UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

COLEGIO DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

Mitigación de vulnerabilidades en una WLAN con la implementación de hardening

TESIS

PARA OPTAR POR EL TÍTULO DE

LICENCIADA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

PRESENTA:

MAGNOLIA ALCALÁ GARCÍA

DIRECTOR

M. EN C. MAGALI CORTEZ VÁZQUEZ

Ciudad de México, agosto de 2018.

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

Dedicatoria

Esta tesis se la dedico especialmente a la familia Serrano Martínez:

Leticia Martínez Aparicio,

Sotico Serrano Méndez

y

Daniel J. Serrano Martínez

Por su infinita bondad, paciencia, consejos y por haberme brindado su apoyo incondicional cuando más lo necesite.

A la familia Gonzales Flores:

Karitza Flores Gonzales

y

Minerva Flores Chávez

Por haber creído en mí y brindarme su apoyo incondicional, pero especialmente por no dejarme caer.

A mis padres:

Ofelia García Cruz

y

Abelardo Alcalá Sánchez

Por haberme dado las bases de mi educación ya que gracias a ello puede continuar con mis estudios y cumplir una de mis grandes metas.

Agradecimientos

Le agradezco profundamente a la familia Serrano Martínez y a la familia Flores Gonzales que me brindaron su apoyo incondicionalmente cuando más lo necesité, ya que gracias a ello pude iniciar y concluir la presente tesis, dándome paso a iniciar un nuevo ciclo.

A mi directora de tesis **M en C. Magali Cortez Vásquez** por haberme aceptado como una de sus tesistas, por su tiempo y paciencia que me brindo en el seguimiento de este trabajo a pesar de no haber sido un tema de su área.

Agradezco a mis lectores:

A la **Dra. Silvia Alejandra Andrade**. Por haber aceptado ser parte de mis lectores donde se tomó el tiempo y dedicación para realizar la lectura de dicha tesis, al **M. en C. José Ignacio Castillo** por haberse dado el tiempo necesario para llevar a cabo de manera minuciosa la lectura de este trabajo, para así poder enriquecerlo a partir de sus observaciones y correcciones, al **M. en C. Joel Jazbek Buendia** por haberme despejado muchas dudas que se me presentaron a lo largo de la tesis y el haber aceptado ser uno de los lectores de este trabajo, donde tuvo el tiempo y dedicación necesaria para la lectura.

Le agradezco inmensamente a Daniel Javier Serrano Martínez por ser un modelo a seguir, así como haberse dado el tiempo necesario para aconsejarme, apoyarme, compartir su conocimiento y haberme impulsado para lograr una de mis metas.

Finalmente, a mi casa de estudios la **Universidad Autónoma de la Ciudad de México** por otorgarme un lugar para iniciar y culminar mi licenciatura, así como haberme otorgado diferentes becas con las cuales pude salir adelante en especial el empastado e impresión de tesis.

Resumen

Las redes inalámbricas de área local han tenido una gran popularidad en los últimos años al ofrecer conectividad sin la necesidad de un medio de transmisión físico guiado, haciendo que la mayoría de los usuarios puedan utilizar diferentes dispositivos para conectarse a internet de una manera más fácil; sin embargo, esta conectividad inalámbrica sacrifica la seguridad de la red, comprometiéndola en diferentes ataques maliciosos.

Para cubrir esta falta de seguridad en una WLAN (Wireless Local Área Network) se desarrollaron diferentes protocolos. WEP fue el primer protocolo de seguridad, sin embargo, es el protocolo más vulnerable para este tipo de redes, WEP plantó las bases para elaborar protocolos más robustos, por lo que fue reemplazado en el 2003 por WPA y en 2004 WPA evolucionó en WPA2. A pesar de que WPA2 es el protocolo más robusto hasta ahora, presenta vulnerabilidades de seguridad, es susceptible a ataques pasivos y a ataques de denegación de servicios.

El presente trabajo está enfocado a identificar las vulnerabilidades presentes al acceder a una WLAN de modo infraestructura, de entorno de pequeña oficina o de oficina en casa (SOHO, Small Office / Home Office) y mitigarlas mediante la implementación de *hardening*, es decir, un conjunto de actividades que permiten robustecer la seguridad.

Se presentan los resultados que demuestran que se logró robustecer una WLAN de entorno SOHO con los puntos de *hardening* propuestos; sin embargo, cabe mencionar que una red inalámbrica ya sea de entorno SOHO o empresarial no estará del todo protegida, dado que la tecnología avanza continuamente dando paso a nuevos e ingeniosos ataques.

Contenido

Dedicatoria 2

Agradecimientos 4

Resumen 7

Contenido 8

Introducción 13

Planteamiento del problema 17

Objetivos 17

Justificación 17

Limitaciones 18

Viabilidad 18

Capítulo 1 Marco teórico 21

1. Antecedentes de redes inalámbricas 21

1.1 Estándares de redes inalámbricas 21

1.1.1 Estándar IEEE 802.11 22

1.1.1.1. Modos de operación de una WLAN. 24

1.1.1.2. Control de acceso al medio 25

1.1.1.2.1 Función de coordinación distribuida 26

1.1.1.2.2 Función de coordinación puntual 27

1.1.1.3. Capa física 28

1.1.1.4 Versiones del estándar 802.11 28

1.2 Ventajas y desventajas de las redes inalámbricas de área local (WLAN) 31

1.3 Evolución de protocolos de seguridad en una WLAN 32

1.3.1 Protocolo WEP 34

1.3.1.1 Autenticación WEP 34

1.3.1.2 Encriptación WEP 35

1.3.1.2.1 Proceso de cifrado de las tramas WEP 37

1.3.1.3 Vulnerabilidades de WEP 37

1.3.2 Protocolo WPA/WPA2 39

1.3.2.1 Autenticación en WPA/WPA2 40

1.3.2.2 Cifrado WPA 43

1.3.2.3 Cifrado WPA2 43

1.3.2.4 Vulnerabilidades de WPA /WPA2 44
1.4 Herramientas para la revisión de seguridad en una WLAN 45
1.4.1 Kali Linux 46
1.4.1.1 Herramientas específicas de Kali Linux para atacar a una WLAN 47
1.4.1.2 Suite AIR 47
1.5 Opciones para robustecer la seguridad en la WLAN 48
1.5.1 Hardening 48
1.5.1.1 Actividades de *hardening* 50
1.5.1.2 Tipos de servidores de autenticación 53
1.5.1.3 Servidor RADIUS 54
1.5.1.3.1 Funcionamiento de RADIUS 54
1.5.1.3.2 Ventajas y beneficios de freeRADIUS 56
1.5.1.3.3 Desventajas del servidor RADIUS 56
1.5.1.3.4 Autenticación IEEE 802.1x 57
1.5.1.3.4.1 Protocolo EAP 58
Capítulo 2 Metodología 63
2. Metodología para identificar vulnerabilidades. 63
2.1 Máquina virtual para la identificación de vulnerabilidades 65
2.2 Implementación de *hardening* en una WLAN 66
2.2.1 Implementación del servidor de autenticación como primer punto de *hardening* 67
2.2.1.1 Instalación del sistema operativo Kali Linux en la Raspberry Pi 3 68
2.2.1.2 Instalación del servidor de autenticación (freeRADIUS) 69
2.2.1.3 Configuración del servidor de autenticación freeRADIUS 70
2.2.1.3.1 Configuración de los archivos clientes y usuarios. 72
2.2.1.4 Configuración del AP de acuerdo a freeRADIUS 72
2.3 Configuración del AP de acuerdo a otros pasos de *hardening* 73
2.3.1 Desactivación del WPS 74
2.3.2 Creación de contraseñas robustas 74
2.3.3 Desactivación de la difusión del SSID 75
2.3.4 Desactivación de la configuración remota 75
2.3.5 Activación del filtrado MAC 75
2.3.6 Gestión del AP 76
2.3.7 Minimización de la potencia 76

2.3.8 Actualización del firmware 77
Capítulo 3 Resultados y conclusiones 81
3 Resultados de los ataques a redes inalámbricas para detectar vulnerabilidades e implementar hardening 81
3.1 Resultados de los ataques a una WLAN con seguridad WEP 81
3.1.1 Resultados del ataque a WEP con las herramientas de la Suite AIR 83
3.1.2 Resultados de los ataques a una WLAN con seguridad WPA/WPA2 personal 83
3.2 Resultados de la implementación de *hardening* en una WLAN 89
3.3 Posibles escenarios en un ataque 94
3.3.1 Ataque a la WLAN con la implementación de *hardening* 96
3.3.1.1 Ataque al ocultamiento del SSID 97
3.3.1.2 Ataque a WPA2 *enterprise* 98
3.3.1.3 Intento de clonación MAC 100
3.4 Revisión de seguridad con y sin la implementación de *hardening* 102
Conclusiones 107
Anexo A. Herramientas de la Suite AIR 109
Anexo B. Creación de la máquina virtual con Kali Linux 115
Anexo C. Instalación del servidor de autenticación freeRADIUS 119
Anexo D. Configuración de *hardening* en dos modelos distintos de AP 121
D.1 Configuración del AP Linksys 38378 121
D.2 Configuración del AP ALCATEL I-240W -A de TELMEX 124
Referencias 129

Introducción

Hoy en día las redes inalámbricas han sido adoptadas por gran parte de la sociedad ya que con ellas se puede enviar, recibir o compartir información. Esto se realiza de una manera sencilla y rápida por medio de diferentes dispositivos como lo son smartphones, laptops, tablets, entre otros, los cuales vienen equipados con una tarjeta de red inalámbrica (WNIC - Wireless Network Interface Card) para conectarse a una red inalámbrica de área local (WLAN - Wireless Local Area Network) o zona WIFI. Por otro lado, las redes inalámbricas están jugando un papel importante en la tecnología de internet de las cosas (IoT-Internet of Things), ya que distintos objetos físicos se conectan diariamente a este tipo de redes, por ello, se prevé que para el año 2020 la mayoría de los dispositivos se conectarán a las redes inalámbricas [1].

En un futuro esto conllevará a una problemática mayor, dado que las WLAN son muy vulnerables. Por ejemplo, en el 2015 Fortinet realizó un estudio en el que se les llamó a las redes inalámbricas el punto más vulnerable de las tecnologías de la información (TI), donde el 49 % de los encargados de TI de todo el mundo aseguraron y clasificaron a este tipo de redes como el elemento más vulnerable de esta infraestructura [2].

En el mes de mayo de 2017, Fortinet realizó una nueva investigación donde más de 1,300 gerentes de ciberseguridad de 11 países respondieron la encuesta sobre los riesgos de la seguridad de las redes inalámbricas, así como el alto nivel de exposición que representan las WLAN, en el cual un 45 % de los encuestados declaró que la filtración de información sensible, tanto de clientes como de la empresa, es la preocupación número uno [3].

El saber que estos problemas están presentes en un entorno empresarial nos lleva a pensar que en un entorno de pequeña oficina o de oficina en casa (SOHO, Small Office / Home Office) las medidas de seguridad son mínimas, ya sea por falta de información o por el simple hecho de mantener una configuración sencilla en la WLAN lo que involucra un mayor riesgo.

Este riesgo podría llegar a reducirse con la implementación de los diferentes protocolos de seguridad, sin embargo, estos siguen presentando vulnerabilidades a tal grado que en octubre de 2017 el protocolo WPA2 fue quebrantado totalmente por el investigador Mathy Vanhoef [4,5], protocolo en el cual se había confiado la seguridad de las WLAN por 14 años, sin importar el entorno en que se encuentren (SOHO o empresarial).

Por otro lado, en un entorno empresarial el tema de seguridad inalámbrica cada vez está más presente, preocupándose por proteger la información de su *core business* que se transmite en la WLAN, diferenciándose con un entorno SOHO, ya que los usuarios que utilizan estas redes como un servicio para enviar y recibir información, tienen una preocupación nula de las medidas de seguridad de la WLAN.

Por dicho motivo en la presente tesis se propone proteger a los dispositivos que se están conectando a las WLAN de entorno SOHO. Una prioridad que se busca en el tema de seguridad inalámbrica es aumentar la seguridad de acceso a las WLAN, por ello es importante revisar los mecanismos de autenticación que involucran específicamente las WLAN de entorno SOHO, con el fin de robustecer su seguridad a partir de una identificación de vulnerabilidades.

En este sentido, en junio de 2017 se realizó un sondeo en la colonia Doctores de la Ciudad de México, para saber qué tipo de seguridad comúnmente se implementa en una WLAN de entorno SOHO y a partir de ello determinar qué actividades *hardening* son convenientes de implementar.

Dicho sondeo, indicó que se detectaron aproximadamente trescientas redes inalámbricas. En la figura I se muestra un gráfico que se realizó a partir de los datos obtenidos del sondeo, así mismo puede apreciarse que la autenticación *enterprise* es prácticamente nula, ya que la autenticación que predomina es la autenticación de clave compartida.

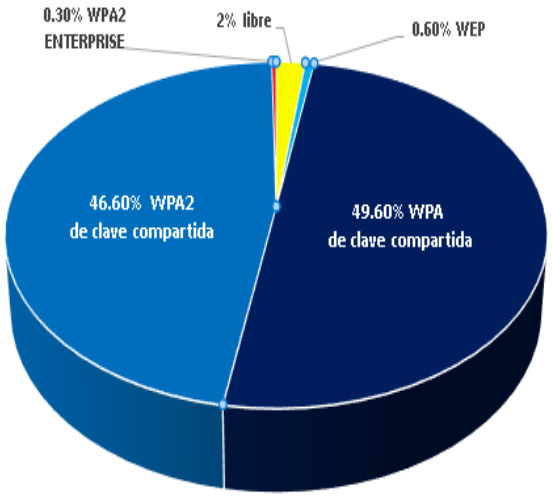


Figura I. Estadística de uso de los protocolos de seguridad en una WLAN en la colonia Doctores de la ciudad de México (diagrama propio)

Así mismo pudo notarse que el estándar WPS (WI-FI Protected Setup) se encuentra activo en la mayoría de las WLAN siendo este un blanco fácil para los atacantes, debido a que es vulnerable a ataques de fuerza bruta[1]. Para ejemplificar esto se tomó una pequeña muestra de todas las redes detectadas en el sondeo. En la figura II puede apreciarse que la mayoría de los usuarios tienen esta configuración.

Figura II. Algunas redes con WPS activo de acuerdo al sondeo en la colonia Doctores (diagrama propio).

Por otro lado, también se observó que en la mayoría de las WLAN existe la emisión del SSID (Service Set Identifier). En la figura III se ejemplifica dicha emisión y puede notarse que regularmente el nombre de la red no es cambiado, es decir, conserva el nombre asignado por default[2] del proveedor de servicios de Internet (ISP).

Figura III. Difusión de SSID de algunas redes detectadas por un dispositivo móvil en la colonia Doctores (diagrama propio).

[1] Se le llama ataque de fuerza bruta a la actividad de hacer coincidir el password con todas las combinaciones posibles de cadenas de texto, hasta encontrar el password que permita el acceso a la red.

[2] La palabra default hace referencia a hacer algo por defecto o dejar de forma predeterminada.

Debido a la importancia que tiene la seguridad de las WLAN, la presente tesis está enfocada a identificar las vulnerabilidades que existen en los protocolos de seguridad que se usan para acceder a dichas redes, específicamente en el momento de realizarse la autenticación. Una vez identificadas estas vulnerabilidades se pretende robustecer la seguridad de una WLAN con la implementación de *hardening,* que consiste en un conjunto de actividades en el que se incorporan diferentes capas de seguridad mismas que serán descritas en el capítulo I de dicha tesis.

Planteamiento del problema

De acuerdo con la literatura, las redes inalámbricas son el punto más vulnerable en las Tecnologías de la Información (TI), por ello un atacante fácilmente podría obtener de manera ilícita las contraseñas WI-FI por lo que la información de los usuarios podría estar expuesta a diversos ataques como: robo de datos, robo de identidad, espionaje, colocación de malware entre otros.

Por ello, se pretende identificar las vulnerabilidades en una WLAN para subsanarlas con *hardening*.

Objetivos

- Objetivo general
    - ❖ Robustecer la seguridad de una WLAN en un entorno SOHO mediante la técnica de *hardening* para subsanar las vulnerabilidades más comunes.
- Objetivos específicos
    - ❖ Identificar las vulnerabilidades más comunes en redes inalámbricas en zonas WIFI.
    - ❖ Implementar un escenario de prueba para la identificación de vulnerabilidades en una WLAN determinada.
    - ❖ Implementar *hardening* con el fin de hacer más robusta la seguridad en las WLAN.

Justificación

Las redes inalámbricas son una tecnología importante para la comunicación, sin embargo, son vulnerables a diferentes ataques informáticos comprometiendo la disponibilidad, la integridad y la confidencialidad de estas redes, por tal motivo es importante robustecer el acceso a la WLAN. Para ello, es necesario identificar las vulnerabilidades de una WLAN para hacer las recomendaciones apropiadas.

Limitaciones

La identificación de vulnerabilidades se llevará a cabo en un escenario de pruebas, en un entorno controlado de manera responsable, con los permisos previamente solicitados a las personas correspondientes, ya que entrar a una red inalámbrica privada es un delito de acuerdo al artículo 286 de la ley orgánica de España de ciberdelitos.

Viabilidad

El trabajo es viable ya que para su implementación se requiere de:

a) Un equipo de cómputo para la identificación de vulnerabilidades en una WLAN, dicha actividad puede realizarse mediante la distribución Kali Linux, un sistema operativo de licencia libre que no implica costos. Este sistema operativo, puede instalarse en una máquina virtual en un equipo de cómputo con el que ya se cuente.
b) Una tarjeta de desarrollo Raspberry PI para la implementación de un servidor de autenticación de licencia libre cuyo costo no excede los $ 1500 MN.
c) Un módem que tenga la capacidad de soportar una autenticación *enterprise* para la implementación de las actividades de hardening, elemento con el que ya se cuenta.

CAPÍTULO I

"Si crees que la tecnología puede solventar tus problemas de seguridad, entonces no entiendes los problemas y no entiendes de tecnología."

Bruce Schneier

Capítulo 1 Marco teórico

1. Antecedentes de redes inalámbricas

Una red inalámbrica es aquella que permite el acceso a diferentes recursos como por ejemplo datos de manera inalámbrica. Para ello, se realiza una conexión entre dos o más nodos que pueden ser dispositivos móviles, para intercambiar información mediante la propagación de ondas de radio en un área determinada [6,7].

Las redes inalámbricas surgieron como un complemento a las redes cableadas siendo éstas una nueva alternativa en la transferencia de información que no depende de un medio físico guiado como lo es el cable, lo que permitió dar mayor movilidad al usuario sin perder conectividad [8].

El origen de las redes inalámbricas se remonta al año de 1979, con una publicación sobre los resultados de un experimento hecho por ingenieros de IBM en Suiza, en la que se reporta el uso de ondas del espectro infrarrojo para crear una red, lo que se consideró como el punto de partida en la evolución de las redes inalámbricas. Posteriormente para el funcionamiento adecuado de esta tecnología fue necesaria la creación de diversos estándares, siendo éstos los que se describen en la siguiente sección.

1.1 Estándares de redes inalámbricas

Los estándares son desarrollados por organismos reconocidos internacionalmente. Estos son acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos, para ser usados consistentemente como reglas, guías o definiciones de características para asegurar que los materiales, productos, procesos y servicios cumplan con su propósito. Uno de estos organismos es el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE - Institute of Electrical and Electronics Engineers) encargado de establecer diferentes estándares para las redes inalámbricas. En 1991 se propuso el estándar 802.11 por parte de la IEEE, sin embargo, este estándar se estableció hasta junio de 1997 [9,10].

En figura 1.1 puede apreciarse que las redes inalámbricas son clasificadas de acuerdo con su cobertura, así mismo son regidas por diferentes estándares para su buen funcionamiento.

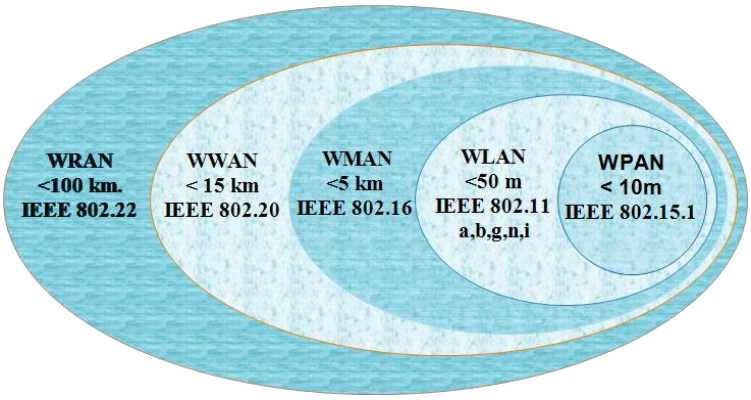


Figura 1.1 Clasificación de redes inalámbricas de acuerdo al radio de cobertura (diagrama propio).

Debido a que este trabajo está enfocado solamente al estudio de las WLAN, cuyo principal estándar es el IEEE 802.11, a continuación, se describe este estándar y sus diferentes versiones: a, b, g, n, i, ad, ac se abordaran en la sección 1.1.1.4 [11].

1.1.1 Estándar IEEE 802.11

El estándar IEEE 802.11 define nueve servicios que deben ser proporcionados por una red inalámbrica con la finalidad de ofrecer una funcionalidad equivalente a una LAN, estos servicios son los siguientes: asociación, autenticación, fin de la autenticación, disociación, distribución, integración, entrega de MSDU (Unidad de datos del servicio MAC), privacidad y reasociación [12].

Por otra parte, en la tabla 1 se describe la terminología que se emplea en el estándar IEEE 802.11

En la figura 1.2 se aprecia la topología del modelo elemental para una WLAN propuesto por el estándar 802.11 así como la forma en que interactúan entre sí cada uno de los componentes en un conjunto extendido de servicios, cabe mencionar que a lo largo del trabajo se definirán más conceptos.

AP (Access Point-Punto de acceso)	Cualquier entidad que tenga la funcionalidad de una estación. Proporciona acceso al sistema de distribución a través del medio inalámbrico a las estaciones asociadas
BSS (Basic Service Set-Conjunto de Servicios Básicos)	Conjunto de estaciones controladas por una sola función de coordinación
Función de coordinación	Es aquella función lógica que determina cuándo una estación que está funcionando dentro de un BSS tiene permiso para transmitir y puede recibir un PDU (Protocol Data Unit)
DS (Distribution System-Sistema de Distribución)	Es el sistema usado para interconectar un conjunto de BSS y LAN integradas para crear un ESS
ESS (Extended Service Set-Conjunto de Servicios Extendido)	Conjunto de uno o más BSS interconectados y LAN integradas que aparece como un único BSS en la capa LLC (Logica Link Control) de cualquier estación asociada con uno BSS
MPDU (MAC Protocol Data Unit-Unidad de Datos del Protocolo MAC)	Unidad de datos intercambiada entre entidades MAC paritarias usando los servicios de la capa física
MSDU (MAC Service Data Unit-Unidad de Datos del Servicio MAC)	Es aquella información la cual es entregada como una unidad entre usuarios MAC
Estación	Cualquier dispositivo que contenga una capa física y MAC compatibles con IEEE 802.11

Tabla 1. Términos IEEE 802.11con base en [12].

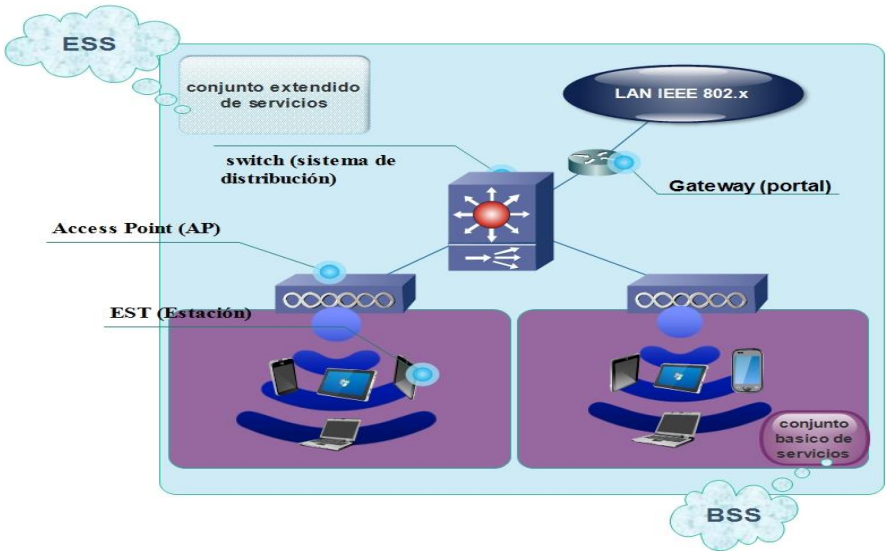


Figura 1.2. Topología IEEE 802.11 (diagrama propio con base en [13]).

1.1.1.1. Modos de operación de una WLAN.

Las redes inalámbricas cuentan con dos modos de operación fundamentales los cuales están definidos por el conjunto de estándares IEEE 802.11, estos son: trabajo en modo infraestructura y en modo ad hoc.

La forma de operación en modo infraestructura en una red inalámbrica sucede cuando todas las estaciones acceden a la red a través de uno o varios puntos de acceso, la definición de un punto de acceso se encuentra en la tabla 1. La configuración formada por el punto de acceso y las estaciones ubicadas dentro del área de cobertura es a lo que se le denomina BSS; es posible vincular varios puntos de acceso con el fin de formar un ESS, como se ilustra en la figura 1.3.

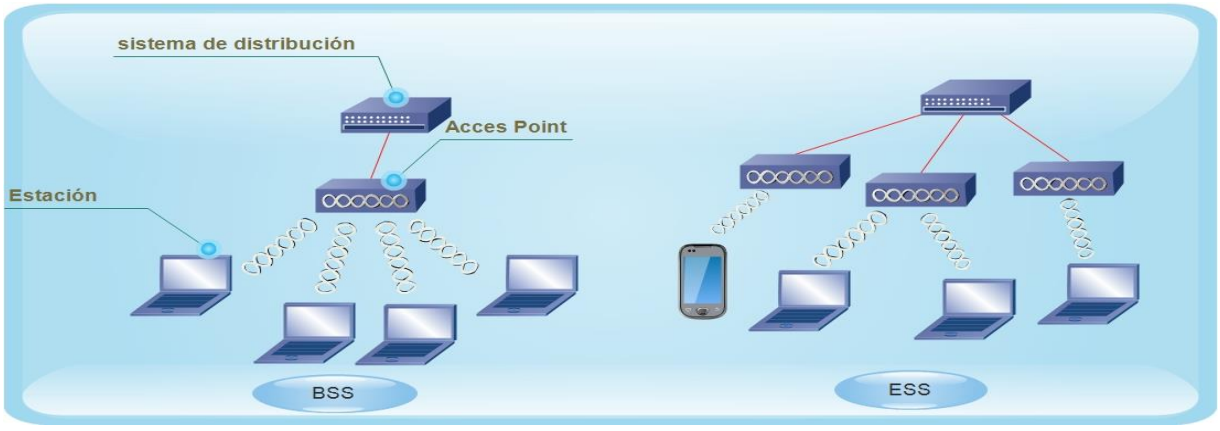


Figura 1.3. Operación en modo infraestructura (diagrama propio).

El modo de operación *ad hoc* o mejor conocido como punto a punto es el método en el que las estaciones se comunican entre sí directamente sin involucrar un servidor central (punto de acceso central). Estas redes son establecidas de manera temporal y normalmente son conformadas por un grupo pequeño de dispositivos cercanos unos de otros.

El modo ad-hoc se denota como un conjunto de servicios básicos independientes (IBSS Independent Basic Service Set). Este modo de operación se muestra en la figura 1.4.

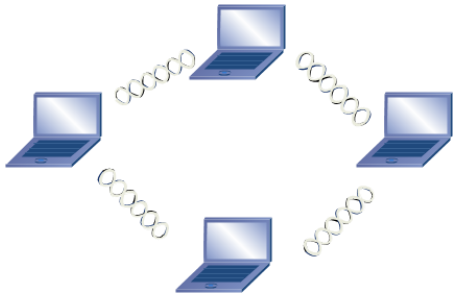


Figura 1.4. Operación en modo Ad-hoc (diagrama propio).

Cabe mencionar que en la presente tesis la identificación de vulnerabilidades exclusivamente considera a las redes inalámbricas de área local que cuentan con el modo de operación en modo infraestructura, todo esto señalado por el estándar 802.11.

Por otra parte, el estándar IEEE 802.11 define el uso de los primeros dos niveles de la arquitectura TCP/IP, capa física y capa de enlace de datos. La capa física especifica las normas de funcionamiento de una WLAN e incluye seis técnicas de transmisión por modulación, dos velocidades de transmisión teóricas de 1 y 2 Mbps y la banda de frecuencias en que opera.

La capa MAC garantiza el éxito de la transferencia, define el protocolo de acceso múltiple por detección de portadora y la prevención de colisiones (CSMA/CA - Carrier Sense Multiple Access/Collition Avoidance) como método de acceso al medio [13,14].

1.1.1.2. Control de acceso al medio

IEEE 802.11 considera a los protocolos de acceso distribuido y de acceso centralizado como algoritmos de MAC. En el protocolo de acceso distribuido la transmisión se distribuye sobre todos los nodos usando un mecanismo de detección de portadora y en el caso de los protocolos

de acceso centralizado, implican una regulación de transmisión por una autoridad central de decisiones.

El algoritmo MAC denominado DFWMAC (Distributed Foundation Wireless MAC) proporciona un mecanismo de control de acceso distribuido sobre un control centralizado opcional. Así mismo la arquitectura MAC de este estándar tiene una subcapa de función de coordinación distribuida (DCF, Distributed Coordination Function) y la subcapa de función de coordinación puntual (PCF, Point Coordination Function). En los siguientes párrafos se aborda de manera general, tanto la función de coordinación distribuida como la función de coordinación puntual.

1.1.1.2.1 Función de coordinación distribuida

La subcapa DCF usa el algoritmo de acceso múltiple con detección de portadora (CSMA, Carrier Sense Multiple Access). Una estación escucha el medio cuando dispone de una trama para transmitir y si el medio está libre entonces la estación podrá transmitir, en caso contrario la estación debe esperar antes de transmitir, hasta que se complete la transmisión en curso para que exista un funcionamiento adecuado de este algoritmo. En la figura 1.5 se ejemplifica dicho proceso.

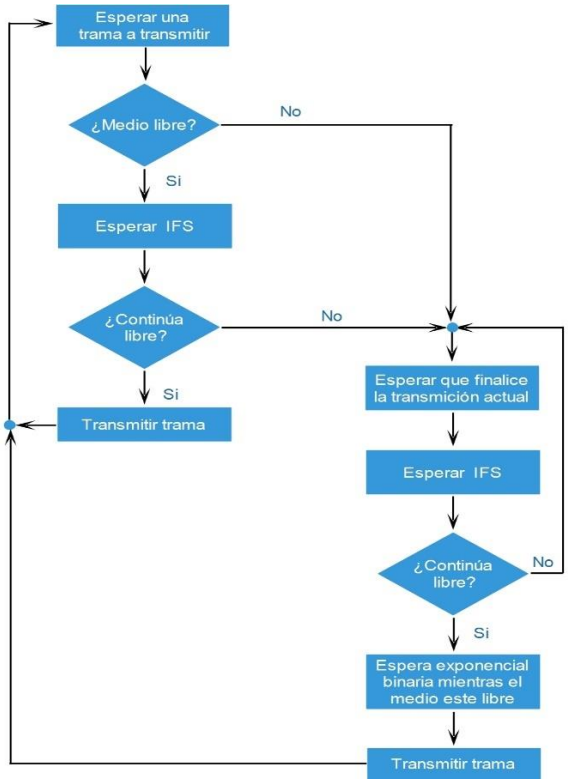


Figura 1.5. Lógica de control de acceso al medio IEEE 802.11 de la función de coordinación puntual, con base en [12].

La DCF incluye un conjunto de retardos que son ordenados de acuerdo a un esquema de prioridades, basado en el uso de tres valores IFS (Interframe Space).

1.- SIFS (Short IFS): es el IFS más pequeño y se utiliza para todas las acciones de respuesta inmediatas.

2.- PIFS (Point Coordination Function IFS): se trata de un IFS de tamaño medio, utilizado por el contador central en el esquema PCF cuando se emite un sondeo.

3.- DIFS (Distributed Coordination Function IFS): constituye el IFS más grande y se usa como un retardo mínimo para las tramas asíncronas que compiten por el acceso al medio. En la figura 1.6 se ilustran los IFS.

El periodo de contención es tiempo de espera aleatorio que una estación debe esperar antes de transmitir si el canal se encuentra ocupado.

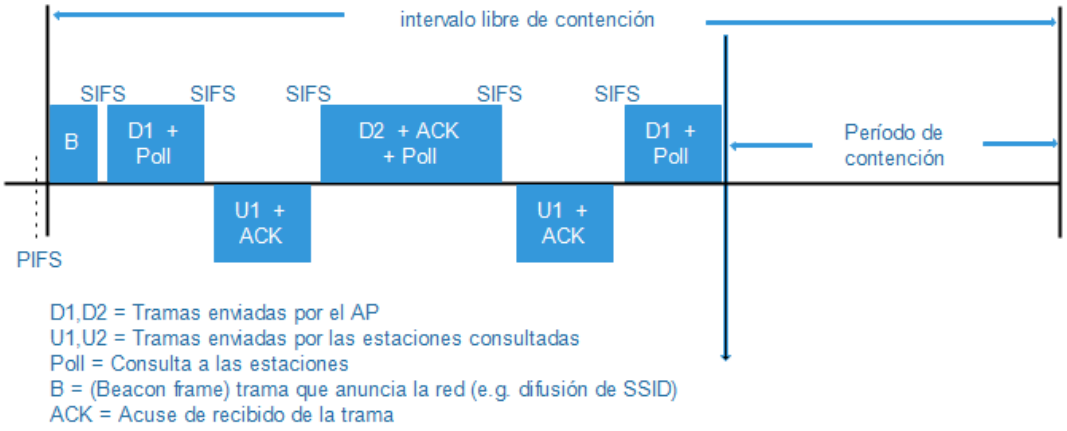


Figura 1.6. Conjunto de retardos IFS con base en [12].

1.1.1.2.2 Función de coordinación puntual

PCF es un método de acceso implementado sobre DCF, el cual consiste en consultar a las estaciones del BSS si tienen tramas para transmitir. La consulta es realizada por un coordinador puntual, el coordinador puntual hace uso de un PIFS cuando emite una consulta, como un PIFS es más pequeño que un DIFS, el coordinador puntual puede adueñarse del medio y bloquear el tráfico asíncrono.

