UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

Estudio de vulnerabilidades en el sistema de seguridad WPA-2 Personal del estándar IEEE 802.11i y propuestas de mejoras a considerar en el sistema WPA-3

Trabajo de Titulación previo a optar por El Título de Ingeniero en Electrónica y Telecomunicaciones

AUTOR:

Alexis Vicente Pardo Sánchez.

DIRECTOR:

Ing. Marco Augusto Suing Ochoa, Mg. Sc.

LOJA - ECUADOR

2022

Certificación

Loja, 11 de Enero de 2022

Ing. Marco Augusto Suing Ochoa Mg. Sc.
DIRECTOR DEL TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo proceso de la elaboración del trabajo de titulación titulado: "Estudio de vulnerabilidades en el sistema de seguridad WPA-2 Personal del estándar IEEE 802.11i y propuestas de mejoras a considerar en el sistema WPA-3" de autoría del estudiante Alexis Vicente Pardo Sánchez, previa a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.

Firmado electrónicamente por:
MARCO AUGUSTO
SUING OCHOA

Ing. Marco Augusto Suing Ochoa Mg. Sc.
DIRECTOR DEL TRABAJO DE TITULACIÓN

Autoría

Yo, **ALEXIS VICENTE PARDO SÁNCHEZ**, declaro ser el autor del presente trabajo de titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi trabajo de titulación en el Repositorio Institucional - Biblioteca Virtual.

FIRMA

Cédula: 1104115439
Fecha: Loja, 1 de Abril del 2022
Correo electrónico: alexis.pardo@unl.edu.ec
Teléfono o Celular: 0986601752

Carta de autorización del trabajo de titulación por parte del autor, para la consulta, producción parcial o total y publicación electrónica del texto completo

Yo, **ALEXIS VICENTE PARDO SÁNCHEZ**, declaro ser el autor del trabajo de titulación titulado: "**Estudio de vulnerabilidades en el sistema de seguridad WPA-2 Personal del estándar IEEE 802.11i y propuestas de mejoras a considerar en el sistema WPA-3**", como requisito para optar al grado de: **INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES**, autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del trabajo de titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, al primer día del mes de abril del dos mil veintidós.

Firma:
Autor: Alexis Vicente Pardo Sánchez
Cédula: 1104115439
Dirección: Loja, (Barrio Nueva Granada)
Correo electrónico: alexis.pardo@unl.edu.ec
Teléfono: 2723572 **Celular:** 0986601752

DATOS COPLEMENTARIOS:

Director del Trabajo de Titulación: Ing. Marco Augusto Suing Ochoa Mg. Sc.

Tribunal de Grado:

Ing. Juan Gabriel Ochoa Aldeán Mg. Sc.
Ing. John Jossimar Tucker Yepez Mg. Sc.
Ing. Franklin Gustavo Jimenez Peralta Mg. Sc.

Dedicatoria

El presente proyecto de investigación lo dedico a mis padres Janeth Sánchez y Vicente Pardo quienes con su arduo esfuerzo y sacrificio me han apoyado en este sendero de estudio y me han apoyado innumerables veces a seguir adelante con mis metas, sueños y anhelos, sin su apoyo incondicional nunca lo hubiera logrado.

Este trabajo también va dedicado mi hermano José Luis quien me ha acompañado y apoyado con sus valiosas palabras y consejos para seguir avanzando con mis estudios y seguir mejorando cada día. De igual manera, este trabajo va dirigido a mis abuelitos Héctor y Zoraida los cuales me supieron brindar su apoyo y cobijo cuando más lo necesitaba, siempre les estaré agradecido.

Mi dedicatoria también va dirigida a mis amigos y compañeros con los que he compartido gratos momentos en todos estos años de estudio y quienes me supieron brindar su apoyo incondicional para cumplir mis objetivos.

Alexis Vicente Pardo Sánchez

Agradecimiento

Agradezco profundamente mis padres quienes me han apoyado incondicionalmente en cada aspecto de mi vida y siempre han creído en mi y en lo que puedo lograr. Gracias a su ejemplo de perseverancia y esfuerzo he podido darme fuerzas para seguir adelante y triunfar en cada meta que me proyecte; estoy eternamente agradecido por su valiosa ayuda.

Al ing. Marco Suing por su asesoría y ayuda en este sendero del conocimiento, quien supo guiarme hasta lograr cumplir con este proyecto de investigación que representa un nuevo peldaño en mi camino como profesional

También agradezco a mi Universidad por permitirme desarrollar mis conocimientos en la carrera que me apasiona y me motiva a convertir en un gran profesional. De igual manera, le doy gracias a cada uno de mis profesores de la carrera en Ingeniería en Electrónica y Telecomunicaciones, quienes me han inculcado sus saberes y experiencias para lograr formarme como un futuro profesional de la patria.

Alexis Vicente Pardo Sánchez

Índice de Contenidos

Índice de Tablas

Índice de Figuras

Índice de Anexos

Acrónimos

AAAK: Authorization, Authentication and Accounting Key

AES: Advanced Encryption Standard

AP: Access Point

AS: Authentication Server

EAP: Extensible Authentication Protocol

CCM: Counter with Counter Mode Cipher Block Chaining Message Authentication Code

CCMP: CCM Protocol

CSMA: Carrier Sense Multiple Access

CSMA/CA: CSMA / Collision Avoidance

CRC: Cyclic Redundancy Verification

DS: Distribution System

GTK: Group Temporal Key

IEEE: Institute of Electrical and Electronics Engineers

ISM: Industrial, Scientific and Medical Radio Bands

ISP: Internet Service Provider

FCC: Federal Communications Commision

FCS: Frame Check Sequence

LAN: Local Area Network

MAC: Media Access Control

MIMO: Multiple Input – Multiple Output

MU-MIMO: Multiple Users – MIMO

MSK: Master Session Key

OFDMA: Orthogonal Frequency-Division Multiple Access

PMK: Pairwise Master Key

PRSN: Pre-Robust Security Network

PSK: Pre-Shared Key

PTK: Pairwise Transient Key

RADIUS: Remote Authentication Dial-In User Service

RSN: Robust Security Network

QoS: Quality of Service

SAE: Simultaneous Authentication of Equals

SAE-PK: SAE-Public Key

SSID: Service Set Identifier

SSL: Secure Sockets Layer

STA: Station

TKIP: Temporal Key Integrity Protocol

TLS: Transport Layer Security

WEP: Wired Equivalent Privacy

Wi-Fi: Wireless Fidelity

WPA: Wi-Fi Protected Access

WPAN: Wireless Personal Area Network

WLAN: Wireless Local Area Network

WMAN: Wireless Metropolitan Area Network

WWAN: Wireless Wide Area Network

WECA: Wireless Ethernet Compatibility Alliance

1. TÍTULO

Estudio de vulnerabilidades en el sistema de seguridad WPA-2 Personal del estándar IEEE 802.11i y propuestas de mejoras a considerar en el sistema WPA-3

2. RESUMEN

En el presente proyecto de investigación se describe el estudio de las vulnerabilidades del sistema de seguridad WPA-2 de Wi-Fi con el fin de presentar propuestas de mejora que pueden ser implementadas en WPA-3.

La metodología empleada para la evaluación del sistema de seguridad, parte del análisis teórico de la tecnología Wi-Fi y su funcionamiento. Luego se estudian los mecanismos de seguridad que emplea para proporcionar de protección a la red. Posteriormente, se contemplan las vulnerabilidades del sistema de seguridad, y cuales son las amenazas que tiene esta tecnología. Finalmente, se realizan las pruebas experimentales para determinar la existencia de tales aperturas en la seguridad de Wi-Fi y contrastar las fallas que esta tiene. Con base en esta metodología, se tiene una estructura bien fundamentada para el planteamiento de las propuestas.

El propósito de este estudio es determinar que tan seguras son las redes que emplean Wi-Fi como tecnología de acceso. Para evaluar tal parámetro se implemento un escenario cotidiano, el cual asemeja a una red domestica que esta presente en cualquier hogar. Los ataques que se le realizaron a la red fueron controlados de forma que no estropearan los equipos.

Palabras claves: Sistema de Seguridad, WPA-2, IEEE 802.11i.

2.1. ABSTRACT

This research project describes the study of the vulnerabilities of the WPA-2 Wi-Fi security system in order to present proposals for improvement that can be implemented in WPA-3.

The methodology used for the evaluation of the security system starts with a theoretical analysis of Wi-Fi technology and its operation. Then, the security mechanisms used to protect the network are studied. Subsequently, the vulnerabilities of the security system and the threats of this technology are considered. Finally, experimental tests are carried out to determine the existence of such openings in Wi-Fi security and to contrast the failures it has. Based on this methodology, there is a well-founded structure for the approach of the proposals.

The purpose of this study is to determine how secure are the networks that use Wi-Fi as access technology. To evaluate this parameter, an everyday scenario was implemented, which resembles a domestic network that is present in any home. The attacks on the network were controlled so as not to damage the equipment.

Keywords: Security System, WPA-2, IEEE 802.11i.

3. INTRODUCCIÓN

En las redes actuales, la seguridad tiene un papel protagónico, debido a que a cada momento viajan miles de millones de bits de información, por las diferentes redes del mundo, las cuales transportan datos de cualquier índole que necesitan ser protegidos. Por lo que, la necesidad de asegurar las comunicaciones y los datos se hace más evidente.

Wi-Fi es el estándar empleado por dispositivos inalámbricos como routers y Access Points para acceder a Internet dentro de una LAN (Local Area Network, Red de Área Local). Estos equipos son usados en la mayoría de hogares y empresas cuando se requiere una solución para el acceso a Internet sin la necesidad de usar cables, brindando conexión a diferentes dispositivos (end-devices) sin estar anclado a un lugar fijo. También, debido a los constantes desarrollos y mejoramientos de la tecnología Wi-Fi, cada vez ha ido evolucionando, logrando alcanzar velocidades semejantes a las ofrecidas por medios cableados (alrededor de 10 Gbps), manteniendo su característica principal de una comunicación sin cables. Esto la hace una opción más llamativa si se desea establecer conexión dentro de una LAN, y es una de las razones por la cual Wi-Fi podría reemplazar a las conexiones cableadas en un futuro.

En términos de seguridad, Wi-Fi aún no es una tecnología que permita establecer comunicaciones seguras entre los diferentes dispositivos que intervienen en la transmisión y recepción de información. Debido a que por la misma naturaleza del medio (aire) que se emplea para transferir datos, es casi imposible impedir que algún usuario que esté dentro del rango de la señal, no reciba información de la red. Aunque se han implementado diferentes métodos de seguridad a través del estándar 802.11i, que incorpora Wi-Fi, la mayoría de estos pueden ser fácilmente evadidos con las herramientas correctas.

Este tipo de problemas, evidencia la necesidad de investigar cuales son los posibles ataques que la red puede sufrir en caso de que exista un atacante (cracker) que desee obtener información confidencial de la empresa o información personal de un hogar. Por

lo que, es necesario precisar cuáles son las fallas de seguridad que tiene el estándar 802.11i, sus protocolos y los mecanismos que emplea para poder mitigar, y si es posible eliminar, estas vulnerabilidades.

El presente proyecto de investigación se centra en analizar la seguridad en las redes inalámbricas basadas en la tecnología Wi-Fi, como método para proponer soluciones con respecto a sus fallas. El análisis se lo aborda de manera teórica, partiendo de su funcionamiento, y los protocolos que emplea para brindar seguridad; y experimental, probando su seguridad a través de ataques controlados, y observando su comportamiento frente a estos. A través de ambos análisis, se podrá obtener conclusiones acerca de la seguridad ofrecida por este estándar y como podría mejorarse para futuras versiones.

La investigación y el análisis del proyecto, se lo realiza en 4 capítulos los cuáles comienzan desde la recopilación teórica de la tecnología Wi-Fi, el estándar de seguridad 802.11i, y su evolución hasta la actualidad, abordados en el primer capítulo. En el segundo capítulo se plantea la investigación del tipo de vulnerabilidades que existen en el estándar 802.11i, cuáles son las fallas que éste tiene y que métodos se utilizan para mitigar los ataques. Luego en el tercer capítulo, se realiza el análisis teórico y experimental de los ataques indagados en el capítulo anterior, evaluando el software a utilizar para los ataques, los equipos que van a recibir el ataque, y el resultado de esos ataques. Y en el último capítulo, se exponen las conclusiones obtenidas con base a la investigación teórica y los resultados experimentales. En este capítulo también se formulan opiniones acerca de mejoras que se pueden realizar al protocolo WPA-3, que es el último sistema basado en 802.11i.

4. MARCO TEÓRICO

4.1. Redes Inalámbricas

Son redes que se caracterizan por establecer las comunicaciones sin la necesidad de un medio que guíe la información entre los puntos a comunicar. Estas redes emplean las ondas electromagnéticas de los diferentes segmentos en que está dividido el espectro electromagnético, para transmitir la información por la atmósfera, sin utilizar cables. Para la transmisión y recepción inalámbrica, se utilizan antenas (Tanenbaum, 2012).

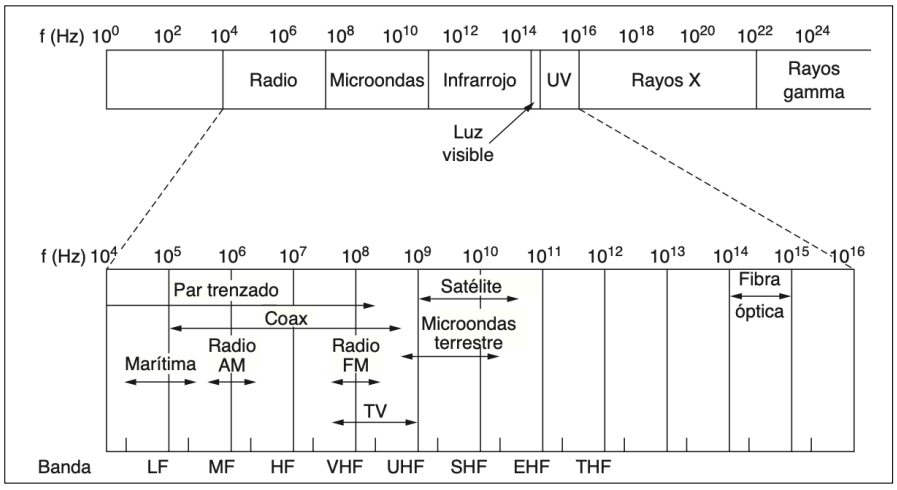


Figura 1: Espectro Electromagnético y su uso en las telecomunicaciones.
Copyright 2012 Redes de Computadoras por Andrew S. Tanenmbaum & David J. Wetherall (Tanenbaum, 2012).

La transferencia de información de forma inalámbrica tiene ciertas propiedades que la hacen una mejor opción frente a la transmisión por medio de redes cableadas. Algunas de estas características son:

- **Movilidad:** Permite el movimiento de los dispositivos conectados dentro de un rango de cobertura de la red, por tanto, no están anclados a un único sitio.

- **Distancia:** Al contrario de los enlaces mediante cables, los enlaces inalámbricos no se limitan a la distancia de un conductor (puesto que no lo utiliza), por lo que, se pueden tener enlaces de decenas o miles de kilómetros como los satelitales.

- **Escalabilidad:** Las redes inalámbricas puede añadir un gran número de dispositivos de cualquier tipo como laptops, smartphones, dispositivos IoT, etc.

- **Flexibilidad:** Las comunicaciones inalámbricas pueden adaptarse a cualquier situación donde se requiera establecer comunicación, por ejemplo: Radioenlaces, Comunicaciones Satelitales, Redes Móviles, Wi-Fi, Bluetooth, Ad-hoc, etc.

- **Practicidad:** La implementación de un enlace inalámbrico no requiere de una planificación compleja, puesto que, solo se necesita que las antenas tengan línea de vista, para que sea factible su comunicación.

(Gupta, 2016)

No obstante, este tipo de redes también son propensas a ciertos problemas que impiden que su funcionamiento sea el óptimo. Las desventajas que presentan estas redes son las siguientes:

- **Seguridad:** Debido a que la transmisión se realiza de manera no guiada, cualquier persona con el dispositivo adecuado puede receptar la información que está viajando por el medio.

- **Rendimiento:** Las condiciones meteorológicas impiden que la red pueda funcionar de manera eficiente, por tanto, su rendimiento podría verse comprometido.

- **QoS (Quality of Service, Calidad del servicio):** La cantidad de errores que presenta este tipo de enlaces, impide que se pueda garantizar un mínimo de servicio para una red.

- **Ancho de Banda:** El ancho de banda en las redes inalámbricas es mucho menor al ofrecido por las redes cableadas.

- **Confiabilidad:** La variabilidad en el rendimiento del enlace por las condiciones meteorológicas y la susceptibilidad a interferencias o atenuaciones por obstáculos del medio, convierten a un enlace inalámbrico en una conexión poco confiable.

- **Coste:** Los costos de mantenimiento de este tipo de redes es elevado, debido al precio de mantenimiento de las antenas y las radio bases que se necesitan.

(Alam & Tariq, 2019)

Las redes inalámbricas son una solución para la mayoría de situaciones donde se requiera establecer de alguna comunicación sin cables. La necesidad de comunicarse mientras se esta en movimiento, ha propiciado el desarrollo de nuevas tecnologías inalámbricas que cumplan está función.

Tabla 1: Tecnologías inalámbricas y sus características.

	WPAN	WLAN	WMAN	WWAN
Tecnología	Bluetooth NFC Zigbee RFID	802.11b 802.11a 802.11n 802.11g 802.11 ac 802.11ax	802.16 802.16a 802.16e	GSM GPRS CDMA 2G 3G 4G
Tasa de Datos	1 a 2 Mbps	11 Mbps a 10 Gbps	> 350 Mbps	10 kbps a 150 Mbps
Rango	Menos de 3m	Menos de 100m	Menos de 50Km	Rango Global
Conectividad	Smartphones, Tablets, Tarjetas Inteligentes, etc.	Smartphones, Tablets, Laptops, Dispositivos IoT, etc	Laptos o Computadores adaptados para esta tecnología.	Smartphones, Tablets, o cualquier equipo compatible con la tarjeta SIM.

Fuente: Autor.

Actualmente, las redes inalámbricas están presentes en casi todas las comunicaciones existentes, debido a los beneficios que proveen. Esto se ve reflejado en las dos tecnologías inalámbricas más populares del mercado: Las redes móviles y la red Wi-Fi.

4.2. IEEE 802.11x

El estándar que destaca dentro de las redes LAN inalámbricas, es IEEE 802.11, comercialmente conocido como Wi-Fi. Esta tecnología es la evolución de la red ALOHANET, puesto que hereda y mejora características como: La conmutación de paquetes, El método de contención CSMA (Carrier Sense Multiple Access, Acceso Múltiple por Detección de Portadora) para evitar colisiones (CSMA/CA)

(CSMA/Collision Avoidance, CSMA/Prevención de Colisiones), Mejoras en la división del ancho de banda, Inclusión de Protocolos de seguridad, entre otras.

Wi-Fi se fundamenta en el uso de las frecuencias que se encuentran distribuidas en el rango denominado bandas ISM[1], que fueron autorizadas para su uso público por la FCC en 1985 (Couch, 2008).

Estas bandas representan una opción atractiva para los fabricantes, puesto que no se requiere de títulos habilitantes para hacer uso de tales frecuencias. En el Ecuador también se adopta esta normativa para las bandas ISM, las cuales no requieren de permisos legales para su uso. Esta banda es muy utilizada en el país, para el despliegue de tecnologías de telecomunicaciones para el hogar como Wi-Fi y Bluetooth; aunque también son empleadas en muchos proyectos que requieren de comunicaciones de forma inalámbrica gratuita.

[1] Las bandas ISM también denominadas bandas no licenciadas, no requieren de un titulo habilitantes para hace uso de ellas. Estas bandas trabajan en las frecuencias de 902-928 MHz, 2.4-2.4835 GHz y 5GHz.

Tabla 2: Versiones y Bandas de Wi-Fi

Versión	Año	Banda de Frecuencia	Tasa de Datos
802.11	1997	2.4 GHz	2 Mbps
802.11a	1999	5 GHz	54 Mbps
802.11b	1999	2.4 GHz	11 Mbps
802.11g	2003	2.4 GHz	54 Mbps
802.11n (Wi-Fi 4)	2009	2.4 GHz y 5 GHz	600 Mbps
802.11ac (Wi-Fi 5) Banda 1	2013	2.4 GHz	1 Gbps
802.11ac (Wi-Fi 5) Banda 2	2016	5 GHz	> 1 Gbps
802.11 ax (Wi-Fi 6)	2019	2.4 GHz y 5 GHz	2.4 Gbps

Nota: Recuperado de Intel Diferentes protocolos de Wi-Fi y velocidades de datos (Intel, 2020).

La posibilidad de utilizar esa parte del espectro radioeléctrico, permitió que compañías del campo de telecomunicaciones puedan crear equipos comerciales que trabajen en un mismo rango de frecuencias. Debido a esto, empresas como 3com, Lucent o Nokia, en 1999, se unieron para formar un grupo de investigación llamado WECA[2], cuyo propósito era el diseño, desarrollo y evolución de una tecnología inalámbrica que tenga compatibilidad con diferentes dispositivos de diversos fabricantes (Hiertz et al., 2010).

El resultado de la investigación y desarrollo de una tecnología inalámbrica para las redes LAN, fue el estándar IEEE 802.11; el cual introdujo una nueva forma de transmitir información dentro de oficinas y hogares, sin utilizar cables. IEEE 802.11

[2] Posteriormente se denominaría Wi-Fi Alliance.

comenzó con tasas de transmisión de 1 a 2 Mbps, lo que para la época era una tasa de transmisión regular, puesto que la Ethernet Clásica alcanzaba 10 Mbps, sin embargo, la característica de poder transmitir datos sin estar limitado a un solo lugar, marcó el inicio para mejores versiones en el futuro. Sumado a esto, en abril del 2000, el grupo WECA certificó la interoperabilidad de la versión 802.11b (versión comercial que se conoce como Wi-Fi). Esta certificación posibilita que cualquier dispositivo compatible con Wi-Fi pueda conectarse a la red, independientemente del fabricante del equipo (Hiertz et al., 2010).

Las características que definen a IEEE 802.11Wi-Fi, según la IEEE son:

- El uso del medio (aire) no tiene un rango máximo de funcionamiento, sin embargo, se conoce que las STA fuera de su cobertura no pueden recibir tramas.

- Cada comunicación establecida está expuesta a otras comunicaciones que se produzcan en el medio.

- El medio empleado en IEEE 802.11 (aire) no es tan fiable como el medio de las redes cableadas.

- Tiene topologías cambiantes, debido a la movilidad que tienen los dispositivos.

- Las STAs no pasan conectadas todo el tiempo, por lo que se entiende que algunas STAs pueden estar ocultas.

- Las propiedades de propagación son variables y asimétricas.

- Las comunicaciones de una red IEEE 802.11 pueden sufrir interferencias de otras redes similares, que trabajan en zonas superpuestas.

(IEEE Computer Society, 2012a)

Actualmente, Wi-Fi se mantiene como la tecnología predilecta para brindar conexión a Internet de forma inalámbrica dentro de la LAN. Aunque no es la única que existe, es la que constantemente se sigue mejorando.

En sus últimas versiones, se logró aumentar su velocidad, ancho de banda y su seguridad con el fin de equipar a las características de las redes cableadas. Su constante mejoramiento puede resultar que en un futuro pueda sustituirlas, al menos dentro de la LAN; aunque este objetivo está lejos de lograrse por motivos de ancho de banda y seguridad.

4.2.1. Trama Wi-Fi

La trama Wi-Fi se compone de 9 apartados que están divididos con base en la información de Control, Tamaño, Dirección, Datos y el CRC (Cyclic Redundancy Verification, Verificación de Redundancia Cíclica) del paquete recibido de la capa superior. Estos segmentos permiten organizar la información referente a donde se debe enviar la trama, que información contiene y si la trama tiene errores.

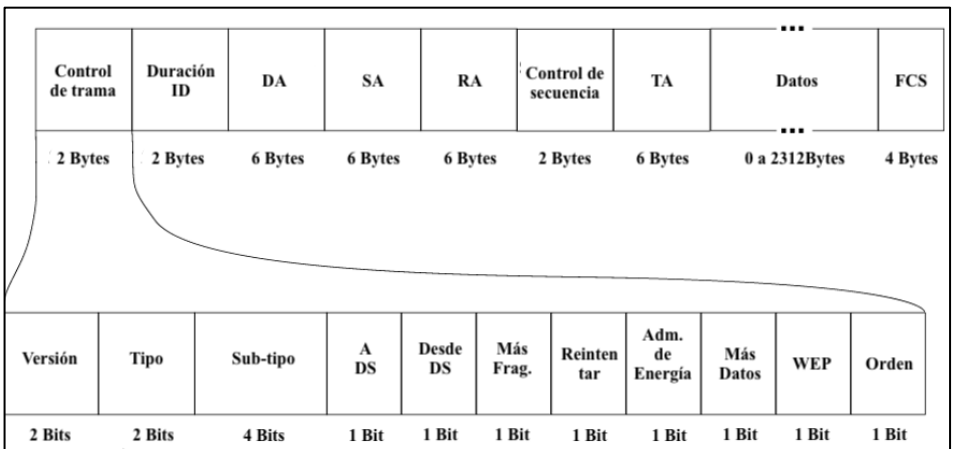


Figura 2: Formato de la trama de IEEE 802.11.
Copyright Finding Datatypes for 802.11 frame por Stackoverflow (Stack Overflow, 2020).

Los 9 apartados que componen la trama Wi-Fi son:

- Control de trama: Identifica el tipo de trama inalámbrica.
  - Versión: Versión de la trama IEEE 802.11
  - Tipo y Subtipo: Indica si la función de la trama es: Control, Datos y Administración
  - A DS: Se establece un 1 para las tramas destinadas al sistema de distribución (Dispositivos en la estructura inalámbrica).
  - Desde DS: Se establece un 1 para las tramas provenientes del sistema de distribución.
  - Más Fragmentos: Se establece en 1 para tramas que tienen otro fragmento.
  - Reintentar: Se establece en 1 si la trama es una retransmisión de la anterior.
  - Administración de Energía: Se establece en 1 para indicar que uno estará en modo ahorro de energía.
  - Más datos: Se establece en 1 para indicar que un nodo que esta en modo ahorro de energía, almacenará más tramas en el búfer.
  - WEP (Wired Equivalent Privacy, Privacidad Equivalente por Cable): Se establece en 1 para indicar que la trama tiene información encriptada por WEP.
  - Orden: Se establece en 1 para indicar que la clase de servicio esta "Estrictamente Ordenada".

- Duración / ID: Representa el tiempo que requiere para transmitir la trama. El tiempo se mide en microsegundos.

- Dirección de Destino (DA): Contiene la dirección MAC (Media Access Control, Control de Acceso al Medio) del nodo de destino final en la red.

- Dirección de Origen (SA): Contiene la dirección MAC del nodo que generó la trama.

- Dirección del Receptor (RA): Contiene la dirección MAC del destinatario inmediato de la trama.

- Control de Secuencia: Indica el número de secuencia asignado a la trama. Las tramas retransmitidas se indican con números de secuencia duplicados.

- Dirección de Transmisión (TA): Contiene la dirección MAC del dispositivo inalámbrico que transmitió la trama.

- Datos / Carga Útil: Contiene la información del usuario. En este campo está contenido el paquete IP.

- FCS (Frame Check Sequence, Secuencia de Comprobación de tramas): Contiene una comprobación de redundancia cíclica (CRC) de 32 bits de la trama.

(Cisco Community, 2020)

4.2.2. Funcionamiento

Al ser una tecnología de acceso inalámbrico, requiere de métodos especiales para asociar a los dispositivos o estaciones (STA), que quieran pertenecer a la red. Esto implica que, dentro de su arquitectura debe incorporar un proceso para que distintos equipos se conecten a la red, sin importar el lugar en el que se encuentren; siempre que estén dentro del su rango de cobertura.

El dispositivo de red inalámbrico da conocer la red a los STA mediante el envió de tramas baliza o beacons[3]. Por medio de estos mensajes, el AP (Access Point, Punto de Acceso) notifica de la presencia de la red a los dispositivos que están dentro de su rango (AlQahtani et al., 2020). En la trama beacon el AP envía información sobre el nombre de la red SSID, su dirección MAC y el sistema de seguridad que emplea.

[3] Las tramas baliza o beacons son tramas de administración que contienen toda la información de la red inálambrica. Estas tramas se envían constantemente. Para ampliar información revisar: https://www.researchgate.net/publication/348778593_BF2FA_Beacon_Frame_Two-factor_Authentication/link/60eb2eb80fbf460db8fd93cb/download

Los 3 procesos más importantes dentro de la arquitectura de IEEE 802.11 para el proceso de establecimiento de la conexión y desconexión, son los siguientes:

4.2.2.1. Asociación

Este proceso busca identificar una STA que requiere asociarse con el AP de la red. Debido a que el dispositivo de red expone su identidad hacia los dispositivos cercanos, por medio de la propagación de su SSID[4] (Service Set Identifier, Identificador del conjunto de servicios), cualquier dispositivo que este dentro de su rango, podrá detectarlo (IEEE Computer Society, 2004c).

El proceso de asociación siempre inicia cuando el STA envía un mensaje de petición hacia el dispositivo de red, solicitando que se le conceda el acceso a la red. Entonces, la decisión de permitir su acceso, recae directamente en el dispositivo de red, si no se ha configurado un servidor de autenticación externo. Por esta razón este dispositivo tiene implementado mecanismos de autenticación para impedir que equipos ajenos a un grupo de trabajo puedan ingresar.

La asociación se puede producir varias veces y de distintos dispositivos; esto es porque el dispositivo de acceso es el equipo encargado de proporcionar conexión a Internet a un considerable número de STAs. Entonces la necesidad de gestionar y controlar la asociación, tiene mayor relevancia en estas redes.

4.2.2.2. Re-Asociación

La re-asociación es un servicio propio de las redes inalámbricas, en la cual se proporciona el paso entre dispositivos de red manteniendo el acceso a Internet. Este proceso es similar al "Handover[5] o Traspaso" de las redes celulares, con la diferencia

[4] Service Set Identifier o Identificador del conjunto de servicios, es una secuencia de 32 bits empleada para identificar la red. Se podría denominar como el nombre de la red.
[5] Sistema utilizado en la telefonía celular que permite cambiar o "pasar" entre celdas sin perder el servicio y siendo totalmente imperceptible para el usuario.

de que las redes celulares tienen un mayor rango de cobertura. Además, para que se produzca tal traspaso los dispositivos de red deben pertenecer a la misma red interna, puesto que cada red tiene sus propias políticas de acceso (IEEE Computer Society, 2004c).

Esta capacidad de conservar la conexión aún cuando se sale del rango de una red y se llega a otra, también tiene sus limitaciones, las cuales son impuestas por temas de seguridad. En las redes seguras no se puede permitir que se realice un traspaso, sin primero haber confirmado la identidad del dispositivo que desea conectarse. Por tanto, el traspaso de una red a otra, no garantiza la conexión, aun si este pertenece a la misma red. Por lo que, para que una STA se conecte al otro dispositivo de red, nuevamente debe iniciar el proceso de asociación.

4.2.2.3. Des-Asociación

La des-asociación es el proceso contrario a la asociación, esta consiste en que una STA envía un aviso al dispositivo de red para terminar la conexión previamente establecida. Aunque la asociación se pueda definir como un proceso porque sigue una serie de pasos para permitir una conexión; la des-asociación no lo es, debido a que la STA solo notifica al dispositivo sobre la elección de finalizar la comunicación, por tanto, el dispositivo de red no puede negociar ni impedir tal requerimiento (IEEE Computer Society, 2004c).

4.2.3. Dispositivos Inalámbricos

El dispositivo de red empleado en las redes Wi-Fi para brindar acceso a Internet, se conoce como AP (Access Point, Punto de Acceso), aunque también se puede utilizar un router inalámbrico, pero no son iguales. Estos se diferencian principalmente en las conexiones físicas, debido a que el AP solo cuenta con una entrada RJ45 para conectarse a Internet; mientras que el Router Inalámbrico, puede tener más entradas RJ45 y una conexión directa con el ISP (Internet Service Provider, Proveedor del

Servicio de Internet). Sin embargo, ambos cuentan con la capacidad de brindar acceso a Internet de forma inalámbrica (CCNA desde Cero, 2018).

Una red básica de Wi-Fi también llamada BSS (Basic Service Set, Conjunto de Servicios Básicos) se compone principalmente de 3 elementos: Los STA o dispositivos finales, el Access Point (AP) y la Puerta de enlace (Gateway). Aunque actualmente los dispositivos AP y Gateway se pueden encontrar unificados en una sola entidad llamada Router Inalámbrico (Rawat et al., 2014).

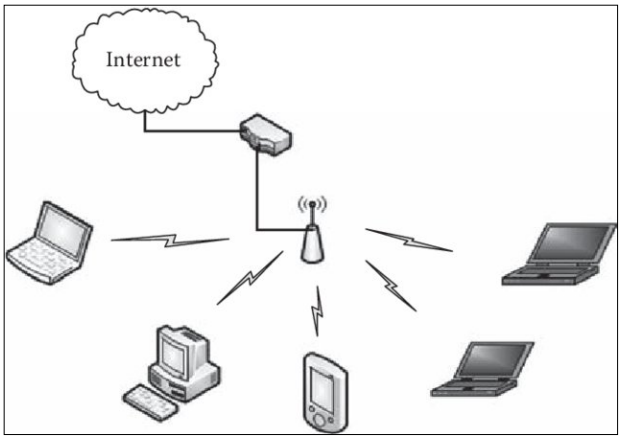


Figura 3: Estructura básica de una red Wi-Fi o BSS (Conjunto de Servicios Básicos).
Copyright Wireless Network Security: An Overview por Danda B Rawat (Rawat et al., 2014).

El propósito del AP es proporcionar de acceso inalámbrico a dispositivos como smartphones, laptops tablets, sensores, etc. Mientras que el Gateway se encarga de encaminar el tráfico generado por los dispositivos o STAs hacia el Internet.

El AP y el Router Inalámbrico incorporan antenas omnidireccionales, para que la señal emitida pueda cubrir la mayoría del área. De esta forma se tiene un mayor rango para que las STA se puedan conectar a la red. Además, debido a que dispositivos van a competir por el medio, se necesita multiplexar el canal mediante distintas técnicas, para que exista eficiencia en el uso del ancho de banda, y se pueda asignar a cada usuario una parte de este.

4.2.4. Modo de transmisión

Un aspecto importante, dentro de la tecnología Wi-Fi, es que la comunicación que se produce entre el emisor y el receptor es Half-Duplex. Es decir, que solo se puede transmitir o recibir a la vez. Esto se debe a la técnica empleada por Wi-Fi para evitar que se produzcan colisiones que interrumpieran la transmisión de datos de todos los usuarios. Esta técnica se conoce como CSMA/CA, la cual consiste en notificar a los demás APs que va a iniciar una transmisión, de esta manera se evita que existan colisiones. Esta técnica es heredada de la antigua red ALOHANET.

Considerando que la naturaleza de la conexión es inalámbrica, es casi imposible tener control sobre todas las comunicaciones, por lo que, si existe una colisión entre alguno de los paquetes que se envían, todas las comunicaciones que se estén realizando en ese momento se deberán suspender momentáneamente hasta resolver la falla. Por tal motivo es que se notifica a los demás AP o Routers Inalámbricos que se va a establecer una comunicación con una STA específica, y por tanto los demás no deben transmitir. Además, cuando existe un número elevado de usuarios conectados a la red, el tiempo de respuesta aumenta, causando retardos (delays) más elevados. Esto también provoca que el servicio colapse o que sufra caídas debido al excesivo ancho de banda utilizado por un usuario.

