UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Evaluación de vulnerabilidades de seguridad en WLANS y propuesta de mejoras

NIEVES TELLO OSCAR EDUARDO
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

CABRERA TIGRERO MAYKER XAVIER
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

MACHALA
2024

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Evaluación de vulnerabilidades de seguridad en WLANS y propuesta de mejoras

NIEVES TELLO OSCAR EDUARDO
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

CABRERA TIGRERO MAYKER XAVIER
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

MACHALA
2024

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

PROPUESTAS TECNOLÓGICAS

Evaluación de vulnerabilidades de seguridad en WLANS y propuesta de mejoras

NIEVES TELLO OSCAR EDUARDO
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

CABRERA TIGRERO MAYKER XAVIER
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

MOROCHO ROMAN RODRIGO FERNANDO

MACHALA
2024

Evaluación de Vulnerabilidades de Seguridad en WLANS y propuestas de mejoras

by Mayker Cabrera - Oscar Nieves

Submission date: 01-Aug-2024 08:55AM (UTC-0500)
Submission ID: 2422328094
File name: Tesis_Cabrera_Mayker_y_Nieves_Oscar-20240801.docx (2.68M)
Word count: 11717
Character count: 65299

Tesis_Cabrera_Mayker_y_Nieves_Oscar-20240801

ORIGINALITY REPORT

7%	5%	1%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universidad Técnica de Machala Student Paper	1%
2	Submitted to Universidad Internacional de la Rioja Student Paper	1%
3	sedici.unlp.edu.ar Internet Source	<1%
4	docplayer.es Internet Source	<1%
5	www.mnb.hu Internet Source	<1%
6	support.apple.com Internet Source	<1%
7	"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derechos Humanos, Volume 25 (2009)", Brill, 2013 Publication	<1%
8	Submitted to Institución Universitaria Digital de Antioquia Student Paper	<1%

9	fr.slideshare.net Internet Source	<1 %
10	prezi.com Internet Source	<1 %
11	www.semanticscholar.org Internet Source	<1 %
12	issuu.com Internet Source	<1 %
13	transportesynegocios.wordpress.com Internet Source	<1 %
14	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Student Paper	<1 %
15	idoc.pub Internet Source	<1 %
16	Submitted to Student Paper	<1 %
17	www.coursehero.com Internet Source	<1 %
18	Submitted to California State University, San Bernadino Student Paper	<1 %
19	Submitted to Universidad Católica Santo Toribio de Mogrovejo Student Paper	<1 %

20	repositorio.uchile.cl Internet Source	<1 %
21	spiral.imperial.ac.uk Internet Source	<1 %
22	www.tdx.cat Internet Source	<1 %
23	repositorio.utmachala.edu.ec Internet Source	<1 %
24	tesis.ucsm.edu.pe Internet Source	<1 %
25	Pedro José Mujica Paredes. "Fotografía desbordada y sus laberintos:El tránsito de las ecologías artístico-visuales concerniente a la postfotografía y fotografía expandida en Ecuador (2011-2022)", Universitat Politecnica de Valencia, 2024 Publication	<1 %
26	asesorias.com Internet Source	<1 %
27	ccnadesdecero.es Internet Source	<1 %
28	hal.univ-smb.fr Internet Source	<1 %
29	bdm.unb.br Internet Source	<1 %

30	comunicacionsradiofrec.blogspot.com Internet Source	<1 %
31	cooperacionespanola.es Internet Source	<1 %
32	elearning.icesi.edu.co Internet Source	<1 %
33	mit.ocw.universia.net Internet Source	<1 %
34	open_jicareport.jica.go.jp Internet Source	<1 %
35	pc-news.com Internet Source	<1 %
36	people.ac.upc.edu Internet Source	<1 %
37	www.csn.es Internet Source	<1 %
38	www.iproup.com Internet Source	<1 %
39	www.repositoriodigital.ipn.mx Internet Source	<1 %
40	www.slideshare.net Internet Source	<1 %
41	Eric Malmi, Juha Raitio, Oskar Kohonen, Krista Lagus, Timo Honkela. "Chapter 19 Identifying	<1 %

	Anomalous Social Contexts from Mobile Proximity Data Using Binomial Mixture Models", Springer Science and Business Media LLC, 2012 Publication	
42	community.teamviewer.com Internet Source	<1 %
43	docstore.ohchr.org Internet Source	<1 %
44	geekwin.metropoliglobal.com Internet Source	<1 %
45	hdl.handle.net Internet Source	<1 %
46	journal.espe.edu.ec Internet Source	<1 %
47	procesogrupal.overblog.com Internet Source	<1 %
48	repositorio.espe.edu.ec:8080 Internet Source	<1 %
49	repositorio.uncp.edu.pe Internet Source	<1 %
50	repositorio.utn.edu.ec Internet Source	<1 %
51	ww2.ufps.edu.co Internet Source	<1 %

52	www.avanceboricua.org Internet Source	<1%
53	www.cacic2016.unsl.edu.ar Internet Source	<1%
54	www.iin.oea.org Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

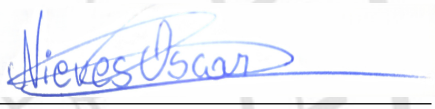
Los que suscriben, NIEVES TELLO OSCAR EDUARDO y CABRERA TIGRERO MAYKER XAVIER, en calidad de autores del siguiente trabajo escrito titulado Evaluación de vulnerabilidades de seguridad en WLANS y propuesta de mejoras, otorgan a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tienen potestad para otorgar los derechos contenidos en esta licencia.

Los autores declaran que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

Los autores como garantes de la autoría de la obra y en relación a la misma, declaran que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asumen la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.



NIEVES TELLO OSCAR EDUARDO
0705704971

CABRERA TIGRERO MAYKER XAVIER
0750504037

DEDICATORIA

Dedico este trabajo de titulación a Dios, por brindar sabiduría y ser la guía indispensable que me permitió culminar esta etapa académica. Agradezco profundamente a mis queridos padres, William Cabrera e Ivoon Tigrero, hacer mención especial a mi abuelita Mirna cuyo apoyo emocional fue determinante en este camino.

Así mismo, es fundamental reconocer a la persona que me brindó el mayor apoyo, amor, confianza y consejos durante toda mi formación académica: mi abuelo Héctor Tigrero. Él siempre creyó firmemente en mí y nunca dudó de que alcanzaría mis metas profesionales. Dedico con todo mi cariño este agradecimiento a él, sabiendo que es la razón de mis éxitos presentes y futuros.

Cabrera Tigrero Mayker Xavier

A mi tía, Ruth Nieves, por ser mi apoyo maternal a lo largo de todo este ciclo de estudios. Gracias por tu infinita paciencia y por estar siempre a mi lado. Tu amor y comprensión han sido fundamentales para superar los momentos difíciles y alcanzar mis metas. A mi primo, Cristhian Suárez, por ser un modelo a seguir y un verdadero mentor. Tu apoyo y guía durante mi camino universitario han sido invaluables. Gracias por enseñarme con tu ejemplo, por tus consejos sabios y por estar siempre dispuesto a ayudarme.

A mi padre, por ser mi pilar económico y emocional. Tu constante motivación y respaldo han sido esenciales para que pueda concentrarme en mis estudios y superarme cada día. Gracias por tus sacrificios, por creer en mí y por impulsarme a alcanzar mis sueños.

A mi abuela, Angelita Peña, por creer en mí incondicionalmente y por tener fe en lo que puedo lograr. Tu confianza ha sido una fuente constante de inspiración y fuerza. Gracias por tus palabras de aliento, por tu cariño inagotable y por ser siempre un ejemplo de perseverancia y amor.

Nieves Tello Oscar Eduardo

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento a mis padres por su constante apoyo a lo largo de este arduo camino académico. También, extendido agradezco al Ing. Rodrigo Morocho y al Ing. Oscar Cárdenas, quienes desempeñaron los roles de Tutor y Co-tutor en este trabajo de titulación. Su orientación y acompañamiento fueron fundamentales para alcanzar este logro.

Además, deseo hacer un reconocimiento especial al Ing. Franklin Arévalo, quien fue mi profesor durante la educación secundaria. Él no solo fue un excelente educador, sino que también se convirtió en un inspirador ejemplo para mí al elegir la carrera de Ingeniería en Tecnologías de la Información.

A todos ellos, mi más sincero agradecimiento por su invaluable contribución en mi formación académica y profesional.

Cabrera Tigrero Mayker Xavier

Agradezco profundamente a mi familia, quienes estuvieron a mi lado durante todo mi camino universitario. Gracias por su apoyo incondicional, su motivación constante y por enseñarme cada día a ser una mejor persona y profesional. Su amor y sacrificios han sido fundamentales para que pueda llegar hasta aquí. A mi abuela y mi tía, por su sabiduría y ternura que siempre me reconfortaron; a mi padre, por su fortaleza y determinación que me inspiraron a seguir adelante; a mi primo, por ser mi compañero de vida y por sus palabras de ánimo en los momentos difíciles. Sin su apoyo, este logro no hubiera sido posible.

Quiero expresar mi sincero agradecimiento al Ing. Rodrigo Morocho y al Ing. Oscar Cárdenas. Gracias por orientarme durante todo el proceso de realización de mi tesis. Su valiosa ayuda, su dedicación y su compromiso fueron fundamentales para el desarrollo y la culminación de este proyecto. Sus conocimientos y consejos me guiaron en cada etapa, y su apoyo constante me dio la confianza para superar los desafíos que encontré en el camino.

Nieves Tello Oscar Eduardo

RESUMEN

En el desarrollo de este proyecto evaluación de vulnerabilidades en entornos WLANs, se inició con una búsqueda bibliográfica detallada sobre los protocolos inalámbricos existentes. Este paso permitió establecer una comprensión sólida y actualizada de las opciones disponibles para optimizar la seguridad en entornos WLAN. Para llevar a cabo la evaluación de vulnerabilidades se utilizó la metodología OWISAN la cual brinda una serie de pasos detallados que permitieron ejecutar en orden el proceso de la investigación, posteriormente se estableció utilizar la distribución de Linux WIFISLAX como herramienta principal para realizar los ataques a los diferentes protocolos de seguridad. Además, se llevó a cabo la investigación de diferentes tipos de ataques a ejecutar siendo estos: ataque de diccionario, hombre en el medio y ataque de desautenticación.

Una vez realizado los diferentes ataques se procedió a identificar las vulnerabilidades que se presentaron en la red, donde se observa el nivel de seguridad que presenta tanto el protocolo WPA2 como el WPA3. Por otro lado, luego de obtener las diferentes vulnerabilidades, se identifica la más importante para cada uno de los protocolos, siendo en WPA2 el ataque de desautenticación y para WPA3 el ataque “men in the middle”, siendo el único ataque capaz de ejecutarse en este protocolo. En base a las mismas se realiza una serie de propuestas de mejoras las cuales aumenten el nivel de seguridad de cada protocolo, obteniendo resultados distintos según el uso de WPA2 y WPA3. Como resultado de mayor relevancia, se identifica que ambos protocolos de seguridad son vulnerables al ataque “men in the middle”, cabe mencionar que este tipo de ataque es posible una vez se logre entrar a la red. Una vez establecidas las mejoras, estas se implementaron en ambos protocolos, posterior a ello se vuelve a realizar los tres ataques y con ello comparar el nivel de seguridad que ofrece cada protocolo, con mejoras implementadas, obteniendo como resultado una amplia mejora en la seguridad de la red, cumpliendo con la hipótesis que se plantea en el presente trabajo, donde se establece que la implementación de controles asegura la protección en un 80% a través del uso de protocolos contra ataques a redes inalámbricas.

Palabras claves: Protocolos inalámbricos, Seguridad WLAN, Vulnerabilidades, Mejoras de Seguridad.

ABSTRACT

In the development of this project, vulnerability assessment in WLAN environments started with a detailed literature search on existing wireless protocols. This step allowed establishing a solid and updated understanding of the options available to optimize security in WLAN environments. In order to carry out the vulnerability assessment, the OWISAN methodology was used, which provides a series of detailed steps that allowed the research process to be carried out in an orderly fashion. In addition, the investigation of different types of attacks to be executed was carried out: dictionary attack, man-in-the-middle attack and deauthentication attack.

The hypothesis put forward in this work is that the implementation of controls ensures 80% protection through the use of protocols against attacks on wireless networks.

Once the different attacks had been carried out, the vulnerabilities presented in the network were identified, where the level of security presented by both the WPA2 and WPA3 protocols was observed. On the other hand, after obtaining the different vulnerabilities, the most important one is identified for each of the protocols, being in WPA2 the deauthentication attack and for WPA3 the "men in the middle" attack, being the only attack capable of being executed in this protocol. Based on these, a series of proposals for improvements are made to increase the security level of each protocol, obtaining different results depending on the use of WPA2 and WPA3. As the most relevant result, it is identified that both security protocols are vulnerable to the "men in the middle" attack, it is worth mentioning that this type of attack is possible once it is possible to enter the network. Once the improvements were established, they were implemented in both protocols, after which the three attacks were performed again and the level of security offered by each protocol was compared with the implemented improvements, obtaining as a result a wide improvement in the network security, fulfilling the hypothesis stated in this work, where it is established that the implementation of controls ensures 80% protection through the use of protocols against attacks on wireless networks.

Keywords: Wireless protocols, WLAN security, Vulnerabilities, Security improvements.

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

GLOSARIO

Vulnerabilidad: Grupo de errores que se ejecutan sin problema permitiendo ataques para interceptar y robar datos que se transmiten mediante una red WIFI:

Riesgo: Acceso a información poco fiables, dispersión y perdida de datos, se accede información ilícita.

Ataque: Conjunto de acciones ofensivas contra sistemas de información los cuales puede ser redes informáticas e incluso a bases de datos.

Seguridad: Se centra en la protección de redes informáticas ante posibles ciberataques.

Protocolo: Es un estándar de comunicación, el cual contiene varias reglas que permite mantener la seguridad de información de una red.

WIFISLAX: Es una distribución de Linux, la cual permite realizar auditorías de seguridad en relación a la informática, destacando una larga lista de herramientas para seguridad y escaneo de red.

WIFI: Es una tecnología de red inalámbrica que conecta dispositivos electrónicos, permitiendo conectarse fluidamente a una red.

WLAN: Tipo de red de área local, esta utiliza comunicación inalámbrica para conectar cualquier dispositivo.

WPA/WPA2: Es un protocolo de integridad el cual evita que intrusos creen una clave de acceso propia. El estándar es remplazo por WPA2 la cual se basa en el mecanismo de seguridad robusta.

WPA3: Protocolo actual de seguridad que muestra mejoras para uso personal y empresarial incluyendo cifrado de datos individualmente.

Adaptador: Hardware que permite enlazar dispositivos entre ellos, pretende enviar y recibir información.

Router: Dispositivo el cual brinda WIFI, por lo general se conecta a un modem.

INTRODUCCIÓN

La evolución tecnológica, genera que las personas tengan mayor acceso a sistemas informáticos. Estos avances aprueban que pueden alcanzar cualquier tipo de información, pero esto causa que aumente el nivel de riesgos y vulnerabilidades con la seguridad de entornos WLAN.

La seguridad informática aparece gracias a la necesidad de brindar soporte a las nuevas tecnologías, infraestructuras de red requerida tanto para empresas como por rede locales. La parte empresarial es quien da información y movilidad a las personas, se debe tratar de manera primordial porque son parte importante de toda organización como sus datos e información. El uso de redes inalámbricas genera el aumento de usuarios y con ello aparecen nuevas herramientas y recursos tecnológicos para emplearse, y nuevas vulnerabilidades, quienes desarrollan nuevas amenazas dado el crecimiento del tráfico de internet, logran que se expanda una superficie de ataque, a medida que sucede, el nivel de riesgo aumenta para empresas o entornos locales generando ataques y que se pierda información.

En respuesta a todo este tipo de vulnerabilidades y riesgos se realizan evaluaciones, auditorias de red con el fin de identificar posibles vulnerabilidades en el entorno WLAN, de esta manera se pueden brindar varias propuestas de mejoras, además de recomendaciones en cuanto a protocolos de seguridad y comparar cuál de ellos es menos propenso a sufrir ataques. Una herramienta para realizar auditoría es WIFISLAX, un entorno Linux que brinda varias herramientas de hacking ético, para que se ejecuten los ataques y en base a observación, realizar propuestas para mejorar la seguridad del entorno WLAN.

i. Declaración y formulación del Problema

Declaración del problema

El incremento de redes de área local inalámbricas, conocidas como WLAN, han generado preocupación respecto a las amenazas de seguridad, las organizaciones dependen cada vez mas de estas redes para su conectividad, impulsando la necesidad de evaluar y mejorar la seguridad de sus infraestructuras informáticas.

A pesar del alto crecimiento tecnológico, las WLAN se ven expuestas a riesgos significativos, accesos no autorizados, ataques cibernéticos, filtración de datos sensibles, etc. La falta de conciencia y la incorrecta implementación de medidas de seguridad que sean efectivas genera vulnerabilidades que amenazan la integridad informativa y su confiabilidad, el alto crecimiento de amenazas genera un escenario donde la auditoria de WLAN es un punto esencial.

Formulación del problema

- **Problema Principal**
    - ¿Cuáles son las principales falencias de control que enfrenta una evaluación de seguridad de WLAN, y como desarrollar estrategias seguras para garantizar la integridad, confidencialidad y disponibilidad de la información?
- **Problemas Específicos**
    - Evaluación de controles de seguridad para proteger la infraestructura inalámbrica y garantizar la integridad de la comunicación de datos en redes WLAN contra posibles amenazas.
    - Conocimiento de seguridad, formar conciencia a usuarios y profesionales TI sobre mejores prácticas de seguridad para el uso de WLAN, contribuyendo a la prevención de amenazas.
    - Fortalecer la seguridad de las redes inalámbricas centrada en la comprensión y la implementación de estrategias para asegurar la integridad de la información.

ii. Objeto de estudio y Campo de acción

Objeto de estudio

- Seguridad de WLAN enfocada a identificar posibles vulnerabilidades, configuraciones inadecuadas y amenazas de seguridad que pueden comprometer la integridad de información.

Campo de acción

- Evaluación de WLAN para identificar posibles vulnerabilidades, configuraciones inadecuadas y amenazas de seguridad que podrían comprometer la integridad de la información.

iii. Objetivos

Objetivo General

- Implementar controles en un entorno WLAN garantizando la seguridad de la infraestructura, mediante la identificación y evaluación de vulnerabilidades.