Por ejemplo, si una red inalámbrica cuenta con una serie de estaciones con tráfico sensible a los retardos, el intercambio de tramas se controla por medio del coordinador puntual, por otra parte, el resto del tráfico compite por el acceso al medio usando CSMA. El coordinador puntual podría emitir consultas a todas las estaciones configuradas para realizar el sondeo mediante un esquema de turno rotatorio, donde primero se emite un sondeo y la estación consultada debe responder con un SIFS, si el coordinador puntual recibe una respuesta se emite un nuevo sondeo usando un PIFS, si durante el tiempo correspondiente en turno no se recibe ninguna respuesta, entonces el coordinador emite una nueva consulta.

1.1.1.3. Capa física

La capa física del estándar 802.11 ha sufrido diferentes extensiones, modificaciones y mejoras, cabe mencionar que esta capa se definió con tres técnicas de transmisión:

- Espectro expandido de secuencia directa (DS-SS)
- Espectro expandido con salto en frecuencias (FH-SS)
- Infrarrojos

Estas técnicas de transmisión trabajan a velocidades de 1 y 2 Mbps, los primeros funcionan en la banda ISM (Industry Scientific and Medical) de los 2.4 GHz a diferencia de los infrarrojos ya que estos funcionan con longitudes de onda de 850 nm y 950 nm [12].

1.1.1.4 Versiones del estándar 802.11

A partir del estándar IEEE 802.11 se desarrollaron diferentes versiones para la operación de una WLAN. En la figura 1.7 se muestra el estándar IEEE 802.11, así como sus diferentes versiones, el estándar 802.11i es el de mayor interés para la realización de la tesis ya que es el único estándar que fue desarrollado para la seguridad en este caso de una WLAN. En los siguientes párrafos se describen brevemente cada una de estas versiones.

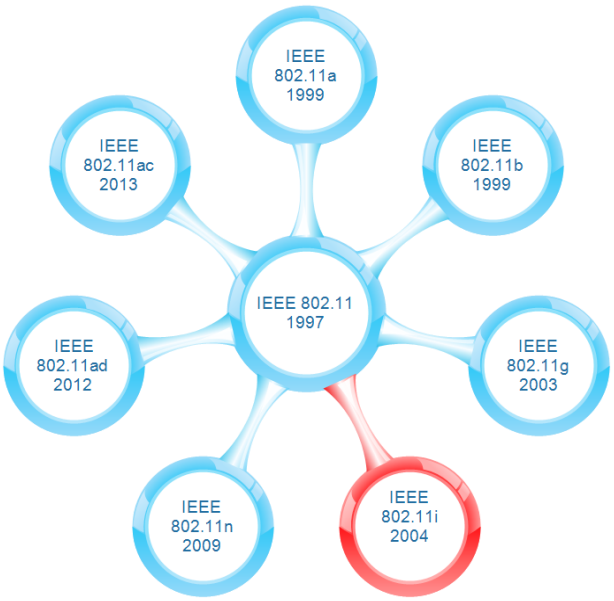


Figura 1.7. Estándar 802.11 y sus versiones imagen propia en base (diagrama propio).

La versión *a* de este estándar fue aprobada en 1999, definió una nueva capa física que opera hasta los 54 Mbps, trabaja en la banda de frecuencia de 5 GHz, lo que le da una ventaja ya que se presentan menos interferencias en dicha banda [11].

La versión *b* de este estándar fue aprobada en el mismo año en el que se aprobó la versión *a*, tiene una velocidad máxima de transmisión de 11 Mbps, utiliza CSMA/CA, y trabaja en la banda de frecuencia de 2.4 GHz. En la práctica la velocidad máxima de transmisión es de aproximadamente 5.9 Mbps sobre TCP y 7.1 Mbps sobre UDP [14].

En 2003 apareció la versión *g* como una mejora de las versiones ya existentes ya que la función de este estándar es incrementar la tasa de transmisión (54 Mbps) casi 5 veces más con respecto a la versión *b*. Cabe mencionar que estos 54 Mbps son una velocidad teórica puesto que el estándar 802.11 utiliza el modo de transmisión half-duplex, lo que significa que transmite y recibe en ambas direcciones, por lo que estos 54 Mbps se reparten entre la recepción y transmisión de datos. Entonces los 54 Mbps se refieren a la velocidad del canal, puesto que en la práctica su rendimiento tan sólo es de 27 Mbps ya que influyen otros factores como lo son la distancia y los obstáculos, los cuales provocan atenuaciones que afectan la velocidad de transmisión.

La versión *g* trabaja en la banda de frecuencia de 2.4 GHz, esta versión a diferencia de la versión *a*, es compatible con la versión *b* del estándar 802.11 [15].

La versión *n* hace uso de las bandas de 2.4 y 5 GHz [13], fue aprobado en el año 2009, permite comunicaciones de datos inalámbricas de hasta 600 Mbps, utiliza tecnología MIMO (Multiple Input-Multiple Output) lo que permite utilizar varios canales a la vez para enviar y recibir datos.

La versión *i* mejor conocida como WPA2 (WI-FI Protected Access 2), se estableció en junio de 2004, está enfocada a la seguridad en redes WLAN. Esta versión mejoró considerablemente con respecto a las primeras normas de seguridad de las redes inalámbricas, ya que proporciona cifrado mejorado para redes que utilizan los estándares 802.11*a* y 802.11*b*. Este estándar introduce varios cambios fundamentales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, lo que proporciona una arquitectura robusta y escalable.

Esta versión llega a los 600 Mbps, fue definida específicamente para mejorar la seguridad y corregir de esta manera al protocolo WEP (Wired Equivalent Privacy) con el protocolo WPA (Wi-Fi Protected Access), lo que mejora a su vez la integridad de la información. Por otro lado, actualiza la CRC (Comprobación de Redundancia Cíclica – Cyclic Redundancy Checksum) del mensaje. WPA implementa un código de integridad MIC (Message Integrity Code), posteriormente se implementa WPA2 el cual requiere un nuevo protocolo de clave de cifrado, conocido como TKIP (Temporal Key Integrity Protocol) y utiliza algoritmos de cifrado AES (Advanced Encryptation Standard) lo que ofrece un nivel de seguridad suficiente para satisfacer a la mayoría de los usuarios, más adelante se hablará a detalle de los protocolos mencionados anteriormente.

La versión *ad* fue propuesta en 2013, ofrece comunicaciones inalámbricas en la banda de 2.4 GHz, 5 GHz y 60 GHz para lograr velocidades de alrededor de 7 Gbps es compatible con las versiones b/g/n/ac, sin embargo, no ha sido aprobado.

IEEE 802.11ac (también conocido como Wi-Fi 5G o Wi-Fi Giga bit) aparece como una mejora al estándar IEEE 802.11n, se empezó a desarrollar entre el año 2011 y el 2013, y finalmente fue aprobado en enero de 2014. Este estándar tiene una velocidad máxima de 1.3 Gbps y opera en la banda de frecuencia de 2.4 GHz y 5.5 GHz, además de ser compatible con IEEE 802.11b/g/n.

En la tabla 1.1 se enlistan los principales estándares y sus respectivos mecanismos de seguridad, los cuales se profundizarán más adelante.

Estándar 802.11	Año de Aprobación	Frecuencia	Características de seguridad
802.11	Jun. 1997	2.4 GHz	WEP (RC4)
a	Sep.1999	5 GHz	WEP (RC4)
b	Sep. 1999	2.4 GHz	WEP (RC4)
g	Jun. 2003	2.4 GHz	WEP (RC4)
i	Jun. 2004		WPA, WPA2 (RC4 y AES)
n	Oct. 2009	2.4/5 GHz	WPA, WPA2 (RC4 y AES)
ac	Enero 2014	2.4/5.5 GHz	WPA, WPA2 (RC4 y AES)
ad	Sin aprobar	2.4/5/60GHz	

Tabla 1.1. Comparativa de seguridad de los estándares IEEE 802.11.

Donde RC4 (Ron's Code 4) es el algoritmo de encriptación tanto para el protocolo WEP como para el protocolo WPA, AES (Advanced Encryptation Standard) es el algoritmo de encriptación para el protocolo WPA2.

1.2 Ventajas y desventajas de las redes inalámbricas de área local (WLAN)

Una WLAN también pude presentar ventajas y desventajas, a continuación, se mencionan algunas ventajas y desventajas de dichas redes [7,16]:

VENTAJAS

- Facilidad de instalación**:** aunque involucra la configuración de protocolos su instalación es sencilla ya que sólo se requiere de un dispositivo con una tarjeta inalámbrica.
- Proporciona mayor movilidad: elimina el tendido de cables en paredes y/o techos lo que le da una mayor movilidad al no depender de este medio físico.
- Flexibilidad**:** una red inalámbrica le permite a la red ir a donde la red convencional no puede ir, ya que le permiten al usuario estar conectado mientras se desplaza con algún dispositivo portátil.
- Velocidad simétrica: ya que WI-FI es bidireccional puede recibir y enviar datos a la misma velocidad.

DESVENTAJAS

- Alcance limitado: el alcance de las redes inalámbricas WLAN es limitado ya que las áreas que puede cubrir WI-FI en edificios es de 75 a 120 metros y en áreas abiertas el alcance puede llegar hasta 300 metros.
- Velocidad**:** las redes inalámbricas no pueden superar la velocidad de las redes alambradas.
- Interferencia**:** debido al rango de frecuencia en el que estas redes inalámbricas trabajan (2.4/5 GHz) son propensas a interferencias de señales muy comunes como por ejemplo los teléfonos inalámbricos.
- Seguridad**:** sin duda alguna esta es una de sus desventajas más importantes, la conexión a las WLAN hoy en día es muy popular ya que se puede acceder a éstas en cualquier parte como por ejemplo restaurantes hoteles o en zonas WI-FI por lo que es probable que un usuario se conecte a una red no segura, exponiéndose de esta forma a ataques como lo son: robo de archivos personales, contraseñas de acceso a bancos, redes sociales y demás.

Este trabajo está enfocado a identificar las vulnerabilidades que pueden existir en las WLAN, por lo que a continuación se revisan los protocolos de seguridad que están presentes en una WLAN.

1.3 Evolución de protocolos de seguridad en una WLAN

La evolución de los protocolos de seguridad en una WLAN obedece a incrementar cada vez más la seguridad en este tipo de redes. En todo sistema de red (LAN o WLAN) existe un modelo de seguridad de la información mejor conocido como la triada CIA la cual está compuesta por las tres propiedades de la información estas son: la integridad, la confidencialidad y la disponibilidad. La integridad se refiere a la capacidad para determinar si la información transmitida ha sido alterada por usuarios no autorizados; la confidencialidad asegura que la información no es divulgada a personas no autorizadas, procesos o dispositivos; mientras que la disponibilidad asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan. En este contexto las WLAN son un blanco fácil y vulnerable a ataques mal intencionados, estos ataques explotan las debilidades o vulnerabilidades presentes regularmente

en el software del AP, al modificarlo silenciosamente y sin autorización, por lo que se compromete la integridad de un recurso.
Por otro lado, la confidencialidad se compromete cuando un intruso accede de manera ilícita a información no pública [17], también puede verse afectada la disponibilidad cuando un atacante provoca la caída de un AP.
Se ha hablado de vulnerabilidad, pero ¿qué es la vulnerabilidad? a continuación, se da una breve definición de ésta:
La vulnerabilidad se refiere a una debilidad la cual se podría desencadenar de manera accidental o explotarse intencionalmente lo que podría causar una brecha de seguridad [18].

De acuerdo con la definición, la confidencialidad, integridad y disponibilidad son los tres aspectos más importantes de la seguridad ya que si se carece de alguno de estos tres existe una vulnerabilidad de seguridad.

La seguridad inalámbrica es considerada más complicada de implementar que la seguridad que se implementa en las redes alambradas debido al medio de transmisión. El estándar IEEE 802.11 definió dos mecanismos básicos de seguridad con el fin de asegurar el acceso a la red, estos son: autenticación de identidad y encriptación.
La autenticación es el proceso en el que se hace una comparación de las credenciales proporcionadas por el usuario con las credenciales que ya existen dentro de una base de datos.
El cifrado o encriptación es el proceso de ocultar los datos a todas aquellas personas no autorizadas que lleguen a interceptarlos para que no sean capaces de entenderlos. La encriptación también asegura al mismo tiempo que los datos sean devueltos a su forma original, por lo tanto, es un proceso bidireccional. Por otra parte, el hecho de tomar datos cifrados y devolverlos a datos legibles es a lo que se le conoce como descifrado.

El primer protocolo de seguridad para el estándar IEEE 802.11 fue WEP (Wired Equivalent Privacy), el cual implementa tanto la autenticación de identidad y encriptación. En el caso de la autenticación, este protocolo permite dos formas: autenticación de sistema abierto y autenticación de clave compartida, no obstante, éste resultó ser muy vulnerable por lo que en el estándar IEEE 802.11i se introducen cambios fundamentales, además de proporcionar una arquitectura robusta [19]. A continuación, el protocolo WEP se explica a detalle.

1.3.1 Protocolo WEP

WEP se aprobó en 1999 y fue el primer protocolo de encriptación del estándar IEEE 802.11. WEP se creó con el fin de satisfacer el control de acceso, privacidad, autenticación e integridad. WEP se fundamenta en el algoritmo de encriptación RC4 (Ron's Code 4) con una clave secreta de 40 o 104 bits, así mismo soporta dos mecanismos de autenticación los cuales son muy básicos, entre ellos se encuentran: autenticación de clave compartida, (mejor conocido como shared-key) y autenticación abierta.

1.3.1.1 Autenticación WEP

En la autenticación de clave compartida, la clave WEP es utilizada para verificar si el usuario puede o no tener acceso a la red inalámbrica, tanto el AP como el cliente realizan el proceso de saludo de cuatro vías (handshake de cuatro vías). El proceso es el siguiente:

1. L estación envía una solicitud de autenticación al AP por el cliente.
2. El AP envía al cliente un número pseudo aleatorio, este número es denominado típicamente como el valor "*nonce*".
3. El cliente encripta el valor *nonce* utilizando la clave WEP y lo envía de nuevo al AP.
4. El AP encripta el mismo valor con la clave WEP comparándolo con lo que el cliente envió. En caso de que los valores coincidan, el cliente tiene la clave WEP correcta por lo tanto el AP reconoce el intento de autenticación.

En la figura 1.8 se representa esquemáticamente este proceso.

Figura 1.8. Autenticación de clave compartida WEP (diagrama propio).

En la autenticación abierta, el cliente envía una solicitud de autenticación al AP y éste devuelve el mensaje de que la estación está autenticada, lo que significa que el AP permite la conexión inalámbrica sin ningún proceso de autenticación previo.

Cabe mencionar que la autenticación de clave compartida no es nada segura dado que, un atacante puede obtener tanto el valor del *nonce*, como la respuesta encriptada al capturar los paquetes emitidos por la red, por lo que la obtención de la clave es muy sencilla.

1.3.1.2 Encriptación WEP

Existen dos sistemas principales para la encriptación de datos siendo estos:

- ***Encriptación de clave compartida:*** utiliza la misma clave para cifrar y para descifrar los datos, esto quiere decir que la misma clave de cifrado que se introduce en el AP es la misma que se utiliza para los clientes de la red.
- ***Encriptación de llave pública:*** las claves de cifrado y descifrado de los datos son diferentes.

El cifrado de WEP se lleva a cabo mediante el algoritmo RC4 el cual es utilizado para generar el *keystream* o secuencia de clave, este algoritmo es simétrico lo que significa que con la misma clave que cifra se puede descifrar, la creación del *keystream* dispone de dos fases llamadas KSA (Key Scheduling Algorithm) y PRGA (Pseudo Random Generation Algorithm). En la figura 1.9 se aprecian estos algoritmos, donde KSA genera un vector inicial de 256 elementos y un vector T con las mismas características del vector S, con estos dos vectores se genera un vector S final, en el cual se auxilia PRGA para generar el *Keystream*.

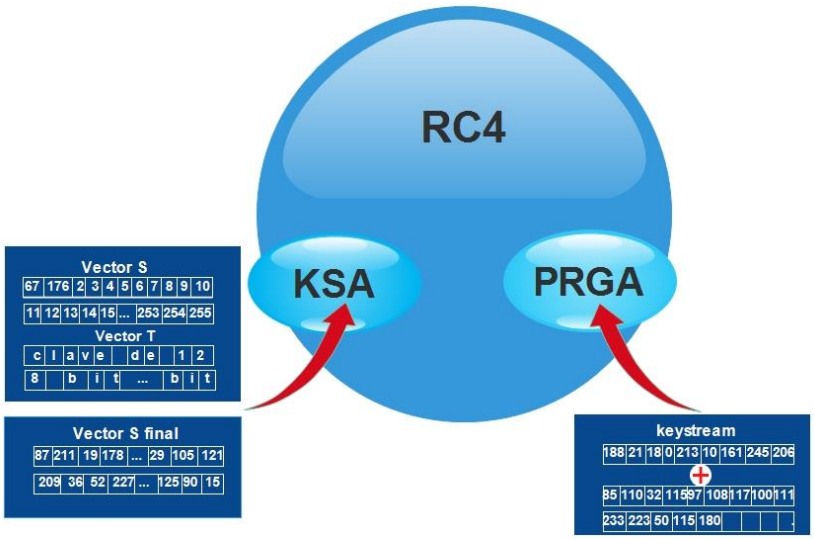


Figura 1.9. Algoritmo RC4 (diagrama propio).

Los métodos básicos para cifrar datos son: cifrado de flujo y cifrado de bloque, donde en el primer método los datos se cifran un byte a la vez y el texto cifrado de salida es de la misma longitud que el texto plano de entrada. En el cifrado de bloque el algoritmo de cifrado funciona en bloques de datos de longitud fija. Por ejemplo: si un algoritmo de cifrado trabaja en bloques de datos de longitud de 32 bytes, un mensaje de texto plano de 128 bytes se dividirá en cuatro bloques únicos de texto cifrado. Cabe mencionar que RC4 es un esquema de cifrado de flujo. En la figura 1.10 se ejemplifican estos dos métodos de cifrado.

Figura 1.10. Cifrado de flujo y cifrado por bloques (diagrama propio).

1.3.1.2.1 Proceso de cifrado de las tramas WEP

Las tramas a cifrar se componen básicamente de una cabecera (header) y un contenido (payload). Primero se debe calcular el CRC del payload con lo que se obtiene el valor de comprobación de integridad (ICV: Integrity Check Value) el cual se añade al final de la trama, posteriormente se selecciona una llave de 40 bits de cuatro posibles, que se genera de manera automática o introducida manualmente, a partir de una clave, dicha clave debe ser conocida por todos los usuarios por lo que se emplean claves muy sencillas y poco cambiantes. A partir de esta clave se generan 4 llaves de 40 bits.

Después de la llave seleccionada se suma el Vector de Inicialización (IV) al comienzo de la llave, el IV se envía en el paquete sin cifrar. Este vector es tan sólo un contador el cual cambia su valor de acuerdo con la generación de tramas de tal forma que, al ser añadió el IV a la llave de 40 bits, se aumenta el número de llaves posibles a emplear [20, 21, 22]. El proceso completo se puede apreciar en la figura 1.11.

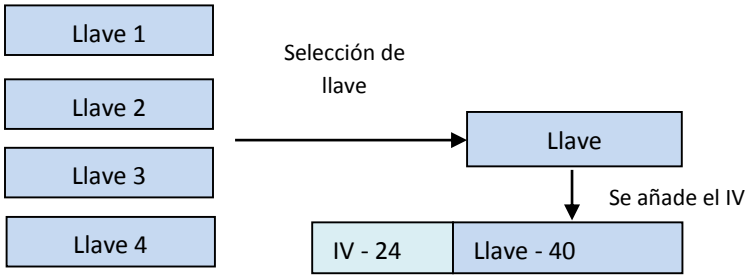


Figura 1.11. Vector de inicialización (diagrama propio)

1.3.1.3 Vulnerabilidades de WEP

WEP no fue creado por expertos en seguridad por lo que se demostró que es vulnerable en el algoritmo de encriptación dado que tiene debilidades de no variación, esta vulnerabilidad se basa en el hecho de que, para ciertos valores de clave, es posible que los bits en los bytes iniciales del flujo de clave dependan de tan sólo unos pocos bits de la clave de encriptación, donde ciertos IV muestran claves débiles. Esta vulnerabilidad fue aprovechada por herramientas de seguridad como AirSnort para descubrir las claves WEP por lo que en la actualidad WEP es obsoleto [23].

En el 2001, WEP fue roto criptográficamente por tres investigadores de seguridad: Scott Fluhrer, Itsik Mantin y Adi Shamir. El ataque que vulneró a WEP es comúnmente conocido como el

ataque FMS. La vulnerabilidad en WEP se debe a que el vector de inicialización de 24 bits es demasiado corto puesto que genera sólo 2^{24} llaves posibles a emplear.

El ataque FMS permite a un atacante descubrir la clave WEP al capturar pasivamente paquetes cifrados, con una tasa de éxito del 50 %. Se deben capturar alrededor de cinco millones de paquetes cifrados, no obstante, un ataque puede tener éxito con muchísimos menos paquetes.

Este ataque se basa en el modo de operación de RC4 y sus dos fases KSA y PRGA, la vulnerabilidad se encuentra en la fase KSA al momento de transmitir los tres primeros bytes de la trama de un texto plano, ya que generalmente estos son los mismos: 0xAA: 0xAA: 0x03, a partir de ello se detectó la relación que existe entre los IV que conforman la entrada al algoritmo KSA y la clave maestra de cifrado. Estos IV reflejan la información de dicha clave y se les dio el nombre de IV débiles los cuales tiene la forma A + 3, 255, X. Donde "A" es el índice del primer byte de la clave maestra, "X" es un valor cualquiera.

En 2004 el ataque de Korek fue introducido el cual se basa en el ataque FMS debido a que este se expande en los cálculos matemáticos del ataque FMS, con el fin de que el ataque sea mucho más rápido y eficaz.

No obstante, en 2007 un nuevo estilo de ataque fue introducido por los investigadores Pyshkin, Tew y Weinman, el ataque es comúnmente conocido como el ataque PTW refiriéndose a los apellidos de los investigadores que lo introducen. Este ataque sólo necesita de 40,000 paquetes para una tasa de éxito del 50 por ciento, mucho menos paquetes de los que necesita el ataque FMS ya que este necesita alrededor de 5 millones de paquetes [20].

En resumen, WEP presenta 3 vulnerabilidades:

- Debilidades en el algoritmo RC4, ya que la debilidad de WEP se centra en la forma de operación de RC4 y sus dos módulos KSA y PRGA lo que permite la desencriptación de un paquete y la obtención de la clave de cifrado.
- Los vectores de inicialización son muy cortos, lo que provoca que en una red varios paquetes utilicen el mismo IV, permitiendo un ataque.
- No existe comprobación de integridad alguna, detección de errores y no es criptográficamente seguro por su linealidad [23].

1.3.2 Protocolo WPA/WPA2

WPA (Wi-Fi Protected Access) solucionó todas las debilidades que presentaba WEP. Este protocolo se considera seguro ya que una de sus principales características es la distribución dinámica de claves y la utilización de nuevas técnicas de integridad y autenticación [24].

WPA fue diseñado como reemplazo temporal para WEP mientras se desarrollaba el estándar IEEE 802.11i (WPA2) el cual se extiende mucho más en las medidas de seguridad. WPA y WPA2 se diferencian poco conceptualmente y difieren principalmente en el algoritmo de cifrado que emplean, mientras WPA basa el cifrado en el uso del algoritmo RC4 al igual que WEP lo único que lo diferencia de WEP es que introduce un protocolo de integridad de llave temporal conocido como (TKIP, *Temporal Key Integrity Protocol*), WPA2 utiliza AES (*Avanced Encryptation Standart*), un cifrado que es mucho más robusto y escalable, así mismo soporta TKIP.

La segunda diferencia notable se encuentra en el algoritmo MIC (Message Integrity Check), utilizado para controlar la integridad del mensaje. Mientras que WPA usa una versión menos elaborada para la generación del código MIC, WPA2 implementa una versión mejorada de este código. A grandes rasgos tanto WPA como WPA2 incrementan el tamaño de las claves y el número en uso e introducen un nuevo mensaje de control de integridad más seguro.

WPA y WPA2 utilizan llaves precompartidas con el fin de autentificar, siempre y cuando no se estén utilizando servidores de autenticación externos, por lo que estas llaves solo se utilizan para autenticación mutua entre el cliente y el AP. Es importante mencionar que la encriptación no utiliza la llave precompartida [20].

WPA y WPA2 distribuyen dinámicamente las claves, tienen una utilización más robusta del vector de inicialización lo que mejora la confidencialidad. Por otro lado, cuentan con nuevas técnicas de integridad y autenticación.

Las principales características de WPA y WPA2 son las siguientes:

- La gestión de llaves de autenticación puede realizarse usando PSK (Pre-Shared-Key) ó 802.1x, éste es un protocolo que permite la autenticación por puerto, posee mecanismos de autenticación, autorización y distribución de claves. Así mismo incorpora controles de acceso mediante un servidor como método de autenticación, proporciona grandes ventajas como por ejemplo: mayor seguridad, incrementa la flexibilidad y control de configuración de acceso, capacidad de expansión, así como una administración simplificada de las credenciales de acceso.
- Cuando el usuario es autenticado de manera correcta se derivan las llaves para proporcionar integridad y encriptación. Estas llaves se guardan en el cliente como en el AP.
- En el caso de WPA, para asegurar la información se hace uso de TKIP y MIC
- Se usan diferentes llaves de encriptación para cada paquete.

1.3.2.1 Autenticación en WPA/WPA2

En el caso de la autenticación tanto en WPA como WPA2 se manejan dos opciones para su implementación:

***Autenticación en modo personal*:** se considera el uso de una clave compartida como método de autenticación para evitar la instalación de un servidor de autenticación, este método de autenticación es usado en entorno SOHO.

Modo Enterprise: está basado en el uso de un servidor de autenticación típicamente RADIUS. Los componentes principales son el cliente que se une a la red, el autenticador[3] que proporciona control de acceso y el servidor de autenticación. El AP divide cada puerto virtual en dos puertos lógicos, uno para el servicio y el otro para la autenticación, lo que constituye el PAE (Port Access Entity) el cual está siempre abierto para permitir la ejecución de tramas de autenticación del servidor.

El cliente y el AP se comunican mediante el protocolo de capa 2 EAPoL (Extensible Authentication Protocol Over LAN), donde el AP convierte los mensajes EAPoL en mensajes

[3] El AP sirve como autenticador.

RADIUS y los reenvía al servidor RADIUS. El servidor de autenticación RADIUS recibe y procesa la solicitud de autenticación. Una vez que el proceso de autenticación se completó, el solicitante y el AP obtienen una clave maestra secreta, MK. A continuación, se describe el intercambio de información entre los elementos.

El primer paso es cuando se hace el intercambio de una petición de asociación inicial entre el cliente y el AP y deciden el uso de una capacidad de seguridad específica.

El segundo paso se lleva a cabo cuando el servidor y el cliente realizan el proceso de autenticación estándar 802.1x y si esta autenticación es satisfactoria el servidor genera y envía una llave maestra al AP. El cliente genera esta misma llave, estas llaves son llamadas PMK (Pairwise Master Key). Posteriormente el cliente y el AP realizan un saludo de cuatro vías (Handshake) para generar un ambiente de confianza entre el cliente y el AP y por último se deriva un MIC y las llaves GTK (Group Transient Key). Para mayor claridad, este proceso se ejemplifica en la figura 1.12 [25].

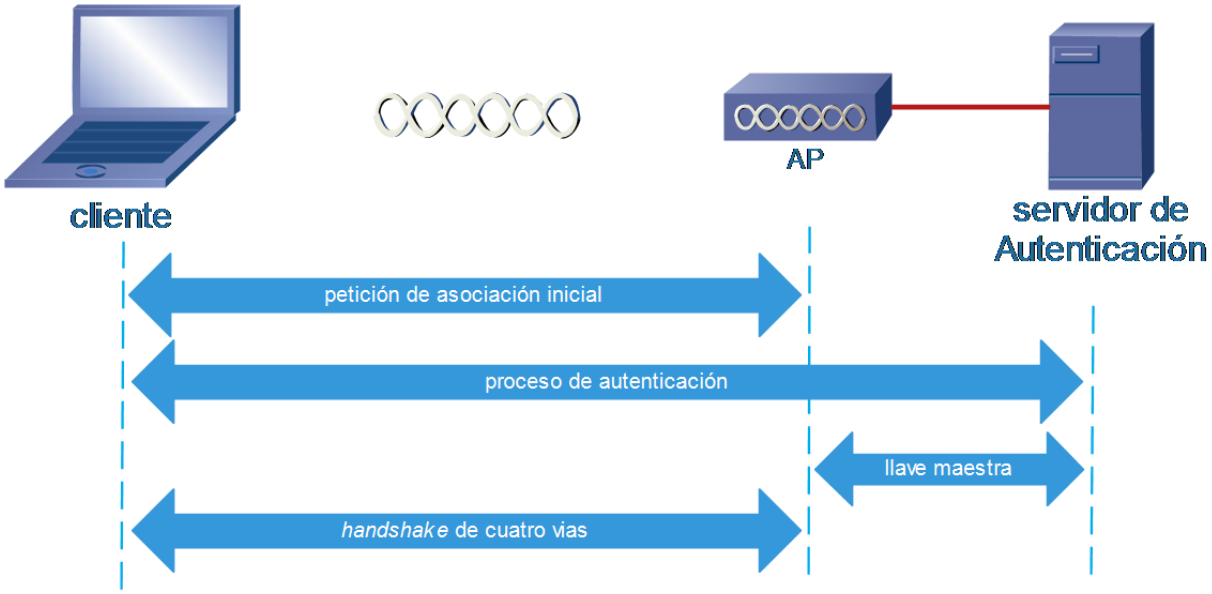


Figura 1.12. Proceso de autenticación WPA /WPA2 enterprise (diagrama propio).

Con la llave PMK se genera una clave de cifrado llamada PTK para cada proceso de autenticación para cada cliente (Pairwise Transient Key) la cual se genera básicamente a partir de dos números aleatorios, uno de ellos generado por el cliente y el otro por el AP, mismos que intercambian para obtener ambos la misma clave PTK. Este proceso se llama saludo de cuatro

vías o 4- *way-handshake* cuyo proceso consta de 4 fases, mismas que se describen a detalle a continuación [16].

Primera fase: una llave maestra en pares (PMK) de 256 bits es independientemente establecida por ambas partes, la cual se genera a partir de la llave PSK y el SSID (Service Set Identifier) de la red. Entonces el AP envía al cliente un número al azar, denominado A-Nonce.

En la segunda fase: el cliente envía un número S-Nonce aleatorio al AP, más un código de integridad de mensaje denominado MIC. Por otra parte, el cliente se encarga de calcular una clave transitoria de pares PTK, la cual es utilizada para cifrar el tráfico. Cabe mencionar que la clave PTK se deriva de la clave PMK, el A-Nonce, el S-Nonce y las direcciones MAC del cliente y del AP.

Tercera fase: se da cuando el AP calcula su propia clave PTK, posteriormente envía al cliente un MIC más un grupo temporal de llaves GTK, estas llaves son utilizadas para descifrar tráfico multicast y broadcast.

En la cuarta fase: el cliente envía un acuse de recibido al AP. En la figura 1.13 se muestra gráficamente el proceso de autenticación (handshake de cuatro vías) [26].

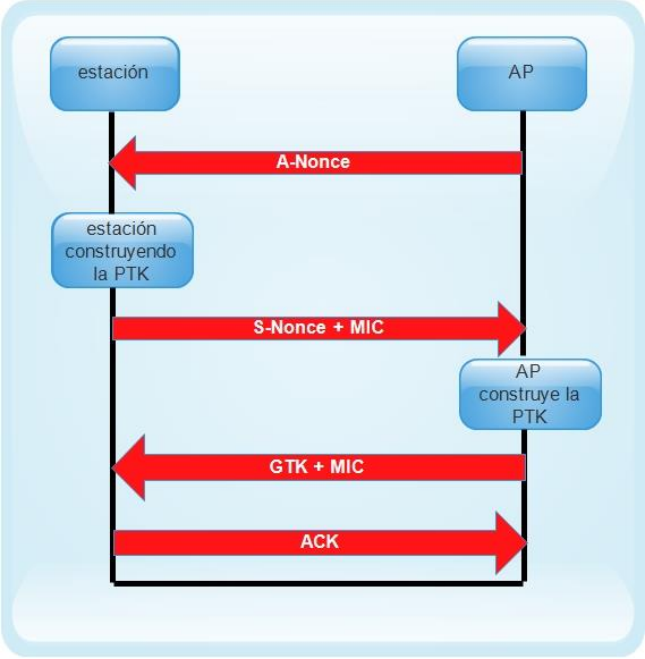


Figura1.13. Handshake de cuatro vías para WPA/WPA2 (diagrama propio).

Cuando el cliente ya se ha autenticado, el protocolo TKIP utiliza 6 claves de cifrado por cada sesión, 4 de estas claves son utilizadas para comunicaciones unicast y 2 para comunicaciones multicast. Estas claves son únicas por cliente y por sesión además de ser cambiadas periódicamente, dichas claves son generadas a partir de las direcciones MAC, el SSID y la clave PTK.

1.3.2.2 Cifrado WPA

WPA basa el cifrado en el algoritmo TKIP que, al igual que WEP, está basado en RC4. A diferencia de éste WPA utiliza un vector de inicialización de 48 bits y una clave de cifrado de 128 bits, así como el protocolo de integridad de clave temporal (TKIP) con el cual la clave de cifrado cambiará cada vez que un paquete se transmita.

TKIP genera un bloque de 4 bytes a partir de la dirección MAC de origen, MAC de destino, de datos y el MIC para calcular la unidad de datos a enviar. Los datos que incluyen al MIC son fragmentados y se les asigna un número de secuencia. Por lo tanto, la mezcla del número de secuencia con la clave temporal genera la clave que será utilizada para el cifrado de cada fragmento.

1.3.2.3 Cifrado WPA2

El cifrado para WPA2 se realiza mediante el algoritmo AES (Advanced Encryptation Standard), el cual es un tipo de cifrado de clave simétrica. WPA2 utiliza grupos de bits de longitud fija (bloques), un cifrado de clave simétrica y utiliza la misma clave tanto para la encriptación como para la desencriptación. En la implementación AES los bits se cifran en bloques de texto plano usando una longitud de clave de 128 bits que se calculan independientemente.

AES utiliza el protocolo CCMP (*Counter-Mode/ CBC-MAC Protocol*) y CCM (Counter with CBC-MAC). Este es un nuevo modo de operación para un cifrado de bloques que permite usar una sola clave tanto para el cifrado como para la autenticación (con diferentes vectores de inicialización).

CBC-MAC se utiliza para generar un componente de autenticación como resultado del proceso de cifrado [27].

En la figura 1.14 se ejemplifica el algoritmo AES, así como los algoritmos con los que se auxilia para poder generar el cifrado.