Debido a esto es que los AP o los Routers Inalámbricos implementan nuevas técnicas para el acceso de múltiples usuarios. Algunas de estas técnicas son las tecnologías MIMO (Multiple Input – Multiple Output, Múltiples Entradas – Múltiples Salidas) y MU-MIMO[6] (Multiple Users – MIMO, Múltiples Usuarios - MIMO), que se emplean para aumentar la eficiencia del espectro empleado para transmitir y recibir información, valiéndose del efecto de la propagación multi-camino.

[6] MIMO y MU-MIMO son tecnologías desarrolladas para comunicar diversos dispositivos de manera simultanea, mediante el uso de conjunto de múltiples antenas (Lynksys, 2017).

4.2.5. Versiones

Actualmente Wi-Fi ha sido tan popular dentro de las redes LAN, que se han desarrollados muchos estándares que mejoran las características del 802.11b original. La mayoría de los estándares 802.11 están diseñados para mejorar la eficiencia de Wi-Fi y aumentar su rango de cobertura. En la tabla 3 se resumen algunas de las versiones de este estándar, que han sido desarrolladas.

Tabla 3: Resumen de estándares IEEE 802.11

Estándar	Ámbito de aplicación
IEEE 802.11	Control de acceso al medio (MAC): Una MAC común para las aplicaciones WLAN Capa física: Infrarrojos a 1 y 2 Mbps Capa física: FHSS (Espectro ensanchado por salto de frecuencia) de 2,4 GHz a 1 y 2 Mbps Capa física: DSSS (Espectro ensanchado por secuencia directa) de 2,4 GHz a 1 y 2 Mbps
IEEE 802.11a	Capa física: OFDM de 5 GHz a velocidades de 6 a 54 Mbps
IEEE 802.11b	Capa física: DSSS de 2,4 GHz a 5,5 y 11 Mbps
IEEE 802.11c	Funcionamiento del puente en la capa MAC de 802.11
IEEE 802.11d	Capa física: Ampliar el funcionamiento de las WLAN 802.11 a nuevos dominios normativos (países)
IEEE 802.11e	MAC: Mejora de la calidad del servicio y de los mecanismos de seguridad
IEEE 802.11f	Prácticas recomendadas para la interoperabilidad de puntos de acceso de varios proveedores
IEEE 802.11g	Capa física: Ampliar 802.11b a velocidades de datos > 20 Mbps
IEEE 802.11h	Físico/MAC: Mejora de IEEE 802.11a para añadir la selección de canales en interiores y exteriores y para mejorar la gestión del espectro y la potencia de transmisión
IEEE 802.11i	MAC: Mejorar los mecanismos de seguridad y autenticación

IEEE 802.11j	Físico: Mejora de IEEE 802.11a para ajustarse a los requisitos japoneses
IEEE 802.11k	Mejoras en la medición de recursos radioeléctricos para proporcionar una interfaz a las capas superiores para las mediciones de radio y red
IEEE 802.11m	Mantenimiento de la norma IEEE 802.11-1999 con correcciones técnicas y de redacción
IEEE 802.11n	Físico/MAC: Mejoras para permitir un mayor rendimiento
IEEE 802.11p	Físico/MAC: Acceso inalámbrico en entornos vehiculares
IEEE 802.11r	Físico/MAC: Itinerancia rápida (transición rápida de BSS)
IEEE 802.11s	Físico/MAC: Red de malla ESS
IEEE 802.11,2	Práctica recomendada para la evaluación del rendimiento inalámbrico 802.11
IEEE 802.11u	Físico/MAC: Inter-funcionamiento con redes externas
IEEE 802.11v	MAC: Gestión de estaciones de forma centralizada o distribuida.
IEEE 802.11w	Similar al 802.11i. Se encarga de proteger a la red de ataques de tramas de gestión.
IEEE 802.11ac	Físico/MAC: Mejoras para permitir un mayor rendimiento. Se alcanza velocidades de 1.3 Gbps y se trabaja en la banda de 5 GHz. Se lo conoce comercialmente como Wi-Fi 5
IEEE 802.11ax	Físico/MAC: Se trabaja en las bandas de 2,4 GHz y 5 GHz e incluso se propone trabajar en la banda de 6 GHz. Introduce la modulación OFDMA. Se lo conoce comercialmente como Wi-Fi 6

Resumen de estándares IEEE 802.11 que muestran las diferentes ramas en las que el estándar ha sido desarrollado. Nota. Recuperado de Data and Computer Communications Octava Edición. Copyright 1985 por William Stallings (Stallings, 2011).

4.2.5.1. 802.11ax (Wi-Fi 6)

La versión actual de Wi-Fi es IEEE 802.11ax, comercialmente conocida como Wi-Fi 6. En esta versión se mejoran las características de la versión anterior introduciendo un nuevo mecanismo de acceso a la red, ampliación del ancho de banda, modo de ahorro de energía, entre otras.

Este estándar puede utilizar las bandas de 2,4 GHz y 5GHz, pero también se propone extender el espectro utilizado hasta la banda de los 6 GHz, permitiendo un aumento en el ancho de banda. También introduce el concepto de OFDMA[7](Orthogonal Frequency-Division Multiple Access, Acceso múltiple por división de frecuencia ortogonal) que permite una mejor eficiencia en el uso de espectro de la señal, y la cual, combinada con la tecnología MU-MIMO permite una comunicación simultanea entre el transmisor y el receptor (Wi-Fi Alliance, 2020c).

Wi-Fi 6 también mejora la seguridad de la red, puesto que implementa la nueva versión del mecanismo WPA-3 que pretende mitigar las fallas de la versión anterior WPA-2, mediante nuevos métodos de seguridad que pueden suplir tales deficiencias (Wi-Fi Alliance, 2020b). Sin embargo, estudios actuales demuestran que el protocolo aún mantiene las mismas vulnerabilidades que sus predecesores. El estudio de este mecanismo se lo realizará en temas posteriores.

4.2.6. Seguridad

La popularidad que ha tenido Wi-Fi, ha posibilitado que este implementada en la mayoría de lugares, donde se necesita proveer de acceso a un gran número de equipos. Esta tecnología está presente en la mayoría de hogares, parques, centros comerciales,

[7] OFDMA es una tecnología introducida en Wi-Fi 6 para mejorar el rendimiento de la red inalámbrica estableciendo sub-portadoras de modulación independiente dentro de las frecuencias. De esta manera se logra la división del ancho de banda en paquetes individuales para cada usuario (Cisco, 2019).

oficinas, hospitales, etc. Lugares en los que generalmente acuden cientos de personas para utilizar tal tecnología para acceder a Internet.

Mediante el AP o Router Inalámbrico, se pueden brindar un acceso múltiple a través de tecnologías como MIMO o MU-MIMO. Las cuales se ven complementadas por técnicas como OFDMA para optimizar el ancho de banda, permitiendo así, que más dispositivos se conecten a la red. Sin embargo, la función más importante que incorpora Wi-Fi, es la seguridad, a través del estándar 802.11i, el cual está diseñado específicamente para proveer de protección a estas redes.

Actualmente se cuenta con dos tipos de redes seguras implementadas en las redes Wi-Fi, estas son: PRSN (Pre-Robust Security Network, Red de Seguridad Previa) y RSN (Robust Security Network, Red de Seguridad Robusta) (Sithirasenan & Muthukkumarasamy, 2014). El esquema de clasificación mencionado se muestra en la figura 4.

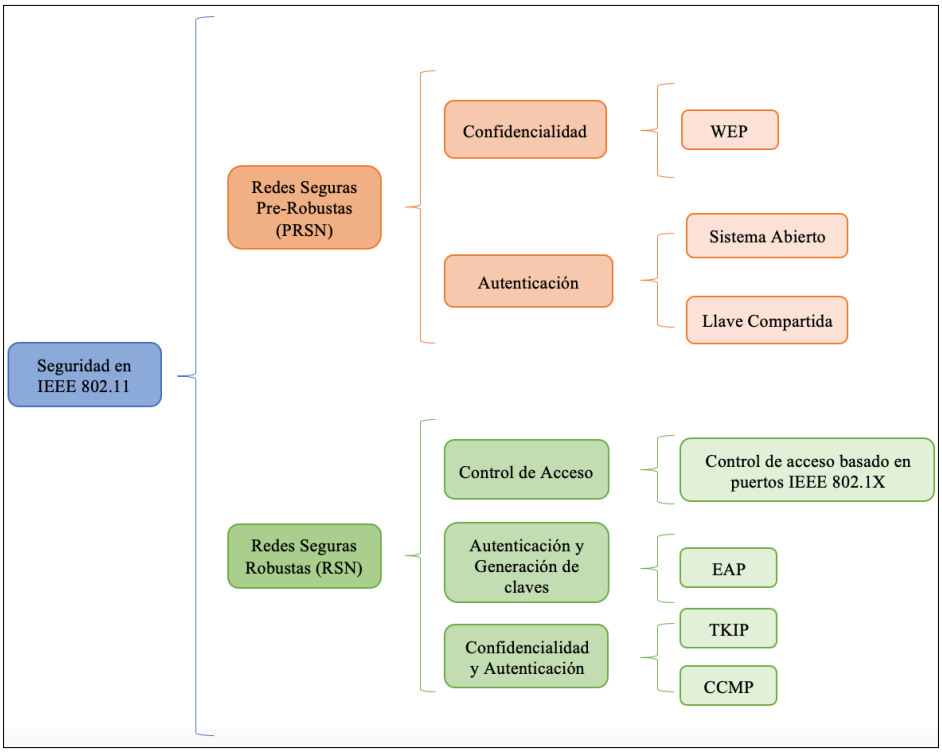


Figura 4: Clasificación de la seguridad en IEEE 802.11.
Copyright 2007 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i por Sheila Frankel, Bernard Eydt, Les Owens y Karen Scarfone (Frankel et al., 2007c).

Dentro de la RSN está especificada la enmienda IEEE 802.11i, en la cual se definen y se detallan los nuevos métodos empleados para proteger las redes inalámbricas. Esta normativa supone una evolución respecto a las redes PRSN.

Mediante el estándar IEEE 802.11i, Wi-Fi provee las herramientas y mecanismos necesarios para proteger la red de intrusos que intentan obtener la información para fines maliciosos. Puesto que existen muchos mecanismos que este estándar incorpora, este estudio se centrara en las versiones más actuales, porque son las que están implementadas en todos los equipos actuales.

4.3. IEEE 802.11i

IEEE 802.11i es la enmienda diseñada por la IEEE para proveer de seguridad a las redes inalámbricas. El propósito para el que fue creado este estándar fue el de reemplazar a las redes que emplean WEP como sistema de seguridad. Las deficiencias encontradas en WEP, abrieron un nuevo campo para el estudio de nuevos métodos de seguridad que debían implementarse en las redes IEEE 802.11.

Los constantes esfuerzos de la IEEE para mejorar la protección de las redes WLAN, propiciaron la creación de nuevas técnicas de cifrado y autenticación. Este conjunto de técnicas desarrolladas para sustituir las utilizadas en WEP se establecen y detallan en 802.11i. Sin embargo, la IEEE no es la única organización que se dedica al mejoramiento de las redes inalámbricas locales.

La Wi-Fi Alliance (anteriormente conocida como WECA) también contribuye en el mejoramiento de las redes Wi-Fi. Su función como alianza es garantizar la interoperabilidad de Wi-Fi en todos sus dispositivos, por tanto, se enfoca en implementar un mecanismo común que brinde de seguridad a la red, este mecanismo se denomina WPA (Wi-Fi Access Protected, Acceso Wi-Fi Protegido). El análisis de este mecanismo se realizará posteriormente.

Después de determinar que WEP ya no era un método seguro para las redes WLAN, este se reemplazó por WPA como una solución temporal. Además, este nuevo método de seguridad, se basaba completamente en las técnicas establecidas en IEEE 802.11i. Es por eso que a IEEE 802.11i se la confunda como un protocolo o una suite de protocolos, más que una enmienda.

No obstante, el mejoramiento de IEEE 802.11i supone el avance de la seguridad en las redes Wi-Fi. Toda red IEEE 802.11 se basa en la estructura propuesta en la enmienda, puesto que constituye el núcleo de las redes actuales.

La columna vertebral de la estructura de IEEE 802.11i se basa en tres parámetros importantes: El algoritmo CCMP (CCM Protocol, Protocolo CCM), el handshake de 4 vías y la normativa IEEE 802.1X. Estos tres métodos de seguridad componen lo que se conoce como Red de Seguridad Robusta o RSN (Frankel et al., 2007d).

4.4. Redes de Seguridad Robusta (RSN)

Las redes RSN se definen como redes inalámbricas seguras que se pueden agrupar con otras redes similares, formando Asociaciones de Red de Seguridad Robusta o RSNA.

"Una RSNA es una conexión lógica entre entidades IEEE 802.11 que se comunican y que se establece a través del esquema de gestión de claves IEEE 802.11i, denominado 4-Way Handshake, que es un protocolo que valida que ambas entidades compartan una clave maestra por pares (PMK)(Pairwise Master Key, Llave Maestra por Parejas), sincroniza la instalación de claves temporales y confirma la selección y configuración de los protocolos de confidencialidad e integridad de datos."(Frankel et al., 2007c).

Las RSNA tienen ciertas características que mejorar la seguridad dentro de las redes inalámbricas, estas son:

- Mecanismos de autenticación mejorados.
- Gestión de Claves Criptográficas.
- Confidencialidad de los datos.
- Autenticación e Integridad del origen de los datos.
- Protección de repetición.

Tales propiedades se basan en el estándar IEEE 802.1X para proporcionar de autenticación y encriptación a las redes RSNA. Esto se debe a que dentro de la estructura de IEEE 802.11, las tramas están diseñadas con un campo de autenticación de terminales. Este campo se emplea para asociar el dispositivo con un DS (Distribution System, Sistema de Distribución) debido al control de direcciones MAC

que se emplea para acceder a la red. El estudio del funcionamiento de 802.1X se lo realiza más adelante.

4.4.1. Jerarquía y Distribución de Claves

Russell y Gangemi en la RFC 2828 definen que la gestión de claves es "el proceso de manipulación y control de las claves criptográficas y el material relacionado (como los valores de inicialización) durante su ciclo de vida en un sistema criptográfico, incluyendo el pedido, la generación la distribución, el almacenamiento, la carga, la custodia, el archivo, la auditoría y la destrucción del material." (Russell & Gangemi, 1991).

La gestión de las claves facilita la organización sobre que métodos de cifrado se utilizarán para la encriptación de datos. La adecuada administración de estas claves, permite diseñar un sistema seguro dentro de la red. Para lograr que el sistema sea lo más seguro posible, las claves deben cumplir los siguientes requisitos:

- Se deben generar de manera aleatoria, para reducir la probabilidad de reproducción por parte de usuarios externos.

- Es necesario que tengan un tiempo de uso, es decir, que se cambien las claves con frecuencia, para impedir filtrado de claves.

- Deben estar encriptadas en todo momento, ya sea cuando están almacenadas en los dispositivos o cuando se transmiten.

- Obligatoriamente tienen que ser eliminadas cuando su uso ya no sea necesario. Esto imposibilita que puedan ser nuevamente usadas, en otro proceso de autenticación.

Estos requisitos se basan en mejorar el sistema de seguridad de las redes PRSNA que usan WEP. A diferencia de un conjunto de claves comunes que se repartían a todos los dispositivos de la red, en RSN se busca una distribución de claves únicas y caducables (temporales), para evitar su clonación.

En las redes RSNA se cuenta con una clave dedicada para funciones como cifrado, autenticación e integridad. Estas claves pueden trabajar en conjunto para realizar una misma acción, es decir, las claves se relacionan así mismas en base a una función. Por tal motivo es que se implementa una estructura jerárquica en la red, de manera que se pueda tener una correcta gestión en el uso de estas claves.

La distribución de las claves en las redes RSNA se basan en las jerarquías descritas en IEEE 802.11i. El propósito de implementar este tipo de estructura dentro de la gestión de claves es para agregar capas de seguridad en toda la red, y agrupar las funciones que guardan relación.

En IEEE 802.11i se describen dos tipos de jerarquía de claves que se fundamentan en el tráfico de la red, siendo estas: Jerarquía de Claves por Pares (Pair Key Hierarchy) para el tráfico del tipo unidifusión; y Jerarquía de Claves de Grupo (Group Key Hierarchy) para el tráfico del tipo difusión.

4.4.1.1. Jerarquía de Claves por Pares

En la Jerarquía de Claves por Pares se parte de dos claves maestras denominadas claves raíz. En las redes RSN a las llaves maestras se las denomina PMK. Las claves raíz son utilizadas como base para generar otras claves para las funciones de integridad y confidencialidad.

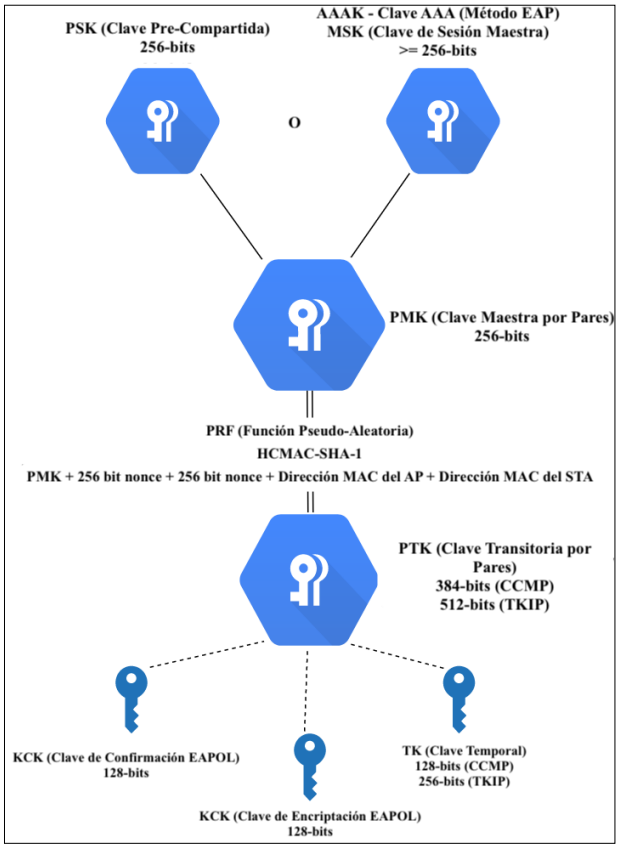


Figura 5: Estructura de la Jerarquía de Claves por Pares.

Como se observa en la figura 5, la clave maestra PMK se puede calcular por medio de dos métodos: El primero consiste en que cada dispositivo tenga configurada la clave de antemano, de modo que, en el proceso de asociación, todas cuenten con ella; este método se conoce como PSK.

Por otro lado, se puede obtener la PMK mediante la clave AAA (Authorization, Authentication and Accounting, Autorización, Autenticación y Registro), también conocida como MSK (Master Session Key, Clave de la Sesión Maestra). Esta consiste en distribuir la clave a través del AP utilizando el protocolo EAP (Extensible Authentication Protocol, Protocolo de Autenticación Extensible), cada vez que un usuario desea conectarse a la red.

La PMK es la llave maestra utilizada para generar la PTK. Para esto, se requiere la PMK, las direcciones MAC de la STA y el AP; y los nonces[8] que estos crean de manera aleatoria en el proceso de crear las claves. Utilizar las direcciones MAC para producir la PTK, imposibilita que exista suplantación de identidad y por ende secuestro de sesión. Además, mediante los nonces, se proporciona información aleatoria que reduce la posibilidad de reproducir la clave.

Para producir la PTK se requiere del algoritmo PRF (Pseudo-Random Function, Función Pseudo-Aleatoria). Este algoritmo, utiliza el código HMAC-SHA-1[9]con las siguientes entradas:

- PMK
- 2 Nonces de 256 bits
- Direcciones MAC del AP y de la STA

El objetivo de PRF es generar claves de longitudes de 128, 192, 256, 384 y 512 bits; que se emplean para la seguridad de IEEE 802.11. Una de las llaves que se crean a partir del cálculo de la función PRF, es la clave PTK.

De la PTK se derivan tres llaves que están diseñadas para proveer de integridad, confidencialidad y autenticación a la red. Las claves que se derivan de PTK son:

- **EAPOL (EAP over LAN, EAP sobre LAN) – KCK (Key Confirmation Key, Clave de Confirmación:** Empleada para brindar de integridad y autenticidad a las tramas de control que van desde la STA al AP, durante el proceso de asociación de las redes RSNA.
- **EAPOL – KEK (Key Encryption Key, Clave de Encriptación):** Esta se encarga de proteger la confidencialidad de las claves y de otros datos utilizados en los procesos de la RSN (Frankel et al., 2007d)

[8] Número aleatorio generado por protocolos o mecanismos de seguridad.
[9] Código de Autenticación de mensajes en clave Hash.

- **TK (Temporal Key, Clave Temporal):** Utilizada para proteger el tráfico proveniente de la STA.

Existen diferentes protocolos criptográficos utilizados para cifrar las claves, y la información que estas contienen. Los dos protocolos que generalmente se emplean son TKIP (Temporal Key Integrity Protocol, Protocolo de Integridad de la Clave Temporal) y CCMP.

4.4.1.2. Jerarquía de Claves de Grupo

La Jerarquía de Grupos se basa en emplear una sola clave para todos los procesos de seguridad. La clave empleada es la GTK (Group Temporal Key, Clave de Grupo Temporal). La GTK es creada por el AP y luego la distribuye a las STAs asociadas.

A pesar de que no exista un proceso definido para la creación de la GMK, en la IEEE 802.11i se establece que debe ser una clave aleatoria.

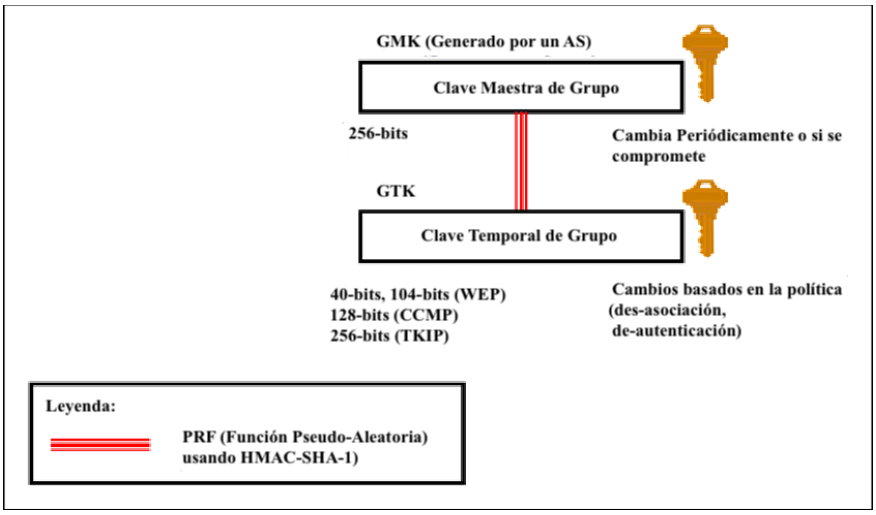


Figura 6: Clave Maestra de Grupo.

4.4.2. Claves

4.4.2.1. Pre-Shared Key (PSK)

El mecanismo PSK consiste en el uso de una clave que se debe implementar en cada dispositivo que interviene en una comunicación IEEE 802.11 (APs y las STAs). En la práctica, existe un AS (Authentication Server, Servidor de Autenticación) que provee de las claves al AP.

Su funcionamiento consiste en que antes de comenzar con el proceso de asociación, cada dispositivo debe contar una clave que debe ser larga y compleja, de tal manera que no pueda ser replicada. Una vez que tales claves se confirman con el AP, se puede empezar a generar tráfico por parte del usuario.

El método para crear las claves PSK es indistinto, puesto que se pueden emplear algoritmos criptográfico generadores, o el uso de una contraseña creada por el usuario. El propósito es impedir que usuarios extraños a la red puedan conocer tal clave para acceder. En caso de que este escenario suceda, se debe realizar de nuevo el mismo proceso, pero con una contraseña diferente. Es por eso, que tal clave debe ser lo más compleja posible. Además, debido a que en IEEE 802.11 no se establece como debe ser la creación ni la distribución de PSK, la elección de la seguridad de la contraseña queda a decisión del administrador de la red o del que la implemente (Jeon et al., 2017).

La importancia de crear una buena clave, determina el grado de vulnerabilidad que puede tener la red. De manera que un correcto diseño de contraseñas puede bloquear el paso a usuarios maliciosos. Sumado a esto, es que, en redes de gran tamaño, se vuelve poco rentable diseñar una contraseña por cada equipo, aunque sería lo ideal. Por lo que una práctica muy común, es la asociación de una misma PSK a un mismo SSID, para evitar tales contratiempos.

Sin embargo, debido a que se emplea una misma clave para todos los dispositivos, todos los usuarios conectados a la red, pueden “ver” el tráfico generado por los demás,

aun cuando la red está bloqueando a usuarios externos. Este parámetro se debe tener muy en cuenta, puesto que es la razón principal, por la que los hackers maliciosos se aprovechan de esta brecha para filtrar el tráfico generados por los dispositivos.

4.4.2.2. Authentication, Authorization, y Accounting Key (AAAK)

También conocida como MSK es una clave que se distribuye a un AP mediante el protocolo EAP, en el proceso de asociación de RSNA. Con esta clave se busca una autenticación única por cada sesión, es decir, que la clave no va a ser la misma en cada sesión que se inicie. Por tanto, cada vez que un usuario se autentica con el AP, la contraseña cambiará.

La creación de esta clave, depende de la técnica de autenticación utilizada con EAP, puesto que este protocolo consta de algunas variantes, de las cuales se puede elegir la más óptima para el sistema de seguridad. La decisión del mecanismo a utilizar queda a elección del administrador de la red o del que la implementa. Por lo que, en el AS o en las STA, se debe escoger una técnica de autenticación EAP para establecer la seguridad en la red RSNA. Cabe recalcar que en base a la técnica de autenticación que se decidió usar, también están ligadas las vulnerabilidades que puedan encontrarse en la red (Frankel et al., 2007a).

La normativa IEEE 802.11i además de los mecanismos en base a llaves antes vistos, también introduce dos protocolos diseñados para proporcionar de confidencialidad e integridad a los datos de una red RSNA. Estos protocolos son: El protocolo de Integridad de Clave Temporal (TKIP) y el Protocolo MAC de Modo Contador con Encadenamiento de Bloques de Cifrado (CCMP).

4.4.3. Protocolos de Integridad y Confidencialidad de Datos

4.4.3.1. Protocolo de Integridad de Clave Temporal (TKIP)

Este protocolo es un conjunto de técnicas de cifrado empleado en dispositivos que incorporan WEP, con el fin de proporcionar una mejor protección sin reducir el rendimiento de la red. TKIP está diseñado para sustituir a WEP sin la necesidad de reemplazar el hardware existente. Esto se debe a que este protocolo está enfocado en una implementación mediante el software, lo cual no requiere una actualización de los equipos. Además, esto permite que en futuras versiones de TKIP se pueda descargar una actualización complementaria para mejorar su protección.

TKIP al igual que WEP emplea el cifrado de flujo para proveer de seguridad a los datos, es decir, que los datos se cifran en bits como si fuera un flujo. La técnica usada en ambos mecanismos es RC4, aunque se diferencian en que WEP lo implementaba con 64 bits puesto que empleaba claves cortas. Mientras que TKIP al ser una mejora ampliaba las claves a 128 o 256.

Algunas de las características que brinda TKIP a las redes IEEE 802.11 son:

- Protección de la confidencialidad a través de RC4 mejorado.
- Protección contra ataques mediante el algoritmo de MIC[10].
- Prevención de reproducción de tramas, mediante números de secuencia para cada trama.
- Implementación de medidas para mitigar ataques, cuando se detectan errores MIC en las tramas.

Dentro del conjunto de técnicas de cifrado de este protocolo, se tienen dos que son la base de la seguridad actual: RC4 mejorado y el código de integridad de mensajes de Michel (MIC). Estas técnicas se basan en algoritmos matemáticos del tipo de hash con

[10] Función del tipo hash, empleada en criptografía para verificar la integridad de los paquetes.

clave que permiten detectar si han existido modificaciones en las tramas enviadas y recibidas.

Mediante estas técnicas de cifrado, TKIP introduce mejoras con respecto a WEP. La principal característica dentro del funcionamiento de TKIP se basa en el uso de la trama IEEE 802.11 para detectar alteraciones en su información. De esta forma detecta si un usuario externo ha intentado falsificar una trama para adentrarse en la red y filtrar la información.

El proceso de funcionamiento de TKIP es el siguiente:

- El primer paso consiste en que el transmisor calcula un código MIC de los campos de la MSDU[11] (MAC Service Data Unit), y lo añade a la misma antes de que sea fragmentada en MPDUs[12] (MAC Protocol Data Unit).

- Posteriormente el receptor recibe la trama y la verifica, comprobando si el cifrado realizado mediante MIC no se ha visto comprometido. También evalúa el ICV[13] (Integrity Check Value) propio de WEP, y la desfragmentación de las MPDU en la MSDU original. Si ha existido algún cambio en alguno de estos parámetros, la trama se descartará.

Debido a que MIC tiene sus limitaciones, aún puede ser vulnerado. Por tanto, TKIP incorpora medidas para mitigar tales ataques. Una de estas medidas se denomina TSC (TKIP Sequence Counter, Contador de Secuencia TKIP) que es la implementación de números de secuencia, es decir, numerar los paquetes para reconocer si alguno fue enviado más de una vez y conocer porque tuvo que realizarse tal reenvío. Si un paquete recibido no coincide con el orden creciente esperado entonces se descarta la trama. Esta técnica es ideal cuando se producen ataques de repetición o duplicado.

[11] Unidad de datos de servicio que se recibe de la subcapa LLC.
[12] Unida de datos de protocolo de la subcapa MAC.
[13] Cadena fija de caracteres incluida en el texto plano usada para verificar su integridad.

A diferencia de los métodos de WEP, TKIP emplea una combinación criptográfica que mezcla la clave temporal, la dirección del transmisor y el TSC en la semilla WEP (IEEE Computer Society, 2004a). Esta mezcla fue desarrollada para impedir que los ataques de clave débil de WEP se sigan realizando.

Se debe hacer hincapié en que TKIP se vale de la estructura de la MPDU de WEP, para implementar las técnicas de cifrado antes mencionadas. En la Figura 6 se muestra la estructura de la trama WEP MPDU. En la nueva trama se aumentan 4 octetos para la extensión de IV WEP, que se muestra como IV Extendido. Además, se amplía el formato de la trama MSDU mediante 8 octetos que se usan para incluir la encriptación MIC. Por tanto, los campos de Datos, MIC, e ICV se encriptan antes de fragmentar las tramas en MPDUs.

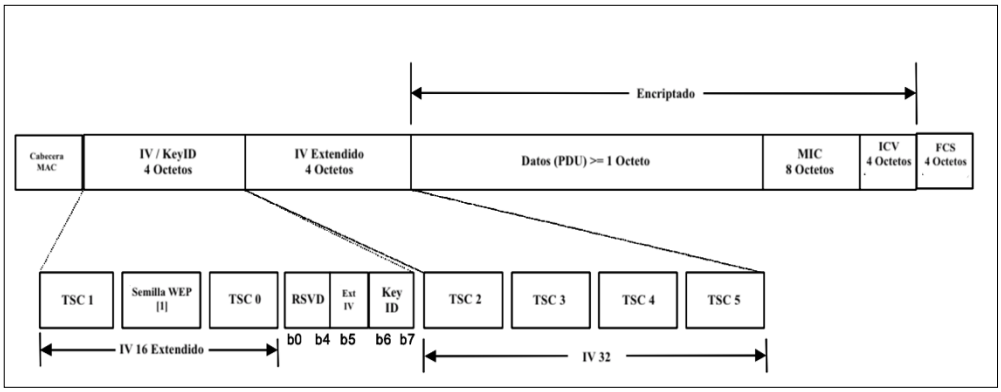


Figura 7: Estructura de la trama extendida TKIP MPDU.
Copyright 2004 IEEE 802.11i por IEEE (IEEE Computer Society, 2004c).

La implementación de TKIP en dispositivos que incorporaban WEP, permite que algunos tipos de ataques que sufre WEP puedan ser mitigados. Algunos de estos ataques son:

- Ataques de inversión de bits.
- Truncamiento, concatenación y empalme de datos (carga útil).
- Ataques de fragmentación.

- Ataques de adivinación por prueba y error de la clave.
- Modificación de los campos de Dirección de Destino de la MPDU.
- Ataques de suplantación de identidad mediante la alteración del campo de Dirección de Origen de la MPDU.

A pesar de las ventajas que supone la sustitución de TKIP por WEP, en la práctica ambos mecanismos tienen sus fallas, aunque TKIP es más seguro. El método de encriptación mediante MIC brinda mayor seguridad a los datos contenidos en la MSDU, pero es vulnerable frente a ataques de repetición. Debido a esto, es que TKIP implementa números de secuencia en cada trama y la confirmación de ICV para impedir que una trama extraña se filtre en la red.

Sin embargo, debido a que TKIP se vale de los mecanismos de seguridad de WEP, es que se desarrollaron nuevas técnicas que permiten ataques más concretos a partes específicas de la trama para poder vulnerarlo.

4.4.3.2. Protocolo MAC de Modo Contador con Encadenamiento de Bloques de Cifrado (CCMP)

CCMP es la base de la seguridad en las redes RSNA debido a que su uso es obligatorio. El propósito de CCMP es sustituir totalmente los mecanismos de cifrado y autenticación de TKIP, y por ende los de WEP. Se considera que TKIP solo era un "envoltorio" sobre WEP, porque empleaba su misma arquitectura de funcionamiento. Entonces la necesidad de crear un nuevo mecanismo que brinde una seguridad completa llevo al desarrollo de CCMP.

Este protocolo se basa en el cifrado por bloques con autenticación por AES (Advanced Encryption Standard, Estándar de Encriptación Avanzado) al contrario del cifrado de flujos empleado por TKIP. "Este cifrado se realiza por medio de CCM que es un modo general de cifrado para bloques de 128 bits como AES."(IEFT, 2003). También se puede ampliar el tamaño a más bloques, pero se requieren de cláusulas específicas.

CCM para IEEE 802.11 emplea una única clave de sesión (TK) de 128 bits para proteger el canal de datos dúplex. El espacio de claves de CCMP tiene un tamaño de 2^{128} y utiliza un número de paquete (PN) de 48 bits para construir un nonce que evite los ataques de repetición. La construcción del nonce permite utilizar la clave tanto para la integridad como para la confidencialidad sin comprometer ninguna de las dos (Frankel et al., 2007b).

Debido a que CCM es un modo de encriptación por bloques, necesita establecer una clave única que se usa para el cifrado de bloques. Por tanto, la seguridad que provea este mecanismo, dependerá en mayor medida de que tan compleja sea la clave. Además, CCM se orienta a una encriptación del conjunto de datos denominados "bloques o paquetes", por tanto, requiere que exista de un almacenamiento que agrupe tales datos para luego encriptarlos; lo que lo hace más seguro.

Los requisitos de entrada para el funcionamiento de CCM son tres:

- Los datos a ser encriptados (payload o carga útil),
- Datos asociados, como la cabecera que se usarán para autenticación,
- Y un valor único denominado "nonce" que se asigna a los dos datos anteriores.

El funcionamiento de CCM consiste en dos técnicas de cifrado muy robustas que son ideales para las redes RSN, que son: CTR (Counter, Contador) y CBC-MAC (Cipher Block Chaining MAC, Encadenamiento de Bloques de Cifrado para MAC). CTR es empleado para proporcionar confidencialidad, mientras que CBC-MAC es usado para brindar autenticación e integridad de los datos. El cifrado realizado por ambas técnicas se lo realiza hacia adelante.

El proceso para proporcionar seguridad a la información, comienza en el transmisor, cuando el cifrado CBC se aplica a los tres requisitos mencionados anteriormente, para obtener un código de autenticación de mensaje, también conocido como MAC (No confundir con la subcapa MAC o la dirección MAC). Luego se aplica el CTR al MAC

y a la carga útil para producir un texto cifrado. De tal manera, este texto cifrado se envía al receptor quien realizará el proceso contrario.

