuestas 'Probe' diseñadas para establecer una conexión automática entre el cliente y el punto de acceso falso.

Dogma

Esta herramienta tiene como objetivo reforzar el ataque llevado acabo por MK5 Karma a través de la difusión de SSIDs falsos. Dogma logra conseguir esto por medio de tramas 'beacon' que son diseñadas apropiadamente y son difundidas a tasas muy altas. Estas tramas 'beacon' se hace pasar como tramas legitimas que difunde una red definido por un SSID genuino que luego es almacenado en una piscina de SSIDs para futuros ataques. Una característica poderosa de Dogma es su habilidad de ser configurado con una dirección MAC específica de origen y destino. Esto da lugar a lanzar ataques 'Broadcast' que hace que cualquier dispositivo WiFi cercano pueda ver las tramas ´beacon´ y responder a ellas de manera automática.

Auto Harvester

Esta herramienta es similar al 'War Driving' solo que en sentido contrario. En vez de obtener nombres SSID de tramas 'beacon' que son difundidos por los puntos de acceso, Auto Harvester los obtiene de las peticiones 'Probe' que son difundidos frecuentemente por los clientes potenciales. Estos nombres de SSID en la mayoría de casos nos proporciona información de cliente como su lugar de trabajo, adonde viven, que lugares visitan con frecuencia etc… Los nombres de las redes que recopila Auto Harvester son almacenadas en una piscina de SSID llamado 'PineAP SSID Pool' para luego ser utilizado por Dogma. Esta herramienta es utilizada para el reconocimiento pasivo en un entorno WiFi.

Recon Mode (Site_Survey)

Diferente que el 'War Driving' donde el auditor escucha pasivamente las tramas 'beacon' siendo difundidos por los puntos de acceso que le permite al auditor tener una imagen general del entorno WiFi, Recon Mode va un paso más allá. A través del monitoreo de canales para tramas 'beacon' y cualquier otra información sensible, Recon Mode logra describir una imagen más completa del entorno WiFi al combinar los puntos de acceso con sus respectivos clientes y cualquier otro dispositivo WiFi que no esté conectado a ninguna red. Esto le permite al auditor o al atacante tener una imagen bien clara del entorno inalámbrico para luego identificar objetivos potenciales y tomar acción utilizando las otras herramientas previamente mencionadas.

2.10.2 Hardware

Adaptador de Red Alfa AWUS036H

Se trata de un adaptador que funciona bajo los estándares IEEE 802.11b e IEEE802.11g. Es uno de los adaptadores de red más populares por su compatibilidad con sistemas operativos como Linux o Mac OS X además de Windows. Posee un gestor que es muy intuitivo y de fácil manejo lo que facilita la familiarización rápida con su funcionamiento.

Características técnicas del adaptador:

- Estándares: IEEE 802.11 b/g USB 2.0
- Luces: 1 led estado/tráfico
- Interfaz: USB 2.0 – mini USB
- Energía: 5V+5%
- Seguridad: WEP 64/128, soporte 802.1X, WPS, WPA, WPA2, WPA-PSK, WPA2-PSK
- Número de antenas: 1
- SO soportados: Windows xp/vista/7, Mac 10.4/10.5/10.6, Linux (kernel 2.6.x)

Ilustración 33: Adaptador de red Alfa AWUS036H.

Antena Alpha de 18 dbi

Antena omnidireccional de alta ganancia (18 dbi) compatible con el adaptador de red AWUS036H.

Ilustración 34: Antena Alpha de 18 dbi.

Laptop Macbook Pro 2011 (cliente)

Características:

- Procesadores Intel Core i7 2.2 GHz
- 16 Gigabytes de memoria RAM
- Gráficos duales Intel (512 Mb) y AMD Radeon (1024 Mb)
- Disco duro de 750 Gigabytes (5400 rpm)
- SuperDrive a 8x de carga por ranura (DVD±R DL, DVD±RW y CD-RW)
- Conexión inalámbrica WiFi basada en la norma 802.11n del IEEE.
- Bluetooth 2.1 + EDR
- 10/100/1000BASE-T Gigabit Ethernet 10/100/1000BASE-T (conector RJ-45).
- Toma de corriente MagSafe.
- Puerto Gigabit Ethernet.
- Un puerto FireWire 800 (hasta 800 Mb/s).
- Dos puertos USB 2.0 (hasta 480 Mb/s).
- Puerto Thunderbolt (hasta 10 Gb/s).
- Ranura para tarjetas SDXC.
- Ranura de seguridad Kensington
- Sistema Operativo: OS X El Capitan (10.11.2)

Ilustración 35: Laptop Macbook Pro late 2011 de 15 pulgadas.

Laptop HP EliteBook 8440p (atacante)

Características:

- Procesadores Intel Core i5 2.4 GHz
- 4 Gigabytes de memoria RAM
- Gráficos NVIDIA NVS 3100M con 512 MB de memoria de vídeo gDDR3 dedicada
- Disco duro de 250 Gigabytes (7200 rpm)
- Unidad óptica grabadora de DVD (DVD±R DL, DVD±RW y CD-RW)
- Una salida de vídeo VGA.12
- Un puerto FireWire
- Interfaz de red Ethernet Gigabit
- Bluetooth 2.1 + EDR y compatibilidad con localización y posicionamiento GPS
- Tres puertos USB 2.0, combinando un cuarto con una conexión eSATA
- Sistema Operativo: Kali Linux 2.0

Ilustración 36: Laptop HP EliteBook 8440p.

Capítulo 3 Desarrollo

3.1 Fases de Pentesting

Para llevar a cabo la prueba de penetración (‘Pentesting’) enfocándonos en el ataque ‘*Rogue Access Point’* o ‘Evil Twin’ que posteriormente se convertirá en un ataque ‘*Man In the MIddle’* se divide en cuatro etapas:

3.1.1 Recopilación de Información

Los adaptadores de red que operan bajo el estándar IEEE 802.11x tienen seis modos de operación. Estos son los modos ‘Master’, ‘Managed’, ‘Ad hoc’, ‘Mesh’, ‘Repeater’ y ‘Monitor’. Para el modo ‘Master’ el adaptador de red funciona como un AP y en modo ‘Managed’ funciona como un cliente de un AP. Los modos ‘Ad hoc’ y ‘Mesh’ se utilizan en redes ‘Ad hoc’ o redes ‘Mesh’ (redes de malla) respectivamente y el modo ‘Repeater’ se utiliza para retransmitir la señal WiFi. En las redes WiFi los paquetes de red son difundidos por los APs lo que significa que todos los clientes que logren captar la señal inalámbrica del AP pueden recibir esos paquetes difundidos pero los datos son entregados a cada cliente basado en la dirección MAC de destino. Para el resto de la información transmitida, si la dirección MAC de destino es diferente, son ignorados por los clientes. A la hora de monitorear todos los datos transmitidos, el adaptador de red debe configurarse en modo monitor. En modo monitor, el adaptador de red tiene la capacidad de capturar todos los datos difundidos por un AP no importando la dirección MAC destino y haciendo el modo monitor ideal para la recopilación de información.

De acuerdo al mapa del Campus Chetumal de la UQROO en la Ilustración 32, se llevará a cabo un proceso de reconocimiento de red cerca de los diferentes edificios denotados por el mapa dado la alta probabilidad que en estos edificios estén albergados los puntos de acceso que difunden la señal de las diferentes redes inalámbricas. Después de llevar a cabo el proceso de reconocimiento de red, se procederá con la recopilación de información acerca de la red inalámbrica que se tiene como el objetivo. El reconocimiento de red tiene como objetivo descubrir la señal de la red inalámbrica ***wlcampus***. Esto se logrará con las herramientas aircrack-ng (airmon-ng y airodump-ng) y recon mode (site_survey) a través de Kali Linux 2.0, el adaptador de red Alfa AWUS036H con la antena Alfa de 18 dbi y el dispositivo WiFi Pineapple Mark V.

i. Como primer paso se conecta el adaptador de red Alfa AWUS036H ya integrada con la antena Alfa de 18 dbi a la laptop HP EliteBook. Luego, se cambia la potencia de transmisión del adaptador de red Alfa a 30 dbm (1000mW) con el comando ‘iwconfig *nombre_del_adaptador* tx power 30’ para que tenga un alcance más amplio para transmitir datos. También se configura el adaptador Alfa en modo monitor con el comando ‘airmon-ng’ desde una línea de comandos en Kali Linux 2.0.

ii. Como segundo paso, desde otra línea de comandos se ejecuta el comando 'airodump-ng' para que el adaptador de red empiece a detectar las diferentes señales inalámbricas WiFi en la vecindad y nos proporcione información valiosa como los ESSIDs, BSSIDs, potencia de señal, canales, tipo de cifrado entre otras para la recopilación de información.
iii. Como tercer paso se identifica la red inalámbrica objetivo que en este caso sería ***wlcampus*** para obtener información de ella tal como su dirección MAC, la potencia de su señal, el canal que utiliza entre otra información.
iv. Como cuarto paso, desde otra línea de comandos se ejecuta nuevamente el comando 'airodump-ng' pero agregándole la dirección MAC del AP que está difundiendo la red ***wlcampus*** y el canal que está utilizando para difundirlo. Esto se realiza para monitorear exclusivamente la red ***wlcampus*** y así obtener más información acerca de los clientes conectados a ella.
v. Para reforzar los pasos anteriores y comprobar que la información recopilada con la herramienta aircrack-ng es confiable, se procede a llevar a cabo un barrido de todas las señales WiFi con el dispositivo de auditoria de redes inalámbricas llamada WiFi Pineapple Mark V. Este dispositivo realiza los pasos anteriores de manera automática con la herramienta que viene integrada por defecto en ella llamado Site Survey. Se procede a abrir una línea de comandos en Kali Linux para ingresar al dispositivo Wifi Pineapple Mark V con una cuenta y contraseña y luego se ejecuta el comando 'site_survey' seguido por el número de segundos que va a durar el barrido de red. Al culminar el tiempo de ejecución de 'site_survey', en la línea de comandos nos aparece la información como BSSID, ESSID, tipo de cifrado, potencia de la señal y canal de todos los puntos de acceso captados con sus respectivos clientes y también nos muestra los clientes que no están conectados a ningún punto de acceso pero que andan en busca de una red inalámbrica cercana a la cual puedan conectarse.

Con estos cinco pasos se logra la recopilación de información del AP o la red que tenemos como objetivo atacar y también estos cinco pasos nos pintan una imagen del entorno inalámbrico en que nos encontramos para tomar las mejores decisiones a la hora de llevar a cabo un ataque de 'Man In The Middle'.

3.1.2 El establecimiento de un punto de acceso falso ('Rogue AP')

Un 'Rogue AP' es un punto de acceso que tiene por objetivo que los usuarios/clientes se conecten a él para, una vez dentro, capturar su tráfico y obtener información sensible como credenciales de correo electrónico, de redes sociales, de cuentas bancarias entre otras. También se denominan de esta forma a los puntos de accesos ilegales y falsos que se instalan en empresas, escuelas y otras organizaciones sin autorización de los responsables de los sistemas informáticos. De esta forma, sirven como punto de entrada y se puedan conectar dispositivos WiFi a la red o hacer intrusiones desde otra ubicación.

Debido a que la red inalámbrica ***wlcampus*** se encuentra implementado con un mecanismo de autenticación en modo abierto, la creación y el establecimiento de un punto de acceso falso es sencilla y efectiva dado que se cuenta con el dispositivo WiFi Pineapple Mark V que integra la suite de herramientas PineAP. La suite PineAP con las herramientas Karma, Dogma y Auto Harvester facilitan en gran medida la creación de uno o varios Rogue APs y la conexión automática de los usuarios o clientes WiFi que están al alcance sin que se den cuenta.

Después de realizar la etapa 1 y recopilar información de la red wlcampus se procede a la creación de un AP falso.

i. Como primer paso de la segunda etapa, se procede a configurar una conexión a internet compartida entre la laptop HP (con Kali Linux) y el dispositivo Wifi Pineapple. Se establece una conexión de la laptop al AP que nos da salida a Internet utilizando la interface 'wlan0' en Kali Linux. Luego se conecta de manera cableada el dispositivo Wifi Pineapple a la laptop. La conexión cableada se realiza conectando un cable UTP directo entre los puertos RJ45 del Wifi Pineapple y la laptop.

   Desde Kali Linux se descarga el script 'wp5.sh' desde la página web 'wifipineapple.com'. Una vez descargado el script, se hace un script ejecutable ingresando el comando 'chmod +x wp5.sh' desde una línea de comandos y luego se ejecuta el script con el siguiente comando 'root/Descargas/wp5.sh'. La primera opción para configurar es la máscara de red y en la línea de comandos nos aparecerá la siguiente información con la máscara de red por defecto 'Pineapple Netmask [255.255.255.0]' que configuraremos con solo darle 'enter' ya que esa es la máscara de red de la dirección IP del dispositivo.

   Luego, se configura la dirección de red del dispositivo Wifi Pineapple. Nos aparece la dirección de red por defecto 'Pineapple Network [172.16.42.0/24]' que configuraremos con solo darle 'enter' ya que esa es la dirección de red de la dirección IP del dispositivo. Luego, se le da 'enter' a la opción por defecto 'Interface between PC and Pineapple [eth0]' para configurar la interface de red entre la laptop HP y el Wifi Pineapple ya que 'eth0' es la interface de red que corresponde a la conexión cableada entre los dispositivos mencionados previamente.

   A partir de aquí, se le da 'enter' a la opción por defecto 'Interface between PC and Internet [wlan0]' para configurar la interface de red entre la laptop HP y la salida a internet ya que 'wlan0' es la interface de red que corresponde a la conexión inalámbrica entre la laptop y el AP con salida a Internet. Luego, se le da 'enter' a la opción por defecto 'Internet Gateway [192.168.19.254]' para configurar la puerta de enlace que hace referencia a la salida a internet. Para las siguientes últimas dos opciones de configuración que configura la dirección IP del Host (laptop HP) y la del dispositivo Wifi Pineapple, se le da 'enter' a cada una de las opciones 'IP Address of Host PC [172.16.42.42]' y 'IP Address of Pineapple [172.16.42.1]' respectivamente ya

que corresponde con las direcciones IP de la laptop y el Wifi Pineapple. Cabe mencionar que el Wifi Pineapple ya viene configurado con una configuración de red (dirección IP 172.16.42.1 /24) y que al momento de conectarlo, de manera cableada a la PC, logra censar la configuración previamente mencionada. Es por eso que en la mayoría de los casos, solo se le da 'enter' a las opciones de configuración a la hora de realizar una conexión compartida a internet entre el Wifi Pineapple y una PC.

En dado caso que no coincidan las configuraciones por defecto con las configuraciones de red reales, se procede a teclearlas manualmente. Por ejemplo, si la máscara de red es de 255.255.0.0 y si la opción por defecto nos da la siguiente información 'Pineapple Netmask [255.255.255.0]', entonces se procede a teclear '255.255.0.0' para que la configuración coincida con las configuraciones reales de red de los dispositivos en juego.

ii. A partir de este punto, ya se tiene salida a internet desde el Wifi Pineapple atreves de Kali Linux y por consiguiente accedemos a las herramientas de software que trae el Wifi Pineapple vía un navegador web con la dirección 172.16.42.1:1471 e ingresando con la cuenta de administrador.

iii. Ya una vez dentro del sistema operativo del Wifi Pineapple donde se encuentran diferentes herramientas de auditoria de redes inalámbricas, seleccionamos la ventana 'Network' y luego la opción 'Access Point' para cambiar el SSID del AP administrativa y le ponemos una contraseña para asegurarnos que nadie tenga acceso al panel de administración del dispositivo. Dentro de la misma ventana de la opción 'Access Point' se configura la parte 'Open Access Point' con el SSID del AP falso que en este caso llevaría el nombre 'wlcampus' sabiendo que ese es el nombre de la red inalámbrica que queremos atacar y también configuramos el canal de difusión para el SSID falso 'wlcampus'. Una vez realizado lo anterior, se procede a guardar la configuración dándole clic a los dos botones 'Save' y ya se tiene el punto de acceso falso activado.

iv. Salimos de la ventana 'Network' y se le da clic a la ventana 'PineAP'. Seleccionamos la opción 'Karma' para familiarizarnos con el portal de configuración de Karma donde se pueden agregar filtros de SSIDs y filtros a clientes inalámbricos por medio de sus direcciones MAC.

3.1.3 La adquisición de clientes

i. Para esta etapa, se habilita Karma desde el portal principal de administración donde se encuentran todas las opciones y ventanas de configuración y herramientas para que envíe respuestas 'Probe' a los dispositivos inalámbricos en busca de cualquier red inalámbrica al alcance, no importando si es la red inalámbrica 'wlcampus'. En la ventana de 'PineAP', seleccionamos el cuadro a lado del nombre 'MK5 Karma' para habilitar esta herramienta y luego se selecciona el cuadro a lado del nombre 'Probes' y el cuadro a lado del nombre 'Associations', esto es para indicarle a Karma que dé respuesta a peticiones 'Probe' y peticiones de asociación a los dispositivos

inalámbricos en busca de la red legitima ***wlcampus*** y cualquier otra red inalámbrica al alcance.

ii. Para finalizar la etapa 3, solo queda esperar a que clientes inalámbricos se empiecen a conectar ya sea de manera voluntaria o a través de las respuestas 'Probe' y 'Associations' que la herramienta Karma empiece a difundir para conectar clientes al AP falso de manera automática. Hasta este punto el ataque 'Roge AP' se extiende a un ataque 'Man In The Middle'.

3.1.4 La intercepción de tráfico de red

Con la implementación exitosa del ataque MITM el atacante puede ahora interceptar el tráfico que pasa por el AP falso en el Wifi Pineapple. Hay muchas herramientas disponibles para realizar la tarea, como Wireshark y Tcpdump pero el propósito de un ataque MITM es capturar la información sensible que los clientes envían y reciben a través de la red en lugar de capturar todo el tráfico. La mayoría de los sitios web que requieren credenciales del cliente, como la banca en línea y redes sociales, por lo general protegen su sesión mediante el protocolo de transferencia de hipertexto seguro (HTTPS). Cualquier trama HTTPS capturado requerirá trabajo extra con el fin de descifrar esas tramas y recuperar la información. El ataque MITM da la oportunidad de que el atacante intercepte esas credenciales sin descifrar cualquier trama HTTPS en absoluto.

Con el objetivo de interceptar sólo los datos valiosos de todo el tráfico, un conjunto de herramientas será utilizado, la combinación de sslstrip, urlsnarf y tcpdump. Sslstrip es una herramienta que evita que un navegador web actualice su conexión regular a una conexión protegida SSL. Además sslstrip crea un certificado válido falso imitando el servidor web que el cliente está tratando de conectarse. Con este modo, el navegador es engañado que la conexión es segura y no hay ninguna advertencia de que la sesión ha sido secuestrada.

La segunda herramienta utilizada en el experimento es urlsnarf. Urlsnarf es una herramienta que escucha sigilosamente peticiones HTTP en formato común de registro (Common Log Format). Urlsnarf muestra todas las solicitudes de URLs interceptadas de tráfico HTTP en un formato de registro común ideal para un análisis no en línea con alguna herramienta de análisis de registros web. Con esta herramienta se pueden conocer todas las URLs de las páginas web que en el instante se están visitando por los clientes (víctimas) del AP falso.

Ettercap es una herramienta que se utiliza para el análisis de protocolos de red y es capaz de interceptar el tráfico, así como realizar espionaje activo en una serie de protocolos. Ettercap tiene cuatro modos de funcionamiento: modo IP, modo MAC, modo ARP y el modo PublicARP. En este experimento el modo IP se utilizará y todo el tráfico de la interfaz 'wlan0' que apunta hacia la víctima será interceptada.

i. Para esta etapa, una vez que los clientes/usuarios inalámbricos se estén conectando al punto de acceso falso, se habilita la herramienta sslstrip al darle clic al texto que dice 'Start' en la ventana llamado 'sslstrip' desde el portal principal de administración del Wifi Pineapple.

ii. Una vez que se habilito la herramienta sslstrip, se procede a habilitar la herramienta urlsnarf. Desde el portal principal de administración, primero se le dio clic al menú desplegable en la ventana llamado ´urlsnarf´ y se seleccionó la interfaz 'wlan0' ya que esa es la interfaz donde se encuentran conectados los usuarios inalámbricos y que hace referencia al punto de acceso falso. Luego de haber seleccionado la interfaz 'wlan0', se le dio clic al texto que dice 'Start' en la misma ventana 'urlsnarf'.

iii. Una vez que se habilitaron las herramientas sslstrip y urlsnarf, seleccionamos la ventana 'sslstrip' para entrar al portal de configuración de la herramienta. Ya dentro del portal de configuración se exploran las opciones 'Output' y 'History' para poder ver el tráfico de red que la herramienta está interceptando en ese mismo instante. Lo mismo aplica para la herramienta urlsnarf, seleccionamos la ventana 'urlsnarf' para entrar al portal de configuración de la herramienta. Ya dentro del portal de configuración se exploran las opciones 'Output' y 'History' para poder ver el tráfico de red que la herramienta está interceptando en ese mismo instante.

iv. Se conecta la laptop Macbook Pro al AP falso para que genere tráfico web y se pueda verificar en tiempo real que las herramientas sslstrip y urlsnarf intercepte el trafico HTTP/HTTPS que la laptop cliente genere.

v. Después de un tiempo transcurrido, se deshabilita sslstrip y urlsnarf al darle clic al texto que dice 'Stop' en el rectángulo de opción con nombre 'Controls' del portal de configuración de sslstrip y también del portal de configuración de urlsnarf.

vi. A partir de este punto se accede a la opción 'History' del portal de configuración de sslstrip y urlsnarf para ver el tráfico web que fue interceptado de una manera ordenada al darle clic al texto 'view'. Luego se le da clic en el texto 'download' para descargar el archivo .log donde se encuentra almacenada todo el tráfico interceptado por sslstrip y urlsnarf para poder analizarlo por separado y sin necesidad de estar conectados al Wifi Pineapple o Internet.

Ilustración 37: Mapa de la UQROO, Campus Chetumal, donde se llevó acabo Pentesting

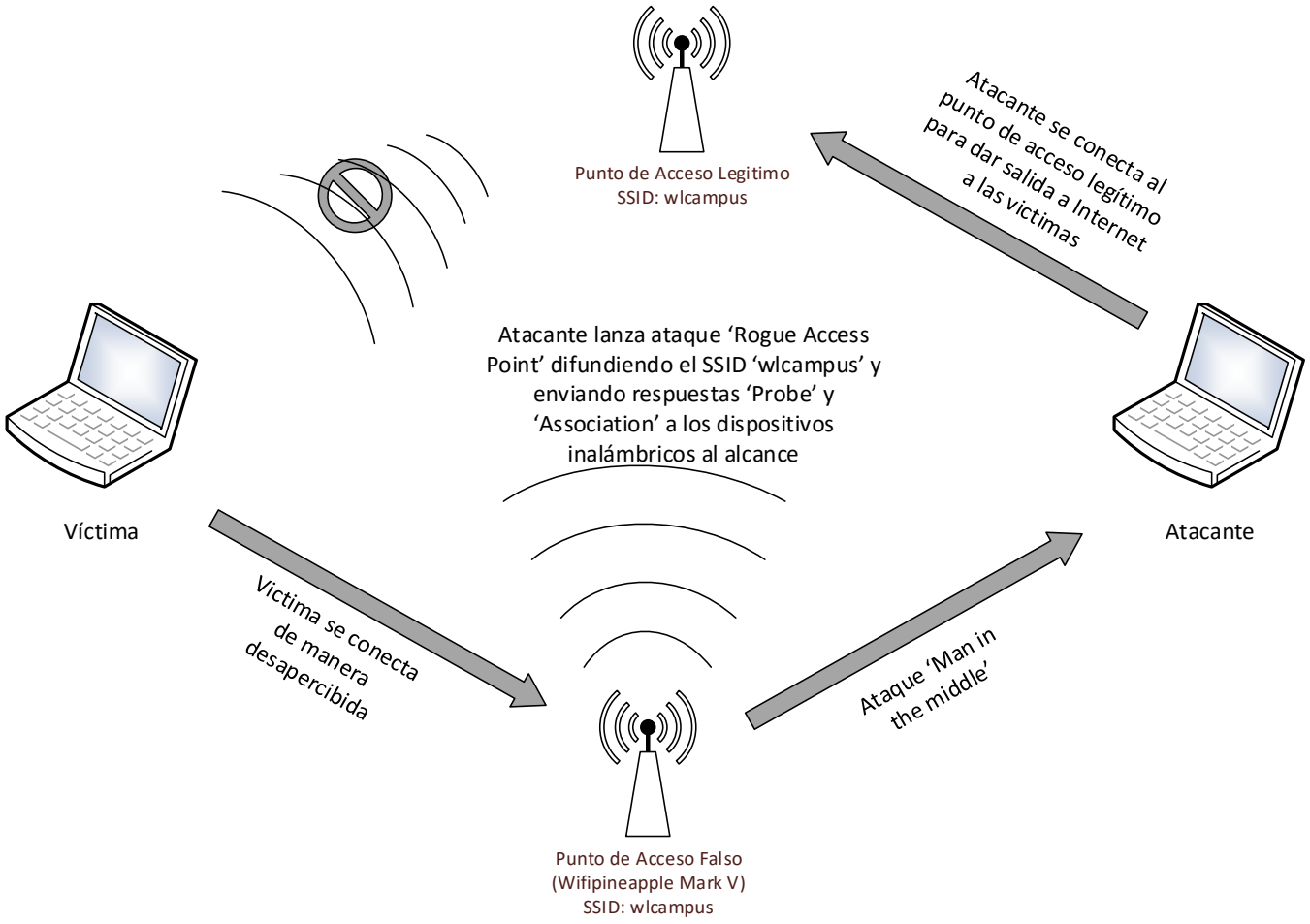

Ilustración 38: Topología de red del ataque 'Rogue Access Point.'

3.2 Fase 1

Para la primera etapa que hace referencia a la recopilación de información, primero se configuró la tarjeta de red Alfa AWUS036H con la antena de 18 dBi en modo monitor y a una potencia de transmisión de 30 dBm (1000 mW) para que tenga un mayor alcance en cuanto a cobertura de la señal inalámbrica.

Después de conectar la tarjeta Alfa a la laptop HP a través de una conexión USB, se verificó que Kali Linux 2.0 reconozca y acepte la tarjeta de red con el nombre de interface 'wlan3' a través del comando 'iwconfig' como se muestra en la Ilustración 39.

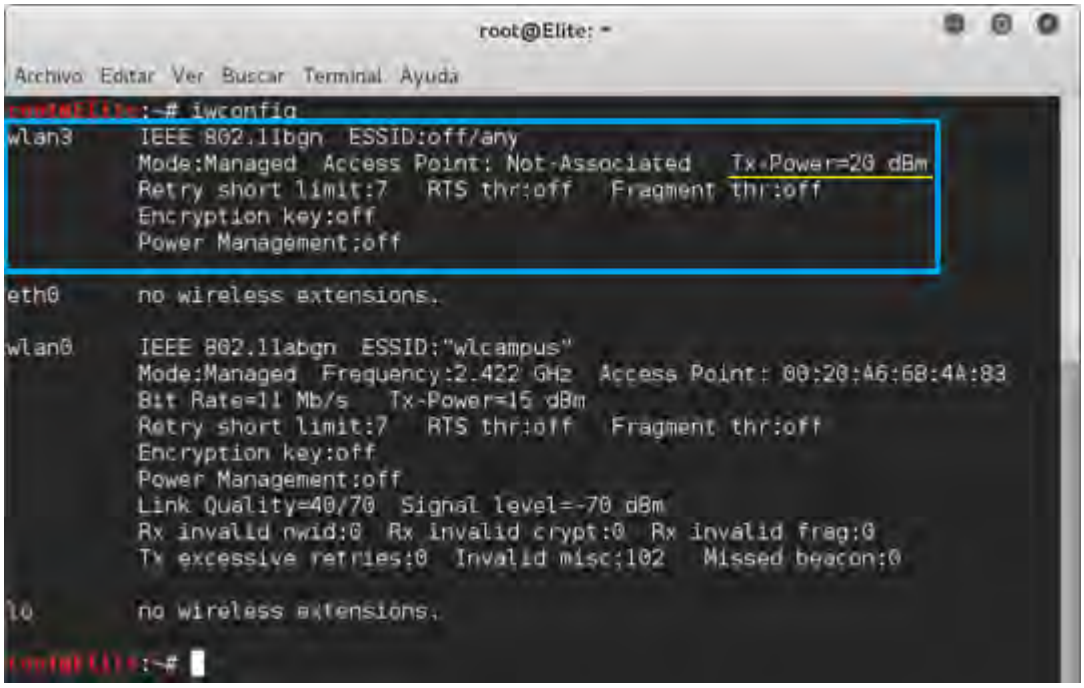

Ilustración 39: Ejecución del comando iwconfig.

A la hora de cambiar la potencia de transmisión de una tarjeta de red inalámbrica, cada país tiene unas leyes que regulan las frecuencias en las que se pueden trabajar y la potencia con la que puede hacerlo. El comando 'iw reg get', de acuerdo a la Ilustración 40, se ejecutó para ver el código del país que se tiene configurado con las frecuencias y su respectiva potencia de transmisión ('Tx-Power=20 dBm') que se pueden configurar en una tarjeta de red inalámbrica. Para este caso, no se tenía ninguna configuración que hace referencia a un código de algún país y por lo tanto, se listan todas las posibles frecuencias y potencia de transmisión que se pueden configurar en una tarjeta de red.

Ilustración 40: Ejecución del comando 'iw reg get'

De acuerdo con la Ilustración 41, para cambiar la potencia de transmisión de la tarjeta de red Alfa AWUS036H primero se ejecutó el comando 'iw reg set ISO_3166-1_alpha-2' que inicializa la configuración exclusivamente para la tarjeta Alfa. Luego se ejecutó el comando 'iw reg set

US' que configura el administrador de las conexiones inalámbricas en Kali Linux y le indica a la tarjeta que puede utilizar únicamente todas las frecuencias y potencias de transmisión asignadas al país de Los Estados Unidos expresado con la abreviación 'US'. El comando 'iw reg get' se utiliza nuevamente para verificar que efectivamente se configuró las frecuencias y potencias de transmisión asignadas a los Estados Unidos y puedan ser utilizados para futuras configuraciones de cualquier tarjeta de red inalámbrica. Cabe mencionar que se configuro Kali Linux para que utilice las frecuencias y potencias de transmisión de los E.E.U.U ya que brinda la opción de poder configurar la tarjeta Alfa para una potencia de transmisión de 30 dbm para la frecuencia inalámbrica de Wifi de 2.5 GHz.

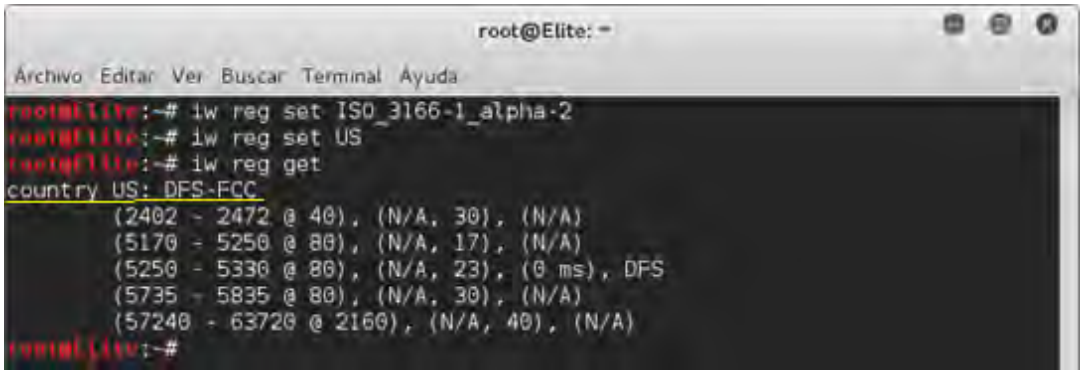

Ilustración 41: Ejecución de los comandos 'iw reg set ISO_3166-1_alpha-2', 'iw reg set US' y 'iw reg get'.