Objetivos específicos

- Analizar la bibliografía referente a los protocolos de seguridad en una WLAN.
- Diseñar un entorno de infraestructura inalámbrica para la clasificación y protocolos en seguridad.
- Evaluar las vulnerabilidades mediante la herramienta WIFISLAX.
- Investigar los protocolos de seguridad inalámbrica actuales, centrándose en estándares como WPA3 y otros mecanismos avanzados.
- Elaborar un conjunto de recomendaciones detalladas y prácticas para fortalecer la seguridad en los entornos WLAN.
- Evaluar los niveles de seguridad en base a las recomendaciones para fortalecer la seguridad en entornos WLAN.

iv. Hipótesis y variables o preguntas de investigación

La implementación de controles de seguridad en entornos WLAN asegura la protección en un 80% mediante el uso de protocolos contra ataques a redes inalámbricas.

- Variable dependiente: La seguridad del sistema, medida a través de la identificación de vulnerabilidades.
- Variable independiente: La implementación de controles de seguridad en entornos WLAN.

v. Justificación

Este trabajo se desarrolla con el propósito de abordar desafíos y aprovechar oportunidades emergentes en el panorama tecnológico actual, destacando la importancia de la ciberseguridad, eficiencia y confiabilidad de las redes, al considerar los beneficios derivados de un análisis de vulnerabilidades en WLANS, permite detectar fallos de seguridad existentes, la propuesta de soluciones se orienta hacia la adopción del protocolo WPA3, respaldado por la utilización de la herramienta Wifixlas, como práctica recomendada en el entorno de auditoría de laboratorio.

Cabe destacar que la elección del WPA3 como enfoque de auditoría se fundamenta en las múltiples vulnerabilidades identificadas en el protocolo WPA2, teniendo la necesidad de mejorar la seguridad en las redes mediante la adopción propuestas de mejoras.

vi. Organización del documento

El proyecto de integración curricular está dividido en diferentes capítulos, mismo que conforma la siguiente estructura del trabajo de titulación:

Capítulo 1: En el primer capítulo se muestra los antecedentes de investigación, históricos, teóricos y contextuales relevantes para evaluar vulnerabilidades en WLANS y proponer mejoras.

Capítulo 2: En este capítulo se desarrolla del prototipo, en el mismo se indica varias definiciones, el enfoque, alcance, diseño de investigación, unidad de análisis, metodología empleada y las herramientas para construir el prototipo.

Capítulo 3: Se muestran los resultados de la evaluación en cada escenario planteada a través del análisis, para desarrollar propuestas de mejoras, además se realiza las conclusiones y recomendaciones.

CAPÍTULO I MARCO TEÓRICO

1.1 Antecedentes de la Investigación

a) Preguntas de investigación

Tabla 1: Preguntas de Investigación

Preguntas de investigación	Descripción y motivación
R.Q.1 ¿Cuáles son las vulnerabilidades más comunes que afectan a las WLANs en la actualidad?	Esta pregunta indaga sobre las vulnerabilidades más frecuentes en las Redes Inalámbricas Locales (WLANs) hoy en día, como posibles puntos de acceso no seguros y protocolos de cifrado débiles. Comprender estas debilidades es crucial para fortalecer la seguridad en WLANs, contribuyendo a la protección de datos y a prevenir ataques cibernéticos
R.Q.2 ¿Cómo han evolucionado las amenazas y vulnerabilidades en las WLANs a lo largo del tiempo?	Esta pregunta busca analizar la evolución histórica de amenazas y vulnerabilidades en las Redes Inalámbricas Locales (WLANs). Comprender este desarrollo a lo largo del tiempo es esencial para diseñar estrategias de seguridad adaptadas y anticiparse a riesgos emergentes, fortaleciendo así la protección de las WLANs.
R.Q.3 ¿Cuál es el impacto de las vulnerabilidades en las WLANs en la seguridad de la información?	Esta pregunta explora el impacto potencial de vulnerabilidades en las Redes Inalámbricas Locales (WLANs) en la seguridad de la información y la privacidad de los usuarios, subrayando la importancia de comprender las posibles repercusiones de fallos de seguridad para desarrollar medidas efectivas y garantizar un entorno inalámbrico seguro y confiable.
R.Q.4 ¿Cuáles son las metodologías y herramientas más utilizadas para evaluar vulnerabilidades en redes inalámbricas?	Esta pregunta busca identificar las metodologías y herramientas más utilizadas en la evaluación de vulnerabilidades en redes inalámbricas, proporcionando una visión práctica y efectiva para fortalecer la seguridad. Entender estas prácticas comunes es esencial para adaptarse a las tendencias actuales y garantizar evaluaciones exhaustivas y precisas en entornos inalámbricos.
R.Q.5 ¿Cuál es la relevancia de mejorar la seguridad en las WLANs, especialmente en un contexto de creciente dependencia de la conectividad inalámbrica?	La creciente interconexión de dispositivos y la transmisión de datos sensibles subrayan la necesidad apremiante de medidas de seguridad robustas para preservar la integridad de las comunicaciones y proteger la información en entornos cada vez más dependientes de la conectividad inalámbrica.
R.Q.6 ¿Cómo contribuye la protección de datos sensibles y la prevención de ataques cibernéticos en la seguridad de las WLANs?	. La motivación radica en explorar cómo fortalecer la seguridad inalámbrica puede tener un impacto directo en la integridad de la información y la resistencia contra amenazas digitales, promoviendo entornos más seguros y confiables.

b) Palabras claves y Cadena(s) de búsqueda

En el proceso de búsqueda de información relevante para el estudio sobre la evaluación de vulnerabilidades en redes inalámbricas (WLAN) y propuestas de mejoras en su seguridad, se utilizó una selección cuidadosa de palabras clave y una cadena de búsqueda estratégica. Las bases de datos digitales seleccionadas y consultadas fueron IEEE Explorer, IET Information Security, IJCSNS y Web of Science.

Palabras clave

- Wireless network
- Vulnerability Assessment
- Security Improvements
- Security Protocols
- Threats to network

Cadena de búsqueda

- Wireless network and security protocols
- (Security protocols or Vulnerability Assessment) and wireless network
- Vulnerability assessment and wireless network
- Security protocols and wireless network

c) Criterios de inclusión y exclusión

Criterio de inclusión:

- Estudios primarios que se centren en la evaluación de vulnerabilidades en redes inalámbricas (WLAN).
- Estudios que aborden la integración y comunicación entre la ingeniería de requisitos y la ingeniería de seguridad, con un enfoque en WLAN.
- Estudios publicados desde enero 2018 hasta hoy.
- Investigaciones que relacionen específicamente los requisitos y la seguridad en WLAN.
- Investigaciones que relacionen el diseño y la seguridad en WLAN.

Criterio de exclusión:

- Estudios secundarios, como revisiones sistemáticas o metaanálisis.
- Artículos cortos de tres páginas o menos.
- Estudios duplicados, considerando solo una copia de cada estudio.
- Artículos que no estén escritos en inglés.
- Estudios que no estén directamente relacionados con las WLAN utilizando los términos clave mencionados.
- Literatura gris, documentos no publicados comercialmente.
- Trabajo redundante de la misma autoría.
- Publicaciones cuyo texto no esté disponible para revisión.
- Estudios cuyo enfoque no se centre en la evaluación de vulnerabilidades de WLAN utilizando los términos clave mencionados, excluyendo temas específicos que no estén directamente relacionados con la seguridad de WLAN.

d) Proceso y resultados de la búsqueda

Para el proceso de búsqueda de información, se indago en diferentes bases de datos científicas, se aplica una indagación con la cadena de búsqueda que se menciona anteriormente y con ello se filtran diferentes artículos de revistas.

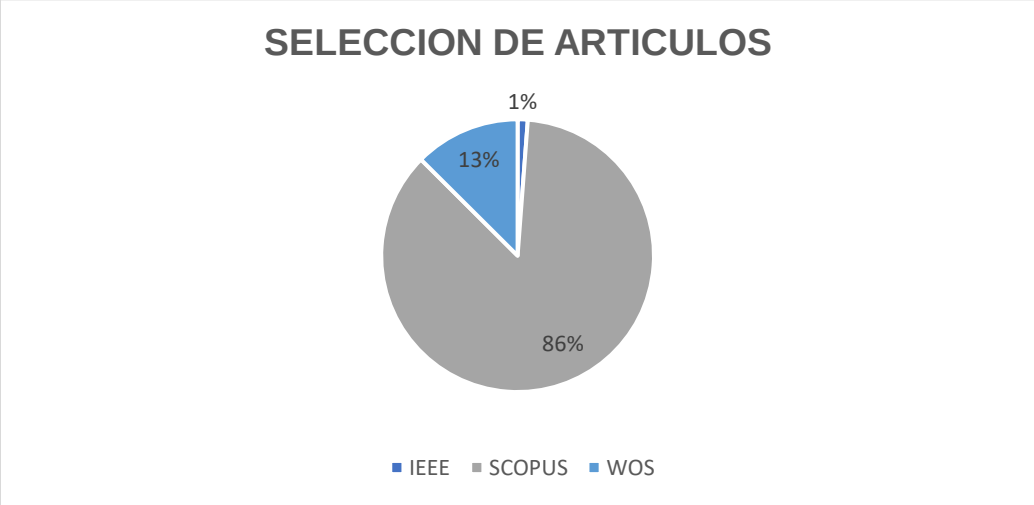


Figura 1: Artículos Encontrados

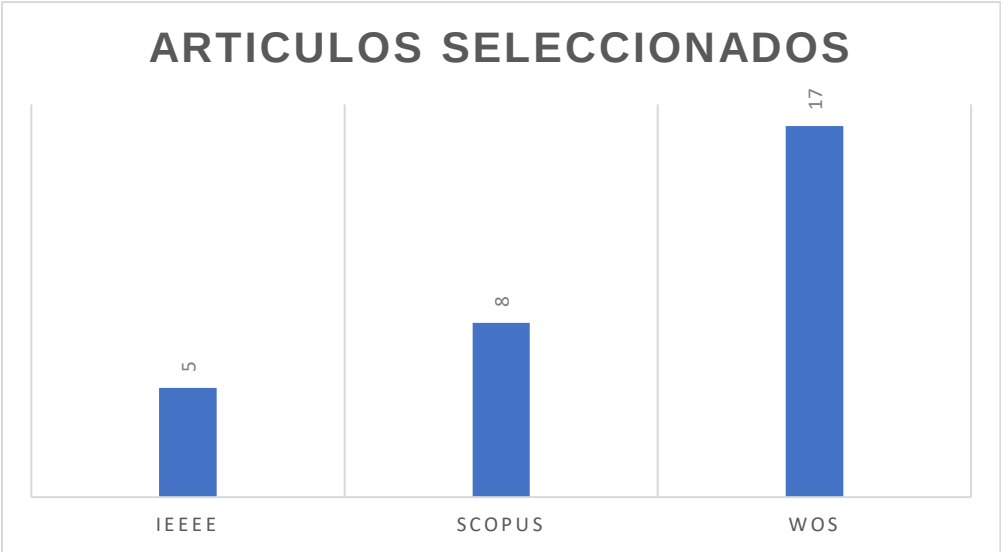


Figura 2: Artículos Seleccionados:

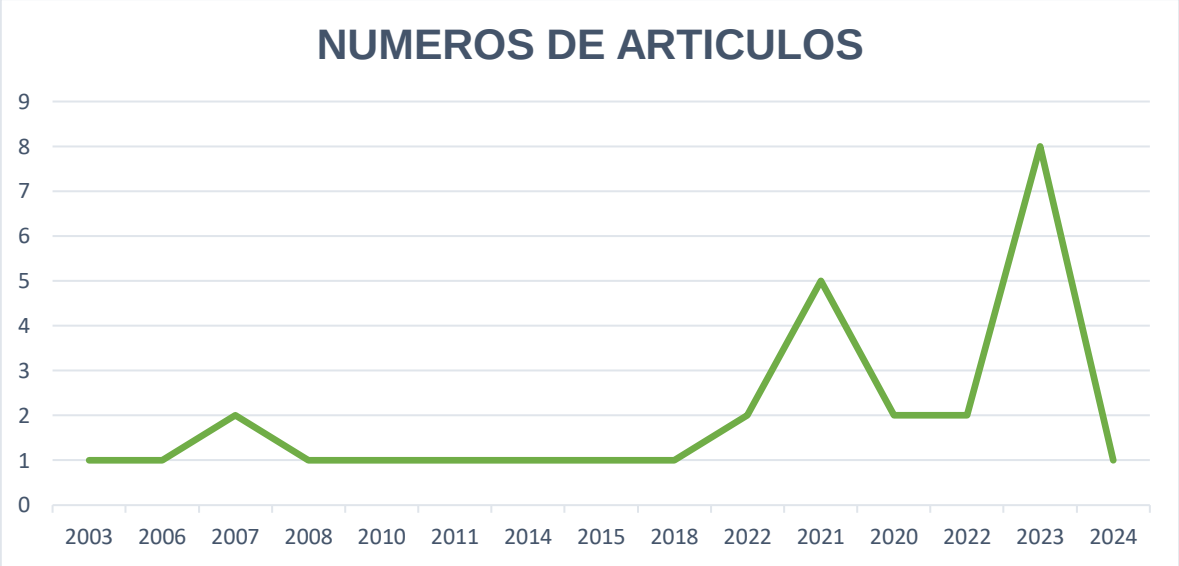


Figura 3: Artículos de acuerdo a los años de publicación

1.2 Antecedentes Históricos

Una red inalámbrica se describe como un sistema de comunicación que facilita la conectividad entre dispositivos electrónicos sin necesidad de utilizar cables físicos.

En [1] menciona que las redes se originan como una extensión de las redes cableadas, presentando una nueva opción para la transferencia de información, es importante destacar que esta modalidad prescinde de un medio físico, lo que proporciona una mayor movilidad a los usuarios sin comprometer la conectividad. [2].

Así, en cuanto a la dependencia tecnológica inalámbrica, la creciente conectividad expone riesgos de seguridad, donde se enfrenta a desafíos y avances importantes centrando los aspectos para la protección de datos y privacidad de los usuarios.

Dentro de un estudio realizada por Julio Barreno y José Ponce [3] menciona que, al abordar el tema de seguridad en redes inalámbricas, es esencial comprender los protocolos de encriptación como WEP o WPA, los cuales son susceptibles a ataques de fuerza bruta, para fortalecer la seguridad, es crucial familiarizarse con los protocolos más avanzados, como WPA2 y WPA3. Según [4] este último destaca como la opción más reciente y eficaz debido a sus mejoras significativas, proporcionando una capa adicional de protección en comparación con sus predecesores. Por otro lado, [5] habla sobre estos protocolos y como brindan seguridad diseñada para proteger redes inalámbricas contra amenazas de seguridad, no obstante, es importante mencionar que el protocolo WPA3 a diferencia del WPA2 cuenta con menor tiempo dentro del mercado, sin embargo, este trabaja como una propuesta de mejora dado dicho protocolo es más seguro e incluso cuando la conexión no lo es, siendo esta su mayor diferencia con su antecesora [6]. Es importante destacar que este protocolo presenta dos modalidades, tanto para uso personal como empresarial, ofreciendo diversas opciones para garantizar la protección de los datos almacenados y el tráfico web, incluso en situaciones de intromisión. En el ámbito empresarial, este protocolo puede ser implementado en redes gubernamentales, corporativas o instituciones financieras, proporcionando una capacidad mejorada de encriptación para salvaguardar información confidencial de manera efectiva. [7].

Según menciona Marco Suing y Alexis Pardo [8] los problemas que se evidencian la necesidad de la investigación para con ello precisar cuáles son las fallas en la seguridad y que mecanismos emplear para mitigar posibles vulnerabilidades.

La creciente dependencia de las WLAN ha suscitado una atención considerable en la comunidad de seguridad informática, algunas investigaciones referentes a lo mencionado han obtenido varios resultados interesantes [9].

El crecimiento continuo del número de usuarios en las redes inalámbricas, acompañando del aumento de herramientas y recursos tecnológicos, ha generado un escenario donde se incrementen las vulnerabilidades y amenazas, este fenómeno se atribuye al aumento del tráfico en internet, que ha propiciado una expansión de los ataques, según este panorama

evolucionando, la cantidad de riesgos asociados también se eleva significativamente. A nivel empresarial, más de un tercio experimenta pérdidas en ingresos como consecuencia de estos desafíos de seguridad. [10].

El riesgo principal al enfocar la seguridad dentro de una red de área local, a implementar este tipo de entorno dentro de un ámbito hogareño no es de mucha necesidad un nivel alto de seguridad, esto debido que los datos que se transmiten no tienen una magnitud de relevancia. En cuanto un escenario de mayor importancia, el cual maneja datos confidenciales, por lo general tiende a ser un objetivo de ataques, pueden darse por temas de prueba, obtención de información, estos riesgos generan una vulnerabilidad de mayor interés [11].

Según menciona [12] a lo largo del tiempo, el impacto de las vulnerabilidades en las WLANs ha experimentado una evolución en respuesta a los cambios tecnológicos, las prácticas de seguridad y las amenazas emergentes, entre las vulnerabilidades más frecuentes se encuentra el riesgo inherente de una red abierta, donde cualquier individuo con acceso a un punto de acceso (AP) y las credenciales necesarias, a través de una interfaz de red inalámbrica (NIC), puede ingresar a la información y obtener acceso a la WLAN. Estos ataques pueden ser desencadenados por factores externos o incluso involuntariamente por empleados, siendo los siguientes los más comunes:

- Intercepción de datos.
- Intrusos inalámbricos.
- Ataques de Denegación de Servicios (DoS).
- APs Falsos/Rogue
- Dispositivos configurados inapropiadamente.
- Usuarios malintencionados interfiriendo en comunicación inalámbrica.
- Puntos de acceso sin autorización.
- Ataques Man-in-the Middle.

Según Alaa Hussein, Zeki Saeed y Fatima Yasein [13] expresa que el acceso no autorizado a una red se considera como intercepción de comunicaciones, al carecer de cifrado o debilidades de protocolos de seguridad, genera que exista un mayor riesgo lo cual compromete a la privacidad que se transmite a través de la red. Las WLANs vulnerables también se convierten en posibles vectores para la propagación de malware, ya que los

atacantes pueden aprovechar las debilidades de seguridad para infiltrar dispositivos y propagar amenazas, la evolución de los estándares WLAN introduce desafíos adicionales ya que nuevas vulnerabilidades surgen con la adopción de tecnologías más avanzadas, resaltando la importancia de la aplicación oportuna de parches y actualizaciones de seguridad [14].