En el lado del receptor, cuando se recibe el texto cifrado, se realiza la desencriptación y la verificación de los datos. Primero se emplea el CTR para descifrar el texto cifrado, con el fin de recuperar la MAC y la carga útil. "Posteriormente se aplica el CBC a la carga útil, los datos asociados y la nonce, para verificar la corrección MAC."(Dworkin, 2007). Si la confirmación de que la información es correcta, supone que la procedencia de la misma, tiene acceso a la misma clave. Por ende, el origen de la información recibida es el correcto.

La estructura de la trama empleada por CCMP para proporcionar de seguridad a IEEE 802.11 se muestra en la imagen 8.

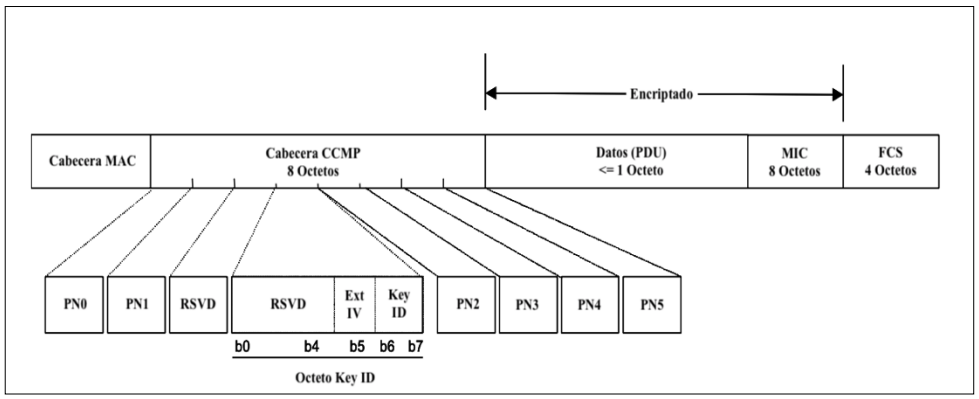


Figura 8: Estructura de la trama extendida MPDU.
Copyright 2004 IEEE 802.11i por IEEE (IEEE Computer Society, 2004c).

En la trama de CCMP se expande 16 octetos el formato de la MPDU original, de los cuales 8 octetos están destinados para la Cabecera CCMP y los otros 8 para el campo MIC. En la imagen 4 se puede observar la falta del parámetro ICV utilizado en WEP y TKIP, puesto que ya no es necesario.

CCMP se vale de dos variables que implementa CCM para indicar en la trama la longitud de los campos de autenticación y datos. Estos valores son M y L:

- M = 8; describe la longitud del campo MIC utilizado para la autenticación y encriptación. El valor de 8 indica el número de octetos que tiene el campo.
- L = 2; indica que el campo Length o Longitud es de 2 octetos. El 2 representa el máximo valor posible en octetos, que puede tener la MPDU.

De esta manera, se pueden emplear los valores antes analizados para crear el texto encriptado que se transmitirán entre el emisor y el receptor de la red RSNA.

4.5. Acceso Wi-Fi Protegido (WPA)

WPA es el sistema de seguridad propuesto por la Wi-Fi Alliance para proporcionar seguridad a las redes Wi-Fi. En este sistema se establece el uso de los mecanismos de protección descritos en 802.11i, es decir, la Wi-Fi Alliance certifica a los equipos que intervienen en la red Wi-Fi, para que implementen los métodos de seguridad del estándar IEEE 802.11i.

Elankayer y Vallipuram enfatizan que WPA: "Se trata de un subconjunto de las capacidades de 802.11i, que incluye un mejor cifrado con el Protocolo de Integridad de Clave Temporal (TKIP), una configuración más sencilla mediante una clave pre-compartida y la posibilidad de utilizar la autenticación de usuarios 802.1X basada en RADIUS (Remote Authentication Dial-In User Service, Servicio de autenticación remota de usuarios de acceso telefónico)."(Sithirasenan & Muthukkumarasamy, 2005)
.

Los dispositivos certificados con WPA pueden formar redes RSN, puesto que WPA es el término empleado por la Wi-Fi Alliance para referirse al subconjunto de los mecanismos provistos por estas redes. No obstante, WPA es un sistema "incompleto" debido a que cuando se diseñó la enmienda IEEE 802.11i, aún no finalizaba su rectificación. Por tanto, cuando se implementó WPA para sustituir a WEP en los nuevos dispositivos, el sistema se definió como "transitorio" hasta que la enmienda se termine. Esto como solución para que las redes Wi-Fi no quedarán desprotegidas.

WPA tienes dos métodos de funcionamiento, uno es mediante PSK y el otro es el empresarial. En sus dos versiones, emplea el protocolo TKIP para proporcionar de autenticación y confidencialidad a la red Wi-Fi. Cabe recalcar que ambas versiones (WPA-Personal y WPA-Enterprise) soportan el mecanismo PSK. Sin embargo, WPA-Enterprise mejora la protección a través de un servidor de autenticación, que puede basarse en el protocolo RADIUS, que es mucho más seguro que las claves compartidas.

A pesar que WPA utiliza el cifrado RC4 al igual que WEP, el uso de TKIP aporta una ventaja significativa en la protección de la red. TKIP añade 3 elementos que mejoran la seguridad: Código de Integridad de mensajes de Michael (MIC), Procedimiento de secuenciación de paquetes y una mezcla de Claves por paquetes.

De igual manera, para el intercambio y gestión de las claves, TKIP utiliza IEEE 802.1X.

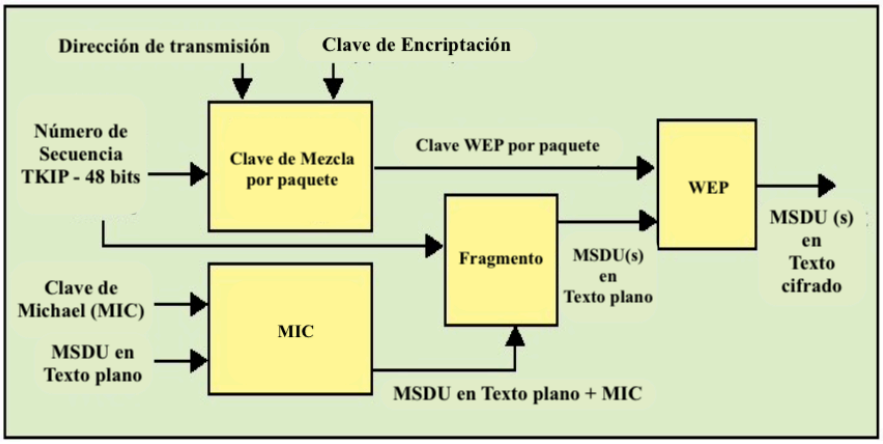


Figura 9: Flujo de Procesamiento de TKIP.
Copyright 2014 A survey on Wi-Fi Protocols: WPA and WPA2 por Mahmoud Khasawneh (Khasawneh et al., 2017).

La Wi-Fi Alliance se enfocó en crear dos sistemas de seguridad para emplearse en dos ambientes de trabajo diferentes. Esto se debió principalmente por que el tipo de información (tráfico) que se producía en ambos entornos, requerían soluciones de

seguridad distintas para sus datos, por tanto, se decidió por desarrollar un sistema para cada uno. Las redes que se consideraron en base al tráfico generado, fueron la red doméstica y la red empresarial.

El tráfico que se produce en un hogar se origina mayormente por el consumo de servicios multimedia como videos o videojuegos, aunque también se genera por aplicaciones de ofimática. Esto implica que los datos que se envían, no tienen un alto grado de confidencialidad. Por tanto, para este tipo de información no se necesita un nivel de seguridad elevado. Con base a esto, el estándar destinado para el uso doméstico se denominó WPA-Personal.
Asimismo, la necesidad de precisar con un sistema de protección para datos de empresas que suelen tener un grado de confidencialidad mayor, llevo a crear el sistema WPA-Enterprise. Este estándar empresarial, se diferencia del estándar doméstico, porque agrega el uso de un servidor dedicado para la autenticación de los dispositivos.

4.5.1. WPA-Personal

Es la solución propuesta por la Wi-Fi Alliance para brindar seguridad a las redes del hogar. WPA-Personal, también llamada WPA-PSK, es un sistema de seguridad para hogares, oficinas u otras redes pequeñas, que no requieren de métodos de cifrado avanzado o de autenticación. Por este motivo, no se implementan servicios de autenticación para los dispositivos en estas redes.

El proceso de identificación entre la STA y el AP cuando se usa el sistema WPA es mediante una clave compartida que ambos dispositivos conocen. Tal clave tiene una longitud de 256 bits que supone mayor complejidad de descifrar. Un parámetro importante en el sistema WPA, es que la clave no se debe transmitir entre la STA y el AP. Por tanto, la clave o contraseña debe ser configurada en el STA y en el AP de forma manual.

La clave es la base para desarrollar el MIC y la clave de encriptación, que se utilizarán para cifrar los MSDU (MAC Service Data Unit, La unidad de datos de servicio MAC)(Khasawneh et al., 2017).

4.5.2. WPA-Enterprise

WPA-Enterprise o WPA-Empresarial, es el sistema de seguridad orientado para empresas, diseñado por la Wi-Fi Alliance. Este sistema se enfoca en mejorar el sistema de identificación de los usuarios en una red empresarial, donde se requiere mayor control de ingreso.

Este sistema emplea un AS que se encarga de autenticar a los dispositivos a través de credenciales. Para realizar un adecuado control de acceso, el AS emplea el protocolo RADIUS que es obligatorio para este sistema.

RADIUS permite identificar que usuarios tienen acceso a los servicios ofrecidos por la red y cuáles no. Además, provee de encriptación para el tráfico generado por los usuarios, por lo que, protege los datos que se originan en la red. Esto imposibilita a los atacantes tener acceso sobre la información producida en la red que puede ser de carácter confidencial.

Para el cifrado de los datos, se emplea el marco de trabajo EAP, con sus diversos mecanismos de seguridad. Los mecanismos a utilizar, dependerán de la elección del administrador de la red.

4.6. Acceso Wi-Fi Protegido 2 (WPA-2)

WPA-2 es la segunda versión del sistema de seguridad establecido por la Wi-Fi Alliance, y es la versión completa de la enmienda IEEE 802.11i. Al contrario de WPA, WPA-2 no es un sistema transitorio en espera de un nuevo estándar. Este sistema se

basa totalmente en la enmienda IEEE 802.11i ya terminada, por lo que implementa los últimos mecanismos de seguridad desarrollados para la protección de las redes inalámbricas.

En su segunda versión, WPA-2, sustituye el cifrado de flujo del algoritmo de encriptación RC4 por el cifrado por bloques de AES de 128 bits, que es empleado tanto para la autenticación como para el cifrado de datos. En esta versión también se reemplaza el protocolo TKIP, por la clave de cifrado PTK. Además, se introduce el protocolo CCMP que trabaja con AES para mejorar la encriptación de la información; y se incluye CCM para proveer de integridad a los datos y de autenticación a los usuarios (Sakib et al., 2014).

Similar a su versión anterior, este sistema también puede emplear dos métodos de autenticación: PSK y el empresarial que emplea un AS. Esto se debe a que también se desarrollaron dos sistemas de seguridad enfocados a los dos tipos de entornos: un entorno doméstico y un entorno empresarial. Estos sistemas son: WPA2-Personal y WPA2-Enterprise.

4.6.1. WPA2 – Personal

El sistema WPA-2 para el ambiente domestico incorpora el mismo mecanismo de autenticación, es decir, se sigue utilizando PSK. A pesar de mantener el mismo sistema para el control de acceso de dispositivos, mejora significativamente, puesto que se sustituyen los mecanismos de cifrado, integridad y autenticación.

Sin embargo, el uso del mecanismo PSK no es aceptado en la enmienda IEEE 802.11i puesto que quedo obsoleto al descubrir la facilidad que tienen los atacantes en obtener la clave compartida. Además, existen muchas vulnerabilidades presentes que comprometen la seguridad de la red.

4.6.2. WPA2 – Enterprise

Este sistema dedicado para uso empresarial, se basa en la autenticación por medio del AS. El servidor mejora la forma en cómo se crean las claves de cifrado para la red. Esto se debe a que los procesos para el diseño de cada clave se hacen de una forma secuencial y jerárquica.

WPA2-Enterprise emplea los mecanismos 802.1X para seguridad de puertos, EAP como protocolo de autenticación, confidencialidad e integridad; y la distribución de claves seguras. Además, adiciona el uso de un AS como equipo de control AAA.

El proceso utilizado en WPA2-Enterprise para la creación de las claves es la Jerarquía de Claves por Pares, analizada anteriormente. El objetivo de implementar esta jerarquía, es el de crear claves que se basen en entradas aleatorias como los nonces, y que limiten el acceso a usuarios externos a la red. La ventaja de esta clave es que una de las entradas para la creación de la PMK es la dirección MAC, del AP y de la STA, lo que limita que atacantes obtenga la clave e intenten acceder. Además, todos los procesos que se envían y se reciben lo hacen a través de los puertos protegidos de IEEE 802.1X.

4.7. Acceso Wi-Fi Protegido 3 (WPA-3)

WPA-3 es la actual versión de los sistemas WPA. En esta versión se añaden nuevas funciones para simplificar el proceso de autenticación, a la vez que se mejora la encriptación. Este nuevo estándar propone mayor seguridad en las redes Wi-Fi, considerando principalmente la confidencialidad del tráfico generado.

WPA-3 se fundamenta en 3 elementos que están presentes en todas sus versiones:

- Emplean los métodos de seguridad actuales.

- Los protocolos heredados son obsoletos, por tanto, no se utilizan.
- Se exige el uso de tramas de gestión protegidas (PMF).

Las dos versiones de WPA-3 desarrolladas para el entorno doméstico y el empresarial, se basan estrictamente en estos 3 elementos. Esto permite que el sistema WPA3-Personal mejore su seguridad frente a ataques de diccionario o de prueba y error. Mientas que el sistema WPA3-Enterprise, aprovecha los últimos mecanismos de seguridad desarrollados, para proporcionar un mayor grado de protección a la red.

WPA-3 también emplea la SAE (Simultaneous Authentication of Equals, Autenticación Simultánea de Iguales) que es un método seguro de autenticación que se basa en una contraseña y en las claves de autenticado de esta. La ventaja que ofrece SAE, es que impide los ataques de diccionario y de prueba y error que los atacantes usan para acceder de forma ilegal a la red.

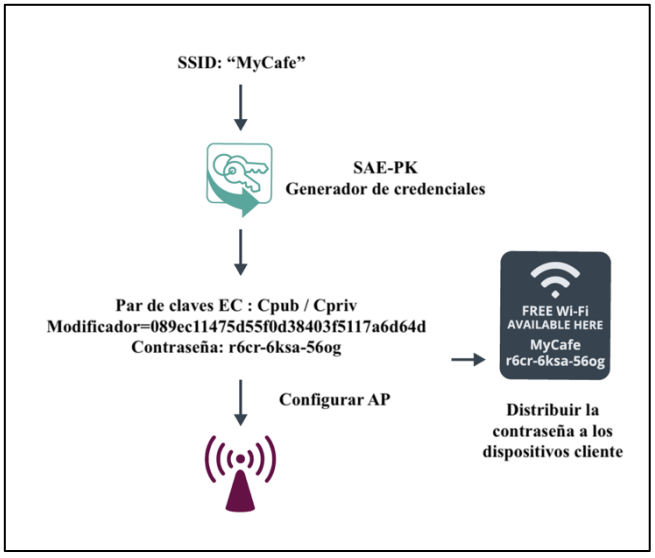


Figura 10: Asociación WPA-3.
Copyright WPA3 SAE Public Key and Transition Disable por Wi-Fi Alliance (Wi-Fi Alliance, 2019).

4.7.1. SAE-PK

WPA-3 también incorpora una extensión de SAE, conocida como SAE-PK. La contraseña SAE-PK se establece igual a una representación de una huella digital de la clave pública del AP, y por lo tanto sirve tanto como un secreto por el cual el AP autentifica STAs para el acceso a la red, y también como un medio para arrancar la confianza en la clave pública estática del AP para STAs para autenticar el AP (Wi-Fi Alliance, 2020d).

.

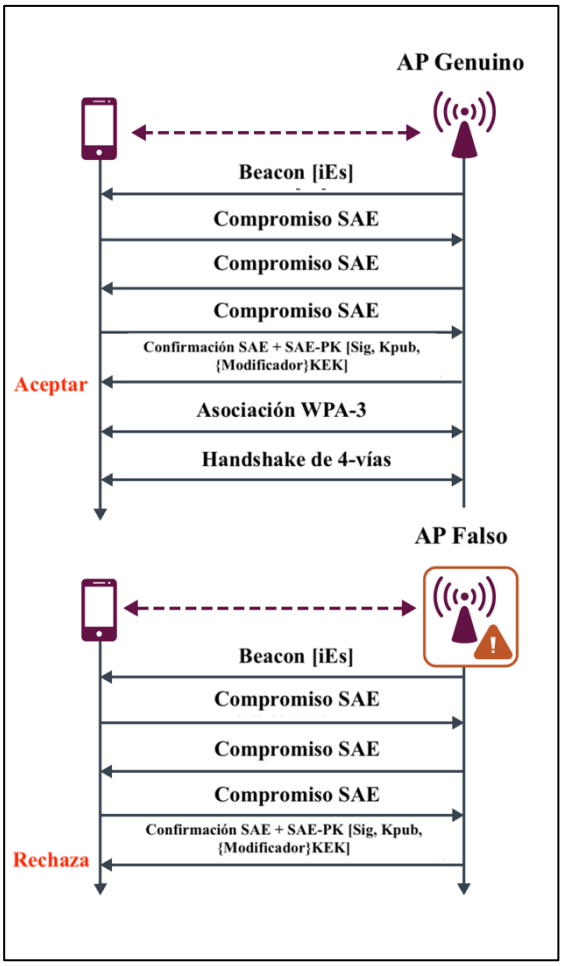


Figura 11: Autenticación SAE-PK con un AP autentico y un AP Falso.
Copyright WPA3 SAE Public Key and Transition Disable por Wi-Fi Alliance (Wi-Fi Alliance, 2019).

SAE-PK está pensado para casos de uso en los que la autenticación se basa en una contraseña que podría ser distribuida u obtenida por un adversario potencial. Un

adversario que tenga conocimiento de la contraseña (pero no de la clave privada análoga a la clave pública del AP) puede obtener acceso a la red, pero no puede hacerse pasar por un AP cuando se utiliza SAE-PK (Wi-Fi Alliance, 2020d).

Esta característica de SAE-PK impide que atacantes externos puedan acceder fácilmente a la red, debido a que emplea un doble proceso de autenticación entre el AP y los STAs. Por tanto, gracias a esta propiedad se pueden evitar ataques como: "Evil Twin o Gemelo Malvado" o Ataques de robo de contraseña (también llamado Ataque de Pre-Imagen).

4.7.2. WPA3 – Personal

En la versión de WPA-3 para el hogar, se mejora la robustez de las contraseñas empleadas para el secreto compartido, aun cuando la contraseña no cumple con la complejidad recomendada.

También se debe mencionar que, WPA-3 Personal implementa un mecanismo denominado "Desactivación de la Transición", el cual consiste en inhabilitar la transición entre WPA-3 a WPA-2 o inferiores, en dispositivos que soportan WPA-3. Este método surgió como medida de seguridad frente al ataque DragonBlood[14] (Vanhoef, 2019).

4.7.3. WPA3 – Enterprise

En el estándar WPA enfocado para empresas, mejora la complejidad de la criptografía utilizada a una de 192 bits. Esta implementación, permite que la protección de datos

[14] DragonBlood es un ataque desarrollado especificamente para WPA-3, que consiste en forzar a los STAs que soportan WPA-3, para que empleen el sistema WPA-2, y de esta manera puedan aprovechar las vulnerabilidades de WPA-2 para sus fines. Este tipo de ataque también se conoce como "Downgrade" .

sensibles como los financieros o los gubernamentales, sea mucho más robusta frente a ataques de Man-in-the-middle.

El sistema de seguridad WPA3 – Enterprise, conserva el uso de los servidores de autenticación para el control de acceso de los equipos. No obstante, con las mejoras en las claves criptográficas de 192 bits, se puede aumentar la seguridad del proceso de transferencia de mensajes, en la etapa de autenticación del cliente RADIUS y el AS. Además, debido a que el tráfico también debe cifrarse, imposibilitara que atacantes puedan filtrar e interpretar la información contenida en los paquetes que viajan en la red (Wi-Fi Alliance, 2020a).

De igual manera, WPA3- Enterprise incorpora el mecanismo de "Desactivación de Transición de WPA3- Personal.

4.7.4. WPA-3 vs WPA-2 Personal

WPA-3 al ser la versión sucesora de WPA-2 implementa nuevos mecanismos de seguridad que mejoran la protección con respecto a su predecesora. La implementación de SAE y SAE-PK como métodos para la asociación de los STAs con el AP, no permiten que ataques como Fuerza Bruta, Diccionario, Evil Twin, DoS, entre otros; tengan éxito en su cometido.

Las mejoras que WPA-3 implementa para solventar las vulnerabilidades presentes en WPA-2 son las siguientes:

- Limitar en el número de intentos de autenticación para impedir el éxito de los ataques de Fuerza Bruta y Diccionario.
- Todos los APs de una red deben tener configurado el sistema SAE, con el fin de evitar la sobrecarga que se puede producir por un ataque de DoS.
- Se implementa un parámetro conocido como "Des-habilitación de Transición" para impedir que los sistemas protegidos por WPA-3, cambien a WPA-2 que es más vulnerable.

(Wi-Fi Alliance, 2021)

A pesar de los esfuerzos realizados para desplegar WPA-3, para dotar a los dispositivos Wi-Fi de mayor protección, la realidad es que WPA-2 es el sistema de seguridad más extendido. Esto se debe a que la diferencia de tiempo hasta que se lanzará el nuevo estándar fue de 14 años, lo que representó un amplio margen de tiempo para que el despliegue e implementación de WPA-2 se realice en casi todos los dispositivos que emplean Wi-Fi. Además, el despliegue de WPA-3 se vio afectado debido a algunas vulnerabilidades encontradas antes de su lanzamiento, por lo que, esto repercutió en su extensión e implementación en los STAs .

4.8. IEEE 802.1X

Es una normativa creada por IEEE que se basa en el control de acceso a la red basada en puertos. En una RSNA esta normativa es utilizada para proveer de servicios de autenticación dentro de una LAN. Para esto se emplea la gestión y distribución de las claves vista anteriormente.

El propósito principal para el diseño de IEEE 802.1X fue para impedir que usuarios externos a una red cableada pública, puedan acceder a la red. Sin embargo, con el desarrollo de las redes inalámbricas esta enmienda fue adoptada por IEEE 802.11i para proporcionar seguridad a las redes Wi-Fi, en las cuales tiene mayor relevancia.

IEEE 802.1X dentro de su estructura comprende de 2 componentes necesarios para su funcionamiento, estos son:

Entidad de Acceso de Puerto IEEE 802.1X (PAE): Este elemento es importante en las redes RSNA. Su propósito es controlar el reenvío de los datos desde y hacia la subcapa MAC (Control de Acceso al Medio). Los AP tienen incorporado un PAE autenticador (también cumplen el rol de autenticador EAP), mientras que los STAs incorporan un PAE suplicante (también cumplen el rol de peer de EAP) (IEEE Computer Society, 2020).

El PAE autenticador es el puerto encargado de autenticar a los solicitantes antes de permitir su acceso a los servicios disponibles en ese puerto. Por el contrario, el PAE suplicante es el puerto que intenta acceder a los servicios ofrecidos por el PAE Autenticador (Oracle, 2009).

Servidor de Autenticación (AS): Este servidor se encarga de autenticar a las STAs. Mientras que los AP implementan funciones para que los dispositivos pertenecientes a una RSNA se identifiquen entre sí, por ejemplo, contraseñas.
Con base a lo expuesto por la IEEE, el proceso de autenticación es el siguiente: “El AS se comunica a través del Autenticador IEEE 802.1X con el Suplemento IEEE

802.1X de cada STA, permitiendo que el STA se autentique ante el AS y viceversa."(IEEE Computer Society, 2004b). La seguridad de la RSNA depende en gran medida del método de EAP empleado para proteger la red.

4.8.1. Generalidades

Puesto que las redes RSNA de IEEE 802.11 emplean la normativa IEEE 802.1X para proporcionar de control de acceso, los servicios empleados para permitir que una nueva STA se conecte, se mantienen. Aunque con mecanismos de seguridad adicionales para controlar el acceso a la red.

4.8.1.1. Asociación

El proceso para que un dispositivo o STA pueda ingresar a la red, se realiza a través de las tramas de 802.11. En IEEE 802.1X las tramas de autenticación se encapsulan en tramas de 802.11, y se envían a un puerto no controlado, en el cual se confirma la identidad de la STA que desea conectarse. Cuando la información de la STA suplicante se confirma, se habilita un puerto controlado que estaba bloqueado para que se pueda enviar el tráfico generado por el usuario. Este proceso generalmente se lo conoce como AKM[15] (Authentication and Key Management, Autenticación y Gestión de Claves). De esta manera, se logra que un usuario que no pertenece a un determinado grupo de trabajo acceda a la red. Por tal motivo es importante que la STA suplicante como el dispositivo autenticador, tengan implementado el bloqueo de puertos (IEEE Computer Society, 2020).

4.8.1.2. Autenticación

Este servicio está diseñado para incluir la seguridad que provee el cable a las redes cableadas, es decir, proporciona un aislamiento entre las demás comunicaciones del

[15] La gestión de autenticación y claves (AKM) es el término utilizado para describir el proceso de autenticación IEEE 802.1X/EAP y la posterior generación de claves de cifrado, y es un componente principal de los protocolos de autenticación extensible (EAP) y IEEE 802.1X. Cada vez que un cliente se asocia o reasegura, debe producirse el proceso completo de AKM, lo que da lugar a una red inalámbrica extremadamente segura y robusta (Capano, 2015).

medio, como lo hace un cable. Esto lo realiza mediante mecanismos de identificación de cada dispositivo que pretende establecer una comunicación con el AP.
Los mecanismos empleados pueden ser PSK o basada en puertos como 802.1X. En el caso de 802.1X se emplea el mecanismo EAP para autenticar las STAs con los ASs y viceversa.

En las RSNA el método utilizado es la autenticación basada en puertos 802.1X puesto que PSK presenta muchas deficiencias en su seguridad. En 802.1X los dispositivos suplicantes y autenticadores se envían información de identificación mutuamente a través de un puerto no controlado. El puerto no controlado se lo utiliza como vía para el control de acceso a la red, por este puerto se envía y recibe la información concerniente a la identidad de los dispositivos, para que se pueda confirmar la autenticidad de la misma.

Una vez que se confirma la identidad de las STAs suplicantes y del AS autenticador, se habilita un Puerto Controlado que estaba bloqueado para impedir el envío de tráfico proveniente de entidades no conocidas. Cuando el Puerto Controlado se habilita, las STAs suplicantes ya pueden conectarse a la red y enviar tráfico.

4.8.1.3. Des-autenticación

La des-autenticación se produce cuando un dispositivo requiere que el proceso de comunicación termine. Por lo tanto, el mecanismo empleado para la autenticación tiene que desasociar al dispositivo. La des-autenticación como tal, no supone un proceso de transmisión de información, ni confirmación de identidad, si no una notificación en la cual el dispositivo sea una STA o un AP, terminaran la conexión. Además, al ser una notificación de finalización en la comunicación, esta no puede ser denegada, por lo que, las entidades podrán des-autenticarse en cualquier momento y sin límites.
La des-autenticación en IEEE 802.1X provoca que el puerto controlado por donde se trasmitía la información, se vuelva a bloquear y termine la comunicación.

4.8.2. Privacidad y Confidencialidad de los datos

En este servicio se introduce el concepto de proteger los datos de manera que no estén expuestos hacia los demás. Esto se debe a que en la arquitectura de IEEE 802.11 todas las STA conectadas a la red, pueden escuchar y recibir el tráfico generado por otras STAs conectadas. Para evitar esta deficiencia, se emplea la encriptación.

La encriptación permite proteger la información enviada, mediante la modificación de la información original, añadiéndole caracteres que solo pueden entender el origen y el destino de la comunicación. En otras palabras, la encriptación convierte los datos originales a una secuencia de caracteres que solo tienen coherencia para el emisor de la información y para el receptor.
En IEEE 802.11 se utilizan principalmente tres algoritmos de encriptación para proporcionar de privacidad y confidencialidad a las diferentes comunicaciones entre los STAs y el AP. Tales algoritmos son: WEP, TKIP y CCMP; vistos anteriormente. La elección de alguno de estos algoritmos para proteger la red, queda a elección del administrador de la red.

Debido a que las redes PRSNA tenían muchas vulnerabilidades, se requería que todos los mecanismos usados para brindar seguridad, sean reemplazados. De esta manera en IEEE 802.11i que emplea 802.1X se desarrollaron nuevas técnicas criptográficas como TKIP o CCMP. Sin embargo, estas técnicas requieren de claves criptográficas para definir cuál es el procedimiento a llevar a cabo para convertir la información que está en texto plano, a información en texto cifrado.

Con base a la necesidad de diseñar nuevas llaves, en IEEE 802.1X se crearon dos protocolos que proveen de estas claves a las entidades que intervienen en la comunicación. Estos protocolos son: “4-Way Handshake o Saludo de 4 vías” y “Group Key Handshake”.

4.8.3. Funcionamiento

IEEE 802.1X busca impedir que el tráfico generado por una STA que no ha sido autenticada, pueda enviarse a través de esa red. Para lograr tal objetivo, IEEE 802.1X introduce la función de puerto bloqueado, que limita que dispositivos no autenticados puedan acceder a la red.

El proceso de que emplea para determinar la identidad de los dispositivos, es a través del saludo 4 vías. Este saludo consiste en una serie de mensajes de confirmación de identidad, en los que interviene, la STA, el AP y en ciertos casos un AS. Los métodos de saludo generalmente empleados son con la clave PSK y mediante un AS por medio del protocolo 802.1X.

4.8.3.1. Saludo de 4 vías empleando PSK

El proceso de saludo de 4 vías comienza, cuando la STA detecta la existencia de un AP cercano, y desea asociarse a este. La forma en que descubre la STA la presencia de un AP, es por medio de las tramas balizas (beacons) o por medio de la monitorización de las redes cercanas. En la figura 8 se detalla el proceso de asociación entre la STA y el AP.

Cuando empieza la asociación, automáticamente se definen los roles de los dispositivos. En el caso de la STA toma el rol de suplicante, mientras que el AP es la entidad autenticadora. De esta manera se comienza la negociación para determinar que método se utilizará para generar la clave. En esta asociación se elige la clave PSK que permitirá generar la PMK y sus llaves derivadas.

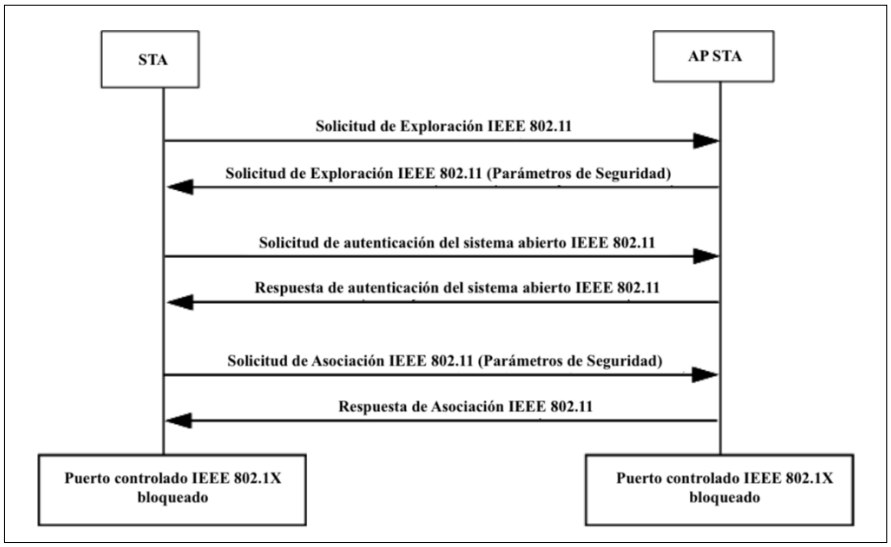


Figura 12: Proceso de asociación en IEEE 802.11.
Copyright 2007 IEEE 802.11i por IEEE (IEEE Computer Society, 2004c).

Luego de la asociación, la entidad suplicante (STA) y la entidad autenticadora (AP) empiezan el saludo de 4 vías. Este saludo consiste en enviar cuatro mensajes, que corresponden al proceso de establecimiento de los métodos de jerarquía de claves a utilizar. Posteriormente se instalará la PTK (Jerarquía de Claves por Pares) y la GTK (Jerarquía de Claves por Grupo) en ambos dispositivos y se desbloqueará el puerto bloqueado de IEEE 802.1X, permitiendo iniciar la comunicación.

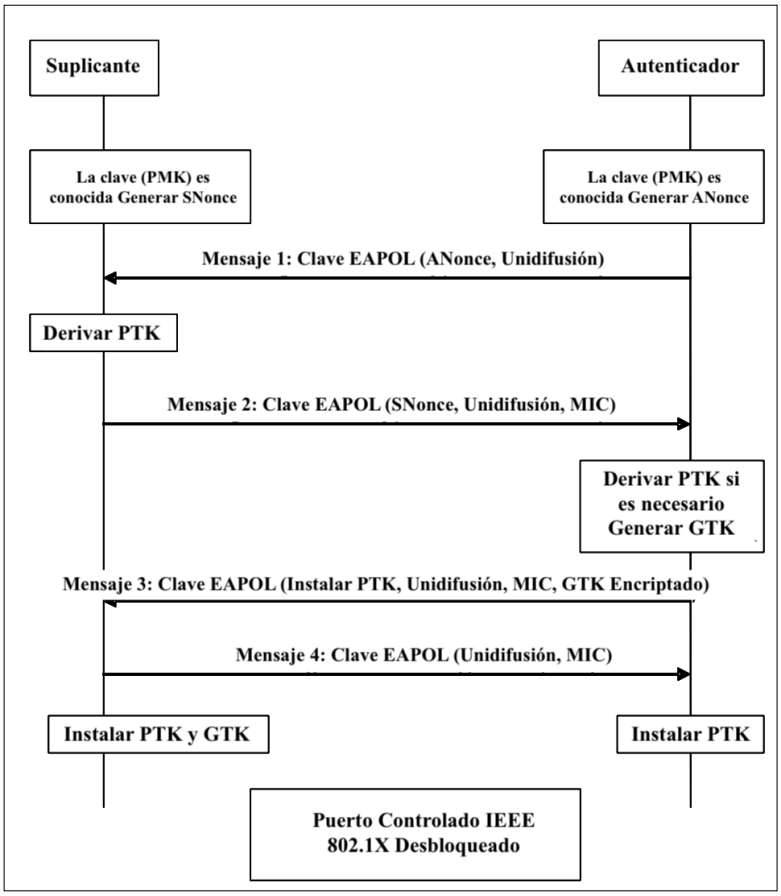


Figura 13: Establecimiento de la Clave por Pares y de la Clave por Grupo.
Copyright 2007 IEEE 802.11i por IEEE (IEEE Computer Society, 2004c).

Luego de realizar el respectivo proceso para la creación de clave y su instalación, la entidad autenticadora (AP) producirá la GTK que será empleada para futuras asociaciones con otras STAs que deseen conectarse a la red.

Para esto, el AP primero debe encriptar la GTK con la PTK para evitar ataques de robo de identidad y suplantación; y luego enviarla a las STAs con el fin de que instalen la clave de grupo y autenticarse. Este proceso se conoce como Intercambio de Claves de Grupo.