Antes de que se configurara la potencia de transmisión a 30 dBm de la tarjeta Alfa, se ejecutó el comando 'ifconfig wlan3' que verificó que la interface 'wlan3' (Alfa AWUS036H) estaba habilitado. De acuerdo a la Ilustración 42, la siguiente información 'UP BROADCAST MULTICAST' indicó que la interface 'wlan3' estaba habilitado y se tenía que deshabilitar para configurar la potencia de transmisión (txpower) de la tarjeta Alfa. Por consiguiente, la interfaz 'wlan3' se deshabilito con el comando 'ifconfig wlan3 down' y para verificar que se deshabilitó, se utilizó el comando 'ifconfig wlan 3' nuevamente. De acuerdo a la Ilustración 41, la siguiente información 'BROADCAST MULTICAST' indicó que la interfaz 'wlan3' se encuentra deshabilitada. A partir de este punto, se configuró el 'txpower' de la tarjeta de red Alfa a través del comando 'iwconfig wlan3 txpower 30' y luego se habilito nuevamente la interfaz 'wlan3' con el comando 'ifconfig wlan3 up'.

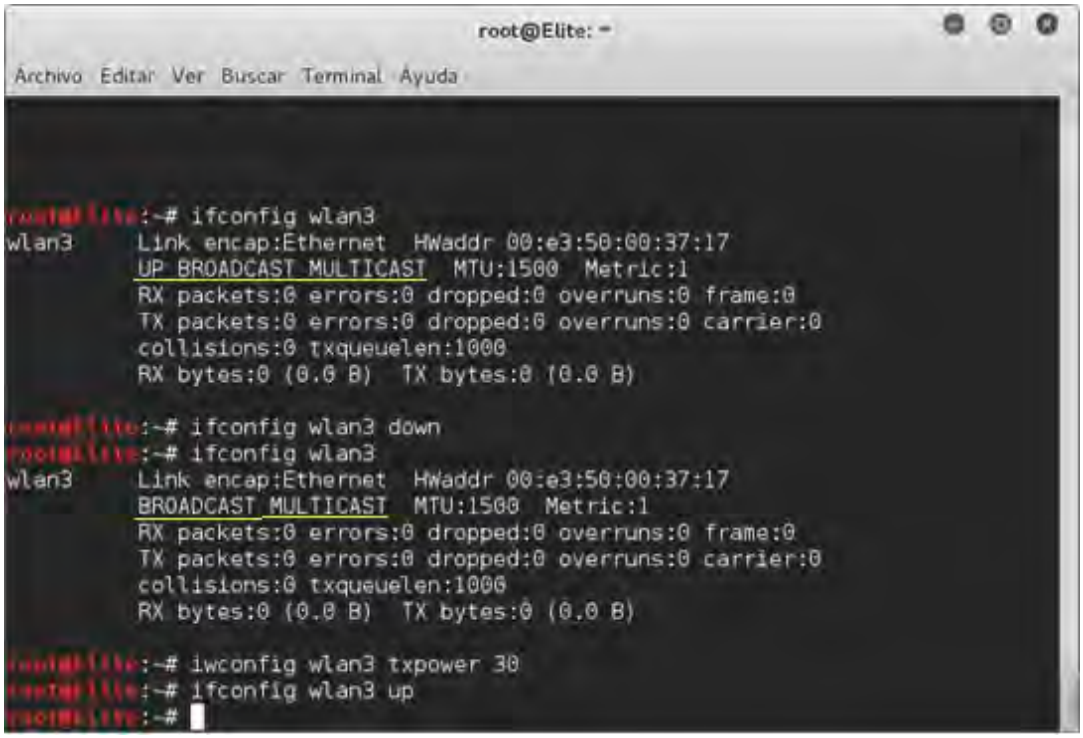

Ilustración 42: Ejecución de los comandos 'ifconfig wlan3', 'ifconfig wlan3 down', 'iwconfig wlan3 txpower 30' y 'ifconfig wlan3 up'.

Después de habilitar la interfaz ‘wlan3’ se ejecutó el comando ‘iwconfig’ que proporciona información de todas las interfaces de red que Kali Linux administra. De acuerdo a la Ilustración 43, se pudo observar que la configuración realizada previamente para cambiar la potencia de transmisión de la tarjeta Alfa se creó exitosamente ya que para la interfaz ‘wlan3’, el ‘txpower’ cambió de 20 dBm a 30 dBm.

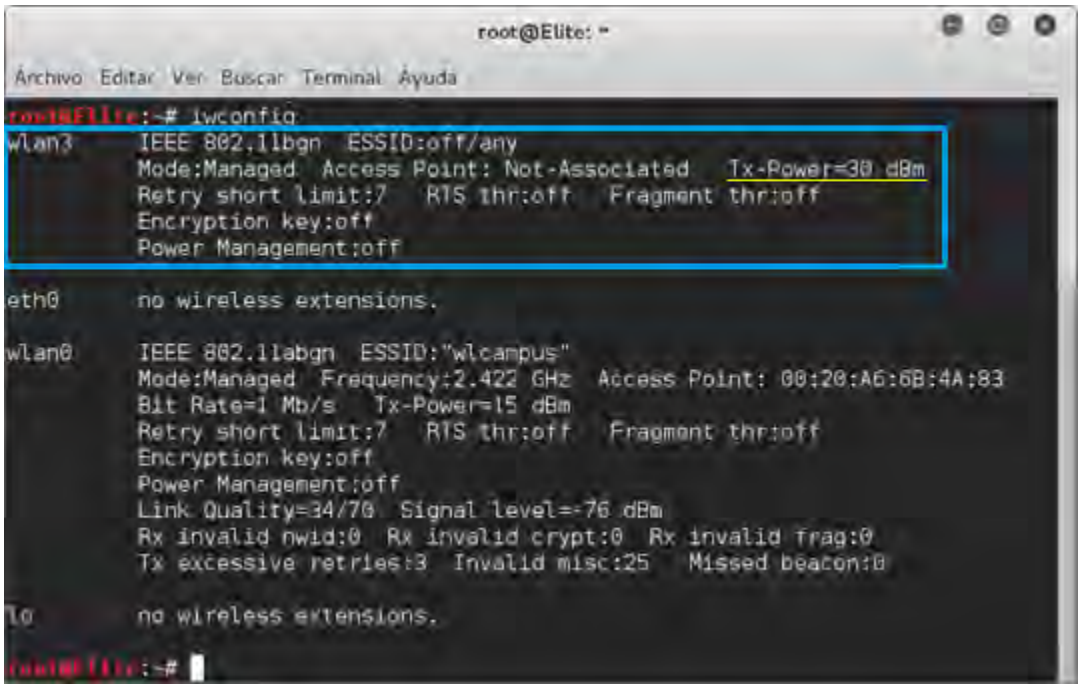

Ilustración 43: Ejecución del comando 'iwconfig'.

De otra parte, se configuró la interfaz ‘wlan3’, que hace referencia a la tarjeta Alfa, en modo monitor a través del comando ‘airmon-ng start wlan3’ para llevar a cabo el proceso de reconocimiento pasivo del entorno inalámbrico. En la parte inferior de la Ilustración 44 muestra la siguiente información ‘mac80211 monitor mode vif enabled for [phy1]wlan3 on [phy1] wlan3mon’ que indica que la interfaz ‘wlan3’ se habilito para funcionar en modo monitor con un nuevo nombre de interfaz ‘wlan3mon’. La Ilustración 45 muestra que se ejecutó el comando ‘iwconfig’ que proporciona la siguiente información ‘Mode:Monitor’ indicando que se habilito el interfaz ‘wlan3’ en modo monitor.

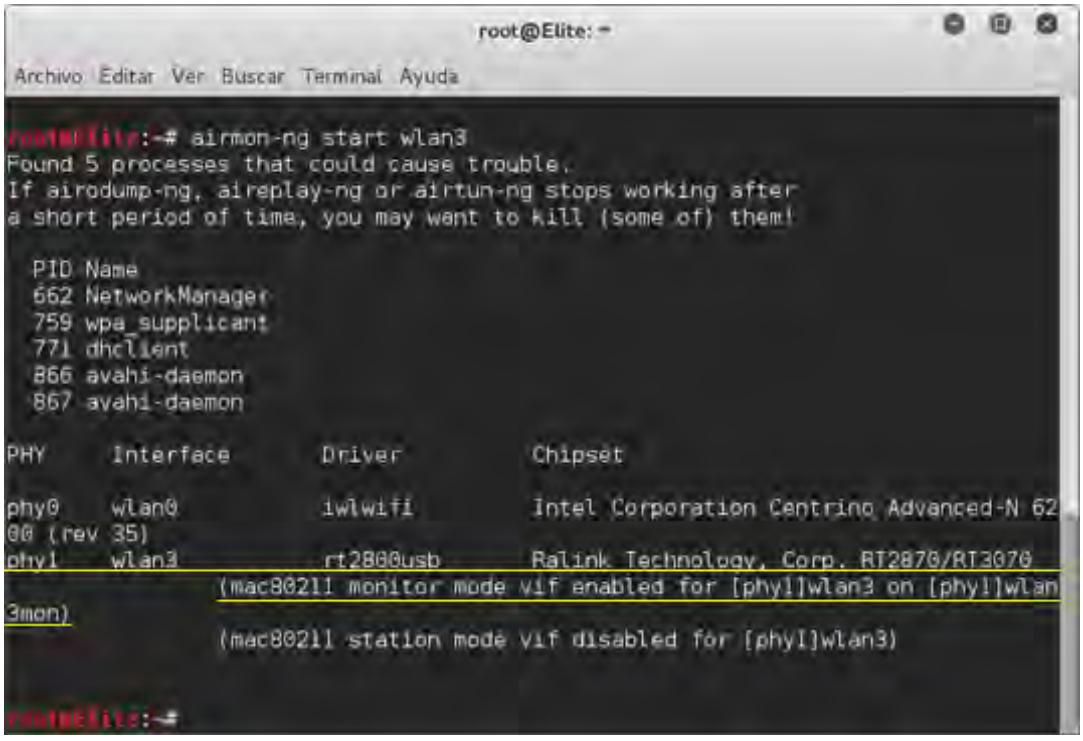

Ilustración 44: Ejecución del comando 'airmon-ng start wlan3'.

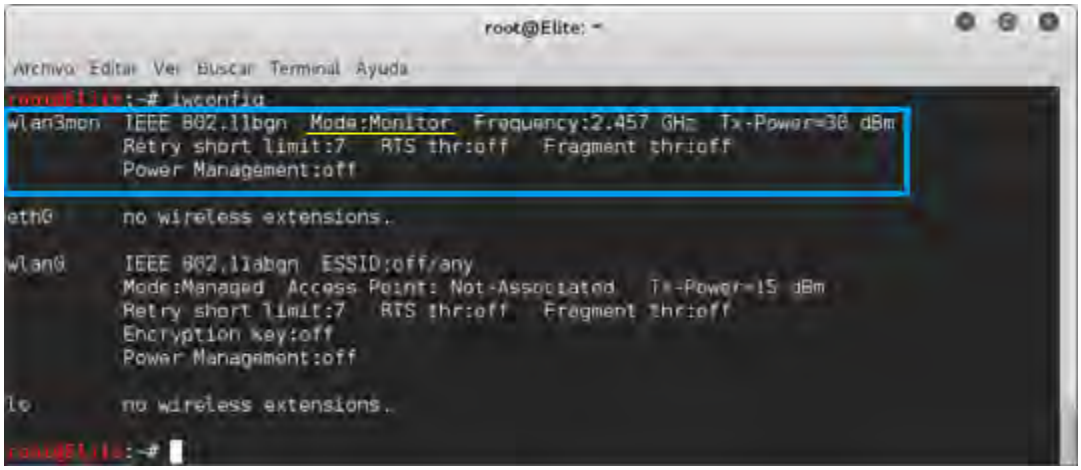

Ilustración 45: Ejecución del comando 'iwconfig'.

La siguiente Ilustración 46 muestra la ejecución del comando ‘airodump-ng wlan3mon’ para capturar paquetes inalámbricos 802.11 y como consecuencia mostrar una lista de los puntos de acceso detectados y también una lista de los clientes conectados pero no se pudo ejecutar el comando con éxito. Lo mencionado anterior se debe a que el administrador de red de Kali Linux (Network Manager) es inestable cuando gestiona los diferentes modos inalámbricos (managed, monitor, ad hoc etc.) a diferentes interfaces y ciertos comandos relacionado con alguna configuración de red suelen no tener éxito al momento de su ejecución. De acuerdo a lo antes mencionado, se ejecutó el comando ‘iwconfig wlan3mon’ que comprueba lo dicho anteriormente

ya que en el paso anterior, la interfaz ‘wlan3mon’ se encontraba en modo monitor y después de haber ejecutado el comando ‘airodump-ng wlan3mon’, el administrador de red de Kali Linux cambió la interfaz a modo ‘managed’. Para corregir este problema, primero se ejecutó el comando ‘ifconfig wlan3mon down’ para deshabilitar el interfaz ‘wlan3mon’. Luego se ejecutó el comando ‘iwconfig wlan3mon mode monitor’ para configurar la interfaz ‘wlan3mon’ en modo monitor. También, se ejecutó el comando ‘ifconfig wlan3mon up’ para nuevamente habilitar la interfaz y luego se ejecutó el comando ‘iwconfig wlan3mon’ donde se pudo observar claramente que la interfaz ‘wlan3mon’ se encuentra habilitado en modo monitor como se muestra en la Ilustración 47.

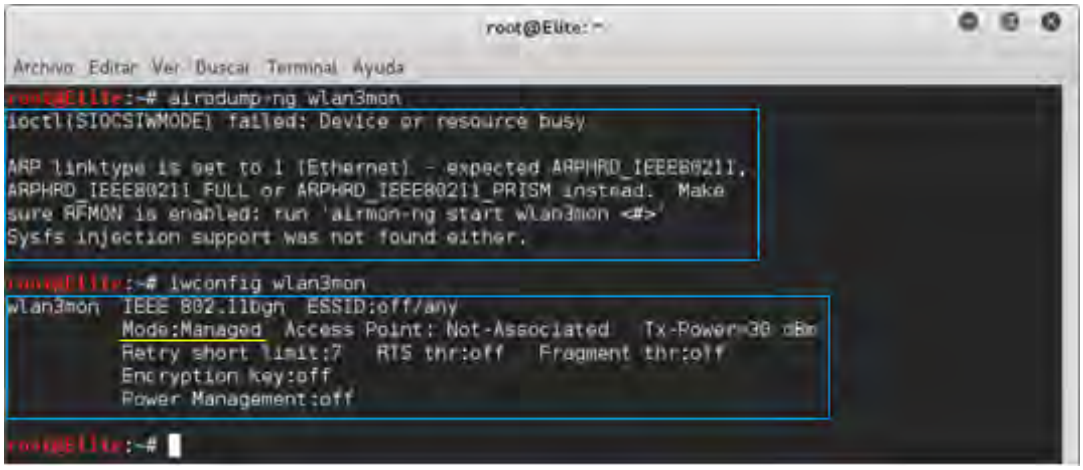

Ilustración 46: Ejecución de los comandos 'airodump-ng wlan3mon' y ‘iwconfig wlan3mon’.

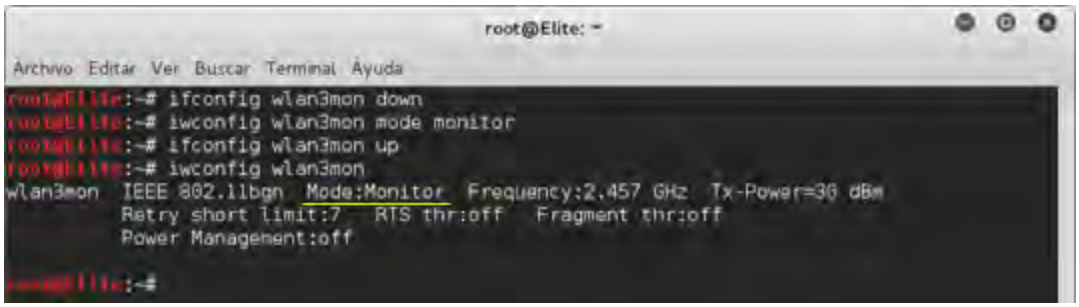

Ilustración 47: Ejecución de los comandos 'ifconfig wlan3mon down', 'iwconfig wlan3mon mode monitor´, 'ifconfig wlan3mon up' y 'iwconfig wlan3mon'.

A través de la herramienta ‘airodump-ng’, se inició el proceso de reconocimiento pasivo del entorno inalámbrico a través de la captura general de tráfico de red inalámbrica para la obtención de información valiosa que es necesaria para realizar el ataque ‘Rogue AP’ a la red inalámbrica ‘wlcampus’. Después de corregir el problema que se presentó en el paso anterior, la Ilustración 48 muestra la ejecución del comando ‘airodump-ng wlan3mon para capturar paquetes inalámbricos 802.11. La Ilustración 49, 50 y 51 muestran una lista de los puntos de acceso detectados para diferentes canales de transmisión. Los datos proporcionados por ‘airodump-ng’ ayudaron a obtener la siguiente información: ESSID, BSSID, potencia de la señal (PWR), tipo de autenticación (AUTH), tipo de cifrado (CIPHER), canal de transmisión (CH),

modo de cifrado (ENC) entre otra información. En la lista de puntos de acceso detectados, se pudo observar que tres APs con BSSIDs 00:1F:45:63:2C:20, 00:1F:45:20:F4:B0 y 00:20:A6:6B:4A:83 difundían la red inalámbrica 'wlcampus' para los canales 6, 8 y 3 respectivamente. También, en la Ilustración 49 y 50 se muestra que el modo de autenticación para los APs que difunden la red 'wlcampus' es en modo abierto sin ningún tipo de autenticación ni cifrado.

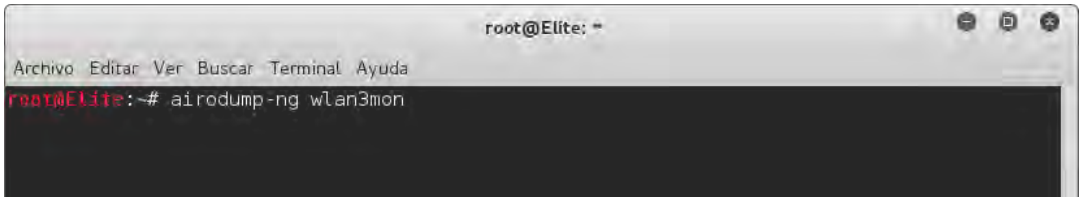

Ilustración 48: Ejecución del comando 'airodump-ng wlan3mon´.'

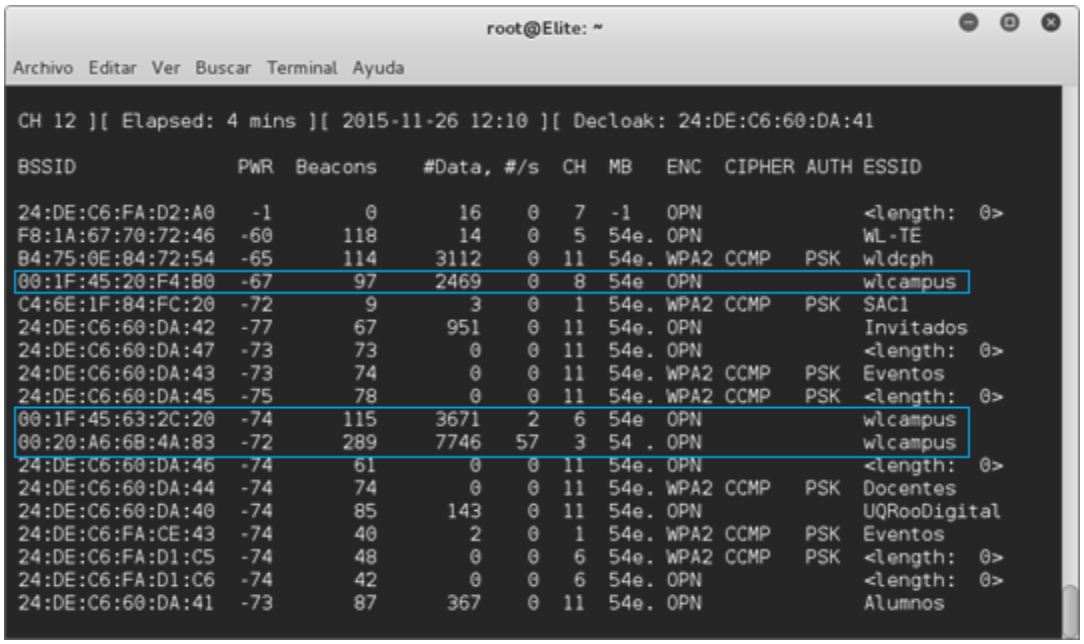

Ilustración 49: Información del entorno inalámbrico generado por la herramienta airodump-ng.

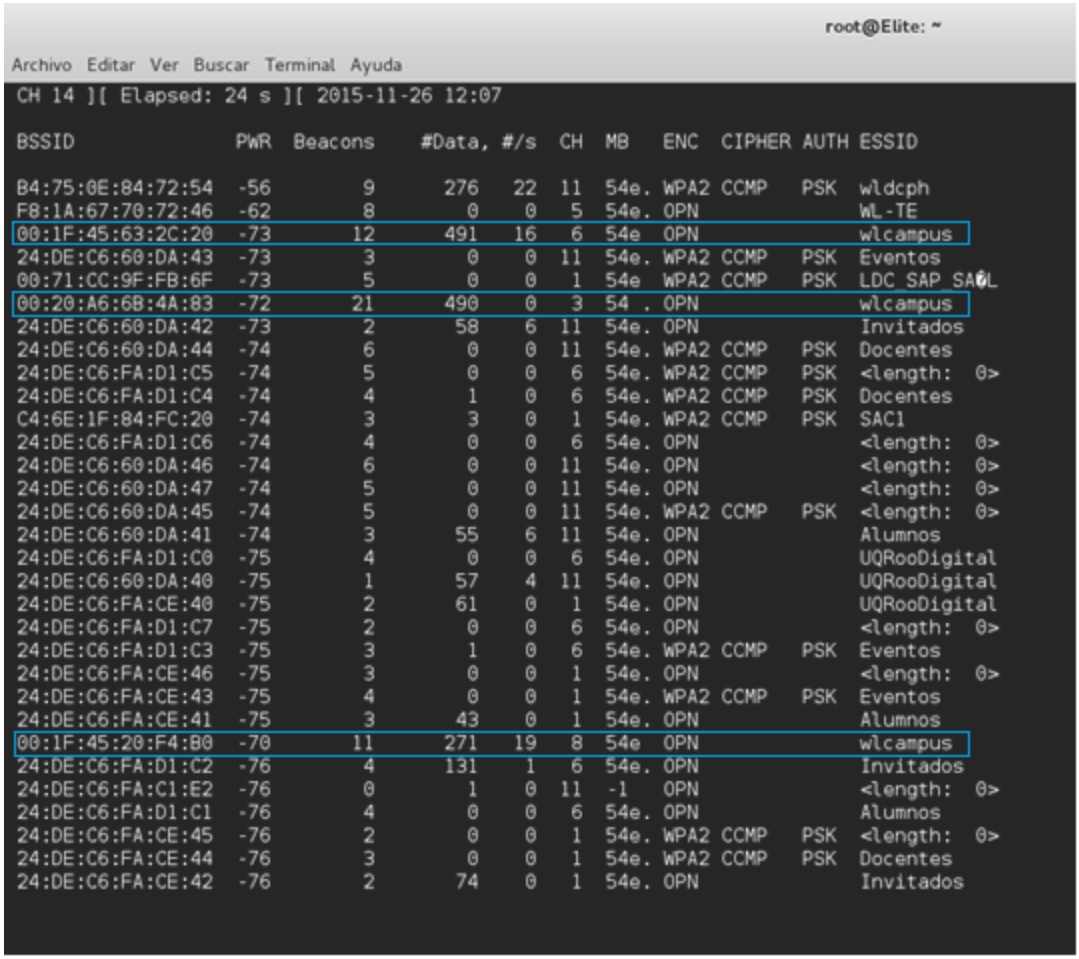

Ilustración 50: Información del entorno inalámbrico generado por la herramienta airodump-ng.

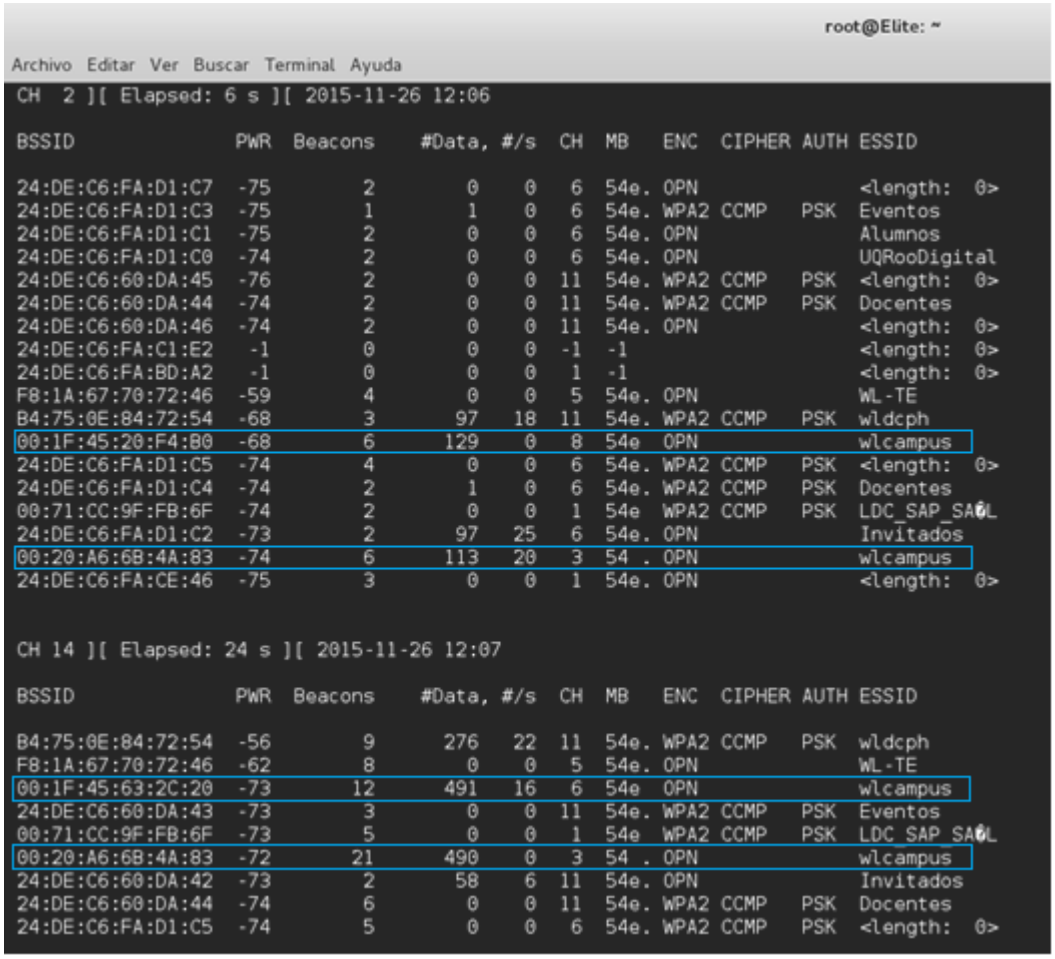

Ilustración 51: Información del entorno inalámbrico generado por la herramienta airodump-ng.

De acuerdo a la Ilustración 52, para monitorear el AP con BSSID 00:1F:45:63:2C:20 que difunde la red inalámbrica ‘wlcampus’, se ejecutó el comando 'airodump-ng -c 6 --bssid 00:1F:63:2C:20 wlan3mon' donde ‘-c’ indica el comienzo de la configuración del canal de transmisión seguido por el número del canal que es 6. Luego, los caracteres ‘--bssid’ indica el comienzo de la configuración del BSSID del AP seguido por su dirección MAC 00:1F:63:2C:20 para monitorear exclusivamente el punto de acceso mencionado sobre el canal 6 y por último ‘wlan3mon’ indica la interfaz que se utilizó para llevar a cabo el monitoreo. Después de ejecutar el comando mencionado anteriormente, se inicia una captura de tráfico de red únicamente para el AP con BSSID 00:1F:45:63:2C:20 y la herramienta ‘airodump-ng’ al momento que captura y analiza los paquetes, arroja una ventana con una lista de clientes conocido como ‘STATION’ como se muestra en la Ilustración 53. En la Ilustración 53, se puede observar en la parte superior que la herramienta ‘airodump-ng’ también proporciona información del AP en cuestión y en la parte inferior proporciona información tal como potencia de la señal para transmitir (PWR), tramas recibidas (Frames), paquetes perdidos (Lost), tasa de transmisión (Rate), BSSID y las tramas ‘Probe’ de los clientes conectados al AP.

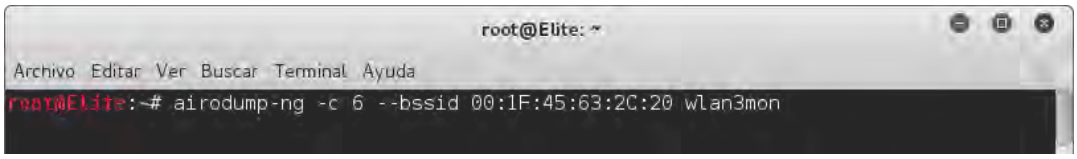

Ilustración 52: Ejecución del comando 'airodump-ng -c 6 --bssid 00:1F:63:2C:20 wlan3mon'.

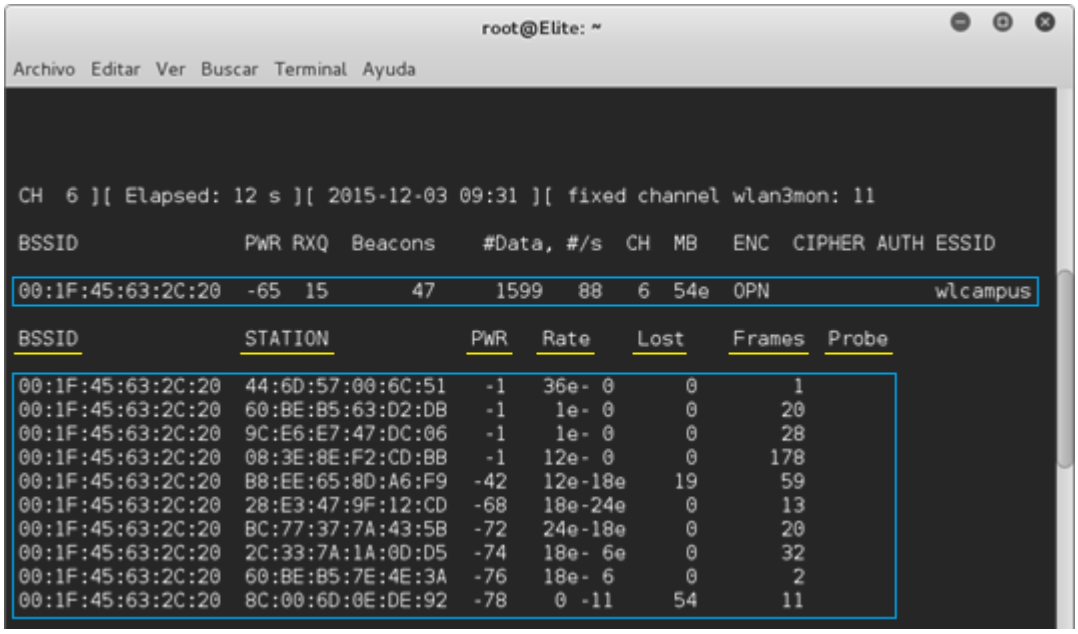

Ilustración 53: Información de la lista de clientes para un AP que difunde la red 'wlcampus'.

De acuerdo a la Ilustración 54, para monitorear el AP con BSSID 00:1F:45:20:F4:B0 que difunde la red inalámbrica ‘wlcampus’, se ejecutó el comando 'airodump-ng -c 8 --bssid 00:1F:45:20:F4:B0 wlan3mon' donde ‘-c’ indica el comienzo de la configuración del canal de transmisión seguido por el número del canal que es 8. Luego, los caracteres ‘--bssid’ indica el comienzo de la configuración del BSSID del AP seguido por su dirección MAC 00:1F:45:20:F4:B0 para monitorear exclusivamente el punto de acceso mencionado sobre el canal 8 y por último ‘wlan3mon’ indica la interfaz que se utilizó para llevar a cabo el monitoreo. Después de ejecutar el comando mencionado anteriormente, se inicia una captura de tráfico de red únicamente para el AP con BSSID 00:1F:45:20:F4:B0 y la herramienta ‘airodump-ng’ al momento que captura y analiza los paquetes, arroja una ventana con una lista de clientes conocido como ‘STATION’ como se muestra en la Ilustración 55. También, de acuerdo la Ilustración 55, se puede observar en la parte superior que la herramienta ‘airodump-ng’ también proporciona información del AP en cuestión y en la parte inferior proporciona información tal como potencia de la señal para transmitir (PWR), tramas recibidas (Frames), paquetes perdidos (Lost), tasa de transmisión (Rate), BSSID y las tramas ‘Probe’ de los clientes conectados al AP.