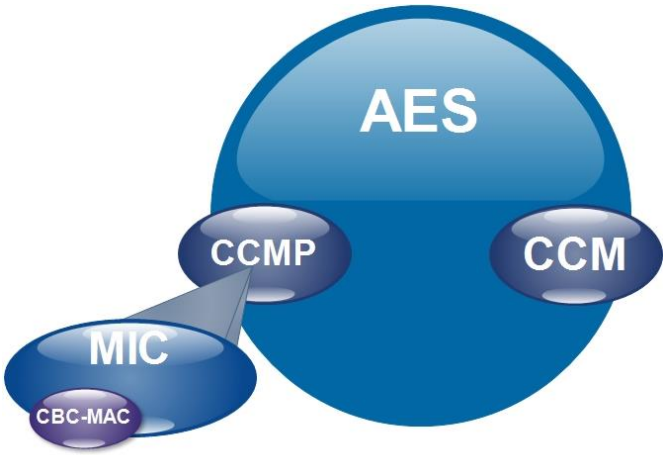


Figura 1.14. Algoritmo AES (diagrama propio).

1.3.2.4 Vulnerabilidades de WPA /WPA2

Si un usuario malicioso quiere atacar una red WPA-PSK va a tratar de capturar el intercambio de números aleatorios, el SSID y las direcciones MAC tanto del cliente como del AP. Una vez teniendo esta información, el atacante puede obtener la desencriptación de la clave para poder conectarse a la red [16, 22].

Algunas vulnerabilidades que están asociadas al protocolo WPA son las siguientes [20]:

- WPA confía en la encriptación RC4 la cual no es una de las opciones más confiables.
- Fisuración WPA-PSK, esta vulnerabilidad permite forzar el PSK para obtener la llave compartida WPA, debido a que un atacante puede ver el valor *nonce* no cifrado enviado al cliente.
- Es susceptible a ataques pasivos por el falseamiento (Spoofing) de autenticación WPA, vulnerabilidad que forza a un usuario a desautenticarse para romper la sesión WPA PSK, dando paso a una denegación de servicios (DoS – Denial of Service).
- Es susceptible a ataques de fuerza bruta al tener activado el WI-FI Protected Setup (WPS), la vulnerabilidad se encuentra en el PIN, al dividirse en dos PIN separados de cuatro dígitos ya que reduce considerablemente el tiempo de la obtención de la clave.

Se han revisado los protocolos de seguridad que se pueden implementar en una red inalámbrica de área local, pero ¿qué tan seguras son estas autenticaciones? ¿Se podrá romper esta seguridad? Para contestar estas preguntas es necesario realizar pruebas de penetración[4] en un entorno controlado.

1.4 Herramientas para la revisión de seguridad en una WLAN

Para identificar las posibles vulnerabilidades existentes en una WLAN es necesario realizar una revisión de la seguridad en dicha red a evaluar, para ello propongo utilizar herramientas que operan en sistemas operativos basados en Linux.

Algunos ejemplos de distribuciones para sistemas operativos basados en Linux que contienen dichas herramientas son: Back Box, Parrot Security, DEFT, NTS, Wifilax y Kali Linux. A continuación, en los siguientes párrafos se hace una breve descripción de las características de estas distribuciones mencionadas.

BackBox: esta distribución está basada en Ubuntu y fue desarrollada para realizar pruebas de *hacking* ético, de penetración de sistemas y redes, así como auditar seguridad, esta distribución es ligera y funciona en sistemas de hardware poco potentes.

Parrot Security OS: es un sistema operativo basado en Debian, es una mezcla de Frozenbox OS y Kali Linux por lo que utiliza los repositorios oficiales de Kali Linux. Con esta distribución se pueden realizar pruebas de penetración, auditar redes y cuenta con herramientas para *hacking* ético.

Digital Evidence & Forensics Toolkit (DEFT): está basado en Ubuntu ofrece herramientas forenses creadas por los propios usuarios y compañías para su propio uso, con esta distribución se pueden realizar auditorías de seguridad.

Network Security Toolkit (NST) basada en Fedora, esta distribución cuenta con herramientas de análisis de seguridad de redes, programas de validación y monitoreo, que puede ser utilizado

[4] Una prueba de penetración se refiere a un ataque de prueba que puede sufrir un sistema informático, red o aplicación web cuya finalidad es encontrar vulnerabilidades que un atacante podría explotar.

en servidores virtuales. NST tiene una interfaz de usuario web (WUI) lo que permite configurar las aplicaciones de seguridad y redes.

Wifilax es una distribución GNU/Linux diseñada para auditorias de seguridad y relacionada con la seguridad informática en general, incluye herramientas de seguridad y auditorias de seguridad como escáner de puertos, creación y diseño de *exploits*, *sniffers*, herramientas de análisis forenses, entre otras.

Kali Linux es denominada como una distribución de seguridad por excelencia, ya que contiene cientos de herramientas que permiten llevar a cabo tareas dentro del marco de pruebas de penetración y auditoria. El ámbito concreto de dicha distribución es la seguridad informática por lo que el análisis forense, el intento de intrusión no autorizada *(gathering)*, la explotación de vulnerabilidades, entre otras se encuentran en Kali Linux.

Para identificar las vulnerabilidades en la presente tesis se utiliza la distribución Kali Linux versión 2017.1 principalmente por la colección de herramientas que proporciona, cabe mencionar que exclusivamente se utilizaran algunas de las herramientas para ataques inalámbricos de la Suite AIR.

1.4.1 Kali Linux

Kali Linux es una distribución de auditorías de seguridad y pruebas de penetración, construida en base a Debian Linux, esta distribución reemplazó a Bactrack Linux y fue completamente reconstruida, incluye una amplia gama de herramientas para la recolección de información, sniffing y spoofing, evaluación de vulnerabilidades, cracking de contraseñas, explotación, ingeniería inversa, investigación forense, entre otras. Las pruebas de penetración inalámbricas son procesos que consisten en la simulación de ataques contra una red con el fin de indicar debilidades o vulnerabilidades de seguridad, las cuales podrían ser utilizadas o aprovechadas por atacantes reales para tener acceso a la red.

Con este tipo de pruebas de penetración de forma práctica se pretenden explotar las vulnerabilidades mediante la realización de un ataque. Dichas pruebas de penetración pueden ser externas o internas, será externa cuando se intenta simular un ataque externo real sin que los que están realizando estas pruebas posean información previa sobre las redes de destino. Sin

embargo, en las pruebas de penetración interna, la información sobre las vulnerabilidades que existen en la red se les proporciona a los auditores para que puedan explotar al máximo las vulnerabilidades existentes.

1.4.1.1 Herramientas específicas de Kali Linux para atacar a una WLAN

Kali Linux cuenta con herramientas para las pruebas de penetración inalámbrica donde existe un conjunto llamado meta paquete inalámbrico Kali-Linux-Wireless con las herramientas de código abierto más conocidas como: la suite Aircrack-ng, Kismet, Fern Wifi Cracker, Wifite, Reaver entre otros.

Existen otras herramientas que no son propias de Kali Linux las cuales pueden ser instaladas en la distribución, una de estas es Wifiphisher. Esta herramienta básicamente engaña a los usuarios creando un punto de acceso falso para obtener su contraseña.

Cabe mencionar que la Suite AIR es el conjunto más completo y popular de herramientas para auditoría a redes inalámbricas en Kali Linux.

1.4.1.2 Suite AIR

La Suite AIR contiene una gran variedad de herramientas con el prefijo *air* algunas de estas herramientas son airmon, aircrack, airodump, aireplay, airdecap, airbase, entre otras. Dichas herramientas permiten cambiar el modo de trabajo de la tarjeta inalámbrica, inyectar paquetes, desautenticar clientes, descifrar tráfico, entre otras funciones. En la tabla 1.2 se describen algunas de las herramientas más populares para auditorias de seguridad de una WLAN de la Suite AIR [16, 26].

Herramienta	Función
Airmon-ng	Cambia el modo de trabajo de la tarjeta inalámbrica al pasarlo a modo monitor.
Airodump-ng	Captura todo lo que circula en el aire independientemente del cifrado o red. En las redes abiertas se puede visualizar el tráfico y se puede capturar información sensible que viaja o circula por el medio de transmisión (en el aire).
Aireplay-ng	Realiza los ataques tanto a los AP como a los clientes asociados a dicho AP.
Aircrack-ng	Realiza ataques de fuerza bruta de diccionario o estadísticos a capturas de tráfico inalámbrico. En función del tipo de cifrado de la red víctima se realiza un tipo de ataque u otro.

Tabla 1.2. Algunas herramientas para auditorias de seguridad de Kali Linux.

En el anexo A se detalla el funcionamiento de estas herramientas.

1.5 Opciones para robustecer la seguridad en la WLAN

Las redes inalámbricas se han vuelto un punto muy atractivo para un gran número de atacantes: muchos usuarios del mundo de la informática han intentado llevar a cabo un ataque sobre todo a redes inalámbricas. Un ejemplo muy claro sobre este tipo de ataques es cuando un usuario intenta obtener la contraseña de una WLAN para poder obtener acceso a internet, siendo este el ataque más sencillo.

Un atacante se vuelve peligroso cuando tiene conocimiento del propio ataque, así como del funcionamiento de las herramientas que se utilizan para explotar las vulnerabilidades de seguridad. Por dicho motivo es necesario dificultar la labor del atacante al robustecer la seguridad en una WLAN mediante la implementación de *hardening*.

1.5.1 Hardening

Hardening es un conjunto de actividades para robustecer la seguridad, cuyo objetivo es proteger la red y estropear el trabajo del atacante. El *hardening* defiende el sistema y gana a su vez tiempo para poder minimizar las consecuencias de un ataque o incluso evitarlo en su totalidad. Este robustecimiento se logra mediante la protección en varias capas, lo que significa que puede protegerse a nivel host, nivel de aplicación, nivel de sistema operativo, nivel de usuario y nivel físico; donde cada nivel necesita un método único de seguridad. En este trabajo sólo se protegerá a nivel host y a nivel usuario.

La eliminación de servicios innecesarios, el cierre de puertos que no estén en uso, la eliminación de usuarios, etc., son una buena actividad para fortalecer la red.

De acuerdo con el estudio realizado anteriormente sobre las vulnerabilidades en una WLAN, se toman las vulnerabilidades encontradas para implementar *hardening*. Se le puede brindar mayor seguridad a una WLAN al robustecer algunas funciones de manera individual en el AP. A pesar de que *hardening* es un método con el cual se pueden implementar múltiples estrategias, su aplicación debe ser personalizada. A continuación, se enlistan en la tabla 1.3 las actividades para la implementación de *hardening* en una WLAN.

Actividades de *hardening*	Tipo de configuración
Servidor de autenticación	Configuración externa
Desactivación del WPS	Configuración interna
Creación de contraseñas seguras	Configuración interna
Cambio de contraseñas periódicamente	Configuración interna
Desactivación de la difusión SSID	Configuración interna
Filtrado MAC	Configuración interna
Gestión del AP	Configuración interna
Minimización de la potencia de AP	Configuración interna
Actualización del firmware	Configuración interna
Enmallado al entorno de la zona WI-FI	Implementación externa

Tabla 1.3. Puntos de hardening propuestos.

1.5.1.1 Actividades de *hardening*

En los párrafos siguientes se describen los puntos de *hardening* mencionados en la tabla 1.3.

Servidor de autenticación: Debido a las vulnerabilidades que se tienen en una WLAN personal, es necesario reforzar la autenticación con una mayor seguridad. Para ello, se migra la autenticación *enterprise* a un entorno SOHO, con el propósito de proporcionar una mayor seguridad. En la sección 1.5.1.2 se describen los diferentes servidores de autenticación, en este caso se llevará a cabo la implementación del servidor RADIUS.

Desactivación del WPS (WI-FI Protected Setup): Es importante la desactivación del WPS ya que con la herramienta *reaver* es posible atacar una WLAN con este tipo de configuración. El WPS permite la conexión de un nuevo dispositivo a la red con el hecho de presionar un botón en el AP sin necesidad de introducir la contraseña, lo que representa una vulnerabilidad en la implementación del estándar WPS la cual podría explotarse para obtener la contraseña del AP.
Creación de contraseñas seguras: es de suma importancia la creación de contraseñas más seguras en tamaño y complejidad, con un mínimo de ocho caracteres donde debe utilizarse una combinación de números, letras tanto minúsculas como mayúsculas, así como caracteres especiales con el fin de que éstas no sean descifradas tan fácilmente. Esto implica que el atacante deberá crear diccionarios mucho más complejos para poder atacar las WLAN.

Cambio de contraseñas periódicamente**:** es indispensable el cambio de contraseñas periódicamente para evitar ser víctima de algún ataque y evitar robo de información.

Caso1: se recomienda cambiar la contraseña WPA/WPA2 cada mes.

Caso 2: se recomienda cambiar las contraseñas en usuarios cada mes y aplica solamente cuando se cuenta con un servidor de autenticación.

Configuración del identificador de conjunto de servicios (SSID) y desactivación de la difusión SSID: Este es un identificador comúnmente conocido como el nombre de la red, de forma predeterminada la mayoría de los AP transmiten el SSID y regularmente no es cambiado. Gracias a esto, los atacantes pueden identificar el AP que desean atacar, lo que crea una vulnerabilidad. Por dicho motivo debe desactivarse y cambiarse el nombre del SSID de la red para hacer más difícil el trabajo a los posibles atacantes.

La desactivación de la difusión del SSID aumenta la dificultad de realizar un escaneo pasivo, por lo que se debe configurar un intervalo de tiempo para anunciar la red (Beacon interval), estableciéndolo en su máximo valor, dicho intervalo es el tiempo transcurrido antes de que el AP anuncie el SSID a través de broadcast.

Filtrado MAC: El filtrado MAC es utilizado para restringir el acceso de ciertos dispositivos a una red inalámbrica. Al dar de alta solamente a los equipos que podrán asociarse a dicha red, permite solamente el acceso a las direcciones MAC especificadas. Esta actividad ayuda en el caso de que el atacante obtenga la contraseña del AP.

Gestión del AP: Es posible que un atacante se filtre a la red donde está el AP, por lo que puede entrar a la configuración de este y realizar distintas configuraciones o modificaciones.

En el caso particular de México, los AP que ofrece un proveedor de servicios de internet (ISP, Internet Service Provider) tienen esta vulnerabilidad de gestión al poder acceder fácilmente a la gestión del AP. En la tabla 1.4 se muestra el modelo del AP que ofrecen algunos ISP, el usuario y la contraseña por default de éstos.

ISP	Dirección IP para acceder al AP	Usuario	Contraseña
Telmex	192.168.1.254	TELMEX	Contraseña que viene por default en el AP
IZZI	192.168.100.1	Admin	Password
Total Play	192.168.100.1	Root	Admin

Tabla 1.4. Comparativa de acceso a la gestión.

En esta pequeña tabla se puede apreciar la poca seguridad que se tiene en los AP para su gestión, siendo este un problema ya que los atacantes suelen tener una base de datos con sus respectivos usuarios y contraseñas. Cabe destacar que la mayoría de los usuarios dejan la configuración establecida por el ISP.

Minimización de potencia del AP: Es necesario limitar la cobertura de la red inalámbrica para que no cubra más del área deseada, para evitar que esta señal llegue a las antenas que utilizan los atacantes, así como evitar que la red sea identificada.

Actualización de *firmware***:** es necesario estar actualizando el firmware de cada AP para poder actualizar los parches de seguridad.

Enmallado al entorno de la zona WI-FI: para evitar ataques denominados *wardrivening*, que consisten en la búsqueda y recolección de datos de una red inalámbrica, donde el atacante está siempre en movimiento; el enmallado bloquea el área de tal forma que la señal no salga del área determinada, así mismo evita que otras señales entren. Esta recomendación es poco utilizada ya que su implementación es muy costosa, la estructura debe ser como una jaula tipo Faraday.

En la figura 1.15 se muestran las capas de seguridad que se le proporcionarían la WLAN de entorno SOHO al implementar *hardening*.

Figura 1.15. Capas de seguridad de hardening (diagrama propio).

1.5.1.2 Tipos de servidores de autenticación

Un servidor de autenticación es un tipo de servidor de red, cuyo objetivo es validar y autenticar a usuarios remotos o nodos que se conectan a un servicio, dicho servidor garantiza que solamente los nodos autorizados tengan acceso a los recursos ofrecidos por éste.

Esencialmente existen tres diferentes tipos de tecnología para sistemas de autenticación siendo estos: LDAP, Kerberos y RADIUS. Se describe en seguida cada uno de estos.

El servidor LDAP (Lightweight Directory Access Protocol) esencialmente es un sistema de base de datos cuya función es almacenar información sobre diversas entidades de la red. En una red típica almacena nombre de usuario, contraseñas asociadas a los nombres de usuarios, información de configuración, derechos asociados con los nombres de los usuarios, entre otros. LDAP es típicamente el núcleo del sistema de autenticación.

Kerberos no almacena nada que no sea nombre de usuario, contraseñas y claves utilizados para identificar los servicios de red LDAP. Este servidor se utiliza para obtener un ticket[5] para el nombre de usuario y contraseña, por lo tanto, LDAP almacena información acerca de los usuarios y kerberos es una forma de autenticar a esos usuarios.

RADIUS (Remote Authentication Dial In User Service) se utiliza para autenticar dispositivos en el momento en que intentan conectarse a una red privada. Es más utilizado por los ISP para garantizar que sólo los clientes puedan conectarse a sus sistemas de acceso telefónico. Es probable que el AP también admita RADIUS para que los usuarios autorizados se conecten de forma segura y al mismo tiempo se mantenga fuera a los usuarios que no estén autorizados [28,29]. Como puede notarse no solo existe un solo servidor de autenticación, pero para el presente trabajo se utilizará RADIUS. A continuación, se describe a detalle el servidor de autenticación RADIUS.

[5] Un ticket es un conjunto de información electrónica que identifica a un usuario o un servicio e indica que privilegios tienen para acceder a la red.

1.5.1.3 Servidor RADIUS

RADIUS es un protocolo de red, cuyo sistema define reglas y convenciones para la comunicación entre dispositivos de red para usuarios remotos. Este protocolo esencialmente cumple con tres funciones principales: autenticar usuarios o dispositivos antes de que a éstos se le permita el acceso a una red, autorizar a los usuarios la utilización de algunos servicios de red específicos, contabilizar y rastrear el uso de dichos servicios.

El protocolo cliente servidor RADIUS tiene diversas ventajas, como por ejemplo: es una solución escalable y abierta, de fácil modificación, separa los procesos de seguridad y comunicación, es adaptable a la mayoría de los sistemas de seguridad, funciona con cualquier dispositivo de comunicación que soporte RADIUS, entre otras.

Por otro lado, RADIUS separa eficazmente los procesos de seguridad que se llevan a cabo en el servidor de autenticación de los procesos de comunicación, lo que permite un único almacenamiento centralizado de información para la autorización y la autenticación, lo que reduce la carga administrativa del control de acceso para un gran número de usuarios remotos [30].

1.5.1.3.1 Funcionamiento de RADIUS

Un servidor RADIUS utiliza una base de datos central para autenticar usuarios remotos. RADIUS funciona como un protocolo cliente-servidor, autentica a cada usuario con una clave de cifrado única cuando se concede el acceso.

Cuando un cliente está configurado para utilizar RADIUS, cualquier usuario de este cliente presentará información de autenticación de inicio de sesión personalizada, donde se espera que el usuario ingrese tanto su nombre de usuario como la contraseña. Una vez que el cliente ha obtenido la información deseada se debe realizar la autenticación donde el cliente creará un *Access- Request* el cual contendrá el nombre de usuario, la contraseña, el ID del cliente y el ID del puerto en el que se accede cuando una contraseña está presente.
La petición de acceso se envía al servidor RADIUS a través de la red, si no hay una respuesta en un periodo de tiempo determinado se realiza un reenvió. Una vez que el servidor RADIUS recibe la contraseña, válida el envío cliente. Si el cliente es válido, el servidor RADIUS consulta

una base de datos de usuario cuyo nombre debe coincidir con la solicitud. Para que el usuario pueda entrar a la red éste debe cumplir una serie de requisitos, que incluye la verificación de la contraseña, así como la especificación de los puertos a los que tiene el acceso autorizado dicho cliente.

El servidor RADIUS puede realizar peticiones de otros servidores para satisfacer la solicitud, en este caso el servidor actúa como cliente. En caso de que algunos de los atributos de estado proxy[6] estuvieran presentes en la solicitud de acceso deben ser copiados sin ser modificados y en orden en el paquete de respuesta, otros atributos pueden colocarse también antes, después o incluso entre los atributos de estado proxy.

En caso de que no se cumpla ninguna condición, el servidor RADIUS enviará un mensaje *Access- Reject* lo que indica que la solicitud de usuario no es válida. En la figura 1.16 se muestra el proceso descrito anteriormente del servidor RADIUS.

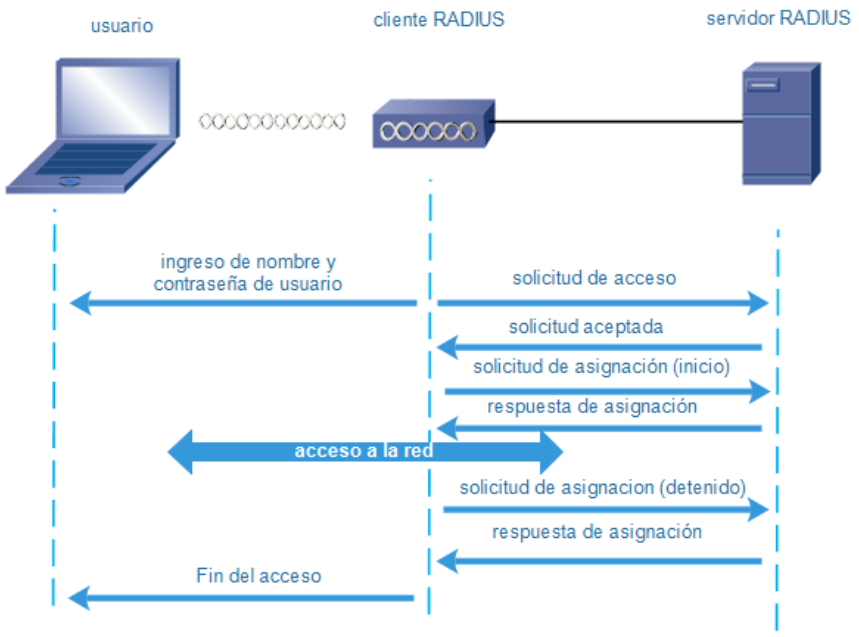


Figura 1.16. Operación del servidor RADIUS (diagrama propio).

Por otro lado, el servidor RADIUS que mayor popularidad tiene es freeRADIUS, el cual es modular y ofrece escalabilidad en el diseño del protocolo. Estas y otras características lo posicionan por encima de otros servidores de autenticación. Así mismo proporciona múltiples beneficios y ventajas las cuales a continuación se describen.

[6] Un proxy es un intermediario que procesa solicitudes de clientes.

1.5.1.3.2 Ventajas y beneficios de freeRADIUS

FreeRADIUS permite más tipos de autenticación que cualquier otro tipo de servidor, es el único servidor RADIUS de código abierto que admite el protocolo EAP (Extensible Authentication Protocol) y también es el único que admite servidores virtuales, el uso de servidores significa que las implementaciones complejas son simplificadas.
El protocolo de diseño modular hace que FreeRADIUS sea fácil de entender lo que simplifica a su vez la agregación o eliminación de módulos. El uso de la memoria también es importante ya que esta flexibilidad permite que el servidor funcione en plataformas que van desde sistemas embebidos hasta máquinas multi-core con gigabytes de RAM.

La escalabilidad le permite al servidor manejar fácilmente una solicitud cada pocos segundos al manejar miles de peticiones por segundo. El servidor RADIUS es el responsable de recibir la solicitud de conexión, autenticar al usuario y devolver al mismo tiempo la información de configuración.

Cada sesión de usuarios individual está cifrada de forma exclusiva, impidiendo que otros usuarios obtengan información privada, a diferencia de una red PSK, en donde cada usuario comparte la misma clave de cifrado.

Un usuario o dispositivo particular puede ser desautorizado mediante la desactivación de la clave de cifrado única correspondiente. Esta desactivación garantiza que el usuario desautorizado no puede acceder a la red con ninguna otra clave, sin afectar las claves de seguridad para otros usuarios.

1.5.1.3.3 Desventajas del servidor RADIUS

Algunas de las desventajas que se pueden presentar en el servidor de autenticación freeRADIUS se describen en los siguientes párrafos.
Interoperabilidad: a pesar de que 802.1x tiene una aceptación casi universal, el uso de los distintos métodos de EAP implica que la interoperabilidad no siempre está garantizada, debido a la incompatibilidad que se presenta en los dispositivos al no contar con los mismos certificados de autenticación, por lo que el servidor RADIUS no otorga el acceso a la red.

Disponibilidad: al tratarse de una configuración de seguridad compleja, muchas de las pequeñas empresas (Pymes) no disponen o hacen uso del estándar 802.1x.

A continuación, se hace una breve descripción del estándar IEEE 802.1x el cual trabaja en conjunto con el servidor RADIUS para realizar la autenticación [31, 32, 33].

1.5.1.3.4 Autenticación IEEE 802.1x

Esta autenticación fue establecida específicamente en un inicio para redes cableadas, donde el mecanismo permite que un cliente, mejor conocido como suplicante, sea autenticado a una red inalámbrica a través del uso de un servidor de autenticación.

IEEE 802.1x está compuesto básicamente por tres entidades funcionales:

- El suplicante que se une a la red
- El autenticador que hace el control de acceso
- El servidor de autenticación que toma las decisiones de autorización

En el caso de las redes inalámbricas el AP es el autenticador. Utiliza PAE (Port Access Entity), donde cada puerto físico se divide en dos puertos lógicos: PAE de autenticación y PAE de servicio. La PAE de autenticación está siempre abierta y permite el paso de procesos de autenticación, mientras que la PAE de servicio sólo se abre tras una autenticación exitosa.

802.1x utiliza una combinación del protocolo de autenticación extensible EAP y RADIUS para autenticar clientes y distribuir las claves. EAP es un entorno para el transporte de varios métodos de autenticación, permite solamente un número limitado de mensajes (Request, Response, Success, Failure), mientras que otros mensajes intermedios son dependientes del método de autenticación como EAP-TLS, EAP-TTLS, PEAP.

Una vez que el proceso se ha completado ambas entidades tanto suplicante como servidor de autenticación tendrán una clave secreta.

La autenticación 802.1x se inicia cuando el AP pide datos de identidad del cliente e incluye el método de autenticación preferido. Se intercambian entonces mensajes apropiados entre el cliente y el servidor de autenticación para generar una clave maestra (MK - Master Key) común.

Al final del proceso, se envía desde el servidor de autenticación al AP un mensaje final EAP Success para el cliente. EAP es un protocolo utilizado por 802.1x para efectuarse la autenticación de un usuario, para conocer este proceso en la siguiente sección se describe a grandes rasgos dicho protocolo [27].

1.5.1.3.4.1 Protocolo EAP

El protocolo EAP es utilizado por el estándar 802.1x y WPA2 *enterprise* para autenticar a un usuario antes de que se le permita el acceso a la red. Debido a que utiliza uno de los muchos métodos disponibles para autenticar un usuario. Este protocolo cuenta con tres componentes más: autenticador, suplicante y servidor de autenticación *backend*.

En el caso del autenticador éste se encarga de controlar quién puede y quién no tener acceso a la red. En una red inalámbrica el autenticador es el AP, el cual debe tener incorporado en sí mismo la seguridad WPA2-*Enterprise*.

El autenticador facilita la transmisión entre el suplicante y el servidor de autenticación. Éste no decide a quién le permite o niega el servicio de acceso a la red, el autenticador sigue las instrucciones del servidor de autenticación de *backend*. El autenticador utiliza TCP/IP para comunicarse con el servidor RADIUS y EAP para comunicarse con el suplicante.

El suplicante concede al cliente acceso a la red, soporta varios métodos de autenticación y utilizará solo uno. Desafortunadamente, para algunos sistemas operativos es posible que no se incluya soporte para un método EAP requerido, lo que se puede resolver con la instalación de un suplicante que incluya el soporte requerido para el método EAP requerido.

El tipo de red en la que se utiliza el suplicante determina la forma en que el suplicante encapsula los paquetes EAP para comunicarse con el autenticador. En la red WI-FI será encapsulado dentro del protocolo EAPoW (EAP over Wireless).

El servidor de autenticación de *backend* es el que decide a quién se le concede o niega el acceso a la red a pesar de que el autenticador controla el acceso, este servidor normalmente es un servidor RADIUS [31].

En el siguiente capítulo se indica la metodología para identificar vulnerabilidades en una WLAN, así como la metodología para la implementación de *hardening* para brindarle mayor seguridad a una WLAN.

CAPÍTULO II

"Los virus informáticos muestran la naturaleza humana: la única forma de vida que hemos creado hasta el momento es puramente destructiva."

Stephen Hawking

Capítulo 2 Metodología

De acuerdo a los objetivos que se plantearon en la presente tesis de implementar *hardenig* para robustecer la seguridad de una WLAN en un entorno SOHO a partir de una identificación de vulnerabilidades, en este capítulo se describe la metodología para llevar a cabo exitosamente dicha implementación.

La siguiente metodología se divide en dos partes, tal que la primera parte se enfoca en la identificación de vulnerabilidades en una WLAN y en la segunda parte se aborda la implementación de *hardening* para solventar las vulnerabilidades.

2. Metodología para identificar vulnerabilidades.

Para realizar la identificación de vulnerabilidades fue necesario seguir los siguientes pasos:

1.- Diseñar un escenario para realizar las pruebas de vulnerabilidad.

2.- Instalar una máquina virtual para realizar los ataques.

3.- Determinar herramientas para realizar ataques.

Dichos pasos se describen a detalle en los siguientes párrafos.

Para identificar las vulnerabilidades se diseñó un escenario de pruebas que consta de: un atacante implementado en una laptop con la distribución Kali Linux; una WLAN conformada por un módem[7] que ejecuta la función de AP y los dispositivos que tiene acceso a la red, estos son: dos celulares con sistema operativo Android, una laptop y una computadora de escritorio a la cual se le adaptó una tarjeta inalámbrica debido a que los ataques se hicieron de forma inalámbrica. Todos los dispositivos anteriormente mencionados forman un BSS.

[7] Originalmente un módem es un sistema que transforma señales analógicas a digitales y viceversa, actualmente tiene funcionalidades de un router, un switch, firewall y un AP.

El escenario de prueba de ataques es el que se muestra en la figura 2.1.

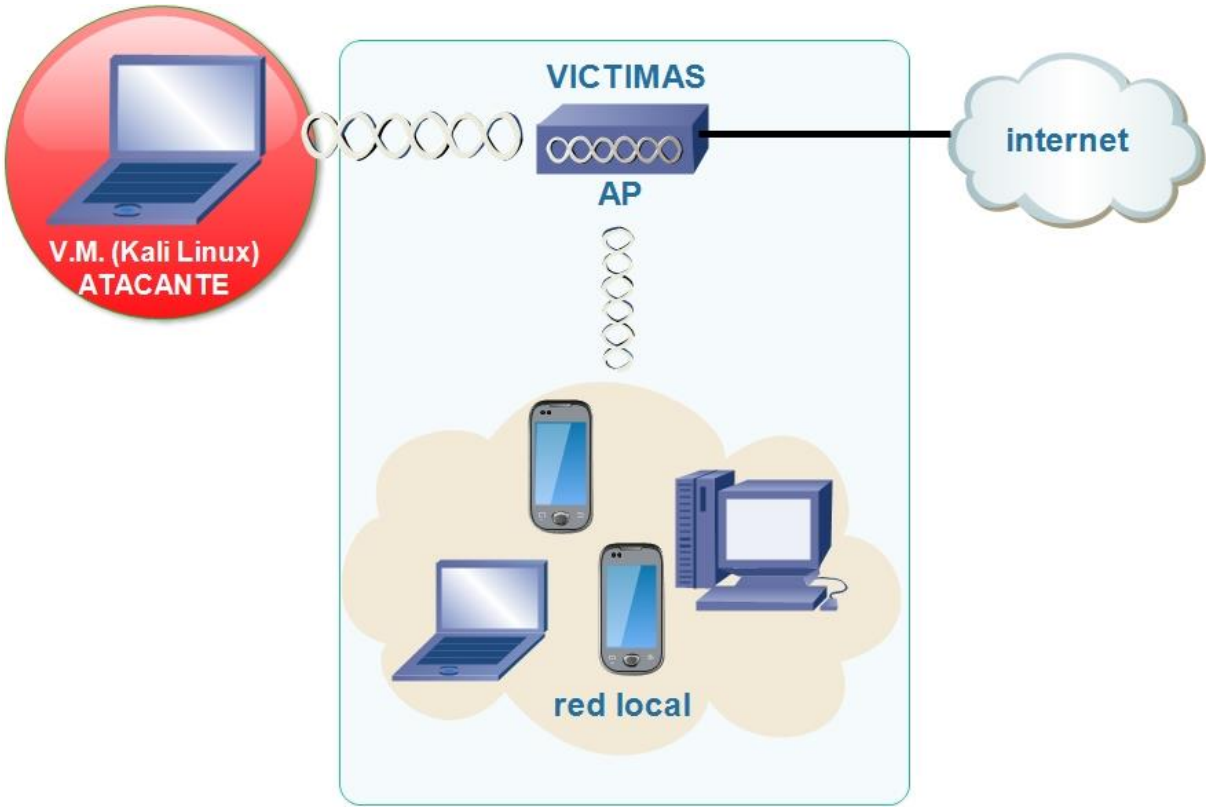


Figura 2.1. Diseño del escenario de pruebas en un BSS (diagrama propio).

Las características de los dispositivos que jugaron el papel de víctimas como el atacante usados en el escenario de pruebas se muestran en la tabla 2.

Dispositivo	Características
Celular Infinix (víctima)	Android versión 6.0, 1GB de RAM, CPU Quad-core
Celular Sony E1(víctima)	Android versión 4.4.2., 512 de RAM, CPU Qualcomm
Laptop Toshiba (víctima)	Sistema operativo windows de 64 bits, 4GB de RAM, procesador Intel core i3
AP ARCADIAN (modelo VRV9529AWAC24) (víctima)	Compatible con los estándares b/g/n/ac con seguridad WEP, WPA, WPA2 (PSK y 802.1x)
Computadora de escritorio (víctima)	Sistema operativo Windows de 32 bits, 512MB de RAM, procesador Intel pentium 4
Laptop Toshiba (atacante)	procesador: Intel(R), Core (TM) i5-3317U CPU@ 1.70GHz, memoria RAM: 8 GB, Sistema operativo Kali Linux de 64 bits, Disco duro: 1 TB

Tabla 2. Características de los dispositivos en el escenario.

No sólo se realizaron ataques en el escenario de pruebas ya que se atacaron AP encontrados en el medio de los cuales se desconocen sus características, cabe resaltar que los ataques a estos AP se realizaron con el permiso previo.