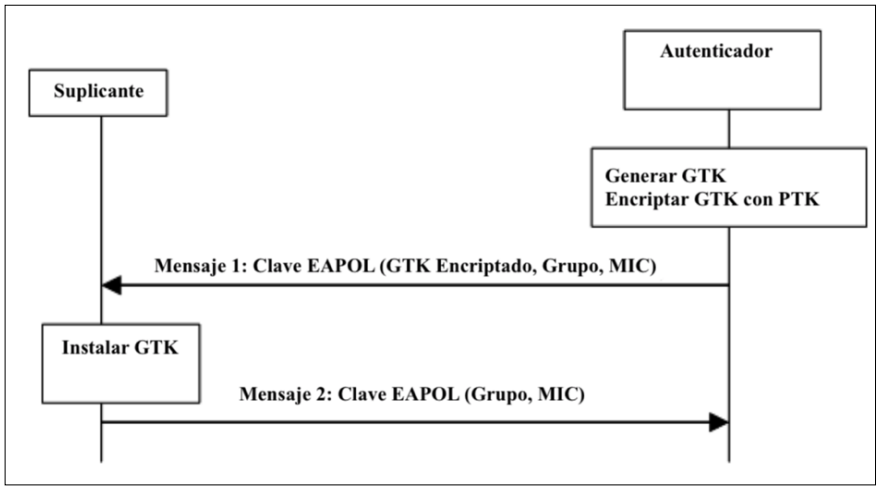


Figura 14: Entrega de la clave de grupo subsecuente.
Copyright IEEE 802.11i por IEEE (IEEE Computer Society, 2004c).

4.8.3.2. Saludo de 4 vías mediante IEEE 802.1X

En este saludo además de la STA y el AP, se agrega el uso del AS como dispositivo autenticador externo. El hecho de autenticar la entidad suplicante con el AS y no con el AP, conlleva a un nivel de seguridad mayor, debido a que el AS es un equipo dedicado a proveer autenticación. Además, no es necesario que el servidor se encuentre físicamente en el mismo lugar de la red, por lo que, en caso se ataques físicos o de software, el ingreso a la red sería más complicado y por ende más seguro.

La conexión establecida entre el AP como dispositivo autenticador local y el AS como dispositivo de autenticador externo, no se específica en la enmienda IEEE 802.11i, sin embargo, se menciona que la conexión debe ser segura.
Aunque las credenciales de autenticación, se distribuyen al suplicante y al AS antes de la asociación (IEEE Computer Society, 2012b).

Al igual que en el saludo de 4 vías con PSK, la detección de una red cercana se realiza mediante el envío de tramas baliza o beacons, o mediante el monitoreo activo.

En el saludo de 4 vías basado en IEEE 802.1X, el proceso de autenticación puede iniciar de dos maneras:

- cuando el suplicante (STA) envía un mensaje EAPOL-Start al autenticador local (AP);
- cuando el autenticador local (AP) envía una solicitud EAP 802.1X al suplicante (STA).

Independiente de la manera utilizada, la autenticación se lleva a cabo entre la STA y AS, a través del puerto IEEE 802.1X no controlado de ambas entidades. Después de confirmar la identidad, los dos dispositivos proceden a crear la PMK que servirá para obtener las claves PTK y GTK posteriormente. La PMK la envía el AS a través de un canal seguro hacia el suplicante.

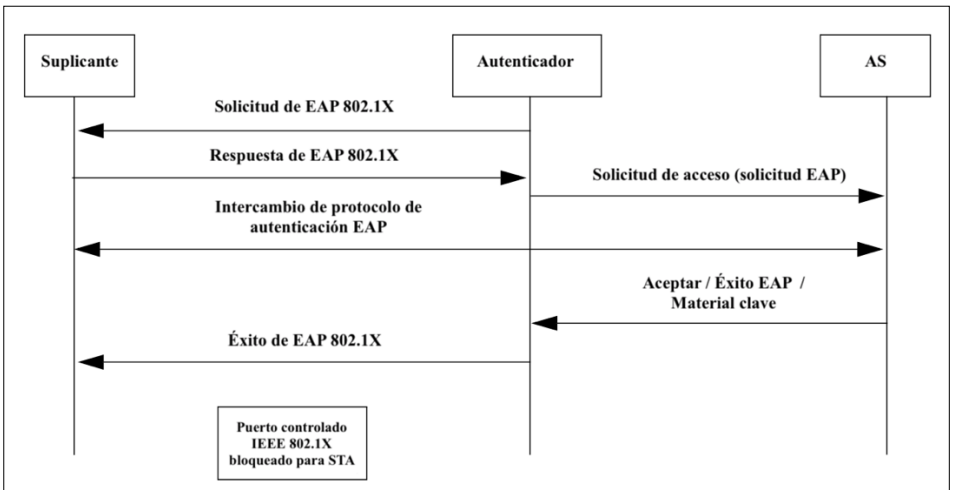


Figura 15*:* Autenticación EAP IEEE 802.1X.
Copyright 2012 IEEE 802.11 and IEEE 802.1X por IEEE (IEEE Computer Society, 2012b).

Puesto que la función del AS es la de confirmar la identidad de la STA registrada en su memoria, ya no será necesario para funciones posteriores. Por tanto, el proceso de saludo de 4 vías únicamente lo realizan la STA y el AP.

Luego de enviar la PMK, se inicia con el saludo de 4 vías mediante las tramas del tipo Clave EAPOL. El saludo se realiza entre el suplicante (STA) y el autenticador local (AP). El proceso de saludo es idéntico al analizado en PSK, por lo que el funcionamiento se describe en la Figura 15.

Este saludo tiene como objetivo cumplir con las siguientes funciones:

- Confirmar que el suplicante (STA o peer) asociado, este activo y cuente con la PMK.
- Verificar que el suplicante tiene la última PMK generada.
- Generar la PTK en base a la PMK.
- Instalar las claves de integridad y cifrado por pares en la red.
- Transferir la GTK y el número de secuencia de la GTK desde el autenticador hasta el suplicante.
- Instalar la GTK y el número de secuencia de la GTK en la STA, y en caso de que no esté instalada, también se lo hará en el AP.
- Acordar el mecanismo de cifrado que se va a utilizar.

Una vez finalizado el saludo de 4 vías entre la STA y el AP, se desbloquearán los puertos controlados IEEE 802.1X, y se permitirá enviar el tráfico por la red.

Si el Autenticador (AP) requiere que la GTK sea cambiada, se generará otra y se la enviará al suplicante, junto con el número de secuencia de la GTK mediante el Intercambio de Clave de Grupo, como se muestra en la Figura 10. De igual manera, en este intercambio también se emplean las tramas Clave EAPOL.

El propósito del intercambio de clave de grupo, es permitir que el suplicante aún pueda recibir tramas de difusión y multidifusión, y en caso de que se requiera, también podrá enviar y recibir tramas de unidifusión.

4.9. Extensible Authentication Protocol (EAP)

4.9.1. Introducción

"EAP (Extensible Authentication Protocol, Protocolo de Autenticación Extensible) es un marco de trabajo (framework) que es compatible con diversos métodos de autenticación."(The Internet Society, 2004). Este marco de trabajo está diseñado para trabajar sobre la capa de enlace de datos o Capa 2 del Modelo OSI. Además, puede utilizarse en cualquier tipo de red, independientemente de la tecnología de acceso que ésta utilice.

La principal función de EAP es proveer de autenticación, utilizando los distintos mecanismos desarrollados para brindar seguridad. Debido a su capacidad de adaptabilidad, se establecieron requisitos genéricos de EAP, para entornos de seguridad comunes y para entornos de seguridad específicos. Esta es la razón por la que EAP se define como un marco de trabajo y no como un protocolo.

En un escenario de asociación entre dispositivos, EAP se emplea para seleccionar el mecanismo de autenticación que se va a utilizar a lo largo de la sesión. A diferencia de otros mecanismos en los cuales se requiere que la entidad autenticadora se actualice para poder soportarlos, EAP permite utilizar un servidor, en el cual están instalados algunos o todos sus mecanismos compatibles. Por lo que, se puede elegir cualquier método que se requiera. Sin embargo, al utilizar un AS, el autenticador local se convierte en un dispositivo de paso.

EAP incorpora dentro su estructura, también incluye la capacidad de eliminar duplicados de las tramas y su retransmisión, aunque esta función depende de lo establecido por las capas inferiores. Así mismo, EAP no soporta la fragmentación, no obstante, algunos de los métodos la pueden soportar.

4.9.2. Funcionamiento

EAP admite diversos mecanismos de autenticación conocidos como “métodos”. Los métodos EAP dependiendo de su función pueden combinar mecanismos de autenticación para proveer del servicio necesario. Debido a esta “flexibilidad” es que este marco de trabajo es muy utilizado en las redes WLAN.

En una red Wi-Fi, EAP se emplea como método de comunicación entre los peers (STA y AS) para acordar que mecanismos que se utilizarán para generar las claves. También permite distribuir tales claves, a través de un canal seguro. La creación de un canal seguro para el envío de información de autenticación en EAP es muy importante, debido a que el AS generalmente puede estar ubicado físicamente en un lugar remoto, por lo que se requiere enviar tales datos a través de Internet. Entonces, la necesidad de tener un camino seguro por donde transmitir la información, toma mayor relevancia (Chen & Wang, 2005).

El funcionamiento de EAP en una red Wi-Fi se puede describir mediante la siguiente serie de pasos:

1. Se inicia la comunicación mediante el proceso de asociación entre el suplicante (STA) y el autenticador (AP). Como se analizó anteriormente el AP puede enviar una solicitud a la STA o la STA puede enviar un mensaje de petición conocido como EAPOL-Start, para iniciar la asociación. La asociación se realiza a través de un puerto no controlado de IEEE 802.1X.

2. Luego el autenticador preguntará las credenciales de identificación del suplicante, mediante un mensaje EAP.

3. El suplicante enviará su información de identificación al autenticador a través de un mensaje de respuesta EAP; y a su vez, el autenticador reenviará tales datos a un AS RADIUS para que confirme la identidad del suplicante.

4. Opcionalmente, en el proceso de autenticación de credenciales del suplicante por parte del AS RADIUS, se crea un túnel SSL (Secure Sockets Layer, Capa de conexión segura) / TLS[16](Transport Layer Security, Seguridad de la capa de transporte) para transportar la información de autenticación.

5. A través del túnel SSL/TLS el AS RADIUS envía el mensaje Challenge encapsulado en un paquete RADIUS hacia el autenticador. El autenticador envía un mensaje EAP consultando las credenciales del suplicante a través de un paquete TTLS o PEAP.

6. El suplicante retornará un mensaje con sus credenciales hacia el autenticador. El autenticador reenviará tal información hacia el AS RADIUS como un mensaje de respuesta.

7. Se cierra el túnel SSL/TLS creado para proveer un canal seguro para la información.

8. Posteriormente, el servidor RADIUS enviará al autenticador, la respuesta de aceptación o rechazo de la información enviada por el suplicante. Así mismo, el autenticador enviará la respuesta del AS al suplicante.

9. Finalmente, si la respuesta fue afirmativa, el suplicante y el autenticador, comenzarán con la creación de la clave y el saludo de 4 vías.

[16] Protocolos de cifrado empleado para la autenticación de dispositivos mediante equipos remotos. Generalmente la comunicación se hace a través de Internet.

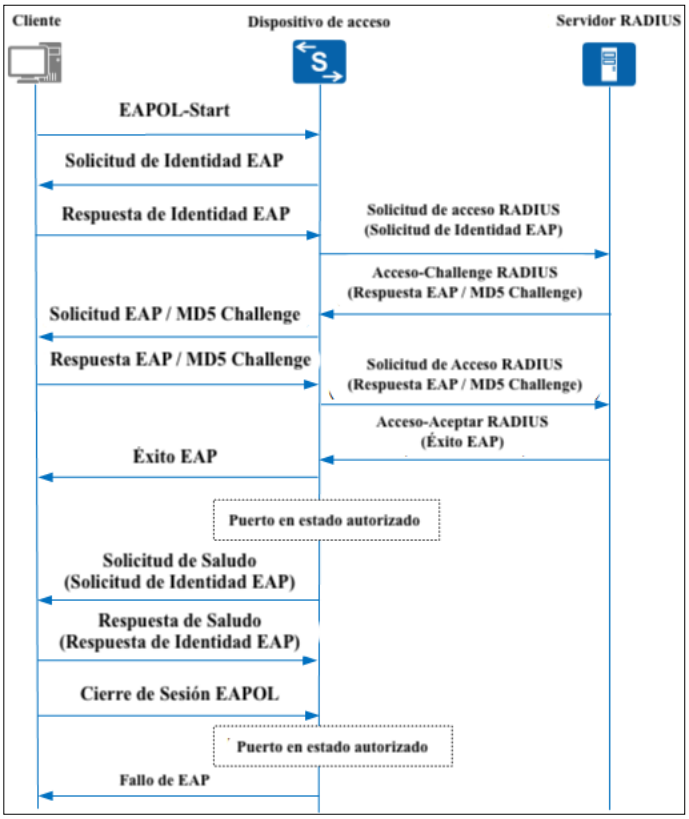


Figura 16: Autenticación mediante EAP.
Copyright 2019 Understanding 802.1X Authentication por Huawei (Huawei, 2019).

4.9.2.1. Multiplexación EAP

La multiplexación EAP consiste en que un servidor EAP configurado con los diferentes métodos EAP pueda diferenciar entre las distintas comunicaciones que tiene al mismo tiempo. Cada comunicación establecida tiene su propio método EAP de autenticación.

Esta aplicación es muy útil para las empresas, puesto que pueden optimizar la seguridad de sus aplicaciones a través de un mismo servidor. A diferencia, de tener que dedicar y configurar un mismo equipo para cada comunicación realizada.

4.9.2.2. Tunelización EAP

La tunelización EAP es una técnica de encapsulación anidada, cuyo propósito es el de enviar dos o más métodos EAP a través de un mismo paquete. Esta función permite que dos o más métodos EAP requeridos para una aplicación, puedan ser enviados en un solo trayecto. Por tanto, ambos métodos enviados deben guardar relación con respecto a la función que se está desarrollando en la comunicación.

Esta característica es aprovechada en las redes WLAN para transportar la información de autenticación mediante uno o más métodos EAP. La tunelización permite crear caminos seguros, cuando se conoce que para la información puede verse comprometida a lo largo del trayecto (Chen & Wang, 2005).

Con referencia a la Figura 16, se puede crear un túnel para enviar las credenciales de identificación entre el suplicante (STA), el autenticador (AP) y el servidor (AS), en caso de que el servidor RADIUS se encuentre ubicado en algún lugar remoto. Para esto se podría emplear un túnel SSL/TLS utilizado para comunicar con servidores a través de Internet.

4.9.3. Métodos EAP

Se conoce como métodos EAP a los distintos mecanismos de autenticación que son soportados por EAP. Estos métodos están diseñados para emplearse en diferentes entornos de las redes, como redes telefónicas o celulares.

Sin embargo, no todos los protocolos son aptos para utilizarse, porque no cuentan con las características de seguridad necesarias para la aplicación. Por tal motivo, no todos los métodos de autenticación soportados por EAP, son utilizados en las redes Wi-Fi.

Existen algunos parámetros que deben cumplir los métodos EAP para que puedan ser utilizados en las redes WLAN, aunque no todos son obligatorios. Los requisitos de los métodos EAP se resumen la tabla 2.

Tabla 4: Requisitos de seguridad de los métodos EAP para las redes WLAN.

Requisito de Seguridad	Nivel de Requerimiento	Explicación
Derivación de clave	Obligatorio	Capacidad del método para derivar la información de la clave que se utilizará para elegir el mecanismo de encriptación en las sesiones de Wi-Fi.
Dificultad de la clave	Obligatorio	Medida de dificultad de la clave de derivación, expresada en número de bits.
Autenticación mutua	Obligatorio	La autenticación mutua se da cuando la STA autentica al AS, y el AS a su vez, autentica a la STA, empleando el mismo método EAP, en el mismo intercambio de información. El uso de un método EAP distinto, en un intercambio de información independiente, no se puede denominar autenticación mutua.
Equivalencia de estado compartida	Obligatorio	El suplicante EAP y el AS deben tener las mismas propiedades de seguridad del método EAP utilizado. Por tanto, deben compartir el número de versión del método, las credenciales proporcionadas y cualquier otro parámetro importante que haya sido negociado. Ambos dispositivos deben reconocer los parámetros del otro dispositivo.
Resistencia frente a ataques del tipo diccionario	Obligatorio	Fortaleza del método EAP, ante un ataque que se basa en "adivinar" la contraseña. Por tanto, el método EAP debe impedir que se capture el tráfico producido, para evitar que el atacante adivine la contraseña.
Resistencia frente a ataques del tipo Man-in-the-middle	Obligatorio	El método EAP debe imposibilitar que un atacante, filtre la información transmitida entre el AP y STA, a través de otro dispositivo que no este autorizado. Este ataque se centra en suplantar la identidad de cualquier dispositivo que interviene en la comunicación Wi-Fi.
Negociación de cifrado protegido	Obligatorio	Hace referencia al acuerdo que se llega, acerca de la clave y mecanismo de cifrado que se utilizará para proveer de integridad y confidencialidad a la comunicación EAP. Este acuerdo, no abarca el

		cifrado que se usará en tráfico generado por la STA y el AP.
Fragmentación y reensamblaje de paquetes	Recomendado	Posibilita que un método EAP pueda manejar paquetes más grandes que un MTU de EAP (1020 Octetos).
Confidencialidad	Recomendado	Se basa en la encriptación que un método EAP puede dar a los distintos mensajes que se producen, durante la asociación de un dispositivo suplicante.
Vinculación con el canal	Opcional	Se utiliza para garantizar que la identidad del dispositivo autenticador (AP) sea suplantada, cuando el equipo este en modo traspaso. Una forma de conseguirlo, es mediante la dirección MAC u otra información propia del dispositivo, la cual servirá como dato de entrada para generar una clave. Esto con el propósito de impedir que existan dispositivos no autorizados, registrados en la red.
Reconexión rápida	Opcional	Capacidad del método para re-asociar de manera segura el mismo dispositivo, pero con menos mensajes que la asociación inicial.

Nota. Recuperado de Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Copyright 2007 por el Instituto Nacional de Estándares y Tecnología NIST.

El ataque Man-in-the-middle es uno de los retos que tienen las redes RSN IEEE 802.11, para lograr un sistema completamente seguro. El problema con este tipo de ataques, es que las redes basadas en EAP son vulnerables.

El modo de operación de Man-in-the-middle es secuestrar la comunicación, mediante la suplantación del dispositivo autenticador de la red (AP). Debido a que el AP es el dispositivo intermedio entre la STA y el AS, todo el flujo de datos que contiene la información de identificación de los equipos, así como de sus credenciales, pasa a través del AP. Por tanto, si un atacante desea filtrar todo el tráfico de la red, simplemente sustituirá el AP de la red por uno falso, y se autenticará como si fuera el dispositivo original.

4.9.3.1. EAP-TLS

EAP-TLS se caracteriza principalmente por su fuerte encriptación que es empleada en la autenticación de las entidades, mediante una clave pública. Esto conlleva a que la infraestructura de la red tenga que ser mucho mayor puesto que los requerimientos de seguridad son elevados. Debido a esto, y al hecho de que se tenga que utilizar un AS como dispositivo autenticador externo, es que este método es utilizado por organizaciones y empresas.

Para que este método funcione adecuadamente, la STA debe tener implementada un certificado único, que se puede introducir a través de herramientas externas.

Se pueden utilizar diversas herramientas para que se pueda crear una infraestructura de clave única (PKI), que es como se conoce a esta configuración. Algunas de estas son dispositivos de almacenamiento externo como USBs, Tarjetas SD, Discos Duros o se puede utilizar el mismo firmware del dispositivo. Además, independiente de la herramienta usada, estas deben estar bloqueadas por alguna clave, frase, o PIN (Número de Identidad Personal), para evitar que algún usuario externo tenga acceso a los certificados.

No obstante, aunque el sistema de seguridad sea mucho más robusto que propuestas anteriores, aún existen ciertos elementos inherentes de las empresas que pueden representar la vulnerabilidad completa del sistema.

El hecho de otorgar la contraseña o el permiso a un empleado, supone que se esta entregando la seguridad completa de la red, y por ende la información total de la empresa. Por tanto, es difícil mantener el control de la estructura si uno o más usuarios cuentan con la clave de acceso a la red, e inclusive se pueden dar casos de que tales empleados realicen copias de tal clave. Debido a esto, es que se asocia la mayoría de ataques suceden desde la parte interna de una red, más que de la externa.

Otro problema que se presenta en estas redes EAP-TLS, es que requieren de más pasos de autenticación que en otros métodos. En usuarios de dispositivos móviles que requieren de un servicio veloz, se verían afectados por este inconveniente.

4.9.3.2. EAP-TTLS

Este método es una mejora a EAP-TLS, puesto que añade la tunelización para agregar el mecanismo de autenticación unidireccional TLS y de la autenticación mutua.

En el caso de la autenticación unidireccional, consiste en la autenticación del AS con la STA, y posteriormente se produce la autenticación de la STA con el AS, y todo esto a través de un túnel seguro de TLS.

La etapa de autenticación de la STA con el AS, se denomina "Método de Autenticación Interna". En esta etapa se utilizan los mensajes conocidos como "InnerApliccation" los cuales describen los algoritmos y protocolos que se soporta. El formato de estos mensajes se conoce como AVP (Pares Atributo Valor) y es compatible con otros protocolos de autenticación, como RADIUS (Chen & Wang, 2005).

El funcionamiento de este método es similar a como se producen las búsquedas en un sitio web. El usuario (STA) confirma la identidad del servidor (AS) por medio del certificado, que fue enviado a través de un canal seguro TLS. Luego el usuario a través de ese mismo canal, envía sus credenciales de identificación para completar la autenticación.

La ventaja que tiene este método frente a EAP-TLS, es que soporta sistemas de autenticación heredados, que son empleados para la autenticación interna de la red. Esto representa que la estructura KPI podría reemplazarse por un sistema menos complejo, que solo requiere la instalación de los certificados en pocos AS y ya no en STAs. Aunque este sistema solo aplica en sistemas de registro robusto, como sistemas biométricos o claves cifradas avanzadas.

Por otra parte, las desventajas que tiene este sistema frente a otros, es que aún es débil frente a ataques Man-in-the-Middle, aunque es más robusto frente a ataques de repetición y de diccionario. Además, este método depende estrechamente del método de autenticación interna que use, por lo que, si se usa un sistema de autenticación débil el sistema completo también lo será.

4.10. RADIUS

4.10.1. Introducción

Actualmente las redes están compuestas de varios dispositivos que generan, envían y reciben tráfico de la misma red o del Internet. La necesidad de gestionar cada dispositivo conectado, se vuelve cada vez más complejo entre aumenta el número de equipos. Además, conforme más equipos tratan de ingresar a la red, se necesita tener mayor control sobre quién es ese dispositivo, que va a hacer y que tiene permitido hacer (Authetication, Authorization and Accounting; Autenticación, Autorización y Registro).

El uso de servidores permite tener una administración centralizada y de manera remota, sobre que dispositivos ingresan a la red y que pretenden realizar. Además, al igual que una base de datos, permiten tener un registro de todas las conexiones producidas.

Para poder realizar una adecuada gestión de autenticación en una red, el servidor debe implementar un protocolo que se encargue de registrar las sesiones y solicitar la identificación de los usuarios, y todo esto sobre Internet. Con base a esto se desarrolló el protocolo RADIUS, que proporciona servicios de AAA a los dispositivos de una determinada red y considera el tipo de servicio para el cual se está solicitando acceso, por ejemplo: Telnet, SSH, PPP, etc.

4.10.2. Generalidades

RADIUS se basa en el modelo cliente-servidor NAS (Network Access Service). La función del cliente es transferir la información del usuario hacia el servidor designado, con el fin de obtener una respuesta que le permita tener acceso al servicio solicitado. Por otra parte, el servidor se encarga de recibir las solicitudes del cliente, y analizar si la información recibida coincide con lo establecido en su configuración. Dependiendo del resultado del análisis, el servidor enviará la respuesta al cliente (IETF, 2000a).

De igual manera, el servidor RADIUS puede prestar su servicio a otros servidores, actuando como un cliente proxy.

4.10.3. Seguridad

La seguridad del protocolo RADIUS se basa en una clave denominada “Secreto Compartido” que esta implementado de manera manual en el cliente y en el servidor. El objetivo de la clave es proporcionar una autenticación segura entre ambas entidades, sin requerir que la información de identidad se envié por la red.

Todos los datos que se transmiten y reciben en una sesión de RADIUS, están encriptados para que no exista riesgo de filtrado de información en todo el trayecto que se recorre desde el cliente hacia el Internet y hacia el servidor.

4.10.4. Funcionamiento

RADIUS al estar basado en un modelo cliente-servidor, se puede describir su modo de operación en dos etapas, la etapa del cliente y la etapa del servidor.

En la primera etapa, el usuario envía su información de autenticación al cliente RADIUS. Tal información puede ser un nombre de usuario y una contraseña que se establecieron con anterioridad.
Una vez que el cliente RADIUS obtiene la información de autenticación del usuario, este procede a armar un paquete de solicitud conocido como “Petición de Acceso”. La solicitud de acceso contiene el nombre y la contraseña del usuario, el identificador del cliente y el identificador del puerto al que el usuario está accediendo. Debido a que se está enviando la contraseña para la autenticación, esta debe ser cifrada mediante el algoritmo MD5 (IETF, 2000b).

Posteriormente, el cliente envía la petición de acceso al servidor RADIUS a través de la red o de Internet. El cliente esperara la respuesta del servidor un determinado tiempo, en caso de que no exista una respuesta, se reenvía el mensaje. Si el servidor principal no envía una respuesta, el cliente puede optar entre enviar la solicitud a otro servidor u otros servidores secundarios.

El servidor al recibir la solicitud con los datos del usuario, procede a corroborar si la información de autenticación coincide con la implementada en su configuración. Si la petición de acceso no cuenta con el secreto compartido, se descartará automáticamente.

Por otro lado, si la información de identificación del cliente es correcta, el servidor buscará en su base de datos, el nombre del usuario solicitante. La entrada con el nombre del usuario, contiene una lista de requisitos que se deben cumplir para permitir el acceso. La verificación de los requisitos siempre va asociada con la contraseña, aunque también se pueden emplear otros parámetros como el identificador del cliente o del puerto.

El servidor también puede comprobar los requisitos de acceso del usuario, a través de otros servidores. Para este caso, el servidor RADIUS funciona como cliente proxy.

Si alguno de los requisitos para el acceso no se cumple, el servidor RADIUS emitirá un mensaje denominado “Acceso-Rechazo” en el cual se indica el rechazo de la solicitud. Por el contrario, si todos los requisitos se cumplen, el servidor puede responder a la solicitud con un mensaje de desafío (challenge) para el usuario (IETF, 2000b).

El mensaje de desafío enviado al cliente busca confirmar la identidad del usuario. En el mensaje se puede incluir un texto que indique al usuario que debe responder a ese desafío. El usuario enviará la respuesta al servidor y este a su vez, puede responder con mensaje de aceptación o rechazo.

Si todos los requisitos de acceso se cumplen, los valores de la configuración del usuario en la base de datos del servidor cambiarán a “Acceso Aceptado”. Estos valores definen el servicio que está solicitando el usuario y cuáles son los parámetros necesarios para usar ese servicio.

5. METODOLOGÍA

En este capítulo se abordará el análisis de la existencia de las vulnerabilidades analizadas en el capítulo anterior, con base a la recopilación teórica y experimental. Para la evaluación experimental se empleará herramientas tanto de software como de hardware, que están enfocadas a vulnerar el sistema de seguridad WPA-2.

El propósito de vulnerar el sistema de seguridad, es obtener información práctica sobre el proceso que realizan los ataques para penetrar la red Wi-Fi. Esto servirá como base de estudio para las mejoras a tener en cuenta en las siguientes versiones de seguridad de esta tecnología. Además, permitirá corroborar o rectificar la hipótesis planteada en este estudio:

- La tecnología Wi-Fi no es segura debido a que su sistema de seguridad es deficiente.

Para determinar las herramientas que se utilizarán para el ataque controlado se consideran los siguientes parámetros:

- Software que sea compatible con los ataques para Wi-Fi.
- Tipos de ataques compatibles con las herramientas.
- Capacidad de resistir frente a los ataques.
- Versión de la tecnología Wi-Fi soportada.
- Versión del sistema de seguridad Wi-Fi que soporta.
- Tipos de mecanismos de seguridad compatibles.
- Compatibilidad con el software utilizado para ejecutar los ataques.
- Rango de distancia (Elementos de Hardware).

5.1. Materiales

5.1.1. Software para el análisis de la seguridad

La elección del software para el análisis de las vulnerabilidades de la tecnología Wi-Fi, constituye el elemento principal de la parte experimental. Las características del sistema informático influyen en los parámetros que se van a evaluar. Por tanto, una adecuada elección del programa o sistema operativo a utilizar, permite obtener resultados más fehacientes.

Para realizar una evaluación de la seguridad informática, generalmente se utiliza un sistema operativo, debido a que permiten instalar un conjunto de herramientas que están destinadas a diferentes tipos de ataques. Dependiendo del sistema operativo, existirá un mayor número de programas o servicios compatibles.

Un parámetro importante a considerar en la elección del sistema operativo, es el propósito por el que fue creado. Existen sistemas operativos desarrollados para ciertas áreas de estudio, los cuales incorporan aplicativos necesarios para ese campo en específico. De igual manera, también hay sistemas operativos multipropósito que están enfocados a desarrollar distintos tipos de tarea de diferentes campos. Sin embargo, requieren de componentes adicionales para ciertos programas determinados.

En el área de seguridad informática, también existen sistemas operativos creados para la evaluación de seguridad de los equipos u otros sistemas. La mayoría de estos, están basados en Linux, por lo tanto, son libres y gratuitos.

Sin embargo, al disponer de algunas alternativas, es necesario determinar cual es la más óptima para este estudio. En la Tabla 3 se muestra el S.O. (Sistema Operativo) más conveniente.

Tabla 5: Requisitos del Sistema Operativo

Requisitos	Descripción	Windows	Mac OS	Kali Linux	Black Arch Linux	Parrot OS
Software dedicado para ataques informáticos	Enfoque del sistema operativo al campo del hacking ético y la ciberseguridad.	✗	✗	✓	✓	✓
Soporte para programas de ataques informáticos	Compatibilidad del S.O. con programas diseñados para ataques informáticos.	✗	✗	✓	✓	✓
Servicios de red deshabilitados	Capacidad para desactivar los servicios de red para evitar ataques hacia el usuario.	✗	✗	✓	✗	✗
Modo Forense	Modo de ejecución del S.O utilizado para buscar información del sistema sin alterar su funcionamiento.	✗	✗	✓	✗	✓
Compatibilidad con la mayoría de tarjetas de red para monitoreo	Capacidad del S.O. para emplear diferentes tipos de tarjetas de red (externas) para monitorear paquetes.	✗	✗	✓	✓	✓
Robustez del Sistema	Resistencia ante amenazas externas existentes que podrían comprometer el S.O.	✗	✓	✓	✓	✓
Soporte para Sniffers (Al menos uno)	Capacidad de ejecutar al menos un programa tipo Sniffer.	✓	✓	✓	✓	✓
Posibilidad de Configurar Servidores de Autenticación	Soporte para la configuración de servidores de autenticación como RADIUS.	✓	✓	✓	✓	✓
Capacidad de ejecutarse en dispositivos móviles	Capacidad de ejecutarse en dispositivos con procesadores ARM, generalemnte dispositivos móviles.	✗	✗	✓	✓	✓
Entorno amigable para usuarios de todos los niveles.	Facilidad de navegación sobre su entorno gráfico para todos los niveles (Inicial, Intermendio y Experto).	✓	✓	✓	✗	✓
Estabilidad	Pocos errores en el sistema.	✗	✗	✓	✓	✓
Fácilmente configurable	Herramientas intuitivas que no son muy complejas de utilizar y configurar.	✓	✓	✓	✗	✓
Compatibilidad con los sistemas de seguridad WPA-2 y WPA-3	Soporte para los sistemas de seguridad de las redes Wi-Fi.	✓	✓	✓	✓	✓
Sistemas basados para ambientes inalámbricos	El sistema operativo fue pensado para trabajar con tecnologías inalámbricas.	✗	✗	✗	✗	✓
Ejecución en equipos con pocos recursos	Capacidad del S.O de ejecutarse adecuadamente en computadores con poco hardware o hardware antiguo.	✗	✗	✓	✓	✓
Disponibilidad de herramientas de Pruebas de Resistencia	Compatibilidad con herramientas que permitan realizar ataques DoS.	✓	✓	✓	✓	✓
Disponibilidad de Información en foros	Existe recopilación teórica sobre el funcionamiento del sistema operativo, las herramientas, ataques y ejemplos.	✓	✓	✓	✗	✗
Gratuidad	El sistema operativo no requiere de una licencia pagada para poder utilizarse.	✗	✗	✓	✓	✓
Código Abierto	El S.O. permite acceder a su código fuente.	✗	✗	✓	✗	✓
Portabilidad	El S.O. puede instalarse en cualquier dispositivo de almacenamiento para poder llevarlo a cualquier lugar.	✗	✗	✓	✓	✓

Fuente: Autor.

Nota: Los requisitos que se muestran en la tabla, son basados en propiedades necesarias para este estudio.

Con base a los requisitos necesarios para la experimentación, se optó por utilizar el sistema operativo Kali Linux como software para realizar las pruebas.

A pesar de que existen alternativas más actuales como Black Arch Linux o Parrot OS; que al igual que Kali Linux, son sistemas enfocados para hacking ético, no cuentan con algunas propiedades necesarias para el estudio.

En la Figura 17, se muestra que la porción más grande es la de Kali Linux. Tal porción representa la mayoría de características que cumple este sistema por encima de los demás. Por tanto, este sistema es el más adecuado para este estudio.

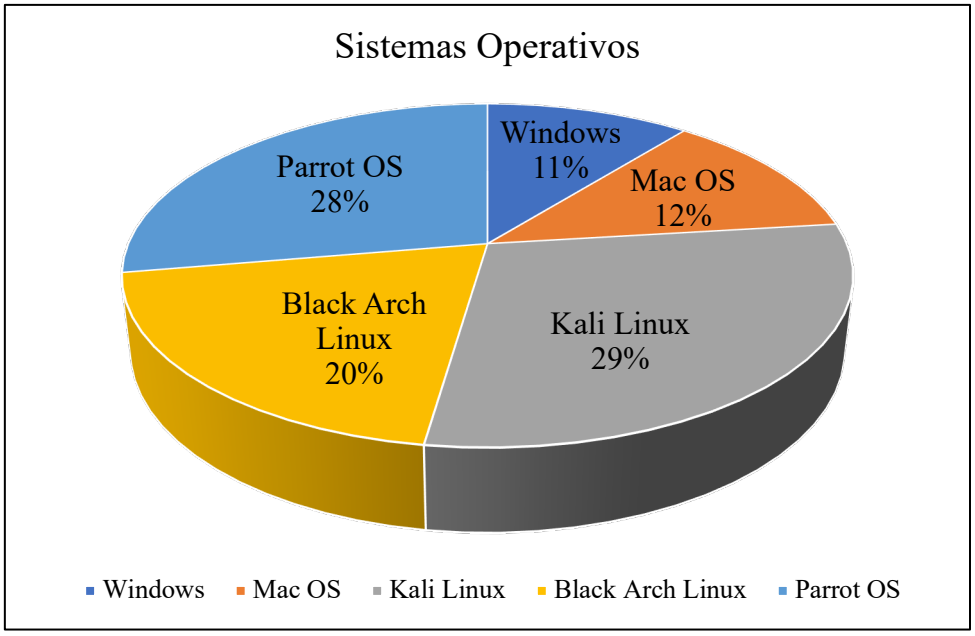


Figura 17: Representación del porcentaje de características cumple cada sistema operativo. Fuente: Autor.

En la Tabla 4 se indican algunas características de Kali Linux que son necesarias para la parte experimental de este estudio. Estas se basan en herramientas o programas que realizan un tipo de ataque en específico.