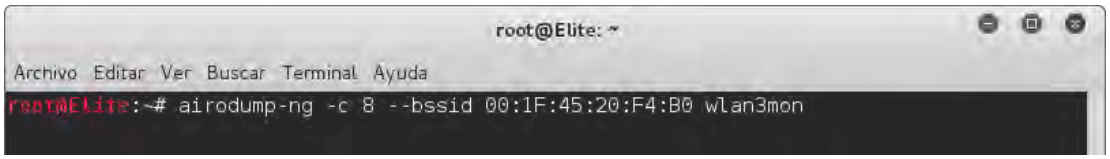

Ilustración 54: Ejecución del comando 'airodump-ng -c 6 --bssid 00:1F:45:20:F4:B0 wlan3mon'.

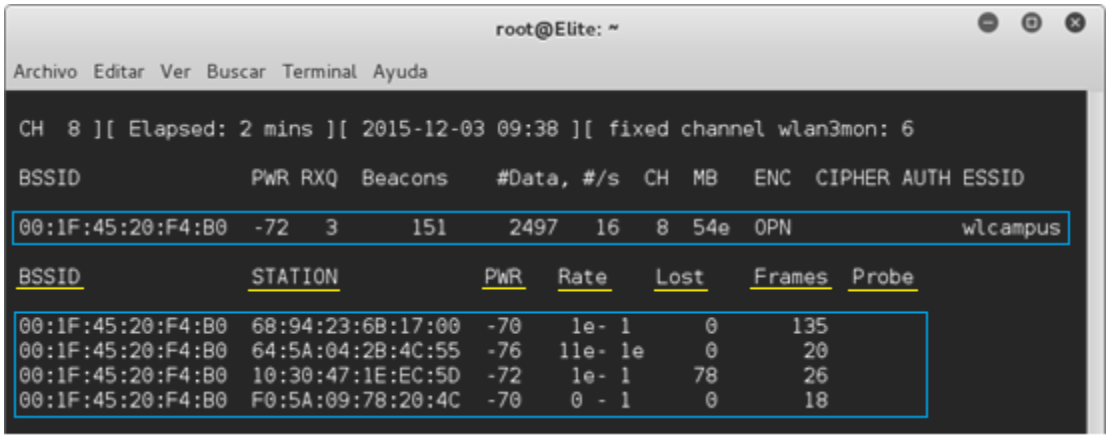

Ilustración 55: Información de la lista de clientes para un AP que difunde la red 'wlcampus'.

De acuerdo a la Ilustración 56, para monitorear el AP con BSSID 00:20:A6:6B:4A:83 que difunde la red inalámbrica 'wlcampus', se ejecutó el comando 'airodump-ng -c 3 --bssid 00:20:A6:6B:4A:83 wlan3mon' donde '-c' indica el comienzo de la configuración del canal de transmisión seguido por el número del canal que es 3. Luego, los caracteres '--bssid' indica el comienzo de la configuración del BSSID del AP seguido por su dirección MAC 00:20:A6:6B:4A:83 para monitorear exclusivamente el punto de acceso mencionado sobre el canal 3 y por último 'wlan3mon' indica la interfaz que se utilizó para llevar a cabo el monitoreo. Después de ejecutar el comando mencionado anteriormente, se inicia una captura de tráfico de red únicamente para el AP con BSSID 00:20:A6:6B:4A:83 y la herramienta 'airodump-ng' al momento que captura y analiza los paquetes, arroja una ventana con una lista de clientes conocido como 'STATION' como se muestra en la Ilustración 57. También, de acuerdo la Ilustración 57, se puede observar en la parte superior que la herramienta 'airodump-ng' también proporciona información del AP en cuestión y en la parte inferior proporciona información tal como potencia de la señal para transmitir (PWR), tramas recibidas (Frames), paquetes perdidos (Lost), tasa de transmisión (Rate), BSSID y las tramas 'Probe' de los clientes conectados al AP.

Ilustración 56: Ejecución del comando 'airodump-ng -c 6 --bssid 00:20:A6:6B:4A:83 wlan3mon'.

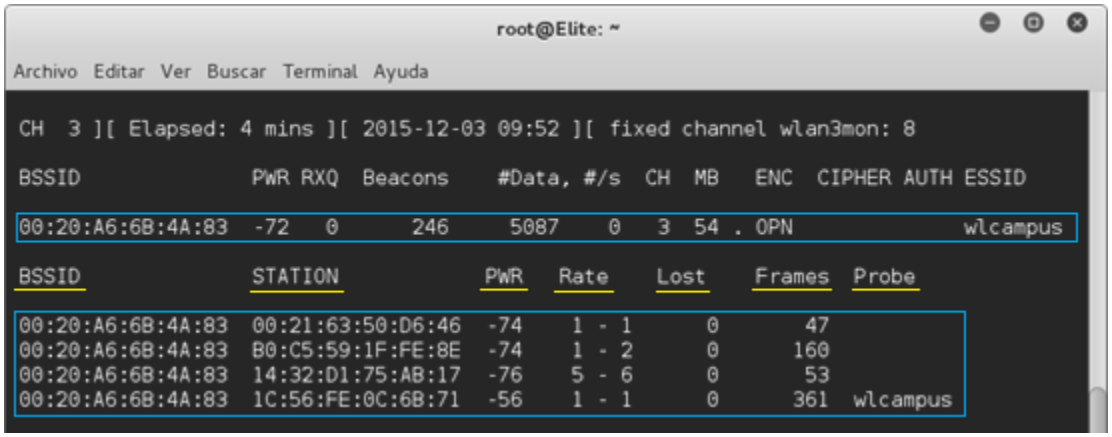

Ilustración 57: Información de la lista de clientes para un AP que difunde la red 'wlcampus'.

Para reforzar los pasos anteriores y comprobar que la información recopilada con la herramienta aircrack-ng es confiable, se llevó a cabo un barrido de todas las señales WiFi con el dispositivo WiFi Pineapple Mark V. De acuerdo a la Ilustración 58, desde una línea de comando se ejecutó el comando 'service Network Manager start' para asegurarnos que el administrador de red de Kali Linux esté activo. Luego se ejecutaron los comandos 'service ssh start' y 'service ssh status' respectivamente para activar el servicio SSH y también para verificar que el servicio se encuentre activo. A partir de este punto, se ejecutó el comando 'ssh root@172.16.42.1' para establecer una conexión segura (cifrada) entre el Wifi Pineapple y Kali Linux y luego se procedió a ingresar la contraseña de administrador del Wifi Pineapple para ingresar al sistema y realizar alguna configuración o utilizar alguna herramienta de auditoria de red. Una vez que se ingresó al sistema del dispositivo, se ejecutó el comando 'site_survey 300' donde el Wifi Pineapple utiliza la herramienta site survey para realizar un barrido de red del entorno inalámbrico por 300 segundos como se puede observar en la Ilustración 59. Al culminar el tiempo de ejecución de la herramienta 'site_survey', la Ilustración 60, 61, 62, 63 y 64 muestra en la línea de comandos la información como BSSID, ESSID, tipo de cifrado, potencia de la señal y canal de todos los puntos de acceso captados con sus respectivos clientes y también nos muestra los clientes que no están conectados a ningún punto de acceso pero que andan en busca de una red inalámbrica cercana al cual puedan conectarse.

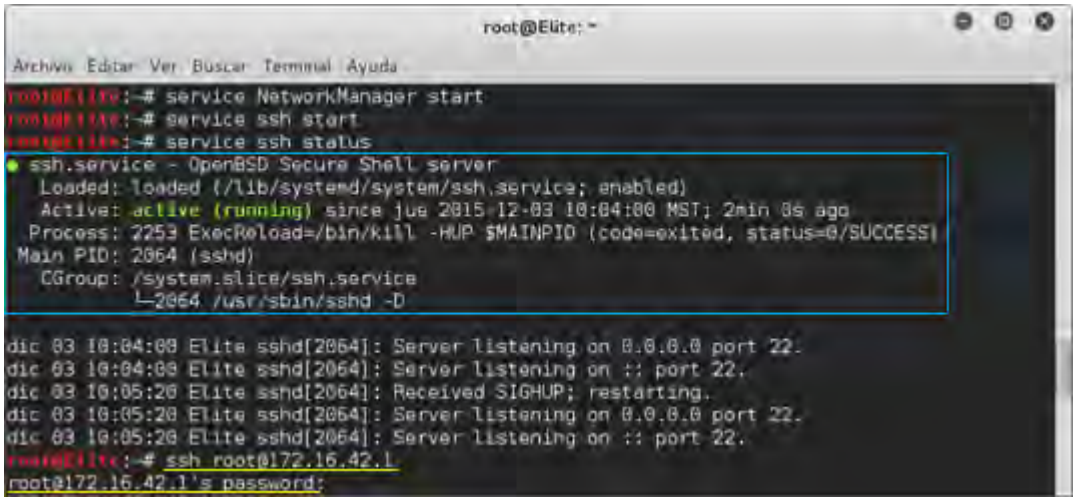

Ilustración 58: Ejecución de comandos para ignresar al Wifi Pineapple Mark V a través de la linea de comandos.

Ilustración 59: Ejecución del comando 'site_survey 300' utilizando el Wifi Pineapple Mark V.

En la Ilustración 60, se observó que el Wifi Pineapple detectó el AP con BSSID 00:1F:45:63:2C:20 que difunde la red 'wlcampus' con los clientes inalámbricos conectados a ella. También, se observó otra información como tipo de seguridad implementada (Security: Open), potencia de la señal inalámbrica (Signal: 32%) y el canal de difusión (Channel: 6). Esto concuerda con la información proporcionada por la herramienta 'airodump-ng' que se utilizó previamente para monitorear la red inalámbrica 'wlcampus'. Es importante mencionar que a cuando hizo el monitoreo y el 'sniffing' de la red 'wlcampus', a medida que el tiempo transcurre, ciertos clientes se desconectan y otros nuevos clientes se conectan a la red. Esto se puede observar comparando el número de clientes que nos proporcionó la herramienta 'airodump-ng'

que es menor de acuerdo a la Ilustración 53 con el número de clientes que nos mostró la herramienta 'site survey' de acuerdo con la Ilustración 60 y 61 para el mismo punto de acceso.

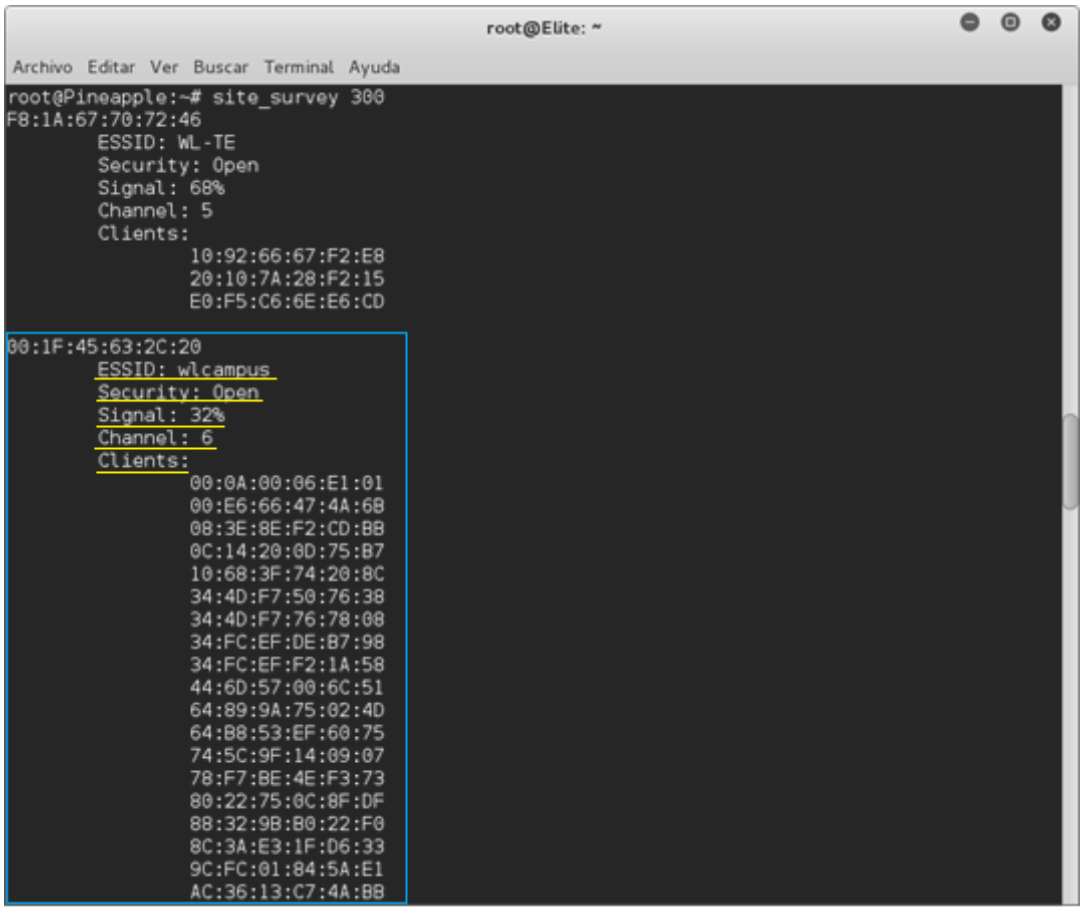

Ilustración 60: Lista de APs con sus respectivos clientes.

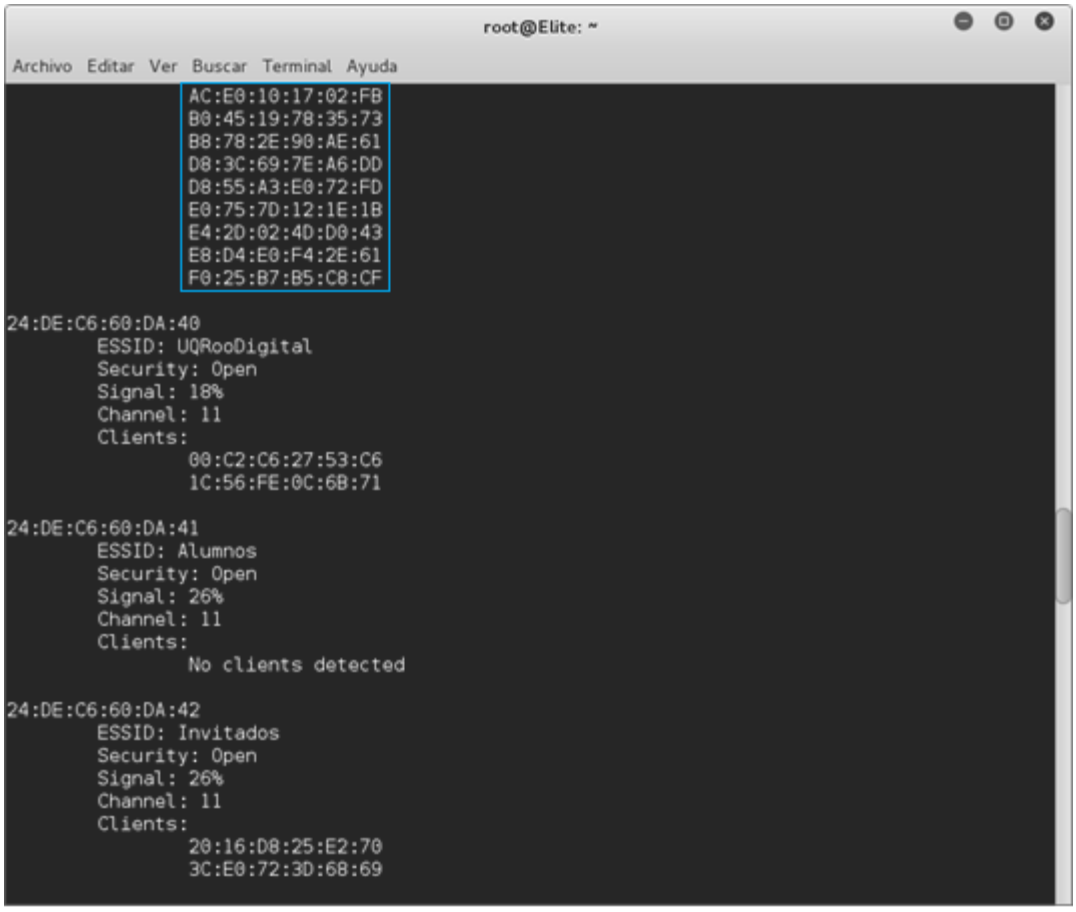

Ilustración 61 (Continuación): Lista de APs con sus respectivos clientes.

En la Ilustración 62, se observó que el Wifi Pineapple detectó también el AP con BSSID 00:20:A6:6B:4A:83 que difunde la red 'wlcampus' con sus respectivos clientes inalámbricos conectados a ella. También, se observó otra información como tipo de seguridad implementada (Security: Open), potencia de la señal inalámbrica (Signal: 26%) y el canal de difusión (Channel: 3). Esto concuerda con la información proporcionada por la herramienta 'airodump-ng' que se utilizó previamente para monitorear la red inalámbrica 'wlcampus'. Es importante mencionar que a cuando hizo el monitoreo y el 'sniffing' de la red 'wlcampus', a medida que el tiempo transcurre, ciertos clientes se desconectan y otros nuevos clientes se conectan a la red. Esto se puede observar comparando el número de clientes que nos proporcionó la herramienta 'airodump-ng' que es menor de acuerdo a la Ilustración 57 con el número de clientes que nos mostró la herramienta 'site survey' de acuerdo con la Ilustración 61 para el mismo punto de acceso.

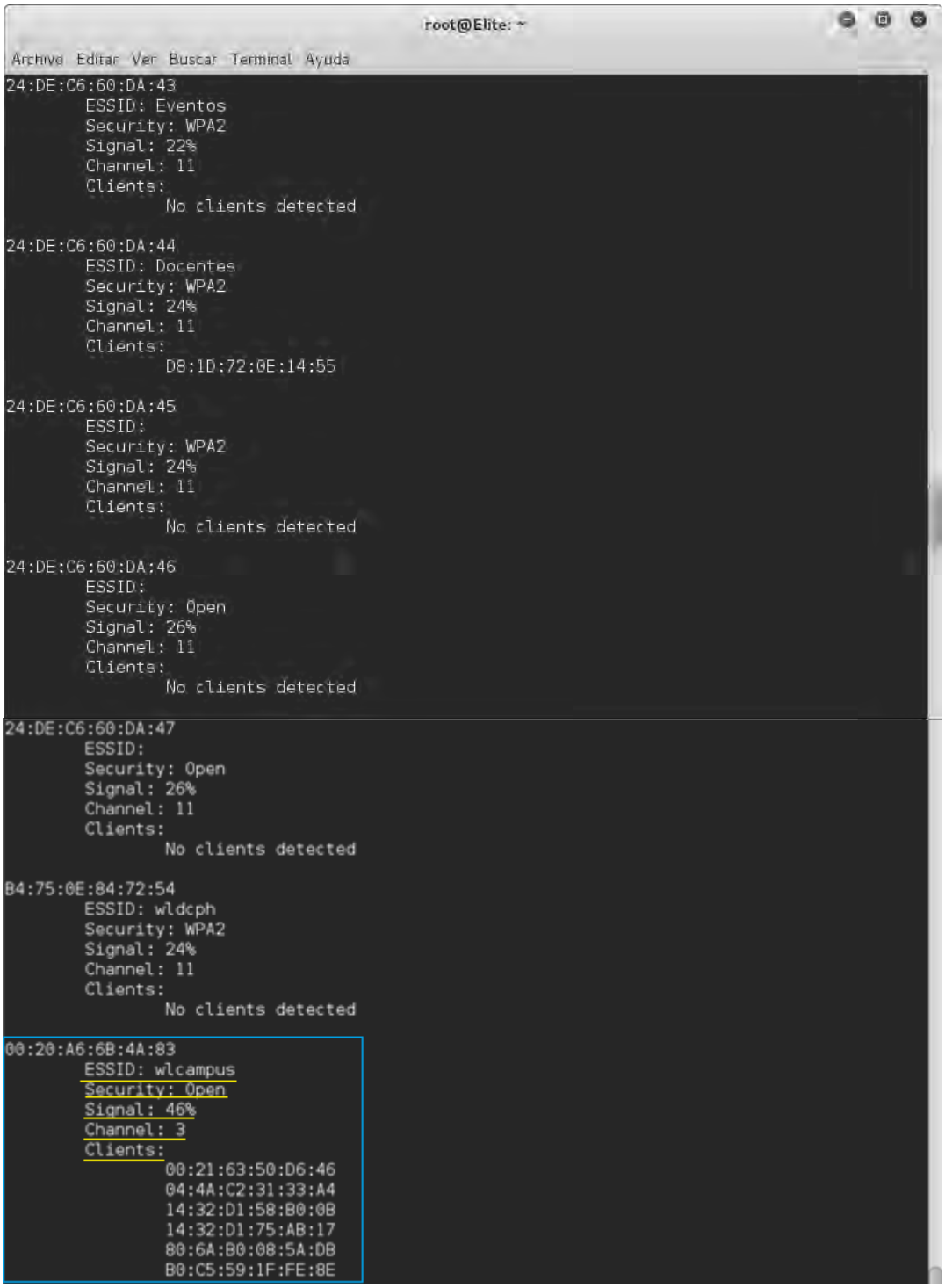

Ilustración 62 (Continuación): Lista de APs con sus respectivos clientes.

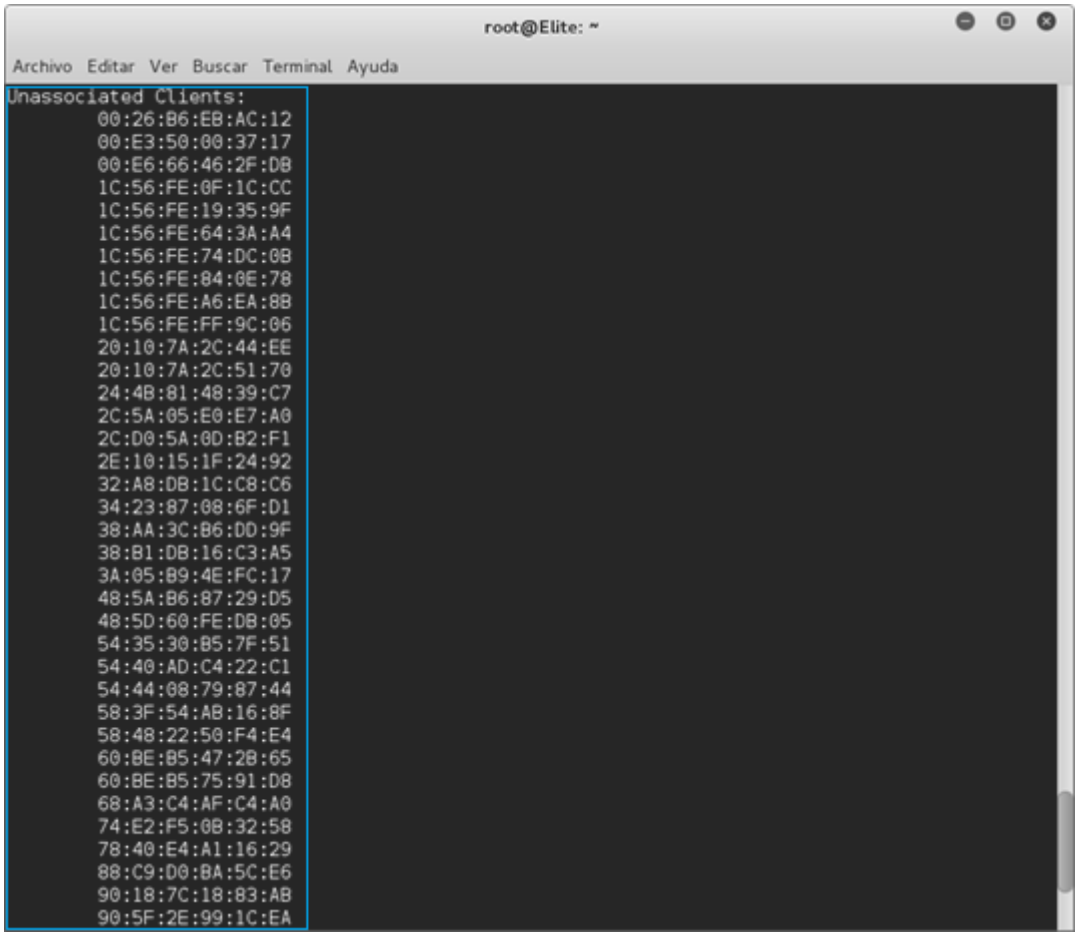

Ilustración 63: Lista de clientes no asociados en busca de un AP cercano.

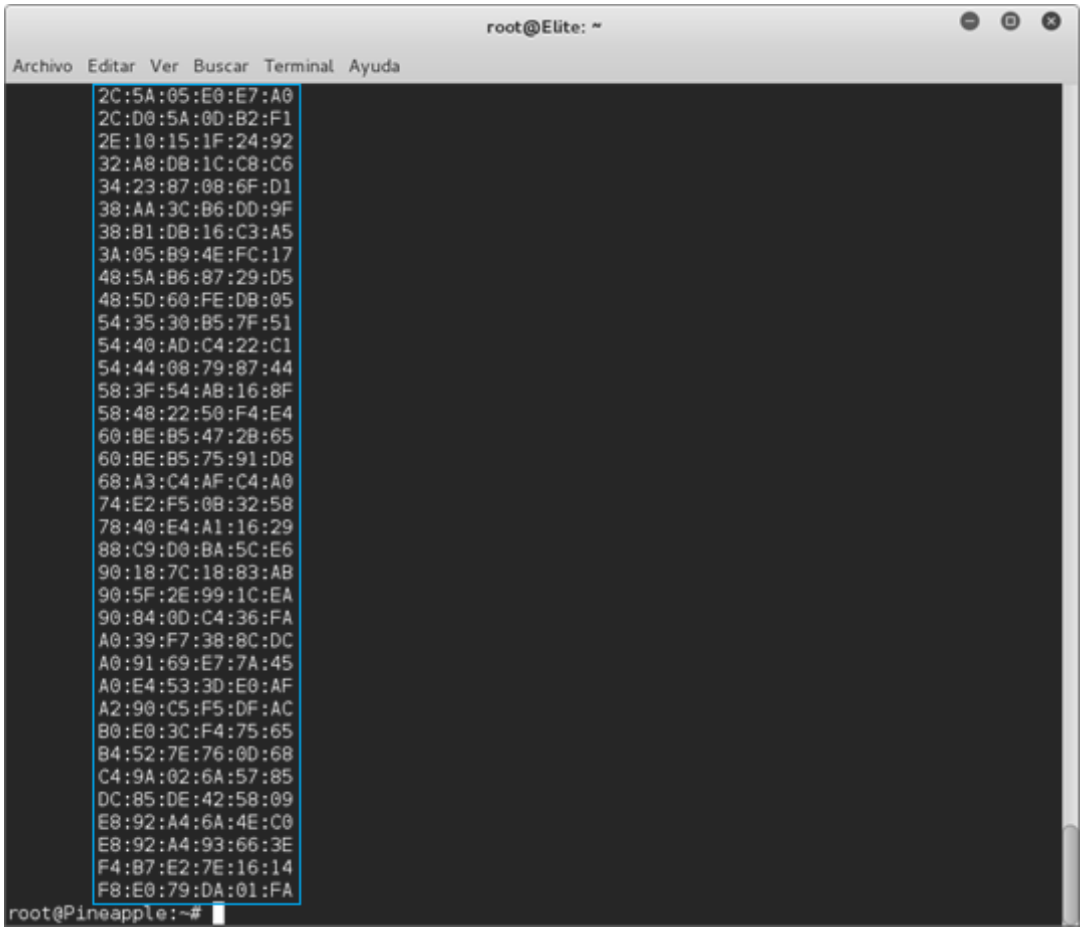

Ilustración 64 (Continuación): Lista de clientes no asociados en busca de un AP cercano.

Cabe mencionar que el dispositivo Wifi Pineapple no logró detectar el AP con BSSID 00:1F:45:20:F4:B0 que también difundía la señal de la red 'wlcampus' para el canal 8 (canal de transmisión de la señal) detectada por la tarjeta Alfa AWUS036H a través de la herramienta 'airodump-ng'. Esto se debe a que la tarjeta Alfa contaba con una antena de 18 dBi y la tarjeta fue configurada para una potencia de transmisión 30 dBm que es mayor a la potencia de transmisión normal de 20 dBm. El Wifi Pineapple cuenta con 2 antenas de 6 dBi por lo que es evidente que no tiene la misma capacidad de potencia de transmisión como la tarjeta Alfa con su antena de 18 dBi.

3.3 Fase 2

La segunda etapa hace referencia al establecimiento de un punto de acceso falso. Primero se verificó que la tarjeta inalámbrica 'wlan0' de la laptop HP (atacante) esté conectada a la red – 'wlcampus' a través de los comandos 'ifconfig' y 'iwconfig' de acuerdo con las Ilustraciones 65 y 66 respectivamente. El AP que difuende la red 'wlcampus' y donde se encuentra conectado

la interface 'wlan0' tiene la dirección MAC (BSSID) 00:1F:45:63:2C:20 de acuerdo a la Ilustración 60 que anteriormente se descubrió en la Etapa 1.

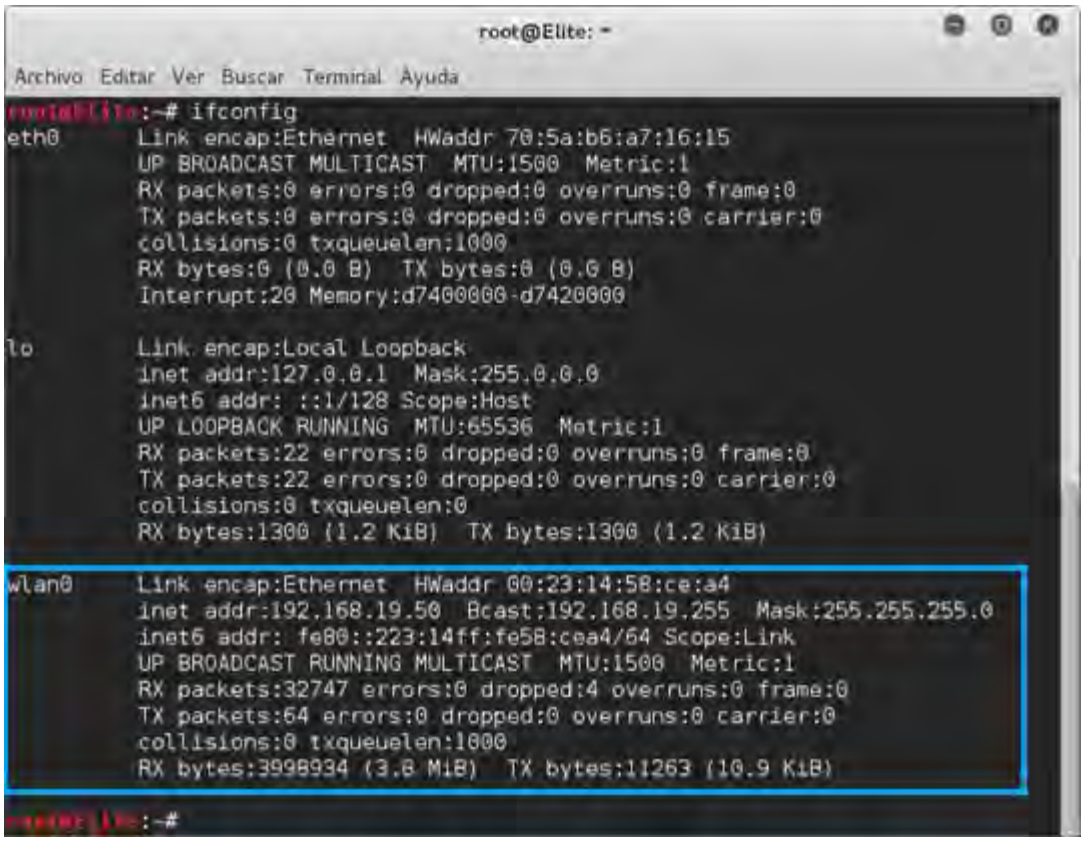

Ilustración 65: Ejecución del comando 'ifconfig'.