Para mitigar estos impactos es necesario que se realicen buenas prácticas de seguridad, por ejemplo, mantener software y fimware actualizados, utilizar protocolos de seguridad y cifrado en las configuraciones de red [15].

El WPA permite que se puede establecer conexiones por lo general hasta ocho enlaces, cada uno de estos cuenta con una integración hasta una navegación, según [16] este protocolo cuenta con tecnología OFDMA la cual permite conexiones de manera simultánea al igual que tecnología BSS lo cual reduce las interferencias.

1.3 Antecedentes teóricos

1.3.1 Definición de una Red:

Una red es definida como una función para agrupar varios tipos de dispositivos y que se comuniquen entre ellos, todo aquel dispositivo que transmite datos forma parte de dicho conjunto, permitiendo la interacción y conectividad de los usuarios [17].

1.3.2 Redes Inalámbricas:

Una red inalámbrica se utiliza para establecer conexiones entre dispositivos sin necesidad de utilizar cableado, posibilitando la transferencia de información, datos, videos, entre varios tipos de dispositivos [17].

Así mismo [18] habla sobre este tipo de redes, permite que aquellos dispositivos que se manejan dentro de un perímetro de la red puedan tener acceso. Existen grupos que se dividen de la siguiente manera:

- Redes inalámbricas de área personal (WPAN)
- Redes inalámbricas de área local (WLAN)
- Redes inalámbricas de área metropolitana (WMAN)
- Redes inalámbricas de área amplia (WWAN)

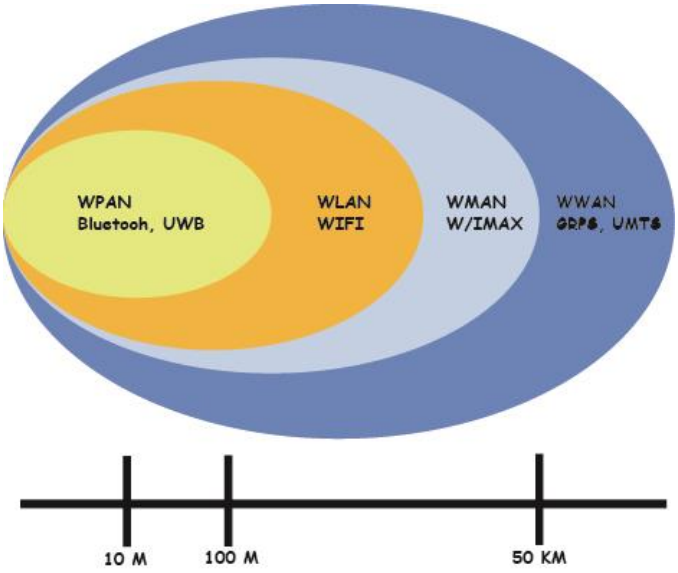


Figura 4: Clasificación de las redes inalámbricas

En la figura 4 se muestra como son los niveles de alcance de distancia para cada uno de las redes inalámbricas.

Para facilitar una expansión sin dificultades en redes inalámbricas y con ello garantizar la compatibilidad, fue necesario que se establezcan estándares, según [19] estos se definen como documentos publicados para establecer procesos específicos diseñados para aumentar confiabilidad entre los materiales, productos, métodos y servicios los cuales se usan dentro de la vida cotidiana. Al implementar estándares se logra proporcionar un marco el cual asegura la Inter operatividad y la eficiencia dentro del desarrollo, despliegue y uso de tecnologías inalámbricas [20].

1.3.4 Seguridad en Redes Inalámbricas:

Las WLANs, están expuestas a varios tipos de amenazas como: intercepción de datos, acceso no autorizado, ataques a la integridad de la red. El estándar de seguridad más común para WLANs, incluye el protocolo WEP (Wired Equivalent Privay), WPA (Wi-Fi Protected Access), WPA2 y WPA3 siendo el más actual en el ámbito de seguridad [21].

1.3.5 Protocolos de Seguridad WLAN:

- **WEP:** es uno de los primeros protocolos de seguridad para WLANs, sin embargo, se muestra su vulnerabilidad ante ataques de fuerza bruta, por tanto, no es recomendable su uso [22].
- **WPA y WPA2:** son mejoras continuas de seguridad, no obstante, se enfrenta a desafíos como ataques de acceso no autorizado, estos pueden comprometer a la seguridad de la red [22].
- **WPA3:** según es la versión estándar más actualizada para protección de red, remplazando a WPA2, este introduce nuevas funciones en redes de seguridad abiertas, aumentando la solidez criptográfica, permitiendo un proceso de autentificación que sea más seguro para todos los puntos finales que sean compatibles con WPA3 [23].

1.3.6 Ataques comunes en WLANs:

Las pruebas de seguridad en WLANs, se realizan bajo un entorno controlado para evitar algún tipo de problema o interferencia, Bashyer Ahmed y Hatiim Alsuwat [24] mencionan algunos de los siguientes tipos de ataques:

- **Escaneo de redes Inalámbricas:** el objetivo es recorrer áreas a través de un dispositivo móvil para identificar y mapear redes Wi-Fi [25].
- **DoS (Denia lof Service):** su objetivo es saturar un sistema, red o servicio para que sea inaccesible para usuarios legítimos.
- **DDoS (Destributed Denia of Service):** trabaja con múltiples sistemas que permiten inundar el objetivo mediante tráfico abrumador, lo cual hace más difícil mitigar que un ataque DoS convencional.
- **MITM (Ataques de hombre en el medio):** Es la intercepción de comunicaciones mediante dispositivos para capturar datos, que el agresor puede controlar la comunicación entre usuarios legítimos, permitiéndole alterar, manipular y cambiar los mensajes intercambiados entre ellos. Además, el atacante puede inducir al usuario legítimo a establecer un canal de comunicación con una estación base simulada, conocida como estación base mendaz en el contexto de un ataque de Hombre en el Medio (MITM).

- **Jamming:** Es una acción maliciosa que se clasifica como un ataque activo, cuyo propósito es interrumpir la conexión entre dos usuarios legítimos, se caracteriza por la creación deliberada de interferencias por parte de una entidad maliciosa con la intención de perjudicar la comunicación entre usuarios válidos. Este tipo de ataque busca bloquear la comunicación entre dispositivos inalámbricos, generando una saturación en el canal de comunicación [26].

1.3.7 Amenazas en WLANS

Una amenaza hace referencia a un tipo de evento, acción o entidad el cual tiene potencial de explotar una vulnerabilidad dentro de una red, las amenazas en WLANS incluyen ataques maliciosos, acceso no autorizado, o cualquier tipo de actividad que comprometa la integridad, confidencialidad o disponibilidad de una red [27].

1.3.8 Riesgos WLANS

Un riesgo se define como una medida de probabilidad de que una amenaza en específico se materialice provocando un impacto adverso dentro de la seguridad de la red, esto implica que tanto la combinación de una amenaza, vulnerabilidad y una consecuencia se manifieste como una posibilidad de acceso no autorizado provocando fuga de información o una interrupción de servicio [27].

1.3.9 Herramientas para evaluación de vulnerabilidades en WLANs:

- **Wifislax:** Se hace referencia a una distribución de GNU/Linux que se fundamenta en las funcionalidades de LiveCD y LiveUSB, facilitando la realización de auditorías de seguridad informática de manera integral, esta distribución cuenta con un conjunto de herramientas especializadas en seguridad, destacando la presencia de escáneres de puertos y vulnerabilidades. Además, proporciona la capacidad de crear exploits, sniffers y herramientas de análisis forense diseñadas específicamente para la evaluación de entornos inalámbricos.
- **Kali Linux:** Sistema operativo usado para proteger y optimizar ordenadores, redes y permitir el descifrado de contraseñas, funciona bajo una licencia GNU GPL que hace una herramienta de código abierto. Cuenta con ms de 600 herramientas de seguridad,

se emplean para pruebas de penetración y la información forense, su distribución comprobando posibles vulnerabilidades en entornos WLANs [28].

- **Airgeddon:** Es una herramienta para pruebas de penetración, misma que permite realizar evaluación de vulnerabilidades en redes inalámbricas, cabe mencionar que el uso de dicha herramienta debe ser ética, algunas de las funciones que cumple son: escaneo de redes, ataques de fuerza bruta, ataque de captura Handshake, ataque MITM, ataque Pixie Dust.

1.3.10 Tipos de ataques

- **Fern Wifi Cracker**

Es una herramienta la cual permite realizar pruebas de penetración diseñada para ayudar a la recuperación de claves tanto en WEP/WPA/WPS, este funciona a través de exploración y captura de tráfico de datos de una red inalámbrica para luego intentar descifrar las contraseñas, esto a través de ataques de fuerza bruta o de diccionario. Es importante que la herramienta para auditoria de seguridad brinde a los administradores de redes evaluar la robustez de la contraseña y con ello tomar medidas con el fin de fortalecer la seguridad de dicha red [29].

- **Flexión**

En seguridad informática, Flexión se asocia a la manipulación de datos dentro de una red para cumplir objetivos especifico, esta puede incluir la modificación de paquetes de datos, explotar vulnerabilidades dentro de protocolos de red e incluso realizar ataques como "Man-in-the-Midle", lo cual podría interceptar, modificar o redirigir el tráfico de red [30].

- **Airodump-ng (airocrack para evaluación de redes)**

Es una herramienta la cual utiliza línea de comando para realizar captura de paquetes de redes inalámbricas, de esta forma recopila datos sobre redes inalámbricas circundantes, lo cual incluye clientes conectados y sus actividades, este se emplea junto con Aircrack-ng el cual permite evaluar seguridad de una red WIFI a través de la recuperación de claves WEP/WPA mediante un ataque de fuerza bruta o de diccionario [31].

- **Wireshark**

Wireshark es una herramienta que permite analizar protocolos de red para capturar y examinar paquetes de datos en una red. Wireshark no se usa directamente para ataques, se utiliza para diagnóstico y análisis. No obstante, esta puede ser empleada por personas malintencionadas para capturar información sensible si se utiliza sin autorización en una red, dentro de entornos legítimos, esta herramienta permite que los administradores de redes puedan realizar análisis de tráfico y con ello dar soluciones a los problemas en la red [32].

1.4 Antecedentes contextuales

Dentro del ámbito de evaluación de vulnerabilidades en WLANs, es fundamental entender el contexto en el cual se desenvuelven estas nuevas tecnologías, la creciente dependencia dentro de entornos caseros y comerciales lleva consigo una proliferación de varios tipos de amenazas y vulnerabilidades las cuales necesitan que se realice una evaluación constante y con ello proponer propuestas de mejoras.

Con el avance del tiempo y la tecnología, la seguridad en las WLANs se ha convertido en un tema crítico, principalmente debido a la naturaleza inalámbrica de la comunicación, la ausencia de protocolos de seguridad adecuados puede hacer que estas redes sean susceptibles a ataques maliciosos. Por este motivo, resulta crucial considerar estándares de seguridad, familiarizarse con herramientas de evaluación de vulnerabilidades e identificar las amenazas o ataques potenciales. Este enfoque proactivo es esencial para salvaguardar la integridad y confidencialidad de la información que se transmite a través de las redes inalámbricas [33].

En cuanto a las redes de área local y su administración como manejo de mantenimiento funcional, siendo una red la cual utiliza determinado número de servicios, el administrador de la red desempeña un papel central en la configuración, identificación y resolución de fallas, gestión de la contabilidad y, especialmente, en la seguridad de la red, su responsabilidad abarca diversos aspectos, desde garantizar la disponibilidad de los servicios hasta monitorear la tasa de transferencia. Además de estas funciones esenciales, el administrador aborda vulnerabilidades especificas en las redes inalámbricas, la implementación de políticas definidas por el administrador es crucial en la optimización del rendimiento de la red en cualquier momento, asegurando que la WLAN esté protegida contra posibles amenazas y vulnerabilidades [34].

Para evaluar las vulnerabilidades dentro del entorno de trabajo es necesaria una herramienta la cual permita realizar el escaneo y con ello detectar ataques dentro de la red, para el presente trabajo el sistema operativo a emplear es WIFISLAX, dado que contiene preinstalado una variedad de herramientas que son diseñadas para evaluar la seguridad de redes inalámbricas, además de permitir realizar pruebas de penetración y evaluaciones de redes, empleando pruebas éticas y auditoria de seguridad.

Es fundamental considerar que el uso de herramientas de seguridad debe hacerse ética y legal, aunque las pruebas de vulnerabilidades puedan evaluar. El acceso no autorizado a una red, incluso con fines de prueba, podría infringir la ley. Es imperativo obtener el consentimiento explícito de la entidad antes de llevar a cabo cualquier evaluación de seguridad.

Los ataques de agotamiento de recursos basados en protocolos representan una amenaza significativa para la seguridad de servidores y sitios web al enfocarse en los recursos críticos del servidor, como memoria, CPU y almacenamiento, estos ataques medidos en paquetes por segundo (pps), aprovechan vulnerabilidades en los protocolos de comunicación de la capa de red. Un ejemplo destacado es el ataque TCP SYN Flood, que emplea señales SYN para obligar al servidor a establecer conexiones ficticias, agotando su capacidad para gestionar nuevas conexiones, la comprensión y la eficaz mitigación de estos ataques son fundamentales para garantizar la disponibilidad e integridad de los servicios en línea [35].

En el contexto de este trabajo, la evaluación se realiza en un entorno real, utilizando dispositivos necesarios para ejecutar la evaluación. esta metodología permite realizar la tarea de forma segura y ética, brindando propuestas de mejoras que puedan ser consideradas por las partes interesadas, el enfoque garantiza la integridad legal y ética de la evaluación de vulnerabilidades, al mismo tiempo que promueve prácticas de seguridad responsables.

1.4.1 Ámbito de Aplicación

La seguridad en WLANS se ha vuelto fundamental, enfatizando la protección de redes, que manejan varios tipos de información, identificando, analizando y mitigar posibles vulnerabilidades y amenazas que comprometan a la integridad de la red, brindando propuestas de mejora.

1.4.2 Establecimiento de Requerimientos

Para implementar el prototipo de seguridad de WLANS en un entorno de red de área local se requiere:

- Topología de red inalámbrica.
- Sistema operativo Linux (WIFISLAX)
- Adaptador de red con estándares IEEE 802.11
- Punto de acceso con estándares IEEE 802.11
- Router que soporte protocolos de seguridad WPA, WPA2, WPA3.

CAPITULO II. DESARROLLO DEL PROTOTIPO

2.1 Definición del prototipo

En cuanto a la definición del prototipo, este consta de una arquitectura de WLAN física diseñada para una red inalámbrica interna, una zona WLAN como la salida a internet, una zona de ataque donde se observa las vulnerabilidades de la red inalámbrica. También se observa el dispositivo que actúa como atacante a la red, permitiendo identificar el tipo de vulnerabilidades de la red según los protocolos de seguridad que utilice.

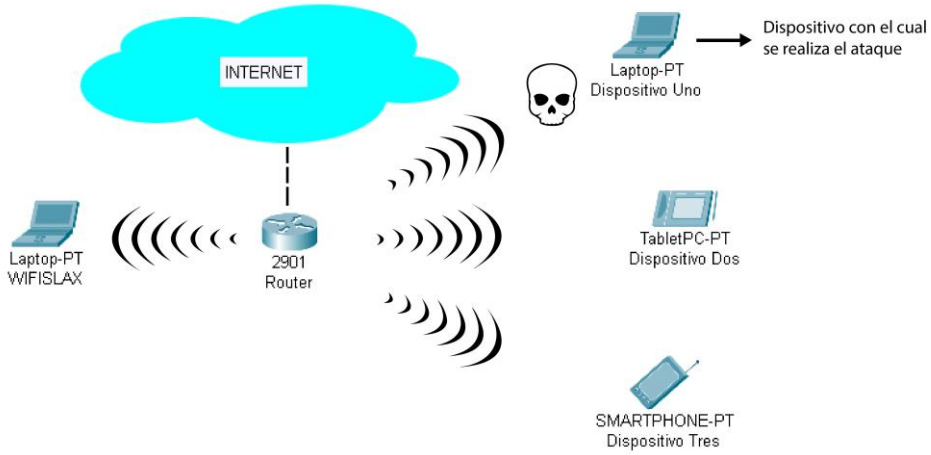


Figura 5: Topología de Red

2.2 Metodología de desarrollo del prototipo

2.2.1 Enfoque, alcance y diseño de investigación

El enfoque que se utiliza es investigación, cuantitativo, al ser un caso experimental, mismo donde se emplean herramientas de escaneo de vulnerabilidades para identificarse y analizarse, además de estar basadas en información y estudios realizados de forma que respalden la información y con ello pronunciar propuestas de mejoras para evitar problemas en la red.

Dentro de la investigación de campo, tanto la recolección de información como el análisis, comprobaciones, aplicación práctica y métodos empleados para llegar a las conclusiones.

Para ello se utiliza el método de análisis que identifica las amenazas que puedan presentarse en una red local, hay que realizar escaneos en diferentes escenarios donde en cada evaluación exista un protocolo de seguridad y observas cuál es de mayor utilidad hoy.

Este estudio adopta un enfoque cuasi experimental que integra elementos cuantitativos y cualitativos para abordar los objetivos específicos establecidos, es primordial proponer mejoras sustanciales para fortalecer la seguridad en entornos de redes inalámbricas, centrándose en una evaluación exhaustiva de vulnerabilidades y en la aplicación de medidas de seguridad específicas para su mitigación.

El proceso de investigación comienza con un análisis detallado de la configuración y estructura actuales de las WLAN, con el propósito de identificar posibles vulnerabilidades y áreas críticas de seguridad, esta fase sienta las bases para la evaluación de riesgos y la determinación de áreas prioritarias que requieren mejoras en la seguridad [36].

Luego, se implementan medidas y protocolos de seguridad específicos, identificados durante el análisis inicial, para contrarrestar las vulnerabilidades detectadas en el entorno WLAN. Estas medidas están diseñadas para abordar de manera efectiva las vulnerabilidades identificadas y mejorar la seguridad global de la red.

El estudio comprende pruebas exhaustivas y evaluaciones de seguridad para verificar la efectividad de medidas implementadas en la protección de la red inalámbrica, estas pruebas involucran análisis cuantitativos y cualitativos para evaluar la eficacia y eficiencia de las medidas de seguridad implementadas.