Tabla 6: Características de Kali Linux

Caracteríticas	Descripción
Captura de Paquetes y Agrietamiento de contraseñas	Esta herramienta es una suite de herramientas que permiten capturar los paquetes, des-autenticar usuarios, inyectar tráfico, descifrar claves, etc. Soporta los ataques de Diccionario y Fuerza Bruta. Además, es compatible con WEP, WPA y WPA-2.
Suplantación de Identidad	Kali Linux cuenta con la herramienta Wifite para falsificar las direcciones MAC de los usuarios conectados, para posteriormente suplantar su identidad. Esta herramienta es compatible con WEP, WPA y WPA-2.
Monitoreo de Paquetes	Se realiza mediante el programa Wireshark. A pesar de que esta herramienta no es propia de Kali, es un aplicativo muy util para analizar el tráfico generado por los usuarios conectados a la misma red.
Vulnerar IEEE 802.1X	Mediante Hostapd-WPE se pueden realizar ataques de suplantación de servidores, para vulnerar el sistema WPA-Enterprise.
APs Falsos	Airmon-ng permite crear Access Points falsos para engañar a los usuarios con el fin de obtener su información personal.
MITM	Se pueden realizar ataques Man-in-the-middle mediante la herramienta Ettercap.
DoS	HPing3 es un aplicativo de Kali Linux para realizar ataques de Denegación de Servicios mediante paquetes de TCP/IP.
Seguridad	Kali Linux se caracteriza por ser un sistema confiable y robusto para realizar auditorias de seguridad. Esto se debe, a que cada nueva versión de este S.O. esta examinada y verificada por los desarrolladores.
Soporta configuración de servidores	Mediante FreeRadius se puede configurar un servidor RADIUS. Este servicio es muy útil cuando se requiere de mayor seguridad en la red, sin querer invertir en un servidor dedicado.
Portable	La versión Kali Linux Live permite ejecutar Kali Linux en cualquier unidad de almacenamiento. Esto proporciona una poderosa herramienta de hackeo que puede ser utilizada en cualquier lugar y en cualquier computador.

Fuente: Autor.

5.1.2. Herramientas de monitoreo

La mayoría de computadores actuales no incluyen una antena que permita realizar el monitoreo de paquetes de las redes Wi-Fi. Este elemento es muy importante para el análisis de seguridad de estas redes, puesto que se requiere de un componente compatible con esta tecnología, para realizar ataques.

A pesar de este problema, existen soluciones complementarias que se pueden emplear para dotar al computador de estas características. En el mercado existen dispositivos denominados “Adaptadores Inalámbricos” que cumplen con esta función.

Los adaptadores inalámbricos, generalmente se emplean para ampliar la ganancia de la señal recibida por el Router o por el AP. Sin embargo, en este estudio, el uso de los adaptadores es para dotar al equipo de la capacidad de monitorear paquetes. Esta característica la puede incorporar cualquier adaptador que tenga un chipset compatible con Kali Linux.

La disponibilidad de estos equipos en el país es limitada, aunque existen varias opciones. No obstante, la elección de cualquier adaptador no influye en los resultados del estudio, puesto que su uso solo se limita a monitorear paquetes y enviar tráfico.

Por tanto, la elección del adaptador inalámbrico radica únicamente en el criterio de selección del autor. Sin embargo, si se considera un parámetro esencial para el estudio, que es la compatibilidad con Kali Linux.

El parámetro principal que se consideró para su adquisición fue la compatibilidad con Kali Linux. Debido a que el sistema operativo Kali Linux, no soporta cierto tipo de adaptadores, se necesita evaluar si el dispositivo obtenido cumple con este requisito.

Tabla 7: Características técnicas de las tarjetas de red para el monitoreo de paquetes.

Características Técnicas	Alfa AWUS036NH	TP-LINK TL-WN722N	Panda PAU06	Sabrent NT-WGHU
Compatibilidad con Kali Linux	Si	Si	Si	Si
Ganancia	5 dBi	4 dBi	N/A	5 dBi
Chipset	Realtek RTL8188RU	Atheros AR9271	Ralink RT3070	Realtek 8187L
Tipo de Antena	1 conector RP-SMA de 2,4Ghz	Desmontable omnidireccional (RP-SMA)	Desmontable omnidireccional (RP-SMA)	Dual omnidireccional
Software disponible (Drivers)	Si	Si	Si	Si
Información disponible	Si	Si	Si	Si
Versión de Wi-Fi soportada	IEEE 802.11b/g/n	IEEE 802.11b/g/n	IEEE 802.11b/g/n	IEEE 802.11b/g/n
Sistema de seguridad Wi-Fi soportados	Admite el cifrado de datos inalámbricos con WEP de 64/128 bits, WPA, WPA2	Soporte WEP 64/128 bits, WPA-PSK/WPA2-PSK, Filtrado inalámbrico de MAC	64/128-bit WEP WPA-PSK / WPA2-PSK WPA / WPA2	Compatible con 64/128 bit WEP, WPA-PSK/WPA2-PSK
Modulación	BPSK, QPSK, CCK y OFDM	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Bandas de frecuencia de trabajo	2.400-2.4835GHz	2.400-2.4835GHz	2.400-2.4835GHz	2.400-2.4835GHz
Modos Inalámbricos	Modo Ad-Hoc/infraestructura	Modo Ad-Hoc/infraestructura	Modo Ad-hoc / infraestructura	Modos ad-Hoc / infraestructura
Interfaz de salida	Mini USB 2.0	USB 2.0	USB 2.0	USB 2.0
Disponibilidad en el país	Si	Si	No	No
Precio	$80	$20	$22	$20

Fuente: Autor.
Nota: Los sistemas de seguridad soportados por los adaptadores inalámbricos, no son relevantes para el análisis de vulnerabilidades, puesto que la seguridad depende únicamente del AP o Router Inalámbrico.

Para este estudio se optó por utilizar el adaptador TP-Link TL-WN722N. Su elección fue basada en las características de: Compatibilidad con Kali Linux y el Filtrado Inalámbrico de MACs. Para mayor información sobre las características de la tarjeta, revisar el Anexo 1.

Figura 18: Adaptador Inalámbrico TP-Link TL-WN722N.
Copyright TP-Link por TP-Link (TP-Link, 2010).

5.1.3. Router Inalámbrico

Los dispositivos encargados de incorporar la seguridad en las redes Wi-Fi, son el Router inalámbrico y el Access Point. Ambos equipos deben ser compatibles con los sistemas de seguridad WPA, WPA-2 y WPA-3, para proteger a la red de amenazas externas.

Para este estudio se requiere que cualquiera de los dos dispositivos soporte el último estándar lanzado por la Wi-Fi Alliance, IEEE 802.11ax comercialmente conocido como Wi-Fi 6. Además de incorporar el último sistema de seguridad disponible que es WPA-3. De igual manera, se debe considerar un equipo con un amplio rango de cobertura.

Tanto el Router como el AP deben establecer un rango de cobertura amplio para cubrir la mayoría de zonas de una habitación u oficina. Esto permite que los usuarios alejados se puedan conectar desde cualquier punto que este dentro del rango de la señal.

El rango de cobertura es un parámetro importante, puesto que en la evaluación de seguridad se necesita probar que un ataque a la red Wi-Fi puede ser proveniente de usuarios que están ubicados a una gran distancia del equipo. Por tanto, se necesita un dispositivo con un amplio rango de funcionamiento, para que los resultados sean lo más fiable posible.

Además, de estas características también es necesario precisar de un equipo que cumpla con algunos otros requisitos. En la tabla 6 se muestran los diferentes dispositivos a evaluar.

Tabla 8: Requisitos del Router Inalámbrico

Requisitos	Descripción	TP-Link AX1800	Asus RT-AX82U	D-link Ac 2100	Netgear Nighthawk RAX40	Linksys MR7350	Xiaomi Wi-Fi AX3
Soporte IEEE 802.1ax	El equipo debe soportar la última version de Wi-Fi, que es Wi-Fi 6.	✓	✓	✗	✓	✓	✓
Soporte para WPA3	El equipo debe incorporar el último sistema de seguridad certificado por la Wi-Fi Alliance, que es WPA-3.	✓	✓	✓	✓	✓	✓
Soporte para WPA-2 Personal y Enterprise	El equipo debe soportar las versiones anteriores de seguridad de WPA-2, en sus dos versiones.	✓	✓	✓	✓	✓	✗
Rango de cobertura mayor	Se requiere que el equipo pueda cubrir una oficina o un hogar.	✓	✓	✓	✓	✓	✓
Tecnología MIMO o MU-MIMO	El equipo debe poder comunicarse con otros dispositivos de forma simultanea.	✓	✓	✓	✓	✓	✓
Rompemuros	Las paredes de un hogar o de una oficina pueden atenuar la potencia de la señal. Por tanto, se necesita un equipo que pueda emitir su señal, a traves de los obstaculos.	✓	✓	✓	✓	✓	✓
Soporte para multiples dispositivos	Combinado con la tecnología MIMO, el equipo debe ser capaz de soportar multiples dispositivos, tales como: Sensores, Computadoras, Laptops, Smartphones, etc.	✓	✓	✓	✓	✓	✓
Compatibilidad con estandares anteriores	El equipo debe ser compatible con los estandarés IEEE 802.11ac/n/b/g.	✓	✓	✓	✓	✓	✓
Mecanismos de filtrado de MACs	Se debe poder controlar el acceso a la red, mediante el acceso de dispositivos configurados previamente por su dirección MAC.	✓	✓	✓	✓	✓	✓
Soporte de Seguridad Firewall	El equipo debe contanr con un cortafuegos para impedir ataques DoS.	✓	✓	✓	✓	✓	✓
Procesardor Eficiente	Se debe tener un procesador potente para que pueda procesar los diferentes flujos de los dispositivos de manera adecuada.	✓	✓	✗	✓	✗	✓
Beamforming	El equipo debe poder establecer un Flujo Individual para cada comunicación con los dispositivos para mejorar la transmisión y recepción de datos.	✓	✓	✗	✓	✓	✓
Trabaja en Doble Banda	Debe poder trabajar en las bandas de 2,4 Ghz y 5 GHz	✓	✓	✓	✓	✓	✓
Soporte para WPS	Se debe poder crear un red WLAN segura.	✓	✓	✓	✓	✓	✗
Software Disponible	El equipo debe contar con drivers y actualizaciones.	✓	✓	✓	✓	✓	✓
Disponibilidad en el país	La disponibilidad en stock del equipo en el país facilita su adquisición.	✓	✗	✓	✗	✗	✗
Interfaz WAN	Debido a que la mayoría de datos buscan salir hacia Internet, el equipo debe tener un puerto WAN. De igual manera los ataques suelen infectar equipos para enviar sus datos a traves de Internet.	✓	✓	✓	✓	✓	✓

Fuente: Autor.

Con base a los requisitos de la parte experimental se decidió por utilizar el Router TP-Link AX1800 para desarrollar los ataques a la red. Esto debido a que este equipo cumple con las características necesarias para el estudio.

En la Figura 19, se muestra que la porción más grande es la de TP-Link AX1800. Tal porción representa que este equipo cumple todas las características. Por tanto, este dispositivo es el más adecuado para este estudio. Para mayor información sobre las características de este Router Inalámbrico, revisar el Anexo 1.

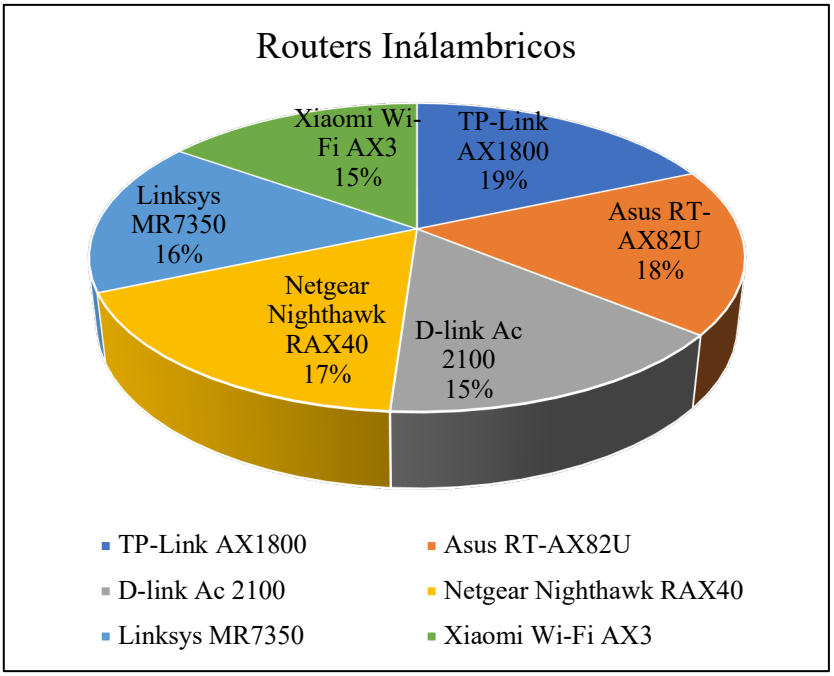


Figura 19: Representación del porcentaje de características cumple cada Router Inalámbrico. Fuente: Autor.

Figura 20*:* Router Inalámbrico TP-Link AX1800 Archer AX20.
Copyright TP-Link por TP-Link (TP-Link, 2020).

5.2. Vulnerabilidades de WPA-2 (Métodos)

5.2.1. Introducción

WPA-2 es el sistema de seguridad implementado en Wi-Fi para proporcionar de protección a la red. Este sistema está basado en los mecanismos de seguridad de IEEE 802.11i. En sus dos versiones (WPA2-Personal y WPA2-Enteprise) se emplea el mecanismo de cifrado AES, que es un sistema de encriptación más robusto que sus versiones anteriores.

Este sistema mejora las características de sus predecesores, incorporando una nueva técnica de cifrado, y mejoras en sus mecanismos de autenticación (Tsekleves, 2017). No obstante, a pesar de la evolución en sus métodos de seguridad, este sistema puede ser fácilmente vulnerado.

La transmisión y recepción de forma inalámbrica de Wi-Fi, la hace susceptible a ataques MITM. La capacidad del AP de extender su rango de cobertura a mayor distancia, posibilita a un atacante de conectarse dentro de este rango para poder vulnerar el sistema.

Además del ataque MITM, las redes Wi-Fi también son propensas a ataques de fuerza bruta. Este ataque busca penetrar la red, adivinando la frase de clave que se establece en el AP, para tener acceso a la red y al tráfico generado. De igual manera sucede con los ataques DoS y DDoS, que buscan colapsar estas redes.

Las dos versiones de WPA-2, son diseñadas para impedir que todo tipo de ataques sean mitigados. Sin embargo, ambos sistemas aún son propensos a ser vulnerados, puesto que lo ataques también han sido mejorados.

5.2.2. Ataques y Vulnerabilidades

5.2.2.1. Denegación de Servicios (DoS)

El ataque DoS en las redes Wi-Fi, tiene como objetivo sobrecargar la capacidad de procesamiento del router o del AP, “mediante inundación de datos, interferencia de radiofrecuencia o el secuestro de las sesiones de capa 2 ” (Arana, 2006).

5.2.2.2. Interferencia de radiofrecuencia

El sistema de seguridad WPA-2 es vulnerable ante este ataque, puesto que se produce a nivel de capa física. Debido a que Wi-Fi, se ejecuta desde la capa de enlace de datos, es imposible tener control sobre ataques que suceden a nivel físico (Pirayesh & Zeng, 2021).

Este tipo de ataque se enfoca a emitir ruido en las bandas de trabajo de Wi-Fi. Debido a que Wi-Fi, trabaja sobre las bandas ISM, específicamente 2,4 GHz y 5 GHz, puede producirse interferencia que interrumpa el funcionamiento habitual de la red.

La interferencia, también puede producirse de manera accidental, debido a que las bandas ISM son libres. Por lo que, otras tecnologías también pueden operar sobre el mismo rango de frecuencia, causando perturbaciones en la red.

Sin embargo, la interferencia como ataque, causa la caída del servicio, porque los dispositivos conectados no podrán conectarse. Esto debido a que las bandas están ocupadas, ya sea por el ruido o por otros dispositivos que están interfiriendo en la comunicación.

5.2.2.3. Inundación de autenticación y asociación

Este ataque aprovecha que las tramas de gestión y control de Wi-Fi no están protegidas, para descubrir la topología de la red y la ubicación de los dispositivos conectados. De esta manera, el atacante puede localizar a cada uno de los dispositivos para infectarlos.

El propósito de este tipo de inundación, es lograr sustituir la identidad de los dispositivos conectados a esa red, para impedir que los dispositivos reales tengan acceso al servicio. Esto se logra, haciendo que los equipos conectados se vuelvan a autenticar ante el AP, puesto que, cuando se envía una petición de acceso al servicio (asociación) se debe enviar la dirección MAC del equipo. Por tanto, el cracker puede receptar la solicitud enviada, para extraer la dirección física. Luego falsifica la dirección y se hace pasar como el dispositivo original.

Mediante este ataque, se impide que los usuarios legítimos, puedan realizar otra vez el proceso de autenticación y asociación. Por consiguiente, no pueden tener acceso a la red. Además, al ser un ataque del tipo inundación, su objetivo es que la capacidad de procesamiento del AP se agote. Esto lo logra, enviando un gran número de peticiones de acceso, para que el AP se sobrecargue.

5.2.2.4. Inundación de des-autenticación

Este ataque se enfoca en enviar mensajes de des-autenticación a los dispositivos, con el fin de desvincularlos de la red. Al ser un ataque derivado de DoS, su objetivo es el de inhabilitar a los equipos para que accedan al servicio.

En Wi-Fi, las tramas de autenticación no están protegidas, por lo que, el atacante puede falsificar la trama para desvincular a los dispositivos de la red. Además, una petición de des-autenticación no puede negarse, por tanto, el AP no realiza un control sobre la STA que desea abandonar la comunicación.

La inundación de des-autenticación también puede estar dirigida hacia el AP. Para esto, el atacante necesita alterar la información de la trama, haciéndose pasar por el AP. Luego, envía el mensaje de des-autenticación a la dirección de difusión, para que todos los dispositivos conectados, finalicen la conexión.

5.2.2.5. Contramedida TKIP

TKIP cuenta con una característica que impide la recuperación de clave, cuando se han recibido dos tramas MIC incorrectas en un intervalo de 1 minuto. Si esto sucede, el AP suspenderá todos los procesos de TKIP por 1 minuto, y se re-negociaran las claves de la Jerarquía de Claves por Pares y de Grupo (Armitage, 2011).

Con base a este mecanismo empleado en TKIP, el atacante aprovecha para enviar mensajes MIC erróneos, para impedir que el AP logre establecer las claves. De esta manera, el ataque logra la denegación del servicio.

Este ataque también es aplicable a los clientes AES, puesto que el AP emplea la clave de grupo TKIP, si existe un cliente TKIP asociado con los clientes AES.

5.2.2.6. Vulnerabilidad/Amenaza IEEE 802.1X / EAP

Esta amenaza surge de una configuración errónea de los certificados, en el sistema WPA2-Empresarial. Dado que este sistema utiliza un AS RADIUS para la autenticación de los dispositivos, se requiere de ciertos certificados que identifiquen a los equipos que intervienen en la comunicación. Sin embargo, algunos clientes de este servidor, son configurados de tal manera, que acepte los certificados de cualquier servidor asociado a una autoridad equivocada.

El atacante aprovecha tal vulnerabilidad, implementando un AP falso que envía los certificados equivocados al servidor. De esta manera, el proceso de asociación y autenticación, simula ser legítimo, por lo que, dentro de la red pasa desapercibido. Posteriormente, el atacante puede enviar un mensaje de des-autenticación a algún dispositivo conectado, para que este envié su información personal a través del mensaje de solicitud de conexión. Luego, con la información de la STA, puede suplantar su identidad para poder filtrar el tráfico de los demás equipos conectados.

Los certificados que utiliza el atacante, también pueden ser legítimos, sin embargo, son obtenido a través de una certificación pública, la cual no es recomendable para un sistema seguro. Por tanto, para mitigar este ataque, se requiere que el cliente configure el AP para que solo acepte los certificados de la autoridad de certificación correcta.

5.2.2.7. Ataques EAP

Este ataque es similar a los del tipo inundación (DoS), porque se basa en el envió de solicitudes de autenticación EAP hasta que el AP agote sus recursos de procesamiento. De igual manera, el ataque EAP también puede ser aplicado a un servidor RADIUS.

Los ataques EAP de inundación se pueden mitigar mediante un bloqueo temporal de 1 minuto, cuando se han producido tres intentos fallidos de autenticación EAP. Además, este método también impide que se realicen ataques fuerza bruta, que

pretenden obtener las credenciales de autenticación, mediante prueba y error (Armitage, 2011).

Sin embargo, también existen ataques que emplean otros mecanismos de EAP para lograr la DoS. Algunos de estos son (Armitage, 2011):

- Utilizar los mensajes EAPOL-Start para inundar la red.
- Recorrer el identificador EAP (0 – 255).

5.2.2.8. Ataque de Diccionario en WPA2-PSK

La frase de clave utilizada en el sistema WPA2-PSK para evitar que intrusos puedan acceder a la red, puede convertirse en un punto de falla. Esto se debe a que la mayoría de usuarios suelen utilizar claves cortas y simples, fáciles de recordar. Por tanto, a través de un recopilatorio de claves comunes (Diccionario), se puede adivinar cual es la combinación correcta.

El atacante puede filtrar los paquetes en la etapa de asociación e intercambio de claves, para obtener la información relacionada con la contraseña. Luego, solo debe configurar un dispositivo con la contraseña para poder generar y enviar tráfico al AP.

5.2.2.9. Ataque TKIP

La versión WPA2-TKIP, que emplea el protocolo TKIP, como mecanismo de cifrado, puede ser fácilmente vulnerada mediante el ataque TKIP. Este consiste en descifrar los paquetes que contienen la información generada por el usuario, sin requerir la clave de encriptación. Los datos se muestran en texto plano, a pesar de que la clave se mantiene oculta.

El éxito de este ataque depende en gran medida del conocimiento que tiene el atacante sobre los bytes del rango de direcciones IP que maneja la red. Esto porque, "el ataque necesita eliminar el último byte del campo de datos cifrados, para poder adivinar la combinación correcta de ese byte" (González, 2013). Posteriormente, el atacante envía todas las combinaciones (1 byte = 8 bits = 2^8 combinaciones) al AP, hasta que se obtenga la correcta.

El proceso de eliminación y adivinación de bytes, se lo realiza con todos los paquetes encriptados. De esta manera, se obtiene todos los datos de los paquetes, sin utilizar la clave de encriptación para descifrar la información.

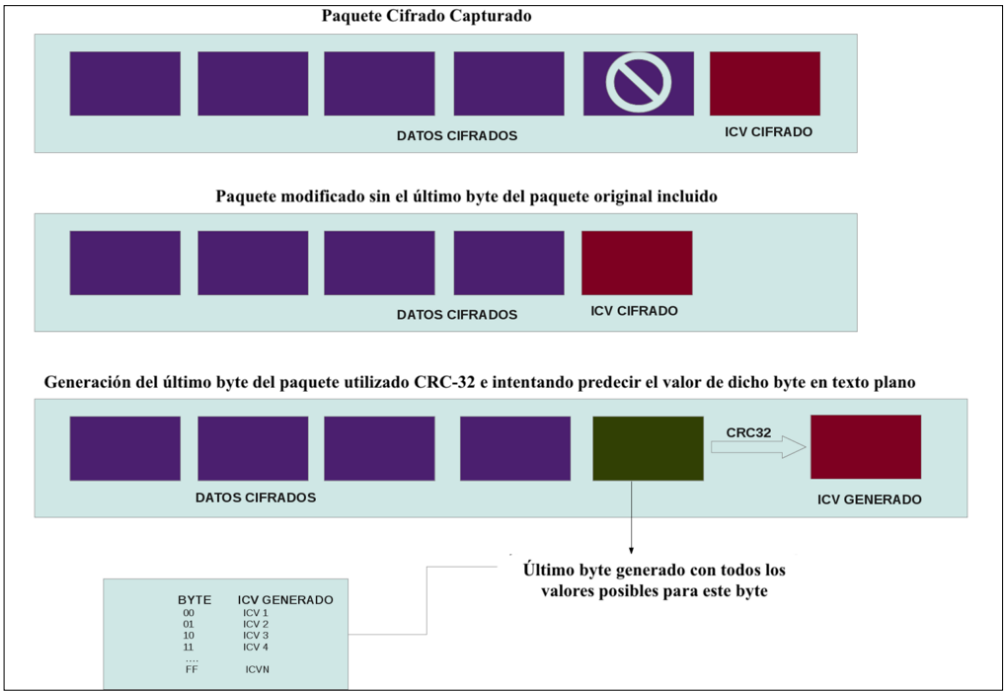


Figura 21: Ataque Kokek ChopChop.
Copyright 2012 Wireless Hacking – Ataques contra WEP – Korek Chopchop – Parte IX por The Hackaway (TheHackerWay (THW), 2012).

Un aspecto importante sobre este ataque es que tiene el mismo principio de funcionamiento que el ataque ChopChop que se realiza en WEP. Esto se debe, a que WPA comparte ciertas características con su predecesor, por lo que, es lógico suponer que los mismos ataques pueden funcionar en ambos sistemas, aunque no de la misma manera.

Para mitigar este ataque se recomienda el uso de AES como método de cifrado.

5.2.2.10. Espionaje

El espionaje dentro de las redes Wi-Fi domésticas, no es muy considerado, debido a las creencias de los usuarios. Sin embargo, esta amenaza es muy común y simple de realizar, puesto que el espía solo requiere obtener la frase de clave o contraseña para tener acceso al tráfico que se origina en la red. Debido a que tal contraseña es la misma para todos los dispositivos que se conecten, solo se necesita conseguirla una vez para comenzar el ataque.

También se debe considerar, que Wi-Fi, permite escuchar el tráfico generado por los otros usuarios conectados, mediante un Sniffer.

Los ataques analizados anteriormente pueden ser utilizados para obtener la contraseña. Sin embargo, este ataque funciona únicamente para el sistema WPA2- Personal, puesto que WPA2-Enterprise distribuye una clave individual para cada equipo.

5.3. Prueba Experimental

5.3.1. Configuración de Kali Linux

Antes de realizar la configuración de Kali Linux, se requiere actualizar el sistema a la última versión disponible. Esto se puede conseguir mediante los siguientes comandos:

- *sudo apt-get update*
- *sudo apt-get upgrade*
- *sudo apt-get dist-upgrade*

Una vez que el sistema operativo está en su última versión, se necesita instalar las cabeceras de Linux para la adecuada instalación de los programas. Se puede utilizar el siguiente comando:

- *sudo apt-get install –y linux-headers-$(uname -r)*

Posteriormente, se deben implementar los programas necesarios para los diferentes ataques.

5.3.2. Configuración de la tarjeta de red

Debido a que por defecto la tarjeta de red esta configurada en modo "Managed" o "Gestionada o Administrada", se debe configurar en modalidad de monitor, para que pueda examinar las tramas que se están enviando constantemente entre los diferentes dispositivos. En este modo de operación la tarjeta es capaz de receptar el tráfico generado por los dispositivos aun cuando no esta asociada a ninguna red.

Antes de configurar la tarjeta, se debe deshabilitar los servicios de red del computador, para evitar que la NIC (Network Interface Card, Tarjeta de Interfaz de red) del computador cause alguna interferencia. Esto se logra a través del siguiente comando:

- *airmon-ng check kill*

Para configurar el adaptador de red en modo monitor, se emplea el siguiente comando:

- *airmon-ng start "interfaz"* (En este caso es la wlan1). Referirse a la Figura 21.

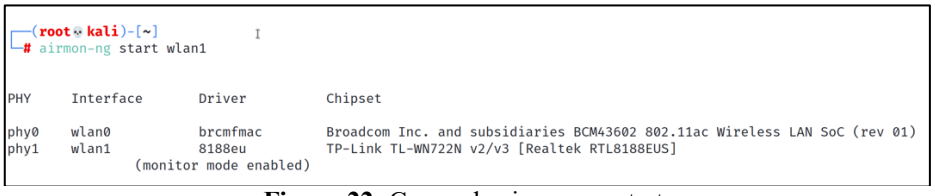


Figura 22: Comando airmon-ng start.
Fuente: Autor.

Se puede confirmar que la tarjeta de red está en modo monitor, mediante el siguiente comando:

- *iwconfig*

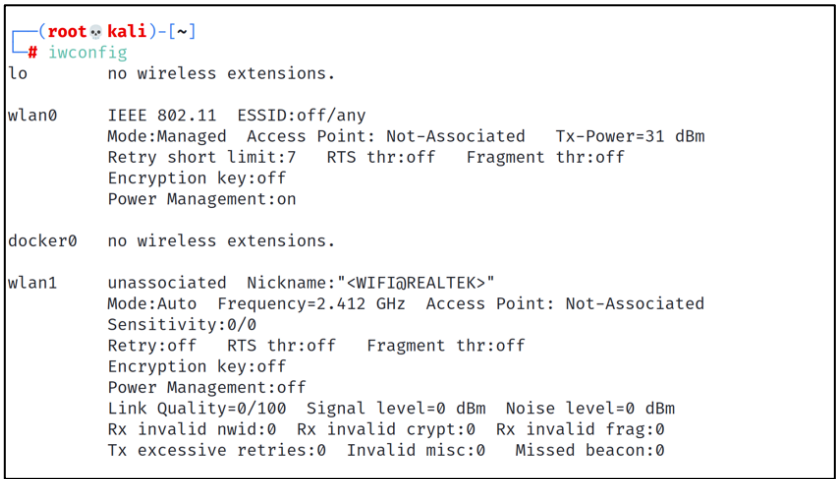


Figura 23: Comando iwconfig.
Fuente: Autor.

5.3.3. Configuración del Router Inalámbrico

El Router Inalámbrico escogido debe ser configurado con los sistemas de seguridad WPA-2 y WPA-3. A través de la interfaz gráfica del router, se pueden modificar los parámetros de seguridad de estos sistemas.

Para acceder a la interfaz gráfica del router, se debe ingresar a cualquier navegador web, como Google Chrome o Mozilla Firefox; y tipiar la dirección IP del router (Generalmente 192.168.0.1).

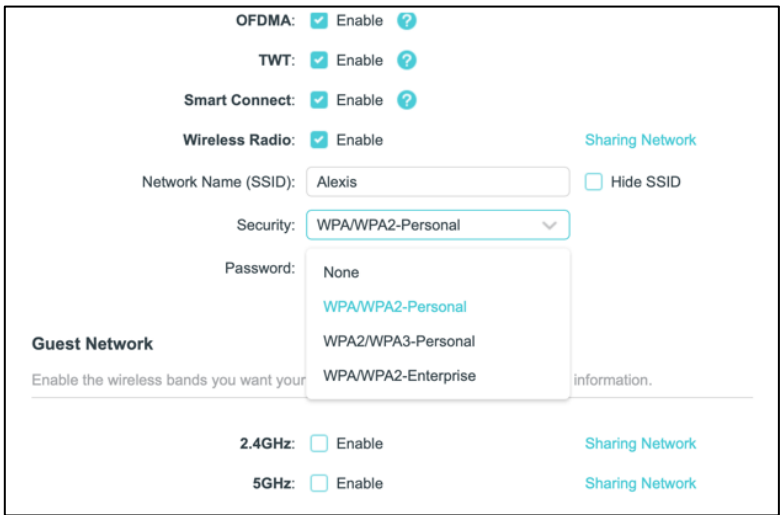


Figura 24: Interfaz gráfica del router TP-Link Archer AX20.
Fuente: Autor.

En la Figura 23 se puede observar los diferentes sistemas de seguridad que soporta el router para proporcionar protección a la red. También permite elegir el sistema de cifrado que se puede utilizar.

Además de estos parámetros, también se agrega una clave de acceso a la red, la cual debe ser lo más compleja posible. Para este estudio, se utilizó una clave lo suficientemente compleja para impedir que un atacante pueda descubrirla con facilidad.

5.3.4. Programas

5.3.4.1. Suite Aircrack

Suite Aircrack es un conjunto de programas desarrollados para evaluar la seguridad de las redes inalámbricas. Generalmente son utilizados para auditar la seguridad de las redes Wi-Fi.

El principio de funcionamiento es el análisis de los paquetes que se envían antes de la asociación. La capacidad de receptar este tipo de paquetes permite al hacker obtener información sobre el dispositivo remitente y destino. Consecuentemente, el atacante puede emplear tal información para ingresar a la red.

La suite de aircrack consta de diferentes aplicativos que permiten realizar auditorías para las redes inalámbricas Wi-Fi. Estas herramientas se centran en 4 tareas que permiten evaluar la seguridad de este tipo de redes. Estas tareas son: Monitoreo, Ataques, Pruebas y Cracking (Aircrack-ng, 2020a).

Algunos de los programas que comprende la suite de Aircrack y que son los más utilizados son:

- Airbase-ng
- Aircrack-ng
- Aireplay-ng
- Airmon-ng
- Airodump-ng

❖ Airmon-ng

Este script se puede utilizar para activar el modo de monitorización en las interfaces inalámbricas. También se puede utilizar para volver del modo monitor al modo gestionado. Introduciendo el comando airmon-ng sin parámetros se mostrará el estado de las interfaces (Aircrack-ng, 2020c).

❖ Aireplay-ng

Según el sitio oficial de Aircrack, se menciona que "Aireplay-ng se utiliza para inyectar tramas. Su función principal es generar tráfico para su posterior uso en aircrack-ng para crackear las claves WEP y WPA-PSK."(Aircrack-ng, 2020b).

Los ataques que soporta este aireplay son (Aircrack-ng, 2020b):

- Ataque 0: Desautenticación
- Ataque 1: Autenticación Falsa
- Ataque 2: Repetición interactiva de paquetes
- Ataque 3: Ataque de repetición de solicitud ARP
- Ataque 4: Ataque KoreK chopchop
- Ataque 5: Ataque de fragmentación
- Ataque 6: Ataque de café-latte
- Ataque 7: Ataque de fragmentación orientado al cliente
- Ataque 8: Modo de migración WPA
- Ataque 9: Prueba de inyección

❖ Airodump-ng

Aircrack define que: "Airodump-ng se utiliza para la captura de paquetes de tramas 802.11 en bruto y es especialmente adecuado para recoger los IVs (Vector de Inicialización) de WEP con la intención de utilizarlos con aircrack-ng."(Aircrack-ng, 2020d).

Además, airodump-ng escribe varios archivos que contienen los detalles de todos los puntos de acceso y clientes vistos (Aircrack-ng, 2020d).

❖ Aircrack-ng

Aircrack-ng es un programa para descifrar claves WEP y WPA/WPA2-PSK de IEEE 802.11 (Aircrack-ng, 2020a).

Para descifrar las claves precompartidas WPA/WPA2, sólo se utiliza un método de diccionario. Se requiere un "handshake de cuatro vías" como entrada. En el caso de los handshakes WPA, un handshake completo se compone de cuatro paquetes. Sin

embargo, aircrack-ng es capaz de trabajar con éxito con sólo 2 paquetes. Los paquetes EAPOL (2 y 3) o los paquetes (3 y 4) se consideran un handshake completo (Aircrack-ng, 2020a).

5.3.4.2. Diccionario (Cupp)

CUPP (Commom User Passwords Profiler, Perfil de contraseñas comunes de los usuarios) es una herramienta desarrollada para crear diccionarios que contienen las claves de acceso a la red Wi-Fi. Esta herramienta se basa en un recopilatorio de las contraseñas comunes que los usuarios generalmente utilizan en sus redes inalámbricas domésticas.

La eficiencia de CUPP depende en gran medida de la debilidad de la clave que el usuario haya establecido. Si la contraseña es una combinación de nombres y apellidos, es fácil descifrarla. Por el contrario, si la contraseña es una combinación de nombres, apellidos, apodos, fechas y caracteres especiales, será casi imposible que se pueda acertar con la clave.