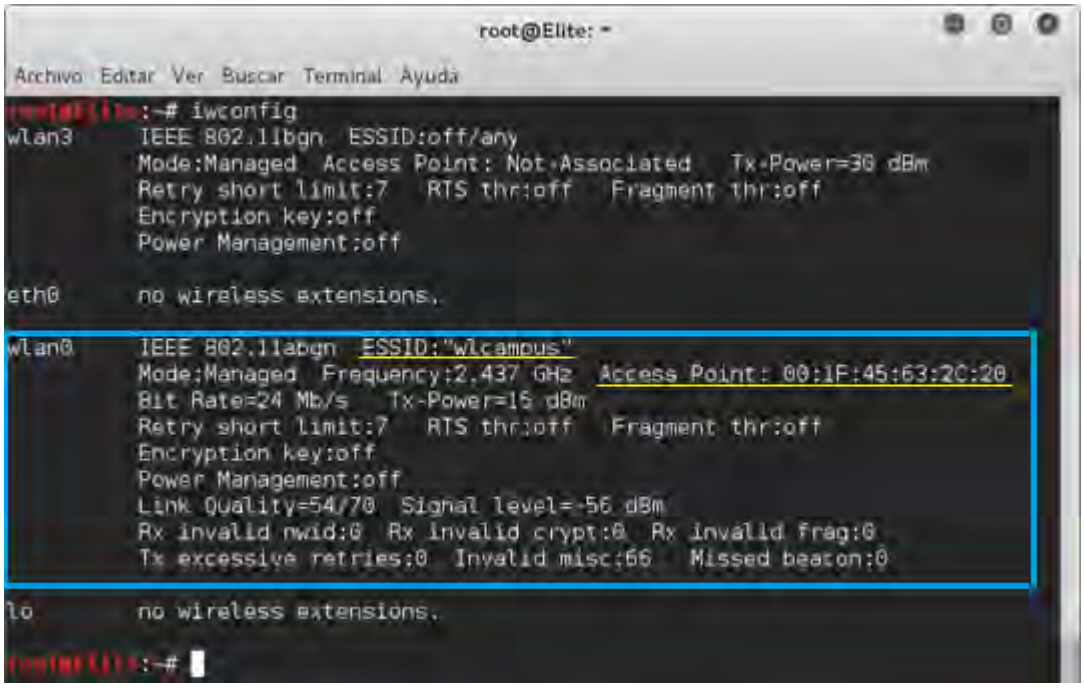

Ilustración 66: : Ejecución del comando 'iwconfig'.

Por otra parte, se verificó la dirección IP del punto de acceso donde se encuentra conectada la interface wlan0 a través de los comandos' ifconfig wlan0' y 'ip route' como se muestra en la Ilustración 67. Claramente se puede observar que la dirección IP del AP es 192.168.207.254 ya que tal dirección IP se le denomina como la puerta de enlace (Gateway). En la Etapa 1 anteriormente, el AP con dirección MAC 00:1F:45:63:2C:20 que difunde la red 'wlcampus' a través del canal 6 y con dirección IP 192.168.20.254 es el AP donde se encuentra conectada la interface wlan0 como se mencionó anteriormente. También se puede observar que la dirección IP de la interfaz 'wlan0' proporcionado por el AP a través de un servidor DHCP es 192.168.20.38 y con una dirección IP de broadcast de 192168.20.255.

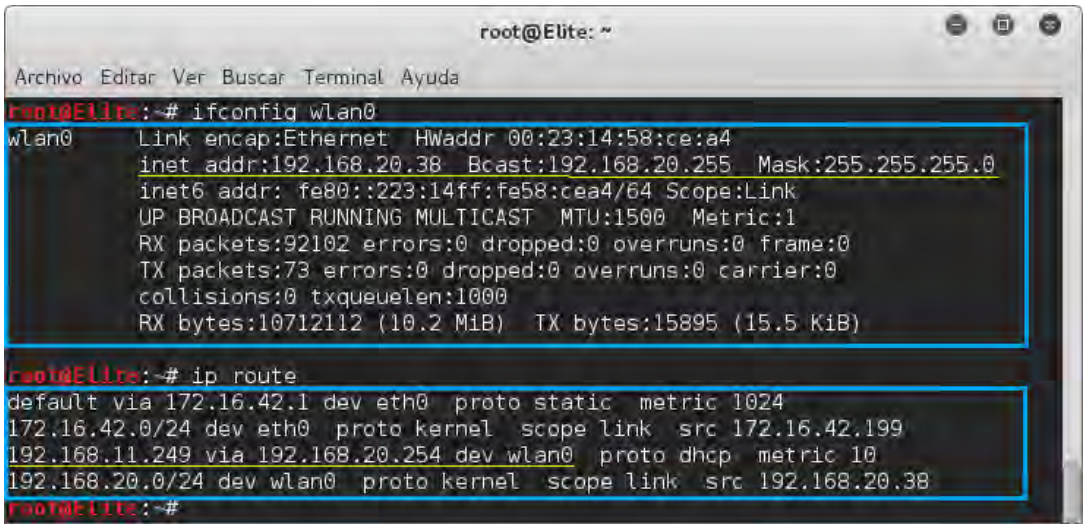

Ilustración 67: Ejecución de los comandos 'ifconfig0' y 'ip route'.

Por el otro lado, tenemos a un usuario de la red wlcampus que en este caso es la laptop Macbook Pro que se conectó a la red wlcampus en el AP donde se encuentra también conectado el atacante o *pentester* (laptop HP). La Ilustración 68 y 69 muestra que evidentemente la laptop Macbook Pro se encuentra conectada de manera inalámbrica a la red 'wlcampus' obteniendo la dirección IP 192.168.20.151. La Ilustración 70 muestra la dirección MAC de la laptop Macbook Pro que es b8:8d:12:31:21:ec la cual se utilizó luego para verificar el éxito del ataque.

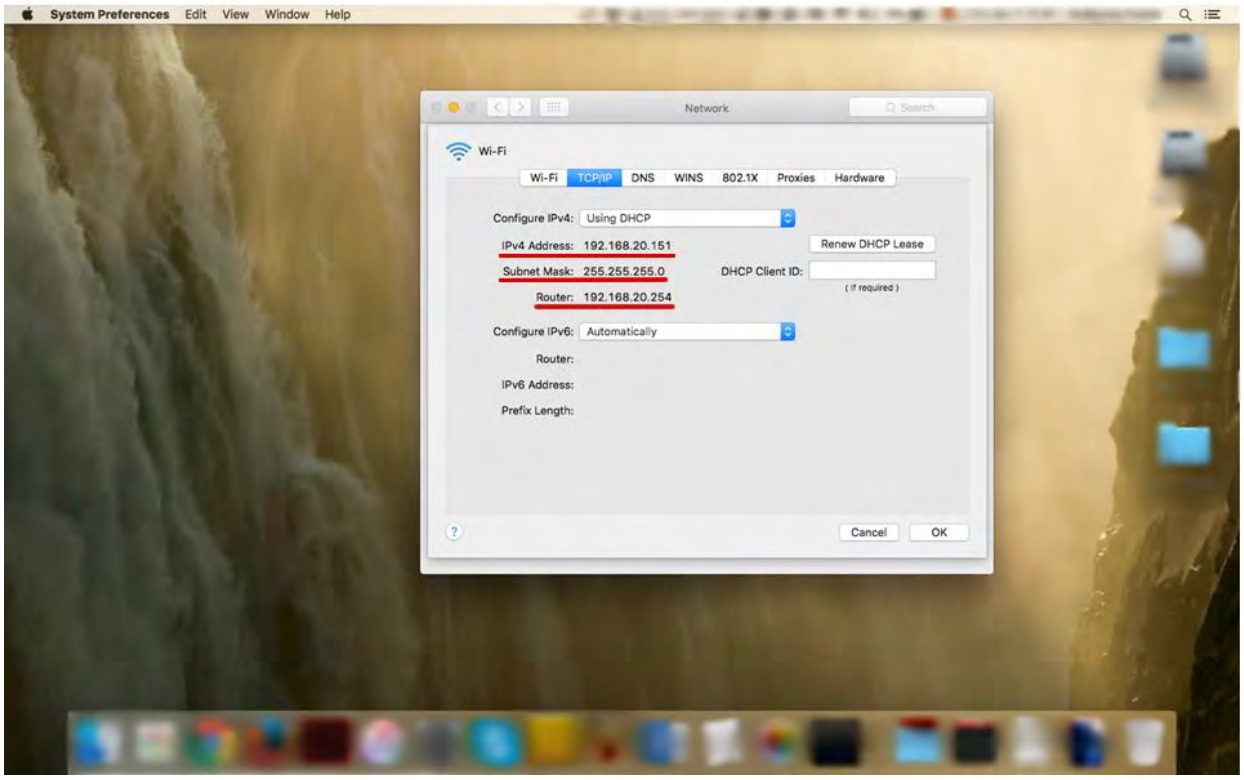

Ilustración 68: Ventana mostrando dirección IP e información de red de la Laptop Cliente conectado a la red 'wlcampus'.

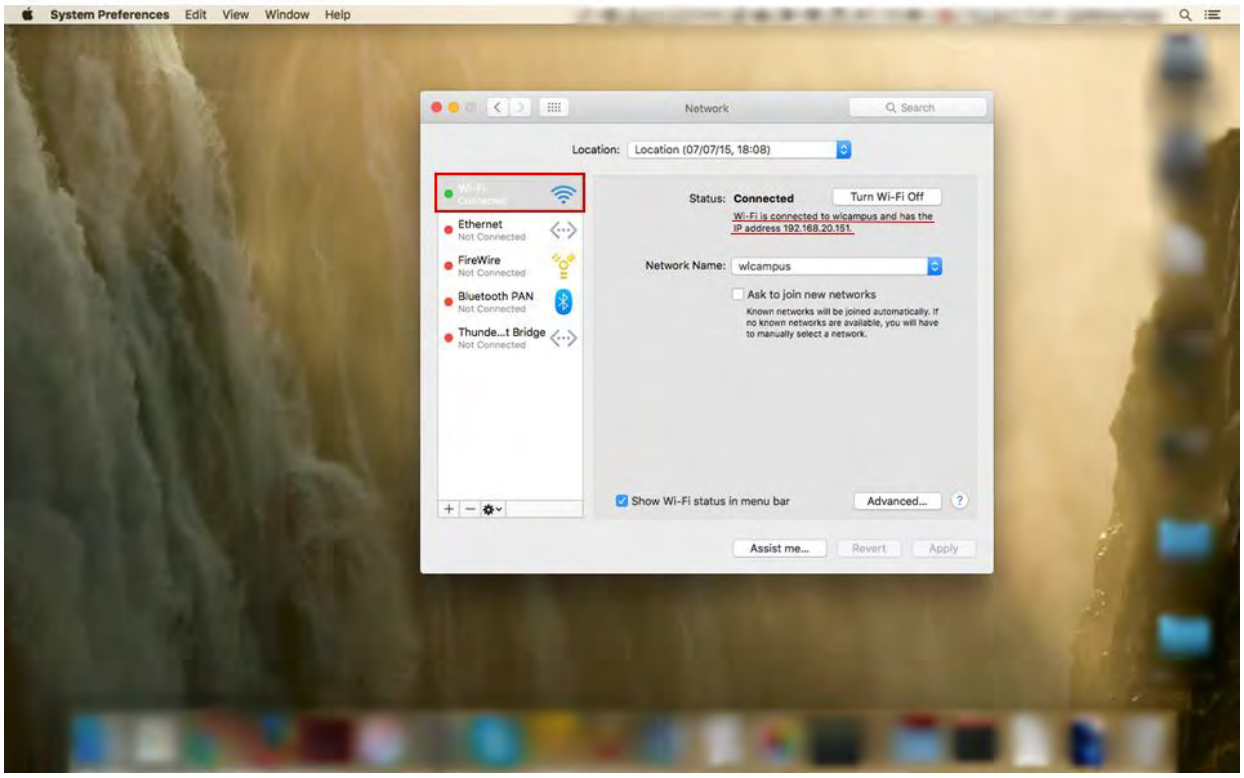

Ilustración 69: Ventana mostrando que la Laptop Cliente está conectado a la red 'wlcampus'.

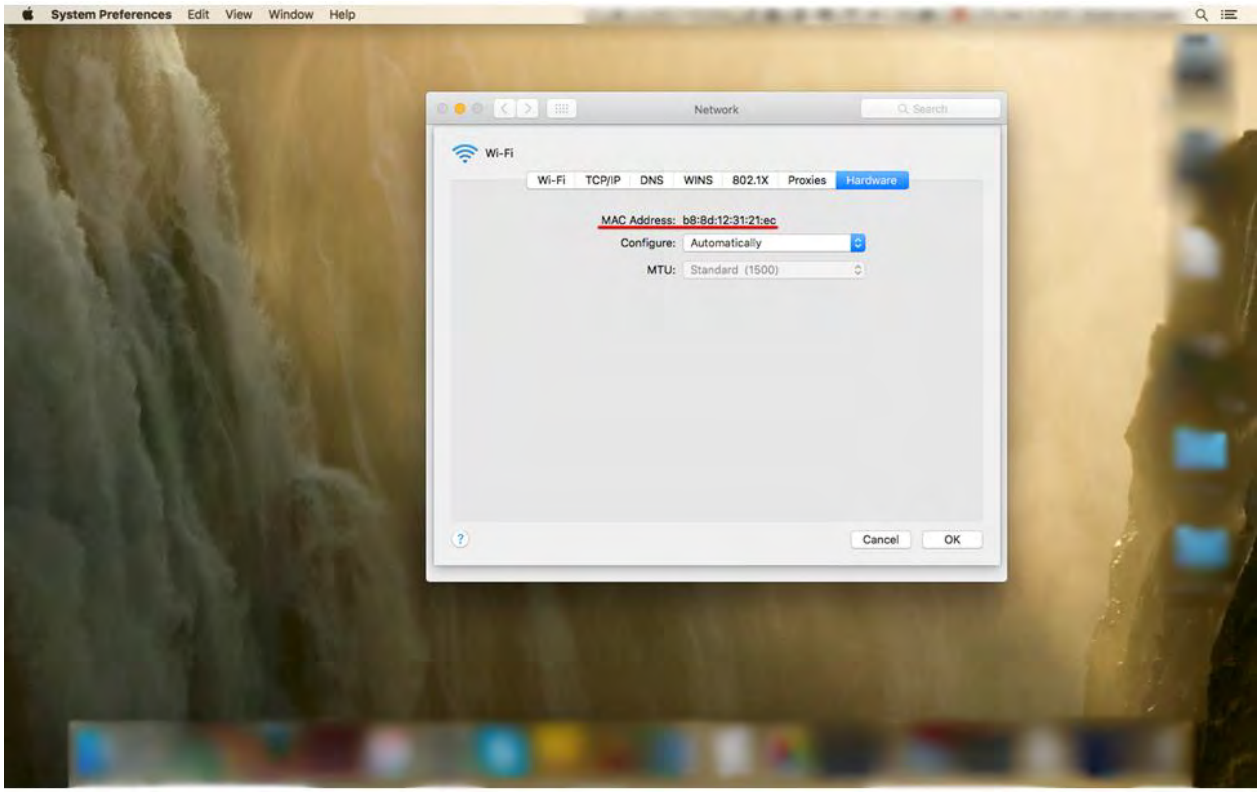

Ilustración 70: Ventana mostrando información sobre la dirección MAC de la laptop cliente.

Una vez que se realizaron los pasos anteriores de la Etapa 2, se configuró una conexión a internet compartida entre la laptop HP y el dispositivo Wifi Pineapple para que los usuarios que se conecten al AP falso tengan salida a Internet y posteriormente se lance un ataque 'Man In the Middle'. Primero, se estableció una conexión cableada del dispositivo Wifi Pineapple a la laptop conectando un cable UTP directo entre los puertos RJ45 de ambos dispositivo. Desde una línea de comandos, se ejecutó el comando '/root/Descargas/wp5.sh' que abre el archivo 'wp5.sh' donde se encuentran varios scripts que permiten una conexión de internet compartida de Kali Linux al Wifi Pineapple. De acuerdo a la Ilustración 71, la primera opción que se configuro es la máscara de red al solo darle 'enter' ya que la máscara de red por defecto 'Pineapple Netmask [255.255.255.0]' es en si la máscara de red de la dirección IP del dispositivo. Luego, se configuró la dirección de red del dispositivo Wifi Pineapple 'Pineapple Network [172.16.42.0/24]', la interface de red entre la laptop HP y el Wifi Pineapple 'Interface between PC and Pineapple [eth0]', la interface de red entre la laptop HP y la salida a internet 'Interface between PC and Internet [wlan0]', la puerta de enlace que hace referencia a la salida a internet 'Internet Gateway [192.168.19.254]', la dirección IP del Host (laptop HP, interfaz eth0) 'IP Address of Host PC [172.16.42.42]' y la dirección IP del dispositivo Wifi Pineapple 'IP Address of Pineapple [172.16.42.1]' con darle 'enter' ya que todas las opciones por defecto coincidían con la configuración real. Cabe mencionar que el Wifi Pineapple ya viene configurado con una configuración de red (dirección IP 172.16.42.1 /24) y que al momento de conectarlo, de

manera cableada a la PC, tiene la capacidad de censar la configuración previamente mencionada a través de los scripts del archivo 'wp5' previamente mencionado.

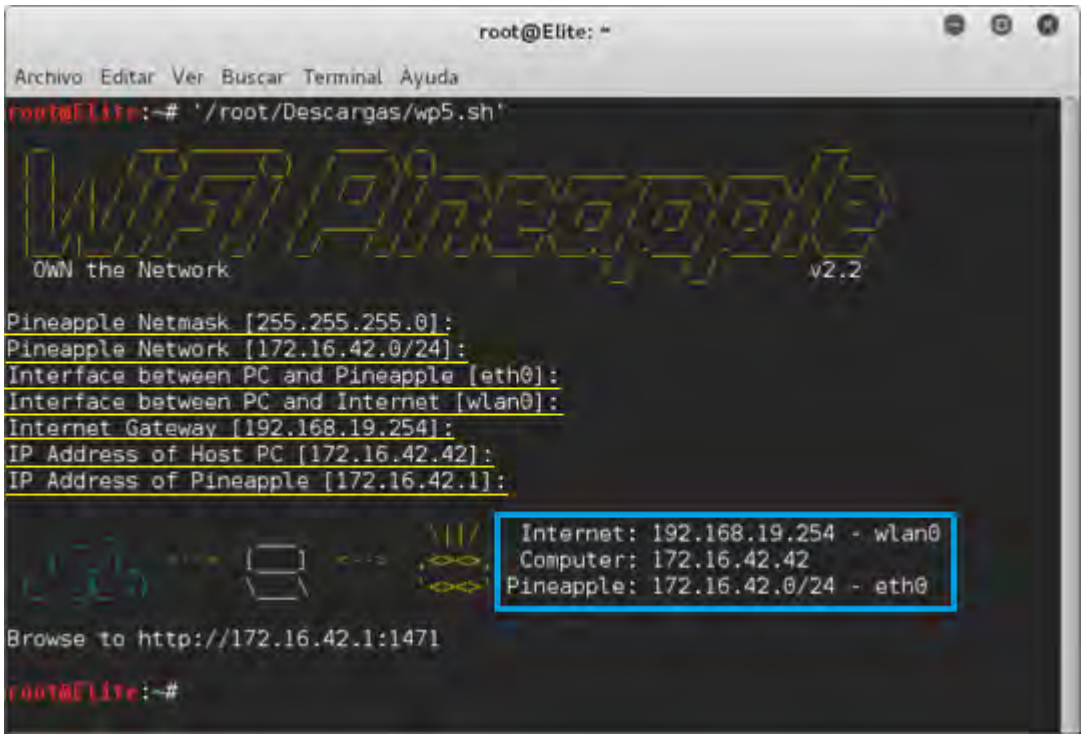

Ilustración 71: Ejecución del comando ''root/Descargas/wp5.sh''.

A partir de este punto, ya se tiene salida a internet desde el Wifi Pineapple a través de la conexión de Internet compartida por Kali Linux y por consiguiente se accedió a las herramientas de software que trae el Wifi Pineapple vía un navegador web con la dirección 172.16.42.1:1471 e ingresando con la cuenta de administrador como se muestra en la Ilustración 72. Por otra parte, ya dentro del sistema operativo del WIfi Pineapple la Ilustración 73 expone de manera gráfica las diferentes opciones de configuración y herramientas que trae el dispositivo en forma de ventanas. Es importante mencionar que se pueden agregar otras herramientas de auditoría de redes inalámbricas descargándolas de internet e instalándolas al dispositivo.

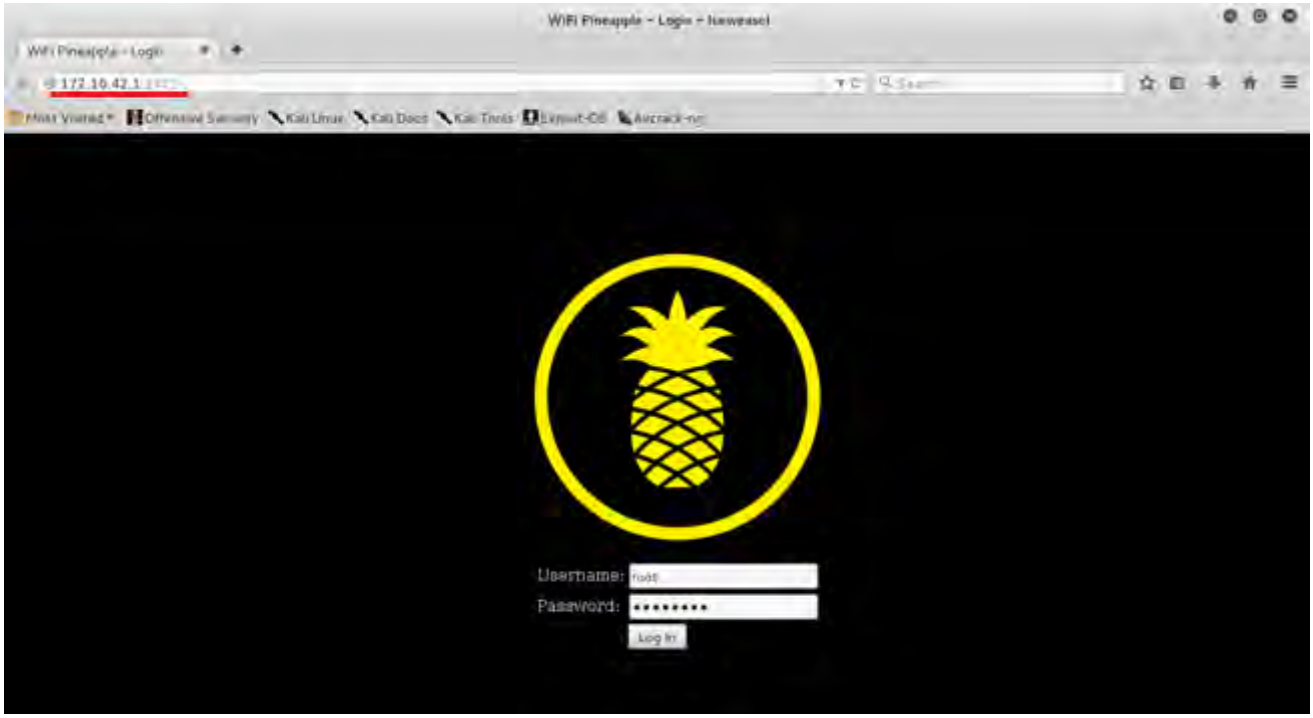

Ilustración 72: Portal de autenticación vía web para ingresar a la interface gráfica del sistema que controla el Wifi Pineapple Mark V

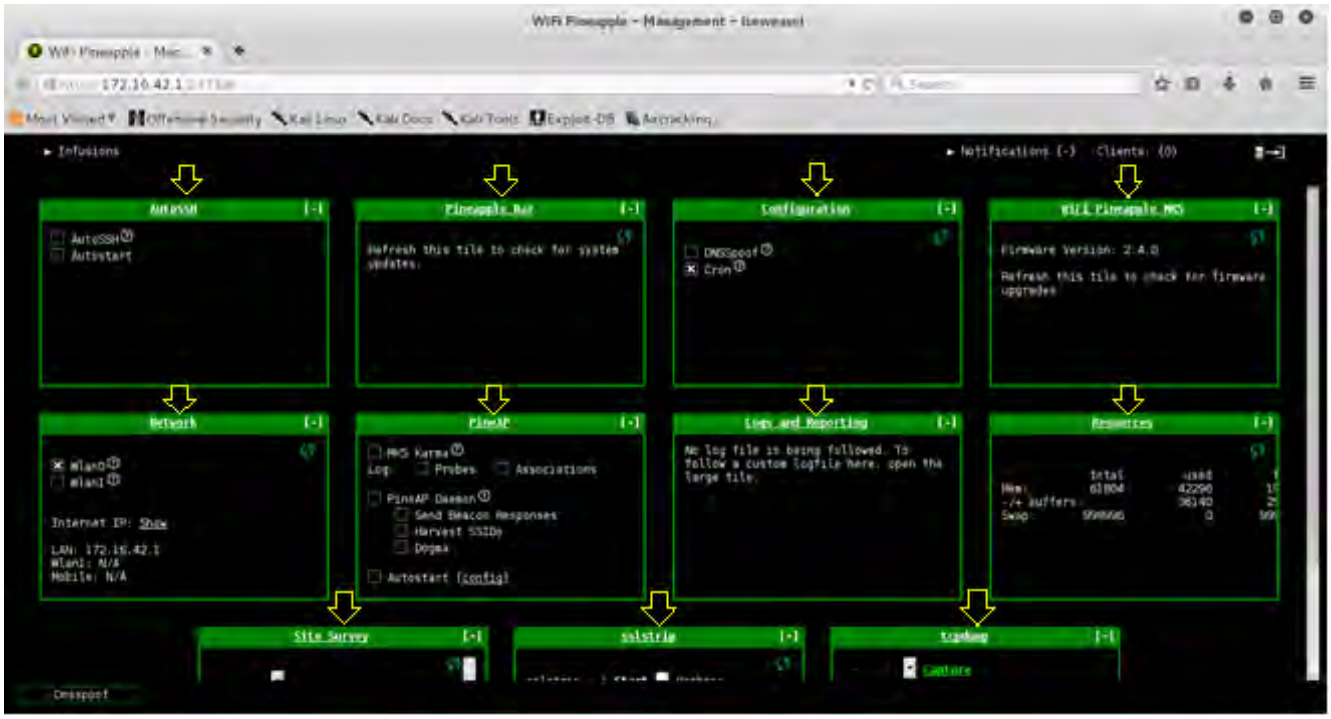

Ilustración 73: Portal con ventanas que hace referencia a diferentes herramientas y opciones de configuración integradas en el Wifi Pineapple Mark V.

Ya una vez dentro del sistema operativo del Wifi Pineapple como se muestra en la Ilustración 74, se seleccionó la ventana 'Network' y luego la opción 'Access Point' donde se configuró la parte superior donde dice 'Open Access Point' con el SSID del AP falso que en este caso llevaría el nombre 'wlcampus' sabiendo que ese es el nombre de la red inalámbrica que queremos atacar y también se configuró el canal de difusión en el canal 6 que hace referencia al AP con dirección MAC 00:1F:45:63:2C:20 configurado en el canal 6. En la parte inferior de la Ilustración 69, donde dice 'Secure Management Access Point', se configuró la opción 'SSID' con el nombre 'ifiw' para cambiar el SSID del AP administrativa y una contraseña de más de 8 caracteres incluyendo caracteres alfanuméricos para asegurarnos que nadie tenga acceso al panel de administración del dispositivo de manera inalámbrica. Una vez realizado lo anterior, se procedió a guardar la configuración dándole click al botón 'Save' en ambos casos.

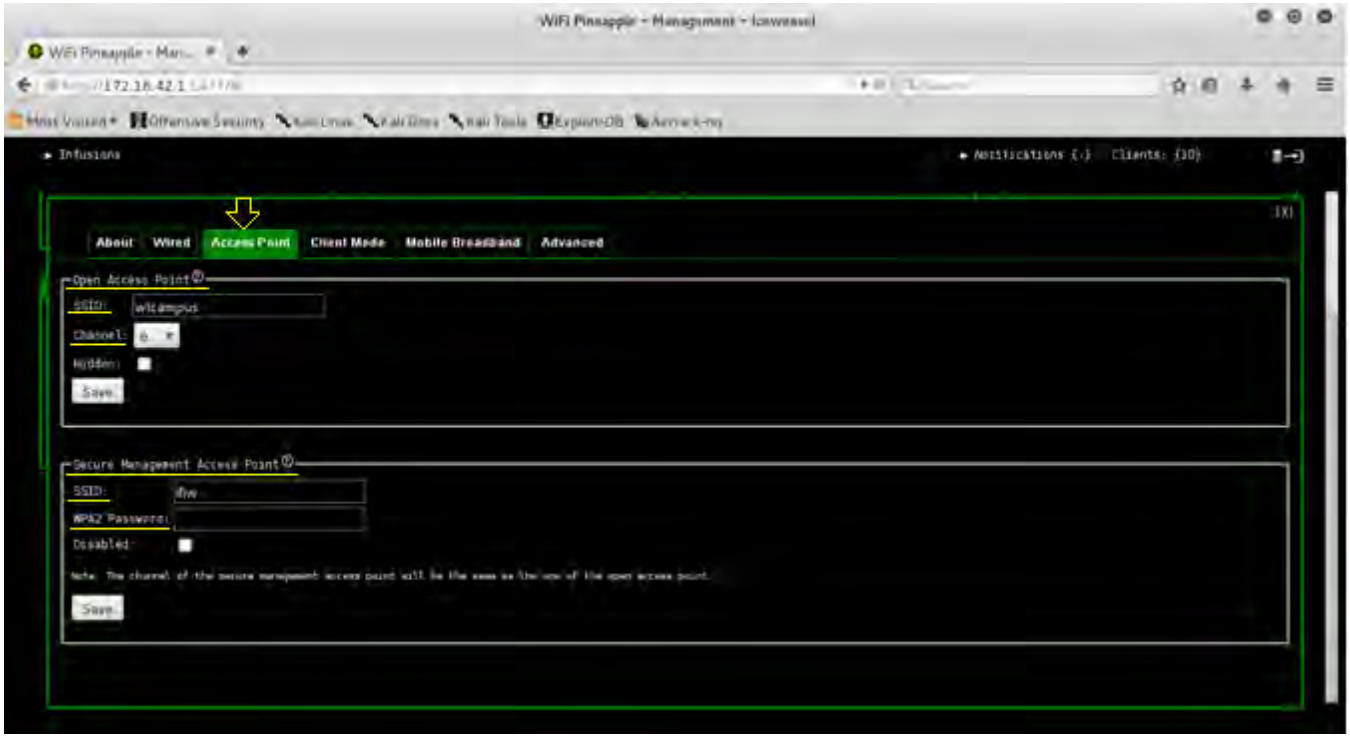

Ilustración 74: Portal de configuración para la opción 'Access Point' para la ventana 'Network'.

Una vez realizada la configuración anterior, se cerró la ventana 'Network' y se le dio clic a la ventana 'PineAP'. De acuerdo a la Ilustración 75, se seleccionó la opción 'Karma' y se puedo observar que podemos configurar el filtrado de clientes y SSID al igual que la dirección física en donde se guardan los archivos de registro (logs) que karma genera pero para este caso se dejó la configuración por default.