Para llevar a cabo los ataques a los protocolos de seguridad de una WLAN, se usó una máquina virtual con la distribución Kali Linux y una tarjeta inalámbrica que trabaja bajo los estándares 802.11 b/g/n con un alcance aproximado de 50 m, con una antena de 5 dBi, que opera a una frecuencia de 2.4 GHz.

Se optó por la instalación de una máquina virtual debido a que ésta se puede ejecutar dentro del sistema operativo principal, sin la necesidad de desinstalar el sistema operativo ya existente. Así mismo, aprovecha los recursos reales del ordenador comportándose como si fuera el sistema operativo principal.

2.1 Máquina virtual para la identificación de vulnerabilidades

El software de virtualización que se utilizó para crear la máquina virtual fue Virtual Box, se optó por esta opción debido a que es un software libre. En el anexo B se describen los pasos a seguir para crear una máquina virtual con Kali Linux.

El siguiente paso fue actualizar el sistema operativo antes de utilizar las herramientas de Kali Linux o la instalación de cualquier otro programa, dicha actualización se realiza mediante los siguientes comandos:

```
# apt-get update
# apt-get upgrade
```

Para atacar a la WLAN deseada, se usan las herramientas que se presentan en la tabla 2.1.

Protocolo	Herramienta
WEP	Ferm-WIFI, Suite AIR
WPA personal	Wifiphisher, Airmon-ng, Airodump-ng, Aireplay-ng, Aircrack-ng
WPA2 personal	Airmon-ng, Airodump-ng, Aireplay-ng, Aircrack-ng
WPA/WPA2 *enterprise*	Hostapd-wep, zcat.

Tabla 2.1. Herramientas para ataques.

Para mitigar las vulnerabilidades que presentan las WLAN se implementó *hardening* mediante la metodología que se indica a continuación.

2.2 Implementación de *hardening* en una WLAN

Para llevar a cabo la implementación de *hardening* se siguen los siguientes pasos:

1.- Implementación de un servidor de autenticación (freeRADIUS)

Una vez que esté configurado el servidor de autenticación éste estará en la topología de la WLAN como se muestra en la figura 2.2.

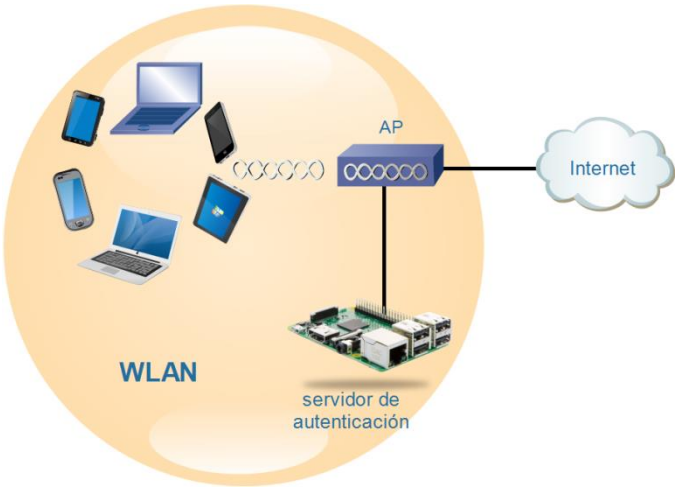


Figura 2.2. Topología de la WLAN con el servidor de autenticación freeRADIUS (diagrama propio).

2.- Configuración del AP.

Estos pasos se describirán a detalle en las siguientes secciones.

En la sección 1.5.1 del capítulo 1 se describió el conjunto de actividades que componen la implementación de *hardening*, sin embargo, se implementaron solamente los siguientes puntos: servidor de autenticación, desactivación de la difusión del SSID, filtrado MAC, cambio del nombre de la red, desactivación del WPS, creación de contraseñas seguras, gestión del AP, minimización de la potencia del AP y actualización del firmware. El enmallado no se implementó debido a que es una actividad muy costosa. Con la implementación de estos puntos de *hardening* se podrá evitar el acceso a la WLAN y complicar el trabajo a usuarios maliciosos

ya que con *hardening* se agregan capas de seguridad por las que deberá pasar el usuario para poder tener acceso a la red.

2.2.1 Implementación del servidor de autenticación como primer punto de *hardening*

Para implementar el servidor de autenticación se siguieron los siguientes pasos:

1.- Instalación del sistema operativo (Kali Linux) en la tarjeta de desarrollo Raspberry Pi3

2.- Instalación del servidor de autenticación (freeRADIUS)

3.- Configuración del servidor de autenticación (freeRADIUS)

4.- Configuración del AP de acuerdo con freeRADIUS

Estos pasos se describen en los siguientes párrafos.

Debido a que se desea migrar la autenticación *enterprise* a un entorno SOHO, el servidor de autenticación no tiene que ser implementado en una PC independiente o tener un servidor de un valor mayor, es por ello que se propuso implementarlo en una tarjeta de desarrollo Raspberry Pi3, cuyo valor aproximado es de $1500 MN con todos los elementos que se utilizaron para poder manipularla, estos son: teclado, mouse, fuente de corriente y una memoria micro SD de 32 GB.

La tarjeta de desarrollo Raspberry PI3 cuenta con un CPU BCM2837 ARMv8 de 64 bits, 1 GB de memoria RAM y compatibilidad con los estándares 802.11 b/g/n. Algunas otras características generales de esta tarjeta se indican en la figura 2.3.

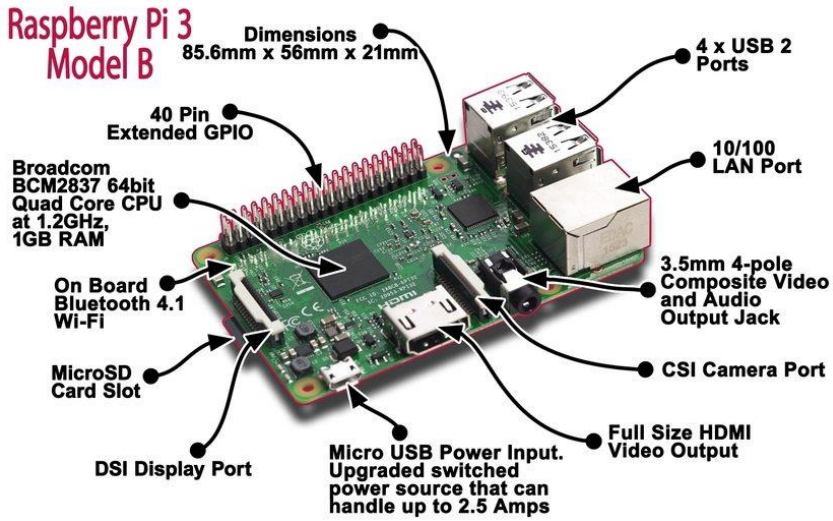


Figura 2.3. Características generales de la Raspberry Pi 3 (figura tomada [32].

La implementación del servidor es posible en la tarjeta Raspberry Pi ya que ésta funciona como un ordenador autónomo capaz de ejecutar algunas versiones Linux, como por ejemplo Raspbian, Ubuntu mate, Kali Linux, entre otras distribuciones.

2.2.1.1 Instalación del sistema operativo Kali Linux en la Raspberry Pi 3

Para implementar freeRADIUS en la tarjeta Raspberry Pi 3, lo primero que se hizo fue instalar el sistema operativo, en este caso se eligió Kali Linux para arquitectura ARM debido a que la presente tesis se inició a trabajar con esta distribución. En la figura 2.4 se muestra la pantalla principal de Kali Linux en la Raspberry Pi 3.

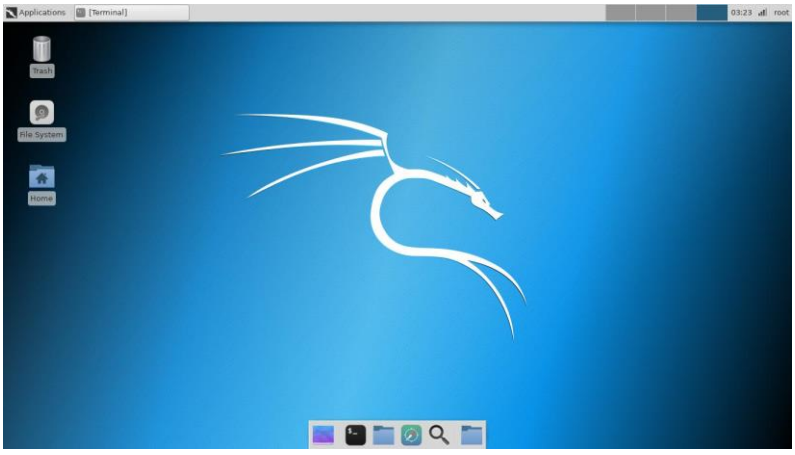


Figura 2.4. Escritorio de Kali Linux en Raspberry Pi3 (diagrama propio).

Una vez que el sistema operativo ha sido instalado éste debe ser actualizado mediante los siguientes comandos: *apt-get update* y *apt-get upgrade*

Para el buen funcionamiento de la distribución Kali Linux fue necesario agregar la dirección de los repositorios faltantes para poder acceder a las bibliotecas, actualizaciones y paquetes, estos repositorios se encuentran en la página oficial de Kali Linux. En el anexo B se indican las bibliotecas que fueron agregadas.

Debido a los cambios realizados en la distribución debe actualizarse nuevamente el sistema operativo. Una vez hecho todo lo anterior se llevó a cabo la instalación del servidor de autenticación como se indica a continuación.

2.2.1.2 Instalación del servidor de autenticación (freeRADIUS)

Para la instalación de freeRADIUS, se utilizó la versión 3.0.15. Antes de la instalación de freeRADIUS, se instalaron los paquetes y las dependencias[8] necesarias, por ejemplo: "dependencias duras" como lo es la dependencia libtalloc. Talloc es un asignador de memoria jerárquico, que necesita freeRADIUS para su instalación. El paquete dpkg-dev instala las herramientas necesarias para desempaquetar y crear los paquetes debs, así mismo incluye la herramienta `autoconfig` y la biblioteca `make` además de construir y cargar los paquetes debían.

Por otro lado, la instalación de OpenSSL es necesaria para poder utilizar la autenticación EAP con el servidor, ya que OpenSSL incluye todas las bibliotecas y archivos de cabecera, como libssl y libssl-dev, si no se tienen instaladas tanto las bibliotecas como los archivos de cabezera necesarios, muchos tipos de EAP no funcionan, de igual manera el paquete `build-dep` es utilizado para instalar todas las bibliotecas y dependencias del paquete fuente de freeRADIUS, Fakeroot. Éste permite construir paquetes en formato deb.

Otro paquete que es importante instalar es el paquete ssl-cert si no se instala causa problemas con los módulos de EAP al iniciar sesión en freeRADIUS, por dicho motivo este paquete debe ser instalado.

[8] Una dependencia es un paquete o paquetes necesarios para que otro paquete pueda instalarse y ejecutarse.

Para que el servidor de autenticación pueda proporcionar la autenticación que se desea, éste debe comunicarse con un cliente por lo que no es suficiente con realizar solamente la instalación de dicho servidor, sino que es necesaria la configuración de sus archivos.

2.2.1.3 Configuración del servidor de autenticación freeRADIUS

Las precondiciones necesarias para configurar el servidor de autenticación son: tener instalado el servidor de autenticación y verificar su funcionamiento. Posteriormente, se inicia el servidor en modo depuración utilizando el siguiente comando:

`#radiusd-X`.

Al ejecutar esta instrucción sobre la línea de comando de la terminal de Kali Linux, el servidor de autenticación responde enviando un mensaje a la salida estándar que es el monitor con el mensaje **ready to process requests,** lo que indica que el servidor fue instalado y configurado exitosamente como muestra la figura 2.5.

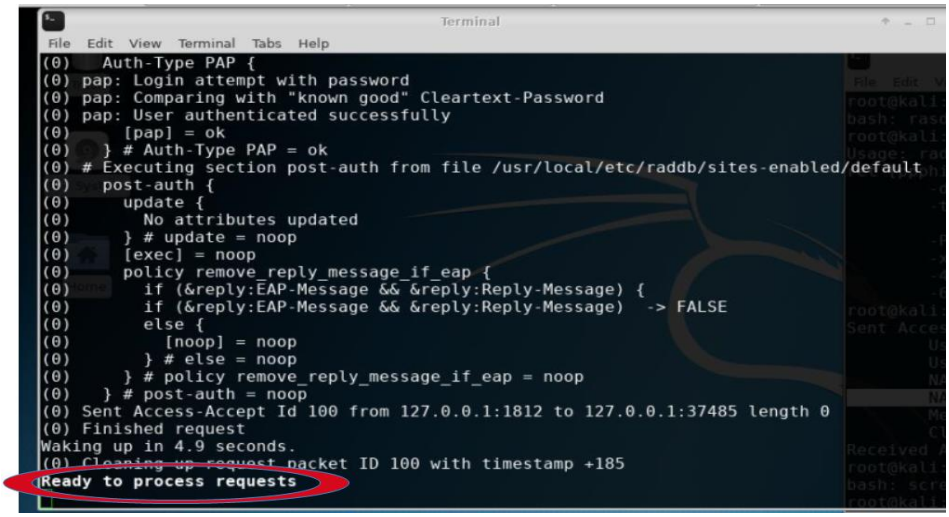


Figura 2.5. Respuesta del servidor freeRADIUS en modo depuración (diagrama propio).

FreeRADIUS posee un archivo de configuración muy grande, por lo que se dividió en varios archivos pequeños los cuales deben ser configurados cuidadosamente, cada archivo cuenta con información adicional para una configuración más sencilla. Estos archivos se encuentran en /usr/local/etc/raddb los archivos que se modificaron fueron: archivo *clients* y el archivo *users.*

Una vez que el servidor está trabajando en modo de depuración se realiza una prueba de autenticación. Para realizar esto, se tiene que agregar un usuario en el archivo *users* el cual se encuentra en la dirección /usr/local/etc/raddb/, en este archivo se agrega el siguiente texto:

```
testingCleartext-password := “hola”
```

Cabe mencionar que cada vez que se configure algún archivo del servidor de autenticación, éste debe reiniciarse y ponerse en modo depuración nuevamente. Una vez hecho esto, se ejecuta el comando *radtets* desde otra terminal, el comando *radtest* se ejecuta de la siguiente manera:

```
root@kali:~# radtest testing hola 127.0.0.1 0 testing123
```

`Radtest` provee una forma simple y conveniente para enviar requerimientos a un servidor RADIUS y analizar las respuestas a estos requerimientos, por otro lado, confirma la comunicación existente entre el servidor de autenticación y el cliente.

Al ejecutar el comando *rasdtest* el servidor debe responder con un **Access-Accept**, como se muestra en la figura 2.6. Esta respuesta indica que el servidor de autenticación está funcionando correctamente. El siguiente paso es agregar un cliente, es importante aclarar que los clientes no son las estaciones, es decir, no son laptops, smartphones, tabletas, etc. ya que éstas no interactúan directamente con el servidor de autenticación, en este caso el cliente es el AP.

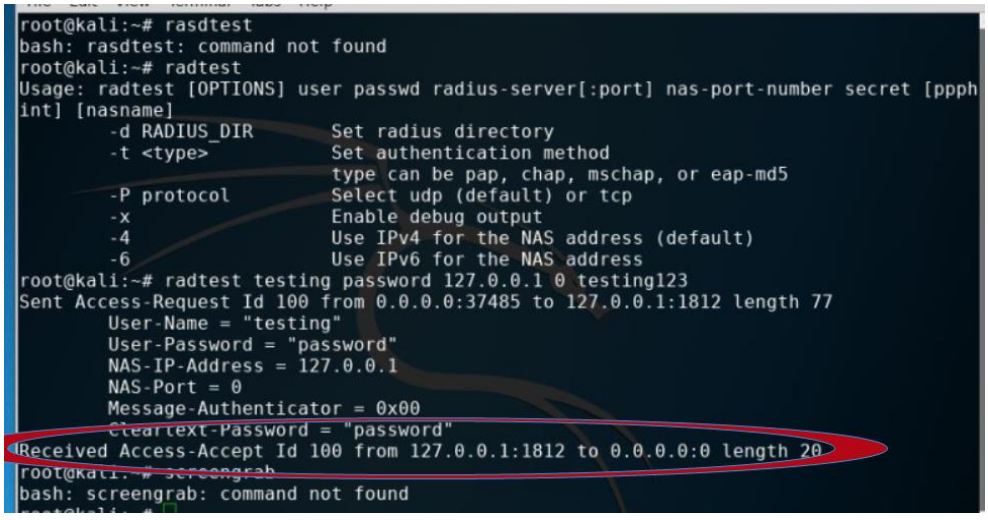


Figura 2.6. Respuesta del servidor de autenticación (diagrama propio).

2.2.1.3.1 Configuración de los archivos clientes y usuarios.

Para llevar a cabo la comunicación que existe entre el cliente y freeRADIUS, se realizó la adición de un cliente en el servidor de autenticación dentro del archivo clients.conf. Este archivo se encuentra en la dirección: /usr/local/etc/raddb/clients.conf. Se debe ingresar la dirección IP del AP, la contraseña que compartirán tanto el servidor de autenticación como el AP, el nombre que se le dará a la red, el tipo de conexión y el SSID. En la figura 2.7 puede apreciarse la configuración del cliente.

Figura 2.7. Adición de cliente (diagrama propio).

Otro archivo que se configuró fue el archivo *users,* éste debe contener todos aquellos usuarios que podrán autenticarse para tener acceso a la red, cada usuario tendrá una contraseña como se muestra a continuación:

Lily Cleartext-Password := "lily01"

Lety Cleartext-Password := "123456"

Atenea Cleartext-Password := "testing"

Hasta aquí los archivos que se tienen que configurar en freeRADIUS. En la siguiente sección se muestra la configuración que se tiene que realizar en el AP para que se pueda llevar a cabo la comunicación entre éste y el servidor de autenticación freeRADIUS.

2.2.1.4 Configuración del AP de acuerdo a freeRADIUS

El cliente también se debe configurar para que pueda interactuar con el servidor de autenticación freeRADIUS, este debe contener la dirección IP del servidor RADIUS, el puerto que utiliza freeRADIUS (1812 UDP) para establecer sus conexiones de autenticación, así como la misma clave secreta que se haya configurado en el servidor dentro del archivo *clients.conf*. Cabe mencionar que se usaron tres AP de tal modo que dos son de un ISP (Arcadian

VRV9529AWAC24 y Alcatel) y el otro es de otro fabricante (Linksys 38378), con el fin de comprobar si era posible implementar el servidor de autenticación en los AP que ofrece un ISP, o si es necesario adquirir un AP con las características que posibiliten la implementación de dicho servidor. Así mismos tanto en esta sección como en la sección de resultados solo se mostrará la configuración de un AP, (siendo éste el que actualmente está operando en la WLAN del escenario de pruebas), la configuración que se realizó en los otros dos AP se documenta en el anexo C.

En la figura 2.8 se aprecia la configuración del archivo *clients.conf* en RADIUS y en el AP, donde puede notarse que el servidor de autenticación tiene tanto el nombre como la contraseña que posee el cliente para que pueda existir la comunicación entre ellos.

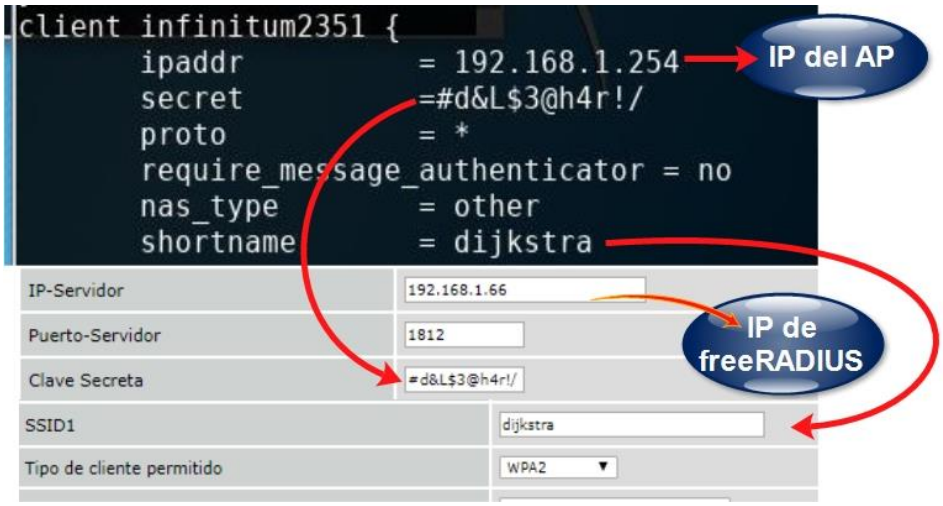


Figura 2.8. Configuración del cliente (diagrama propio).

Una vez que está configurado el servidor de autenticación éste estará en la topología de la WLAN como se muestra en la figura 2.2.

2.3 Configuración del AP de acuerdo a otros pasos de *hardening*

Para robustecer aún más la seguridad fue necesario configurar el AP de manera interna para implementar los siguientes pasos:

1.- Desactivación del WPS

2.- Creación de contraseñas robustas

3.- Desactivación de la difusión del SSID

4.- Desactivación de la configuración remota

5.- Activación del filtrado MAC

6.- Gestión del AP

7.- Minimización de la potencia

8.- Actualización del firmware

Dichos pasos se describen a detalle a continuación.

2.3.1 Desactivación del WPS

Dentro del AP se tiene que deshabilitar la configuración WPS, esta actividad se puede realizar dentro de la sección de configuración inalámbrica como se muestra en la figura 2.9 para evitar un posible ataque.

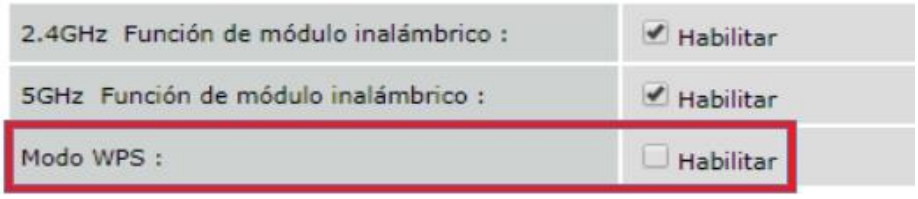


Figura 2.9. Desactivación del WPS (diagrama propio).

2.3.2 Creación de contraseñas robustas

Se crearon contraseñas robustas tanto en el servidor de autenticación como en el AP para hacer la labor más difícil al atacante, la creación de dichas contraseñas se menciona en el capítulo 1 de este trabajo. En la figura 2.10 del lado izquierdo se muestra la configuración de los usuarios que podrán tener acceso a la red y puede notarse que las contraseñas tienen cierto grado de dificultad, en el lado derecho de la figura se muestra la configuración del AP que interactuará con el servidor.

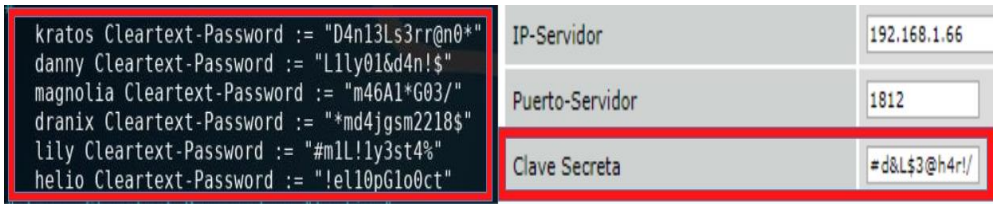


Figura 2.10. Creación de contraseñas seguras (diagrama propio).

2.3.3 Desactivación de la difusión del SSID

La desactivación del SSID es importante para que el nombre de la red no pueda ser vista tan fácilmente, motivo por el cual se desactivó dicha difusión como puede verse en la figura 2.11.

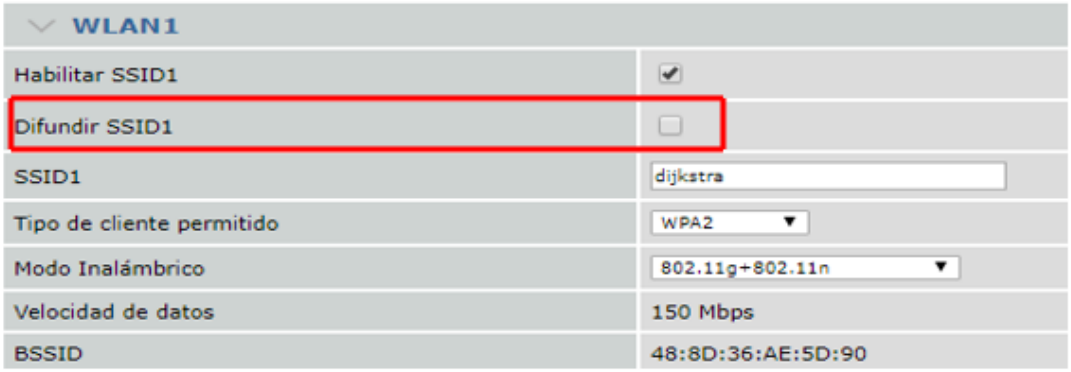


Figura 2.11. Desactivación del SSID de la red (diagrama propio).

2.3.4 Desactivación de la configuración remota

En caso de que un usuario malicioso pueda acceder a la red éste podría tener acceso al AP y si la configuración remota está activada la red puede verse comprometida, debido a que el atacante podría hacer las configuraciones adecuadas para su beneficio. Para evitar esto es forzoso desactivar esta característica, cabe mencionar que esta configuración no se puede realizar en todos los AP como en el caso de los AP Arcadyan VRV9529AWAC24 de TELMEX.

2.3.5 Activación del filtrado MAC

El filtrado MAC permite la conexión solamente a aquellos dispositivos que estén dados de alta en la lista de direcciones MAC y evita el acceso a la red a usuarios no deseados, o bien puede usarse este filtrado en forma de lista negra ingresando las direcciones MAC de los dispositivos que no deben tener acceso a la WLAN, esta opción no se recomienda ya que las direcciones MAC de los atacantes se desconocen motivo por el cual no se podría evitar que entren a la red. En la figura 2.12 se muestra el filtrado de las direcciones MAC con acceso a la WLAN en el escenario de pruebas.

Figura 2.12. Filtrado MAC. (diagrama propio).

2.3.6 Gestión del AP

Es de vital importancia el cambio de contraseña que viene por default en el AP, ya que si un intruso tiene acceso a la red este podría tener acceso a la configuración del AP, (siempre y cuando cuente con el modelo y la contraseña de dicho AP), por ejemplo, la contraseña por default para los AP Arcadyan VRV9529AWAC24 de TELMEX es (*7mFbWKKHFs)* y se ha cambiado por otra como se muestra en la figura 2.13.

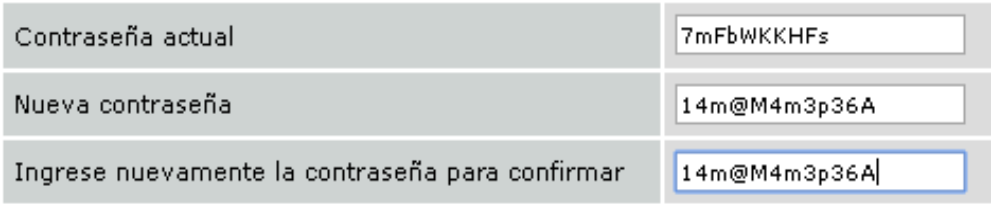


Figura 2.13. Cambio de contraseña para gestión del AP (diagrama propio).

2.3.7 Minimización de la potencia

La minimización de la potencia es una buena actividad para evitar que la red inalámbrica no cubra más allá del área deseada, ya que para que un ataque tenga éxito necesita alcanzar una potencia aproximadamente de -60 dBm. Existen AP que cuentan con potencia baja, media, alta y máxima, y otros que solo tienen baja, media y alta. El AP que se configuró cuenta con estos

tres niveles y se configuró en baja como se muestra en la figura 2.14, la cual cubre perfectamente el área deseada.

Figura 2.14. Minimización de la potencia (diagrama propio).

2.3.8 Actualización del firmware

Esta actualización es importante para que se actualicen los parches de seguridad cabe mencionar que en algunos AP se necesita bajar el firmware y actualizarlo manualmente como en el caso de los ARCADYAN VRV9529AWAC24 de TELMEX, mientras que en otros la actualización es automática. En la figura 2.15 se muestra que la actualización del firmware del AP ARCADYAN VRV9529AWAC24 debe realizarse manualmente.

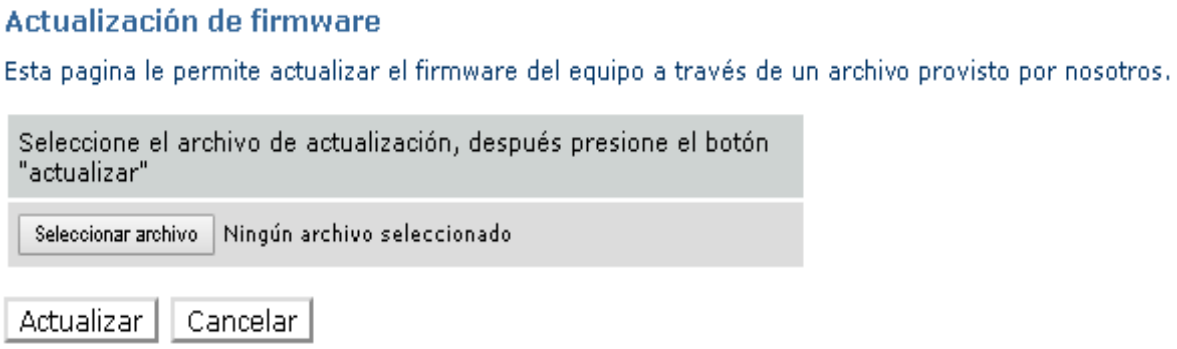


Figura 2.15. Actualización del firmware en el AP (diagrama propio).

Una vez que la red inalámbrica se ha robustecido mediante la implementación de *hardening*, se evalúa la seguridad de dicha red mediante una revisión.

La revisión de la seguridad de WLAN se lleva a cabo en dos partes, tal que la primera parte consta en la realización de una revisión previa al robustecimiento, es decir, antes de la implementación de *hardening* y una segunda revisión después del robustecimiento, con el fin de hacer una comparativa.

Para realizar la revisión de seguridad se utilizó Kali Linux, primero se puso la tarjeta inalámbrica en modo monitor. El siguiente paso fue realizar un escaneo para detectar el tráfico inalámbrico

y poder ver las redes aledañas, el nombre de la red, la intensidad de la señal del AP, las estaciones que están conectadas, así como ver el tipo de autenticación que se está usando. Por otro lado, se probó la eficiencia del robustecimiento de la WLAN. Esta revisión de seguridad se detalla en el siguiente capítulo.

CAPÍTULO III

"Ser capaz de superar la seguridad no te convierte en un hacker, de la misma forma que hacer un puente a un coche no te convierte en un ingeniero mecánico"

Eric S. Raymond

Capítulo 3 Resultados y conclusiones

En el presente capítulo se describen los resultados obtenidos al realizar el análisis de vulnerabilidades que pueden presentar las WLAN. Así mismo, incluye los resultados que se obtuvieron al implementar *hardening* en una WLAN.

En la primera parte se documentan los resultados de ataques a los protocolos WEP, WPA Y WPA2 con las herramientas Fern wifi crack, wifiphisher y la Suite AIR. En la segunda parte se documentan los resultados obtenidos de la implementación de *hardening* en el AP Arcadian VRV9529AWAC24.

3 Resultados de los ataques a redes inalámbricas para detectar vulnerabilidades e implementar hardening

Se realizaron cinco ataques con la misma herrmienta tanto al escenario de pruebas como a las redes que se encontraron en el medio, con el propósito de estimar un tiempo promedio de respuesta de las herramientas para romper la seguridad, donde los primeros ataques se iniciaron en una WLAN con autenticación WEP, posteriormente se atacaron los protocolos WPA y WPA2.

3.1 Resultados de los ataques a una WLAN con seguridad WEP

Con la herramienta Fern wifi crack, se realizó un escaneo para localizar las redes cercanas y se seleccionó la red que se deseaba atacar, los cinco ataques convergieron entre 1.07 y 1.39 min. Finalmente se obtuvo un tiempo promedio de 1.08 min. En la figura 3.0 se muestra el gráfico de los cinco ataques que se realizaron a la WLAN con autenticación WEP.

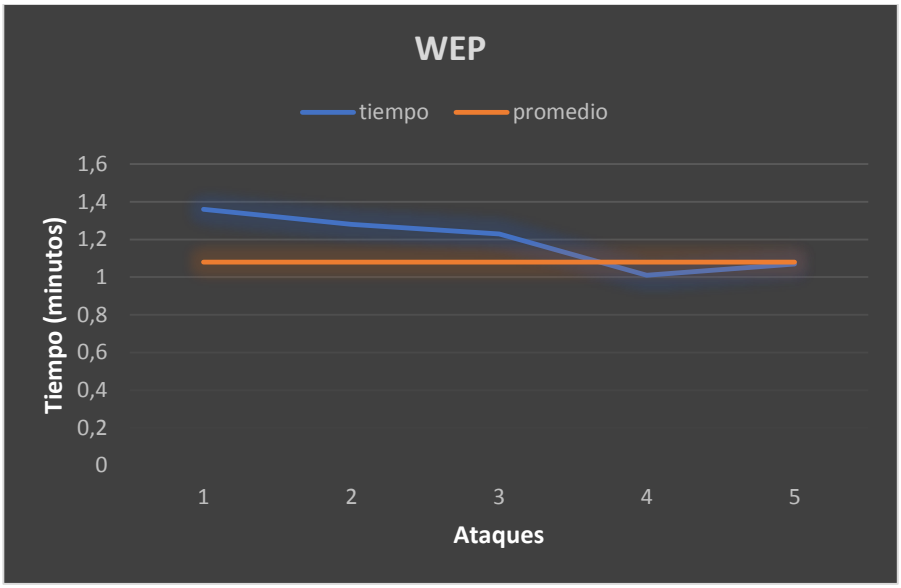


Figura 3.0. Ataques a una WLAN con seguridad WEP (diagrama propio).

En la figura 3.1 se muestra la obtención de la clave WEP en un tiempo promedio de 1.08min.