A partir de los resultados obtenidos en estas pruebas de seguridad, se elaborarán recomendaciones detalladas y mejoras adicionales para fortalecer aún más la seguridad de la WLAN. Estas recomendaciones se centrarán en aspectos técnicos, operativos y estratégicos, con el objetivo de proporcionar una protección más sólida.

Finalmente, se harán pruebas y análisis adicionales para validar las mejoras implementadas, buscando reducir significativamente la probabilidad de amenazas de seguridad y vulnerabilidades en las redes inalámbricas, asegurando un entorno más seguro y estable para las comunicaciones WLAN.

Por otro lado, el alcance es de carácter descriptivo analítico, al implementar el escenario WLAN y el escaneo de vulnerabilidades, permitirá identificarlas y proponer propuestas de mejoras para fortalecer la seguridad, esto incluirá un análisis detallado de la configuración y

estructura actual de las WLAN para identificar posibles riesgos, amenazas y puntos críticos de seguridad.

Se implementarán medidas y protocolos específicos para contrarrestar las vulnerabilidades detectadas, seguidos de pruebas exhaustivas y evaluaciones de seguridad para verificar la efectividad de estas medidas en la protección de la red inalámbrica, las recomendaciones y mejoras adicionales se basarán en los hallazgos de estas pruebas, centradas en fortalecer aún más la seguridad de la WLAN.
La investigación bus validar la eficacia de las mejoras y contramedidas implementadas mediante pruebas y análisis posteriores, asegurando una mayor protección y estabilidad en el entorno de WLAN. El alcance estará delimitado por el análisis específico de ciertos tipos de vulnerabilidades, métodos de evaluación técnica y la identificación de protocolos de seguridad a implementar.

El diseño de la investigación será experimental, en base a toda la investigación que se realiza, mediante practica de todas las propuestas, este enfoque implica la manipulación de una variable independiente, en este caso, las "medidas de control de vulnerabilidades", las cuales se identifican a través de ataques realizados por el sistema operativo wifislax, una distribución de Linux diseñada para auditorías de seguridad. El objetivo es observar cómo estas vulnerabilidades impactan en la seguridad de las WLAN, siendo esta última la variable dependiente en el estudio.

El propósito de este enfoque es proponer mejoras en la seguridad de las WLAN, se implementan diversos protocolos y medidas de seguridad con el fin de analizar su eficacia y determinar las formas más efectivas de proteger las redes inalámbricas.

2.2.2 Metodología o métodos específicos

Metodología OWISAM

Open Wireless Security Assessment Methodology es una metodología para evaluar seguridad inalámbrica abierta, cuenta con el uso de licencias “Creative Commons”, teniendo la ventaja de que toda la comunidad pueda emplear la metodología, modificarla y mejorarla en base a la necesidad. OWISAM define un total de 64 controles que se agrupan en 10 distintas

categorías las cuales especifican pruebas necesarias para garantizar una correcta evaluación de seguridad sobre la infraestructura inalámbrica [37].

Estructura de la metodología (7 fases)

- **Planificación:** Se realiza los pasos antes de un análisis técnico.
- **Recopilación de información:** Análisis de dispositivos (pasivo).
- **Identificación de dispositivos:** Extraer información que sea relevante de la infraestructura de red.
- **Ataques:** identificar las debilidades de los dispositivos Wi-Fi.
- **Acceso a la red:** Analizar e interactuar con la infraestructura.
- **Pruebas sobre normativa y directivas:** Verificar que se cumplan los controles normativos que se presenten.
- **Generación de resultados:** generar informes, analizar la evidencia y clasificar los riesgos.

2.2.3 Herramientas y/o Materiales

Para el desarrollo de la propuesta investigativa es necesario los siguientes materiales:

- **Herramientas de software:**
  - WIFISLAX
- **Material de Hardware:**
  - Laptops
  - Punto de acceso.
  - Dispositivo de red.
  - Dispositivo de red que soporte WPA3.
  - Modulo para WPA3.

2.3 Desarrollo del prototipo

Para el desarrollo del prototipado, en primera instancia se llevó a cabo una revisión bibliográfica para entender el funcionamiento de un entorno WLAN, seguido de una coordinación con las partes interesadas, siguiendo la metodología OWISAM (Open Wireless Security Assessment Methodology), con el fin de delimitar el alcance del proyecto. Este capítulo se enfoca en el diseño detallado de la topología de la red y la creación de una variedad de escenarios representativos de seguridad en redes de área local inalámbricas (WLAN).

Planificación:

En cuanto a la planificación, se deben establecer los pasos previos a la evaluación y análisis técnicos.

1) Establecer la topología o escenario en el cual se va a trabajar.
2) Identificar los dispositivos compatibles con WPA, WPA2 y WPA3.
3) Revisar el manual de Wifislax para una buena práctica y correcta instalación del sistema operativo.
4) Una vez instalado correctamente el SO, se procede a realizar las configuraciones, esto incluye montar los módulos para evaluar y usar herramientas proporcionadas.
5) En base a los diferentes tipos de escenarios se debe realizar un escaneo en la red para identificar las vulnerabilidades, esto según el nivel de seguridad que presente cada escenario.

2.3.1 Topología de red

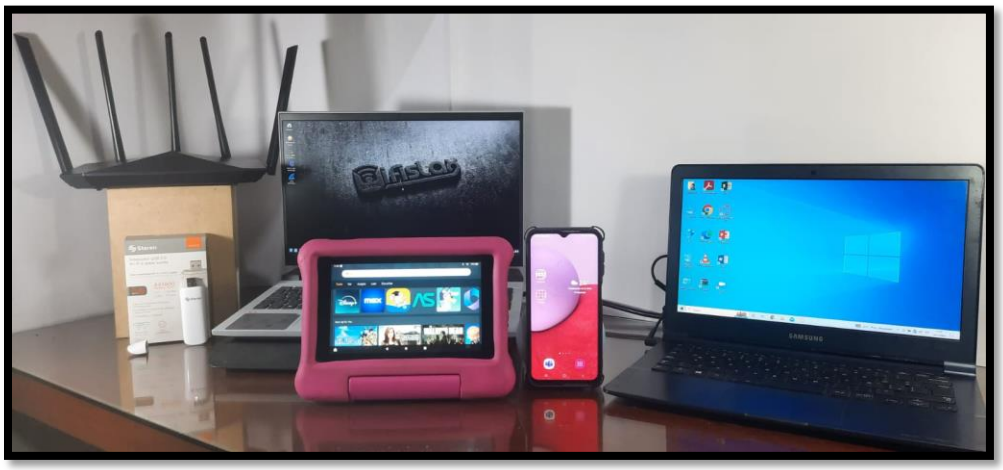


Figura 6: Topología de red / En proceso de Mejora

En la figura 6 se muestra el escenario que se plantea para realizar el escaneo y pruebas de vulnerabilidad, con una maquina principal la cual posee el SO Wifislax siendo la herramienta principal, por otro lado, se necesita un punto de acceso para establecer las conexiones a los diferentes dispositivos a través de WiFi, para este escenario se cuenta con dos portátiles y un celular, estos tendrán las respectivas configuraciones de seguridad en diferentes niveles para realizar los escaneos y con ello detectar vulnerabilidades en base a los niveles de seguridad que mantenga cada dispositivo.

2.4 Ejecución de Prototipo

Siguiendo la topología propuesta, se realizan ajustes específicos tanto en el entorno WLAN como en la herramienta WIFISLAX para optimizar la ejecución de los ataques dirigidos a la red. Estas configuraciones están diseñadas para potenciar la capacidad de detección de vulnerabilidades, lo que resulta crucial para fortalecer la seguridad de la red inalámbrica.
A continuación, se muestra las siguientes tablas con las respectivas configuraciones.

2.4.1 Ataques con protocolo WPA/WPA2

- **Configuraciones para evaluación y uso de la herramienta.**

Tabla 2: Proceso de Configuración de Herramienta

Configuración para evaluación y uso de la herramienta	
Proceso	**Anexo**
1. Primero se muestra que el adaptador está activado en la herramienta WIFISLAX	Ver figura 8
2. Se verifica el comando para colocar el adaptador en modo monitor, para realizar la respectiva auditoria a la red inalámbrica, para evaluar su vulnerabilidad.	Ver figura 9
3. Se muestran todos los dispositivos conectados a la red local.	Ver figura 10

- **Identificación de Dispositivos / Redes**

Tabla 3: Proceso de Identificación de Dispositivos

Proceso de Identificación de Dispositivos / Redes	
Proceso	**Anexo**
1. Se muestran las redes inalámbricas disponibles. Las redes a usar con las rojas y verde. - Verde: Protocolo WPA3 - Rojo: Protocolo WPA2	Ver figura 11
2. Se verifica el listado de direcciones MAC	Ver figura 12

Ataque 1:

Tabla 4: Información Ataque Uno

Procedimiento de Evaluación	**Ataque 1**	**Pag 1**
Nombre del Ataque:	**Ataque de Diccionario**	
Herramienta Utilizada:	**Fern WIFI Cracker**	
Proceso	**Observación**	**Evidencia en anexos**
1. Se visualiza la herramienta Fern WIFI Cracker, esta permite realizar un ataque de diccionario a la red que se seleccione.	La herramienta Fern WIFI Cracker no utiliza comandos, el proceso se puede visualizar en anexos.	Ver figura 13
3. Se realiza el escaneo de redes disponibles con la herramienta mencionada, se observa que solo reconoce a redes que usan el protocolo WPA y WPA2, por lo que no se puede realizar este tipo de ataque a redes que utilicen el protocolo WPA3.		Ver Figura 14
4. Se muestra como a través del ataque tipo diccionario realizado con la herramienta Fern WIFI Cracker se obtiene la contraseña de la red, lo cual demuestra una vulnerabilidad en la red que utiliza el protocolo WPA/WPA2.		Ver Figura 15

Ataque 2:

Tabla 5: Información Ataque Dos

Procedimiento de Evaluación	**Ataque 2**	**Pag 1**
Nombre del ataque:	**Men in the Middle (Hombre en el medio)**	
Herramienta Utilizada:	**Ettercap**	
Proceso	**Observación**	**Evidencia en anexos**
1. Se muestra la herramienta Ettercap la cual permite realizar ataques "men in the middle" o también conocido como "hombre en el medio"	La herramienta Ettercap no utiliza comandos, esta permite colocar en modo monitor para realizar el ataque.	Ver figura 16
2. Se realiza el respectivo escaneo para identificar los dispositivos conectados a la red a la cual se ejecuta el ataque.		Ver Figura 17
3. Una vez realizado el escaneo se obtiene la información de la red luego de ejecutar el ataque "men in the middle".		Ver Figura 18

Ataque 3:

Tabla 6: Información Ataque Tres

Procedimiento de Evaluación	**Ataque 3**	**Pag 1**
Nombre del ataque:	**Desautenticaión**	
Herramienta Utilizada:	**Aircrack-ng**	
Proceso	**Observación**	**Evidencia en anexos**
1. Se realiza un ataque de fuerza bruta a los dispositivos de la red para capturar todos los paquetes que se envían al dispositivo de la red para conectarse.	La herramienta Fern WIFI Cracker no utiliza comandos, el proceso se puede visualizar en anexos.	Ver figura 19
2. Se ejecuta el ataque con la finalidad de obtener el "handshake" lo cual permite que la herramienta "Aircrack-ng" pueda realizar ataques de fuerza bruta o ataque de diccionario hacia la contraseña de la red inalámbrica.		Ver Figura 20
3. Se visualizan los paquetes que se genera al realizar la Desautenticaión de los equipos, el archivo que genera la herramienta, se le coloca el nombre de "testet80-01", la herramienta genera los archivos *cap, .csv, .kismet.csv y .kismet.netxmel.* Esto permite emplear el paquete para adentrarse a la red a la cual se realiza el ataque.		Ver Figura 21

2.4.2 Propuestas de mejoras para protocolo WPA2

Propuesta y recomendaciones de mejoras para implementar al protocolo WPA2

Para mejorar el protocolo WPA2 se implica varios enfoques, desde ajustes hasta implementación de tecnologías.

Tabla 7: Propuestas de mejoras para WPA2

Recomendación	Descripción
1. Actualizaciones de firmware.	Se debe asegurar que los dispositivos que utilizan WP2 deben estar actualizados con los últimos parches de seguridad, permitiendo que se corrijan vulnerabilidades y mejorar la resistencia a ataques.
2. Uso de contraseñas robustas.	Se debe promover el uso de contraseñar largas y complejas para redes WIFI protegidos por WPA2 lo que dificulta los intentos de descifrado con ataques de fuerza bruta.
3. Monitoreo de red/Auditoria de red	Se implementan sistemas para monitorear la red la cual pueda detectar sospechas e intentos de intrusión, al ser continuo permite respuesta más rápido a posibles amenazas.
4. Implementación de Cortafuegos	Un cortafuegos, también conocido como firewall, actúa como una barrera entre tu red privada y el mundo exterior, filtrando el tráfico de datos entrante y saliente según reglas predefinidas.
5. Implementación de WPA3.	Migrar a WPA3 como versión más reciente del protocolo WIFI el cual ofrece mejora en la seguridad, esto incluye protección contra ataques de fuerza bruta y una mayor autentificación.

2.4.3 Ataques con Protocolo WAP3

Tabla 8: Información Ataque 1

Procedimiento de Evaluación	Ataque 1	Pag 1
Nombre del ataque:	**Ataque de Diccionario**	
Herramienta Utilizada:	**Fern WIFI Cracker**	
Proceso	**Observación**	**Evidencia en anexos**
1. Se selecciona el adaptador de red con el cual se realiza el ataque, siendo WLAN 1 MON se procede a detectar las redes que están cerca.	Se detectan seis redes de las cuales ninguna es la red que está bajo el protocolo WPA3	Ver figura 22

Tabla 9: Información Ataque 2

Procedimiento de Evaluación	Ataque 1	Pag 1
Nombre del ataque:	**Men in the Middle**	
Herramienta Utilizada:	**Ettercap**	
Proceso	**Observación**	**Evidencia en anexos**
1. Se muestra la herramienta Ettercap y se realiza ataque "men in the middle" el cual busca receptar los datos que se dan desde un dispositivo a otro.	Se busca receptar datos de un dispositivo a otro.	Ver figura 23
2. Una vez escaneado los dispositivos conectados a la red que posee el protocolo WPA3 se selecciona los dispositivos que se desea verificar el envió de datos de un dispositivo a otro.	Se está dentro del protocolo WPA3 buscando los paquetes que se generen entre dispositivos.	Ver figura 24
3. Luego de realizar el ataque "men in the middle" a la red WPA3 se puede observar cualquier tipo de paquete que se generen entre los dispositivos seleccionados.	Se visualiza paquetes que se generan entre los dispositivos seleccionados.	Ver Figura 25
4. Se escoge un paquete el cual muestra información importante, obteniendo el nombre de usuario y la contraseña encriptado dado que tiene el protocolo HTTP.		Ver Figura 26

Tabla 10: Información Ataque 3:

Procedimiento de Evaluación	**Ataque 1**	**Pag 1**
Nombre del ataque:	**Desautenticaión**	
Herramienta Utilizada:	**Aircrack-ng**	
Proceso	**Observación**	**Evidencia en anexos**
1. Bajo el comando *airodump* se realiza un análisis de las redes que se encuentran cerca del área local.	Se visualiza la red a la cual se realiza ataque, se muestra la señal, ganancia y otros datos adicionales de la misma.	Ver figura 27
2. Utilizando el comando *aireplay-ng –deauth 0 -a 58:D9:D5:8:3E:8C wlan1* Se realiza ataque de desautenticacion al protocolo WPA3 donde se observa los dispositivos conectados a la red y también se visualiza el ataque como tal.	Se espera obtener el handshake donde se espera encontrar la clave de la red, esto no sucede puesto que no puede capturar el handshake, se utiliza el comando *airodump-ng -w testeo80 --bssid 58:D9:D5:8A:3E:8C wlan1.*	Ver figura 28
3. Documentos generados junto con el comando anterior, donde encuentra información para visualizar contraseñas de la red.	Se muestran documentos generados.	Ver Figura 29
4. No se logra capturar handshake, por lo tanto, no se puede obtener la contraseña de internet.	No se obtiene contraseña.	Ver Figura 30

2.4.4 Propuestas de mejoras para protocolo WPA3

Propuesta y recomendaciones de mejoras para implementar al protocolo WPA3

Para mejorar el protocolo WPA3 se implica varios enfoques, desde ajustes hasta implementación de tecnologías.

Tabla 11: Propuestas de mejoras para WPA3

Recomendación	Descripción
1. Configurar una red de invitados	Configurar una red de invitados separada, mantiene que la red principal sea más segura, aislando los dispositivos de invitados.
2. Habilitar el Filtrado de Direcciones MAC.	Configurar el router para permitir solo dispositivos específicos a través de sus direcciones MAC.
3. Protocolo WPA3.	Migrar a WPA3 como versión más reciente del protocolo WIFI el cual ofrece mejora en la seguridad, esto incluye protección contra ataques de fuerza bruta y una mayor autentificación.

CAPITULO III. EVALUACION DEL PROTOTIPO

3.1 Plan de Evaluación

3.1.1 Objetivo.

Valorar los resultados en base a la evaluación de vulnerabilidades mediante la ejecución de ataques utilizando la herramienta WIFISLAX, implicando una comparativa entre los protocolos se seguridad y proponer mejoras para fortalecer la red.

3.1.2 Cronograma.

Cronograma de Actividades

	JUNIO		JULIO		
	Semana 10	Semana 11	Semana 12	Semana 13	Semana 14
Análisis de informes preliminares					
Elaboración de escenarios de prueba					
Estudio de herramientas					
Realización de Ataques					
Comparación de protocolos de seguridad					
Elaboración de recomendaciones					
Generación de informe final.					
Presentación conclusiones y recomendaciones					

3.1.3 Diseño de escenarios de prueba

Se cuenta con dos portátiles y un dispositivo móvil que configuran seguridad para escanear y detectar vulnerabilidades según los niveles de seguridad.

3.1.4 Recopilación de Información.

Para determinar un porcentaje que represente el nivel de seguridad se lleva a cabo una investigación sobre los ataques de mayor frecuencia a la red, dicha investigación proporciona una base sólida para comparar el impacto que tiene las mejoras que se implementan (Ver Capítulo I). Primero se identifican los tipos de ataques más comunes y luego se proponen mejoras para ser implementadas en la red, seguido se repiten los ataques originales para evaluar si las mejoras reducen de forma efectiva las vulnerabilidades identificadas (Ver

Capítulo II). Este enfoque permite establecer un marco objetivo para medir con éxito las propuestas de mejoras para la seguridad de WLANS.