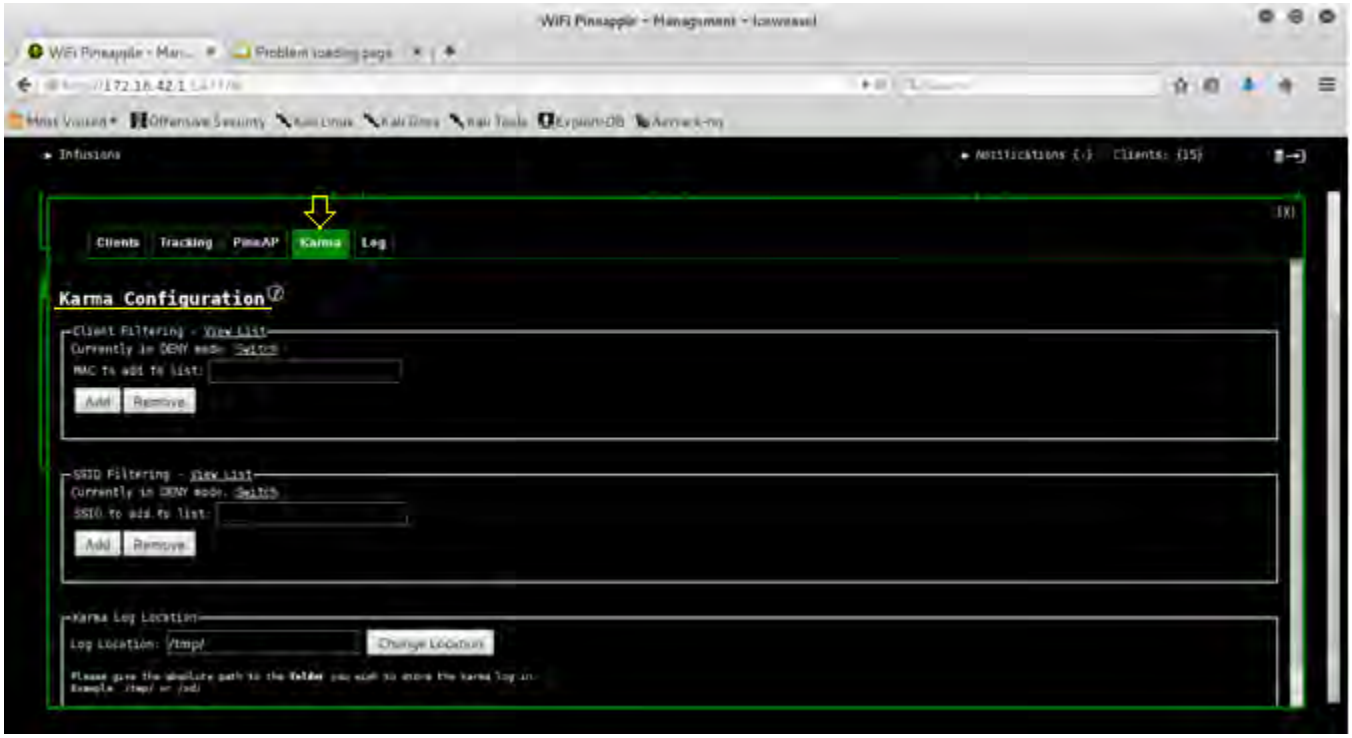

Ilustración 75: Portal de configuración para la opción 'Karma' para la ventana 'PineAP'.

3.4 Fase 3

Una vez terminada la Etapa 2, se volvió al portal principal donde se encuentran todas las ventanas de configuración y las herramientas de auditoría. En la ventana de 'PineAP', se seleccionó el cuadro a lado del nombre 'MK5 Karma' para habilitar esta herramienta y luego se seleccionó el cuadro a lado del nombre 'Probes' y el cuadro a lado del nombre 'Associations', esto es para habilitar e indicarle a Karma que dé respuesta a peticiones 'Probe' y peticiones de asociación a los dispositivos inalámbricos en busca de la red legitima ***wlcampus*** y otras redes inalámbricas en el área como se muestra en la Ilustración 76. Como consecuencia, los clientes automáticamente son conectados al dispositivo Wifi Pineapple a través del AP falso 'wlcampus' creado anteriormente y esto se demuestra a través de la Ilustración 77 y 78. En la Ilustración 77 se puede observar en la parte superior izquierdo un texto que dice 'Clients: {19}' que es precisamente el número de clientes/usuarios inalámbricos que están siendo víctimas del ataque Rogue AP. Por consiguiente, al darle click al mismo texto 'Clients: {19}', el software del dispositivo nos lleva directo a un portal que nos da un reporte con información de los clientes inalámbricos conectados al AP falso como se muestra en la Ilustración 77 y 78. Este reporte se puede encontrar al darle click a la ventana 'PineAP' y una vez dentro del portal de la herramienta, se selecciona la opción 'Clients'. La información que el reporte da especifica la dirección MAC de cada dispositivo conectado (HW Address), la dirección IP del dispositivo que le fue asignado por el Wifi Pineapple a través de DHCP (IP Address), el SSID que la herramienta Karma recibió por parte de los clientes a través de sus peticiones 'Probe', el nombre del

dispositivo del cliente (Hostname) y un temporizador de la actividad más reciente de los clientes (Last Seen).

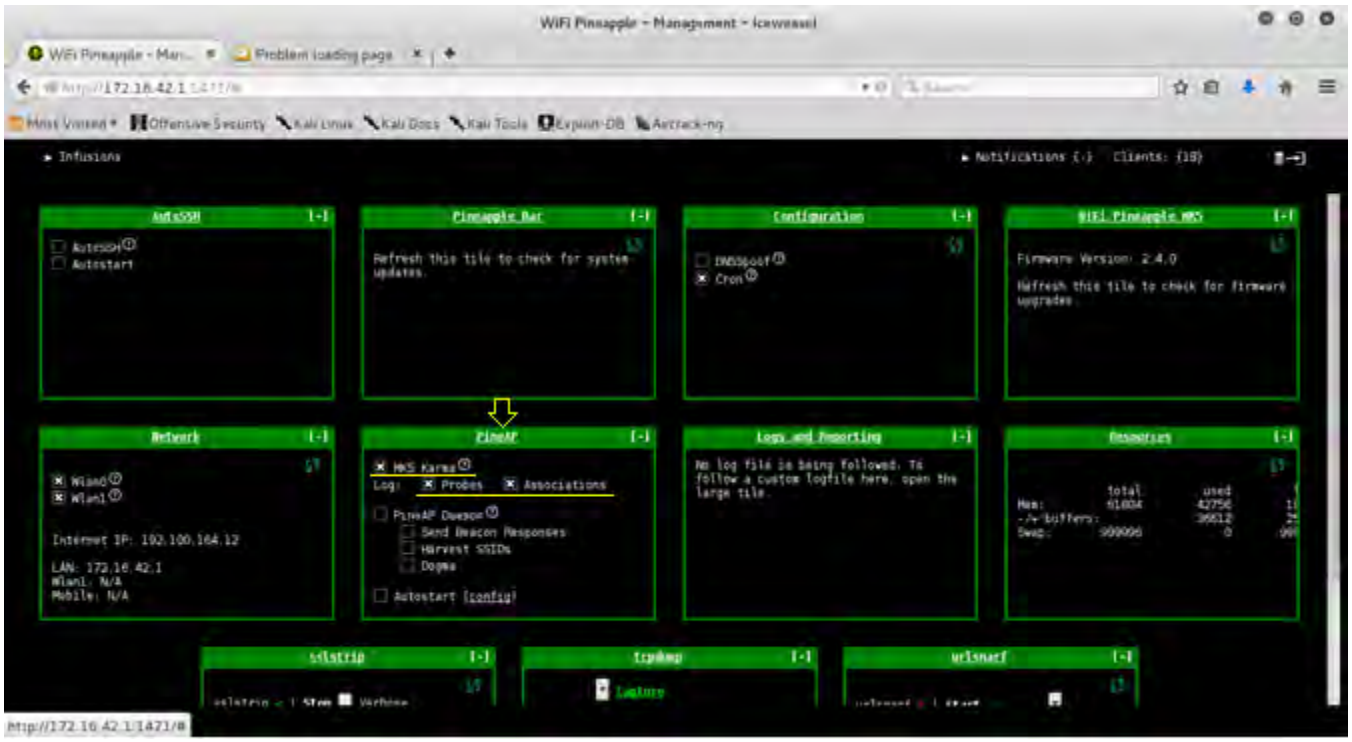

Ilustración 76: Portal con ventanas que hace referencia a diferentes herramientas y opciones de configuración integradas en el Wifi Pineapple Mark V.

Por otra parte, de acuerdo a la Ilustración 77, 79 y 80, la Laptop Macbook Pro que representa a un cliente de la red 'wlcampus' ha sido víctima del ataque Rogue AP ya que se encuentra conectado al AP falso. En la Ilustración 77 se puede observar que uno de los clientes conectados al AP falso es el dispositivo con dirección MAC b8:8d:12:31:21:ec que corresponde a la dirección MAC de la Laptop Macbook Pro. También, en la Ilustración 79 y 80 confirma que la laptop Macbook Pro tiene una dirección IP 172.16.42.170 y se encuentra conectado a la red 'wlcampus' pero del AP con dirección IP 172.16.42.1 que hace referencia a la dirección IP del Wifi Pineapple funcionando como un AP falso. Al utilizar la herramienta Karma y el hecho de que la señal del punto de acceso falso esté más potente o se encuentre más cerca de los clientes inalámbricos son dos factores fundamentales que determinaron el éxito de este ataque ya que después de aproximadamente 3 minutos de haber lanzado el ataque, los clientes se empezaron a conectar automáticamente y en menos de 5 minutos el Wifi Pineapple tenía conectados 20 clientes.

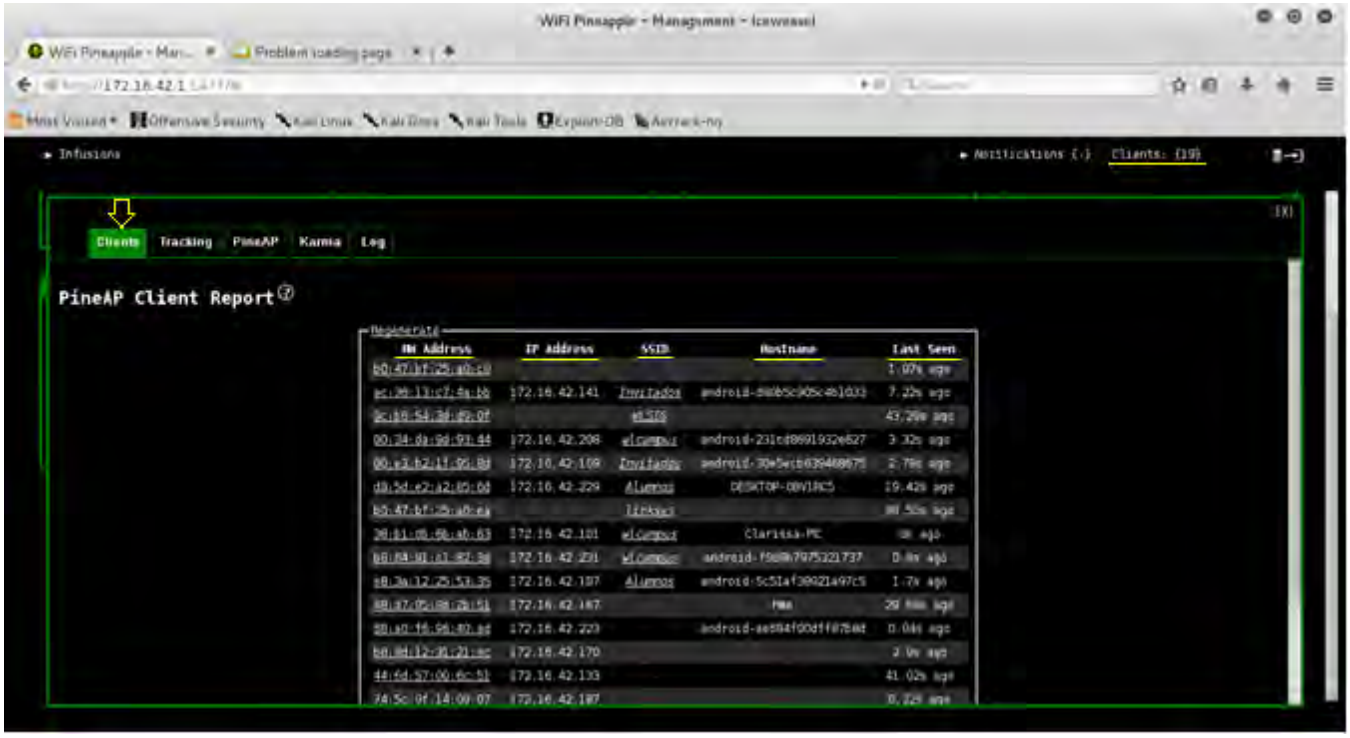

Ilustración 77: Portal que da un reporte de los clientes conectados al punto de acceso falso a través de la herramienta 'PineAp'.

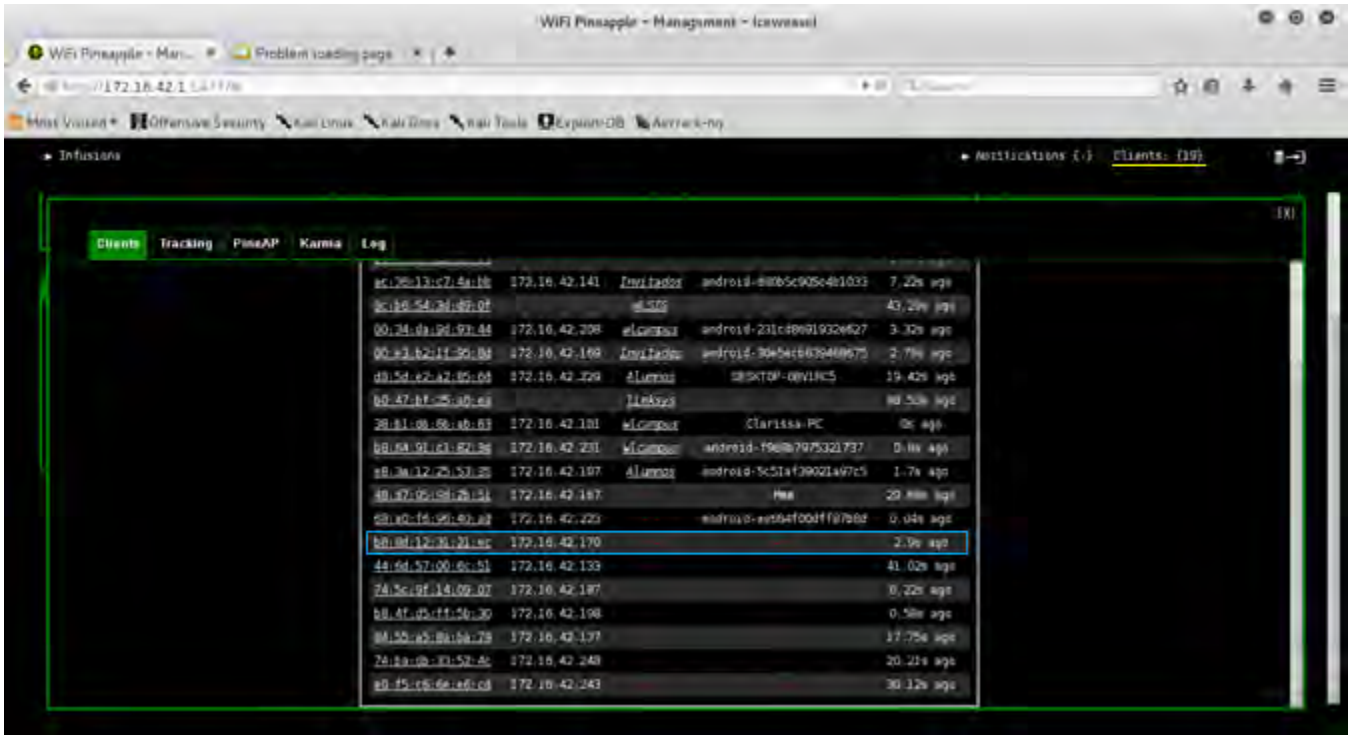

Ilustración 78 (Continuación de la Ilustración 71): Portal que da un reporte de los clientes conectados al punto de acceso falso a través de la herramienta 'PineAp'

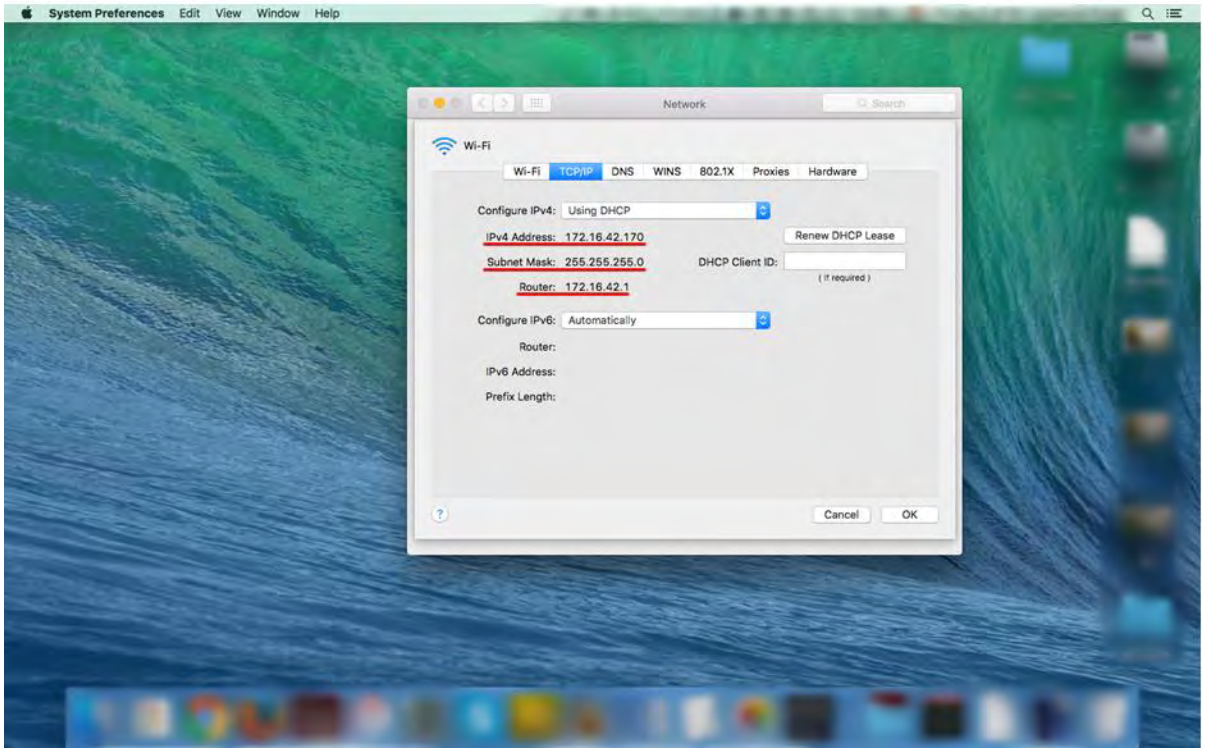

Ilustración 79: Ventana mostrando dirección IP e información de red de la Laptop Cliente conectado al AP falso

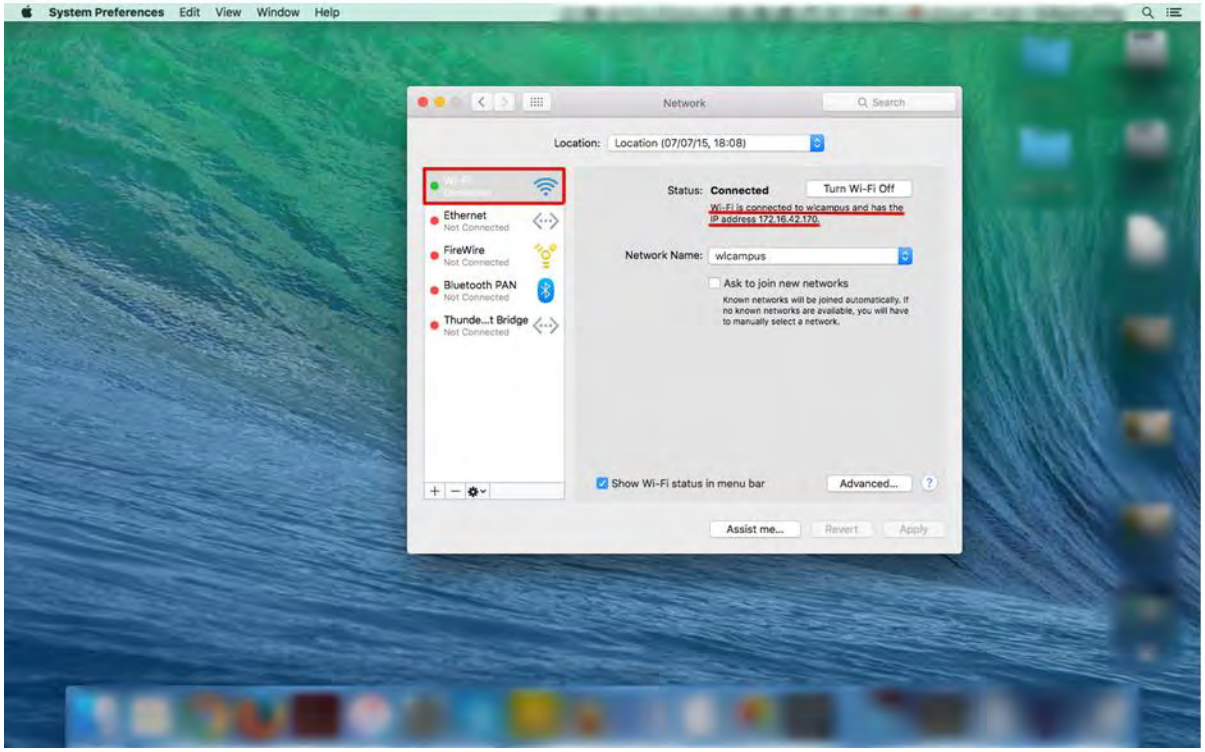

Ilustración 80: Ventana mostrando dirección IP e información de red de la Laptop Cliente conectado a la red 'wlcampus' que difunde el punto de acceso falso.

También, dentro del portal de la herramienta 'PineAP' se encuentra la opción 'Log' la cual se seleccionó para poder ver las peticiones 'Probe' y peticiones 'Association' que la herramienta Karma recibió de los clientes inalámbricos que se encontraban en el rango de cobertura de la señal inalámbrica del Wifi Pineapple como se muestra en las Ilustraciones 81 y 82. El Wifi Pineapple a través de Karma toma todas las peticiones 'Probe' y peticiones 'Association' y las analiza para luego darnos información de la fecha y horario que se recibieron las peticiones, la dirección MAC del dispositivo que envió la petición y el nombre de la red inalámbrica (SSID) a quien fue enviado la petición como se muestra en la Ilustración 81 y la Ilustración 82.

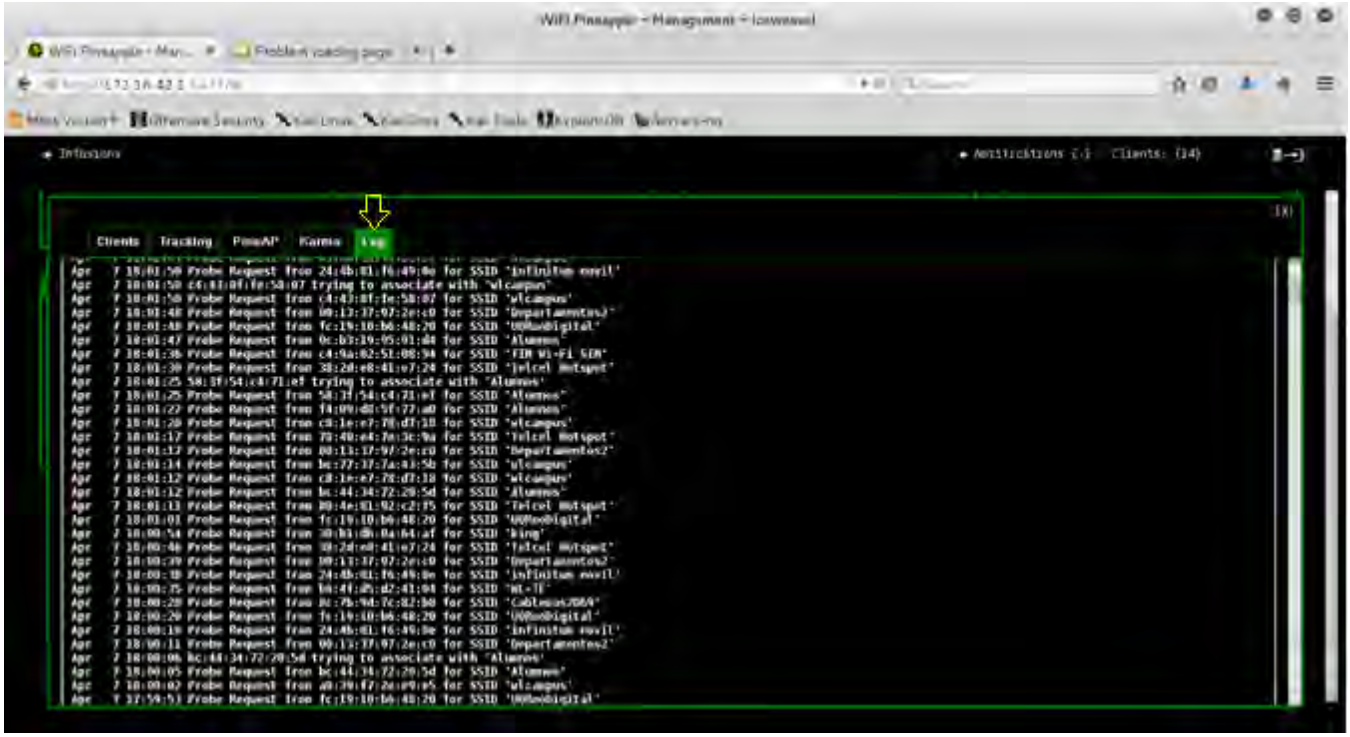

Ilustración 81 (Continuación): Portal de la opción 'Log' de la ventana 'PineAP' con información de todas las peticiones 'Probe' y peticiones 'Association' recibidas por la herramienta 'Karma'.

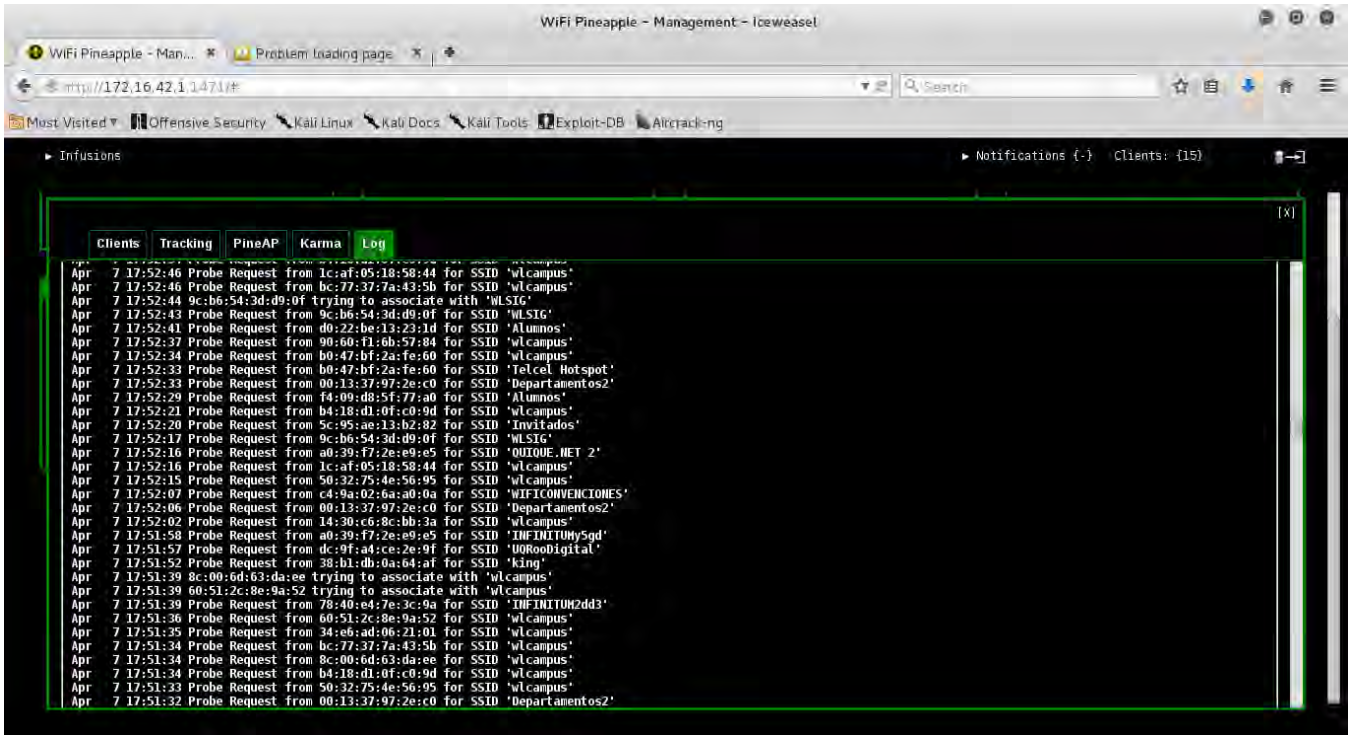

Ilustración 82 (Continuación): Portal de la opción 'Log' de la ventana 'PineAP' con información de todas las peticiones 'Probe' y peticiones 'Association' recibidas por la herramienta 'Karma'.

3.5 Fase 4

Para esta etapa, una vez que los clientes/usuarios inalámbricos se conectaron al punto de acceso falso, se extendió el ataque 'Rogue AP' a un ataque de hombre en medio (Man In the Middle Attack). La parte interesante es que previamente se realizó una conexión compartida de Internet entre el Wifi Pineapple y la laptop HP (*pentester*/atacante) que a su vez les permitió a los usuarios conectados al AP falso tener salida a Internet. El ataque 'Man in the middle' se llevó a cabo con el objetivo de interceptar cualquier tipo de tráfico de red de los usuarios hacia Internet y de Internet hacia los usuarios. Este ataque se implementó ejecutando las herramientas sslstrip y urlsnarf. Para ejecutar la herramienta sslstrip, se le dió clic al texto que dice 'Start' en la ventana llamado 'sslstrip' de acuerdo a la Ilustración 83. Para habilitar la herramienta Urlsnarf, primero se le dio clic al menú desplegable en la ventana llamado ´urlsnarf´ y se seleccionó la interfaz 'wlan0' ya que esa es la interfaz donde se encuentran conectados los usuarios inalámbricos y que hace referencia al punto de acceso falso. Luego de haber seleccionado la interfaz 'wlan0', se le dio clic al texto que dice 'Start' en la misma ventana 'urlsnarf' como se muestra en la Ilustración 83.