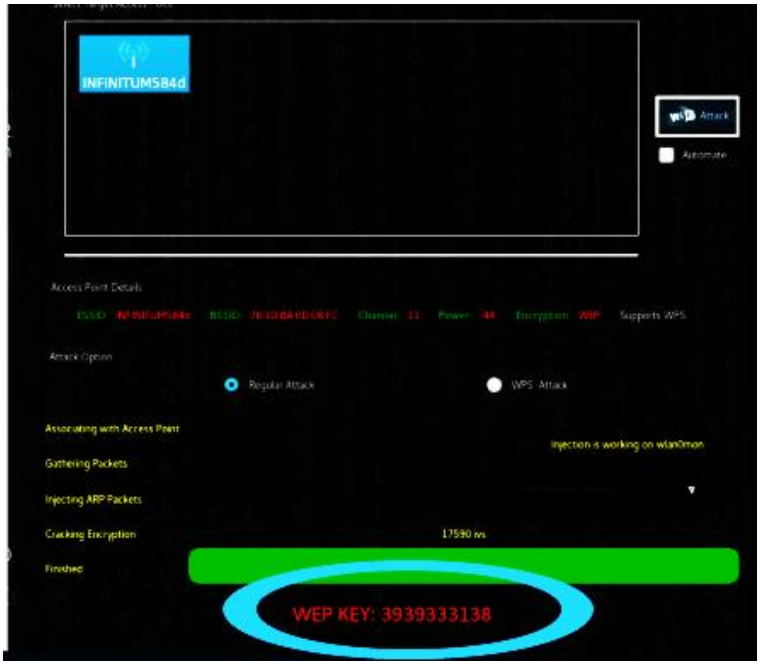


Figura 3.1. Obtención de contraseña con la herramienta Fern WIFI Cracker (diagrama propio).

3.1.1 Resultados del ataque a WEP con las herramientas de la Suite AIR

La primera red que se atacó con las herramientas de la Suite AIR fue al escenario de pruebas con seguridad WEP, los dispositivos que jugaron el papel de víctima fueron una laptop y un teléfono celular. Cabe mencionar que el ataque a un dispositivo móvil requiere más tiempo para llevarse a cabo, ya que tardó aproximadamente alrededor de 16 min con 25 seg, en cambio los 5 ataques que se efectuaron a la WLAN víctima en la cual estaba autenticado un usuario con una laptop fue menor, estos tardaron en promedio 7 min con 9 seg. En la figura 3.2 se muestra la obtención de la contraseña de dicho ataque, cabe aclarar que la clave que se obtuvo es la que trae por default el AP. Así mismo, en este ataque no fue necesaria la utilización de un diccionario como en WPA que se describe a continuación.

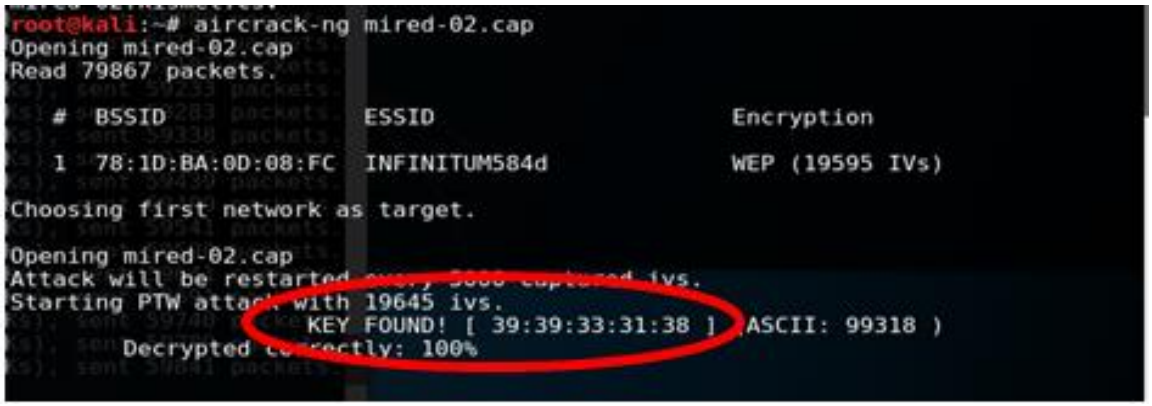


Figura 3.2. Obtención de contraseña con WEP con aircrack-ng (diagrama propio).

En la siguiente sección, se muestran los resultados obtenidos de los ataques a los protocolos WPA y WPA2.

3.1.2 Resultados de los ataques a una WLAN con seguridad WPA/WPA2 personal

En esta sección se presentan los resultados a los ataques WPA personal y WPA2 personal, cabe mencionar que los resultados de WPA2 son muy similares a los de WPA.

Para violar la seguridad de una WLAN con protocolos WPA y WPA2 fue necesario utilizar las herramientas de la Suite AIR, así como una base de datos de posibles contraseñas o mejor

conocido como diccionario, Kali Linux por su parte cuenta con un diccionario para este propósito. Los resultados que se obtuvieron se documentan a continuación.

En un principio se hicieron diferentes intentos de ataques para poder vulnerar una WLAN con seguridad WPA, todos ellos sin éxito. Por este motivo se recurrió a una revisión de diferentes diccionarios que se encuentran en internet. Sin embargo, éstos resultaron ser completamente inútiles ya que sólo son una colección de posibles contraseñas, que no garantizan encontrar la contraseña de la red que se estaba atacando. Entonces fue necesaria la creación de un nuevo diccionario el cual se crea a partir de la información obtenida del entorno de la red (ingeniería social[9]). Este diccionario genera las posibles contraseñas que puede tener la red a partir de la información proporcionada, a diferencia de los diccionarios que se encuentran en la red que contienen contraseñas aleatorias que no tienen nada que ver con la red que se está atacando, (la creación de este diccionario se detalla en el anexo A). En la figura 3.3 se muestra la obtención de la clave de acceso a la red como resultado del ataque a una WLAN con seguridad WPA.

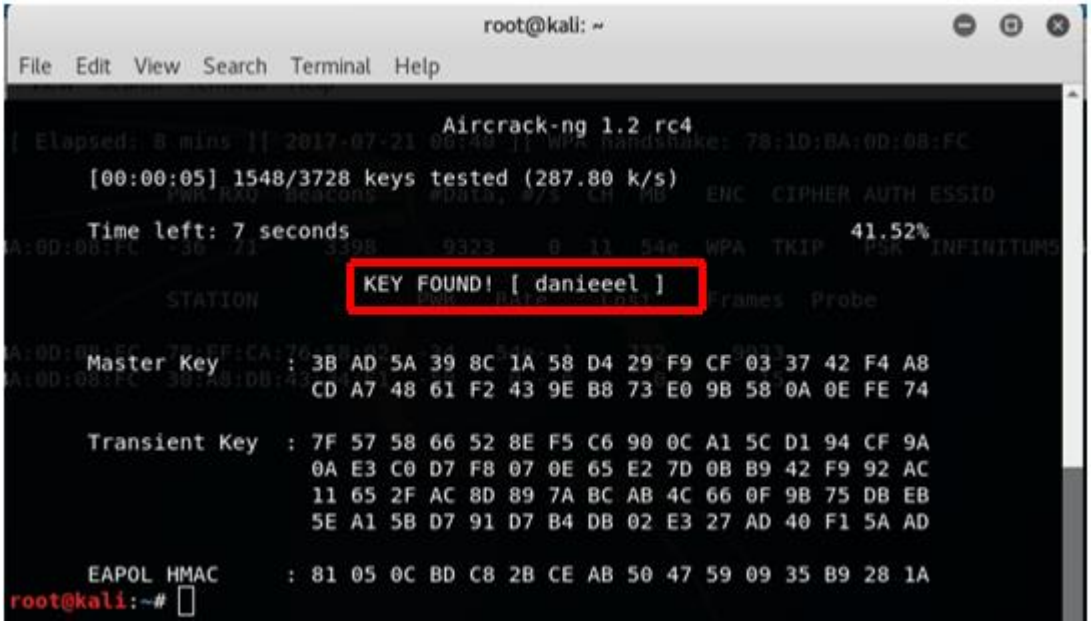


Figura 3.3. Ataque a WPA con las herramientas de la Suite AIR (diagrama propio).

En la figura 3.4 se puede apreciar el tiempo promedio en que converge un ataque es de 7.4 min y el tiempo estimado de convergencia de los 5 ataques realizados. Cabe aclararse que estos tiempos son tomados tanto para WPA como para WPA2, una vez que se tiene el conocimiento

[9] La ingeniería social se refiere a los medios para conseguir que los usuarios revelen información confidencial [18].

de la función de cada una de las herramientas utilizadas para cada ataque así mismo el diccionario ya se tenía creado.

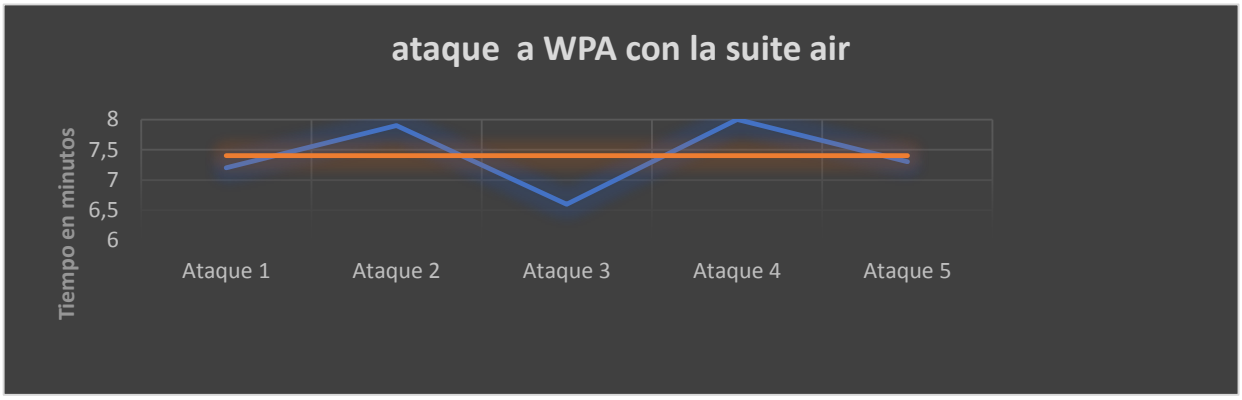


Figura 3.4. Tiempo promedio en que converge cada ataque con la Suite AIR (contraseña débil) (diagrama propio).

En la imagen 3.3 se puede apreciar que en el ataque anterior se obtuvo una contraseña muy sencilla, a pesar de que la WLAN tiene una seguridad basada en el protocolo WPA. Por lo tanto, la contraseña se mejoró con una combinación de números, letras y caracteres especiales. Así mismo se procedió a realizar otro ataque, para verificar la eficiencia tanto de la herramienta como la del diccionario. En la figura 3.5 se ven los resultados de dicho ataque.

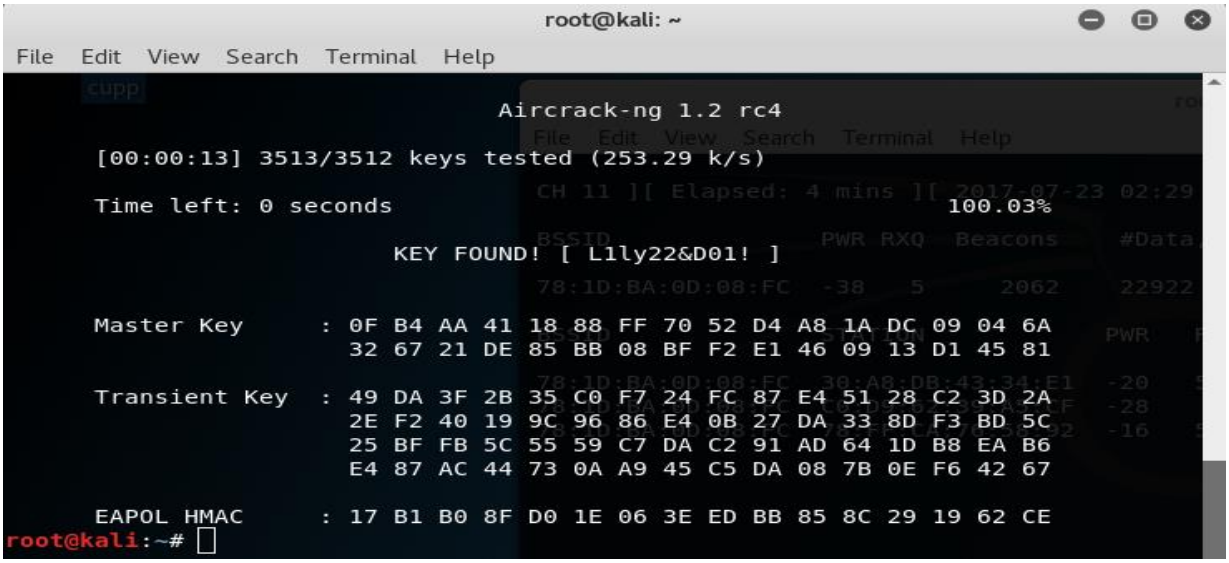


Figura 3.5. Ataque al protocolo WPA con la Suite AIR (diagrama propio).

En la figura 3.6 se aprecia el tiempo en el que se vulneró la red con seguridad WPA, a pesar de tener una contraseña más robusta. El tiempo promedio fue de 7 min 5seg.

Por otro lado, se realizó un ataque más al protocolo WPA con la herramienta Wifiphiser, donde la contraseña fue obtenida mediante engaños. Los resultados de dicho ataque se encuentran en el anexo D.

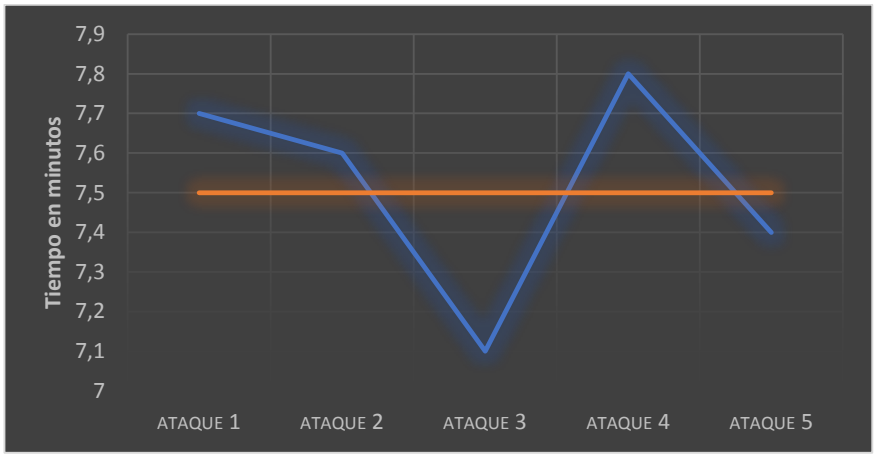


Figura 3.6. Tiempo estimado en que converge cada ataque para una contraseña robusta (diagrama propio).

Con el fin de romper la autenticación WPA2 se realizó un ataque a este protocolo cuyo ataque convergió en un tiempo promedio de 12 min 35 seg. En la figura 3.7 se muestran los resultados de dicho ataque.

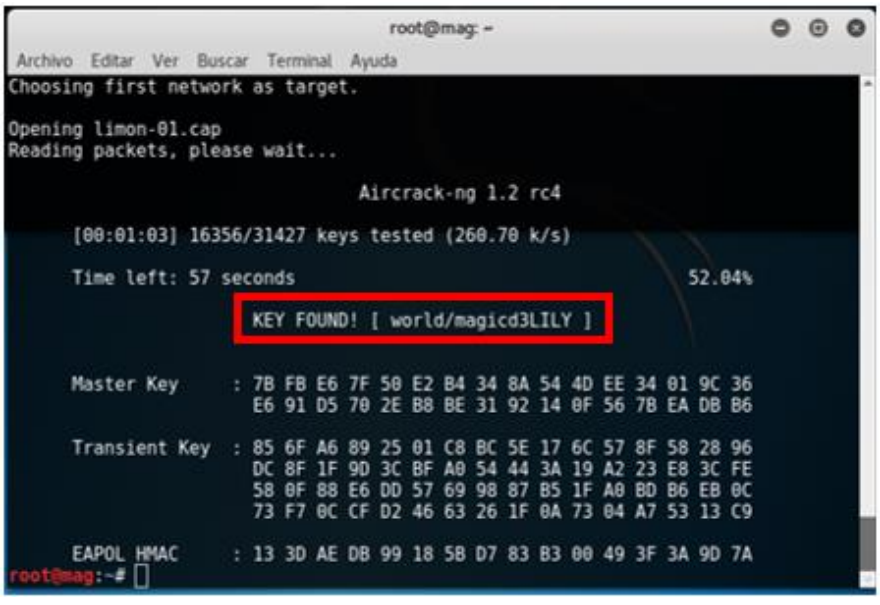


Figura 3.7. Ataque a WPA2 con la suite AIR (diagrama propio).

Con Wireshark se capturaron los paquetes correspondientes al momento de establecerse el saludo *handshake* de cuatro vías, entre la estación y el AP. Cabe mencionarse que esta captura

fue tomada después de haberse realizado la reinyección de paquetes ARP, ya que este ataque obliga al usuario a desautenticarse para forzar una nueva autenticación lo que permite obtener el *handshake*. En la figura 3.8 puede verse el intercambio de mensajes entre el AP, la estación y el protocolo encargado de establecer la autenticación (EAPOL).

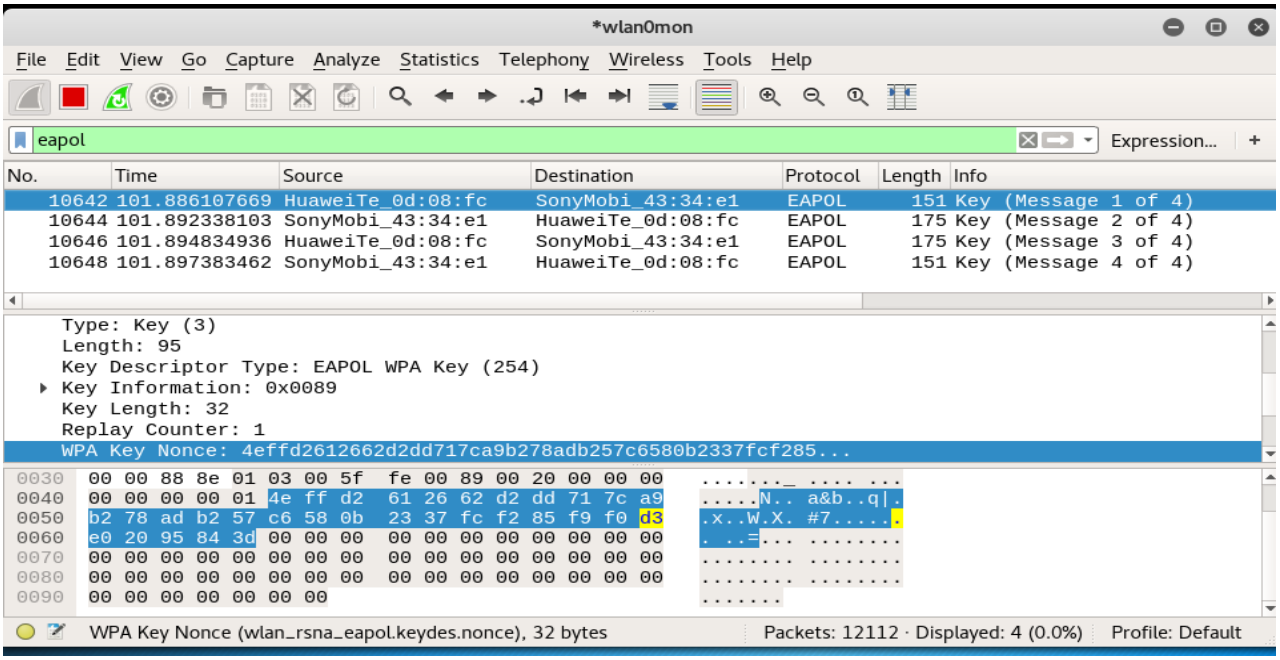


Figura 3.8. Intercambio de paquetes en handshake (diagrama propio).

Debido a que se atacaron los protocolos WEP, WPA y WPA2 con las herramientas de la Suite AIR. En la figura 3.9 se muestra un gráfico con la desviación estándar y el promedio en que dichos ataques convergieron. Así mismo, puede notarse que el tiempo de diferencia en los cinco ataques que se realizaron a cada protocolo es relativamente muy pequeño.

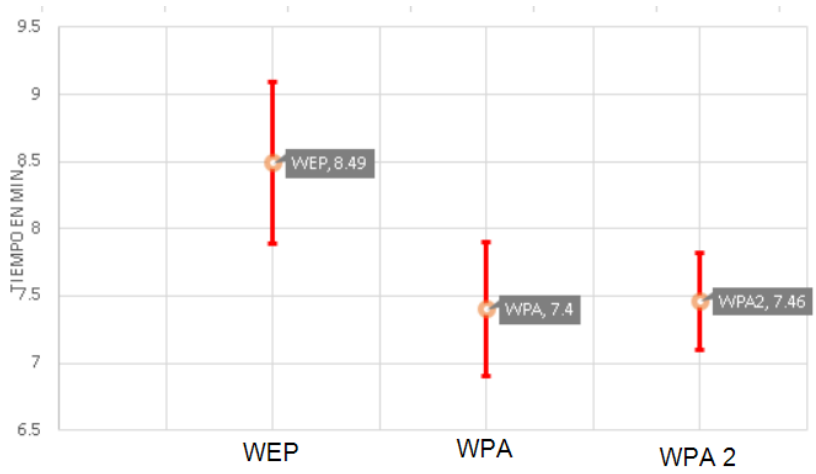


Figura 3.9 Desviación estándar y tiempo promedio en que los ataques convergen con la Suite AIR (diagrama propio).

Cabe mencionar que en el grafico de la figura 3.9 falta incluir el tiempo de la creación de los diccionarios para vulnerar a los protocolos WPA y WPA2, (tiempo que no podría estimarse).

Una vez que se obtuvieron los resultados de la identificación de vulnerabilidades, se procedió a implementar los puntos de *hardening* que se propusieron para robustecer la seguridad en la WLAN, los resultados obtenidos de esta implementación se documentan en la siguiente sección.

En la sección anterior, la seguridad WEP, WPA y WPA2 de tipo personal presentó vulnerabilidades a diferentes ataques con diferentes herramientas, ya que al utilizarse estas herramientas para atacar a los protocolos de seguridad se encontraron ciertos elementos que influyen en que el ataque sea más sencillo, estos son: la emisión del SSID, este y la MAC del AP son unos de los elementos que son requeridos por la herramientas en el proceso de un ataque de desautenticación, la potencia la cual indica si es posible que un ataque converja o no y al estar configurada al máximo como en el ejemplo de figura 3.10, indica que un ataque tiene un mayor éxito, otro elemento que también es primordial es el tipo de cifrado el cual indica a qué tipo de autenticación (modo personal o *enterprise*) se está enfrentando el atacante . En la figura 3.10 se muestran estos elementos.

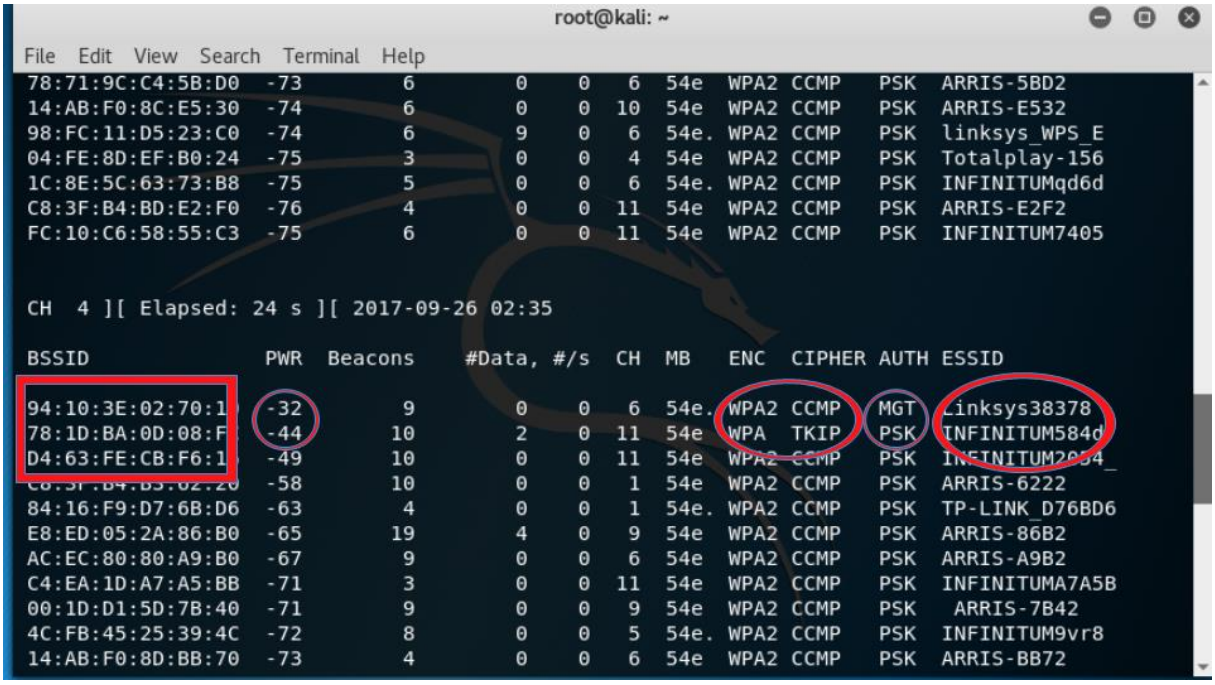


Figura 3.10 Elementos que influyen en un ataque a una WLAN sea más sencillo (diagrama propio).

En el caso de la autenticación WPA/WPA2 *enterprise*, para realizar los ataques se utilizaron las herramientas airmon-ng, hostapd-wep y zcat. Los resultados de este ataque se documentarán después de la implementación del servidor de autenticación y la implementación completa de *hardening*.

3.2 Resultados de la implementación de *hardening* en una WLAN

Después de la implementación de *hardening* se pudieron observar algunos cambios en la seguridad de la WLAN de un entorno SOHO. En los siguientes párrafos se hace un análisis del robustecimiento que se le aportó a la red con cada una de las capas de hardening que se implementaron de acuerdo con la figura 1.15 del capítulo 1.

Se intentó acceder a la red como comúnmente se hace, por ello se actualizó el estado del WIFI de un smartphone y una laptop, para escanear las redes que estos dispositivos alcanzaban a detectar, debido a que la emisión del SSID no existe, en el momento en que los dispositivos hacen un escaneo de redes cercanas, se observó que la red no se da a conocer.

Por otra parte, si un usuario quiere acceder a esta red oculta debe agregarla manualmente. En la figura 3.11 se muestra la agregación de una nueva red en un smartphone.

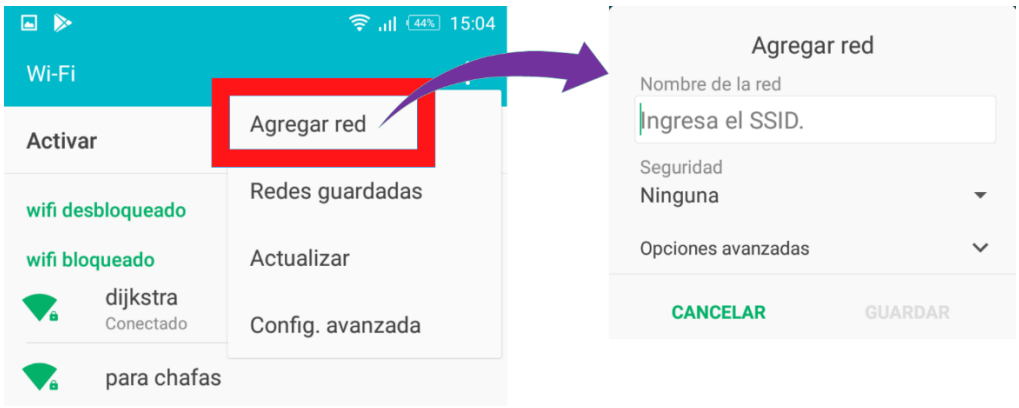


Figura 3.11. Agregación de una nueva red (diagrama propio).

Se ingresan los datos correspondientes al nombre de la red, en este caso "Testhardening". Debido a que la WLAN ahora cuenta con un servidor de autenticación, en la opción de seguridad se eligió la correspondiente a 802.1x, donde se tienen que proporcionar las credenciales necesarias como el nombre de usuario y contraseña, estos datos deben ser los mismos que están alojados dentro del servidor de autenticación. En la figura 3.12 se ejemplifica el intento de autenticación con los datos correspondientes

Figura 3.12. Credenciales para ingresar a la red (diagrama propio).

Por otro lado, cabe mencionar que el servidor de autenticación freeRADIUS se pudo instalar en el AP Arcadyan VRV9529AWAC24 de un ISP sin necesidad de comprar otro AP que sea compatible con el servidor. En la figura 3.13 se muestra la implementación de dicho servidor en el escenario de pruebas.

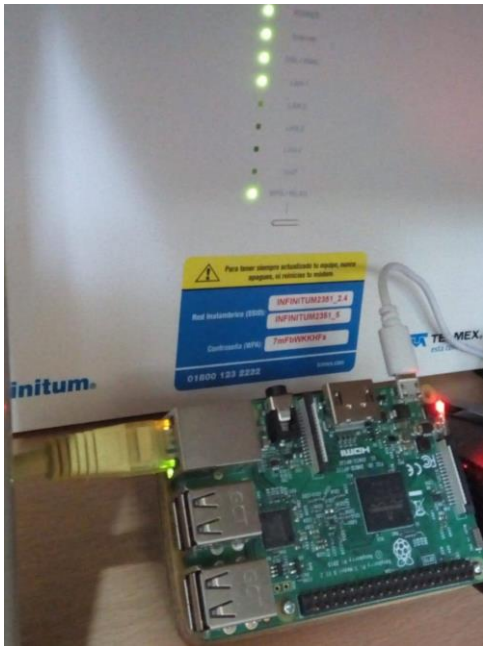


Figura 3.13. Servidor de autenticación en entorno SOHO (diagrama propio).

Una vez que se autentica el usuario, el servidor de autenticación le permitirá el acceso a la red. Así mismo cuando las credenciales se verifican dentro del servidor de autenticación, éste autenticará de manera legítima al usuario y le concederá el acceso a dicha red, cuando esto es correcto el servidor de autenticación mostrará en la pantalla de salida un mensaje de aceptación como se muestra en la figura 3.14.

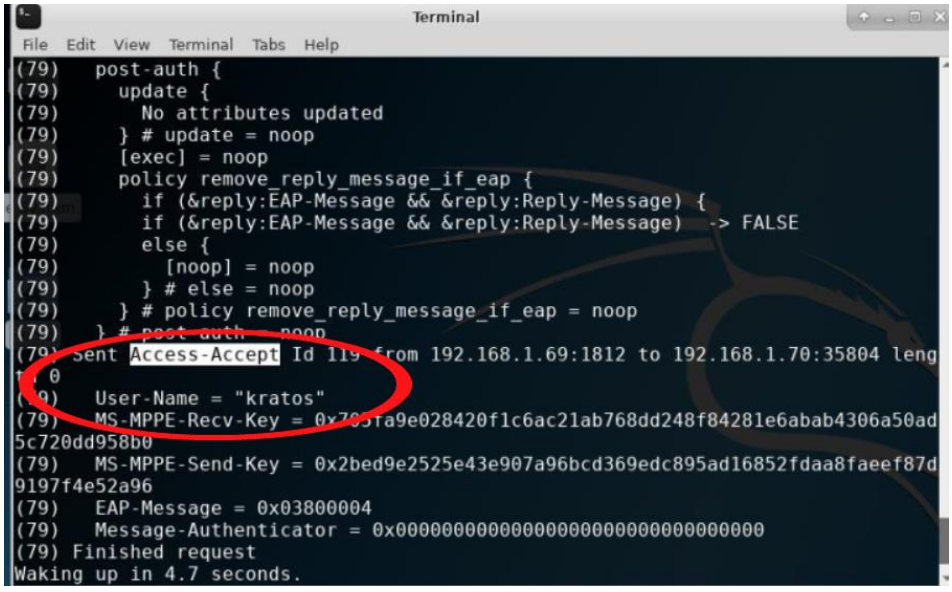


Figura 3.14. Respuesta del servidor de autenticación al aceptar un usuario (diagrama propio).

Por otro lado, si un usuario quisiera intentar acceder a la red con las credenciales incorrectas el servidor de autenticación le negará el acceso y éste mostrará un mensaje de denegación como se indica en la línea 17 de la figura 3.15.

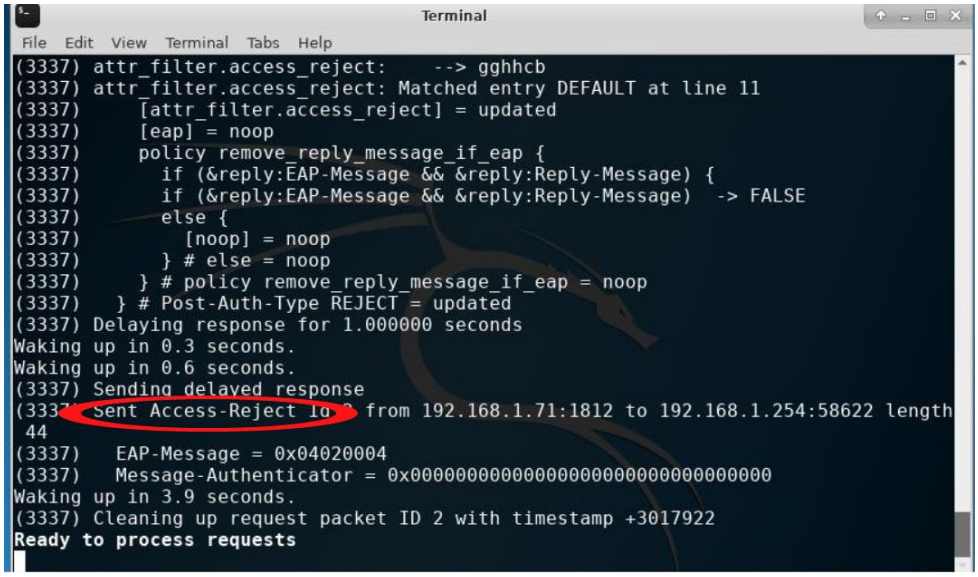


Figura 3.15. Denegación de acceso a la red por parte del servidor de autenticación (diagrama propio).

Ahora bien, si un usuario mal intencionado obtiene las credenciales e intenta acceder a la red con estas, el AP le negará el acceso debido a que existe un filtrado MAC y el servidor de autenticación mostrará un mensaje similar al que se muestra en la línea 15 de la figura 3.16.