3.1.5 Análisis de datos y propuestas de mejoras.

Utilizar la herramienta WIFISLAX para identificar vulnerabilidades y luego establecer las propuestas de mejoras incluyen el escenario donde se generan los ataques de red, de esta manera realizar la comparación.

3.1.6 Comparación y evaluación

Comparar resultados en base a las mejoras que se proponen, su porcentaje e identificar las diferencias significativas que comprueben el nivel de seguridad en la red.

3.1.7 Generación de Informe.

Documentar los hallazgos en informe lo cual incluya los resultados de la evaluación para comparar el nivel de seguridad una vez implementadas las propuestas de mejoras junto a las recomendaciones más relevantes.

3.1.8 Resultados de Evaluación

Implementación de propuestas para mejorar la seguridad del protocolo WPA2 y WPA3.
Según las recomendaciones planteadas, se aplican estas para verificar su funcionalidad y cantidad porcentual de cumplimiento para mejorar la seguridad de la red WLAN.

3.1.9 Aplicación de mejoras / Generación de Ataques WPA2.

Tabla 12: Ataques por 2da Vez a protocolo WPA2

Ataque	Observación	Anexo
Ferwificracker WPA2	Si se implementa una contraseña robusta, esta puede ser detectada por la herramienta, dependiendo del diccionario que se emplee, caso contrario muestra error.	Ver Figura 39

Ataque	Observación	Anexo
Ettercap WPA2	Se muestran los paquetes que se envían por la red, no se mostró mejoría de seguridad, al aplicar las mejoras.	Ver Figura 40
Aircrack WPA2	Existe una demora al detectar los dispositivos de la red, al igual que la contraseña, sin embargo, el ataque logra implementarse.	Ver Figura 41

3.1.10 Aplicación de mejoras / Generación de Ataques WPA3

Tabla 13: Ataques a protocolo WPA3 por segunda vez

Ataque	Observación	Anexo
Ferwificracker WPA3	No se puede realizar el ataque ya que la herramienta no reconoce redes con el protocolo WPA3.	Ver Figura 42
Ettercap WPA3	Se tarda en reconocer los dispositivos en la red, sin embargo, el ataque puede realizarse.	Ver Figura 43
Aircrack WPA3	No se puede realizar el ataque, al hacer el análisis de la red se dificulta ya que esta se muestra por ocasiones.	Ver Figura 44

Para llevar a cabo una evaluación comparativa del nivel de mejora en la seguridad de los protocolos se establece una escala de Likert, misma que permite medir en base a una serie de preguntas la efectividad de cada mejora implementada en los protocolos.

Escala de Likert:

1. Muy ineficaz (si el ataque no se realiza después de las 72 horas)
2. Ineficaz (si el ataque se realiza entre 48 y 72 horas)
3. Moderadamente eficaz (si el ataque se realiza entre 24 y 48 horas)
4. Eficaz (si el ataque se realiza alrededor de las 24 horas)
5. Muy eficaz (si el ataque se realiza justo antes de las 24 horas)

Declaración a evaluar Uno: "El diccionario utilizado para el primer ataque al protocolo de seguridad fue eficaz dentro del límite de 72 horas."

Interpretación:

- **Puntuación 1 y 2**: Indican que el diccionario fue poco efectivo.
- **Puntuación 3 y 4:** Indican que el diccionario fue relativamente efectivo.
- **Puntuación 5:** Indica que el diccionario fue muy efectivo, alcanzando su máximo potencial justo antes del límite de 72 horas.

Declaración a evaluar Dos: "Evalúe la efectividad del ataque man-in-the-middle realizado con la herramienta ettercap para encontrar envíos de paquetes a través de la red dentro del límite de 72 horas."

Interpretación:

- **Puntuación 1 y 2:** Indican que el ataque man-in-the-middle realizado con ettercap fue poco efectivo en encontrar envíos de paquetes.
- **Puntuación 3 y 4:** Indican que el ataque man-in-the-middle realizado con ettercap fue relativamente efectivo en encontrar envíos de paquetes.
- **Puntuación 5:** Indica que el ataque man-in-the-middle realizado con ettercap fue muy efectivo, alcanzando su máximo potencial justo antes del límite de 72 horas.

Declaración a evaluar Tres: "Evalúe la efectividad del ataque de desautenticación utilizando la herramienta aircrack para encontrar información de la red como contraseñas y envío de paquetes dentro del límite de 72 horas."

Interpretación:

- **Puntuación 1 y 2:** Indican que el ataque de desautenticación utilizando aircrack fue poco efectivo en encontrar información de la red como contraseñas y envío de paquetes.

- **Puntuación 3 y 4:** Indican que el ataque de desautenticación utilizando aircrack fue relativamente efectivo en encontrar información de la red como contraseñas y envío de paquetes.
- **Puntuación 5:** Indica que el ataque de desautenticación utilizando aircrack fue muy efectivo, alcanzando su máximo potencial justo antes del límite de 72 horas en encontrar información de la red como contraseñas y envío de paquetes.

3.1.11 Nivel de mejora de seguridad en base a propuestas de mejoras aplicadas para WPA2

Los resultados que se obtienen luego de aplicar los ataques por segunda vez con los controles implementados son:

Tabla 14: Resultados en base a escala de Likert

Ataque	Observación	Puntuación
Diccionario	El uso de contraseña robusta al igual que otras mejoras permite que exista menos posibilidad de encontrar la misma a través de un diccionario, sin embargo, utilizando el diccionario seleccionado el ataque puede ejecutarse en 8 horas.	5
Men in the Middle	A diferencia del primer intento de ataque en esta muestra mejoras significativas, ya que se necesita hasta de 30 horas para que pueda ser ejecutado el ataque.	3
Desautenticación	El ataque intenta de forma constante desautentificar los dispositivos a la red compromete la seguridad de la red, buscando obtener el handshake, no obstante, el tiempo que toma en realizar dicho ataque luego de implementar controles es de hasta 32 horas.	3

Fuente: Elaboración Propia

Una vez obtenido los resultados de evaluación se genera una escala porcentual la cual permite evaluar el nivel de efectividad de cada propuesta de mejora para el protocolo de seguridad.

Tabla 15: Alcance de Recomendaciones para Protocolo WPA2

Recomendación	Descripción	Alcance
1. Actualizaciones de firmware.	Se debe asegurar que los dispositivos que utilizan WP2 deben estar actualizados con los últimos parches de seguridad, permitiendo que se corrijan vulnerabilidades y mejorar la resistencia a ataques.	5%
2. Uso de contraseñas robustas.	Se debe promover el uso de contraseñas largas y complejas para redes WIFI protegidos por WPA2 lo que dificulta los intentos de descifrado con ataques de fuerza bruta.	20%
3. Monitoreo de red/Auditoria de red	Se implementan sistemas para monitorear la red la cual pueda detectar sospechas e intentos de intrusión, al ser continuo permite respuesta más rápido a posibles amenazas.	5%
4. Implementación de Cortafuegos	Un cortafuegos, también conocido como firewall, actúa como una barrera entre tu red privada y el mundo exterior, filtrando el tráfico de datos entrante y saliente según reglas predefinidas.	10%
5. Implementación de WPA3.	Migrar a WPA3 como versión más reciente del protocolo WIFI el cual ofrece mejora en la seguridad, esto incluye protección contra ataques de fuerza bruta y una mayor autentificación.	60%

Fuente: Elaboración Propia

1. **Actualización de Firmware**

Tabla 16: Mejora Uno

Detalle	Porcentaje Esperado	Porcentaje de Cumplimiento	Anexo
Se verifica que el Firmware sea correctamente actualizado, cumpliendo con el 5% del nivel de mejora en la seguridad de la red	5%	5%	Ver Figura 31

Fuente: Elaboración Propia

Se llevan a cabo los ataques con mejoras implementadas. Sin embargo, la efectividad de la actualización del Firmware es solo del 5%, lo que significa que no proporciona una seguridad completa para el protocolo WPA2, pero mantiene siempre actualizado a los dispositivos.

2. **Contraseñas Robustas**

Tabla 17: Mejora Dos

Detalle	Porcentaje Esperado	Porcentaje de Cumplimiento	Anexo
Se verifica uso de contraseña robusta cumpliendo con el 20% de mejora de seguridad en la red WLAN.	20%	15%	Ver Figura 32

Fuente: Elaboración Propia

El uso de contraseñas robustas incrementa significativamente la seguridad contra intentos de descifrado de contraseñas, alcanzando un nivel de seguridad del 15% para el protocolo WPA2.

3. **Monitoreo de Red / Auditoria de Red**

Tabla 18: Mejora Tres

Detalle	Porcentaje Esperado	Porcentaje de Cumplimiento	Anexo
Se realiza el respectivo monitoreo de la red, verificando el cumplimiento del 5% de mejora de seguridad en la red.	5%	5%	Ver Figura 33

Fuente: Elaboración Propia

El monitoreo constante de la red ayuda a prevenir y detectar posibles vulnerabilidades a tiempo, mejorando la efectividad hasta un 5% en la defensa contra ataques al protocolo WPA2.

4. **Implementación de Cortafuegos**

Tabla 19: Mejora Cuatro

Detalle	Porcentaje Esperado	Porcentaje de Cumplimiento	Anexo
Se realiza la implementación de un cortafuegos verificando el cumplimiento en la seguridad de la red.	10%	5%	Ver Figura 34

Fuente: Elaboración Propia

La implementación de cortafuegos no garantiza un alto nivel de seguridad debido a que está más orientada a proteger contra ataques de inundación como ICMP y TCP, los cuales no están directamente relacionados con el protocolo WPA2.

5. **Implementación de WPA3**

Tabla 20: Mejora Cinco

Detalle	Porcentaje Esperado	Porcentaje de Cumplimiento	Anexo
Se implementa como mejora principal el uso del protocolo se seguridad WPA3 el cual brinda el mayor porcentaje de mejora en la seguridad de la red.	60%	60%	Ver Figura 35

Fuente: Elaboración Propia

La implementación del protocolo WPA3 en dispositivos ofrece un nivel de seguridad avanzado por sí mismo, gracias a sus mejoras significativas en comparación con el WPA2 mejorando por si solo en un 60% a la seguridad de la misma.

3.1.12 Nivel de mejora de seguridad en base a propuestas de mejoras aplicadas para WPA3

Tabla 21: Resultados en base a escala de Likert

Ataque	Observación	Puntuación
Diccionario	No es posible realizar el ataque ya que herramientas como ferwificracker no reconoce dispositivos con el protocolo WPA3.	1
Men in the Middle	El uso de contraseña robusta al igual que otras mejoras permite que exista menos posibilidad de encontrar la misma a través de un diccionario, sin embargo, el ataque puede ejecutarse dependiendo del nivel de seguridad.	2
Desautenticación	No es posible realizar el ataque ya que herramientas como ferwificracker no reconoce dispositivos con el protocolo WPA3.	1

Fuente: Elaboración Propia

Propuestas de mejoras y su nivel de porcentaje para mejorar la red con protocolo WPA3.

Tabla 22: Alcance de Mejorar para Protocolo WPA3.

Recomendación	Descripción	Alcance
1. **Configurar una red de invitados.**	Configurar una red de invitados separada, manteniendo a la red principal sea más segura, aislando los dispositivos de invitados.	10%
2. **Habilitar el filtrado de direcciones MAC.**	Configurar el router para permitir solo dispositivos específicos a través de sus direcciones MAC..	30%
3. **Protocolo WPA3.**	Se mantiene el uso de Protocolo WPA3.	60%

Fuente: Elaboración Propia

1. **Configurar una red de invitados**

Tabla 23: Mejora Uno

Detalle	Porcentaje Esperado	Porcentaje de Cumplimiento	Anexo
Se configura una red de invitados que evite acceso a la red principal de dispositivos seleccionados, garantizando un 10% de mejora en la seguridad de la misma.	10%	10%	Ver Figura 36

Fuente: Elaboración Propia

La implementación de una red de invitados mejora la seguridad al separar claramente el tráfico entre usuarios empresariales y visitantes. Esto ayuda a proteger la red principal al limitar el acceso de los usuarios no autorizados a recursos sensibles.

2. **Habilitar el filtrado de direcciones MAC.**

Tabla 24: Mejora Dos

Detalle	Porcentaje Esperado	Porcentaje de Cumplimiento	Anexo
Se realiza un filtrado de direcciones MAC para negar acceso a dispositivos a la red, buscando cumplir con una mejora de 30% en la misma.	30%	20%	Ver Figura 37

Fuente: Elaboración Propia

Esta mejora depende de la configuración específica del router. Por ejemplo, el modelo Steren AX1500 permite crear una lista negra de dispositivos, lo cual permite seleccionar qué dispositivos no pueden conectarse a la red. Sin embargo, esta medida no garantiza una seguridad total, ya que no es posible predecir desde qué dispositivo podrían originarse o ser dirigidos ataques a la red.

3. Protocolo WAP3.

Tabla 25: Mejora Tres

Detalle	Porcentaje Esperado	Porcentaje de Cumplimiento	Anexo
Se implementa como mejora principal el uso del protocolo se seguridad WPA3 el cual brinda el mayor porcentaje de mejora en la seguridad de la red.	60%	60%	Ver Figura 38

Fuente: Elaboración Propia

La introducción del protocolo WPA3 en dispositivos proporciona un nivel de seguridad notablemente superior debido a sus mejoras significativas respecto al WPA2, lo que incrementa la seguridad en un 60% por sí mismo.

Como conclusión de la evaluación de prototipo, se puede determinar que la hipótesis plateada "La implementación de controles de seguridad en entornos WLAN asegura la protección en un 80% mediante el uso de protocolos contra ataques a redes inalámbricas." Se cumple, puesto al implementar medidas de control en cada uno de los protocolos, se concreta una mejora en el nivel de seguridad de la red WLAN.

CONCLUSIONES

- La revisión sistemática de la literatura proporcionó una comprensión del estado actual del conocimiento y las propuestas formuladas por otros autores en relación con el tema de investigación planteado.
- El entorno físico WLAN implementado proporciona un escenario propicio para la efectiva ejecución de la herramienta WIFISLAX, permitiendo así la evaluación de vulnerabilidades en la red.
- Durante esta evaluación, a través de la herramienta WIFISLAX, se realizaron exitosamente diversos ataques de seguridad, revelando vulnerabilidades significativas en los protocolos de seguridad empleados.
- Se llevó a cabo la investigación de protocolos de seguridad, enfocándose en WPA2 y WPA3. Para el primer protocolo WPA2 presenta varias vulnerabilidades, el uso de fernwificracker a través de un diccionario genera la clave de usuario, al igual que la herramienta ettercap y aircrack-ng, destacando la necesidad de medidas adicionales para brindar mayor protección a la integridad de la información. La aplicación de mejoras como uso de contraseñas robustas, actualización de firmware, aumentan significativamente la seguridad de la red.
- Al evaluar los niveles de seguridad El protocolo WPA3 se caracteriza por la capacidad para resistir ataques los cuales están dirigidos contra redes WLAN en entorno tanto empresariales como no empresariales, mejorando de manera significativa la seguridad proporcionando una experiencia fiable para el usuario quien busca proteger sus datos y la privacidad en línea.

RECOMENDACIONES

- Es importante que se mantenga constante actualización sobre la información acerca del estado de conocimiento sobre los diferentes ataques a la red, debido al constante aumento de amenazas que puede presentar una red, es recomendable actualizar la revisión literaria sobre el tema.
- Es recomendable implementar un entorno WLAN con mayor número de dispositivos, por ejemplo, un servidor, lo cual permite que se realice una auditoría más eficaz, obteniendo mayor número de posibles vulnerabilidades a evaluar, al igual que el uso de un adaptador específico para este tipo de trabajo puesto que a pesar de utilizar un COM-8235 este requiere de instalación de algunos drivers para su funcionamiento.
- El uso de la herramienta WIFISLAX otorga un gran número de herramientas para realizar escaneo de red y con ello detectar vulnerabilidades, sin embargo, es importante que se utilice otro tipo de herramienta dependiendo del nivel de auditoría que se realice.
- Es necesario implementar varias mejoras al protocolo WPA2, ya que presenta un gran número de vulnerabilidades. Las mejoras propuestas proporcionan una base sólida para aumentar la seguridad de manera efectiva, considerando que se pueden aplicar defensas más avanzadas para este protocolo de seguridad.
- Es recomendable migrar al protocolo de seguridad WPA3 debido a su alto nivel de seguridad, lo cual es especialmente adecuado para entornos con alto tráfico de información. Esta migración garantiza una protección robusta de la red, aumentando la confianza en la seguridad de los datos transmitidos y almacenados.

vii. ELEMENTOS ADMINISTRATIVOS

4.1. Cronograma

Tabla 26: Cronograma de actividades

Nombre actividad	Fecha inicio	Duración en días	Fecha fin
Selección de tema	17-nov	7	24-nov
Planteamiento de Problema	24-nov	3	27-nov
Campo de Estudio	27-nov	2	29-nov
Objetivos	29-nov	9	8-dic
Hipótesis y Variables	29-nov	9	8-dic
Estado del Arte	9-dic	11	20-dic
Proceso de búsqueda	9-dic	11	20-dic
Metodología	20-dic	6	26-dic
Método Especifico	27-dic	6	2-ene
Propuesta	2-ene	3	5-ene
Resultado de Propuesta	5-ene	4	9-ene
Corrección 1 en base a sugerencias	22-ene	5	27-ene
Investigación de dispositivos a utilizar	22-ene	2	24-ene
Definición de Prototipo	23-ene	3	26-ene
Adquisición de dispositivos	25-ene	1	26-ene

Tabla 2: Cronograma de actividades

Nombre actividad	Fecha inicio	Duración en días	Fecha fin
Aplicación de Metodología	31-ene	30	1-mar
Estudio herramienta de evaluación	31-ene	7	7-feb
Diseño de escenario, entorno WLAN	6-feb	3	9-feb
Identificación de ataques	6-feb	3	9-feb
Aplicación de evaluación	8-feb	10	18-feb
Aplicación de ataques	10-feb	20	1-mar
Identificar las vulnerabilidades y fallas en la red	15-mar	45	29-abr
Indagar propuestas de mejora	1-may	10	11-may
Aplicar propuestas de mejora	15-may	30	14-jun
Evaluar las mejoras implementadas	17-jun	10	27-jun
Comparar niveles de seguridad en base a las mejoras	1-jul	10	11-jul