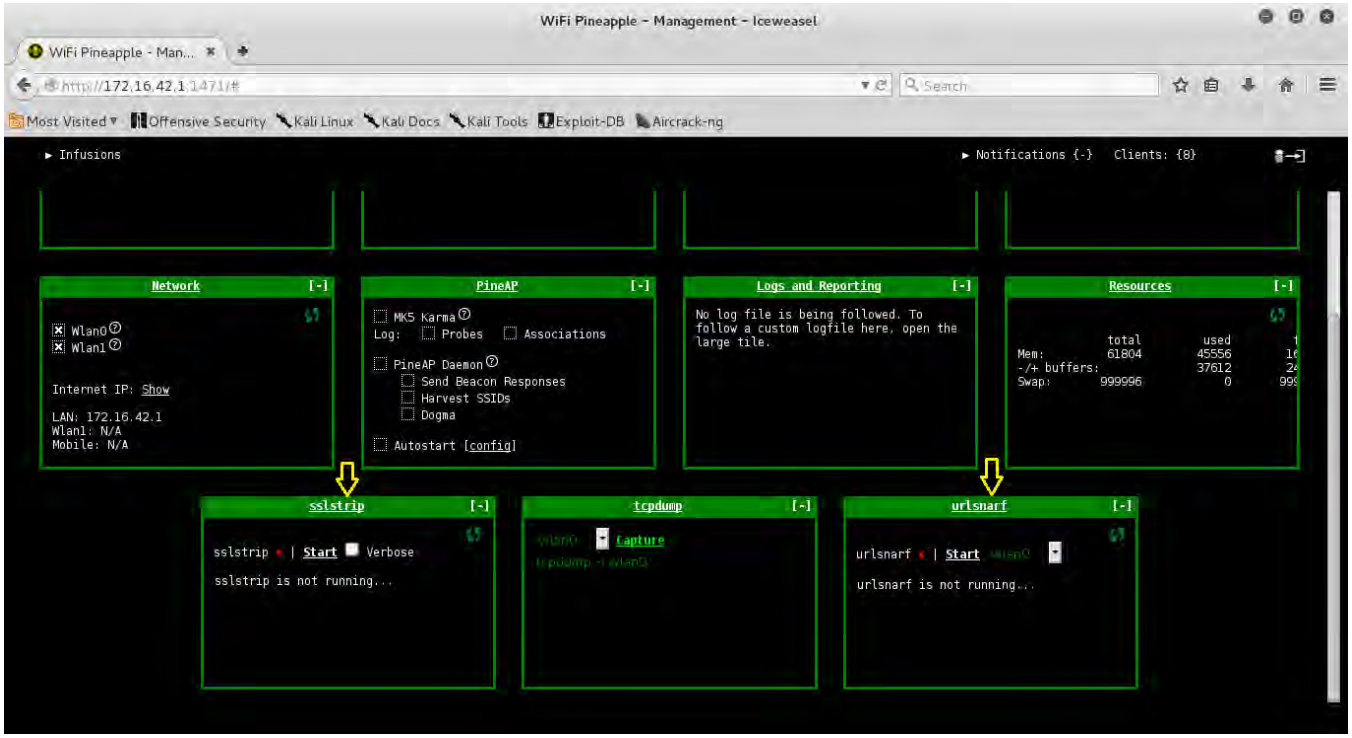

Ilustración 83: Ventanas de las herramientas 'sslstrip' y 'urlsnarf' en el portal principal de configuración del dispositivo Wifi Pineapple.

Una vez que se habilitaron las herramientas sslstrip y urlsnarf, se seleccionó la ventana 'sslstrip' para entrar al portal de configuración de la herramienta. En el portal de configuración se le dio clic a la opción con nombre 'Output' y luego se le dio clic al texto que dice 'Refresh' para que muestre todo el tráfico interceptado por sslstrip como se ve en la Ilustración 84. La herramienta sslstrip y urlsnarf se habilitaron de 7 a 8 minutos. Luego se deshabilito la ejecución de sslstrip al darle clic al texto que dice 'Stop' en el rectángulo de opción con nombre 'Controls' de acuerdo a la Ilustración 84. Una vez que se deshabilitó sslstrip, se seleccionó la opción 'History' y luego se le dio clic al texto 'view' para ver el tráfico que sslstrip intercepto de un manera ordenada como se muestra en la Ilustración 85 y 86. En el tráfico interceptado por sslstrip durante los 8 minutos se observó el tráfico HTTP que sslstrip convirtió de HTTPS a HTTP.

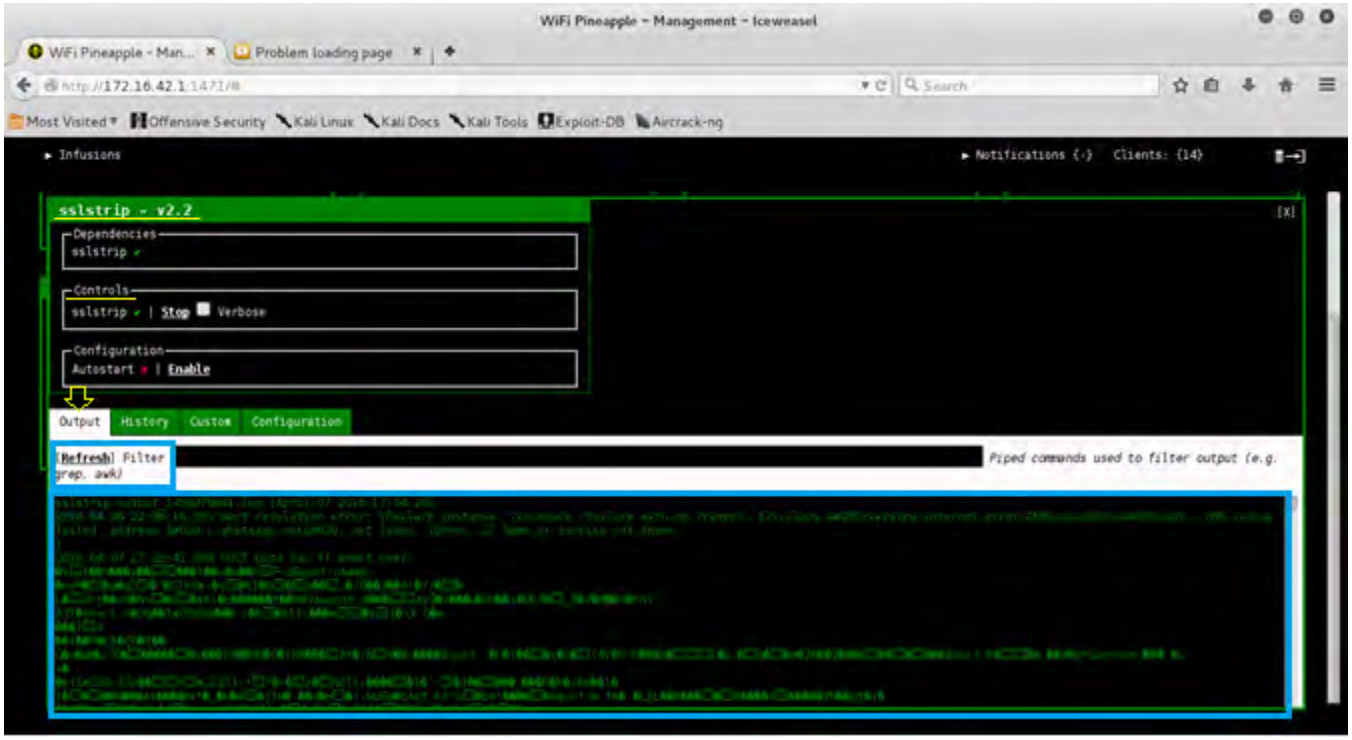

Ilustración 84: Portal de la opción 'Output' de la ventana de configuración 'sslstrip'.

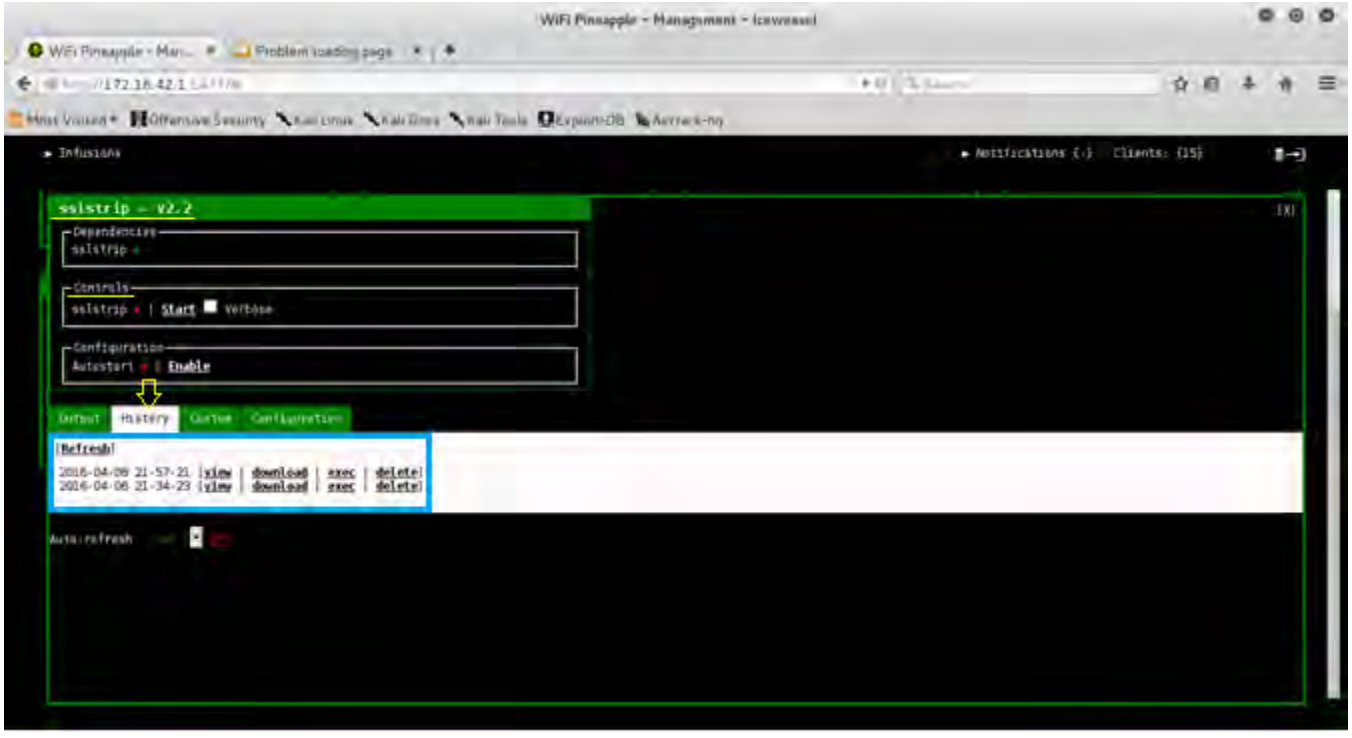

Ilustración 85: Portal de la opción 'History' de la ventana de configuración 'sslstrip'.

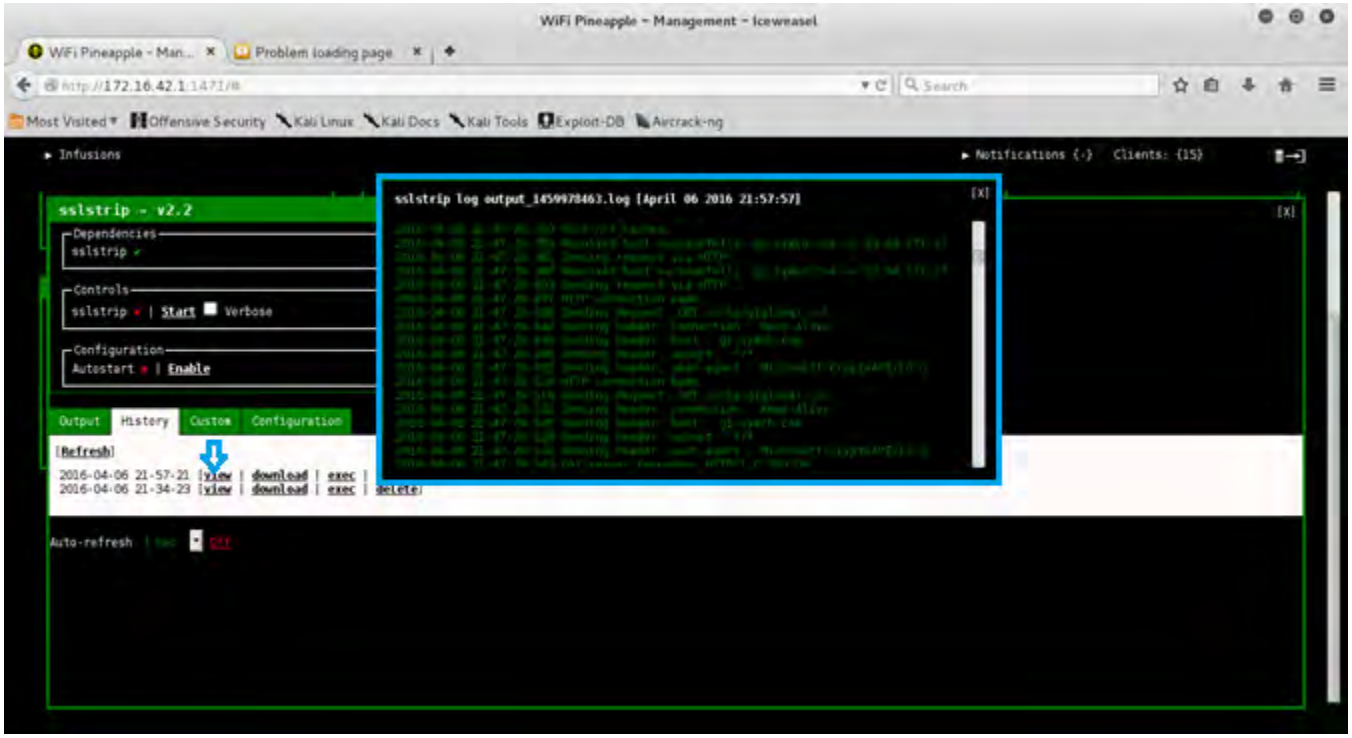

Ilustración 86: Ventana emergente de un archivo .log gestionado por el portal de la opción 'History' de la ventana de configuración 'sslstrip'.

La herramienta sslstrip brinda la opción de descargar el tráfico de red que fue interceptado y analizarlo aparte. Por consiguiente, se le dio clic al texto 'download' y se descargó el archivo 'output_1459978463.log' para analizarlo aparte con cualquier programa de edición de archivo de texto y sin necesidad de estar logeado al portal web del Wifi Pinapple como se muestra en la Ilustración 87. Una vez que se descargó el archivo .log, se abrió con un editor de texto para su análisis como se muestra en la Ilustración 87. La Ilustración 88 que concuerda con la Ilustración 86 mostró el tráfico HTTP interceptado de alguna de las víctimas conectado al Wifi Pineapple. La URL que se muestra en la Ilustración 88 'g2.symcb.com' hace referencia a un al establecimiento de una conexión hacia la dirección de Internet '23.64.171.27' que hace referencia al servidor del sitio web de Symantec. Symantec es una organización que provee certificados de seguridad para realizar conexiones con sitios web que implementan HTTPS. Por otra parte. La Ilustración 89 muestra el tráfico HTTP interceptado por sslstrip para la URL 'www.memedeportes.com' que hace referencia a la página web que se visitó con la Laptop Mac book Pro que se utilizó exclusivamente para ser víctima del ataque en cuestión. Por último, la Ilustración 90 muestra una pequeña parte del tráfico HTTP interceptado para la página web 'www.mercadolibre.com.mx' donde se observó que una de las víctimas estaba realizando búsquedas de ciertos artículos informáticos como cables y adaptadores, teclados y ratones entre otras. Cabe mencionar que la herramienta sslstrip no funcionó al 100% dado que muchas de las páginas web que implementan el cifrado a través de HTTPS, implementan el protocolo HSTS (HTTP Strict Transport Security). El protocolo HSTS establece una conexión cifrada entre el servidor web (que contiene la página web) y el navegador web del cliente. HSTS informa y

obliga al navegador web a realizar conexiones seguras de transferencia de hipertexto (HTTPS) sin que el usuario tenga que introducir en la barra de direcciones este protocolo que utiliza SSL/TLS para crear un canal cifrado. La mayoría de los navegadores web en sus versiones más recientes soportan el protocolo HSTS. Por consiguiente, si sslstrip se ejecuta por si solo con el objetivo de capturar cuentas (usuarios y contraseñas), es prácticamente imposible que funcione ya que el protocolo HSTS se lo impediría.

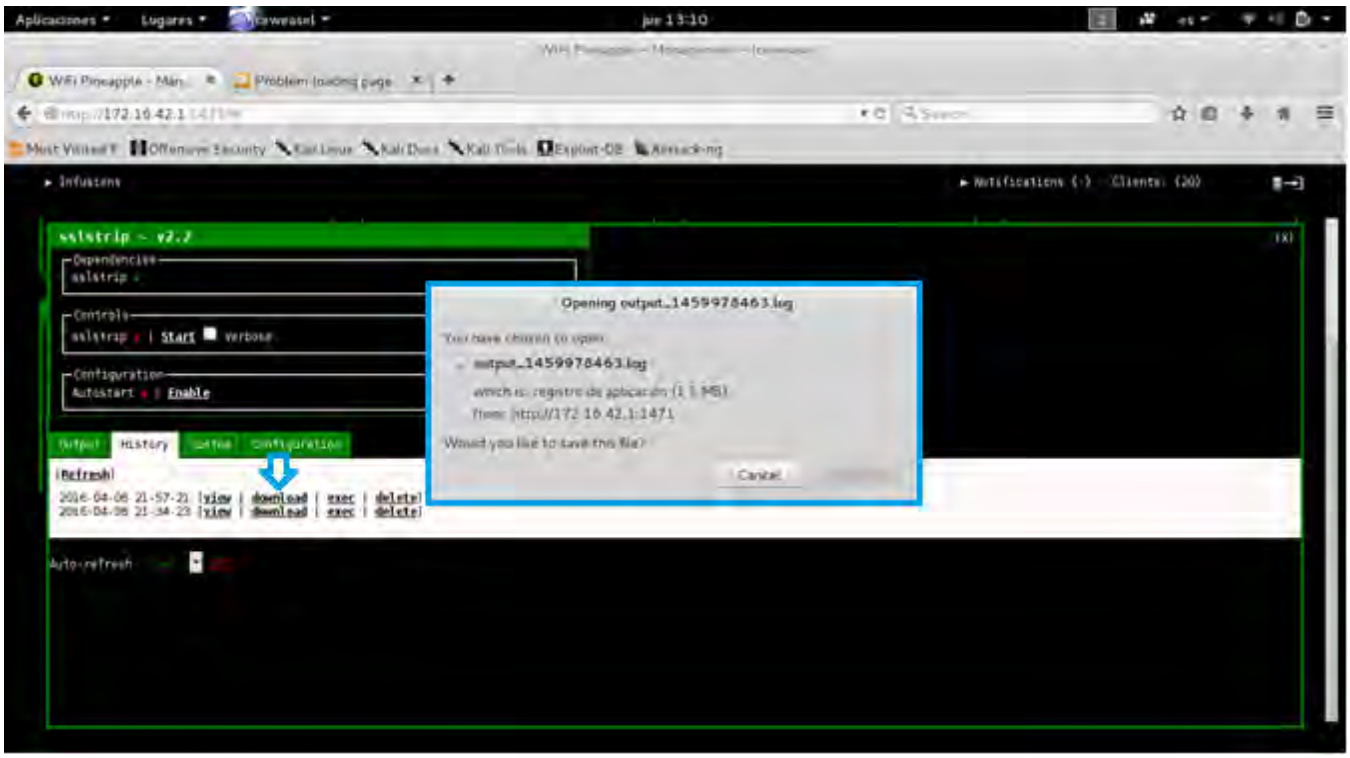

Ilustración 87: Notificación emergente para descarga el archivo 'output_1459978463.log' gestionado por el portal de la opción 'History' de la ventana de configuración 'sslstrip'.

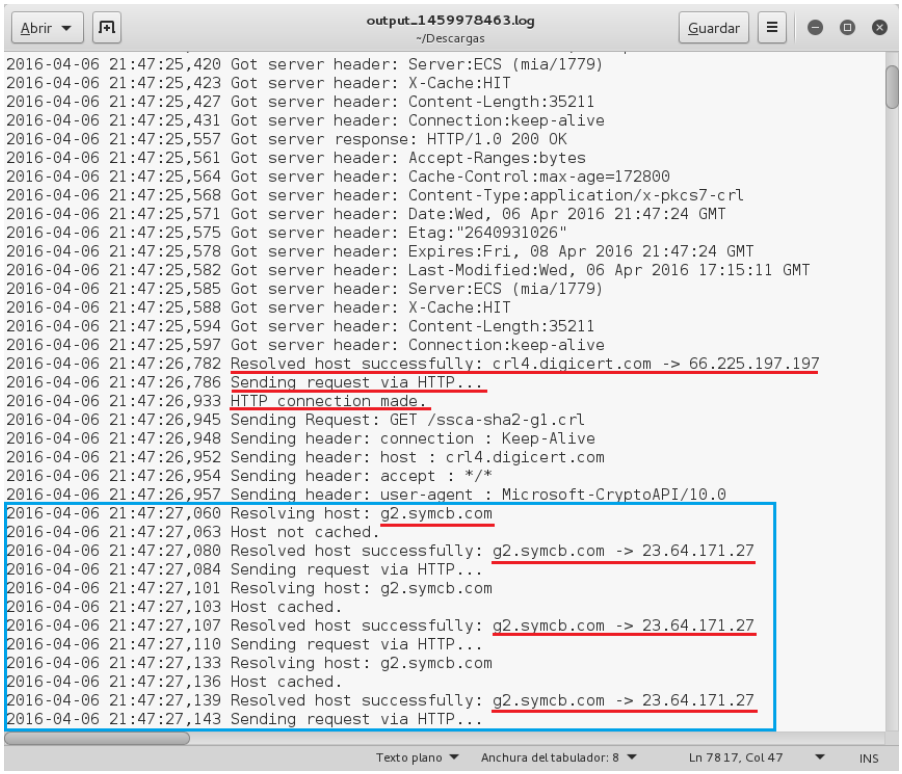

Ilustración 88: Archivo de texto output_1459978463.log mostrando tráfico HTTP interceptado por sslstrip.

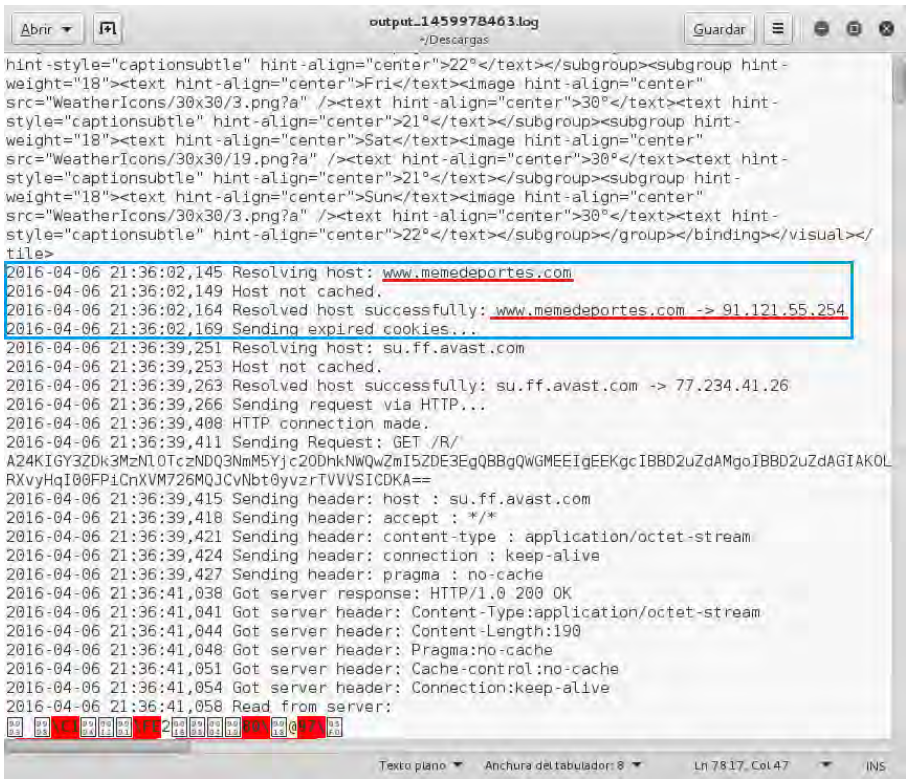

Ilustración 89 (Continuación): Archivo de texto output_1459978463.log mostrando tráfico HTTP interceptado por sslstrip.

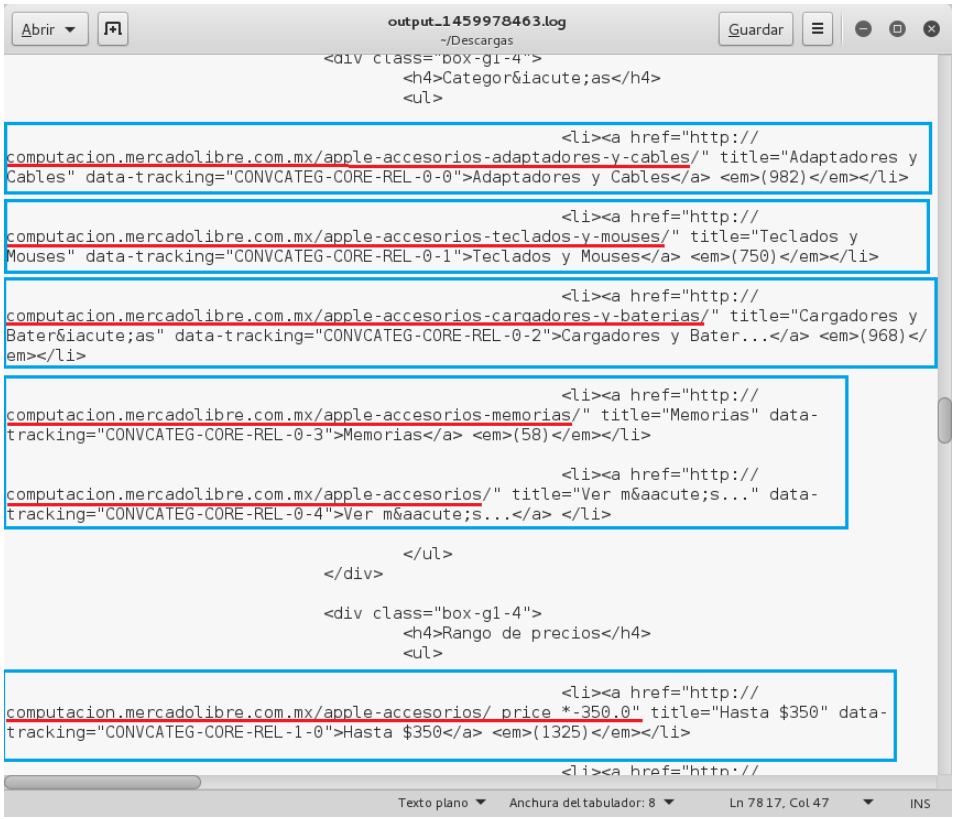

Ilustración 90 (Continuación): Archivo de texto output_1459978463.log mostrando tráfico HTTP interceptado por sslstrip.

A partir de este punto, se seleccionó la ventana 'urlsnarf' para entrar al portal de configuración de la herramienta. En el portal de configuración se le dio clic a la opción con nombre 'Output' y luego se le dio clic al texto que dice 'Refresh' para que muestre todo el tráfico HTTP interceptado por urlsnarf como se ve en la Ilustración 91. Como ya se había mencionado antes, las herramientas sslstrip y urlsnarf se habilitaron de 7 a 8 minutos. Luego se deshabilito la ejecución de urlsnarf al darle clic al texto que dice 'Stop' en el rectángulo de opción con nombre 'Controls' de acuerdo a la Ilustración 91. Una vez que se deshabilitó urlsnarf, se selecciónó la opción 'History' y se exploró la parte inferior del portal para ver el trafico HTTP interceptado por urlsnarf como se muestra en la Ilustración 92. Durante los 8 minutos que se habilitó urlsnarf, en un determinado momento se utilizó la laptop Macbook Pro para surfear la página web 'www.memedeportes.com' como se puede ver en la Ilustración 93. Unos segundos después de haber accedido a la página web mencionada anteriormente, se accedió portal de urlsnarf determinar y verificar si se logró interceptar el tráfico web generado por la laptop Macbook Pro a través de la página web 'memedeportes.com'. De acuerdo a la Ilustración 92, se pudo observar claramente que la herramienta urlsnarf intercepto el tráfico web generado al acceder a la página web 'www.memedeportes.com' a través del laptop cliente MacBook Pro.

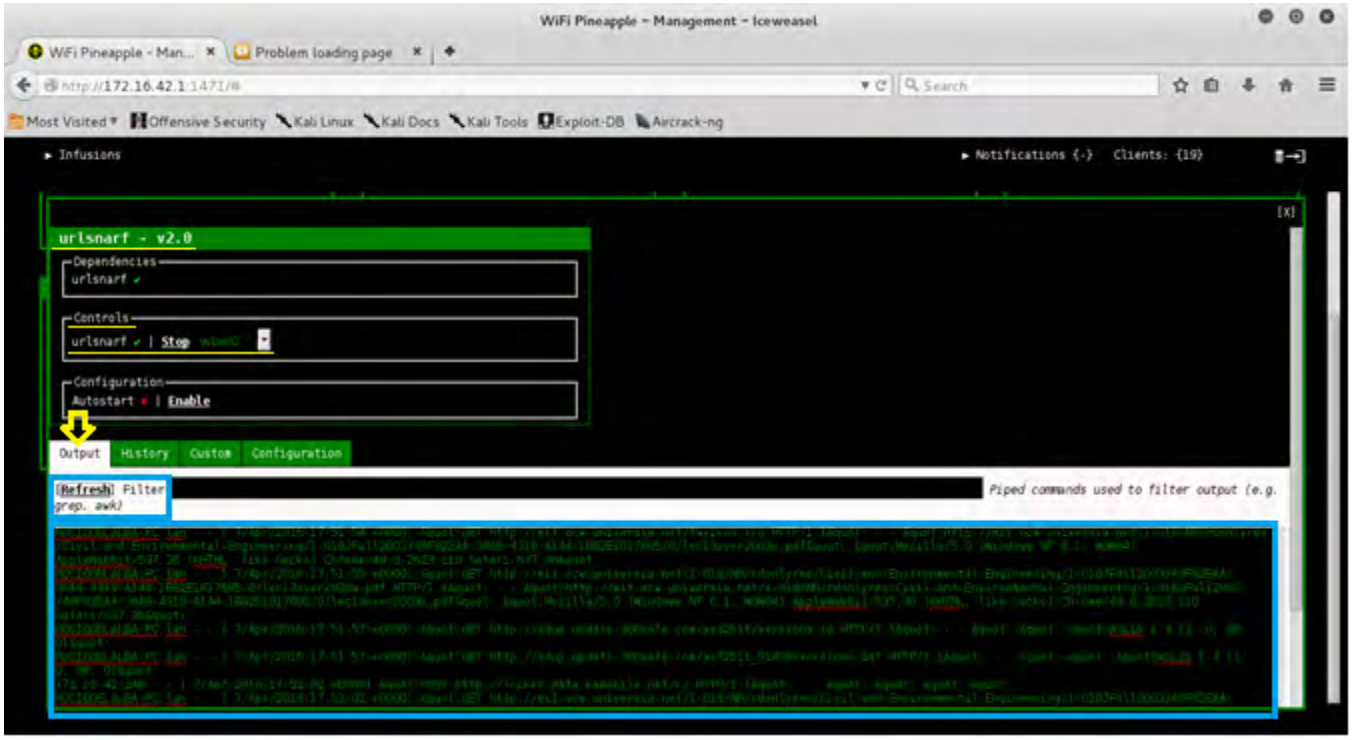

Ilustración 91: Portal de la opción 'Output' de la ventana de configuración 'urlsnarf'.

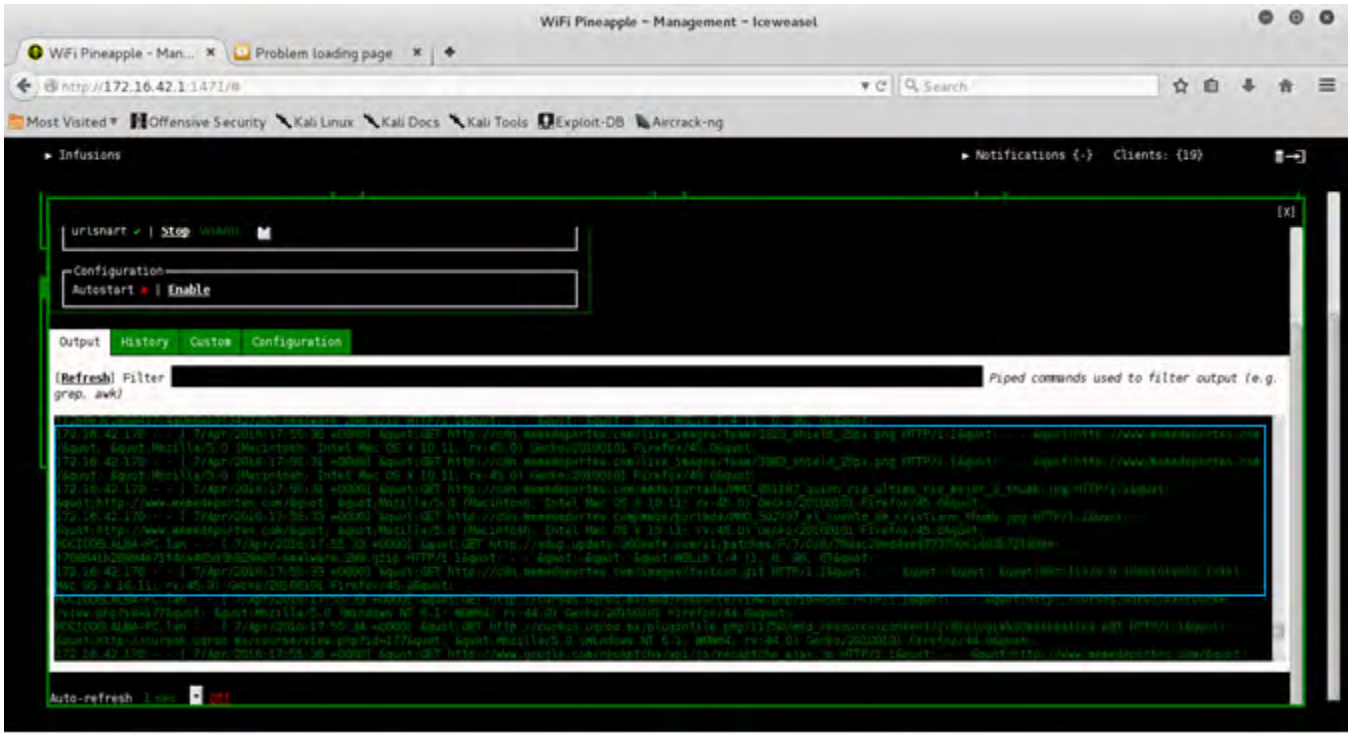

Ilustración 92: Portal de la opción 'Output' de la ventana de configuración 'urlsnarf' exponiendo el tráfico web de URL interceptado.