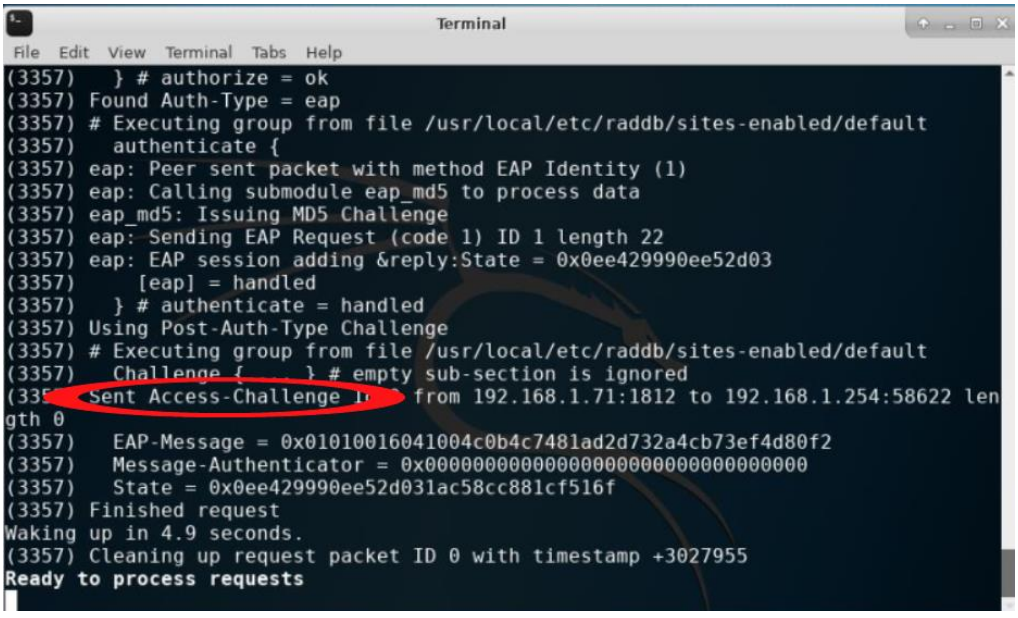


Figura 3.16. Acceso denegado a la red por parte del servidor de autenticación (diagrama propio).

Así mismo, el usuario observará algo similar a lo que se muestra en la figura 3.17, donde su dispositivo se quedará intentando acceder a la red.

Figura 3.17. Intento de autenticación desde un dispositivo móvil diagrama propio.

Por otra parte, se realizó un nuevo ataque para verificar la eficiencia de la implementación de *hardening* en la WLAN. El ataque se hizo a una distancia de 35 m, donde había 3 obstáculos (muros) para simular la distancia en la que podría encontrase un atacante. La intensidad de la señal se comportó de manera inestable hasta llegar al punto en que la calidad de enlace no fue suficiente debido que el dispositivo ya no pudo ver la red. En la figura 3.18 se nota que la potencia es muy baja lo que indica que un ataque no podría concretarse.

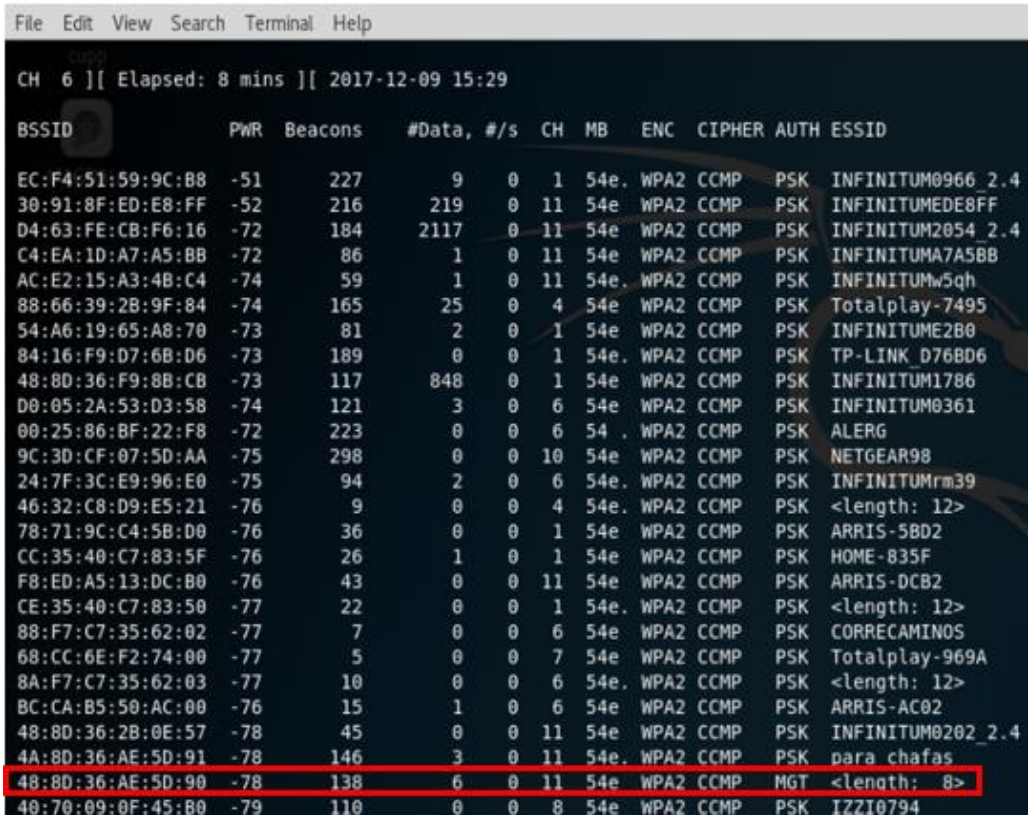


Figura 3.18. Potencia de la señal de la red víctima diagrama propio.

A pesar de que se robusteció la red ésta no es segura al 100%. A continuación, se describen algunos escenarios de ataques posibles, y cómo esta implementación de *hardening* ayuda en algunos casos.

3.3 Posibles escenarios en un ataque

Red encontrada: esto se puede evitar al bajar la potencia del AP y el ocultamiento del SSID, si un usuario malicioso se encuentra muy cerca o dentro del área de cobertura de red no podrá verla, en la figura 3.20 se muestran las capas de seguridad que están protegiendo la red, en caso de que el atacante tenga conocimientos de seguridad y realice un escaneo con alguna herramienta para auditorías de seguridad y logre ver la red, el atacante realizará un ataque pasivo para obtener el SSID de la red inalámbrica.

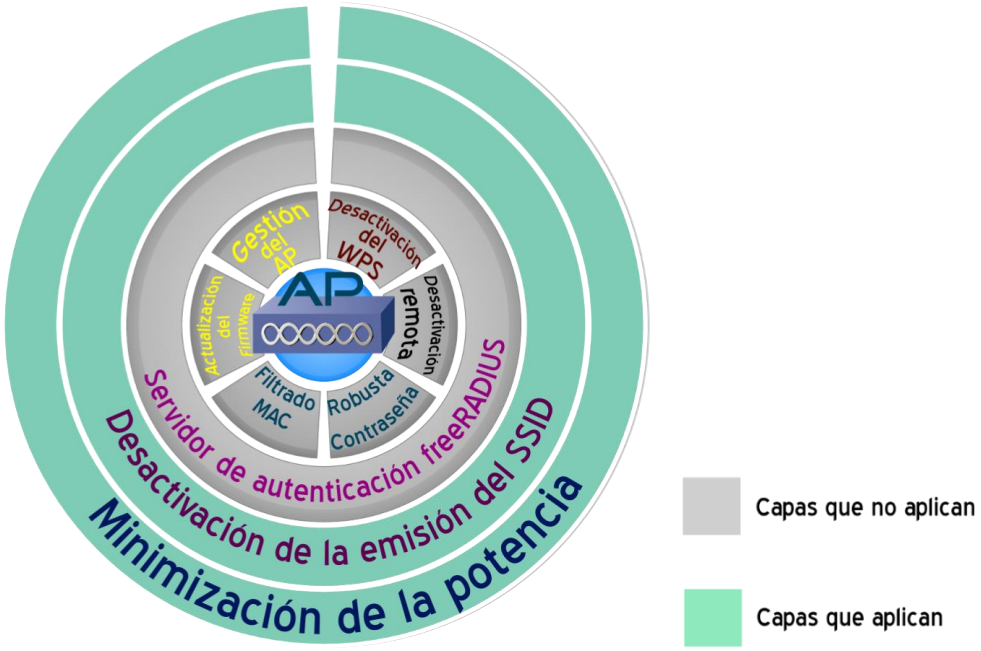


Figura 3.20 Activación de las capas al intentar encontrar la red (diagrama propio)

Obtención del SSID: En caso de que el SSID sea obtenido mediante un ataque a pesar de ser oculto, el atacante se enfrentara a la autenticación mediante el servidor freeRADIUS, al llegar el atacante a este punto se someterá a un proceso de autenticación, donde, el servidor solicitara las credenciales pertinentes (usuario y contraseña) para proporcionar el acceso a dicha red. En la figura 3.21 se muestra la capa de seguridad que está protegiendo la red.

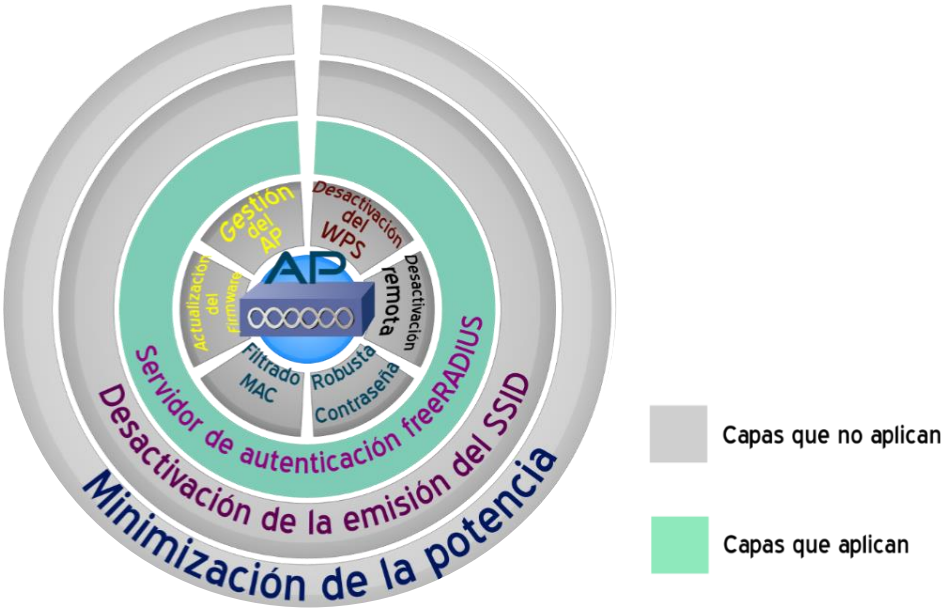


Figura 3.21. Activación de capa RADIUS al intentar acceder a la red (diagrama propio)

Obtención de credenciales del servidor freeRADIUS: en freeRADIUS se hace la configuración de usuarios que podrán tener acceso a la red, donde a cada usuario se le asigna una contraseña, ésta debe ser robusta y no tan fácil de descifrar para que en caso de que esta autenticación se quebrante y las credenciales sean obtenidas por el atacante, al tratar de acceder a la red éste caerá en el filtrado MAC de acuerdo con la figura 3.22.

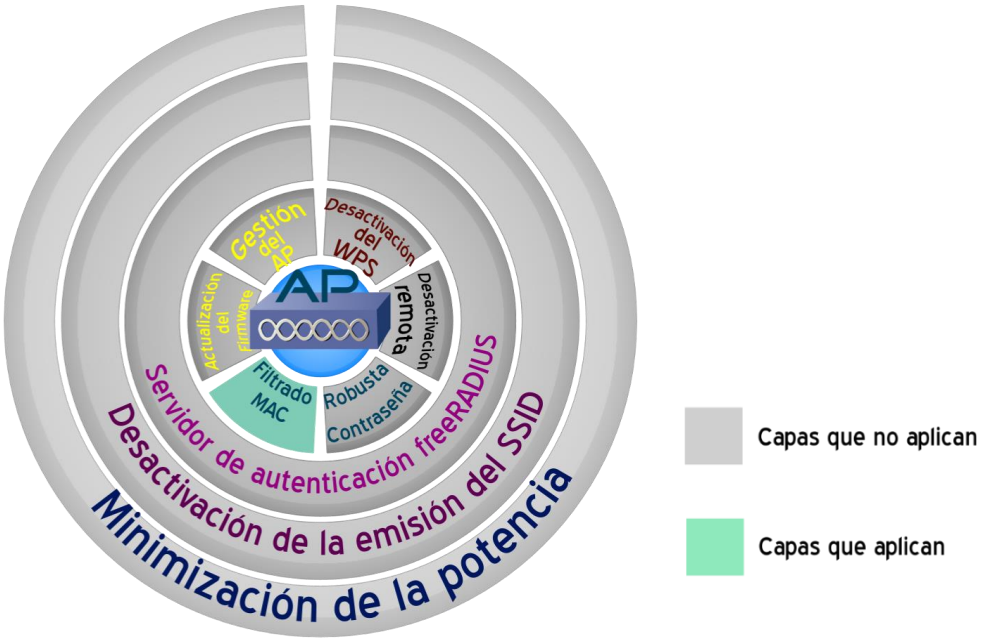


Figura 3.22. Activación de filtrado MAC al intentar encontrar la red (diagrama propio)

Acceso a la red: este escenario es el caso más extremo, ya que el atacante tiene acceso total a la red y podría capturar la información sensible que viaja en la red; sin embargo, llegar hasta aquí es un poco complicado. Por otro lado, si se intenta hacer una denegación de servicio esta no será posible ya que la contraseña para ingresar al AP fue cambiada. En la figura 3.23 se muestra la capa de seguridad que está protegiendo la red.

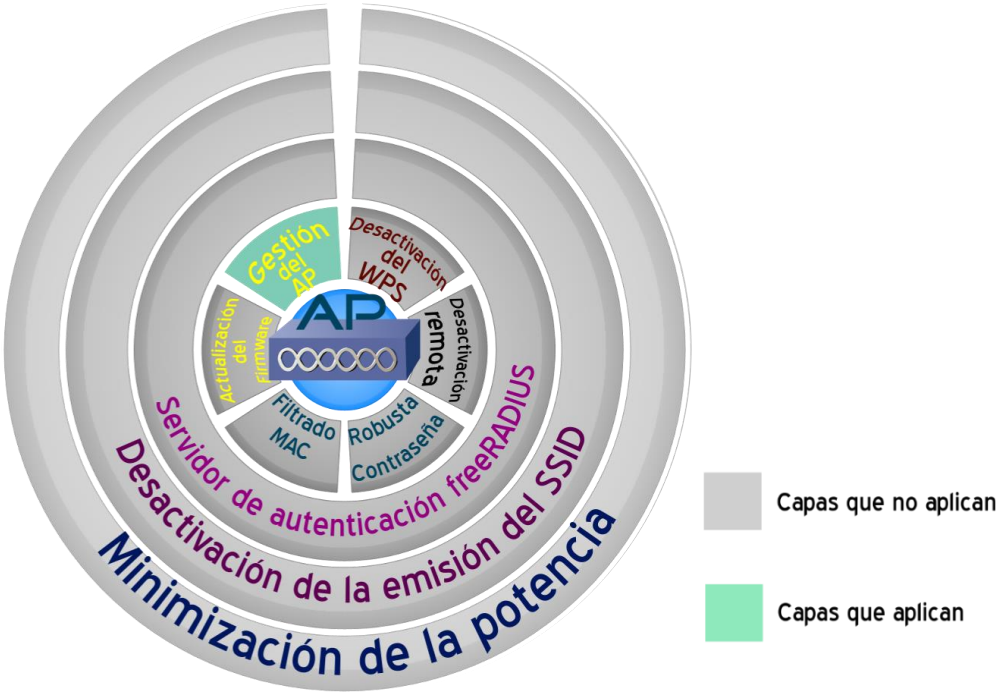


Figura 3.23. Activación de capa que protege a la red (diagrama propio)

Para ilustrar estos posibles escenarios de manera práctica se realizó un ataque más a la WLAN con la implementación de *hardening*, cuyos resultados se documentan a continuación.

3.3.1 Ataque a la WLAN con la implementación de *hardening*

Se realizó un nuevo escaneo de redes para localizar la WLAN que se deseaba atacar, en este caso la emisión del SSID esta desactivado por lo que no se da a conocer el nombre de dicha red, como se muestra en la figura 3.24. Cabe mencionar que el escaneo tardo en promedio 6 min.

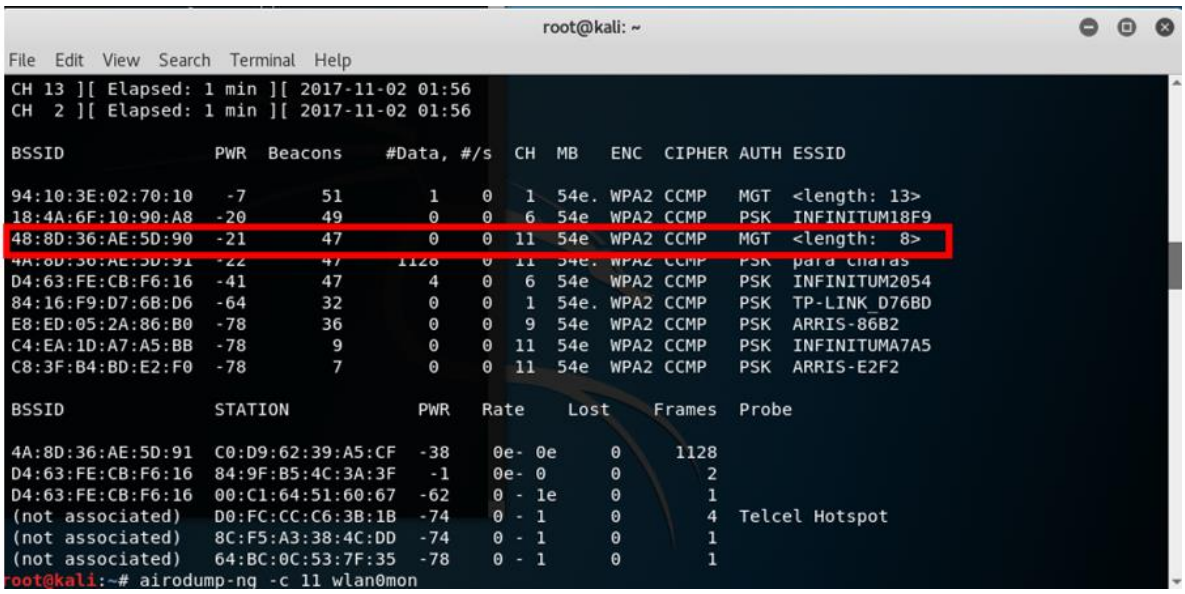


Figura 3.24. Escaneo de redes (diagrama propio).

3.3.1.1 Ataque al ocultamiento del SSID

Como se menciona anteriormente sobre la no emisión el SSID, se realizó un ataque para poder obtenerlo. En la figura 3.25 se muestra el resultado de dicho ataque, en la parte inferior de la imagen se aprecia la inyección de paquetes para desautenticar y autenticar inmediatamente al dispositivo que en ese momento se encontraba en la red, para obtener de esta forma el SSID. Este ataque tardo en un tiempo promedio de 9 min; sin embargo, el ataque podría tardar más tiempo. En la parte superior de la imagen se aprecia el nombre de la WLAN que se obtuvo.

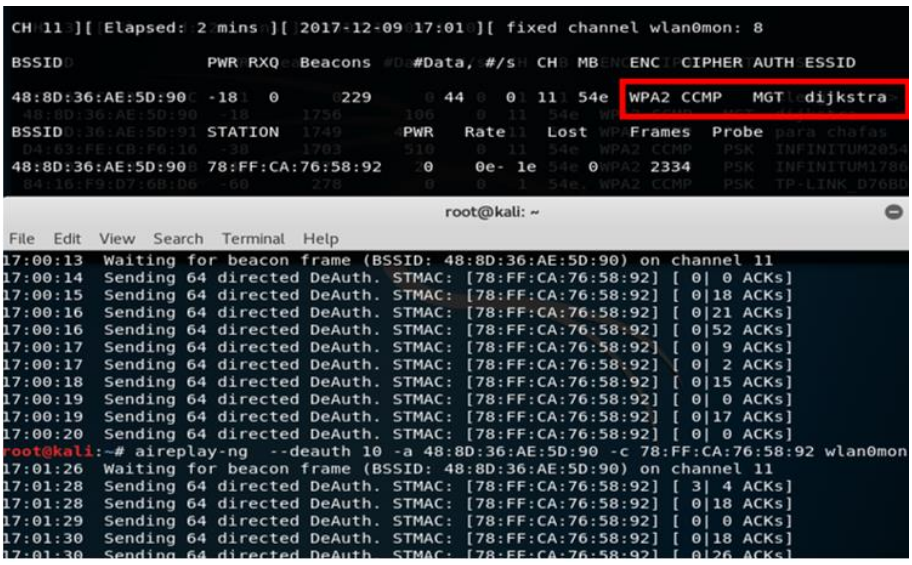


Figura 3.25. Obtención del SSID (diagrama propio).

En la imagen 3.24 también se observa que al realizar un escaneo de redes se obtiene el tipo de cifrado, el cual indica el tipo de autenticación que se está usando, en este caso es autenticación *enterprise*.

3.3.1.2 Ataque a WPA2 *enterprise*

Dado que se trata de una autenticación *enterprise*, fue necesario crear un APF (Access Point False) mediante la herramienta hostapd-wep, para obtener las credenciales encriptadas de los usuarios, dicho ataque tardo en promedio 5 min, tiempo en el cual se generó este mismo. En la figura 3.26 se aprecia la creación del APF y el momento en que este aparece en los dispositivos autenticados a la red.

Figura 3.26. Creación del APF (diagrama propio).

Comparando este ataque con los ataques que se hacen a WPA y WPA2 personal el APF tiene que estar en espera hasta que una víctima se desuatentique y autentique nuevamente a la red, con el fin de obtener el nombre de usuario y la contraseña encriptada, tiempo que no podría estimarse. En este caso para apresurar el proceso se deshabilitó la tarjeta inalámbrica del dispositivo y se volvió a habilitar. En la figura 3.27 se muestra la obtención de las credenciales de autenticación encriptadas.

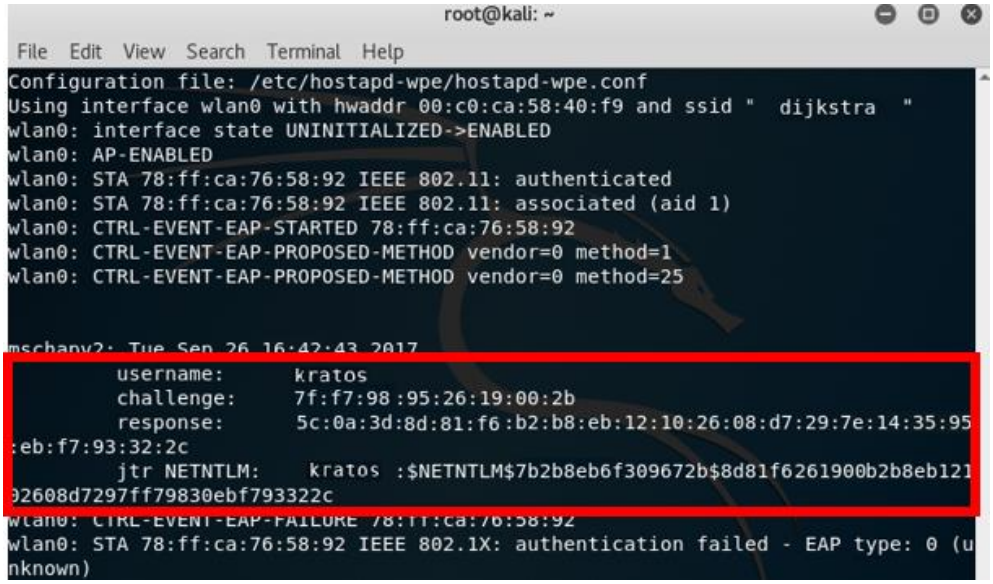


Figura 3.27. Obtención de credenciales del servidor de autenticación (diagrama propio).

Para desencriptar la contraseña obtenida del usuario RADIUS fue necesaria la creación de un nuevo diccionario, ya que el diccionario que se creó anteriormente con base en la información de la red sin autenticación *enterprise*. Puesto que el APF captura todas las credenciales del servidor de autenticación, se tienen que generar diferentes diccionarios por cada usuario RADIUS, donde la información para crear el diccionario tiene que ser acorde al usuario. Como se puede observar en el ejemplo de la figura 3.27 el nombre que se le asignó al usuario que tiene acceso a la red no es como tal un nombre, por este hecho se potencializa la dificultad de crear un diccionario que contenga las credenciales adecuadas. Para fines demostrativos se editó un diccionario que se había creado anteriormente para ejemplificar cómo se descifran estas contraseñas. La desencriptación de la contraseña se realizó mediante el comando “zcat” cuyos resultados se muestran en la figura 3.28.

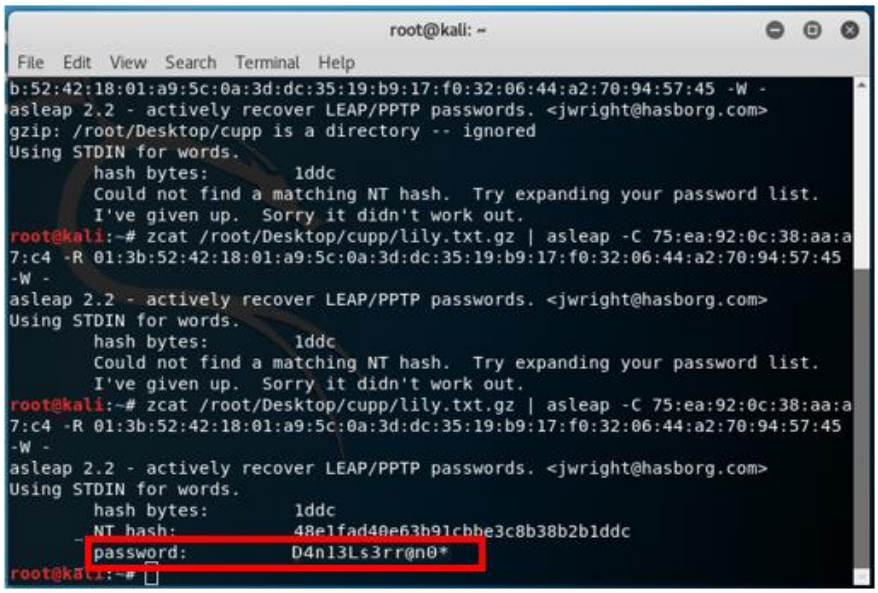


Figura 3.28. Desencriptación de contraseña de un usuario RADIUS.

Una vez que se obtuvieron las credenciales se intentó acceder a la red con ellas, pero no fue posible debido al filtrado MAC

3.3.1.3 Intento de clonación MAC

Para verificar el funcionamiento del filtrado MAC que está habilitado como parte de *hardening* se realizó un nuevo ataque para clonar la MAC de un dispositivo que en ese momento se encontraba conectado a la red. En la figura 3.29 se muestra la clonación MAC.

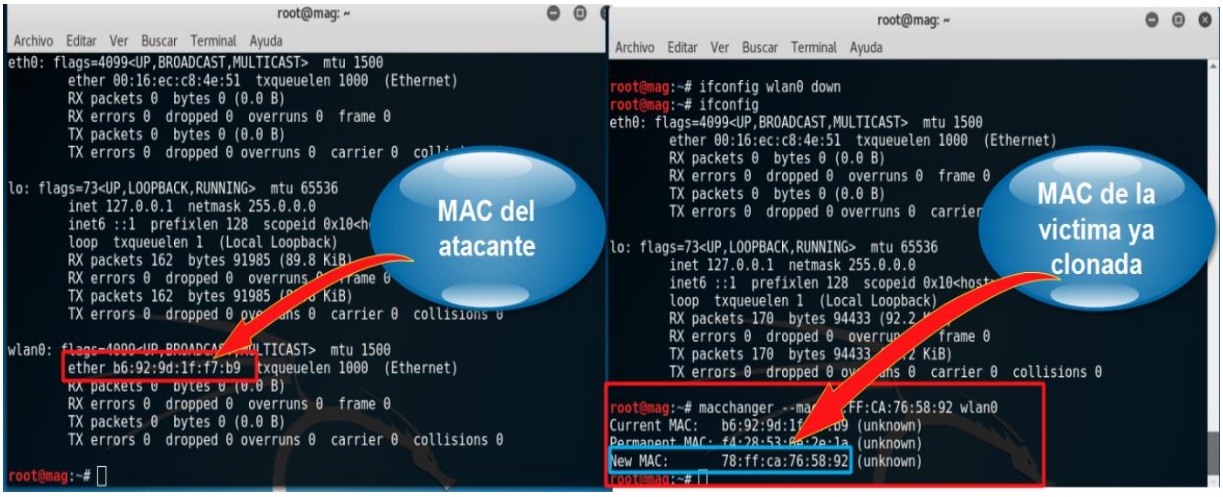


Figura 3.29. Clonación MAC.

Sin embargo, no fue posible acceder a la red ya que la clonación sólo duraba de 6 a 10 segundos.

Por otro lado, se realizó el mismo ataque a la WLAN con el AP Linksys 38378 con el fin de comparar el comportamiento de las redes con diferentes AP. En este caso se nota el momento en que el APF aparece en el dispositivo que se encuentra autenticado a la red, como se muestra en la imagen 3.30.

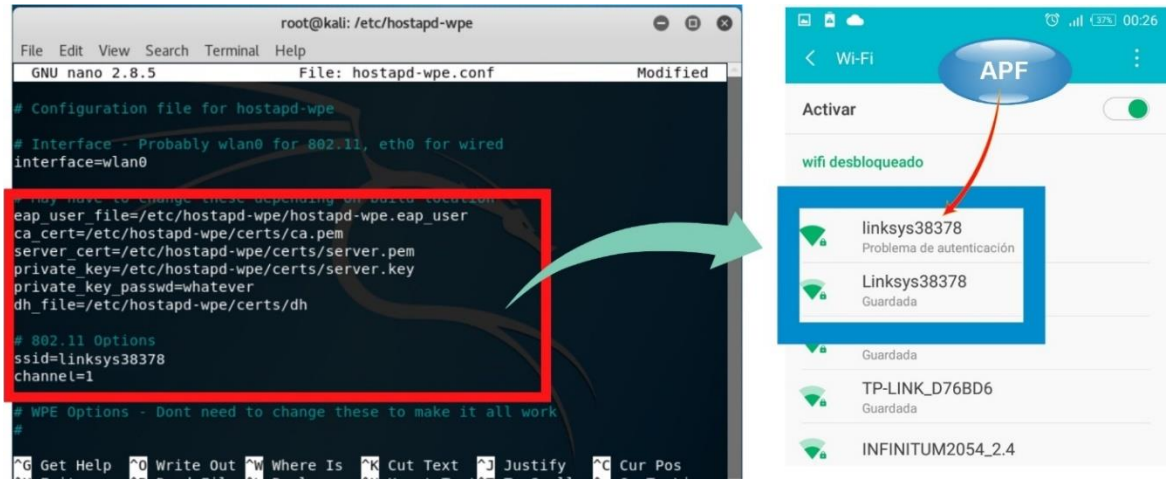


Figura 3.30. Creación del APF.

El APF desautentica al usuario inmediatamente y lo redirecciona a él mismo, donde realiza una petición de credenciales, si esta petición se ignora habrá una denegación de servicio. En el lado izquierdo de la figura 3.31 se puede apreciar la petición de credenciales y en el lado derecho se muestra la denegación de servicio al ser ignorada ésta.

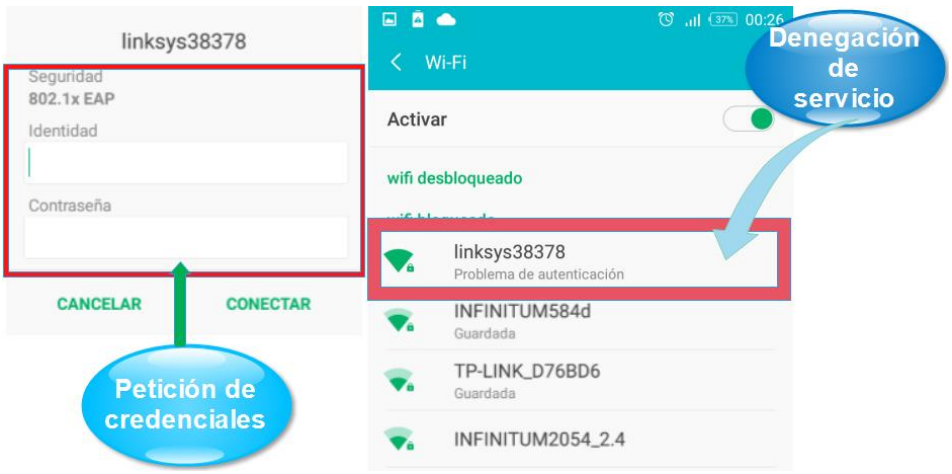


Figura 3.31. Acceso denegación a la WLAN.

Por último, se realizó una revisión de la seguridad en la WLAN de entorno SOHO, los resultados obtenidos de dicha revisión se mostrarán a continuación.

3.4 Revisión de seguridad con y sin la implementación de *hardening*

Para valorar la seguridad en la WLAN, se realizó una revisión de seguridad antes de la implementación de *hardening* y después de dicha implementación, con el fin de determinar qué tan segura es la WLAN en ambos escenarios. Para notar las diferencias de dicha revisión, se tabularon los resultados obtenidos de las tres WLAN en las que se implementó *hardening*, donde se realizó una comparativa con los tres AP que se utilizaron siguiendo el siguiente formato que se muestra en la tabla 3.0. De acuerdo con la información de la tabla puede notarse que la implementación de *hardening* variara de acuerdo con las características del AP en uso, como en el caso de la configuración remota y la potencia.

	Sin la implementación de hardening			**Con la implementación de hardening**		
	Linksys	Arcadyan	Alcatel	Linksys	Arcadyan	Alcatel
Emisión de SSID	Si	Si	Si	No	No	No
Contraseña para la gestión del AP	Por default	Por default	Por default	Cambiada	Cambiada	Cambiada
Desactivación de la configuración remota	No	No aplica		Si	No aplica	
Protocolo de autenticación	WPA/WPA2 PSK	WPA/PSK	WPA2/PSK	WPA/WPA 2 *enterprise* 802.1x	WPA/WPA2 *enterprise* 802.1x	WPA/WPA2 *enterprise* 802.1x
Filtrado MAC	No	No	No	Si	Si	Si
Minimización de potencia	Máxima	Alta	Alta	No aplica	Baja (cubre el área deseada)	Baja (cubre el área deseada)
Desactivación del WPS	No	No	No	Si	Si	Si
Contraseñas seguras	Por default	No	No	Si	Si	Si
Actualización del firmware	Actualizado	Actualizado	Actualizado	Actualizado	Actualizado	Actualizado

Tabla 3.0. Revisión de la seguridad con y sin hardening.