Este aplicativo también tiene sus limitaciones, puesto que si se presentan claves de mayor complejidad (Claves Fuertes), el diccionario necesitará un mayor número de combinaciones para que se logre acertar, sin embargo, esto no garantiza su éxito.

No obstante, la ventaja principal de CUPP es que permite crear diferentes tipos de combinaciones, que se basan en información concerniente al usuario. Por tanto, se puede tener mayor posibilidad de que se acierte con la combinación correcta. Además, esta herramienta incorpora mecanismos que permiten aumentar el número de combinaciones y permutaciones de las claves previamente obtenidas, logrando obtener una mayor cantidad de claves que pueden ser la correcta.

5.3.4.3. Wifiphisher

En la página oficial de Kali Linux Tools, Wifiphisher es definido como: una herramienta de seguridad que monta ataques automatizados de phishing[17] contra redes WiFi con el fin de obtener frases secretas u otras credenciales (Tools, 2016).

Es un ataque de ingeniería social que, a diferencia de otros métodos, no incluye ningún tipo de fuerza bruta. Es una forma fácil de obtener credenciales de portales cautivos y páginas de acceso de terceros o frases de contraseña secretas WPA/WPA2 (Tools, 2016).

5.3.4.4. Xerosploit

Xerosploit es un kit de herramientas de pruebas de penetración cuyo objetivo es realizar ataques de hombre en el medio con fines de prueba. Trae varios módulos que permiten realizar ataques eficientes, y también permite realizar ataques de denegación de servicio y escaneo de puertos (GitHub, 2019).

5.3.5. Ataques

5.3.5.1. Fuerza Bruta y Diccionario

El ataque de fuerza bruta tiene como objetivo obtener la clave de la red Wi-Fi para acceder al tráfico generado internamente. El proceso de obtención de la clave es capturando el "Handshake" de los STA con el Router o AP, en el cual está contenida la clave. Por tanto, mediante un diccionario se puede internar descubrir la contraseña a través de la prueba y error.

[17] Phishing es un ataque que se basa en la ingeniería social, debido a que realiza un estudio de patrones de comportamiento de los usuarios en la red, para lograr captar su atención a través de ofertas de toda índole. Es decir, que los ataques de este tipo atraen a los usuarios a través de propuestas o engaños que se pueden realizar a través de Internet.

Este ataque se puede realizar mediante la suite de Aircrack, mientras que para el diccionario se puede emplear diccionarios como Cupp o Crunch, que se pueden crear en base a datos que se conocen del usuario o la red.

Para capturar el handshake se siguen los siguientes pasos:

1. Habilitar el modo monitor de la tarjeta de red.

   airmon-ng start "interfaz de la tarjeta de red"

2. Monitorear las redes disponibles o que están dentro de la cobertura.

   airodump-ng "interfaz de la tarjeta de red"

3. Seleccionar la red en específico a monitorear y capturar su tráfico.

   airodump-ng -c "Canal de la red" -bssid "Dirección MAC del router de la red" --write "Nombre del archivo .cap" "Interfaz de la tarjeta de red"

4. Realizar en otra ventana de terminal un ataque de des-autenticación para que se realice nuevamente el handshake y así capturarlo.

   aireplay-ng -0 "Número de mensajes a enviar" -a "Dirección MAC del router de la red" --ignore-negative-one "Interfaz de la tarjeta de red"

5. Emplear un diccionario (Creado o Preestablecido) para intentar "adivinar" la contraseña de la red.

   aircrack-ng "Dirección de la ubicación del archivo .cap" -w "Dirección de la ubicación del diccionario"

El proceso de conseguir la combinación correcta de caracteres, puede llegar a ser muy complejo, puesto que depende de la dificultad de la contraseña establecida.

En la mayoría de los hogares las contraseñas configuradas suelen ser sencillas, puesto que se pueden recordar con facilidad. En este escenario el ataque de fuerza bruta puede ser exitoso debido a que la clave no es muy compleja.

No obstante, si se configura una clave lo suficientemente compleja, sería casi imposible poder descifrar la combinación correcta. Esto se debe a que existen millones de posibles soluciones a una misma contraseña. Además, dependiendo de la cantidad de caracteres establecidos, la clave podría llegar a tener miles de millones de resultados probables.

Por tanto, el éxito de este tipo de ataque radica en la cantidad y calidad de las claves recopiladas en el diccionario. Si el diccionario cuenta con claves generadas en base a información personal de los usuarios, este tiene mayor probabilidad de acertar con la combinación correcta.

Para la creación del diccionario personalizado se pueden utilizar dos herramientas CUPP y Crunch.

❖ Diccionario CUPP

El diccionario CUPP permite crear diccionarios personalizados, los cuales son más eficientes, puesto que se generan en base a la información personal del usuario. Para crear este diccionario se debe utilizar los siguientes comandos:

- cd /cupp
- sudo ./cupp.py -i

Luego, se muestra un menú en el cual se deben introducir los datos del usuario y de sus familiares, por ejemplo: Su nombre, apellidos, Apodo, Fecha de Nacimiento, etc. Referirse a la Figura 24.

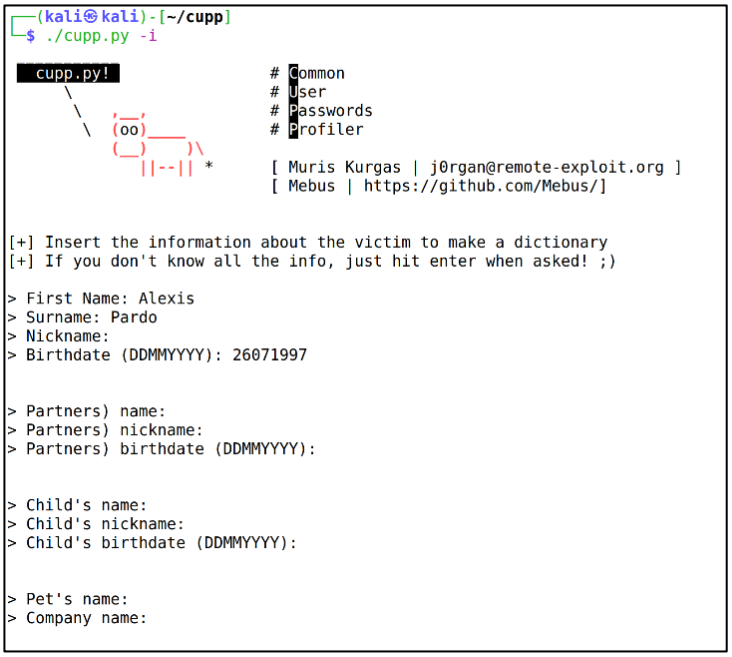


Figura 25: Diccionario CUPP.
Fuente: Autor.

Posteriormente, se añaden las funciones de agregar información adicional sobre el usuario. También, se tienen funciones que permiten añadir caracteres especiales, y reemplazar las letras por números.

Además, se puede mejorar un diccionario previamente creado, concatenando todos los caracteres de todas las claves generadas. Esto se logra mediante el siguiente comando:

- *sudo ./cupp.py -w "Nombre del archivo"*

❖ Diccionario Crunch

CRUCH es una alternativa al diccionario CUPP. Este diccionario incorpora ciertas funciones adicionales que permiten crear claves más precisas y en menor tiempo.

El comando para ejecutar el diccionario crunch, es el siguiente:

- *sudo crunch "Número mínimo de caracteres" "Número máximo de caracteres"*

  A este comando se le puede añadir funciones adicionales como:

- Añadir caracteres específicos que se van a utilizar en la creación de la clave:

  sudo crunch "Número mínimo de caracteres" "Número máximo de caracteres" "Caracteres a utilizar"

- Utilizar un "alfabeto" de caracteres predeterminado para crear claves:

  sudo crunch "Número mínimo de caracteres" "Número máximo de caracteres" /usr/share/rainbowcrack/charset.txt

- Crear un diccionario con base a una clave incompleta, en la cual se tiene:

  sudo crunch "Número mínimo de caracteres" "Número máximo de caracteres" -t "Parte de la clave o Patrón de la clave" (@; %; ^ ; ,)

  Donde:
  @: Completa con letras minúsculas.
  ,: Completa con letras mayúsculas
  %: Completa con números.
  ^: Completa con caracteres especiales como @,#,=,etc.

- Generar claves mediante la permutación de caracteres específicos:

  sudo crunch "Número mínimo de caracteres" "Número máximo de caracteres" -p "Caracteres específicos"

5.3.5.2. Denegación de servicios (DoS)

La denegación de servicios en las redes Wi-Fi busca impedir que los usuarios puedan tener acceso a la red o salida hacia Internet. Para esto, el atacante aprovecha una característica propia de estas redes, como es la des-autenticación. Debido a que la des-autenticación es una notificación de finalización de la comunicación, no puede negarse, por tanto, el Router Inalámbrico no puede realizar ningún control sobre esta acción.

Con base a este conocimiento, el atacante puede inundar de mensajes de des-autenticación al Router Inalámbrico, para que todos los dispositivos asociados a él, se desconecten. Para este ataque se deben seguir los siguientes pasos:

1. Activar el modo monitor de la tarjeta de red

   airmon-ng start "Interfaz de la tarjeta de red"

2. Detectar las redes disponibles

   airodump-ng "Interfaz de la tarjeta de red"

3. Monitorear una red en específico para obtener su tráfico

   airodump-ng -c "Canal de la red victima" --bssid "Dirección MAC del AP o Router" -w "Nombre del archivo de salida" "Interfaz de la tarjeta de red"

4. Lanzar el ataque DoS a la red victima

   aireplay-ng -0 "Número de mensaje de desautenticación a lanzar" -a "Dirección MAC del AP o Router" "Interfaz de la tarjeta de red"

5. Lanzar el ataque DoS a un dispositivo en específico

   aireplay-ng -0 "Número de mensaje de desautenticación a lanzar" -a "Dirección MAC del AP o Router" -c "Dirección MAC del dispositivo""Interfaz de la tarjeta de red"

   Este ataque puede resultar letal, si se realiza desde más computadoras. Si el atacante logra infectar más computadoras, puede dirigir este ataque a una red en específico, causando el colapso de la misma.

5.3.5.3. Gemelo Malvado (Evil Twin)

Este ataque busca obtener información del usuario mediante la falsificación o imitación de un entorno gráfico en el que se debe ingresar información personal. Su objetivo es suplantar un portal interactivo en el cual se ingresan datos sobre contraseñas o cuentas del individuo, para registrarlas en un archivo que puede ser utilizado por el atacante para adueñarse de tales cuentas.

Puesto que este ataque se fundamenta en el uso de portales web o entornos gráficos, se requiere del uso de un servidor que genere un sitio similar al que se presentaría el original. Por tanto, se necesita de un aplicativo que cumpla esta característica.

Para el ataque del gemelo malvado se tienen aplicativos como Fluxion o Wifiphisher, que generan páginas web de forma automática. En este caso se empleó la herramienta Wifiphisher que permite más opciones de portales que pueden utilizarse.

La elección de la red y de los tipos de portales que se van a utilizar se lo hace mediante la selección gráfica del ataque en específico. Para iniciar el ataque, se debe ingresar en el terminal en modo root el siguiente comando:

- *sudo wifiphisher*

Posteriormente se debe elegir la red que se desea atacar; para esto se empleará las flechas para moverse por el menú, y con la tecla “Enter” se seleccionará la red. Referirse a la Figura 26.

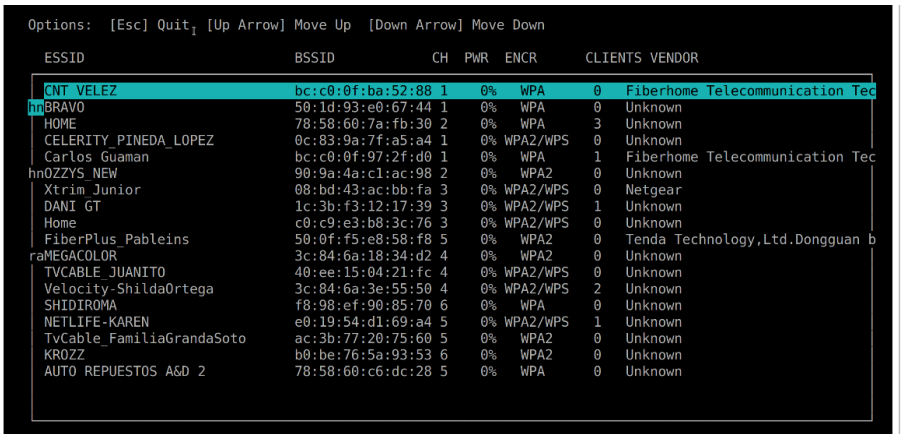


Figura 26: Herramienta Wifiphisher.
Fuente: Autor.

Luego se elegirá el tipo de ataque que se planea usar para obtener la información del usuario. En este caso se empleó el ataque de actualización del firmware que mostrará una ventana de actualización en el dispositivo de la víctima.

Finalmente, el usuario ingresará los datos solicitados y el atacante podrá tener acceso a ellos mediante la ventana del terminal, que es donde se muestran.

5.3.5.4. Man-in-the-Middle

El acceso al tráfico que generan los usuarios, dota al atacante de la capacidad de conseguir patrones de comportamiento sobre las acciones que se realizan en la red.

El análisis acerca de los sitios que los usuarios visitan frecuentemente, permite al atacante establecer patrones de búsqueda. Estos comportamientos pueden ser rutinas que el atacante puede usar como punto de partida para lanzar ataques en ciertos horarios en los cuales los usuarios tienen preferencias por ciertos sitios.

El propósito de este ataque es obtener información personal del usuario mediante la suplantación o modificación de una página web, que generalmente es una de las más buscadas por los usuarios.

Para este ataque se emplea el programa Xerosploit, que se ejecuta mediante el siguiente comando:

- *sudo python3 xerosploit.py*

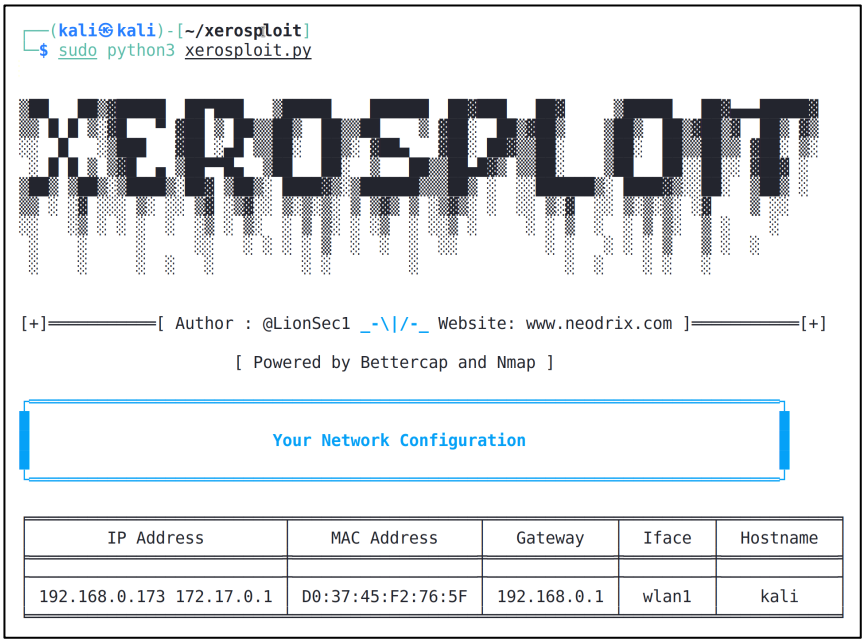


Figura 27: Aplicativo Xerosploit para realizar ataques MITM.
Fuente: Autor.

Para empezar con este ataque tipo MITM, se requiere escoger la tarjeta de red que se utilizará para receptar el tráfico. Para esto se utiliza el comando:

- *help*

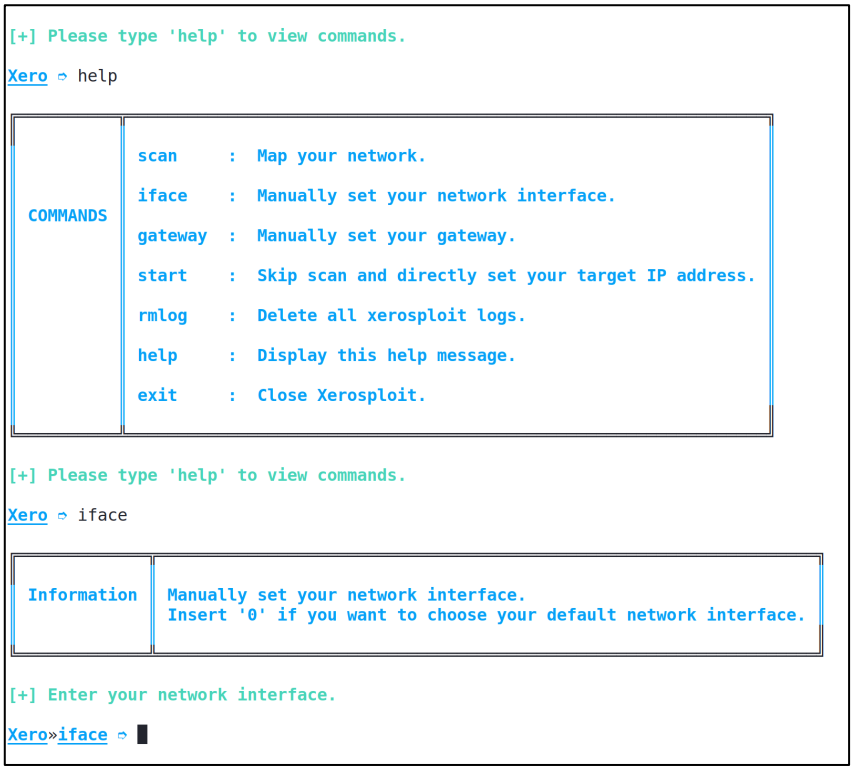


Figura 28: Menú de configuración de Xerosploit.
Fuente: Autor.

Este comando despliega un sub-menú que permite configurar algunos parámetros antes de comenzar el ataque. Mediante el comando *"iface"* se puede modificar la tarjeta de red a utilizar, simplemente se debe escribir el nombre de la tarjeta, por ejemplo: wlan1.

Como primer paso para lanzar un ataque MITM, se debe escanear los equipos conectados a esa red, por medio del comando *"scan"*. Cuando el escaneo finalice, se puede escoger un equipo en especifico para atacar, introduciendo la dirección IP del mismo. También se puede atacar a todos, para esto se debe escribir el comando *"all"*.

```
Xero ➪ scan

[++] Mapping your network ...

[+]═══════════[ Devices found on your network ]═══════════[+]

| IP Address    | Mac Address       | Manufacturer              |
|---------------|-------------------|---------------------------|
| 192.168.0.1   | 00:5F:67:A4:0B:38 | (Unknown)                 |
| 192.168.0.193 | A4:C3:F0:5A:E9:34 | (Intel Corporate)         |
| 192.168.0.205 | CA:DF:97:2A:AB:2B | (Unknown)                 |
| 192.168.0.248 | 1C:CC:D6:46:9D:48 | (Xiaomi Communications)   |
| 192.168.0.173 | D0:37:45:F2:76:5F | (This device)             |

[+] Please choose a target (e.g. 192.168.1.10). Enter 'help' for more information.

Xero ➪ 192.168.0.193

[++] 192.168.0.193 has been targeted.
```

Figura 29: Direcciones IP y MAC de los equipos conectados a la red.
Fuente: Autor.

Xerosploit cuenta con diversos tipos de ataques, estos se pueden observar mediante el comando *"help"*. Para el ataque del tipo MITM se empleará el ataque de Sniff que permite capturar la información de los paquetes HTTP/HTTPS de los usuarios. Para seleccionar el ataque solo se debe tipearlo.

```
Xero»modules ➪ help

| MODULES | pscan       :  Port Scanner                                  |
|         | dos         :  DoS Attack                                    |
|         | ping        :  Ping Request                                  |
|         | injecthtml  :  Inject Html code                              |
|         | injectjs    :  Inject Javascript code                        |
|         | rdownload   :  Replace files being downloaded                |
|         | sniff       :  Capturing information inside network packets  |
|         | dspoof      :  Redirect all the http traffic to the specified one IP |
|         | yplay       :  Play background sound in target browser       |
|         | replace     :  Replace all web pages images with your own one |
|         | driftnet    :  View all images requested by your targets     |
|         | move        :  Shaking Web Browser content                   |
|         | deface      :  Overwrite all web pages with your HTML code   |

[+] Which module do you want to load ? Enter 'help' for more information.

Xero»modules ➪
```

Figura 30: Menú de ataques que puede realizar Xerosploit.
Fuente: Autor.

5.3.5.5. Captura de Credenciales con un Sniffer (Des-encriptación de TLS)

La captura de credenciales no se considera como un ataque, puesto que su propósito no es vulnerar la seguridad de una red. Sin embargo, su principio de funcionamiento supone una amenaza contra cualquier sistema de seguridad, puesto que mediante una vulnerabilidad propia de Wi-Fi se puede conseguir las claves del usuario en base al análisis del tráfico generado.

Este tipo de amenaza se puede definir como un ataque complementario, debido a que requiere que el hacker este conectado a la red Wi-Fi, como si fuera otro usuario. Por tanto, primero se necesita vulnerar la seguridad de la red mediante otros ataques, como Ataques de Diccionario o de Evil Twin (Gemelo Malvado), para luego filtrar el tráfico HTTP.

Para la captura de credenciales primero se necesita crear un archivo donde este guardado todo el tráfico generado por los usuarios de la red. Para crear este archivo se emplea el siguiente comando:

- export SSLKEYLOGFILE = "Dirección donde se desea guardar el archivo": Export SSLKEYLOGFILE="/home/kali/sslkeylogfile.log"

Posteriormente, para obtener el tráfico HTTP de los usuarios, se utiliza un sniffer como puede ser Wireshark. Por medio de esta herramienta, el hacker analiza el tipo de tráfico que se está produciendo, para poder determinar los sitios que se visitan y poder obtener las credenciales.

Luego, en el archivo generado anteriormente estará almacenado el tráfico generado, el cual contiene las claves de sesión TLS, que se emplean para des-encriptar la información contenida en las búsquedas del usuario.

Finalmente, este archivo se debe cargar en el sniffer, mediante la siguiente configuración:

- Preferencias -> Protocolos -> TLS -> (Pre)-Master-Secret log filname -> Browse -> “Elegir Ruta del Archivo”.

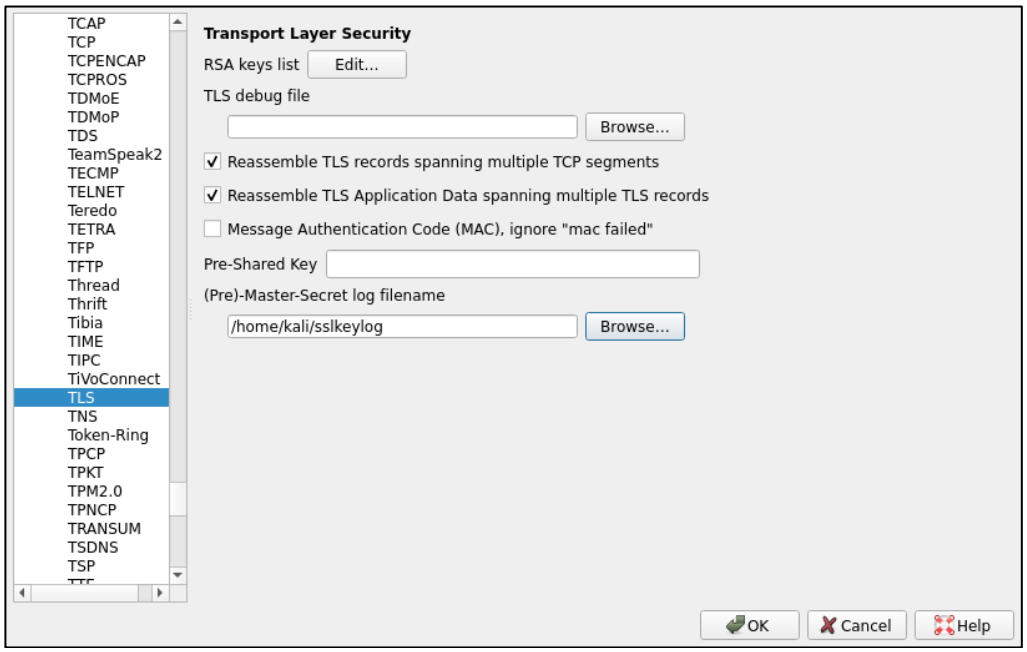


Figura 31: Menú del protocolo TLS de Wireshark.
Fuente: Autor.

Se debe hacer mención que la factibilidad de este ataque radica en que se deben capturar las claves de sesión TLS, por tanto, el ataque debe comenzar antes de que el usuario comience a generar tráfico mediante el navegador.

6. RESULTADOS

6.1. Resultado del ataque de Fuerza Bruta y Diccionario

Este ataque se lo realizó considerando dos tipos de claves de acceso, de forma que se pueda evaluar la seguridad del router en base a las claves generadas. El propósito de utilizar dos tipos de clave, es para determinar como influye el tipo de clave utilizada en la seguridad de la red.

Los parámetros a considerar para la elección de las claves a utilizar fueron:

- Cantidad de caracteres (Igual o mayor a los 8 caracteres mínimos requeridos)
- Uso de letras mayúsculas y minúsculas
- Uso de números
- Inclusión de caracteres especiales
- Creación de clave con base en la información personal del usuario.

6.1.1. Ataque de Diccionario y Fuerza Bruta para una clave sencilla

Para el primer ataque se configuró una clave sencilla, fácil de recordar y con información personal del usuario. La clave se compone de letras minúsculas y números que comprenden el número mínimo de caracteres requeridos para la contraseña.

La contraseña creada se configuró para el sistema de seguridad WPA2-PSK, con encriptación AES. Además, se configuro el router con la mayoría de tecnologías Wi-Fi (Wi-Fi 4, 5 y 6) para que sean compatibles con la mayoría de dispositivos. Referirse a la Figura 32.

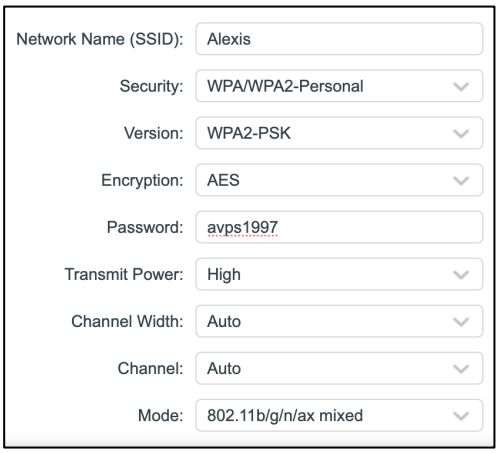


Figura 32: Configuración del Router con una contraseña sencilla.
Fuente: Autor.

En este primer ataque se obtuvo como resultado, la vulneración casi inmediata de la red, debido a que la contraseña configurada es sencilla. Por tanto, solo se necesitó un diccionario con la clave mínima requerida (8 caracteres) para obtener la contraseña y penetrar la red. No obstante, a pesar de la simplicidad de la clave, se generaron más de 25 mil posibles combinaciones, para conseguir la correcta. Revisar el Anexo 2.

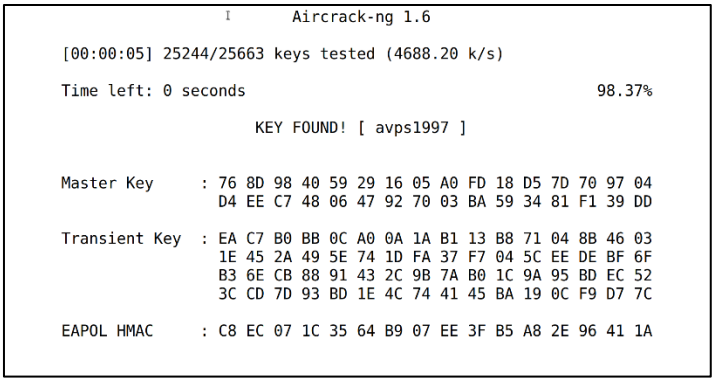


Figura 33: Obtención de la contraseña de la red mediante el aplicativo Aircrack-ng.
Fuente: Autor.

El resultado obtenido muestra que la capacidad de penetrar una red domestica se centra en el conocimiento del atacante para crear un diccionario, con base a la información personal del usuario.

La capacidad del atacante de limitar el rango de caracteres e información para la creación de la clave, repercute en la fiabilidad que tiene el diccionario para generar la

combinación correcta. Entre mayor sea el número de caracteres a evaluar, mayor será el número de combinaciones que se deben crear para lograr encontrar la correcta.

6.1.2. Ataque de Diccionario y Fuerza Bruta para una clave compleja

Para el segundo ataque, se estableció una clave compleja que no contiene información del usuario, está compuesta de caracteres especiales, y sobrepasa el mínimo de caracteres requeridos. Además, esta contraseña combina caracteres especiales y alfanuméricos, por lo que, es una clave con una complejidad elevada.

Al igual que en el primer ataque, se configuró el router para que sea compatible con la mayoría de las versiones de Wi-Fi. De igual forma, se estableció que el método de encriptación sea AES. Referirse a la Figura 34.

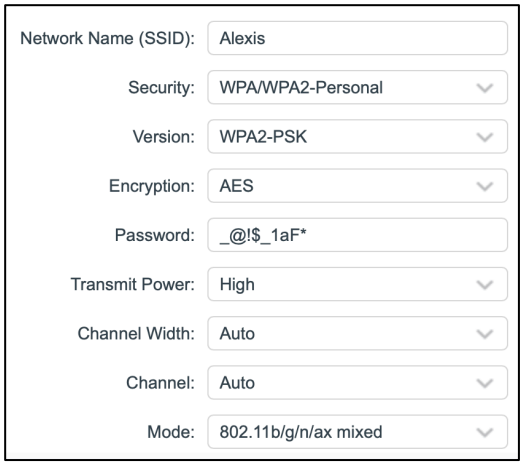


Figura 34: Configuración del Router con una contraseña compleja.
Fuente: Autor.

El resultado del segundo ataque fue un fracaso, debido a que el diccionario no logró generar la combinación correcta. El diccionario recopilo más de 19 millones de posibles combinaciones, sin embargo, ninguna coincidió con la contraseña configurada. Referirse a la Figura 35 y revisar el Anexo 2.

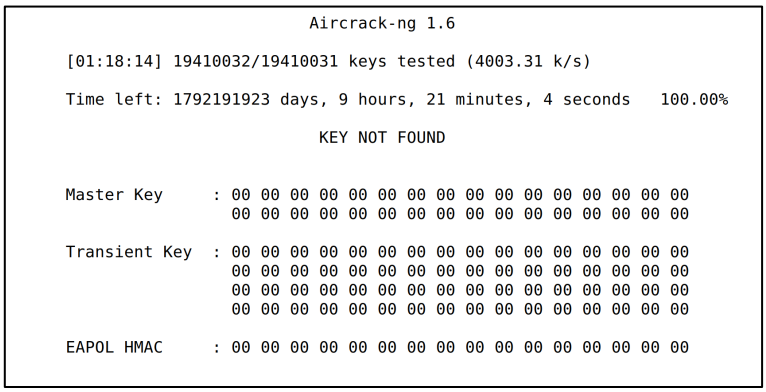


Figura 35: Intento fallido de obtención de la contraseña de la red mediante el aplicativo Aircrack-ng. Fuente: Autor.

En este nuevo resultado se puede determinar que la complejidad de la contraseña influye en la seguridad de la red. A pesar de la cantidad de contraseñas que se generaron para la creación del diccionario, ninguna fue la correcta.

Al contrario del caso anterior, la creación del diccionario no tenía un punto de partida como el conocimiento de la información del usuario, por tanto, el proceso de generar un diccionario era más complejo y tardado.

También se debe considerar que, al no haber relación entre la contraseña y los datos del usuario, daba como resultado la necesidad de crear un diccionario con todas las posibles combinaciones. Por tanto, la cantidad de posibles combinaciones que resultan para generar este diccionario pueden ser infinitas.

Se debe hacer mención que el generar una gran cantidad de claves puede agotar el almacenamiento del equipo, por lo que, se necesita de una memoria de gran capacidad, si se desea almacenar todas las claves. Esto también se puede interpretar como un límite físico para la creación de un diccionario. No obstante, la cantidad de claves a generar depende de la herramienta a utilizar.

6.2. Resultado del ataque Evil Twin (Gemelo Malvado)

Para este ataque se partió de la configuración de la contraseña compleja, con el fin de obtenerla empleando otro método. Debido al resultado del ataque anterior, se requirió buscar otras herramientas que permitan penetrar la red.

En este ataque se empleó el programa Wifiphisher, que incorpora la herramienta Evil Twin mediante un portal web, para poder conseguir la información del usuario.

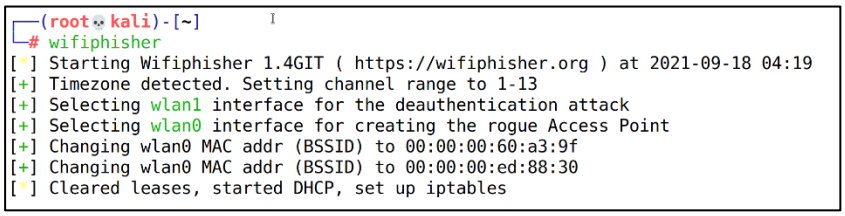


Figura 36: Comando Wifiphisher.
Fuente: Autor.

El resultado de este ataque fue exitoso, puesto que se pudo obtener la contraseña de la red, por medio de un AP falso y el portal interactivo creados por el mismo programa. Referirse a la Figura 36.

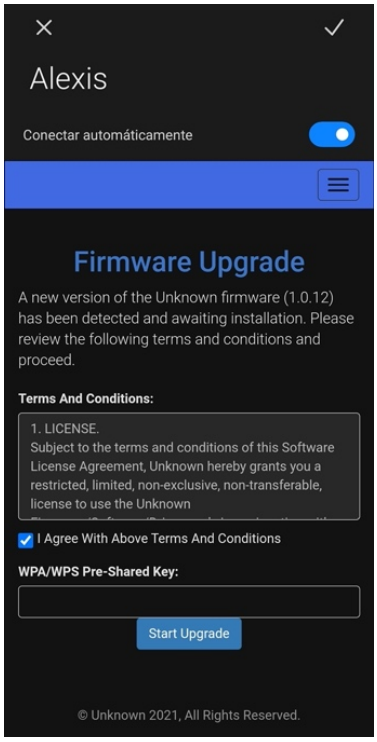


Figura 37: Portal Interactivo que se muestra en el dispositivo del usuario.
Fuente: Autor.

Por medio de este ataque se pudo engañar al usuario para que ingresará la clave de red y así obtenerla en un primer intento. De esta manera, se puedo conseguir la contraseña, sin requerir de aplicativos extra como un diccionario. Referirse a la Figura 38.

```
┌──(root💀kali)-[~]
└─# sudo wifiphisher
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2021-09-18 05:13
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wlan1 interface for the deauthentication attack
[+] Selecting wlan0 interface for creating the rogue Access Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:6c:77:3e
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:f7:45:aa
[+] Sending SIGKILL to wpa_supplicant
[*] Cleared leases, started DHCP, set up iptables
[+] Selecting Firmware Upgrade Page template
[*] Starting the fake access point...
[*] Starting HTTP/HTTPS server at ports 8080, 443
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher
[+] Captured credentials:
wfphshr-wpa-password=_@!$_1aF*
```

Figura 38*:* Obtención de la clave de red mediante la herramienta Wifiphisher.
Fuente: Autor.

Se debe mencionar que el éxito de este ataque radica en la capacidad de la aplicación o del hacker para desarrollar un portal interactivo, lo suficientemente creíble para que la víctima no se percate del ataque. En este caso, se empleó el portal por defecto del programa, para efectuar el ataque.