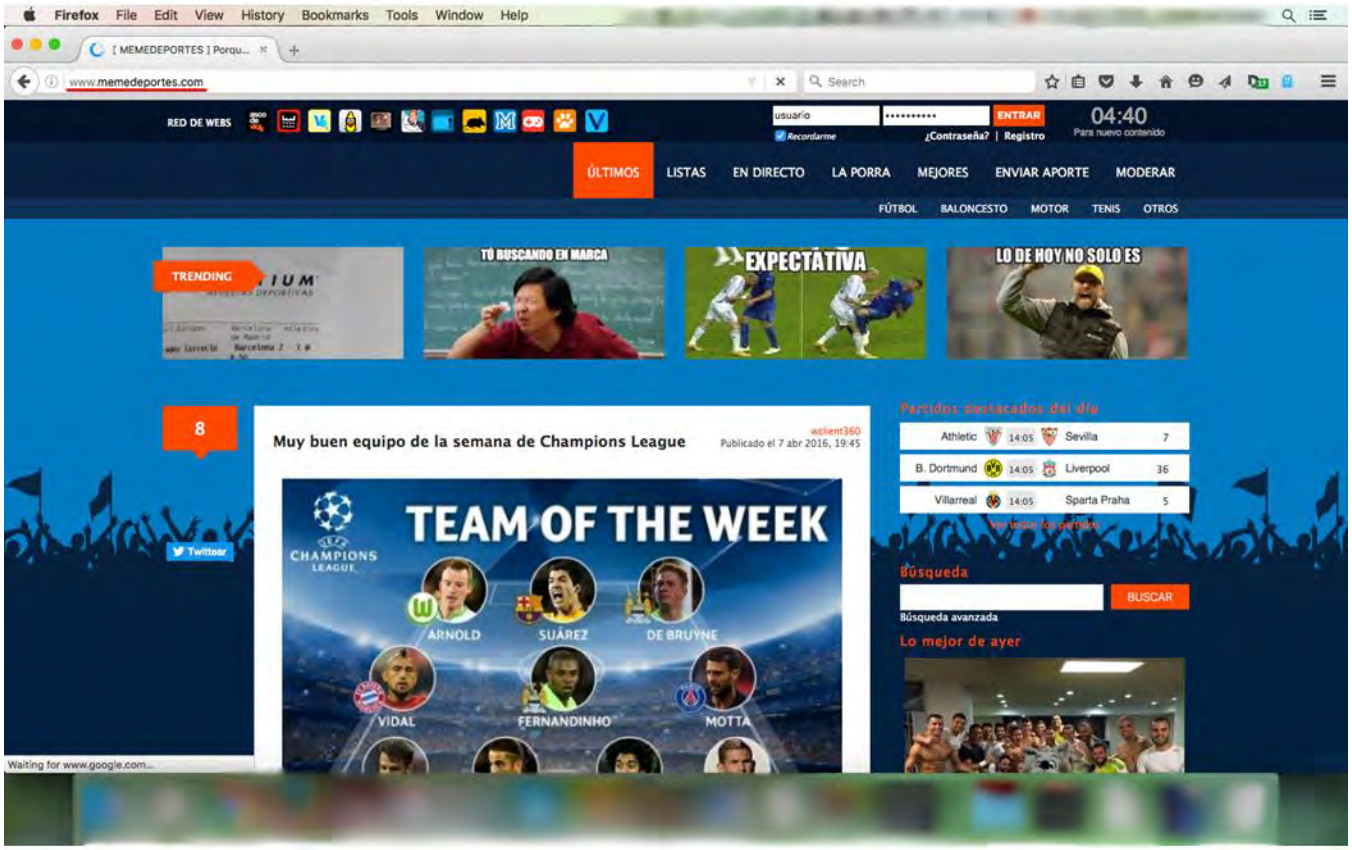

Ilustración 93: Ventana del navegador web Firefox accediendo a la página web 'www.memedeportes.com'.

Después de haberse transcurrido 8 minutos se deshabilito la ejecución de urlsnarf al darle clic al texto que dice 'Stop' en el rectángulo de opción con nombre 'Controls' de acuerdo a la Ilustración 94. Una vez que se deshabilitó urlsnarf, se seleccionó la opción 'History' y luego se le dio clic al texto 'view' para ver el tráfico que urlsnarf intercepto de un manera ordenada como se muestra en la Ilustración 95. La herramienta urlsnarf brinda la opción de descargar el tráfico web que intercepto y poder analizarlo aparte. Por consiguiente, se le dio clic al texto 'download' y se descargó el archivo 'output_1460051151.log' para analizarlo aparte y sin necesidad de estar conectado al portal web del Wifi Pineapple como se muestra en la Ilustración 96.

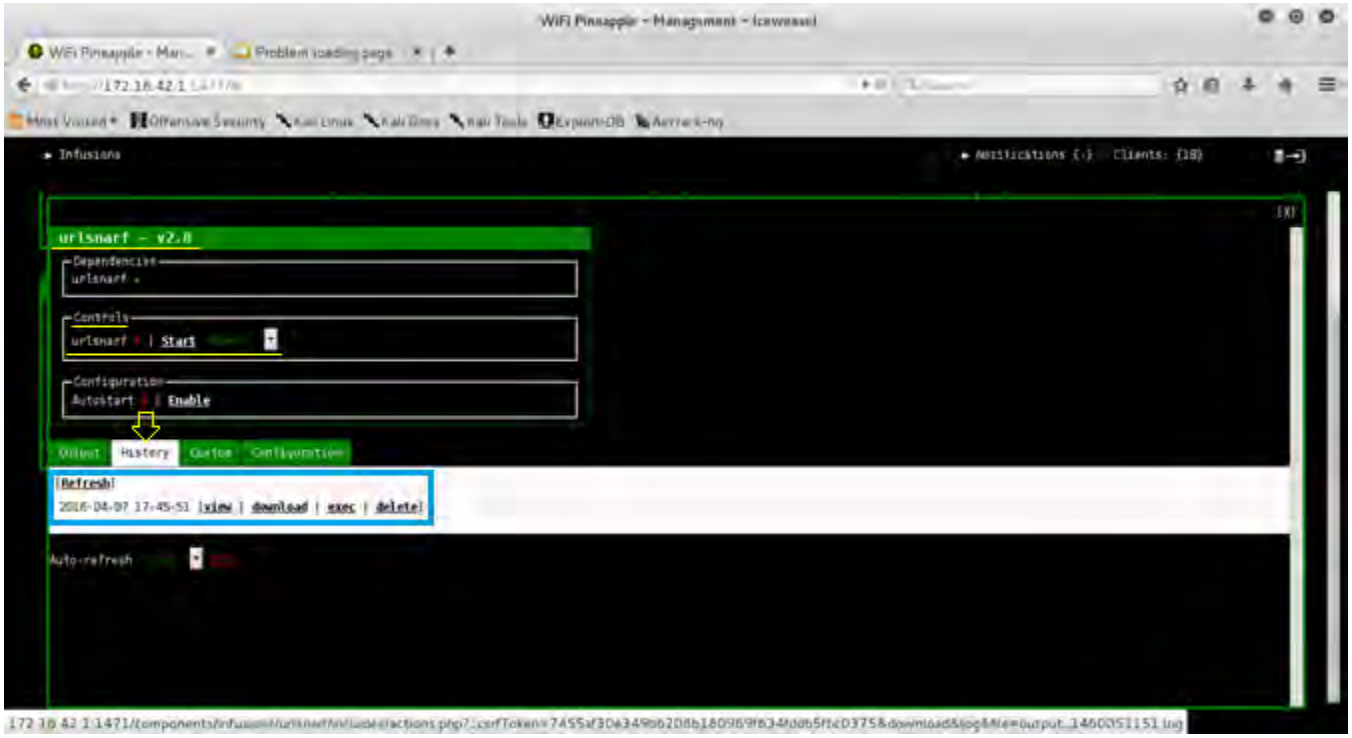

Ilustración 94: Portal de la opción 'History' de la ventana de configuración 'urlsnarf'.

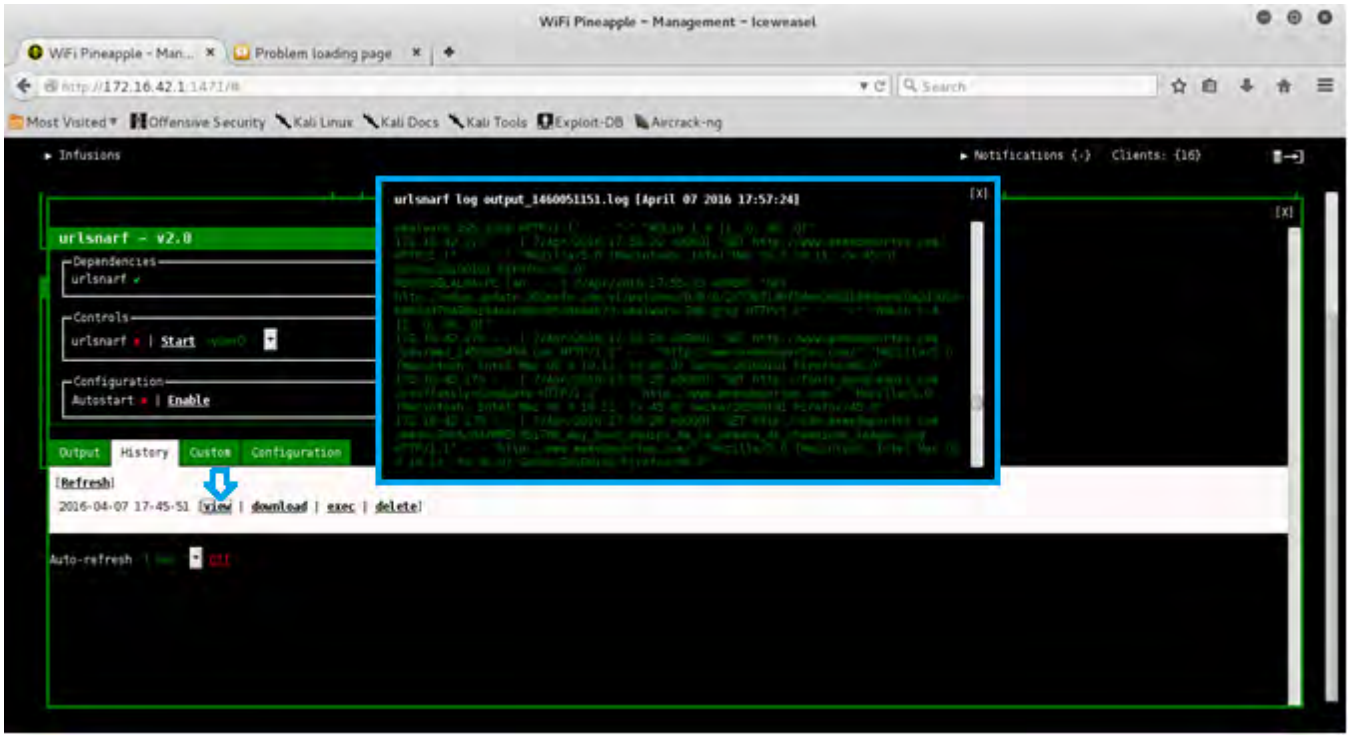

Ilustración 95: Ventana emergente de un archivo .log gestionado por el portal de la opción 'History' de la ventana de configuración 'urlsnarf'.

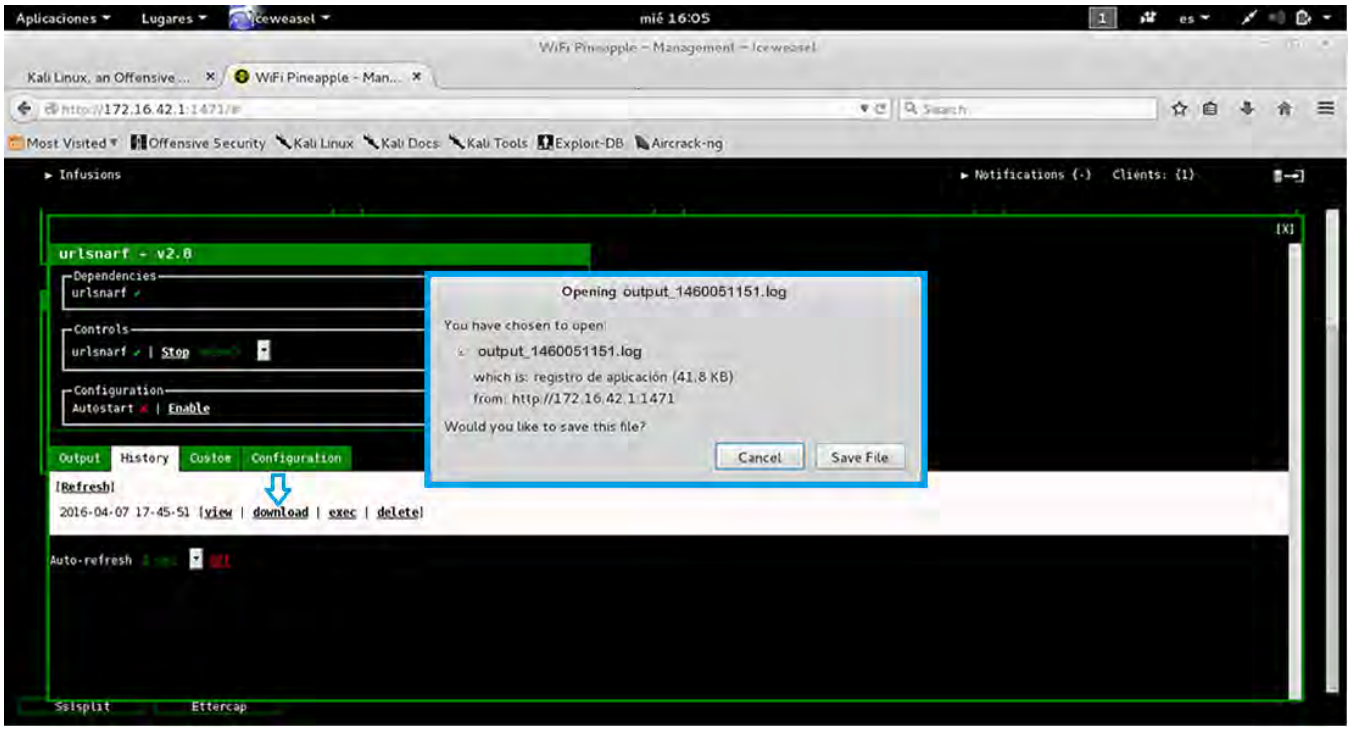

Ilustración 96: Notificación emergente para descarga el archivo 'output_1460051151.log' gestionado por el portal de la opción 'History' de la ventana de configuración 'urlsnarf'.

Una vez que se descargó el archivo .log, se abrió con un editor de texto para su análisis como se muestra en la Ilustración 96. La Ilustración 97 que concuerda con la Ilustración 95 mostró la URL 'www.memedeportes' que fue generada por la Laptop Macbook Pro (víctima) siendo interceptada por urlsnarf. Por otra parte, la Ilustración 98 muestra algunas de las URLs 'router.infolinks.com', 'www.invialgo.com', 'www.linkedin.com', 'www.facebook.com' generadas por un equipo de cómputo (víctima) llamada 'Clarissa-PC' siendo interceptado por urlsnarf. Por último, la Ilustración 99 muestra también algunas de las URLs 'cursos.uqroo.mx', 'sdup.update.360safe.com' generadas por un equipo de cómputo (víctima) llamada 'ROCIODELALBA-PC' y la URL 'clients3.google.com' para un equipo móvil llamado 'android-3f1140a7ed73cle5' que fueron interceptados por urlsnarf. Es importante mencionar que al analizar profundamente el archivo de texto generado por urlsnarf, se obtiene mucha otra información además de las URLs como lo son, nombre de la víctima que generó la URL, fecha y hora que se intercepto la URL, información del equipo de cómputo que genera las URLs, el nombre y versión del navegador web entre otra información.

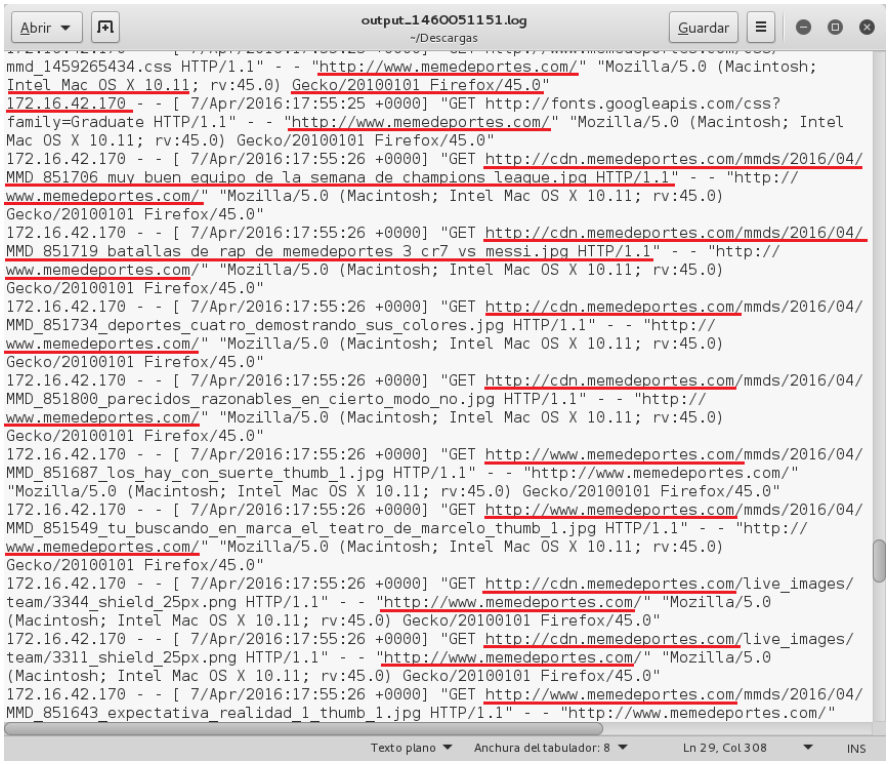

Ilustración 97: Archivo de texto output_1460051151.log mostrando URLs interceptadas por urlsnarf.

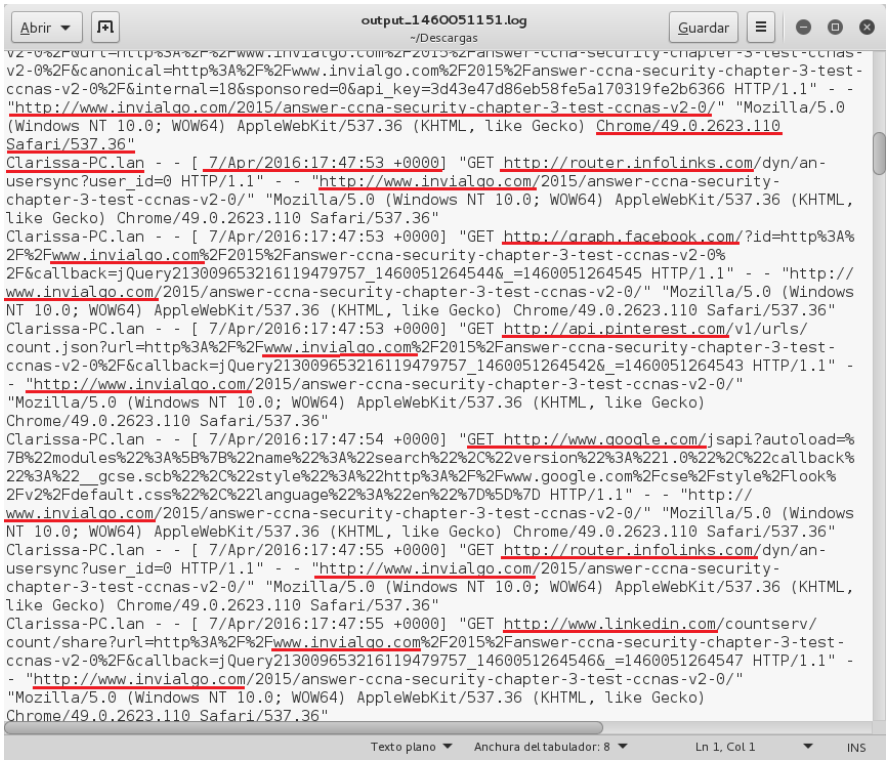

Ilustración 98 (Continuación): Archivo de texto output_1460051151.log mostrando URLs interceptadas por urlsnarf.

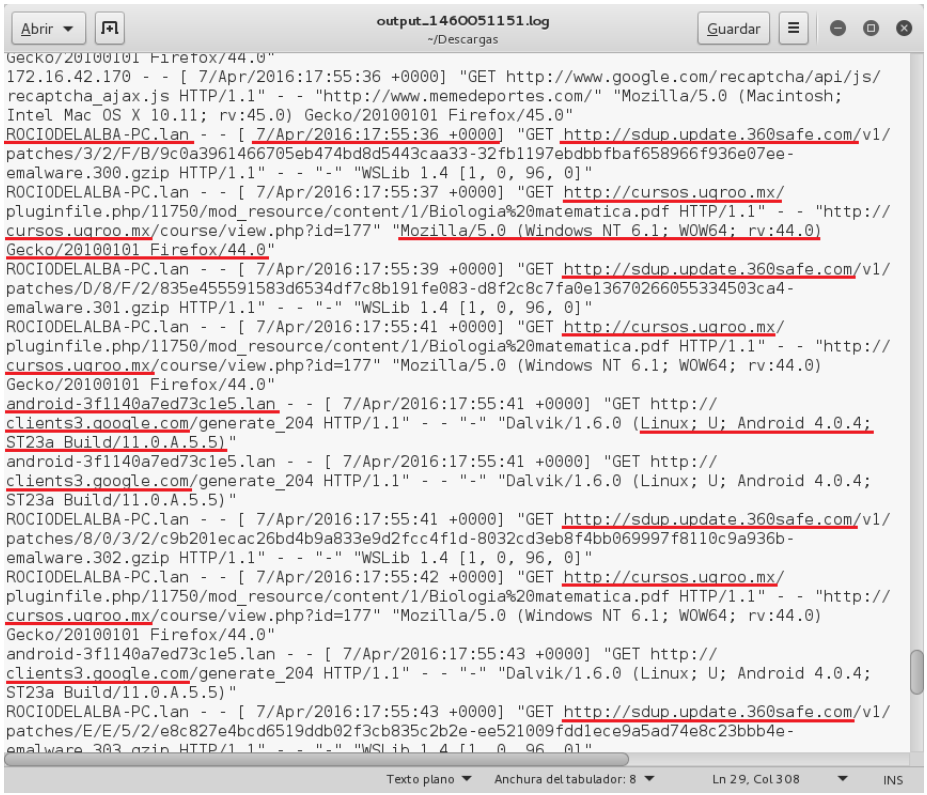

Ilustración 99 (Continuación): Archivo de texto output_1460051151.log mostrando URLs interceptadas por urlsnarf.

Capítulo 4 Resultados y Conclusiones

4.1 Resultados de las fases

Implementar las cuatro etapas en las que se dividió el desarrollo, se obtuvieron los siguientes resultados:

- Para la primera etapa que se enfocó en la recopilación de información del ambiente inalámbrico 802.11 en la Universidad de Quintana Roo, campus Chetumal se observaron los diferentes puntos de acceso con sus respectivos SSID que difunden y también se pudo obtener otra información valiosa como ESSID, BSSID, potencia de la señal (PWR), tipo de autenticación (AUTH), protocolo de cifrado (CIPHER), canal de transmisión (CH) y modo de cifrado (ENC). Al analizar esta información desplegada por la herramienta 'aircrack-ng', se pudo observar y obtener información de 3 puntos de acceso que difunden la red inalámbrica 'wlcampus' de acuerdo al radio de cobertura del adaptador alfa AWUS036h con su antena de 18 dbi que se utilizó juntamente con 'aircrack-ng' para realizar el escaneo inalámbrico. Una vez que se obtuvo información de los puntos de acceso que difunden la red 'wlcampus' se realizó un escaneo inalámbrico con 'aircrack-ng' para esos 3 puntos de acceso encontrados dándonos como resultado información para cada uno de los APs sobre los clientes conectados a ellos.

  La herramienta 'aircrack-ng' proporcionó información de los clientes por cada AP tal como potencia de la señal para transmitir (PWR), tramas recibidas (Frames), paquetes perdidos (Lost), tasa de transmisión (Rate), BSSID y las tramas 'Probe' de los clientes conectados al AP. Para corroborar la información obtenida anteriormente, se realizó un escaneo del ambiente inalámbrico con el dispositivo Wifi Pineapple y la herramienta 'site_survey' dándonos como resultado información detallada y organizada de todos los puntos de acceso detectados con sus respectivos clientes además de aquellos clientes inalámbricos que no estaban conectados a ningún AP. Se observó información por cada AP como tipo de seguridad implementada (Security:), potencia de la señal inalámbrica (Signal:) y el canal de difusión (Channel:) y esto concordaba con la información proporcionada por la herramienta 'airodump-ng' que se utilizó para monitorear la red inalámbrica 'wlcampus'. La información obtenida es esta primera etapa del desarrollo de la investigación fue de gran importancia por el hecho que el *pentester*, atacante, o usuario malicioso puede tomar decisiones acertadas del tipo de ataque que puede llevar a cabo a ciertos objetivos en específico para luego comprometer la red ya sea a través de la intercepción y/o robo de información, denegación de servicio, inyección de malware etc.

- Para la segunda y tercera etapa del desarrollo, los resultados obtenidos fueron los deseados ya que el proceso de ejecutar un ataque de punto de acceso falso es sencillo con la ayuda del dispositivo Wifi Pineapple Mark V y las herramientas tales como Karma

que ya trae integrada. Después de configurar que el Wifi Pineapple tenga salida a Internet, crear el AP falso y habilitar Karma para que dé respuestas a peticiones 'Probe' y 'Association', a los pocos segundos varios clientes inalámbricos de la red 'wlcampus' y de otras redes inalámbricas fueron víctimas de este ataque sin que ellos se dieran cuenta.

Después de 3 minutos de haber lanzado el ataque ya se habían conectado como 20 clientes al punto de acceso falso que se creó con el dispositivo Wifi Pineapple. El portal de configuración del Wifi Pineapple, ademas de mostrarnos cuantos clientes se encuentran conectados al punto de acceso falso también muestra información de las victimas tales como dirección MAC, dirección IP, nombre del equipo informático, el SSID que el equipo víctima estaba buscando y actividad más reciente. Este tipo de información es tan valiosa ya que le permite al atacante tomar decisiones para lanzar ataques más sofisticados como ataques al sistema andriod, ataque llamado 'Phising attack' etc. El ataque 'Rogue AP' no pudo haber tenido tanto éxito sin la primera etapa del desarrollo del proyecto. En la primera etapa fue donde se logró obtener información valiosa, mencionada en el párrafo anterior y en el capítulo 3, que nos ayudó a saber el tipo de ataque a lanzar, cuando lanzarlo y como lanzarlo. Por ejemplo, algo que se tiene que monitorear son las horas pico que son las horas donde los puntos de acceso tienen la mayor cantidad de clientes conectados y la cantidad del tráfico de red incrementa. El saber este tipo de información impacta a gran escala el éxito de un ataque como 'Rogue AP' y muchos otros ataques de red porque al final lo que más interesa a un atacante o usuario malicioso son los clientes inalámbricos que pueden ser víctimas de cualquier ataque informático.

- Para la cuarta etapa, al momento de extender el ataque de punto de acceso falso a un ataque de hombre en medio (Man In the Middle) interceptando parte del tráfico de red con las herramientas sslstrip y urlsnarf, los resultados obtenidos fueron los deseados aunque se complicó obtener una cuenta y contraseña de usuario al momento que se realizó esa prueba de ingresar a una página web HTTPS.

  La información interceptada primeramente por sslstrip, mostró las URLs siendo visitadas por los clientes conectados al AP falso, dirección IP de las páginas web visitadas, las peticiones HTTP GET, tipo de conexión web entre otras. Sslstrip intercepto la URL 'www.memedeportes.com' al momento que la Laptop Macbook Pro visitó esa página web. También, al momento de analizar el archivo .log generado por sslstrip del tráfico que logró interceptar se pudo concluir que algún equipo víctima estaba realizando una conexión hacia la dirección de Internet '23.64.171.27' que hace referencia al servidor del sitio web de Symantec. También se pudo observar el tráfico HTTP interceptado por sslstrip para la URL 'www.memedeportes.com' que hace referencia a la página web que se visitó con la Laptop Mac book Pro que se utilizó exclusivamente para ser víctima del ataque en cuestión y la página web 'www.mercadolibre.com.mx' interceptada donde se observó que una de las víctimas estaba realizando búsquedas de ciertos artículos

informáticos como cables y adaptadores, teclados y ratones entre otras. Por otra parte, las URLs interceptadas por urlsnarf mostraron la URL 'www.memedeportes' que fue generada por la Laptop Macbook Pro (víctima).
El archivo de texto generado por urlsnarf también mostró algunas de las URLs como 'router.infolinks.com', 'www.invialgo.com', 'www.linkedin.com', 'www.facebook.com' generadas por un equipo de cómputo (víctima) llamada 'Clarissa-PC', las URLs 'cursos.uqroo.mx', 'sdup.update.360safe.com' generadas por un equipo de cómputo (víctima) llamada 'ROCIODELALBA-PC' y la URL 'clients3.google.com' para un equipo móvil llamado 'android-3f1140a7ed73cle5'.

La información específica mencionada para el tráfico interceptado por sslstrip y urlsnarf es un parte de todo el tráfico interceptado que se muestra en el archivo de texto para ambas herramientas. Exponer toda la información interceptada por sslstrip y urlsnarf con un análisis profundo esta fuera del alcance de esta investigación. Es importante mencionar que sslstrip ya no funciona para hacer la conversión de HTTPS a HTTP ya que la mayoría de sitios web HTTPS, si no es que todas, implementan el protocolo HSTS (HTTP Strict Transfer Security). Sslstrip por sí misma no puede vulnerar el protocolo HSTS y se necesita la combinación de otras herramientas para ataques 'Man In the Middle' como bettercap, mitmf, ettercap entre otras. Lastimosamente, el sistema operativo del Wifi Pineapple solo tiene soporte para la herramienta ettercap pero al momento de probarlo en conjunto con sslstrip, ettercap era muy inestable y dejaba de funcionar casi al instante por lo que no se pudo vulnerar el protocolo HSTS. Si se hubiese podido lograr vulnerar HSTS, su hubiese podido obtener información aún más sensible como cuentas y contraseñas de correos, redes sociales entre otras. Sin embargo, las herramientas sslstrip y urlsnarf lograron interceptar información valiosa de las víctimas obteniendo asi resultados favorables para la cuarta (última) etapa del desarrollo del proyecto que consistía en el ataque 'Rogue Access Point' extiendose luego a un ataque 'Man In The Middle'.