Así mismo, se realizó una revisión más con las herramientas de la Suite AIR, la cual consiste en un ataque a la red con la herramienta airodump, dicho ataque revelara los elementos necesarios para que un ataque tenga éxito sin demandar mucho tiempo y que sea sencillo de realizar. Estos elementos se indican en la figura 3.32, en base a esta revisión se verificó si existe una diferencia en una WLAN con *hardening* y sin *hardening*.

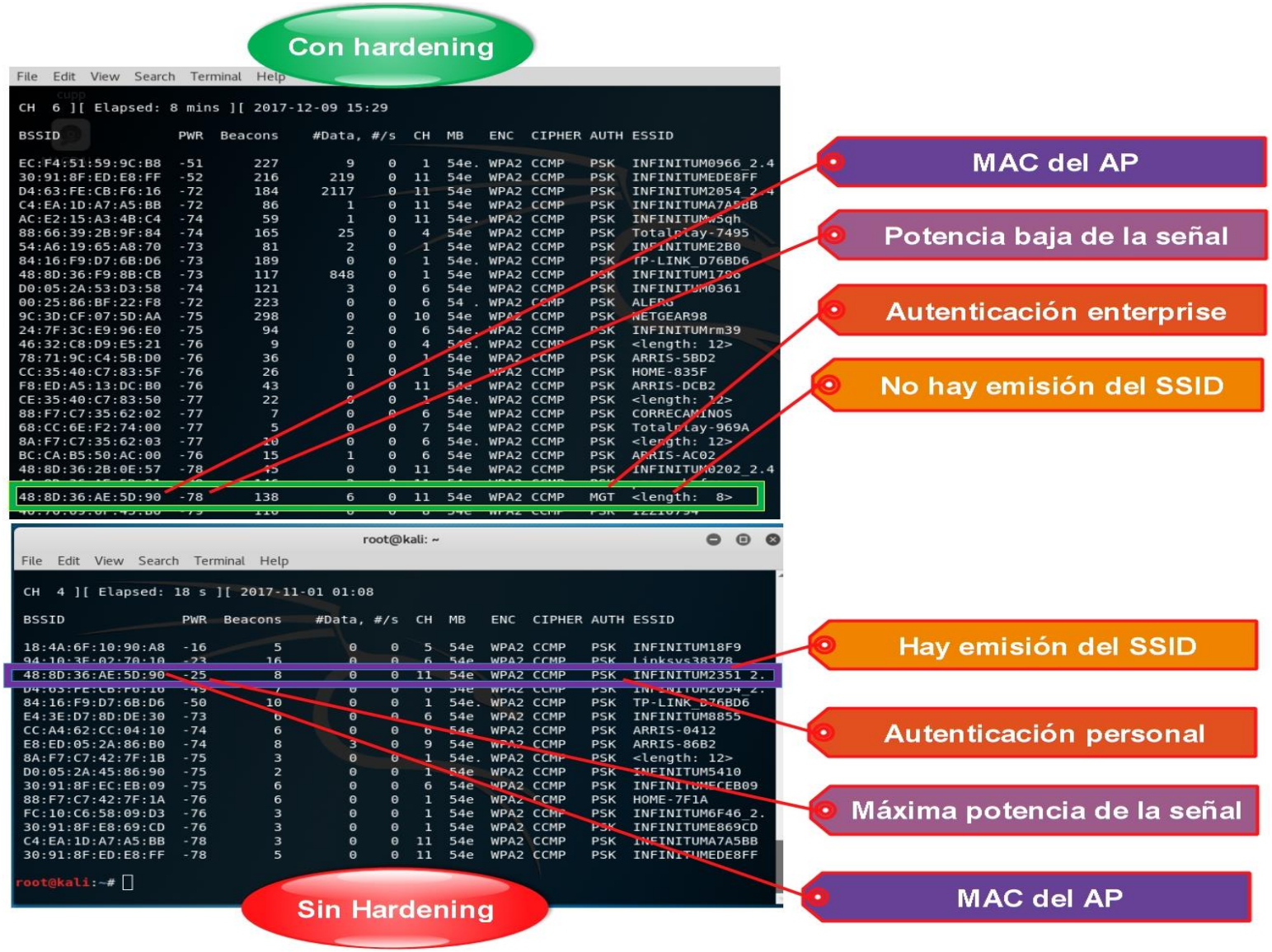


Figura 3.32. Revisión de la seguridad de la WLAN con y sin hardening (diagrama propio)

Por otro lado, para comprobar el funcionamiento del servidor de autenticación éste se puso a prueba durante dos meses, tiempo en el cual ha estado en funcionamiento sin ser interrumpido. En la figura 3.33 se muestra el momento en el que el servidor de autenticación inicio a trabajar con cero procesos, y en la figura 3.34 se muestran 3,331 procesos, siendo éstos los que se han registrado durante dos meses consecutivos de trabajo.

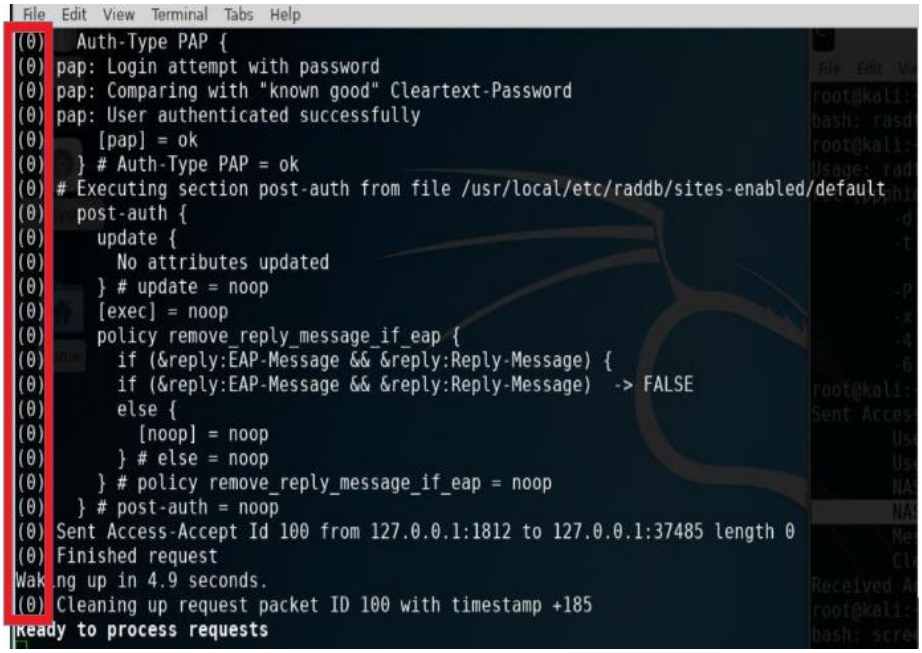


Figura 3.33. Procesos registrados en el servidor de autenticación freeRADIUS al iniciarlo (diagrama propio).

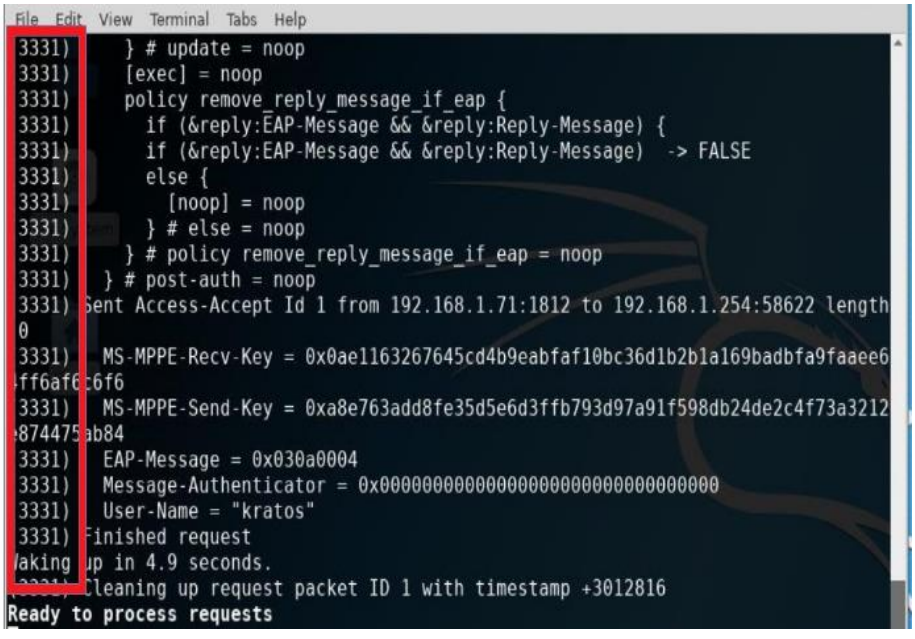


Figura 3.34. Procesos registrados del servidor de autenticación durante dos meses de trabajo (diagrama propio).

Conclusiones

a) Conclusiones de la identificación de vulnerabilidades

Los protocolos de seguridad para una WLAN fueron evolucionando poco a poco para brindar una mayor seguridad; sin embargo, WPA2 fue el último protocolo de seguridad que se diseñó para este tipo de redes en el 2004. Han pasado 14 años confiando la seguridad en este protocolo y como consecuencia, en septiembre del 2017 se ha roto completamente. A pesar de ello, la problemática se sigue resolviendo con parches de seguridad, pero a medida que avanza la tecnología esta se puede aprovechar para realizar ataques mejor diseñados a una WLAN. Por dicho motivo es forzosa la creación de un nuevo protocolo de seguridad.

Para poder concretar un ataque con las herramientas de la Suite AIR, primero que nada, debe conocerse el funcionamiento adecuado de todas y cada una de las herramientas de la suite. Así mismo es necesaria la utilización de un diccionario, el cual debe ser construido de acuerdo con la información obtenida de la WLAN que se desea atacar para que exista una mayor probabilidad de éxito, este debe construirse con base en ingeniería social, por lo que se debe pensar como víctima y atacante. Por otro lado, los diccionarios que se encuentran en la red resultan ser completamente inútiles, debido a que estos son una base de datos de posibles contraseñas, lo que no garantiza que se encuentre en dicho diccionario la contraseña de la WLAN que se está atacando.

Con los ataques que se realizaron a los protocolos de seguridad WEP, WPA y WPA2 de una WLAN, se comprobó que son vulnerables en la parte autenticadora.

Al realizar los 5 ataques a cada protocolo se comprobó que WEP es el más vulnerable en comparación a los protocolos WPA y WPA2, ya que WEP fue vulnerado en menor tiempo y con menor esfuerzo, puesto que no fue necesaria la creación de un diccionario de fuerza bruta, tal que el tiempo de convergencia de WPA y WPA2 dependerá del diccionario, el tiempo podría ser muy corto o prolongado.

b) Conclusiones de la implementación de *hardening*

Es posible implementar un servidor de autenticación en un entorno SOHO a un bajo costo de hardware si se cuenta con un AP que soporte una autenticación *enterprise*.

Se verificó que la autenticación *enterprise* se puede migrar a un entorno SOHO con la utilización de una tarjeta de desarrollo raspberry PI3, como servidor de autenticación.

Se comprobó que el protocolo WPA2 *Enterprise* es mucho más seguro debido que se usan credenciales de autenticación para cada usuario.

Se le brindó una mayor seguridad a la WLAN de entorno SOHO al implementar todos los puntos de *hardening* a excepción del enmallado.

Un punto de acceso falso estará en espera de credenciales, debido a ello, si existen problemas de autenticación o de denegación de servicios, es probable que el punto de acceso no sea auténtico.

Por otro lado, no se pudieron realizar algunas actividades de *hardening* en los AP, debido a sus características, por ejemplo, en el caso del modelo linksys 38378 no se pudo realizar la configuración de la potencia, y en el caso de los AP que ofrecen los ISP como en el caso del AP Arcadyan VRV9529AWAC24 no se pudo llevar a cabo la desactivación de configuración remota debido a las características de dichos AP.

Así mismo en algunos AP existe una delimitación en el tamaño de las contraseñas, por mencionar el AP Arcadyan VRV9529AWAC24 de Telmex el cual sólo permitió ingresar un número máximo de 12 caracteres para crear la contraseña de acceso a la red.

A pesar de que se logró un mejor robustecimiento en la WLAN con la implementación de *hardening*, claramente puede notarse que una WLAN ya sea de entorno SOHO o empresarial, nunca estará completamente protegida, debido a que la tecnología avanza continuamente.

c) Conclusiones no técnicas

Desarrolle las habilidades para poder penetrar una red poco segura, pero por ética profesional este conocimiento sólo se podría aplicar en auditorias profesionales. Por otro lado, los usuarios no deberían estar a la espera de que su red sea atacada, para empezar a tomar medidas de seguridad.

Gracias a este trabajo aprendí a seguir una metodología para llevar a cabo un proyecto en tiempo y forma.

Anexo A. Herramientas de la Suite AIR

En este anexo se describe el funcionamiento de las herramientas de la Suite AIR que fueron utilizadas para atacar a los protocolos WEP, WPA y WPA2.

airmon-ng: herramienta que permite activar o desactivar la tarjeta en modo monitor, la tarjeta se desactiva si se teclea el siguiente comando: ***airmon-ng stop wlan0***. Para poner la tarjeta inalámbrica en modo monitor se teclea el siguiente comando: ***airmon-ng start wlan0***. Se pueden visualizar los parámetros que se muestran en la figura A1.

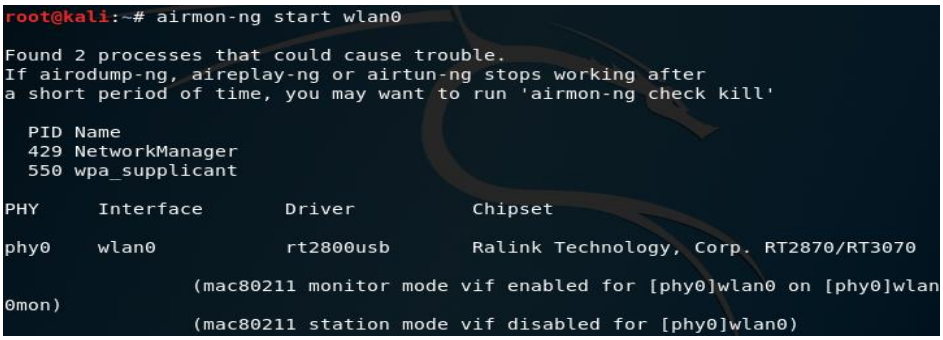


Figura A1. Activación de la tarjeta inalámbrica en modo monito (diagrama propio).

Una vez ejecutado el comando anterior los procesos que aparecen en la pantalla deben ser eliminados para que las siguientes acciones puedan ser ejecutadas. Esta acción se realiza con el comando kill seguido de los números de proceso PID, en este caso sería "***kill 429 550"***.

airodump-ng: herramienta que permite interceptar y analizar el tráfico inalámbrico con ayuda de la interfaz inalámbrica en modo monitor. Para ejecutar dicha herramienta se teclea el siguiente comando: ***airodump-ng*** nombre de la tarjeta. En la figura A2 se puede visualizar el tráfico capturado con airodump-ng.

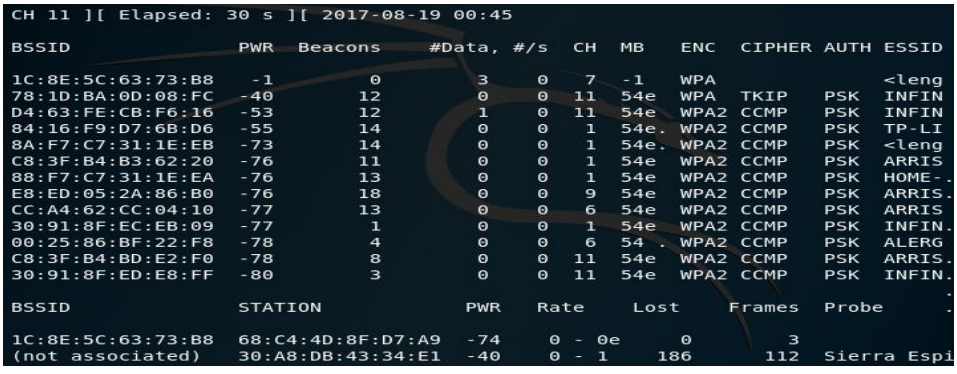


Figura A2. Captura de tráfico con airodump-ng (diagrama propio).

En la figura A2, CH representa el canal de comunicación, BSSID es la dirección MAC del AP, PWR es la potencia o intensidad de la señal[10], el termino Beacons se refiere al número de paquetes de anuncio de red que ha enviado el AP, Data es el número de paquetes de datos, #/s es el número de paquetes, MB hace referencia a la velocidad mínima soportada por el AP, ENC se refiere al algoritmo de cifrado que usa el AP puede ser OPN, WEP,WPA o WPA2; CIPHER es el tipo de cifrado de datos el cual puede ser RC4, TKIP o CCMP; AUTH es el método de autenticación, por lo regular suele ser PSK; ESSID hace referencia al nombre de la red, Station es la dirección MAC del cliente asociado al AP.

aireplay-ng es una herramienta que permite realizar diversos ataques a los AP y clientes asociados a este mismo, como por ejemplo:

- Desautenticación: este ataque permite desautenticar a uno o varios clientes de un AP.
- Autenticación falsa: permite asociarse a un punto de acceso, siempre y cuando el punto de acceso lo permita.
- Inyección de paquetes: este ataque permite capturar un paquete ARP y reinyectarlo contra el AP generando de esta forma demasiado tráfico.

En la figura A3 se puede apreciar el ataque de desautenticación e inyección de paquetes mediante el siguiente comando ***aireplay-ng -0 5 -a*** MAC del punto de acceso -h MAC falsa nombre de la tarjeta.

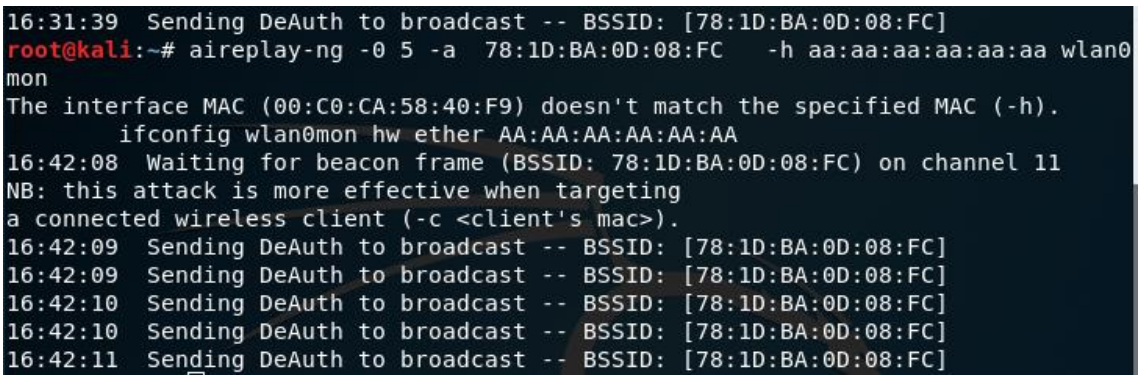


Figura A3. Ataque de desautenticación con la herramienta aireplay (diagrama propio).

[10] La interpretación de la potencia varía de acuerdo con el modelo de la NIC ya que en algunos ésta será mejor mientras más cerca al 0 se encuentre y en otros modelos mientras más cerca al 100.

Después de esta operación el cliente volverá a autenticarse con el AP, obteniéndose de esta forma el handshake como se muestra en la figura A4.

Aircrack-ng: herramienta que permite obtener la clave del archivo CAP, como se muestra en la figura A4. La clave de acceso a la WLAN se obtiene mediante la siguiente herramienta: ***aircrack-ng -w/usr/share/wordlists/rockyou.txt datos.01.cap.***

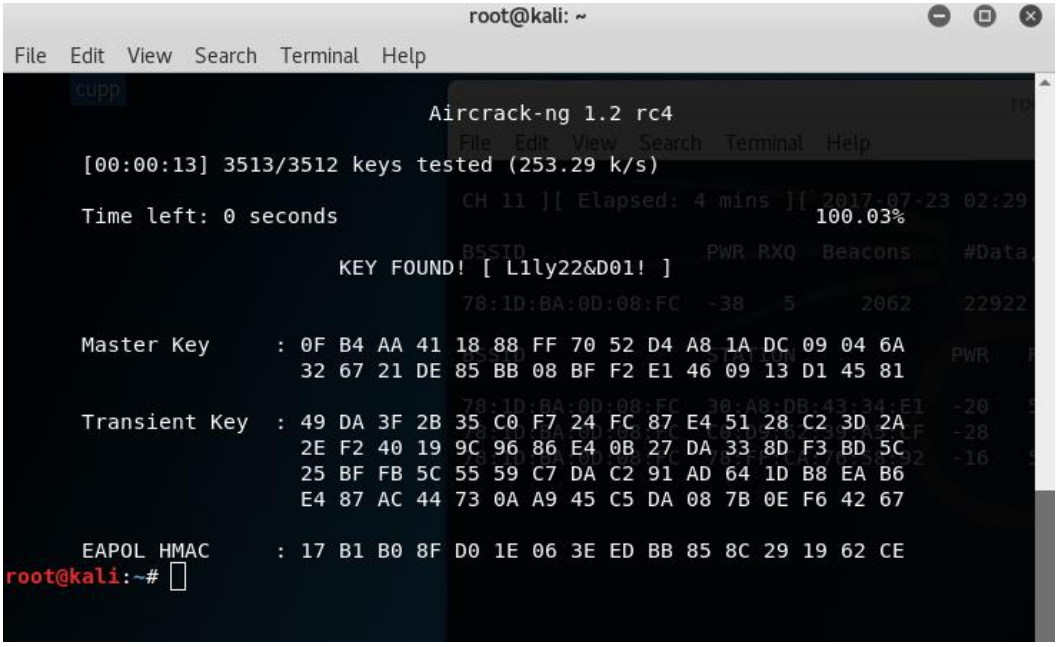


Figura A4. Obtención de la contraseña del archivo CAP (diagrama propio).

Donde rockyou.txt es el diccionario para fuerza bruta que se esté utilizando, el cual puede ser construido con la herramienta cupp (Common User Passwords Profile) como se explica a continuación.

Creación de diccionario con la herramienta cupp

El primer paso es descargar la herramienta con el comando git clone como se muestra en la figura A5.

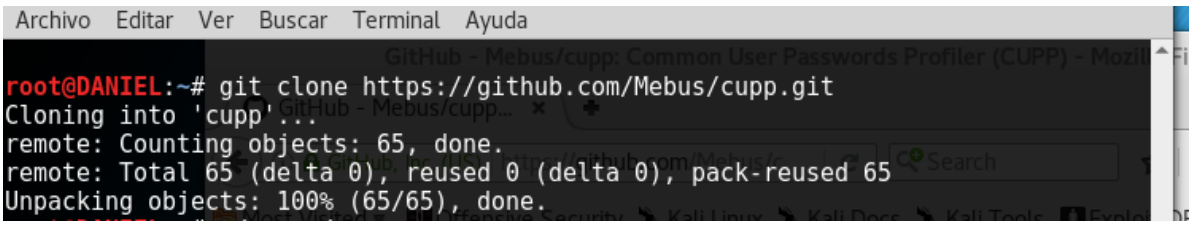


Figura A5. Descarga de la herramienta cupp (diagrama propio).

Posteriormente se procede a configurar la herramienta cupp con una serie de datos como por ejemplo: nombres, fechas de nacimiento, apellidos, apodos, nombres de mascotas, entre otros. Dichos datos son utilizados para realizar una combinación de palabras con las cuales se genera finalmente un diccionario como se observa en la figura A6 que muestra el proceso con el que se obtuvo un diccionario de 35602 palabras.

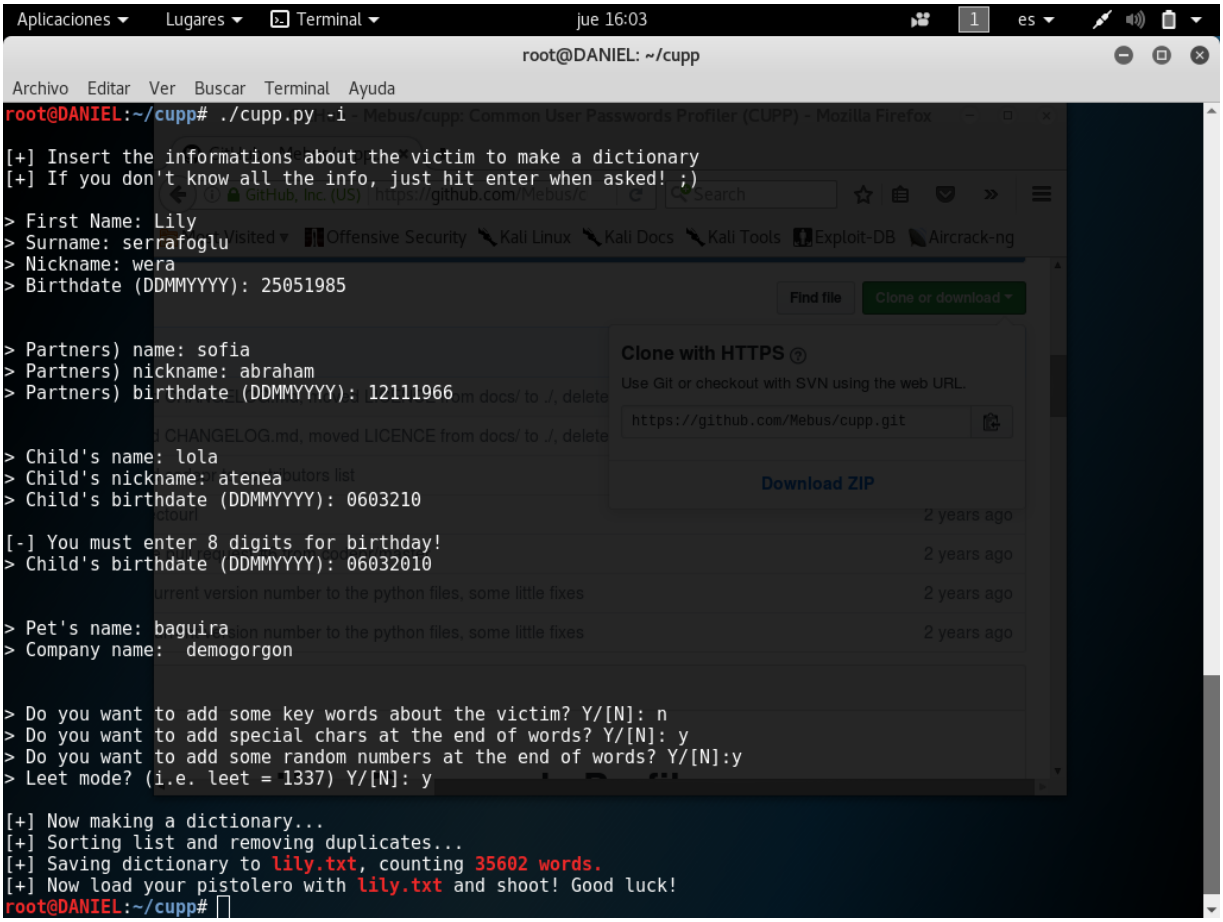


Figura A6. Creación de un diccionario con la herramienta cupp (diagrama propio).

En la figura A7 se muestra una parte del diccionario que se generó a partir de los datos que se proporcionaron. Puede apreciarse que existe tanto una combinación de letras y números como de caracteres especiales.

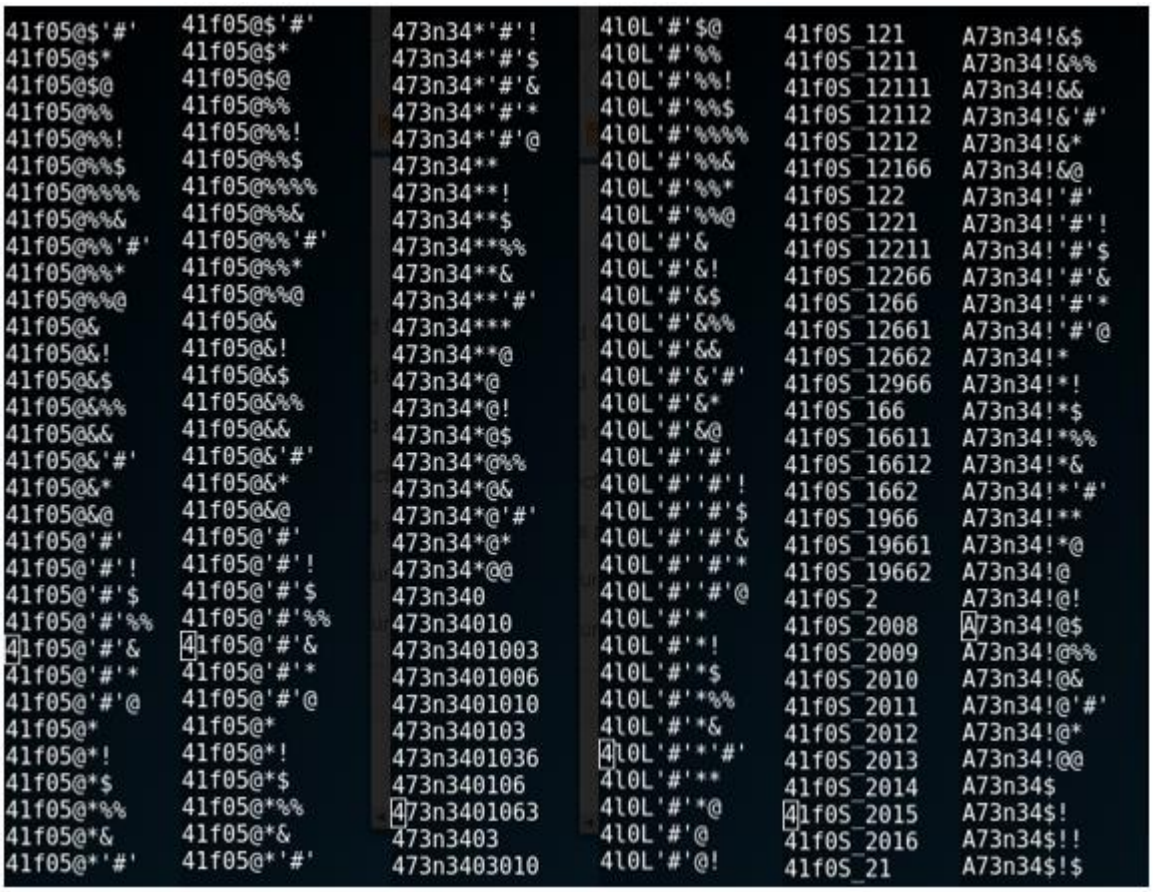


Figura A7. Fragmento del diccionario de contraseñas creado con la herramienta cupp (diagrama propio).

Anexo B. Creación de la máquina virtual con Kali Linux

En este anexo se describe detalladamente la creación de una máquina virtual con la distribución Kali Linux, que fue utilizada para realizar los ataques tanto al escenario de pruebas como a las WLAN encontradas en el medio inalámbrico.

1. Para crear una máquina virtual se debe descargar el OVA (Open Virtualization Appliance) de Kali Linux que es un formato para que la máquina virtual genere los requerimientos del sistema operativo. Posteriormente debe descargarse el OVA para Virtual Box desde la página de Kali Linux. En la figura B1 se muestra este OVA, en este caso se descargó la versión 2017.1.

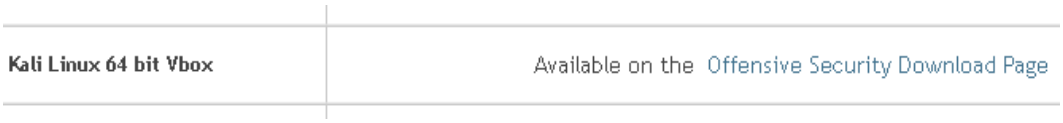


Figura B1. OVA Kali Linux (diagrama propio).

2. En Virtual Box en lugar de crear una nueva máquina se tiene que ir al apartado de archivo y seleccionar importar servicio virtualizado como se muestra en la figura B2.

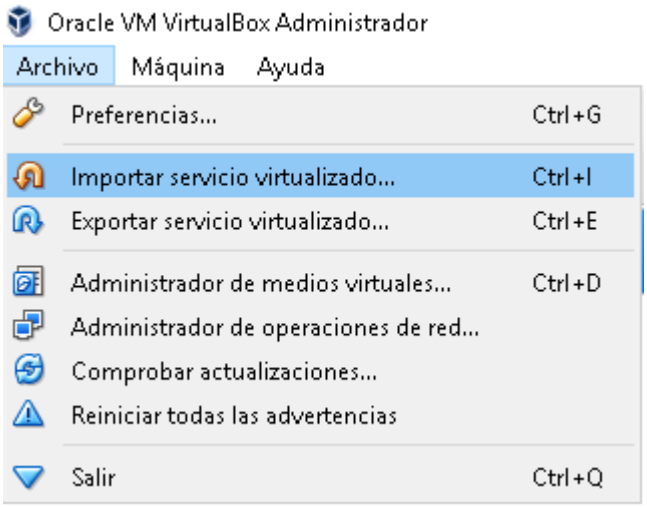


Figura B2. Importación del servicio virtualizado (diagrama propio).

3. El siguiente paso es importar el OVA a Virtual Box, debe seleccionarse el archivo de servicio donde se encuentra la descarga de éste como se muestra en la figura B3.

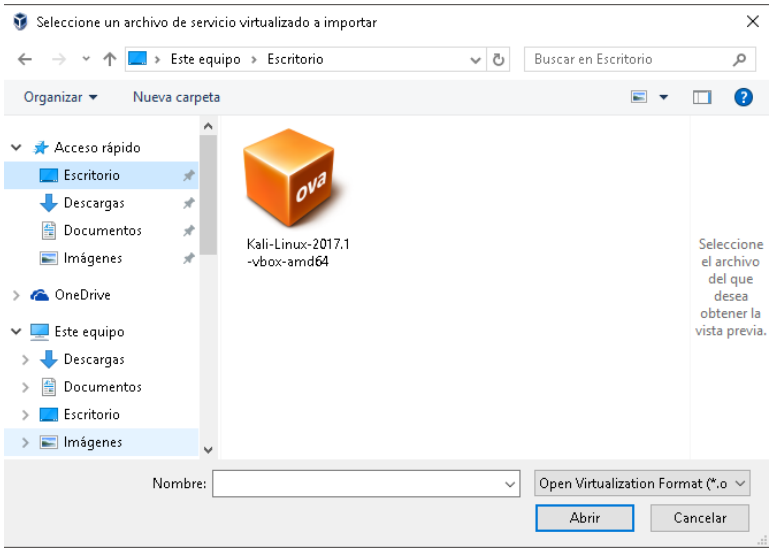


Figura B3. Importación del archivo (diagrama propio).

4. Después se muestran las descripciones generales de la máquina virtual como lo es el CPU y memoria RAM. En la figura B4 pueden apreciarse mejor estas características.