La capacidad de adaptabilidad del portal con las configuraciones del dispositivo, aporta un extra para su credibilidad. En referencia a la Figura 37, se puede observar que el portal se adapta al modo oscuro del dispositivo, por lo que, puede pasar desapercibido por el usuario.

Po contra, el idioma en el que se presenta el texto, no concuerda con el configurado en el dispositivo, por lo que, puede interpretarse con algún tipo de ataque que se esta efectuando en la red.

6.3. Resultado del ataque de Denegación de Servicios (DoS)

Para la denegación de servicio se empleó la herramienta Aireplay-ng que permite enviar mensajes de des-autenticación a todos los dispositivos o a un dispositivo en específico de una red.

Mediante los mensajes de des-autenticación, se logró que los dispositivos que estaban conectados a la red no pudieran asociarse durante un período de tiempo considerable. Además, se impedía que los dispositivos tengan acceso al servicio de Internet.

Para detectar la red victima se empleó la herramienta Airodump-ng. Esta herramienta permitió identificar si había dispositivos asociados a los cuales se les podría lanzar el ataque. Referirse a la Figura 39.

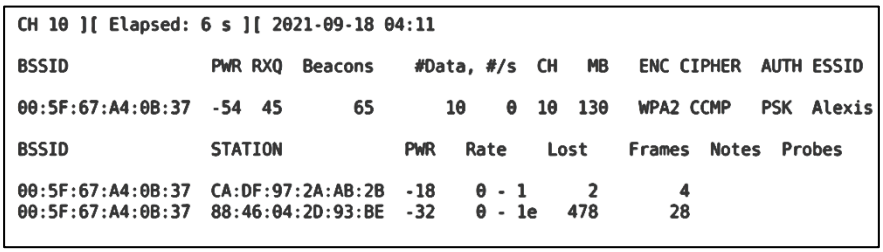


Figura 39: Monitoreo de la red victima y de los dispositivos conectados mediante la herramienta Aireplay-ng.
Fuente: Autor.

Para este ataque se consideró realizarlo desde un enfoque individual y grupal, para evidenciar como este tipo de ataques puede afectar a los usuarios conectados a una misma red. En el enfoque individual se busca lanzar el ataque a un único usuario aún cuando estén conectados muchos otros. Mientras que, para el enfoque grupal se busca efectuar el ataque para todos los dispositivos asociados a esa red.

6.3.1. Resultado del ataque DoS a todos los dispositivos de la red

En este primer ataque se enviaron 20 mensajes de des-autenticación a todos los dispositivos de la red, de manera que finalice su asociación con el Router, y no pudieran volver a conectarse. Referirse a la Figura 40.

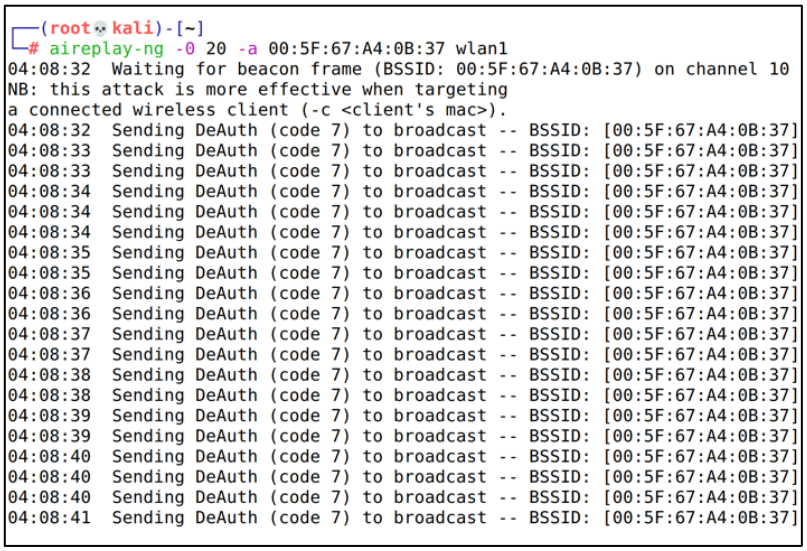


Figura 40: Mensajes de des-autenticación mediante la herramienta Aireplay-ng.
Fuente: Autor.

El resultado de este ataque fue exitoso, puesto que todos los dispositivos asociados finalizaron su conexión con el router de manera inmediata. Además, no lograron conectarse nuevamente a la red, durante un período considerable.

Esta apertura en la seguridad dentro de la estructura de Wi-Fi, permitió que el autor pudiera desvincular a los dispositivos, mientras se seguían enviando mensajes de des-autenticación para lograr colapsar el router.
De esta manera, el hacker pudo denegar el servicio de conexión a Internet para los usuarios de la red, mientras podía efectuar un ataque que busque agotar la capacidad de procesamiento del router por medio de una inundación de paquetes, que finalizaría con la sobrecarga del equipo.

Cabe recalcar, que este ataque se realizo desde un único dispositivo como método para efectividad del ataque, sin embargo, se pudo haber potenciado la letalidad del mismo, por medio de una inundación de paquetes desde otras computadoras.

6.3.2. Resultado del ataque DoS a un único usuario de la red.

La siguiente prueba se la realizó lanzado 20 mensajes de des-autenticación a un dispositivo en específico para impedir que este se pudiera conectar a la red. El resultado de este ataque también fue exitoso, puesto que se pudo desconectar a un único dispositivo, mientras los demás mantenían el servicio. Referirse a la Figura 41.

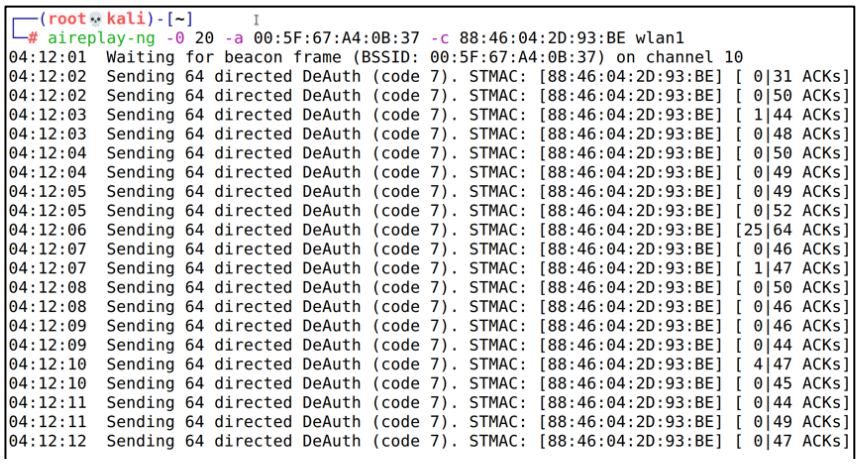


Figura 41: Mensajes de des-autenticación mediante la herramienta Aireplay-ng.
Fuente: Autor.

Esta vulnerabilidad presente en la tecnología Wi-Fi puede se aprovechada por el autor para suplantar a ese usuario en la conexión de la red, para filtrar todo el tráfico de los demás usuarios.

También se puede emplear este ataque para redirigir al usuario a una red falsa en la cual se busca que el usuario genere tráfico concerniente a su trabajo, con el fin de obtener información confidencial de la empresa donde este laborando.

6.4. Resultado del Ataque Man-in-the-Middle

El ataque de MITM se lo realizó con el programa Xerosploit, que permitió el "sniffing o analisis de paquetes" que se envían entre los dispositivos terminales y el router. Para este ataque se empleo el filtrado de paquetes HTTP para conocer los sitios web que visitan los usuarios de esa red.

En la Figura 42 se pueden observar los datos que permitieron al autor realizar un análisis sobre el comportamiento de búsqueda de los usuarios. Se pueden destacar las direcciones IP de los equipos que solicita el sitio web, y el servidor web, además de las URL de las páginas que se han visitado.

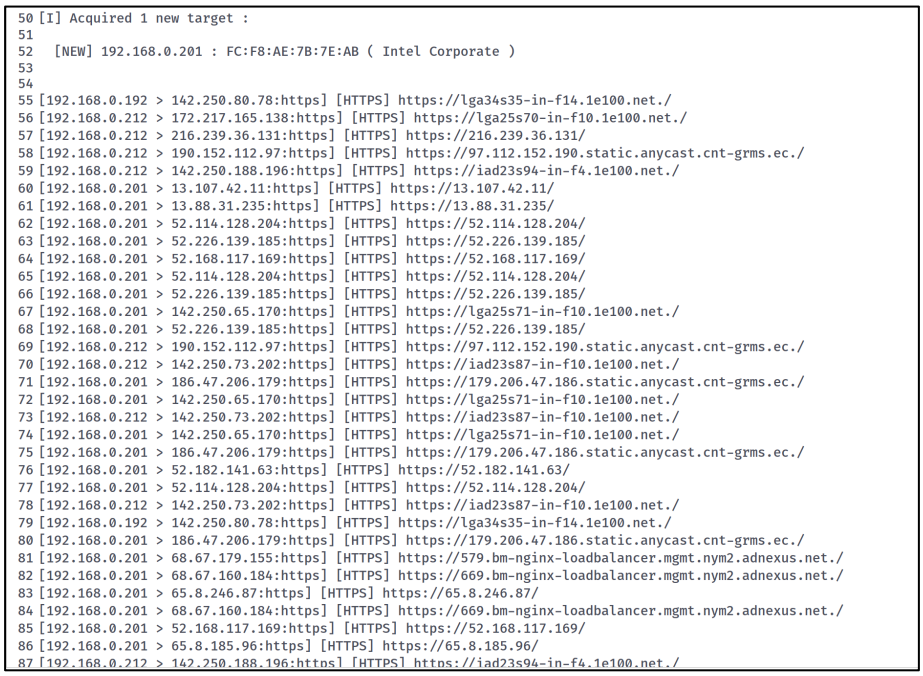


Figura 42: Filtrado de tráfico HTTPS mediante la herramienta Xerosploit.
Fuente: Autor.

El resultado de este ataque fue exitoso puesto que se tuvo acceso al tráfico HTTPS originado en la red, sin que los usuarios hubieran estado conscientes de la presencia de un atacante en la red, por lo que, el análisis de tráfico realizado por el autor no puede ser detectado.

El resultado obtenido de este ataque puede ser muy útil para realizar minería de datos, para obtener patrones de búsqueda de los usuarios. Por medio de este análisis de búsqueda, el atacante puede automatizar programas que se ejecuten cuando se visite un sitio en especifico, de forma que el programa busque recopilar las credenciales de acceso cada vez que se acceda a esa pagina web.

También se debe mencionar que este tipo de ataques es ampliamente usado para infectar con un virus a todos los equipos de una red, de forma que puedan controlarse a distancia. El propósito de este accionar, es la capacidad de realizar ataques del tipo DDoS a una red en especifico para colapsarla. El ataque de este tipo más conocido es “Mirai”, el cual se caracteriza por infectar dispositivos IoT como cámaras IP o equipos de red, para realizar ataques de denegación de servicios (Antonakakis et al., 2017).

6.5. Resultado de la Captura de Credenciales con un Sniffer

Para este ataque se partió de la premisa de que el hacker estaba conectado a la red, y por tanto tenía acceso al tráfico de todos los usuarios. También, se consideró que el ataque se llevó a cabo antes de que se empezará a generar tráfico, esto con el fin de poder capturar las claves de sesión SSL o TLS.

En este tipo de ataque, se empleó el sniffer Wireshark para la captura, filtrado y desencriptación del tráfico HTTP. Para este caso, se filtro credenciales educativas, las cuales se emplean para ingresar al Entorno Virtual de Aprendizaje de una Universidad. Referirse a la Figura 43.

Figura 43: Análisis del tráfico HTTP mediante la herramienta Wireshark.
Fuente: Autor.

El resultado del ataque fue exitoso, puesto que se pudo obtener las credenciales del usuario para ingresar al portal educativo. En la Figura 38 se observa el contenido del paquete HTTP analizado. Revisar Anexo 3.

Figura 44: Resultado del análisis del paquete HTTP que contiene las credenciales del usuario. Fuente: Autor.

Este tipo de ataque también puede realizarse para sitios de entidades financieras, gubernamentales, militares, o para cualquier tipo de portal que requiera credenciales de acceso.

La letalidad de esta amenaza radica principalmente en la capacidad que tiene el atacante de ingresar a la red. Por medio de la vulnerabilidad de Wi-Fi que permite que cualquier usuario en la red pueda observar el tráfico de los demás, un agente externo al grupo, en principio, puede capturar todo el tráfico generado, para luego analizarlo y obtener la información de su interés.

6.6. Resultado General de los ataques

6.6.1. Resultados entre WPA-2 TKIP y WPA-2 AES

Los resultados obtenidos para ambos métodos de cifrado con respecto a los diferentes ataques realizados fueron exactamente los mismos. A pesar de que AES es un método de encriptación mucho más robusto que TKIP, se pudo vulnerar de forma sencilla.

El motivo de este resultado similar es debido a las herramientas de auditoria actuales. Los constantes desarrollos de mejores aplicativos que permitan una adecuada evaluación de los sistemas de seguridad actuales, han permitido que se puedan crear programas que puedan encontrar fallas en su estructura, a pesar de que los sistemas sean lo más robustos posibles.

Otro factor importante a considerar son los grupos dedicados al hacking, sea ético o no. Al igual que existen organizaciones que buscan el mejoramiento de los sistemas mediante la detección de puntos de falla, también existen personas que tiene otros propósitos que buscan encontrar aperturas en estos sistemas con el fin de obtener información valiosa para los usuarios o empresas.

Cabe recalcar que en términos de des-encriptación AES presenta una mayor complejidad para descubrir el mensaje que TKIP, puesto que, AES emplea un algoritmo de cifrado más robusto que TKIP. Además, AES fue desarrollado para WPA-2, por tanto, su función fue sustituir a TKIP de WEP (Revisar la Sección 1.4.5).

Actualmente, aún esta disponible el cifrado TKIP para dar soporte a dispositivos antiguos (Anteriores al 2006). Referirse a la Figura 45. Sin embargo, no se debe considerar el cifrado TKIP como un mecanismo de seguridad actual, puesto que es muy vulnerable frente a muchos ataques. A día de hoy, TKIP se considera como un mecanismo de cifrado obsoleto.

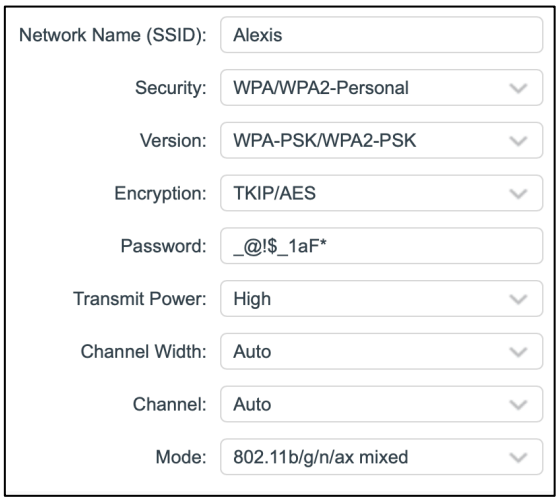


Figura 45: Tipos de cifrados disponibles en el Router.
Fuente: Autor.

6.6.2. Resultados entre WPA-2 Personal y WPA-2 Enterprise

Los resultados obtenidos para WPA-2 Personal difieren totalmente frente WPA-2 Enterprise o Empresarial. El sistema WPA-2 Personal, en principio, presenta algunos puntos de fallas que hacen que este sistema sea vulnerable frente a ataques. Mientras que WPA-2 Enterprise, al ser un sistema basado en la Autenticación Autorización y Registro por medio de un servidor dedicado, presenta mayor robustez frente a los mismos ataques.

La seguridad que ofrece WPA-2 Enterprise es superior a WPA-2 Personal, debido a que esta enfocado a proveer de protección a empresas. Este sistema de seguridad requiere de un servidor RADIUS, que permita llevar un control sobre los usuarios que desean conectarse a la red. De esta manera, se puede prevenir ataques provenientes de usuarios externos que buscan su colapso.

Se debe hacer mención a que el servidor RADIUS al ser un equipo dedicado para brindar seguridad a la red, tiene un coste elevado por el servicio que brinda. Sin embargo, existen alternativas en el mercado de manera gratuita como FreeRadius, en la que solo se requiere de un equipo que funcione como servidor.

No obstante, la configuración de este tipo de servidor en el router, no es posible, puesto que, no se permiten direcciones IP del tipo “Loopback”, que es la utilizada por defecto por el programa.

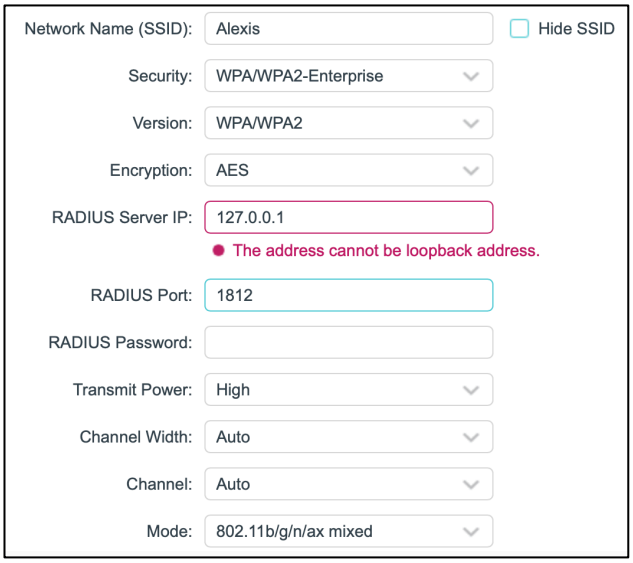


Figura 46: Proceso fallido de configuración del servidor FreeRADIUS en el Router.
Fuente: Autor.

La seguridad de WPA-2 Enterprise es mejorada con el uso de protocolos como EAP, la encriptación MIC y los mecanismos de IEEE 802.1X. Por tanto, al contario de WPA-2 Personal, los mensajes que se envían entre el equipo y el autenticador, están protegidos.

También se debe mencionar, que actualmente existen herramientas que están enfocadas en vulnerar el sistema WPA-2 Enterprise, por medio de la captura de los mensajes *“Hashes”* que contienen las credenciales de acceso. Algunas de las herramientas utilizadas para este tipo de ataques son: Easy-Creds, John the Ripper o Hashcat. El análisis del funcionamiento de estos programas se sale del alcance de la investigación de este proyecto.

Con base a la comparación teórica, se puede inferir que el sistema WPA-2 Enterprise es mucho más robusto que WPA-2 Personal y que debería ser sustituido por el primero.

Sin embargo, la seguridad que proporciona el sistema empresarial no se requiere en un ambiente domestico, puesto que la información que se produce en el hogar no necesita de una mejor protección.

7. DISCUSIÓN

El presente trabajo tuvo la finalidad de poner a prueba la seguridad del sistema WPA-2 Personal con el fin de corroborar la hipótesis planteada para este trabajo de investigación. Por tanto, con fundamentación en los resultados, se pudo contrastar que la tecnología Wi-Fi con su sistema de seguridad WPA-2 Personal, aún tiene graves problemas de seguridad frente a distintos tipos de ataques.

Los resultados experimentales arrojaron que los equipos provistos con el sistema de seguridad WPA-2 Personal pueden ser vulnerados mediante ataques iterativos como los de Prueba y Error, Diccionario, Fuerza Bruta e Inundación de Mensajes. Además, también se comprueba que las fallas dentro de la estructura de Wi-Fi favorecen a los atacantes para descifrar el tráfico generado para la obtención de credenciales.

De igual forma, el acceso al tráfico generado por todos los usuarios, puede ser empleado por los hackers para introducir malware dentro de la red, para que todos los equipos conectados, se infecten. De esta manera, se podría crear una red masiva de equipos controlados desde diferentes partes del mundo, que puede ser utilizada para ataques de Denegación de Servicios Distribuida a una red remota.

A través de los ataques también se demostró la facilidad con la que cualquier persona puede efectuar los mismos en la red. La disponibilidad del software y hardware permitieron realizar esta investigación, sin embargo, tales herramientas también pueden ser empleadas para otros fines, como la evaluación de seguridad de una red.

Finalmente, las redes Wi-Fi a pesar de tener las vulnerabilidades analizadas en el capitulo anterior, generalmente no requiere de seguridad extra debido a que tales ataques suelen ser poco comunes. No obstante, la popularidad de Wi-Fi ha tomado fuerza en estos últimos años debido al desarrollo de nuevas versiones que pueden resultar útiles en diversos mercados, por lo que, si se logra ampliar su campo de aplicabilidad sin solventar tales fallos de seguridad, podría ser peligrosa su implementación.

8. CONCLUSIONES

Mediante los resultados teóricos y experimentales se pudo demostrar que el sistema WPA-2 Personal y Wi-Fi en general, aún presenta graves problemas de seguridad, los cuales pueden aprovecharse por usuarios con intenciones maliciosas para sus fines poco éticos. Por tanto, se puede concluir que:

- WPA-2 Personal en sus versiones TKIP y AES presenta aperturas en su seguridad debido a la capacidad que se tiene de capturar los mensajes para descifrarlos. En comparación con EAP y RADIUS de 802.1X, estos presentan mayor robustez debido al control de acceso que se realiza sobre los mensajes de asociación a través de los puertos controlados y no controlados.
- La seguridad provista por 802.1X es superior a 802.11x, porque incorpora métodos de gestión más rigurosos sobre el acceso de dispositivos solicitantes. A pesar que 802.11 en su versión Enterprise también implemente el mecanismo de asociación mediante los puertos controlados y no controlados, su estructura inalámbrica aún lo hace vulnerable a ataques de suplantación como Evil Twin.
- Wi-Fi presenta un punto de falla dentro de su estructura que permite que todos los usuarios conectados a la red, puedan observar el tráfico generado por los demás usuarios mediante un Sniffer. Por tanto, se concluye que el flujo compartido de los datos, presente en Wi-Fi, es una apertura en la seguridad, puesto que le permite al atacante obtener los datos de los usuarios con solo conectarse a la red.
- La estructura de Wi-Fi posibilita la desvinculación de uno o todos los usuarios de una red mediante una inundación de mensajes de des-autenticación que pueden ser enviados por un usuario externo a la red. Por tal motivo, es una amenaza presente en Wi-Fi debido a la capacidad que tiene el atacante para des-asociar a un dispositivo y suplantar su identidad.
- Aumentar la complejidad de la contraseña empleada para la asociación de las STAs con el AP, impide que los atacantes puedan penetrar la red a través de ataques del tipo Fuerza Bruta y Diccionario. Sin embargo, también se pueden

emplear métodos como Evil Twin o ataques de Ingeniería Social como el Phishing para lograr vulnerar la red.

- El ataque de Fuerza Bruta puede ser aprovechado por los crackers para conectarse a cualquier red e infectar a los equipos protegidos por el sistema WPA-2 Personal, mediante la implementación de un virus. De esta manera, logra convertirlos en equipos "zombies", que pueden ser controlados a la distancia para realizar ataques DDoS.
- WPA-3 mejora completamente la seguridad de las redes Wi-Fi, debido a la incorporación del mecanismo de asociación SAE y a la eliminación de métodos de autenticación de WPA-2 como PSK y AAAK. No obstante, WPA-3 aún permite la retro-compatibilidad con los estándares anteriores, por lo que, puede se aprovechado para realizar ataques del tipo "Downgrade" como Dragonblood.
- En WPA-3 los ataques de "Evil Twin" ya no son posibles, puesto que, mediante el mecanismo SAE-PK se busca confirmar la identidad del AP, para evitar que exista la suplantación de este dispositivo de red.

8.1. PROPUESTAS DE MEJORA PARA WPA-3

WPA-3 es el actual estándar de seguridad disponible para las redes Wi-Fi. Este sistema es una mejora frente a su antecesor, puesto que mejora la forma en como se realiza la asociación de dispositivos e impide el éxito de ataques como Fuerza Bruta, Evil Twin, Suplantación del AP, etc. Esto lo hace mediante los métodos SAE y SAE-PK, los cuales solventan tales vulnerabilidades encontradas en la versión anterior.

Se debe hacer mención, que actualmente el sistema de seguridad más extendido sigue siendo WPA-2, debido a la poca apertura de los fabricantes para crear dispositivos compatibles con WPA-3. Por tanto, la falta de adopción del estándar WPA-3 provoca que los dispositivos con soporte para WPA-2 sean vulnerables a los ataques antes analizados.

Con base a los problemas encontrados en WPA-2 se propone lo siguiente:

- Rediseño de la estructura de Wi-Fi en el cual se considere la implementación de una notificación de confirmación de des-asociación del dispositivo. Esta sugerencia se plantea como solución a los ataques de inundación de mensajes de desautenticación.

- Aprovechar la tecnología OFDMA presente en Wi-Fi 6, para agregar un identificador a cada conjunto de sub-portadoras para cada dispositivo, de forma que solo se acepten los mensajes provenientes para ese identificador.

- Con base a la conclusión 3, se sugiere implementar un sistema de flujos de tráfico independientes en las redes Wi-Fi, para impedir que otros usuarios conectados a la misma red puedan observar la información de los demás. Esta propuesta se plantea como una solución para evitar que se puedan realizar ataques de filtrado de datos y robo de información.

- Se puede mejorar el sistema SAE-PK de WPA-3 mediante la implementación de un método de asociación que requiera la aprobación de otros equipos conectados, cada vez que un STA nuevo intenta asociarse a la red. El funcionamiento de tal mecanismo podría basarse en la estructura del sistema de Blockchain.

- Mejorar el sistema de encriptación aumentando aún más el número de bits empleados para incrementar la complejidad de la clave de cifrado. Sin embargo, se debe mencionar que el aumento en el número de bits repercute en la capacidad de procesamiento de los dispositivos (STAs, APs y Routers Inalámbricos).

9. RECOMENDACIONES

Con base a la experiencia obtenida realizando la parte experimental de este trabajo de investigación se puede recomendar que:

- Para mejorar la seguridad en los hogares que emplean Wi-Fi como tecnología de acceso, se establezcan contraseñas complejas que contengan al menos: 1 letra mayúscula, 1 minúscula, 1 carácter especial, y que tengan más de 8 caracteres.

- Para las empresas se recomienda utilizar el sistema de seguridad WPA-2 Enterprise o Empresarial, puesto que mejora significativamente la protección frente a ataques debido al uso de un servidor de autenticación AS, que realizar el control de acceso y lleva un registro de actividad de los dispositivos.

- Es recomendable siempre tener instalada la última actualización del sistema de seguridad, con el último parche de seguridad disponible, puesto que este tiene complementos que solucionan algún error existente o protegen de algún ataque.

- En las empresas se recomienda actualizar los equipos cada cierto tiempo, puesto que la mayoría de equipos antiguos son vulnerables a ataques, que en la versión actual del sistema de seguridad, están resueltos. Por ejemplo: WPA-2 es vulnerable frente a ataques de Evil Twin, mientras que en WPA-3 este ataque ya no funciona.

- De forma general, se recomienda que todos los dispositivos Wi-Fi se actualicen a la versión WPA-3, puesto que esta mejora completamente la seguridad y soluciona casi todas las vulnerabilidades que presenta WPA-2.

- La creación de los diccionarios requiere un nivel de procesamiento elevado, debido a la cantidad de caracteres que se tienen que generar, por tanto, para

agilizar su creación se puede emplear un computador con un procesador y una tarjeta gráfica más potentes.

- Si se desea realizar un ataque DoS o DDoS, se recomienda que el equipo con el que se planea realizar las pruebas sea lo más robusto posible, puesto que puede sobrecargarse por la inundación de peticiones.

- Se recomienda instalar Kali Linux en una USB como un Sistema Operativo portable, puesto que permite realizar los ataques desde cualquier lugar, sin estar limitado a un único dispositivo.

- Antes de comprar el adaptador de red, se recomienda revisar si es compatible con el S.O. a utilizar, puesto que, la mayoría de tarjetas de red no son compatibles, por la falta de los drivers que se necesitan para habilitar el modo monitor.

- Para el ataque de captura de claves de inicio de sesión SSL o TLS, se recomienda mantener ejecutado el Sniffer todo el tiempo, puesto que se necesita capturar estos paquetes antes de iniciar el tráfico web, por tanto, es preferible que esté ejecutándose en todo momento para no perder estos paquetes.

- En caso de realizar un ataque del tipo Diccionario, es recomendable crear el diccionario con anterioridad, debido a que, dependiendo de la cantidad de caracteres a generar, este puede tardarse horas e incluso días para crear el archivo con todas las posibles combinaciones.

9.1. TRABAJOS FUTUROS

Debido a la pandemia el acceso a los edificios esta sumamente restringido, por lo que, tener acceso a un lugar que cuente con el servidor de autenticación para realizar pruebas de seguridad en la versión WPA-2 Enterprise es complicado. Por tanto, este trabajo puede servir como punto de partida para la evaluación de seguridad del sistema WPA-2 Enterprise o Empresarial mediante el uso del protocolo RADIUS para comunicarse con el servidor de autenticación.

Por tanto, para estudios futuros se puede considerar analizar la seguridad del sistema WPA-2 empresarial en un ambiente real como la oficina de alguna empresa, para determinar si los ataques realizados en este proyecto de investigación son capaces de vulnerar la seguridad de la red. Los ataques que se pueden considerar para evaluar el sistema WPA-2 Enterprise son:

- Fuerza Bruta o Diccionario
- Evil Twin o Gemelo Malvado
- Denegación de Servicio

Las nuevas investigaciones también pueden extender el estudio comparando WPA-2 Empresarial con la versión de hogar WPA-2 Personal e inclusive con versiones actuales del mismo sistema de seguridad, como WPA-3 Personal y Empresarial.

Este estudio también puede servir como referencia para estudios futuros acerca del sistema de seguridad WPA-3; el cual a día de hoy no puede ser analizado debido a que son muy limitadas las herramientas disponibles para su evaluación. Por tanto, para futuras investigaciones se puede partir de los ataques realizados, las herramientas empleadas y de los resultados obtenidos, como base de próximos proyectos.

10. BIBLIOGRAFÍA

Aircrack-ng. (2020a). *Aircrack-ng*. https://www.aircrack-ng.org/

Aircrack-ng. (2020b). *Aireplay-ng*. http://www.aircrack-ng.org/doku.php?id=aireplay-ng

Aircrack-ng. (2020c). *Airmon-ng*. http://www.aircrack-ng.org/doku.php?id=airmon-ng

Aircrack-ng. (2020d). *Airodump-ng*. http://www.aircrack-ng.org/doku.php?id=airodump-ng

Alam, R., & Tariq, M. A. (2019). *A Survey on Wired and Wireless Network*. https://doi.org/332319614

AlQahtani, A. A. S., Alamleh, H., & Gourd, J. (2020). *BF2FA: Beacon Frame Two Factor Authentication*. https://doi.org/10.1109

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). *Understanding the Mirai Botnet*. https://doi.org/978-1-931971-40-9

Arana, P. (2006). *Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)*.

Armitage, S. (2011). *Known wireless attacks*. 1–5. https://community.jisc.ac.uk

Capano, D. E. (2015). *Control Engineering | Wireless security: Port-based security, EAP, AKM*. https://www.controleng.com/articles/wireless-security-port-based-security-eap-akm/

CCNA desde Cero. (2018). *Diferencias entre Access Point y Router*. https://ccnadesdecero.es/diferencia-access-point-router/

Chen, J.-C., & Wang, Y.-P. (2005). *Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience*. https://doi.org/0163-6804/05

Cisco. (2019). *What Is OFDMA?* https://www.cisco.com/c/en/us/products/wireless/what-is-ofdma.html#~q-a

Cisco Community. (2020). *802.11 frames : A starter guide to learn wireless sniffer traces*. https://community.cisco.com/t5/wireless-mobility-documents/802-11-frames-a-starter-guide-to-learn-wireless-sniffer-traces/ta-p/3110019

Couch, L. W. (2008). 8-11 Redes inalámbricas de datos. In L. M. Castillo (Ed.), *Sistemas de comunicación digitales y analógicos* (Séptima Ed, pp. 637–638).

Pearson.

Dworkin, M. (2007). *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality* (Vol. 1). https://doi.org/800-38C

Frankel, S., Eydt, B., Owens, L., & Scarfone, K. (2007a). Authentication, Authorization, and Accounting Key (AAAK). In *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i* (Primera Ed, pp. 4–5). National Institute of Standards and Technology.

Frankel, S., Eydt, B., Owens, L., & Scarfone, K. (2007b). *Counter Mode with Cipher Block Chaining MAC Protocol (CCMP)*. https://doi.org/20899-8930

Frankel, S., Eydt, B., Owens, L., & Scarfone, K. (2007c). Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. In *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i* (pp. 4.1-4.14).

Frankel, S., Eydt, B., Owens, L., & Scarfone, K. (2007d). Security Framework for Robust Security Networks. In *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i* (Primera, pp. 4-1-4–14). National Institute of Standards and Technology.

GitHub. (2019). *LionSec/Xerosploit: Efficient and advanced man in the middle framework*. https://github.com/LionSec/xerosploit

González, P. (2013). *Hacking WiFi: Descifrando tráfico WEP sin tener la clave, Ataque ChopChop (Parte 9)*. https://www.flu-project.com/2013/12/hacking-wifi-descifrando-trafico-wep.html

Gupta, S. (2016). *A Comparative Analysis of Wired and Wireless Network Architecture*.

Hiertz, G. R., Denteneer, D., Stibor, O., Zang, Y., Costa Pérez, X., & Walke, B. (2010). The IEEE 802.11 Universe. *IEEE Communications Magazine*, 2–4. https://doi.org/0163-6804/10

Huawei. (2019). *Understanding 802.1X Authentication*. https://support.huawei.com/enterprise/es/doc/EDOC1100086527

IEEE Computer Society. (2004a). *802.11i IEEE Standard for Information technology—Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifica*.

IEEE Computer Society. (2004b). *802.11i IEEE Standard for Information technology—*

Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifica. https://doi.org/978-0-7381-7245-3

IEEE Computer Society. (2004c). Overview of Services. In J. Walker (Ed.), *802.11i* (Cuarta, pp. 9–12). IEEE Computer Society.

IEEE Computer Society. (2012a). 4.2 How WLAN systems are different. In A. P. Stephens (Ed.), *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* (Primera, pp. 44–45). IEEE Computer Society.

IEEE Computer Society. (2012b). IEEE Std 802.11 and IEEE Std 802.1X-2004. In A. P. Stephens (Ed.), *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* (1st ed., pp. 83–91). IEEE Computer Society.

IEEE Computer Society. (2020). IEEE 802.1X. In *Port* (Cuarta, pp. 16–17). IEEE Computer Society.

IEFT. (2003). *RFC-3610: Counter with CBC-MAC (CCM)*. CCM. https://datatracker.ietf.org/doc/html/rfc3610

IETF. (2000a). *RFC - 2865: Remote Authentication Dial In User Service (RADIUS)*. https://datatracker.ietf.org/doc/html/rfc2865

IETF. (2000b). *RFC - 2866: RADIUS Accounting*. https://datatracker.ietf.org/doc/html/rfc2866

Intel. (2020). *Diferentes protocolos de Wi-Fi y velocidades de datos*. https://www.intel.la/content/www/xl/es/support/articles/000005725/wireless/legacy-intel-wireless-products.html

Internet Lifeguard. (2018). *WPA2 802.11i*. http://internetlifeguard.network/blog/WPA2-80211i/

Jeon, S., Yu, C., & Suh, Y.-J. (2017). Pre-shared Key Agreement for Secure Public Wi-Fi. *ArXiv*, *1711.22093*, 1–4.

Khasawneh, M., Kajman, I., Alkhudaidy, R., & Althubyani, A. (2017). *A Survey on Wi-Fi Protocols: WPA and WPA2*. https://doi.org/10.1007/978-3-642-54525-2_44

Lynksys. (2017). *¿Qué es MU-MIMO?* https://www.linksys.com/es/r/resource-center/qué-es-mu-mimo/

Oracle. (2009). *Configuring Network Access Control*. https://docs.oracle.com/cd/E19859-01/820-3252-11/FP44ucg_8021x_NW_Access_Control.html

Pirayesh, H., & Zeng, H. (2021). *Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey*.