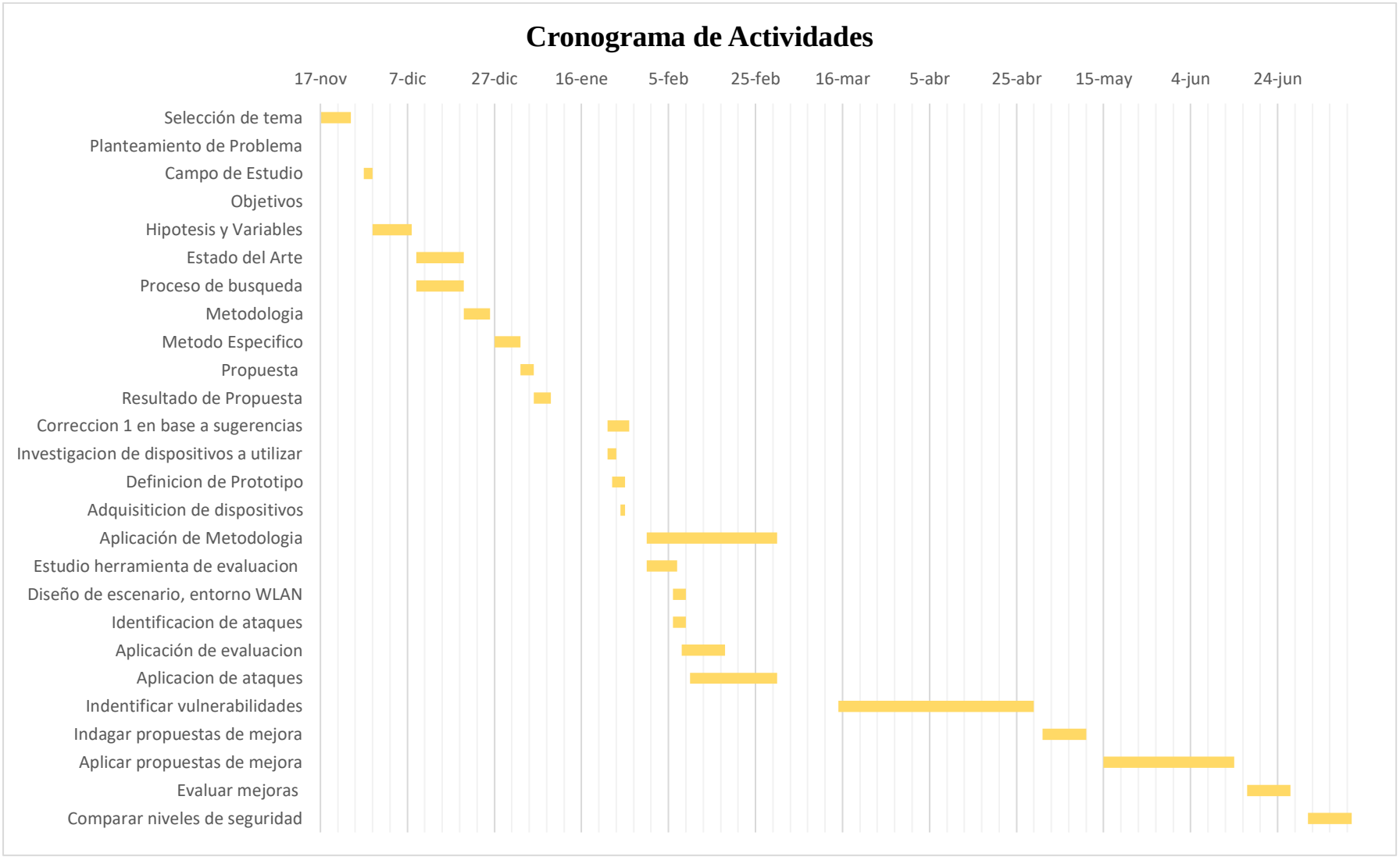


Figura 7: Diagrama de Cronograma

4.2. Presupuesto

Tabla 27: Presupuesto

Tipo/Concepto	Cantidad	Unid. Med.	P. Unitario ($)	Total ($)
Sistema Operativo - Linux (WIFISLAX)	-	Horas	$0.00	$0.00
Hardware				
- Laptop (8 gb ram. 455 ssd, amd ryzen)	500	Horas de uso	$0.35	$175.00
- Laptop (16 gb ram, 455 ssd, i511va)	500	Horas de uso	$0.35	$175.00
- Laptop (8 gb ram, 455 ssd, i35ta)	500	Horas de uso	$0.35	$175.00
- Punto de acceso	1	Monetario	$21.00	$21.00
- Celular smartphone.	1	Horas de uso	$0.00	$0.00
- Adaptador usb	1	Monetario	$30.00	$30.00
- Router WPA3	1	Monetario	$93.00	$93.00
Personal				
- Estudiante de TI 1	500	Horas de Uso	$2.00	$1000.00
- Estudiante de TI 2	500	Horas de Uso	$2.00	$1000.00
Servicio Virtual				
- Internet	2	Mensual	$30.00	$30.00
Total, costos				**$2699.00**
Costos indirectos – imprevistos	**10%**			$269.00
			Total	**$2968.00**

viii. REFERENCIAS BIBLIOGRÁFICAS

Bibliografía

[1] K. Murugesan, S. Sriram y K. Kumar, «Closed WiFi Hotspot - Truly Hidden Network,» *IEEE International Conference on Consumer Electronics (ICCE),* pp. 1-06, 2023.

[2] M. Cortez Vazquez, «Mitigacion de vulnerabilidades en una WLAN con la implementavcion de hardening.,» Mexico, 2018.

[3] J. Borreno Neninger y J. Ponce Guerrero, «Impacto en la seguridad de las redes inalámbricas,» Manabi, 2023.

[4] D. Zhang y J. Song Dong, «Assessing certificate validation user interfaces of WPA supplicants,» *ACM Digital Library,* pp. 501-513, 2022.

[5] M. Natkaniec y M. Bednarz, «Wireless Local Area Networks Threat Detection Using 1D-CNN,» *Sensors,* vol. 23, nº 12, 2023.

[6] Movistar, «Movistar,» 02 2023. [En línea]. Available: https://www.movistar.es/blog/amplificador-smart-wifi/protocolo-wpa3/#:~:text=WPA3%20vs%20WPA2,sistema%20de%20seguridad%20más%20resistente.. [Último acceso: 14 12 2023].

[7] Cisco, «Cisco,» 02 12 2023. [En línea]. Available: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/wpa3-dep-guide-og.html. [Último acceso: 14 12 2023].

[8] M. Suing Ochoa y A. Pardo Sanchez, «Estudio de vulnerabilidades en el sistema de seguridad WPA-2 Personal del estándar IEEE 802.11i y propuestas de mejoras a considerar en el sistema WPA-3.,» Loja, 2022.

[9] M. Dasari, «Real time detection of MAC layer DoS attacks in IEEE 802.11 wireless networks,» *IEEE Annual Consumer Communications & Networking Conference (CCNC),* pp. 939-944, 2017.

[10] CISCO y Stephen Fallas, «Blog Cisco Latinoamerica,» 25 04 2018. [En línea]. Available: https://gblogs.cisco.com/la/sg-stfallas-lo-mas-destacado-del-reporte-de-ciberseguridad-cisco-2018/. [Último acceso: 22 12 2023].

[11] L. F. Dominguez Vega, «Montaje y control de una red Wi-Fi® asegurada a nivel empresarial con WPA2-Enterprise,» *Revista Cubana de Ciencias Informáticas,* vol. 12, nº 1, pp. 58-73, 2018.

[12] X. Sun, Z. Ye , L. Bo, X. Wu y Y. Wei, «Automatic software vulnerability assessment by extracting vulnerability elements,» *Journal of Systems and Software,* vol. 204, 2023.

[13] A. Hussein, Z. Saeed y F. Yasein, «A New Method for Ensuring the Integrity in Wireless LAN (WiFi),» *nternational Conference for Natural and Applied Sciences (ICNAS),* pp. 1-4, 2022.

[14] J. C. Borrero Neninger y J. L. Ponce Guerrero, «Impacto en la seguridad de las redes inalambricas,» *Techinnovation,* vol. 2, nº 1, pp. 62-71, 2023.

[15] I. A. Coronel Suarez y D. I. Quirumaby Yagual, «Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web,» *Revista Científica y Tecnológica UPSE,* vol. 9, nº 2, pp. 91-109, 2022.

[16] J. I. Castillo Velazquez, M. Alcala Garcia y D. J. Serrano Martinez, «Hardening as a best practice for WLAN Security Meanwhile WPA3 is released,» *IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX)*, pp. 1-5, 2019.

[17] P. Alvarado Medellin, S. Aguilar Escarcia y A. Ramirez Aguilar , «Sistema dinámico para el monitoreo y control de redes inalámbricas de sensores que operan bajo el protocolo de comunicación ZigBee,» *Ingeniería, investigación y tecnología,* vol. 20, nº 1, 2019.

[18] S. Wail Nourildean, M. Yousra y H. Ali Attallah, «Virtual Local Area Network Performance Improvement Using Ad Hoc Routing Protocols in a Wireless Network,» *Computers,* vol. 12, nº 2, 2023.

[19] P. E. Godoy Trujillo y L. A. Caiza Quishpe, «Características y ventajas existentes en la conexión inalámbrica y fibra óptica. Una revisión bibliográfica.,» *Journal Of Engineering Sciences,* vol. 4, nº 9, pp. 14-25, 2022.

[20] R. Nazir y A. Ali , «Survey on Wireless Network Security,» *ARCHIVES OF COMPUTATIONAL METHODS IN ENGINEERING,* vol. 29, pp. 1591-1610, 2022.

[21] D.-Y. Hwang, K. Yeon y J. Gyun, «CAN Security Protocol Using Modified MAC,» *International SoC Design Conference,* pp. 308-309, 2020.

[22] D. S. Pacheco, «Seguridad en redes de comunicaciones: Perspectivas y desafíos.,» *Revista chilena de ingeniería,,* vol. 30, nº 2, pp. 215-217, 2022.

[23] E. Baray y N. Kumar, «WLAN Security Protocols and WPA3 Security Approach Measurement Through Aircrack-ng Technique,» *th International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 23-30, 2021.

[24] B. Ahmed y Hatim Alsuwat, «5th Generation Wireless Networks Security: Challenges and Solutions,» *International Journal of Computer Science and Network Security,* vol. 22, nº 6, pp. 157-162, 2022.

[25] A. Kejiou y G. Bekaroo, «A Review and Comparative Analysis of Vulnerability Scanning Tools for Wireless LANs,» *3rd International Conference on Next Generation Computing Applications (NextComp)*, pp. 1-6, octubre 2022.

[26] A. Halbouni, L.-Y. Ong y M.-C. Leow, «Wireless Security Protocolos WPA3: A Systematic Literature Review,» *IEEE Xplore,* vol. 11, pp. 112438-112450, 2023.

[27] J. Marquez Diaz, «Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas.,» *Revista de Bioética y Derecho,* nº 46, pp. 85-100, 2019.

[28] D. G. IONOS, «IONOS,» 23 Agosto 2023. [En línea]. Available: https://www.ionos.es/digitalguide/servidores/configuracion/kali-linux/. [Último acceso: 26 Diciembre 2023].

[29] A. Yacchirema y D. Aulema , «Análisis de los Sistemas de Ataque y Protección en redes inalámbricas Wi Fi, bajo el Sistema Operativo Linux,» Universidad de las Fuerzas Armadas, Quito, 2021.

[30] R. Chango Saavedra y D. Gualpa Sarabia, «IMPLEMENTACIÓN DE PRUEBAS DE HACKEO ÉTICO PARA EVALUAR EL SISTEMA DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RHELEC,» Universidad Politecnica Salesiana, Cuenca, 2023.

[31] J. E. Sanchez, «SISTEMA DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RHELEC,» Universidad Politecnica de Madrid, Madrid, 20121.

[32] M. Echeverria, M. Garaycoa y A. Tusev, «ARE ECUADORIAN MILLENNIALS PREPARED AGAINST A CYBERATTACK?,» *Revista Chakiñan*, vol. 1, nº 10, pp. 73-86, 2020.

[33] D. F. Vasconez Acuña, «Red inalambrica tipo malla estandar 802.11 de transmision y la optimizacion de cobertura en los colegios de la provincia de Tunguragua.,» Universidad Tecnica de Ambato, Ambato, 2014.

[34] M. Virrarreal y J. Arroyo, «Evaluación de una red inalámbrica de banda ancha para VoIP,» *Enfoque UTE*, vol. 10, nº 4, pp. 28-44, 2019.

[35] A. Alahmadi, M. Aljabri, D. Alharthi y G. Rayani, «DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions,» *Electronics*, vol. 12, nº 14, 2023.

[36] H. R. Gonzalez Brito y R. Montesino Perurena, «Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web.,» *Revista Cubana de Ciencias Informáticas*, vol. 12, nº 4, pp. 52-65, 2018.

[37] OSIWAM, «OSIWAM,» 2024. [En línea]. Available: https://osiwan.com/about-us-two/. [Último acceso: 3 enero 2024].

Anexos

- **Proceso de Configuración de Herramienta**

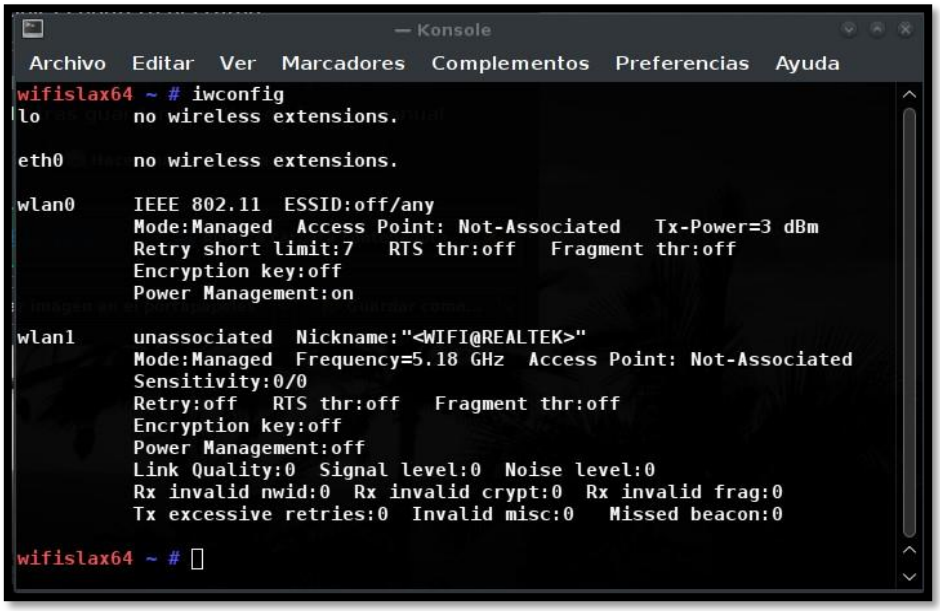


Figura 8: Estado del Adaptador de Red

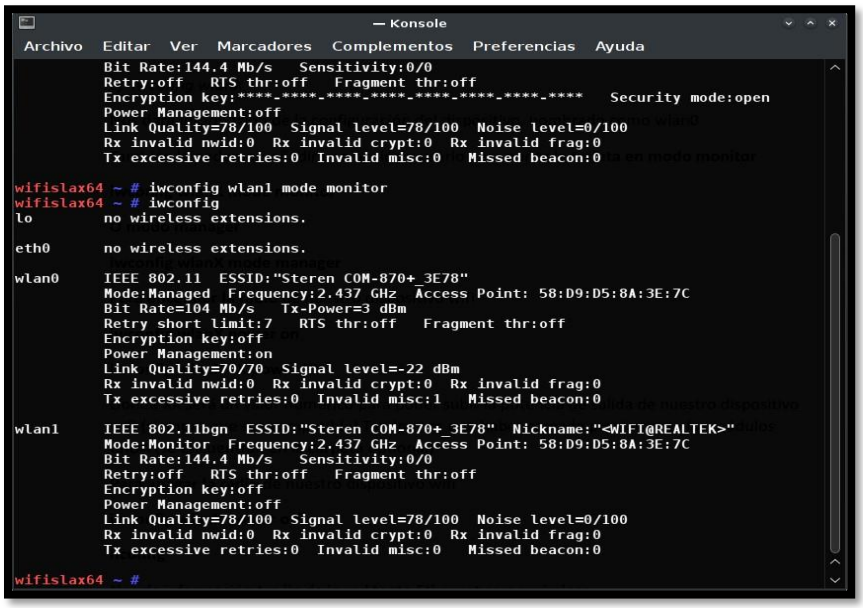


Figura 9: Adaptador en modo Monitor

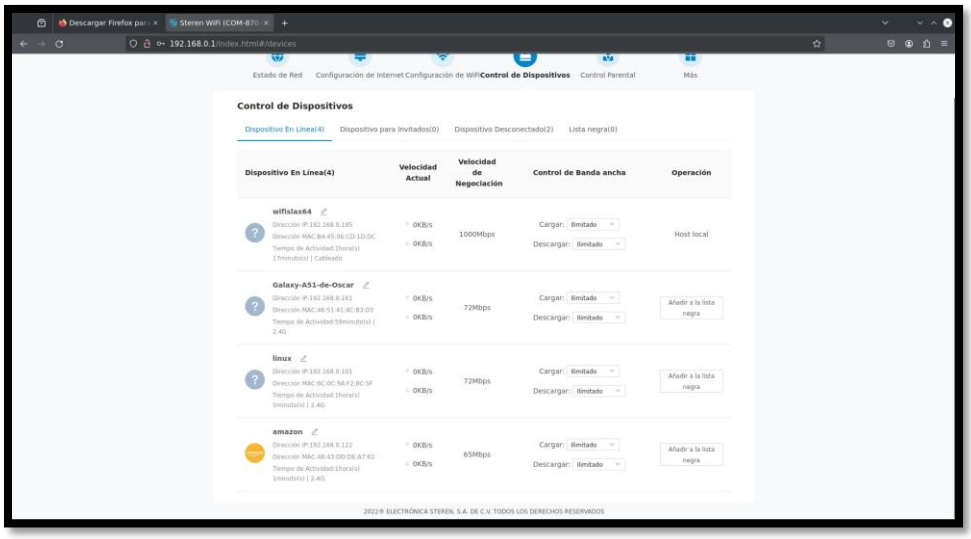
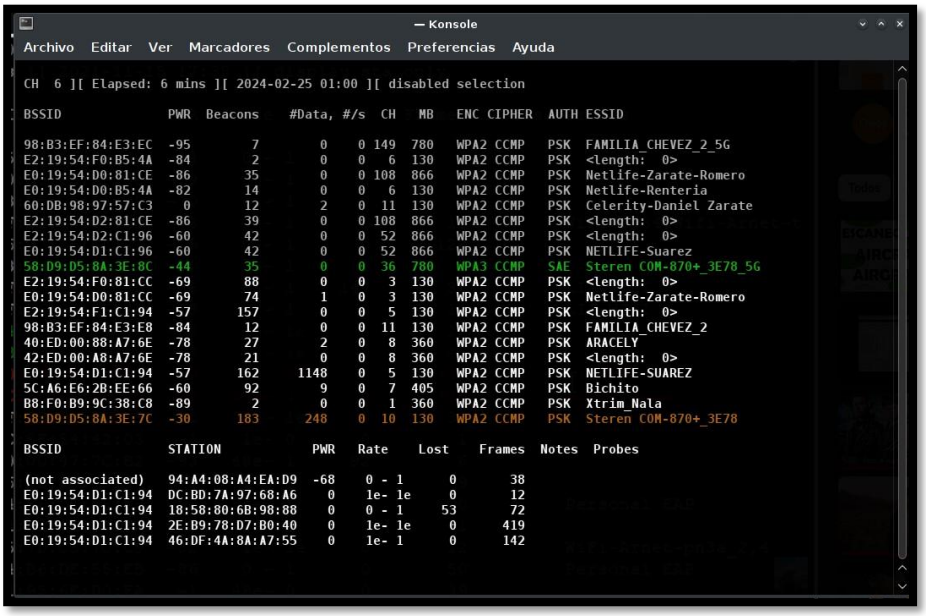