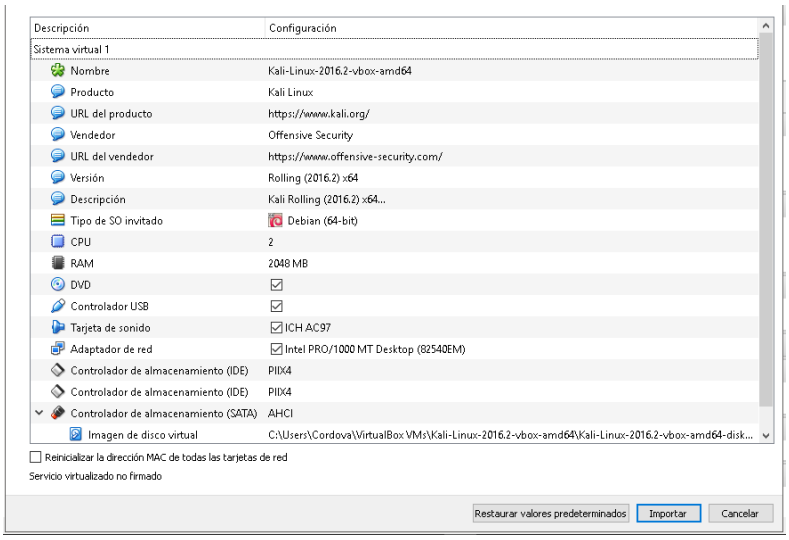


Figura B4. Características de la VM Kali Linux (diagrama propio).

5. El siguiente paso consta en seleccionar la opción importar, para importar las características necesarias para configurar la máquina virtual. En la pantalla se verá algo similar a lo que se muestra en la figura B5.

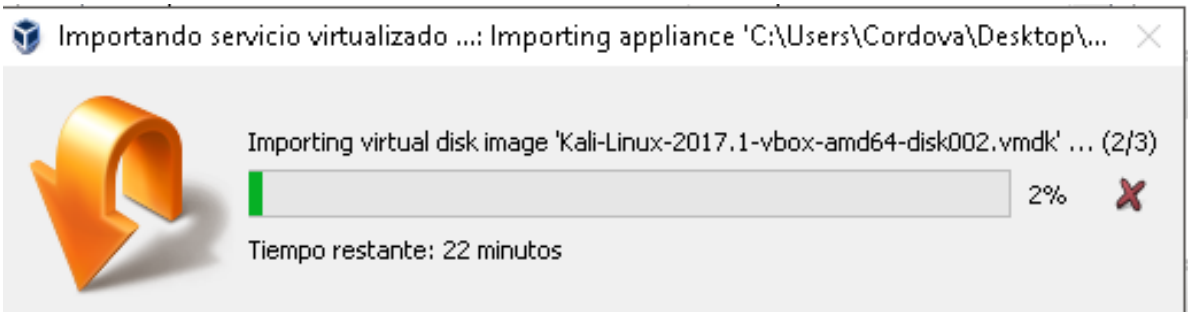


Figura B5. Configuración de la máquina virtual (diagrama propio).

6. Una vez que se inicie Virtual Box, en la ventana principal aparecerá la instalación del sistema operativo Kali Linux como se muestra en la figura B6.

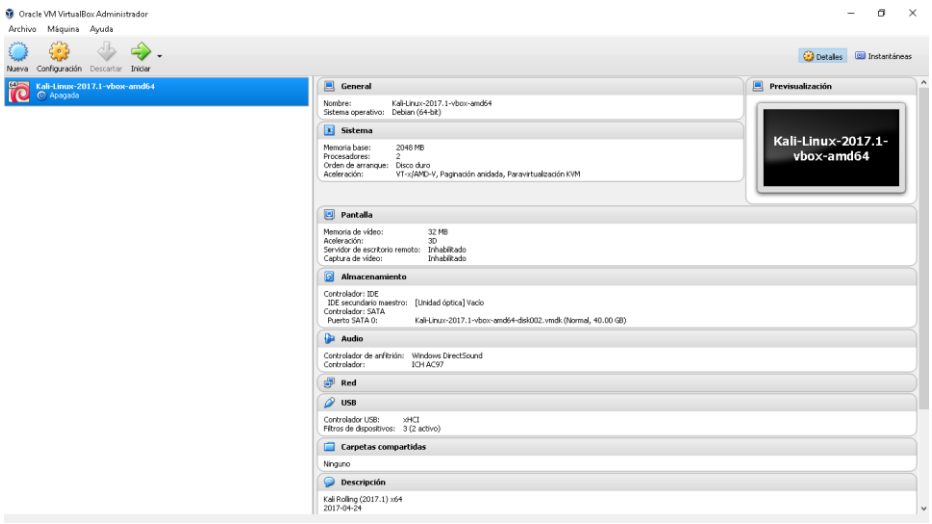


Figura B6. Ventana principal de Virtual Box (diagrama propio).

7.- Bibliotecas agregadas en Kali Linux

En esta sesión se indican las bibliotecas necesarias que requiere Kali Linux para su funcionamiento óptimo, estas bibliotecas se encuentran en la página oficial de Kali Linux. Las siguientes líneas deben agregarse en el archivo sources.list de Kali Linux.

deb http://http.kali.org/kali kali-rolling main contrib non-free

deb http://old.kali.org/kali sana main non-free contrib

deb http://old.kali.org/kali moto main non-free contrib

Anexo C. Instalación del servidor de autenticación freeRADIUS

En este anexo se indica la instalación del servidor de autenticación freeRADIUS paso a paso. En la sección 2.2.1.2 del capítulo 2 se explica el por qué deben ser instaladas tanto las dependencias duras como los paquetes de dicho servidor.

Instalación de dependencias

Las dependencias duras se instalan mediante el siguiente comando para el buen funcionamiento del servidor:

1. `root@kali:~# apt-getinstalllibssl-devlibtalloc-devlibkqueue-dev` (dependencias duras)

2. Instalación del paquete dpkg-dev: este paquete instala las herramientas necesarias para desempaquetar y crear paquetes en formato deb, así mismo incluye las ordenes `autoconf` y `make,` además de construir y cargar paquetes en formato debian.

   ```
   root@kali:~# apt-get install dpkg-dev
   ```

3. Instalación de OpenSSL: esta instalación es necesaria para poder utilizar la autenticación EAP con el servidor, ya que OpenSSL incluye todas las bibliotecas y archivos de cabecera, como libssl y libssl-dev y si no se tienen, muchos tipos de EAP no funcionan.

   ```
   root@kali:~# apt-get install openssl
   ```

4. `build-dep` es utilizado para instalar todas las bibliotecas y dependencias del paquete fuente de freeRADIUS, con el siguiente comando:

   ```
   root@kali~# apt-get build-dep freeradius.
   ```

5. Posteriormente debe instalarse Fakeroot. Este comando permite construir paquetes en formato deb como usuario sin privilegios que es la forma recomendada. Fakeroot puede ejecutar diversos comandos con privilegios de root para la manipulación de archivos como lo es el comando dpkg-buildpackage.

   ```
   root@kali:~# apt-get install fakeroot
   ```

6. El siguiente comando se ejecuta dentro de la carpeta de código fuente de FreeRADIUS. Utiliza la información especificada dentro de la carpeta debian para compilar el código fuente y posteriormente crear los distintos paquetes de FreeRADIUS. La opción -b es

para compilar sólo el binario y la función de la opción -uc es para omitir la firma de los paquetes.

```
root@kali:~# fakerootdpkg-buildpackage -b -uc
```

7. Si el paquete ssl-cert no está instalado causa problemas con los módulos de EAP al iniciar sesión en freeRADIUS, por dicho motivo este paquete debe ser instalado.

```
root@kali:~# apt-get install ssl-cert
```

Instalación del servidorfreeRADIUS

Toda la instalación se realizó de la forma source code de acuerdo con los siguientes pasos:

1. Descargar freeRADIUS desde su sitio oficial. Para evitar posibles errores debe descargarse la versión a la cual actualmente se le esté dando soporte.

```
root@kali:~# wget ftp://ftp.freeradius.org/pub/freeradius/free
radius-server- 3.0.15.tar.gz
```

2. Se descomprime con el siguiente comando

```
root@kali:~# tar -xzvf freeradius-server-3.0.15 tar.gz
```

3. Se construye la fuente directamente, este paso es opcional ya que se utiliza en caso de que se desee evitar la creación de paquetes freeRADIUS, en caso de ser así primero deben instalarse las dependencias necesarias como se indicó anteriormente. La fuente se construye con los siguientes comandos.

```
A.1   root@kali:~# ./configure

B.1   root@kali:~# make

C.1   root@kali:~#makeinstall
```

Nota: make install puede tardar varios minutos en instalar freeRADIUS.

Anexo D. Configuración de *hardening* en dos modelos distintos de AP

En este anexo se describe la configuración de todos los puntos posibles de *hardening* en los AP Linksys 38378 y Alcatel I-240W-A.

D.1 Configuración del AP Linksys 38378

1.1 En el AP se deben ingresar los siguientes datos: dirección IP del servidor RADIUS, el puerto de comunicación de freeRADIUS (1812) y la clave secreta que comparten, esta es la que se configuró en el servidor dentro del archivo *clients.conf*. En la figura D1 se aprecia dicha configuración.

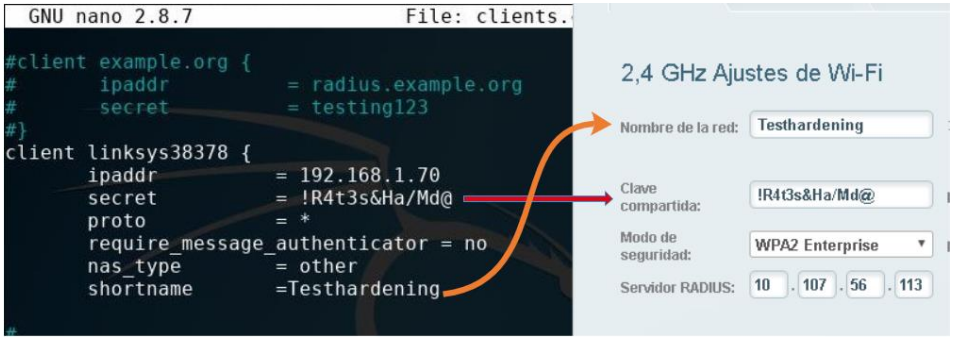


Figura D1. Configuración del cliente (diagrama propio).

1.2 Desactivación del WPS

En la figura D2 se muestra la deshabilitación del estándar WPS.

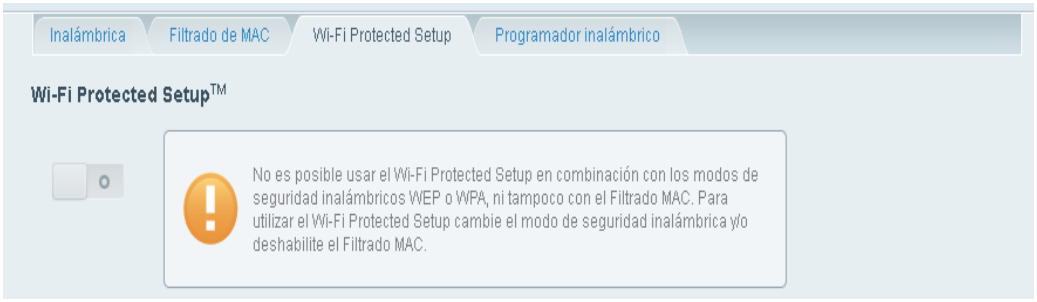


Figura D2. Desactivación del WPS (diagrama propio).

1.3 Contraseñas robustas

En la figura D3 del lado izquierdo, se muestra la configuración de los usuarios que podrán tener acceso a la red, puede notarse que la contraseñas tiene cierto grado de dificultad, en el lado derecho se muestra la configuración del AP que interactúa con el servidor.

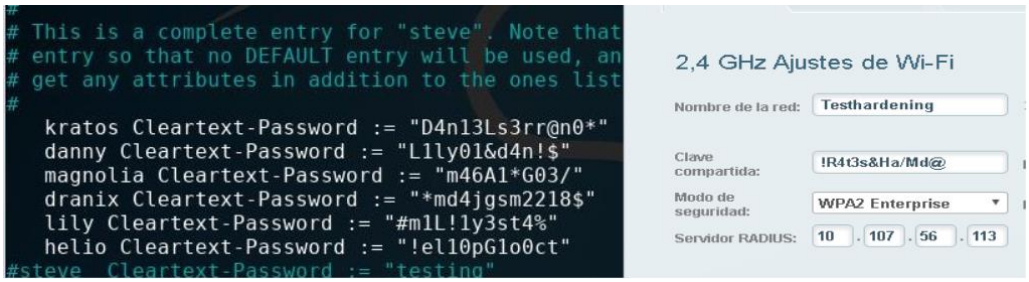


Figura D3. Creación de contraseñas seguras (diagrama propio).

1.4 Desactivación de la difusión SSID

En la figura D4 se muestra la desactivación del SSID en el AP.

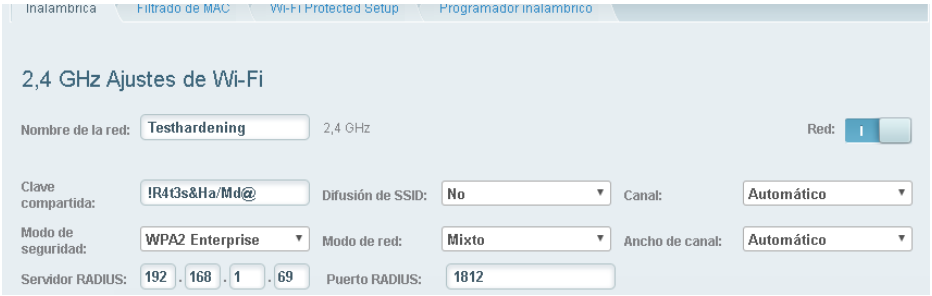


Figura D4. Desactivación del SSID (diagrama propio).

1.5 Desactivación de la configuración remota

En los AP Linksys se tiene la opción de desactivar la configuración remota como se muestra en la figura D5.

Figura D5. Deshabilitación al acceso remoto (diagrama propio).

1.6 Filtrado MAC

En el filtrado MAC solo 3 dispositivos se dieron de alta, estos son los que podrán acceder a la WLAN. En la figura D6 se muestra el filtrado de las direcciones MAC.

Figura D6. Filtrado MAC. (diagrama propio).

1.7 Gestión del AP

La contraseña por default para los AP Linksys es *admin* y se ha cambiado por otra como puede notarse en la imagen D7.

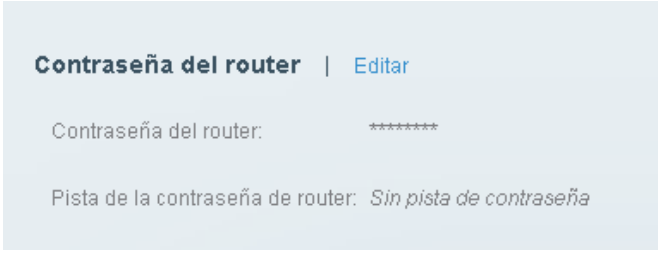


Figura D7. Cambio de contraseña (diagrama propio).

1.8 Minimización de la potencia

La minimización de la potencia en el caso particular del AP Linksys no se pudo llevar a cabo.

1.9 Actualización del firmware

Esta actualización es importante para que se actualicen los parches de seguridad en este caso la actualización es automática como se muestra en la figura D8.

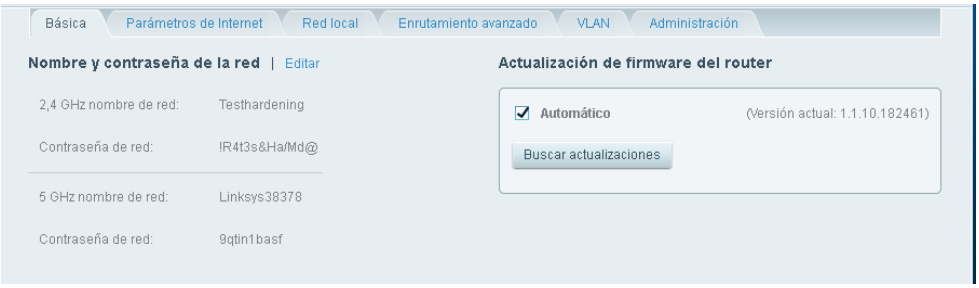


Figura D8. Actualización del firmware en el AP (diagrama propio).

D.2 Configuración del AP ALCATEL I-240W -A de TELMEX

2.1 Adición de la dirección IP del servidor RADIUS y el puerto de comunicación de freeRADIUS (1812) en el AP. En la figura D9 se aprecia dicha configuración.

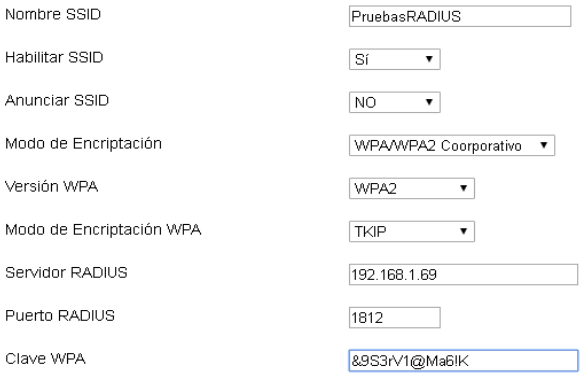


Figura D9. Configuración del cliente (diagrama propio).

2.2 Desactivación del WPS del AP Alcatel I-240W -A.

En la figura D10 se muestra la deshabilitación del WPS en el AP.

Figura D10. Desactivación del WPS (diagrama propio).

2.3 Desactivación de la difusión SSID del AP Alcatel I-240W -A

En la siguiente figura D11 se muestra la desactivación del SSID del AP.

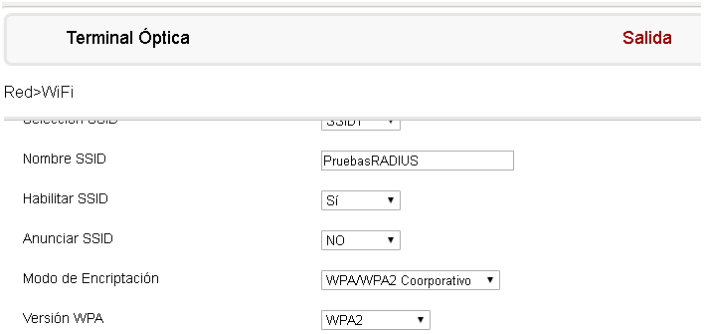
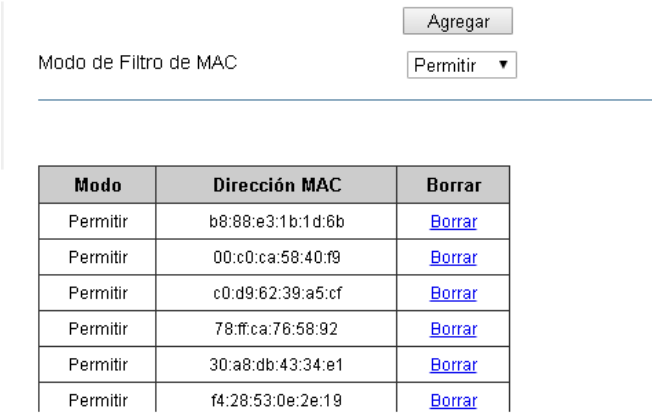


Figura D11. Desactivación del SSID de la red (diagrama propio).

2.4 Filtrado MAC en el AP Alcatel I-240W –A.

Se agregan las direcciones MAC de los 6 dispositivos que podrán tener acceso a la WLAN con autenticación *enterprise*. En la figura D12 se muestra dicho filtrado.



Modo	Dirección MAC	Borrar
Permitir	b8:88:e3:1b:1d:6b	Borrar
Permitir	00:c0:ca:58:40:f9	Borrar
Permitir	c0:d9:62:39:a5:cf	Borrar
Permitir	78:ff:ca:76:58:92	Borrar
Permitir	30:a8:db:43:34:e1	Borrar
Permitir	f4:28:53:0e:2e:19	Borrar

Figura D12. Filtrado MAC. (diagrama propio).

2.5 Gestión del AP

La contraseña por default para los AP Alcatel I-240W -A de TELMEX es la clave que se le asigna al AP de fábrica y fue cambiada por otra como puede notarse en la imagen D13.

Figura D13. Cambio de contraseña (diagrama propio).

2.6 Minimización de la potencia

Para el AP ALCATEL I-240W -A de TELMEX se selecciona la potencia más baja en este caso es el 25% como se muestra en la figura D14.

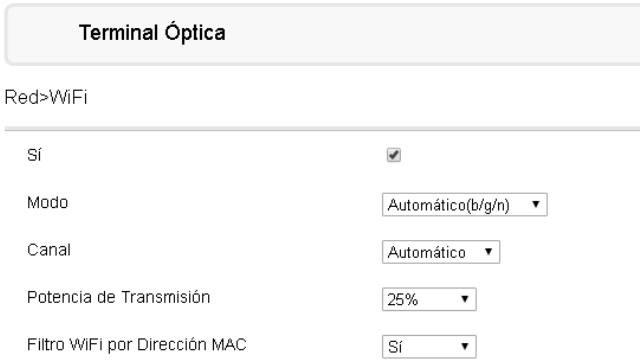


Figura D14. Minimización de la potencia (diagrama propio).

2.7 Actualización del firmware

En este caso la actualización del firmware debe realizarse manualmente como se muestra en la figura D15.

Figura D15. Actualización del firmware en el AP (diagrama propio).

Anexo E. Ataque a WPA con wifiphisher

En este anexo se describen los resultados obtenidos del ataque al protocolo WPA de clave compartida con la herramienta Wifiphisher, dicho ataque se describe en los siguientes párrafos. Se realizó un monitoreo de redes con el fin de ver las redes aledañas mediante la emisión del SSID, una vez que estas fueron identificadas se seleccionó la red que se deseaba atacar. El ataque consistió en desautenticar a los clientes para que éstos proporcionen de manera voluntaria sus credenciales a un AP falso, el cual fue generado por la herramienta Wifiphiser. En la figura E1 se muestra la red que se atacó.

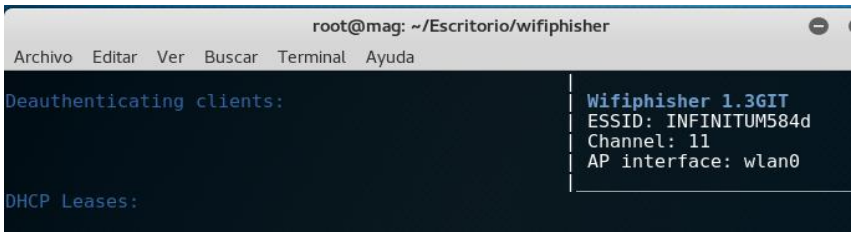


Figura E1. Red atacada con la herramienta wifiphiser a partir de la emisión del SSID (diagrama propio).

En la figura E2 se muestra el momento en el que el cliente intenta autenticarse a un AP falso y lo invita a proporcionar sus credenciales mediante una página web.

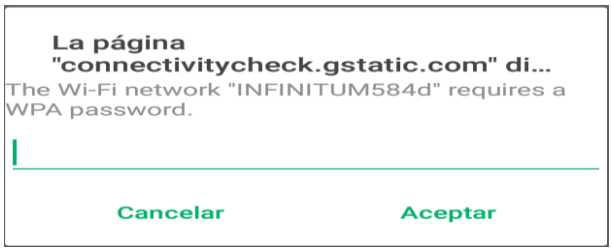


Figura E2. Petición de credenciales para autenticarse a la WLAN (diagrama propio).

Una vez que el usuario ha proporcionado sus credenciales, el atacante obtiene de manera inmediata la contraseña de dicha red como se muestra en la figura E3.

Figura E3. Obtención de contraseña con Wifiphisher (diagrama propio).

Como se observa en la figura E3 la contraseña que se obtuvo no es robusta, motivo por el cual se realizó un ataque más a la WLAN considerando una contraseña más robusta compuesta por una combinación de letras y números; no obstante, las credenciales se volvieron a obtener como se muestra en la figura E4.

Figura E4. Obtención de contraseña con seguridad WPA (diagrama propio).

En el tercer ataque se obtuvo una contraseña con una combinación de números, letras y caracteres especiales y como se esperaba las contraseñas fueron obtenidas ya que el usuario inconscientemente las ingreso. En la figura E5 se muestra la contraseña obtenida.

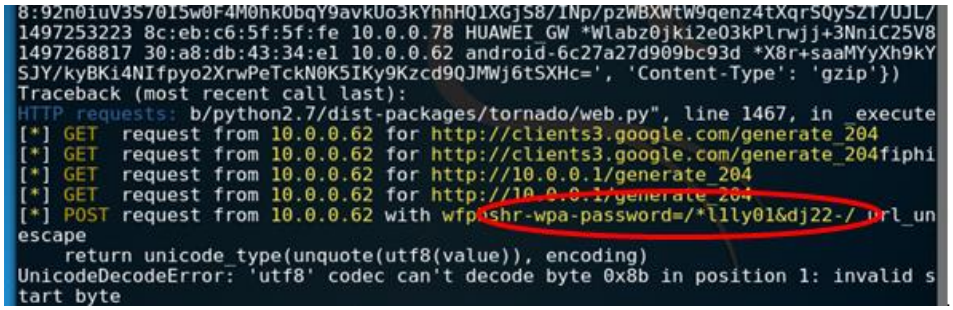


Figura E5. Obtención de contraseña robusta con la herramienta Wifiphisher de seguridad WPA (diagrama propio).

Una vez dentro de la WLAN, con esta misma herramienta también se pudieron obtener las credenciales de autenticación para entrar a Facebook (correo electrónico y contraseña) una de las redes sociales más populares, en la figura E6 se muestran los resultados de dicho ataque.

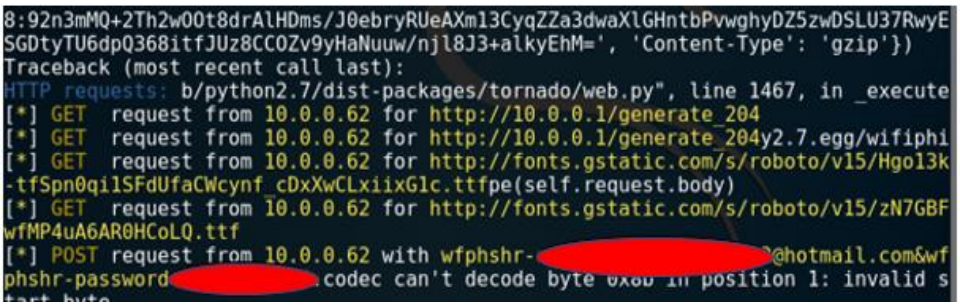


Figura E6. Obtención de credenciales de Facebook con la herramienta wifiphisher (diagrama propio).

Referencias

[1] Gartner, S. The Digital Industrial Economy; [en línea]; 2013 [consulta: Abril. 25 2017] Disponible en: http://www.gartner.com/newsroom/id/2602817

[2] mundo contac. Redes inalámbricas: el punto más vulnerable; [en línea]; 2015 [consulta 24 Mar. 2017] Disponible: http://mundocontact.com/redes-inalambricas-el-punto-mas-vulnerable/

[3] Becerra, J. Seguridad en Redes inalámbricas, la "preocupación más recurrente" para CIOs y CISOs; [en línea]; 2017 [consulta: 12 de septiembre de 2017] Disponible: http://cio.com.mx/seguridad-en-redes-inalambricas-la-preocupacion-recurrente-cios-cisos/

[4] Kaspersky KRACK. Tu WI-FI ya no es seguro; [en línea]; 2017 [consulta feb. 2018] Disponible: https://latam.kaspersky.com/blog/krackattack/11578/

[5] Vanhoef, M., Piessens, F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2; [en línea]; 2017 [consulta feb. 2018] Disponible: https://papers.mathyvanhoef.com/ccs2017.pdf

[6] Chamorro, L., Pietrosemol, E. Redes inalámbricas para el desarrollo en América Latina y el Caribe. Serie Temas emergentes, pp3, 2008.

[7] Cisco. Lo que usted necesita saber sobre las redes inalámbricas; [en línea]; [consulta 24 feb.2017] Disponible: http://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectados anonimos/wireless/pdfs/brochure_wireless.pdf

[8] Salvetti, D. Redes Wireless. Users Buenos Aires. pp.14 - 26, 2011, ISBN: 978-987-1773-98-5.

[9] Gunther, A. A history of Wireless standards: WI-FI back to basics; [en línea]; 2015 [consulta: 15 feb.2017] Disponible: http://boundless.aerohive.com/technology/wi-fi-back-to-basics-a-history-of-wireless-standards.html

[10] Reid, N., Seide R. Manual de Redes Inalámbricas 802.11 (Wi-Fi); McGraw-Hill, 2005.

[11] Mifsud, E., Lerma, R. Despliegue de redes inalámbricas; [en línea]; [consulta: 13 Mar. 2017] Disponible:https://serviciosenred2012inma93.files.wordpress.com/2012/03/diapositivas-u-t-9.pdf

[12] Stallings, W. Comunicaciones y redes de computadoras. Madrid. Pearson educación. pp 558-580, 2004.

[13] Colmenares J. Estándares IEEE 802; [en línea]; 2008 [consulta: 28 feb 2017] Disponible: http://estandaresieee802redes.blogspot.mx/

[14] IEEE. Principales estándares 802.11; [en línea]; [consulta: 28 feb. 2017] Disponible: http://ieeestandards.galeon.com/aficiones1573579.html

[15] UNAM. Estándar IEEE 802.11 WiFi; [en línea]; [consulta: 28 feb. 2017] Disponible: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/164/A6.pdf?sequence=6

[16] Mohammad, R., Mohammad M. A Security Solution for Wireless Local Area Network (WLAN), 2007 International Symposium on High Capacity Optical Network and Enabling Technologies, Dubai, 2007 pp 1- 6 doi: 10.1109/HONET.2007.4600239.

[17] José Ignacio Castillo Velázquez. Redes de datos: contexto y evolución, Edit. SAMSARA, pp 164,165, 2016.

[18] Todd Laummnie. CompTIA Network+ Certification. Canada, Edit. Sybex, pp 343, 2015

[19] J. Gu, J. Zhao and W. Li, "Research on WLAN security technology based on IEEE 802.11," *2011 3rd International Conference on Advanced Computer Control*, Harbin, 2011, pp. 234-237. doi: 10.1109/ICACC.2011.6016404

[20] Wrightson, T. Wireless Network Security A Beginner's Guide New York Chicago San Francisco. McGraw Hill, 2012.

[21] Hassan A, Abdirazak M, Shamsuzzman S, Anam T, Khan Z, Mahmudur R, Comparative study of WLAN security protocols: WPA WPA2, 2015 3rd international Conference on Advanced in Electrical Engineering, Dhaka, Bangladesh, 2015 pp165, 166.

[22] Panda software, seguridad en redes inalámbricas; [en línea]; 2005 [consulta 25 May 17] Disponible: http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf

[23] Guillaume.L. Seguridad Wi-Fi – WEP, WPA y WPA2; [en línea]; 2006 [consulta 18 Abril. 2017]. Disponible en: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_ wifi_ES.pdf

[24] Barajas, S. Protocolos de seguridad en redes inalámbricas; [en línea]; [consulta 10 feb. 2017] Disponible en file:///C:/Users/Acal%C3%A1/Downloads/1341353071.Protocolos%20de%20seguridad%20de%20redes%20wifi.pdf

[25] Ariganello, E., Barrientos, E. Redes Cisco CCNP a Fond. Guía de estudios para profesionales. México. Alfaomega Ra-Ma, 2011.

[26] Alamanni, M. Kali Linux Wireless Penetration Testing Essentials. Packt Publishing limited. pp 25,26, 43-45, 61,62, 2015.

[27] Jyh-Cheng Chen, Ming-Chia Jiang and Yi-wen Liu, "Wireless LAN security and IEEE 802.11i," in *IEEE Wireless Communications*, vol. 12, no. 1, pp. 27-36, Feb. 2005. pp 1-19 doi: 10.1109/MWC.2005.1404570.

[28] Akin, T. Hardening Cisco Routers, Estados Unidos de America: O'REALLY. pp 39-50, 2002.

[29] Mallery, J., Zann,J., Kelly, P., Seagren, E. Hardening Network Security, New York McGraw-Hill/Osborne, pp 242-275, 2004.

[30] freeRADIUSD. The FreeRADIUS Technical Guide; [en línea]; 2014 [consulta 13 Sep. 2017] Disponible en: http://networkradius.com/doc/FreeRADIUS%20Technical%20Guide .pdf

[31] Van der Walt, D. FreeRADIUS beginnerr´s guide. Birmingham [U.K.]: Packt Pub. Ltd., pp 27-72, 2011.

[32] dekok, A. Deployig RADIUS: Configuring EAP, Deployinggradius.com; [en línea]; 2017 [consulta 16 Sep. 2017] Disponible en: http://deployingradius.com/documents/configuration/eap.html

[33] Rigney,C. RFC 2865 Remote Authentication Dial In User Service (RADIUS), Network Working Group, 2000.

[34] Raspberry PI3 Model B, 2017; [en línea]; [imagen]; Disponible en: https://www.takealot.com/raspberry-pi-3-model-b-1gb-project-board/PLID41466406

ABSTRACT

Wireless local area networks (WLAN) become very popular SINCE 2000 because they offer connectivity without the need for a physical guided transmission medium, making it easier for most users to use different devices to connect to the Internet. However, this wireless connectivity sacrifices security of the network, compromising it by different malicious attacks.

To fill this security gap in a WLAN, different protocols were developed. WEP was the first security protocol, however, it is the most vulnerable protocol for this kind of networks, but it established the foundations for developing more robust protocols. WEP was replaced in 2003 by WPA wich evolved into WPA2 in 2004. Although WPA2 is the most robust protocol, IT is susceptible to passive attacks and denial-of-service attacks. Last october 2017 a security vulnerability was discovered.

This work is focused on identifying vulnerabilities when accessing a WLAN infrastructure in a small office or home office environment (SOHO) and mitigating them through the implementation of hardening, it means a set of activities that strengthen security.

Results show a SOHO environment WLAN was strengthened with the proposed hardening procedures; however, it is worth mentioning a wireless network, whether a SOHO or an enterprise environment, it will not be completely protected, due to technology is constantly evolving as new ways for attacks a paper.

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

AUTONOMUS UNIVERSITY OF MEXICO CITY

SCIENCE AND TECHNOLOGY COLLEGE

Vulnerabilities mitigation in a WLAN with hardening implementation

THESIS

TO OBTAIN THE GRADE OF

BACHELOR IN ENGINEERING IN ELECTRONIC SYSTEMS AND TELECOMUNICATIONS

PRESENTS:

MAGNOLIA ALCALÁ GARCÍA

THESIS ADVISOR

M. Sc. MAGALI CORTEZ VÁZQUEZ

Mexico City, August 2018.