El ataque Rogue Access Point también se llevó a cabo en un ambiente controlado, es decir, se tenía control del punto de acceso legítimo. Como primera instancia, se ejecutó el ataque Rogue AP hacia un el punto de acceso legítimo configurado en modo abierto. Para el AP genuino, se utilizó el un AP LINKSYS E900 configurado en modo abierto y con el servició de dhcp habilitado para conectar a los clientes inalámbricos automáticamente al AP. Para este escenario se utilizaron 3 clientes inalámbricos: una laptop con Windows 10, una laptop con Mac OS X 10.11.4 y un móvil Iphone 5s. Estos tres clientes inalámbricos se conectaron al AP legítimo antes de lanzar el ataque. Luego se colocó el AP genuino a una distancia más lejana que el dispositivo Wifipineapple utilizado para lanzar el ataque. Al ejecutar el ataque de Punto de Acceso falso al AP LINKSYS E900, a los pocos segundos que el SSID falso se difundió a través del Wifipineapple, los 3 clientes se conectaron al AP de manera automática sin notificar al usuario.

Por otra parte, el ataque se repitió hacia el mismo AP legítimo, pero con algunos cambios en la configuración. Primero, se habilito el protocolo de seguridad WPA2 para poder conectar a los

clientes al AP a través de una contraseña y cifrar el tráfico de red que transita en la red inalámbrica. Nuevamente, se conectaron los 3 clientes mencionados anteriormente al AP genuino. Al ejecutar el ataque para este escenario, ya no funcionó como la vez anterior donde los 3 clientes se conectaron automáticamente al AP sino que al momento que los adaptadores de red de los 3 equipos informáticos recibieron respuestas 'Probe' de la herramienta Karma (Wifipineapple) para conectarse a una red abierta y falsa, se le notificó al usuario. La advertencia indicaba que se estaba realizando una conexión a una red inalámbrica abierta dando la opción de aceptar o no la conexión. Para laptop con Windows 10 se procedió a aceptar la conexión al AP falso. Sin embargo, se habilito un servicio de VPN con la aplicación Hotspot Shield para crear una conexión cifrada y navegar y acceder a sitios web y servidores en internet de manera segura. El en dispositivo Wifipineapple se ejecutó la herramienta sslstrip y urlsnarf para interceptar el tráfico de la laptop hacia y de internet y vice versa. Al momento de navegar en diferentes sitios web, el tráfico interceptado por sslstrip y urlsnarf estaba cifrado y solo un 5% del tráfico interceptado era legible y prácticamente insignificante. Cabe mencionar que habilitar WPA2 en un punto de acceso no previene un ataque Rogue AP pero añade una capa más de seguridad entre los clientes inalámbricos y el AP que puede influir negativamente en el éxito del ataque Rogue AP. También, utilizar un servicio de VPN por parte de los usuarios es importante para mantener nuestra información que transita en la red privada. Aunque seamos víctimas de un ataque Rogue AP, al utilizar una VPN para navegar y acceder a sitios web y servidores en internet, se agrega una capa de seguridad fuerte para proteger nuestra información de ser descifrada por terceros. No es sencillo lanzar ataques hacia clientes que utilizan VPNs para descifrar la información que generan porque se necesita herramientas y técnicas más sofisticadas como ingeniería social para interceptar y obtener información sensible y valiosa de las víctimas. Es importante mencionar también que aunque la utilización de una VPN no previene un ataque Rogue AP, está protege la integridad de la información en caso de que sea interceptada por terceros.

4.2 Conclusiones

En esta tesis, el problema que se analizó fue el hecho qua la información de los usuarios que transita en red inalámbrica 'wlcampus' puede ser fácilmente interceptada por terceros. El problema radica en que no existe ningún tipo de cifrado en los datos transmitidos sobre la capa 2 (capa de enlace de datos dado) debido al privilegio que se le da a los usuarios para conectarse fácilmente a la red y utilizar cualquier servicio disponible. El ataque llamado 'Rogue AP' fue llevado a cabo hacia la red inalámbrica 'wlcampus' con la intención de demostrar que esta red es altamente vulnerable por el simple hecho de que no tiene ningún tipo de autenticación como WPA y/o WPA2 y no implementa ningún mecanismo de cifrado como TKIP y/o AES. El ataque 'Rogue AP' fue realizado con la ayuda del dispositivo Wifi Pineapple Mark V que es un dispositivo especializado para la auditoría de redes inalámbricas. Este dispositivo realizó el ataque 'Rogue AP' de manera automática utilizando herramientas como PineAP, MK5 Karma,

Beacon Response, Auto Harvester entre otras y sin necesidad de ejecutar varios comandos manualmente. Después del éxito en realizar el ataque de un AP falso, se lanzó con mucha facilidad un ataque llamado 'Man In The Middle' donde la información de los usuarios conectados al AP falso fue interceptada. De esta manera, se comprobó que la red inalámbrica 'wlcampus' es susceptible y vulnerable a ataques como 'Rogue AP' y 'Man in the middle' que pone en riesgo la integridad y privacidad de la información de los usuarios que utilizan esta red inalámbrica.

Por lo tanto, es necesario que se aborde este problema por parte de las entidades responsables de la Universidad de Quintana Roo, campus Chetumal para implementar distintos mecanismos de seguridad como los que se enuncian a continuación teniendo como objetivo garantizar la seguridad de la información de los usuarios que utilizan la red 'wlcampus'.

4.3 Recomendaciones

Propuesta de plan de acción: (Inc., 2015)

Hacer esto:	Resultado de la acción:
Establecer reglas estrictas y asegurarse de que estén bien publicadas.	Sólo el personal autorizado de TI puede conectar equipos de red. Todos los dispositivos que se conectan a la red, incluyendo los puntos de acceso inalámbricos, se ajustan a las políticas de seguridad de la empresa o institución. **Nota**: Algunas universidades incluso expulsan o suspenden a los estudiantes que se encuentran atrapados con puntos de acceso no autorizados o redes ad-hoc.
Cambiar las reglas de clasificación para los APs o dispositivos informáticos no autorizados.	De forma predeterminada, los dispositivos desconocidos se clasifican como sospechosos. Cuando se cambia este valor predeterminado a no autorizado, el controlador clasifica automáticamente cualquier punto de acceso de terceros o clientes como un AP no autorizado, y se puede aislar opcionalmente el punto de acceso al descartar todos los paquetes hacia y desde el dispositivo.
Eliminar los puntos de acceso benignos de la lista de APs falsos para que los APs no autorizados se destacan.	Cuando se agrega SSID de redes seguras y / o nombres de proveedores a la lista de SSID que pueden introducirse en la red, estos puntos de acceso no se pueden clasificar como no autorizados o falsos.
Añadir intrusos conocidos a la lista de no autorizados.	Puntos de acceso de terceros están aislados cuando se añaden a la lista de no autorizados. Todos los paquetes se descartan hacia y desde estos puntos de acceso.
Utilice una fuerte seguridad	El estándar de seguridad IEEE 802.11i utiliza IEEE 802.1X para la autenticación mutua entre la red y el cliente. Esto significa que los clientes que intentan acceder a los recursos de red deben ser autenticados por la red. En una línea similar, el cliente verifica la autenticidad de la infraestructura de red al que se está uniendo antes de comenzar la transmisión de datos. Con el protocolo 802.1X, las credenciales utilizadas para la autenticación, tales como contraseñas de inicio de sesión, no se transmiten sin cifrar sobre el medio

	inalámbrico. Además, 802.1X proporciona las claves de cifrado dinámicas por usuario, para cada sesión así eliminando la carga administrativa y los problemas de seguridad asociados con las claves de cifrado estáticas. La seguridad está configurado en perfiles de WLAN.
Utilice el escaneo activo de puntos de acceso, además del escaneo pasivo.	El escaneo activo envía tramas de tipo 'probe' con un nombre SSID nulo para buscar puntos de acceso y clientes no autorizados. El escaneo activo está habilitado por defecto en los radio-perfiles. Se recomienda que no se cambie esta configuración.
Asegurarse de que se tenga una firma inalámbrica habilitada y se debe cambiar sobre una base regular.	Una firma inalámbrica es un conjunto de bits en una trama de gestión enviado por un punto de acceso como un identificador. Si alguien intenta simular los paquetes de gestión de un punto de acceso, el administrador de la Red puede detectar el intento de suplantación.
Asegurarse que esté habilitado el registro (logging) y comprobar los mensajes de registro y mensajes traps de actividad sospechosa.	Por defecto, un controlador genera un mensaje de registro cuando se detecta o desaparece un equipo no autorizado.
Inmediatamente investigar los puntos de acceso ad-hoc y aumentar la seguridad de ellos o eliminarlos.	Una red ad hoc es uno que se forma directamente entre dos dispositivos cliente. Redes ad hoc suponen una amenaza para una empresa o institución debido a que los controles de seguridad impuestas por la infraestructura se pasan por alto. Uno de los peligros es un empleado que trae una laptop con adaptador inalámbrico habilitado, se conecta a un puerto por cable en el trabajo, y deja la interfaz inalámbrica habilitada. En este escenario, un hacker en una zona vecina se podría conectar directamente al cliente, creando una amenaza para la seguridad de la red cableada. El hacker en este punto podría buscar información sobre el dispositivo cliente del empleado, y potencialmente obtener acceso a la red corporativa a través de las interfaces inalámbricas y por cable simultáneamente. Esta situación puede poner a la empresa en violación de las políticas de regulación para su industria. El agujero de seguridad proporcionada por los puntos de acceso ad-hoc no es la red ad-hoc en sí, sino el puente que proporciona a otras redes.
Inmediatamente investigar tramas de puentes inalámbricos y eliminar la fuente.	Un atacante utiliza una laptop con dos adaptadores inalámbricos-Una tarjeta es utilizada por el punto de acceso no autorizado y el otro se utiliza para reenviar solicitudes a través de un puente inalámbrico al punto de acceso legítimo. .
Utilice switches gestionados de la red y utilizar su seguridad basada en puertos para permitir sólo determinadas direcciones MAC o deshabilitar los puertos no utilizados.	Un punto de acceso conectado al azar en los puertos de este switch no funcionará.
Considere el uso de direcciones IP estáticas en	Cuando se utiliza direcciones IP estáticas, un intruso que instala un punto de acceso falso tiene que asignar manualmente una dirección IP al punto de acceso antes de que pueda tener acceso a la red.

lugar de haberlos asignados por un servidor DHCP.	
Activar contramedidas automáticas para reaccionar inmediatamente a los equipos no autorizado o equipos sospechosos.	Las contramedidas pueden atacar o aislar transmisores no autorizados y / o sospechosas empleando diversos métodos de ataque. (Honeypot)

Implementación de un sistema basado en sensores llamado WIPS (Wireless Intrusion Prevention System)

Un sistema de prevención de intrusiones inalámbrico (WIPS) es un dispositivo de seguridad dedicado o aplicación de software integrado que supervisa y monitorea el espectro de radio de red de una LAN inalámbrica para puntos de acceso falsos y otras amenazas inalámbricas. Un WIPS compara las direcciones MAC de todos los puntos de acceso inalámbrico en una red contra las firmas conocidas y previamente autorizadas de los puntos de acceso inalámbricos conocidos y alerta al administrador cuando se encuentra una discrepancia. Para eludir la suplantación de direcciones MAC, algunos WIPS de gama alta son capaces de analizar las firmas de radiofrecuencia únicas que generan los dispositivos inalámbricos y bloquear las huellas digitales de radio de equipos informáticos desconocidos. (Rouse, 2015)

El PCI Security Standards Council recomienda el uso de WIPS para el escaneo inalámbrico de red. Además de proporcionar una capa de seguridad para redes LAN inalámbricas, un WIPS también es útil para el monitoreo del rendimiento de la red y descubrir puntos de acceso con errores de configuración. Hay tres formas básicas para desplegar un WIPS. La primera, que es la menos popular e inferior a las otras dos, que se conoce como segmentación de tiempo o de tiempo compartido. En este tipo de instalación, el punto de acceso inalámbrico cumple una doble función, proporcionando el tráfico de red con conectividad inalámbrica mientras escanea de forma periódica para los puntos de acceso no autorizados. En el segundo enfoque, que se conoce como WIPS integrado, es un sensor que está integrado en el punto de acceso autorizado que escanea continuamente las radio frecuencias en busca de puntos de acceso no autorizados. En el tercer método, que se conoce como WIPS superposición, sensores se despliegan a lo largo de un edificio para monitorear las frecuencias de radio. Los sensores transmiten los datos que recogen a un servidor centralizado para su posterior análisis, toma de acción y el almacenamiento de registro de archivo. Este enfoque es más caro, ya que requiere hardware dedicado, pero también se cree que es más eficaz. (Rouse, 2015)

Hardware WIPS superpuesta se asemeja a un servidor de rack y los sensores asociados se asemejan a puntos de acceso Wi-Fi. La mayoría de los sistemas WIPS de superposición comparten los mismos componentes fundamentales: (Rouse, 2015)

- Sensores - monitorea el espectro radioeléctrico y envía registro de archivos (logs) a un servidor de administración centralizado.

- Servidor de administración - recibe información captada por los sensores y toma las acciones de defensa adecuados basándose en esta información.
- Servidor de base de datos - almacena y organiza la información capturada por los sensores.
- Consola - proporciona una interfaz para los administradores a la hora de configurar y gestionar los WIPS.

Mientras que el WIPS de superposición ofrece muchas características y protecciones valiosas, puede ser bastante costoso dependiendo del número de sensores y las características de los servidores. Es importante mencionar que el sistema WIPS es hasta la fecha el sistema más eficaz para la detección y prevención de ataques de punto de acceso falso.

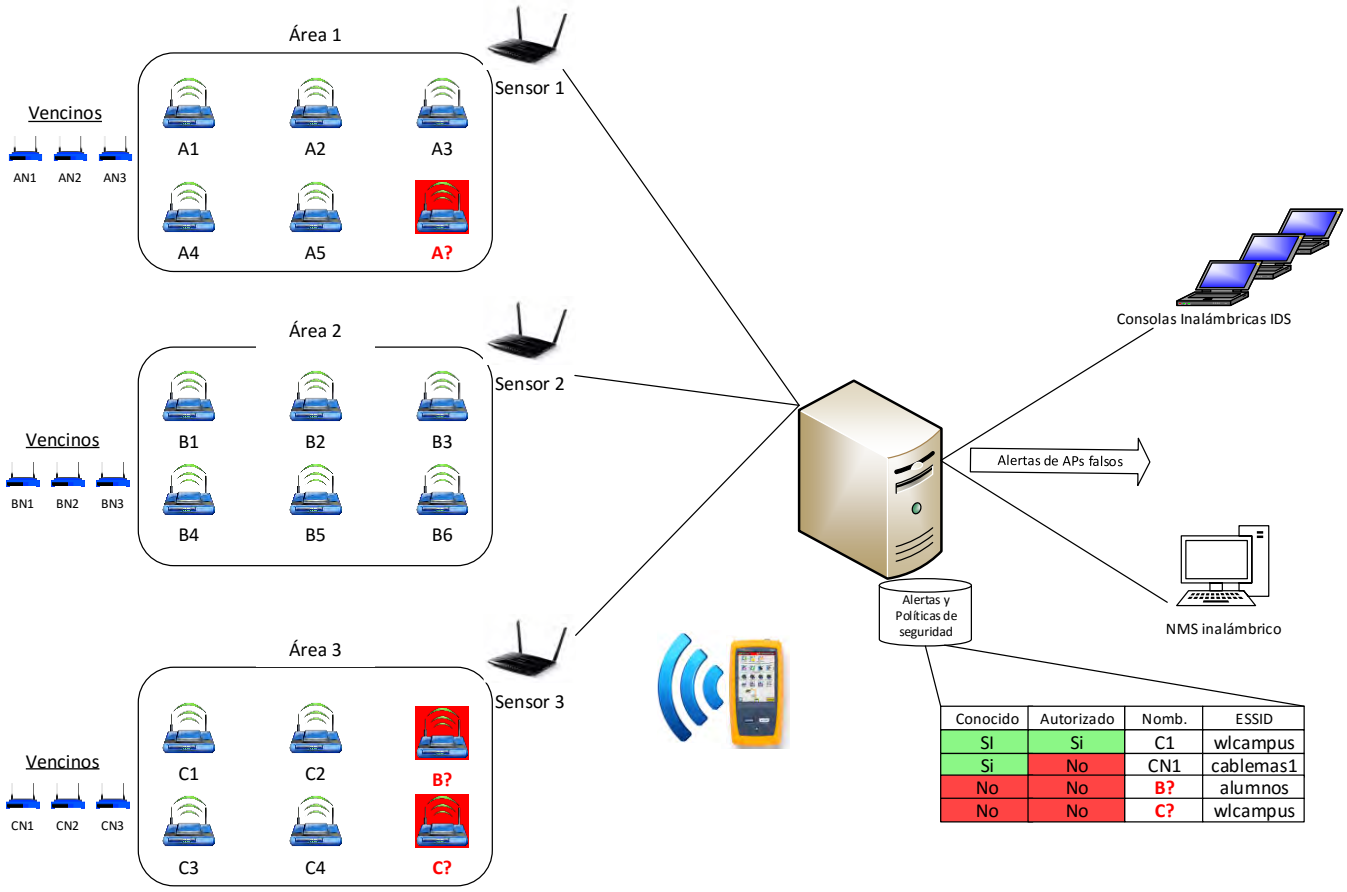

Ilustración 100: Topología de un WIPS.

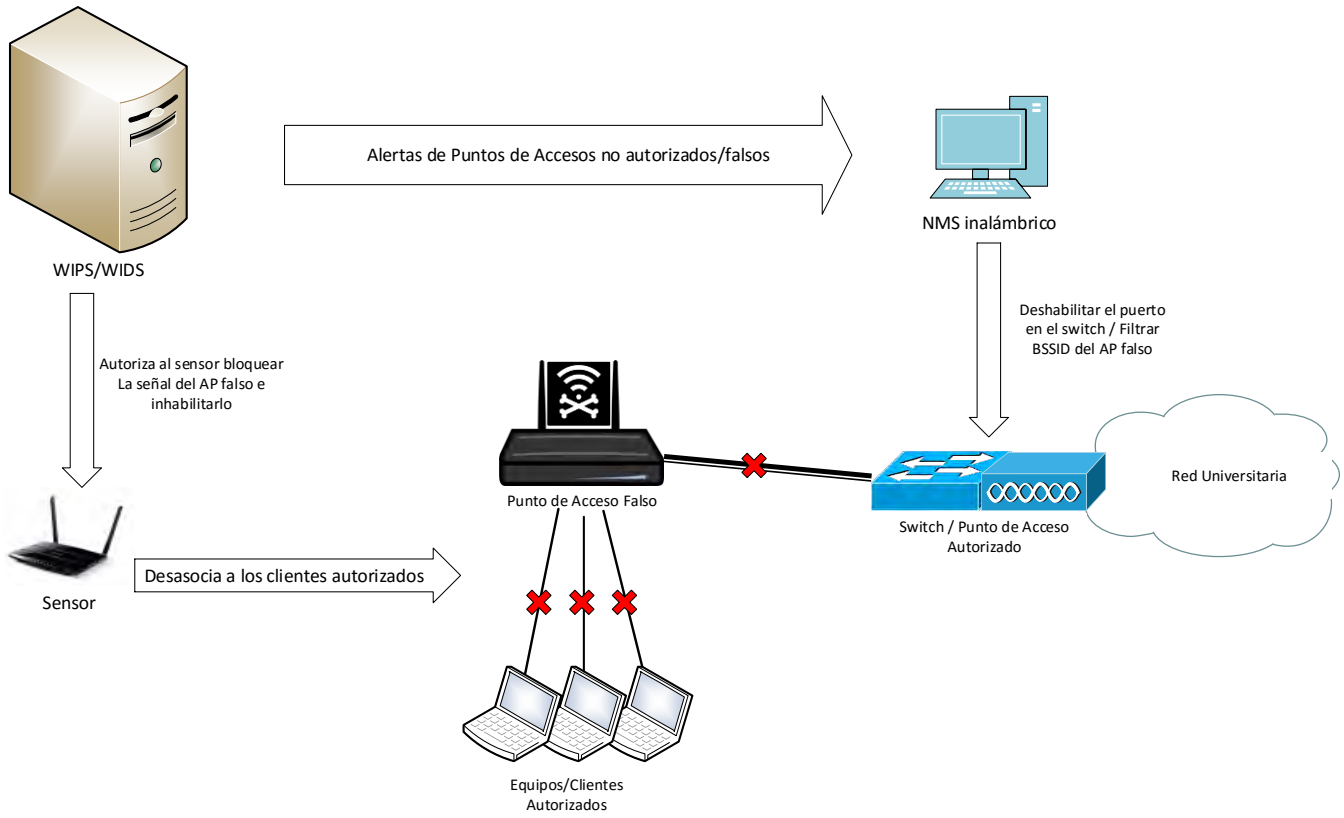

Ilustración 101: Detección y prevención de un ataque Rogue Access Point a través de un WIPS/WIDS

Filtrado de direcciones MAC

Todo adaptador de red (término genérico de la tarjeta de red) tiene su propia dirección física (que se denomina dirección MAC). Esta dirección está representada por 12 dígitos en formato hexadecimal divida en grupos de dos dígitos separados por guiones. Las interfaces de configuración de los puntos de acceso les permiten, por lo general, mantener una lista de permisos de acceso (llamada ACL; Lista de control de acceso) que se basa en las direcciones MAC de los dispositivos autorizados para conectarse a la red inalámbrica. Esta precaución algo restrictiva le permite a la red limitar el acceso a un número dado de equipos. Sin embargo, esto no soluciona el problema de la seguridad en las transferencias de datos.

Mejorar la autenticación

Para administrar la autenticación, autorización y contabilidad (AAA) de manera más eficaz, se puede usar un servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota). El protocolo RADIUS (definido por la RFC 2865 y la 2866) es un sistema cliente/servidor que permite administrar de manera central cuentas de usuarios y permisos de acceso relacionados.

Configuración de una VPN

Una red privada virtual (Virtual Private Network (VPN)) es una tecnología que proporciona una manera de proteger información que es transmitida sobre Internet. Esta tecnología permite a los usuarios establecer una conexión cifrada virtual punto a punto mejor conocido como un 'túnel' hacia los recursos que se desea acceder vía Internet. Para todas las comunicaciones que requieran un alto nivel de seguridad, es mejor utilizar un cifrado cerrado de datos al instalar una VPN.

Utilización de Honeypots Inalámbricos

Honeypot significa en inglés, "tarro de miel". Es una herramienta que se usa casi exclusivamente en el campo de la seguridad informática. Su función se basa en atraer y analizar ataques realizados por bots o hackers. Su objetivo es atraer atacantes para ver sus patrones de ataque, generar diccionarios para recopilar que palabras usan en ataques (para no usarlas en tu sistema), conocer al enemigo y su perfil. Un honeypot puede implementarse utilizando un punto de acceso de bajo costo en modo abierto (sin ningún tipo de autenticación y cifrado) desplegado como una red por separado con algunos clientes conectados a ella y también con un poco de tráfico inalámbrico transitando en la red. Si un atacante está en busca de un punto de acceso en modo abierto, el honeypot implementado lo atraerá. Una vez que el atacante se conecta al honeypot, todas las actividades que él/ella realicen serán monitoreadas. Los administradores de red podrán estudiar los métodos que los atacantes utilizan y podrán ver qué tipo de información están intentando capturar, que tipos de ataques con malware están intentando de inyectar en la red. Por consiguiente, un honeypot tiene la capacidad de mantener a un atacante temporalmente activo y alerta al administrador para tomar las medidas necesarias con el objetivo de salvaguardar la red.

Resumen de Mecanismos de Seguridad para implementar (Leira, May 2010)

Autenticación:

- Utilizar IEEE 802.1X

Protocolo de Autenticación:

- PEAP
- TTLS
- TLS (para una infrastructura de llave pública (PKI))

Estos protocolos no son mutuamente exclusivo y pueden implementarse simultáneamente.

Servidor RADIUS:

- FreeRADIUS
- Microsoft IAS/NPS
- Cerebrum

Cabe mencionar que el administrador de red tiene la libertad de escoger un servidor RADIUS de acuerdo a su propio criterio pero no todos los servidores implementan el protocolo EAP, métodos PEAP, TTLS y TLS que deberían ser requerimientos fundamentales.

Cifrado:

- Como mínimo TKIP (WPA)
- preferiblemente AES (WPA2)

Lo ideal sería utilizar únicamente AES pero por razones de compatibilidad, la mayoría de las redes también deben implementar TKIP. Ambos protocolos pueden utilizarse simultáneamente pero existe la posibilidad que algunos clientes tengan problemas a la hora de conectarse a la red.

Certificado de Seguridad:

- Auto-generado
- adquirido de un CA reconocido.

La opción que se elija dependerá de la situación y necesidades de la red. Teóricamente, un certificado de seguridad auto-generado es más confiable pero en práctica, el riesgo asociado con un certificado comprado es bajo. Se deberá tener un certificado para el servidor RADIUS pero la decisión de utilizarlo o no se basa en la opción de implementar una base de datos de usuarios o administrar un PKI.

Privilegios de Usuario

Dividir y alojar a los usuarios en diferentes VLANS dependiendo de su grupo de usuario al que pertenece ya sea estudiante, profesores, visitantes etc. Utilizar RADIUS configurado para delegar dinámicamente la asignación de una VLAN y solo un SSIF. La VLAN deseada puede ser asignado por el servidor RADIUS o puede ser obtenido de la base de datos de usuario si contiene la información necesaria. Utilizar filtros de red ordinarios para asignar privilegios por cada VLAN.

Base de Datos de Usuario

Implementar una base de datos de usuario para la autenticación. Diferentes tipos de base de datos de usuarios existen pero la base de datos que se implemente debe facilitar su gestión, guardar las contraseñas de manera confiable y la verificación de las contraseñas deberá realizarse con MS-CHAPv2. También deberá tener la capacidad de comunicarse con el tipo de servidor RADIUS que haya sido implementado.

Utilización de Puntos de Acceso autónomos y simples (Productos SoHo)

Utilizar WPA-PSK con una contraseña de 20 caracteres como mínimo. Los caracteres de la contraseña deberán ser alfanuméricos ya que los procedimientos de algunos productos para generar las claves no funcionan correctamente con caracteres especiales.

Puntos a tener en cuenta cuando se implementan puntos de acceso autónomos.

- No se debe permitirle al usuario poder ver y acceder a la dirección IP administrativa del AP. Establecer la dirección IP administrativa del AP en una red que no puede ser accesible de manera inalámbrica.
- En caso de tener varios VLANS, el AP deberá tener un enlace 'trunk'. Es importante que los enlaces 'trunk' no tengan más VLANs de las necesarias para la red inalámbrica.
- Utilizar una comunicación cifrada a la hora de configurar (SSH/HTTPS).

Puntos a tener en cuenta cuando se tiene una infraestructura inalámbrica con controlador o controladores

- Asignar a los puntos de acceso a una red administrativa por separado que únicamente se le permita comunicarse con el controlador inalámbrico (todo el tráfico entrante y saliente pasa por el controlador).
- Utilizar una comunicación cifrada a la hora de configurar (SSH/HTTPS).
- Tomar ventaja de las funciones del controlador para monitorear activamente cualquier punto de acceso sospechoso o falso que aparezca en la red.

Bibliografía

Álvarez, Y. P. (2006). *Tesis: SEGURIDAD AL ACCESO DE INFORMACIÓN EN LA IMPLANTACIÓN DE UNA RED INALÁMBRICA.* Caracas, Venezuela: Universidad Central de Venezuela.

Alan Holt, C.-Y. H. (2010). Chapter 1: Introduction, Chapter 3: Medium Access Control, Chapter 4: Physical Layer, Chapter 6: Wireless Security, Chapter 7: Configuring Wireless Networks. En C.-Y. H. Alan Holt, *802.11 Wireless Network: Security and Analysis.* London, Dordrecht, Heidelberg, New York: Springer-Verlag.

Andres, R. (12 de Octubre de 2014). *Cómo conectarte, crear y configurar tu propia red VPN*. Obtenido de computerhoy.com: http://computerhoy.com/paso-a-paso/internet/como-conectarte-crear-configurar-tu-propia-red-vpn-7981

Beggs, R. W. (Junio de 2014). Part 1: The Attacker's Kill Chain, Part 2: The Delivery Phase (Chapter 8 and 9). En R. W. Beggs, & V. B. Jones (Ed.), *Mastering Kali Linux for Advanced Penetration Testing* (págs. 15-168, 203-256). Birmingham, Reino Unido: Pack Publishing Ltd.

CCM Benchmark Group. (Junio de 2014). *Wi-Fi wirless network security (802.11 or WiFi)*. Obtenido de ccm.net: http://ccm.net/contents/806-wi-fi-wireless-network-security-802-11-or-wifi#q=wireless+network+security&cur=1&url=%2F

Gast, M. S. (2005). *802.11 Wireless Networks: The Definitive Guide* (Second Edition ed.). (M. Loukides, Ed.) Sebastopol, Estados Unidos: O'Reilly Media, Inc.

Inc., J. N. (14 de 09 de 2015). *wireless rogue ap*. Obtenido de www.juniper.net: http://www.juniper.net/techpubs/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-rogue-ap.html

Johns, A. (enero de 2015). *Mastering Wireless Penetration Testing for Highly Secured Environments.* (K. C. Kunal Parikh, Ed.) Birmingham, Reino Unido: Pack Publishing Ltd.

Joshua Wright, J. C. (2015). Part I Hacking 802.11 Wireless Technology. En J. C. Joshua Wright, *HACKING EXPOSED WIRELESS: Wireless Security Secrets & Solutions* (3rd Edition ed., pág. 29 to 263). New York, Chicago, San Francisco, Athens, London, Madrid, Mexico City, Milan, New Delhi, Singapore, Sydney, Toronto, United States: McGraw-Hill Education.

Leira, J. (May 2010). *Recommended Security System for wireless networks* (Best Practice Document ed.). (TERENA, Trad.) Norway: UNINETT led working group on mobility.

Luz, S. D. (23 de Agosto de 2015). *10 herramientas imprescindibles para realizar auditorías Wi-Fi con PC*. Obtenido de redeszone.net: http://www.redeszone.net/2015/08/23/10-herramientas-imprescindibles-para-realizar-auditorias-wi-fi-con-pc/

Martín, M. M. (enero 2015). *Proyecto Fin de Carrera: Análisis, diseño y despliegue de una red WiFi en Santillana del Mar.* Madrid, España: Escuela Politécnica Superior, Universidad Autónoma de Madrid.

Montoya, D. E. (2014). 2.10 Identificación de vulnerabilidades en aplicaciones web, 2.11 Vulnerabilidades en servidores HTTP, 2.12 Identificación y Ataque de versiones vulnerables de OpenSSL, Capítulo IV: Ataques en el segmento de red local. En D. E. Montoya, *Python Para Pentesters* (págs. 92-147, 233-286). Madrid: Zeroxword Computing S.L.

Nagy, A. V. (20 de March de 2013). *802.11ac Channel Planning*. Obtenido de revolutionwifi.net: http://www.revolutionwifi.net/revolutionwifi/2013/03/80211ac-channel-planning.html

Ola, G. (Otoño 2013). *Tesis: PENETRATION TESTING ON A WIRELESS NETWORK--USING BACKTRACK 5.* Turku, Finlandia: Turku University of Applied Sciences.

Poole, I. (2015). *Wi-Fi / WLAN Channels, Frequencies, Bands & Bandwidths*. Obtenido de radio-electronics.com: http://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php

Rouse, M. M. (Marzo de 2015). *WIPS (wireless instrusion prevention system)*. Obtenido de whatistechtarget.com: http://whatis.techtarget.com/definition/WIPS-wireless-intrusion-prevention-system

Systems, C. (2015). */cisco/cisco1/course/module4/4.4.4.8/4.4.4.8*. Obtenido de http://itroque.edu.mx: http://itroque.edu.mx/cisco/cisco1/course/module4/4.4.4.8/4.4.4.8.html

Viggiani, F. (Mayo de 2013). *Tesis: An approach to automated penetration testing on stability and integrity for usage in production environments.* Stockholm, Suecia: KTH Royal Institute of Technology, NTNU Norwegian University of Science and Technology.