Figura 10: Dispositivos Conectados

- **Proceso de Identificación de Dispositivos**



S

Figura 11: Redes Inalámbricas

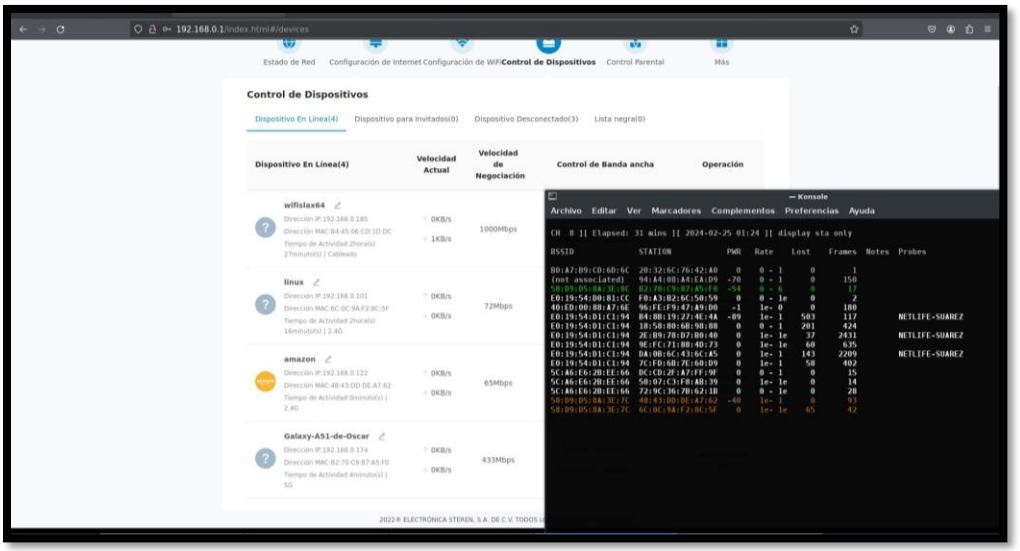


Figura 12: Listados de Direcciones MAC

- **Ataques**

Ataque Uno – Ataque de Disccionario

Figura 13: Ataque de Diccionario

.

Figura 14: Escaneo de Redes Disponibles.

Figura 15: Se muestra password de la red "Sterem COM-B70+_3E78"

Ataque 2

Ataque “Men in the Middle”

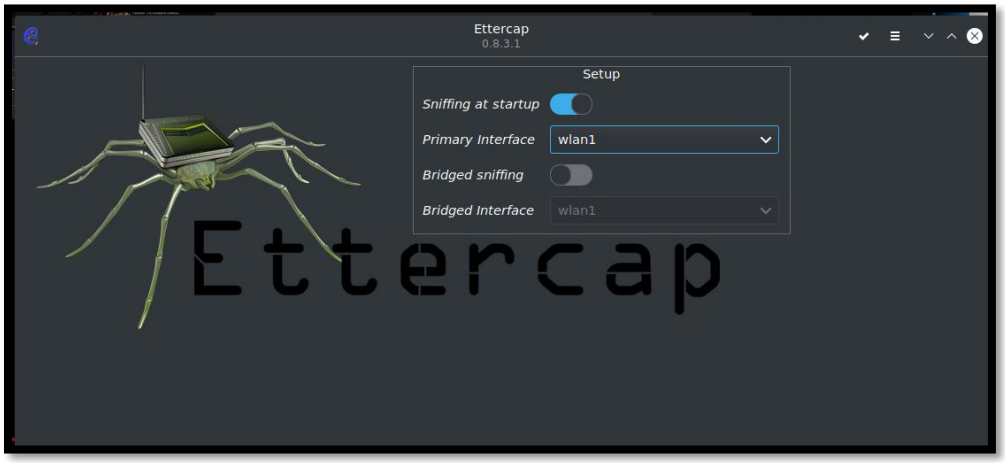


Figura 16: Ataque a través de la herramienta "Ettercap"

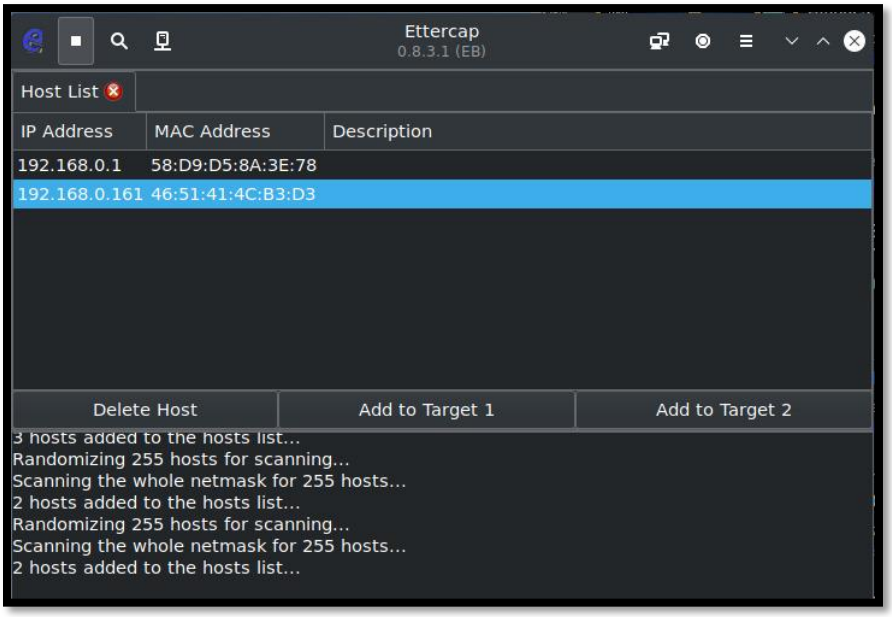


Figura 17: Escaneo de los dispositivos conectados a la red a la cual se realiza el ataque

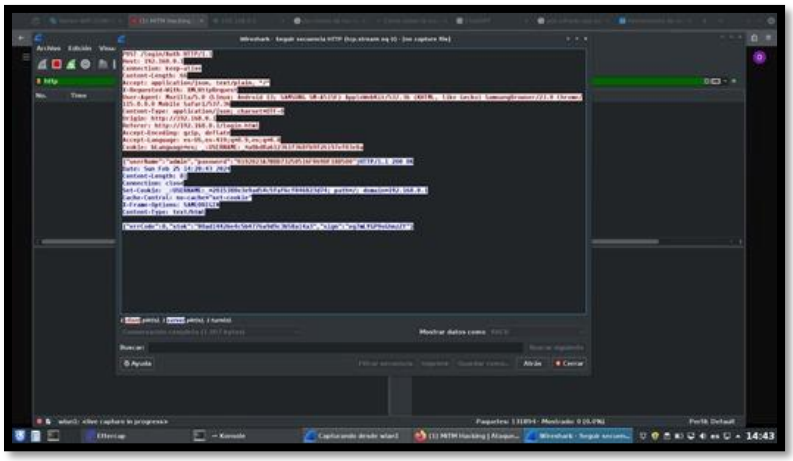


Figura 18: Captura de información luego del ataque

Ataque 3

Ataque de desautentificación

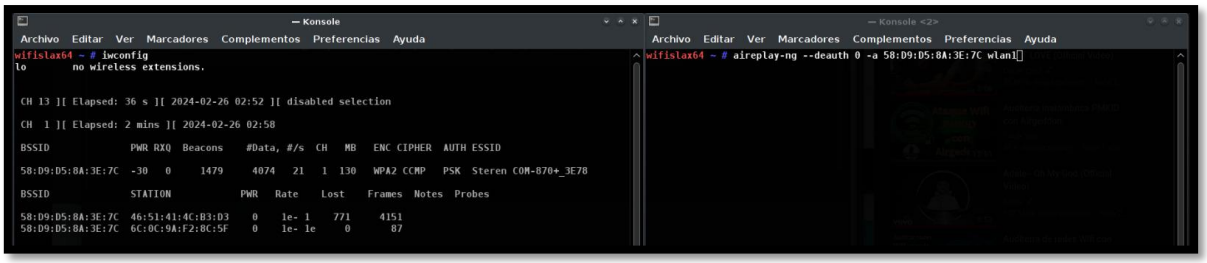


Figura 19: Ataque Desautenticaión

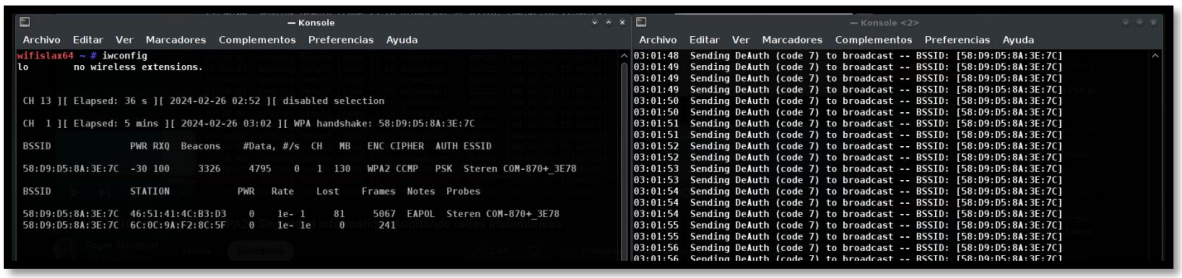


Figura 20: Ejecución de ataque

Figura 21: Visualización de paquetes generados mediante la herramienta "wireshark"

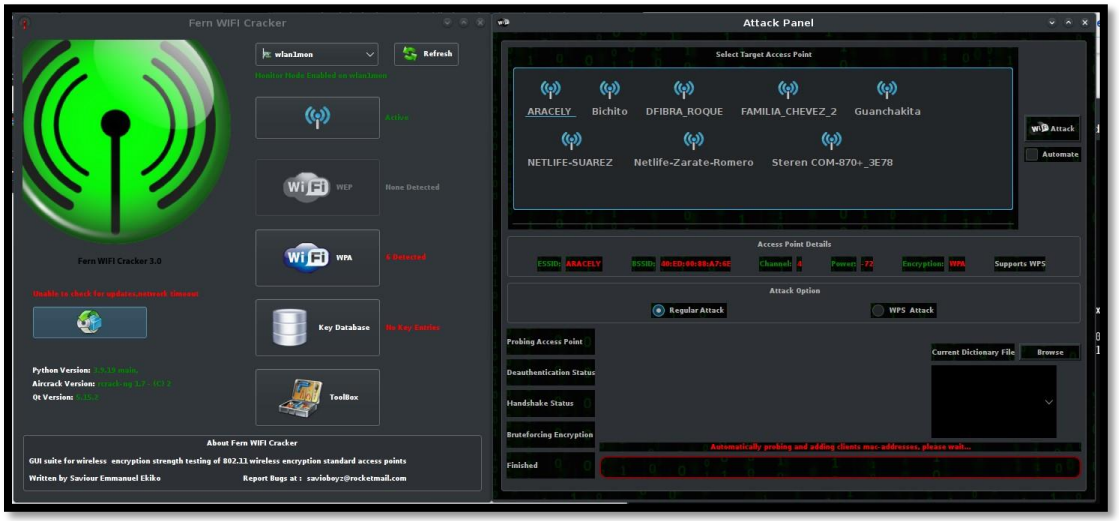


Figura 22: Visualización de redes sin detección de protocolo WPA3

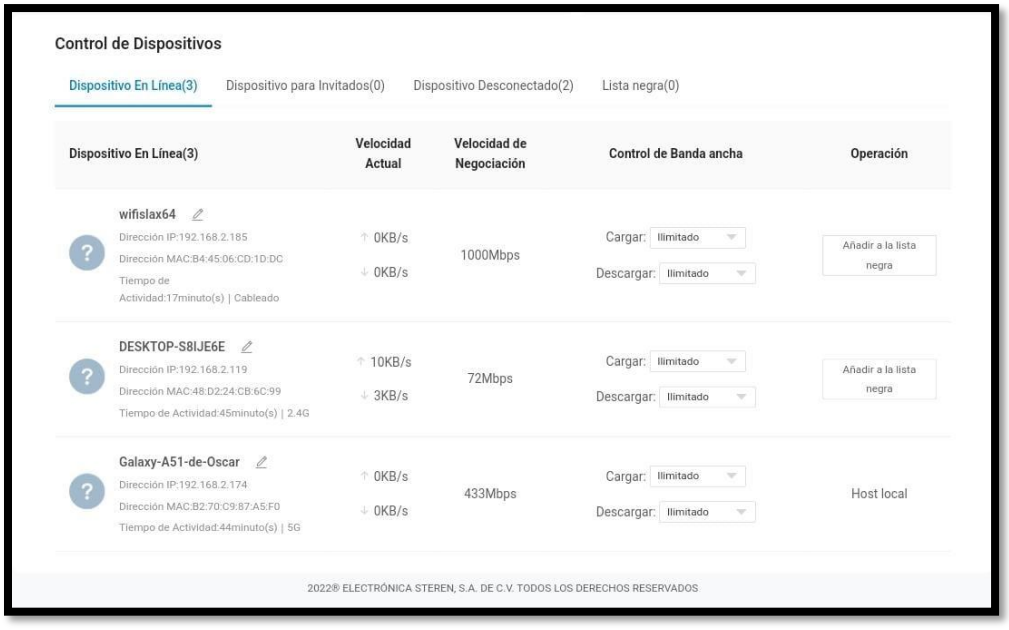


Figura 23: Herramienta Ettercap para realizar ataque “Men in The Middle”

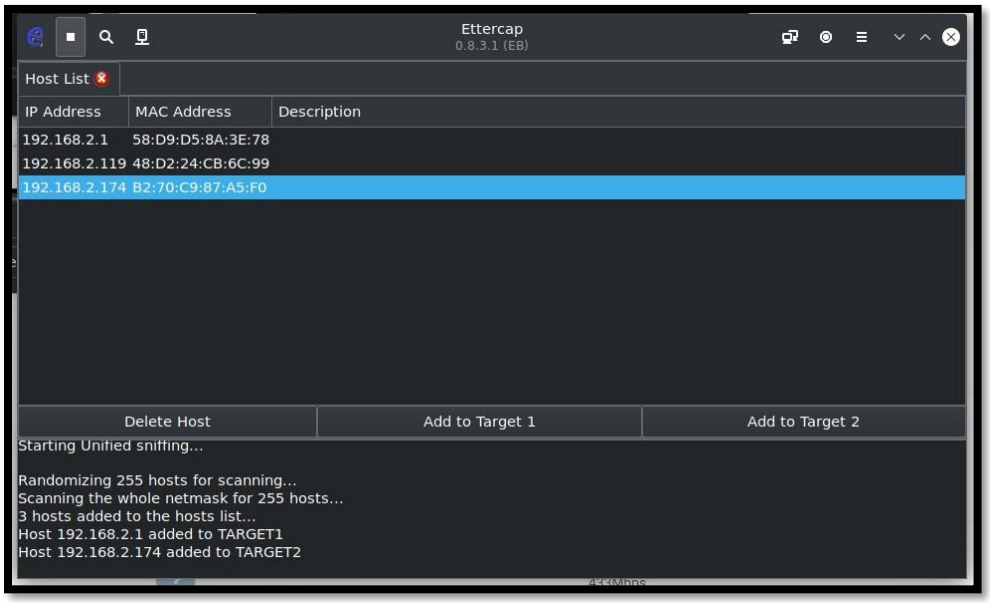


Figura 24: Ettercap elección de dispositivos a atacar.