Rawat, D. B., Yan, G., Bista, B. B., & Chandra, V. "Vigs." (2014). WLAN in AP Mode. In *wireless network Security: an overview* (pp. 208–210).

Russell, D., & Gangemi, G. T. (1991). *Computer security basics*. 448.

Sakib, A. K. M. N., Jaigirdar, F. T., Munim, M., & Akter, A. (2014). Security Improvement of WPA 2 (Wi-Fi Protected Access 2). *International Journal of Engineering Science and Technology (IJEST)*, *3*, 1–8.

Sithirasenan, E., & Muthukkumarasamy, V. (2005). *IEEE 802.11i WLAN Security Protocol A Software Engineer's Model*. https://www.researchgate.net/publication/29453869_IEEE_80211i_WLAN_Security_Protocol_A_Software_Engineer%27s_Model

Sithirasenan, E., & Muthukkumarasamy, V. (2014). *IEEE 802.11i WLAN Security Protocol A Software Engineer's Model*.

Stack Overflow. (2020). *C++ - finding datatypes for 802.11 frame*. https://stackoverflow.com/questions/43780806/finding-datatypes-for-802-11-frame

Stallings, W. (2011). Security Mechanisms. In M. Hirsch, T. Dunkelberger, M. Haggerty, A. Michael, & S. Disanno (Eds.), *Network Security Essentials: Applications and Standards* (Fourth, pp. 17–18). Pearson Prentice Hall.

Tanenbaum, A. & W. D. (2012). Transmisión Inalámbrica. In *Redes de computadoras* (Quinta, pp. 91–99). Pearson.

The Internet Society. (2004). *RFC 3748: Extensible Authentication Protocol (EAP)*. https://datatracker.ietf.org/doc/html/rfc3748

TheHackerWay (THW). (2012). *Wireless Hacking – Ataques contra WEP – Korek Chopchop – Parte IX – Seguridad en Sistemas y Técnicas de Hacking.* https://thehackerway.com/2012/04/16/wireless-hacking-ataques-contra-wep-korek-chopchop-parte-ix/

Tools, K. L. (2016). *Wifiphisher - Penetration Testing Tools*. https://en.kali.tools/?p=90

TP-Link. (2010). *TP Link TL-WN722N* (No. 1; pp. 1–7). TP-Link.

TP-Link. (2020). *TP-Link AX1800 Dual Band Wi-Fi Router* (pp. 1–7). TP-Link.

Tsekleves, E. (2017). *Exposing WPA2 security protocol vulnerabilities*.

Vanhoef, M. (2019). *Dragonblood: Analysing WPA3's Dragonfly Handshake*. https://wpa3.mathyvanhoef.com/

Wi-Fi Alliance. (2019). *WPA3™ Security Considerations*.

Wi-Fi Alliance. (2020a). *Discover Wi-Fi: Security*. https://www.wi-fi.org/discover-wi-fi/security

Wi-Fi Alliance. (2020b). *Security Roadmap and WPA3 Updates*.

Wi-Fi Alliance. (2020c). *Wi-Fi CERTIFIED 6*. https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6

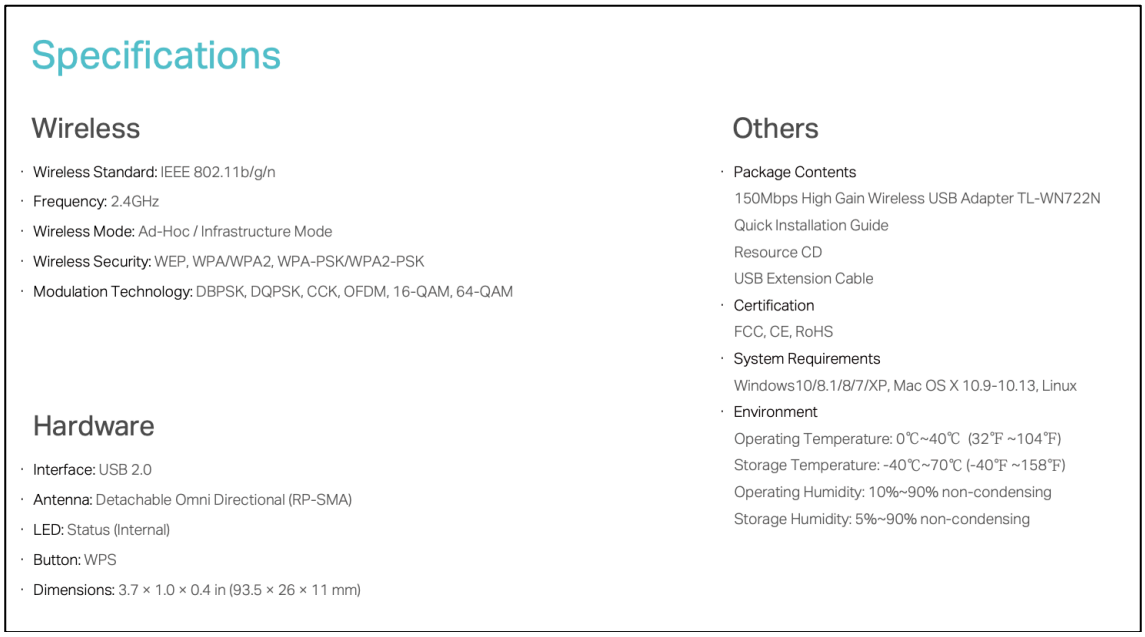
Wi-Fi Alliance. (2020d). *WPA3-Specification Version 3.0*.

Wi-Fi Alliance. (2021). *Wi-Fi Protected Access ® Security Considerations*.

11. ANEXOS

Anexo 1: Datasheets de los dispositivos

Tarjeta de Red TP-Link WN722N Versión 3.20



Specifications

Wireless

- **Wireless Standard:** IEEE 802.11b/g/n
- **Frequency:** 2.4GHz
- **Wireless Mode:** Ad-Hoc / Infrastructure Mode
- **Wireless Security:** WEP, WPA/WPA2, WPA-PSK/WPA2-PSK
- **Modulation Technology:** DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM

Hardware

- **Interface:** USB 2.0
- **Antenna:** Detachable Omni Directional (RP-SMA)
- **LED:** Status (Internal)
- **Button:** WPS
- **Dimensions:** 3.7 × 1.0 × 0.4 in (93.5 × 26 × 11 mm)

Others

- **Package Contents**
  150Mbps High Gain Wireless USB Adapter TL-WN722N
  Quick Installation Guide
  Resource CD
  USB Extension Cable
- **Certification**
  FCC, CE, RoHS
- **System Requirements**
  Windows10/8.1/8/7/XP, Mac OS X 10.9-10.13, Linux
- **Environment**
  Operating Temperature: 0℃~40℃ (32℉ ~104℉)
  Storage Temperature: -40℃~70℃ (-40℉ ~158℉)
  Operating Humidity: 10%~90% non-condensing
  Storage Humidity: 5%~90% non-condensing

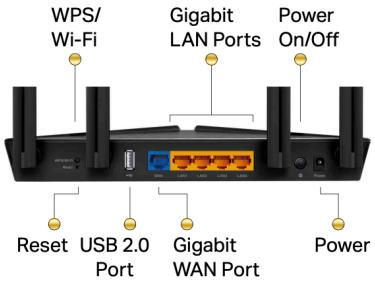
Figura 47: Especificaciones técnicas de la tarjeta de red TP-Link WN722N.
Copyright TP-Link por TP-Link (TP-Link, 2010).

Router Inalámbrico TP-Link AX1800 Archer AX20

Specifications

Hardware

- Ethernet Ports: One Gigabit WAN Port, four Gigabit LAN Ports
- USB Port: One USB 2.0 Port
- Buttons: WPS/Wi-Fi Button, Power On/Off Button, Reset Button
- Antennas: Four External Antennas
- External Power Supply: 12V/1.5A
- Dimensions (W x D x H): 10.2 × 5.3 × 1.5 in (260.2 × 135.0 × 38.6 mm)



Wireless

- Wireless: 1201 Mbps (5 GHz, 11ax) + 574 Mbps (2.4 GHz, 11ax), compatible with 11a/b/g/n/ac Wi-Fi standards
- Frequency: 2.4 GHz and 5 GHz
- Transmit Power:
  FCC:<30dBm(2.4 GHz & 5.15 GHz~5.825 GHz)
- Reception Sensitivity:
  5 GHz:
  11a 6Mbps:-97dBm, 11a 54Mbps:-79dBm
  11ac VHT20_MCS0:-96dBm, 11ac VHT20_MCS11:-66dBm
  11ac VHT40_MCS0:-94dBm, 11ac VHT40_MCS11:-63dBm
  11ac VHT80_MCS0:-91dBm, 11ac VHT80_MCS11:-60dBm
  11ax HE20_MCS0:-95dBm, 11ax HE20_MCS11:-63dBm
  11ax HE40_MCS0:-92dBm, 11ax HE40_MCS11:-60dBm
  11ax HE80_MCS0:-89dBm, 11ax HE80_MCS11:-58dBm
  2.4 GHz:
  11g 6Mbps:-97dBm
  11n HT20_MCS0:-97dBm, 11n HT20_MCS7:-78dBm
  11n HT40_MCS0:-95dBm, 11n HT40_MCS7:-75dBm
  11ac VHT20_MCS0:-96dBm, 11ac VHT20_MCS11:-67dBm
  11ac VHT40_MCS0:-94dBm, 11ac VHT40_MCS11:-64dBm
  11ax HE20_MCS0:-96dBm, 11ax HE20_MCS11:-64dBm
  11ax HE40_MCS0:-93dBm, 11ax HE40_MCS11:-61dBm
- Wireless Function: Enable/Disable Wireless Radio, WMM, Wireless Statistics
- Wireless Security: WPA/WPA2-Personal, WPA2/WPA3-Personal, WPA/WPA2-Enterprise

Figura 48: Especificaciones técnicas de Hardware y Wireless del Router Inalámbrico TP-Link AX1800. Copyright TP-Link por TP-Link (TP-Link, 2020).

Specifications

Software

- Quality of Service: Device Prioritisation
- WAN Type: Dynamic IP/Static IP/PPPoE/PPTP(Dual Access)/L2TP(Dual Access)
- Management: Access Control, Local Management, Remote Management
- DHCP: Server, DHCP Client List, Address Reservation
- NAT Forwarding: Port Forwarding, Port Triggering, UPnP, DMZ
- Dynamic DNS: DynDns, NO-IP, TP-Link
- Access Control: Parental Controls, Local Management Control, Host List, White List, Black List
- Firewall Security: SPI Firewall, IP and MAC Address Binding
- Protocols: IPv4, IPv6
- USB Sharing: Supports Samba(Storage)/FTP Server/Media Server
- Guest Network: 2.4 GHz Guest Network, 5 GHz Guest Network
- VPN Server: OpenVPN, PPTP VPN

Others

- Certification:
  FCC, CE, RoHS
- System Requirements:
  Microsoft Windows 98SE/NT/2000/XP/Vista™/7/8/8.1/10, MAC OS, NetWare, UNIX or Linux
  Internet Explorer 11, Firefox 12.0, Chrome 20.0, Safari 4.0, or other Java-enabled browser
  Cable or DSL Modem
  Subscription with an internet service provider (for internet access)
- Environment:
  Operating Temperature: 0°C~40°C (32°F ~104°F)
  Storage Temperature: -40°C~70°C (-40°F ~158°F)
  Operating Humidity: 10%~90% non-condensing
  Storage Humidity: 5%~90% non-condensing
- Package Contents
  Wireless Router Archer AX20
  Power Adapter
  RJ45 Ethernet Cable
  Quick Installation Guide

Figura 49: Especificaciones técnicas de Software y Otros del Router Inalámbrico TP-Link AX1800. Copyright TP-Link por TP-Link (TP-Link, 2020).

Anexo 2: Combinaciones del diccionario CRUNCH

Diccionario con combinaciones para la clave sencilla: avps1997 (Resumido)

4l3x15&!*
4l3x15&!@
4l3x15&$
4l3x15&$!
4l3x15&$$
4l3x15&$%
4l3x15&$&
4l3x15&$'#'
4l3x15&$*
4l3x15&$@
4l3x15&%
4l3x15&%!
4l3x15&%$
4l3x15&%%
4l3x15&%&
4l3x15&%'#'
4l3x15&%*
4l3x15&%@
4l3x15&&
4l3x15&&!
4l3x15&&$
4l3x15&&%
4l3x15&&&
4l3x15&&'#'
4l3x15&&*
4l3x15&&@
4l3x15&'#'
4l3x15&'#'!
4l3x15&'#'$
4l3x15&'#'%
4l3x15&'#'&
4l3x15&'#'*
4l3x15&'#'@
4l3x15&*
4l3x15&*!
4l3x15&*$
4l3x15&*%
4l3x15&*&
4l3x15&*'#'
4l3x15&**
4l3x15&*@
4l3x15&@
4l3x15&@!
4l3x15&@$
4l3x15&@%
4l3x15&@&
4l3x15&@'#'
4l3x15&@*
4l3x15&@@
4l3x15'#'
4l3x15'#'!
4l3x15'#'!!
4l3x15'#'!$
4l3x15'#'!%
4l3x15'#'!&
4l3x15'#'!*
4l3x15'#'!@
4l3x15'#'$
4l3x15'#'$!
4l3x15'#'$$
4l3x15'#'$%
4l3x15'#'$&
4l3x15'#'$*
4l3x15'#'$@
4l3x15'#'%
4l3x15'#'%!
4l3x15'#'%$
4l3x15'#'%%
4l3x15'#'%&
4l3x15'#'%*
4l3x15'#'%@
4l3x15'#'&
4l3x15'#'&!
4l3x15'#'&$
4l3x15'#'&%
4l3x15'#'&&
4l3x15'#'&*
4l3x15'#'&@
4l3x15'#'*
4l3x15'#'*!
4l3x15'#'*$
4l3x15'#'*%
4l3x15'#'*&
4l3x15'#'**
4l3x15'#'*@
4l3x15'#'@
4l3x15'#'@!
4l3x15'#'@$
4l3x15'#'@%
4l3x15'#'@&
4l3x15'#'@*
4l3x15'#'@@
4l3x15*
4l3x15*!
4l3x15*!!
4l3x15*!$
51x3l4$$
51x3l4$$!
51x3l4$$$
51x3l4$$%
51x3l4$$&
51x3l4$$'#'
51x3l4$$*
51x3l4$$@
51x3l4$%
51x3l4$%!
51x3l4$%$
51x3l4$%%
51x3l4$%&
51x3l4$%'#'
51x3l4$%*

51x314$%@
51x314$&
51x314$&!
51x314$&$
51x314$&%
51x314$&&
51x314$&'#'
51x314$&*
51x314$&@
51x314$'#'
51x314$'#'!
51x314$'#'$
51x314$'#'%
51x314$'#'&
51x314$'#'*
51x314$'#'@
51x314$*
51x314$*!
51x314$*$
51x314$*%
51x314$*&
51x314$*'#'
51x314$**
51x314$*@
51x314$@
51x314$@!
51x314$@$
51x314$@%
51x314$@&
51x314$@'#'
51x314$@*
51x314$@@
51x314%
51x314%!
51x314%!!
51x314%!$
51x314%!%
51x314%!&
51x314%!'#'
51x314%!*
51x314%!@
51x314%$
51x314%$!
51x314%$$
51x314%$%
51x314%$&
51x314%$'#'
51x314%$*
51x314%$@
51x314%%
51x314%%!
51x314%%$
51x314%%%
51x314%%&
51x314%%'#'
51x314%%*
51x314%%@
51x314%&
51x314%&!
51x314%&$
51x314%&%
51x314%&&
51x314%&'#'
51x314%&*
51x314%&@
51x314%'#'
51x314%'#'!
51x314%'#'$
51x314%'#'%
51x314%'#'&
51x314%'#'*
51x314%'#'@
51x314%*
51x314%*!
51x314%*$
51x314%*%
51x314%*&
51x314%*'#'
51x314%**
51x314%*@
51x314%@
51x314%@!
51x314%@$
51x314%@%
51x314%@&
51x314%@'#'
51x314%@*
51x314%@@
51x314&
51x314&!
51x314&!!
51x314&!$
51x314&!%
51x314&!&
51x314&!'#'
51x314&!*
51x314&!@
51x314&$
51x314&$!
51x314&$$
51x314&$%
51x314&$&
51x314&$'#'
51x314&$*
51x314&$@
51x314&%
51x314&%!
51x314&%$
51x314&%%
51x314&%&
51x314&%'#'
51x314&%*
51x314&%@
51x314&&
51x314&&!
51x314&&$
51x314&&%
51x314&&&
51x314&&'#'
51x314&&*
51x314&&@
51x314&'#'
51x314&'#'!
51x314&'#'$
51x314&'#'%
51x314&'#'&

51x314&'#'*
51x314&'#'@
51x314&*
51x314&*!
51x314&*$
51x314&*%
51x314&*&
51x314&*'#'
51x314&**
51x314&*@
51x314&@
51x314&@!
51x314&@$
51x314&@%
51x314&@&
51x314&@'#'
51x314&@*
51x314&@@
51x314'#'
51x314'#'!
51x314'#'!!
51x314'#'!$
51x314'#'!%
51x314'#'!&
51x314'#'!*
51x314'#'!@
51x314'#'$
51x314'#'$!
51x314'#'$$
51x314'#'$%
51x314'#'$&
51x314'#'$*
51x314'#'$@
51x314'#'%
51x314'#'%!
51x314'#'%$
51x314'#'%%
51x314'#'%&
51x314'#'%*
51x314'#'%@
51x314'#'&
51x314'#'&!
51x314'#'&$
51x314'#'&%
51x314'#'&&
51x314'#'&*
51x314'#'&@
51x314'#'*
51x314'#'*!
51x314'#'*$
51x314'#'*%
51x314'#'*&
51x314'#'**
51x314'#'*@
51x314'#'@
51x314'#'@!
51x314'#'@$
51x314'#'@%
51x314'#'@&
51x314'#'@*
51x314'#'@@
51x314*
51x314*!
51x314*!!
51x314*!$
51x314*!%
51x314*!&
51x314*!'#'
51x314*!*
51x314*!@
51x314*$
51x314*$!
51x314*$$
51x314*$%
51x314*$&
51x314*$'#'
51x314*$*
51x314*$@
51x314*%
51x314*%!
51x314*%$
51x314*%%
51x314*%&
51x314*%'#'
51x314*%*
51x314*%@
51x314*&
51x314*&!
51x314*&$
51x314*&%
51x314*&&
51x314*&'#'
51x314*&*
51x314*&@
51x314*'#'
51x314*'#'!
51x314*'#'$
51x314*'#'%
51x314*'#'&
51x314*'#'*
51x314*'#'@
51x314**
51x314**!
51x314**$
51x314**%
51x314**&
51x314**'#'
51x314***
51x314**@
51x314*@
51x314*@!
51x314*@$
51x314*@%
51x314*@&
51x314*@'#'
51x314*@*
51x314*@@
51x31407
51x3140726
51x31407266
51x31407267
51x314076
51x31407626
51x3140767
51x31407697
51x314077

Diccionario con combinaciones para la clave compleja: _@!$_1aF* (Resumido)

_!'#'$@
_!'#'$@
_!'#'$@!
_!'#'$@!
_!'#'$@!!
_!'#'$@!!
_!'#'$@!$
_!'#'$@!$
_!'#'$@!%
_!'#'$@!%
_!'#'$@!&
_!'#'$@!&
_!'#'$@!'#'
_!'#'$@!'#'
_!'#'$@!*
_!'#'$@!*
_!'#'$@!@
_!'#'$@!@
_!'#'$@$
_!'#'$@$
_!'#'$@$!
_!'#'$@$!
_!'#'$@$$
_!'#'$@$$
_!'#'$@$%
_!'#'$@$%
_!'#'$@$&
_!'#'$@$&
_!'#'$@$'#'
_!'#'$@$'#'

_!'#'$@$*
_!'#'$@$*
_!'#'$@$@
_!'#'$@$@
_!'#'$@%
_!'#'$@%
_!'#'$@%!
_!'#'$@%!
_!'#'$@%$
_!'#'$@%$
_!'#'$@%%
_!'#'$@%%
_!'#'$@%&
_!'#'$@%&
_!'#'$@%'#'
_!'#'$@%'#'
_!'#'$@%*
_!'#'$@%*
_!'#'$@%@
_!'#'$@%@
_!'#'$@&
_!'#'$@&
_!'#'$@&!
_!'#'$@&!
_!'#'$@&$
_!'#'$@&$
_!'#'$@&%
_!'#'$@&%
_!'#'$@&&
_!'#'$@&&

_!'#'$@&'#'
_!'#'$@&'#'
_!'#'$@&*
_!'#'$@&*
_!'#'$@&@
_!'#'$@&@
_!'#'$@'#'
_!'#'$@'#'
_!'#'$@'#'!
_!'#'$@'#'!
_!'#'$@'#'$
_!'#'$@'#'$
_!'#'$@'#'%
_!'#'$@'#'%
_!'#'$@'#'&
_!'#'$@'#'&
_!'#'$@'#'*
_!'#'$@'#'*
_!'#'$@'#'@
_!'#'$@'#'@
_!'#'$@*
_!'#'$@*
_!'#'$@*!
_!'#'$@*!
_!'#'$@*$
_!'#'$@*$
_!'#'$@*%
_!'#'$@*%
_!'#'$@*&
_!'#'$@*&

_!'#'$@*'#'
_!'#'$@*'#'
_!'#'$@**
_!'#'$@**
_!'#'$@*@
_!'#'$@*@
_!'#'$@@
_!'#'$@@
_!'#'$@@!
_!'#'$@@!
_!'#'$@@$
_!'#'$@@$
_!'#'$@@%
_!'#'$@@%
_!'#'$@@&
_!'#'$@@&
_!'#'$@@'#'
_!'#'$@@'#'
_!'#'$@@*
_!'#'$@@*
_!'#'$@@@
_!'#'$@@@
_!'#'%
_!'#'%
_!'#'%!
_!'#'%!
_!'#'%!!
_!'#'%!!
_!'#'%!!!
_!'#'%!!!
_!'#'%!!$
_!'#'%!!$
_!'#'%!!%
_!'#'%!!%
_!'#'%!!&
_!'#'%!!&
_!'#'%!!'#'
_!'#'%!!'#'
_!'#'%!!*
_!'#'%!!*
_!'#'%!!@
_!'#'%!!@
_!'#'%!$
_!'#'%!$
_!'#'%!$!
_!'#'%!$!
_!'#'%!$$
_!'#'%!$$
_!'#'%!$%
_!'#'%!$%
_!'#'%!$&
_!'#'%!$&
_!'#'%!$'#'
_!'#'%!$'#'
_!'#'%!$*
_!'#'%!$*
_!'#'%!$@
_!'#'%!$@
_!'#'%!%
_!'#'%!%
_!'#'%!%!
_!'#'%!%!
_!'#'%!%$
_!'#'%!%$
_!'#'%!%%
_!'#'%!%%
_!'#'%!%&
_!'#'%!%&
_!'#'%!%'#'
_!'#'%!%'#'
_!'#'%!%*
_!'#'%!%*
_!'#'%!%@
_!'#'%!%@
_!'#'%!&
_!'#'%!&
_!'#'%!&!
_!'#'%!&!
_!'#'%!&$
_!'#'%!&$
_!'#'%!&%
_!'#'%!&%
_!'#'%!&&
_!'#'%!&&
_!'#'%!&'#'
_!'#'%!&'#'
_!'#'%!&*
_!'#'%!&*
_!'#'%!&@
_!'#'%!&@
_!'#'%!'#'
_!'#'%!'#'
_!'#'%!'#'!
_!'#'%!'#'!
_!'#'%!'#'$
_!'#'%!'#'$

_!'#'%!'#'%
_!'#'%!'#'%
_!'#'%!'#'&
_!'#'%!'#'&
_!'#'%!'#'*
_!'#'%!'#'*
_!'#'%!'#'@
_!'#'%!'#'@
_!'#'%!*
_!'#'%!*
_!'#'%!*!
_!'#'%!*!
_!'#'%!*$
_!'#'%!*$
_!'#'%!*%
_!'#'%!*%
_!'#'%!*&
_!'#'%!*&
_!'#'%!*'#'
_!'#'%!*'#'
_!'#'%!**
_!'#'%!**
_!'#'%!*@
_!'#'%!*@
_!'#'%!@
_!'#'%!@
_!'#'%!@!
_!'#'%!@!
_!'#'%!@$
_!'#'%!@$
_!'#'%!@%
_!'#'%!@%
_!'#'%!@&
_!'#'%!@&
_!'#'%!@'#'
_!'#'%!@'#'
_!'#'%!@*
_!'#'%!@*
_!'#'%!@@
_!'#'%!@@
_!'#'%$
_!'#'%$
_!'#'%$!
_!'#'%$!
_!'#'%$!!
_!'#'%$!!
_!'#'%$!$
_!'#'%$!$
_!'#'%$!%
_!'#'%$!%
_!'#'%$!&
_!'#'%$!&
_!'#'%$!'#'
_!'#'%$!'#'
_!'#'%$!*
_!'#'%$!*
_!'#'%$!@
_!'#'%$!@
_!'#'%$$
_!'#'%$$
_!'#'%$$!
_!'#'%$$!
_!'#'%$$$
_!'#'%$$$
_!'#'%$$%
_!'#'%$$%
_!'#'%$$&
_!'#'%$$&
_!'#'%$$'#'
_!'#'%$$'#'
_!'#'%$$*
_!'#'%$$*
_!'#'%$$@
_!'#'%$$@
_!'#'%$%
_!'#'%$%
_!'#'%$%!
_!'#'%$%!
_!'#'%$%$
_!'#'%$%$
_!'#'%$%%
_!'#'%$%%
_!'#'%$%&
_!'#'%$%&
_!'#'%$%'#'
_!'#'%$%'#'
_!'#'%$%*
_!'#'%$%*
_!'#'%$%@
_!'#'%$%@
_!'#'%$&
_!'#'%$&
_!'#'%$&!
_!'#'%$&!
_!'#'%$&$
_!'#'%$&$

_!'#'%$&%
_!'#'%$&%
_!'#'%$&&
_!'#'%$&&
_!'#'%$&'#'
_!'#'%$&'#'
_!'#'%$&*
_!'#'%$&*
_!'#'%$&@
_!'#'%$&@
_!'#'%$'#'
_!'#'%$'#'
_!'#'%$'#'!
_!'#'%$'#'!
_!'#'%$'#'$
_!'#'%$'#'$
_!'#'%$'#'%
_!'#'%$'#'%
_!'#'%$'#'&
_!'#'%$'#'&
_!'#'%$'#'*
_!'#'%$'#'*
_!'#'%$'#'@
_!'#'%$'#'@
_!'#'%$*
_!'#'%$*
_!'#'%$*!
_!'#'%$*!
_!'#'%$*$
_!'#'%$*$
_!'#'%$*%
_!'#'%$*%
_!'#'%$*&
_!'#'%$*&
_!'#'%$*'#'
_!'#'%$*'#'
_!'#'%$**
_!'#'%$**
_!'#'%$*@
_!'#'%$*@
_!'#'%$@
_!'#'%$@
_!'#'%$@!
_!'#'%$@!
_!'#'%$@$
_!'#'%$@$
_!'#'%$@%
_!'#'%$@%
_!'#'%$@&
_!'#'%$@&
_!'#'%$@'#'
_!'#'%$@'#'
_!'#'%$@*
_!'#'%$@*
_!'#'%$@@
_!'#'%$@@
_!'#'%%
_!'#'%%
_!'#'%%!
_!'#'%%!
_!'#'%%!!
_!'#'%%!!
_!'#'%%!$
_!'#'%%!$
_!'#'%%!%
_!'#'%%!%
_!'#'%%!&
_!'#'%%!&
_!'#'%%!'#'
_!'#'%%!'#'
_!'#'%%!*
_!'#'%%!*
_!'#'%%!@
_!'#'%%!@
_!'#'%%$
_!'#'%%$
_!'#'%%$!
_!'#'%%$!
_!'#'%%$$
_!'#'%%$$
_!'#'%%$%
_!'#'%%$%
_!'#'%%$&
_!'#'%%$&
_!'#'%%$'#'
_!'#'%%$'#'
_!'#'%%$*
_!'#'%%$*
_!'#'%%$@
_!'#'%%$@
_!'#'%%%
_!'#'%%%
_!'#'%%%!
_!'#'%%%!
_!'#'%%%$
_!'#'%%%$

_!'#'%%%%

_!'#'%%%%

_!'#'%%%&

_!'#'%%%&

_!'#'%%%'#'

_!'#'%%%'#'

_!'#'%%%*

_!'#'%%%*

_!'#'%%%@

_!'#'%%%@

_!'#'%%&

_!'#'%%&

_!'#'%%&!

_!'#'%%&!

_!'#'%%&$

_!'#'%%&$

_!'#'%%&%

_!'#'%%&%

_!'#'%%&&

_!'#'%%&&

_!'#'%%&'#'

_!'#'%%&'#'

_!'#'%%&*

_!'#'%%&*

_!'#'%%&@

_!'#'%%&@

_!'#'%%'#'

_!'#'%%'#'

_!'#'%%'#!

_!'#'%%'#!

_!'#'%%'#$

_!'#'%%'#$

_!'#'%%'#%

_!'#'%%'#%

_!'#'%%'#&

_!'#'%%'#&

_!'#'%%'#*

_!'#'%%'#*

_!'#'%%'#@

_!'#'%%'#@

_!'#'%%*

_!'#'%%*

_!'#'%%*!

_!'#'%%*!

_!'#'%%*$

_!'#'%%*$

_!'#'%%*%

_!'#'%%*%

_!'#'%%*&

_!'#'%%*&

_!'#'%%*'#'

_!'#'%%*'#'

_!'#'%%**

_!'#'%%**

_!'#'%%*@

_!'#'%%*@

_!'#'%%@

_!'#'%%@

_!'#'%%@!

_!'#'%%@!

_!'#'%%@$

_!'#'%%@$

_!'#'%%@%

_!'#'%%@%

_!'#'%%@&

_!'#'%%@&

_!'#'%%@'#'

_!'#'%%@'#'

_!'#'%%@*

_!'#'%%@*

_!'#'%%@@

_!'#'%%@@

_!'#'%&

_!'#'%&

_!'#'%&!

_!'#'%&!

_!'#'%&!!

_!'#'%&!!

_!'#'%&!$

_!'#'%&!$

_!'#'%&!%

_!'#'%&!%

_!'#'%&!&

_!'#'%&!&

_!'#'%&!'#'

_!'#'%&!'#'

_!'#'%&!*

_!'#'%&!*

_!'#'%&!@

_!'#'%&!@

_!'#'%&$

_!'#'%&$

_!'#'%&$!

_!'#'%&$!

_!'#'%&$$

Anexo 3: Paquetes SSL o TLS des-encriptados

GET /css/alertify.css HTTP/1.1
Host: sac.unl.edu.ec
Connection: keep-alive
sec-ch-ua: "Google Chrome";v="93", " Not;A Brand";v="99",
"Chromium";v="93"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/93.0.4577.63 Safari/537.36
sec-ch-ua-platform: "Linux"
Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8
Purpose: prefetch
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: style
Referer: https://sac.unl.edu.ec/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: cookiesession1=678B289B01234567898901234ABC2EF3;
_ga=GA1.3.139735224.1630724018; _gid=GA1.3.1732987845.1630724018;
PHPSESSID=pjup9jkjp0achi0vi9jv2emdb1
GET /img/pattern07.png HTTP/1.1
Host: sac.unl.edu.ec
Connection: keep-alive
sec-ch-ua: "Google Chrome";v="93", " Not;A Brand";v="99",
"Chromium";v="93"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/93.0.4577.63 Safari/537.36
sec-ch-ua-platform: "Linux"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/

*;q=0.8

Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://sac.unl.edu.ec/css/login.css?v=1.5
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: cookiesession1=678B289B01234567898901234ABC2EF3;
_ga=GA1.3.139735224.1630724018; _gid=GA1.3.1732987845.1630724018;
PHPSESSID=pjup9jkjp0achi0vi9jv2emdb1
GET /cas/js/cas.js;jsessionid=CBC418C16C84C64D735098FEAB434DBC HTTP/

1.1

Host: sac.unl.edu.ec
Connection: keep-alive
sec-ch-ua: "Google Chrome";v="93", " Not;A Brand";v="99",
"Chromium";v="93"

sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/93.0.4577.63 Safari/537.36
sec-ch-ua-platform: "Linux"

Accept: */*

Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script

Referer: https://sac.unl.edu.ec/cas/login?service=https://
estudiantes.unl.edu.ec/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=CBC418C16C84C64D735098FEAB434DBC;
cookiesession1=678B289B01234567898901234ABC2EF3;
_ga=GA1.3.139735224.1630724018; _gid=GA1.3.1732987845.1630724018;
PHPSESSID=pjup9jkjp0achi0vi9jv2emdb1; _gat_gtag_UA_52918784_7=1
GET /cas/favicon.ico;jsessionid=CBC418C16C84C64D735098FEAB434DBC HTTP/

1.1

Host: sac.unl.edu.ec
Connection: keep-alive
sec-ch-ua: "Google Chrome";v="93", " Not;A Brand";v="99",
"Chromium";v="93"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/93.0.4577.63 Safari/537.36
sec-ch-ua-platform: "Linux"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/

*;q=0.8

Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://sac.unl.edu.ec/cas/login?service=https://
estudiantes.unl.edu.ec/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=CBC418C16C84C64D735098FEAB434DBC;
cookiesession1=678B289B01234567898901234ABC2EF3;
_ga=GA1.3.139735224.1630724018; _gid=GA1.3.1732987845.1630724018;
PHPSESSID=pjup9jkjp0achi0vi9jv2emdb1; _gat_gtag_UA_52918784_7=1
POST /cas/login;jsessionid=CBC418C16C84C64D735098FEAB434DBC?
service=https://estudiantes.unl.edu.ec/login HTTP/1.1
Host: sac.unl.edu.ec
Connection: keep-alive
Content-Length: 170

Cache-Control: max-age=0
sec-ch-ua: "Google Chrome";v="93", " Not;A Brand";v="99",
"Chromium";v="93"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: https://sac.unl.edu.ec
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/93.0.4577.63 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://sac.unl.edu.ec/cas/login?service=https://
estudiantes.unl.edu.ec/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=CBC418C16C84C64D735098FEAB434DBC;
cookiesession1=678B289B01234567898901234ABC2EF3;
_ga=GA1.3.139735224.1630724018; _gid=GA1.3.1732987845.1630724018;
PHPSESSID=pjup9jkjp0achi0vi9jv2emdb1; _gat_gtag_UA_52918784_7=1

username=alexis.pardo%40unl.edu.ec&password=avps1997&lt=LT-1356367-9Ul
2FKQIUTBVI9vgMntd7XMPfE7Prf-
sac.unl.edu.ec&execution=e1s1&_eventId=submit&submit=INICIAR+SESI%C3%93N

Anexo 4: Certificado de traducción

English Speak Up Center

Nosotros "English Speak Up Center"

CERTIFICAMOS que

La traducción del documento adjunto solicitado por el señor **ALEXIS VICENTE PARDO SÁNCHEZ** con cédula de ciudadanía número **1104115439** cuyo tema de investigación se titula: **"Estudio de vulnerabilidades en el sistema de seguridad WPA-2 Personal del estándar IEEE 802.11i y propuestas de mejoras a considerar en el sistema WPA-3",** ha sido realizada por el Centro Particular de Enseñanza de Idiomas "English Speak Up Center".

Esta es una traducción textual del documento adjunto, y el traductor es competente para realizar traducciones.

Loja, 1 de abril de 2022

Mg. Sc. Elizabeth Sánchez Burneo

DIRECTORA ACADÉMICA

DIRECCION: SUCRE 207-46 ENTRE AZUAY Y MIGUEL | TELF: 2565842 - 0995263264