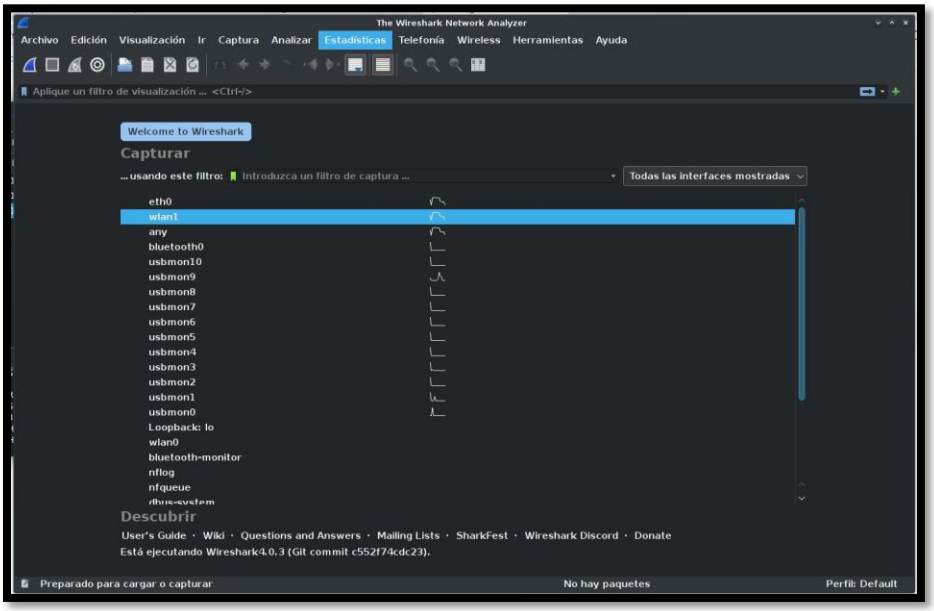


Figura 25: Herramienta Wireshark

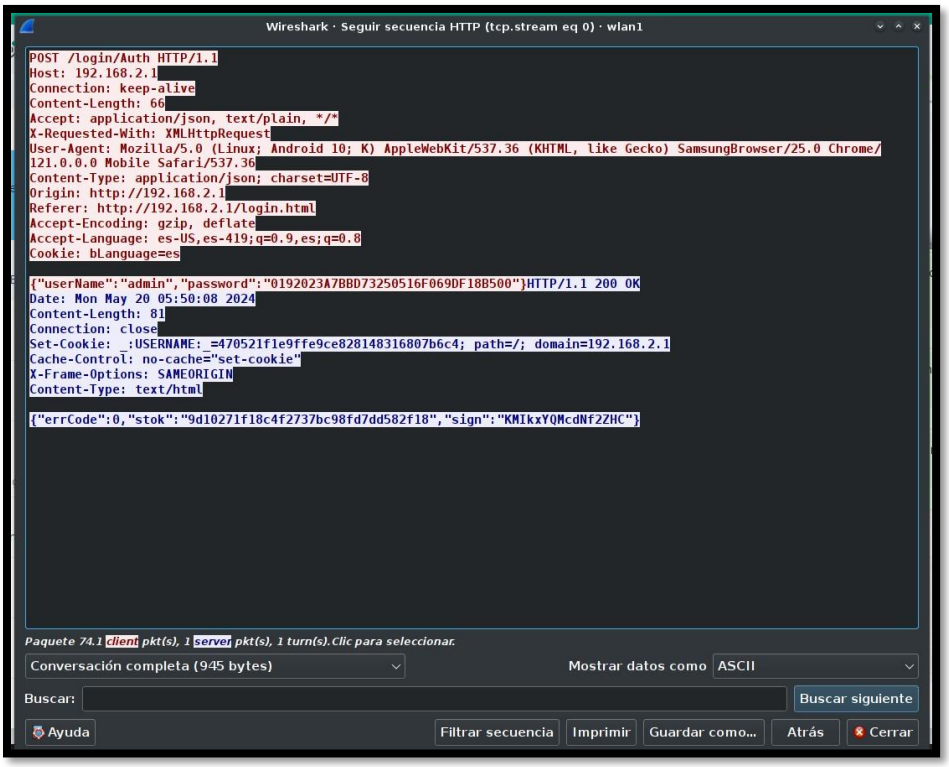


Figura 26: Información de Contraseñas.

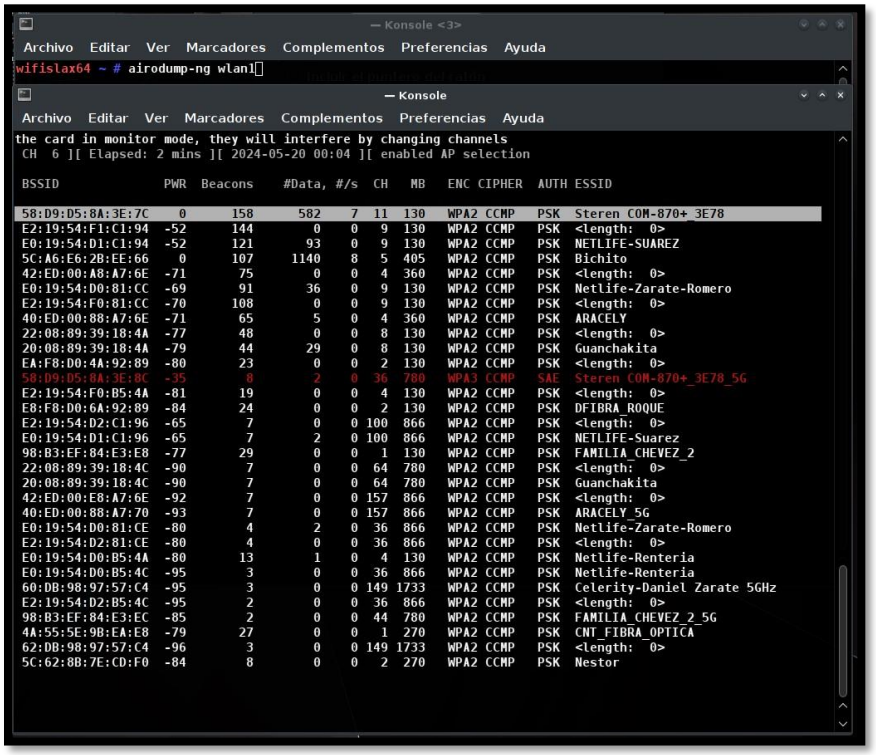


Figura 27: Visualización del protocolo WPA3

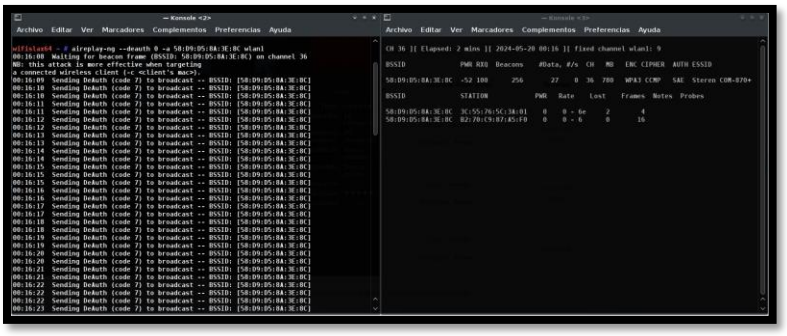


Figura 28: Desautenticacion

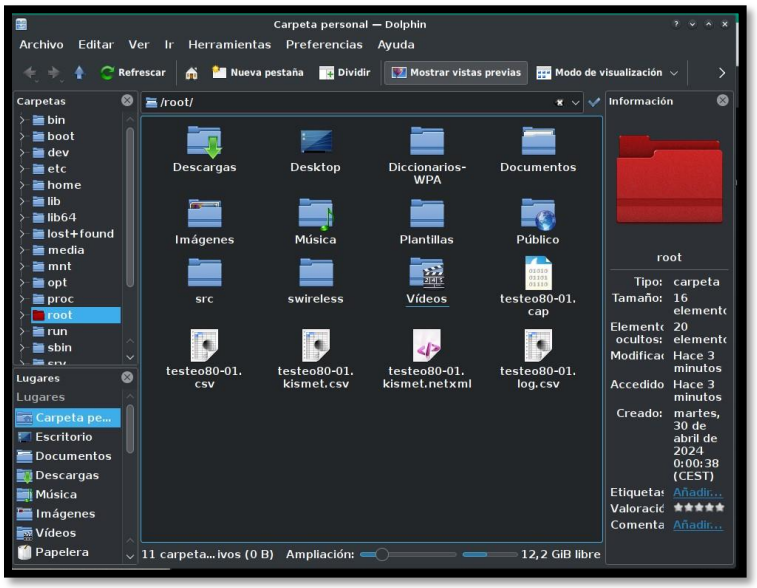


Figura 29: Documentos Generados

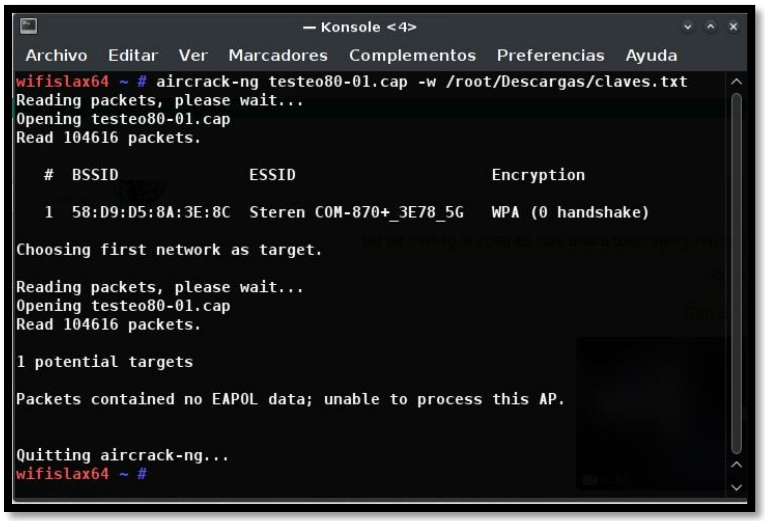


Figura 30: Obtención de clave fallida

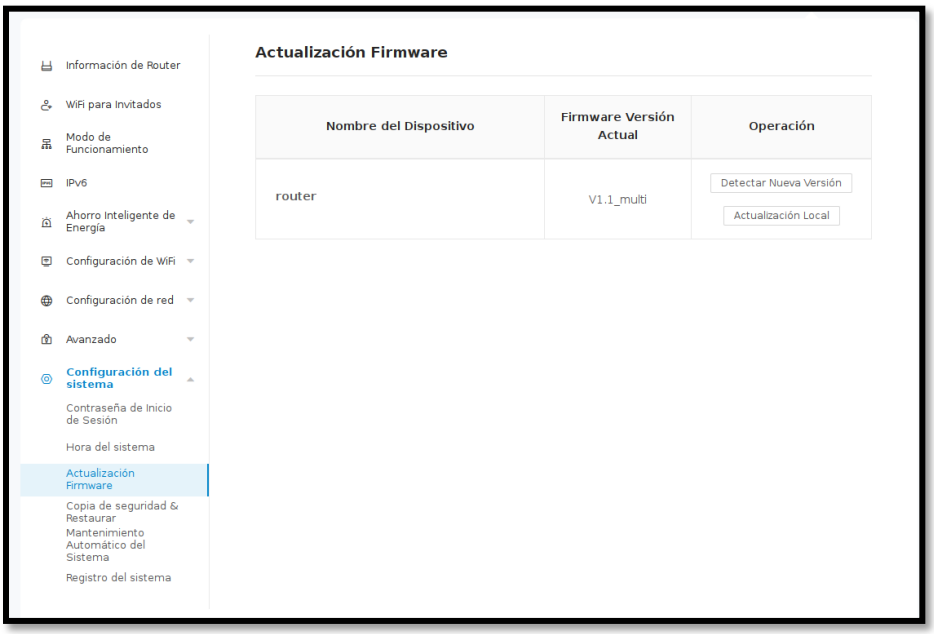


Figura 31: Actualización de Firmware

Figura 32: Uso de Contraseñas Robustas

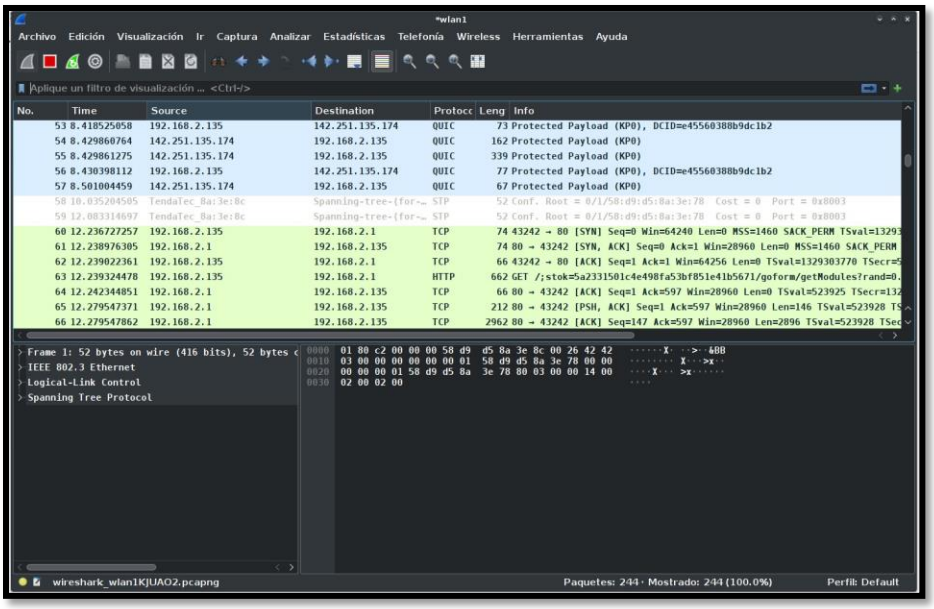


Figura 33: Monitoreo de Red

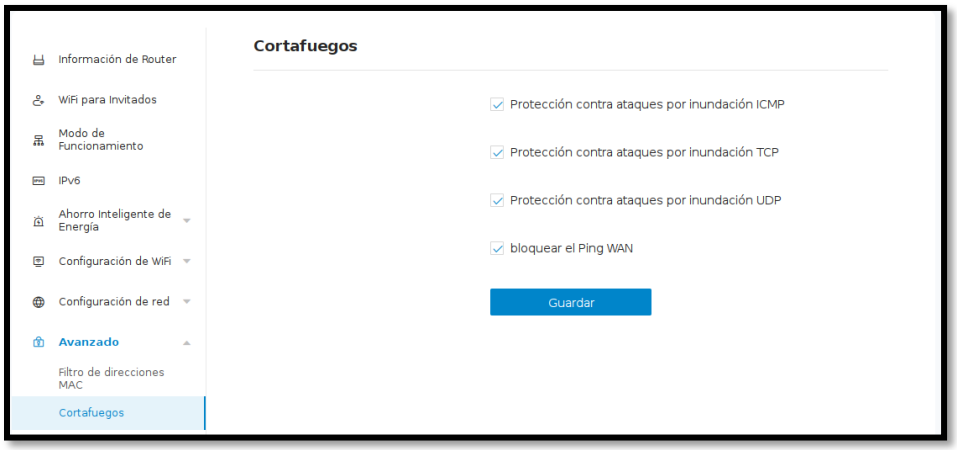


Figura 34: Implementación de Cortafuegos

Figura 35: Implementación protocolo WPA3

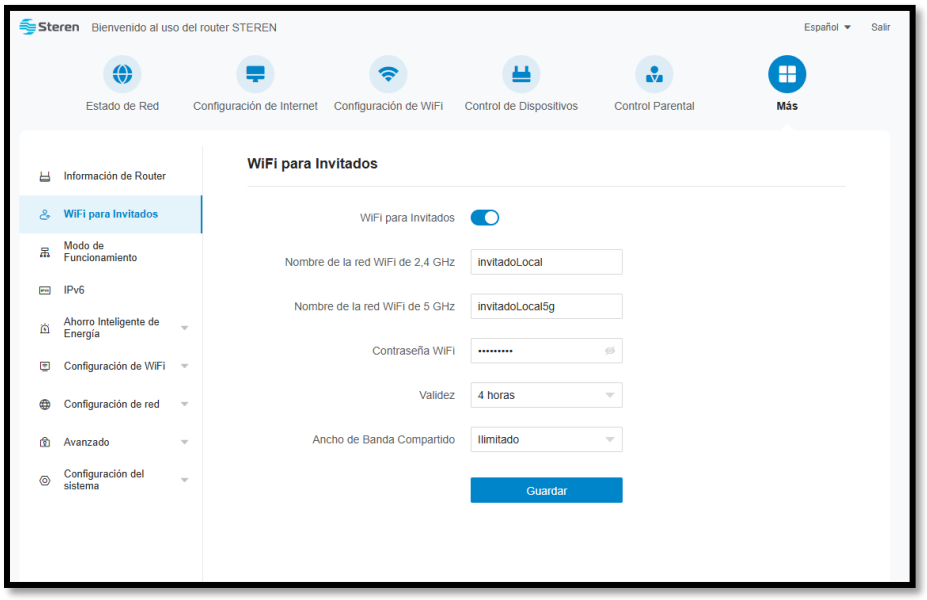


Figura 36: Configuración Red de Invitados

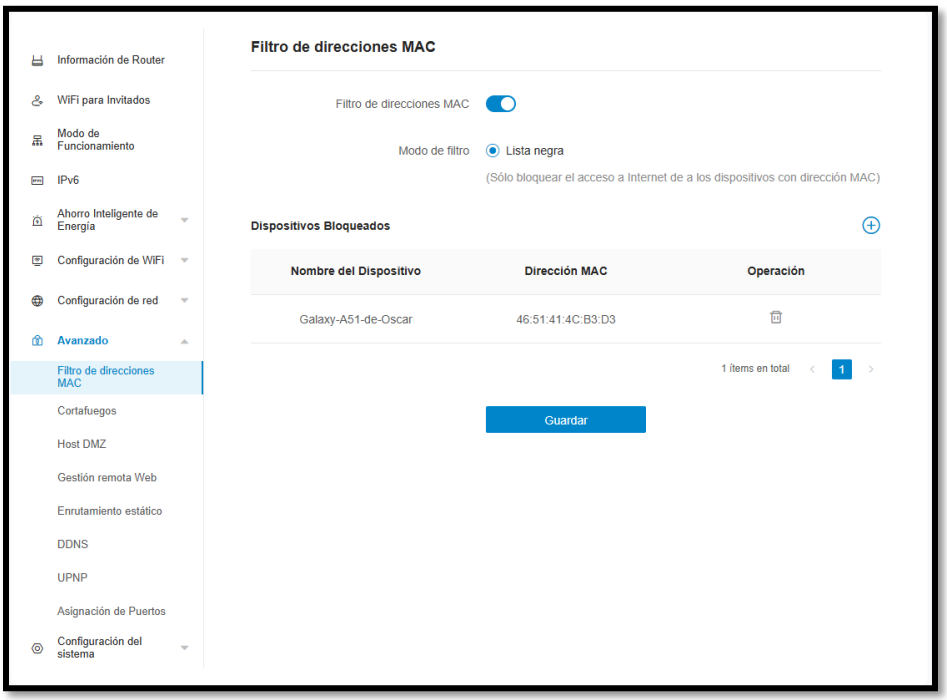


Figura 37: Filtro de Direcciones MAC

Figura 38: Implementación de Protocolo WPA3

Figura 39: Ataque de diccionario a WPA2 por 2da vez

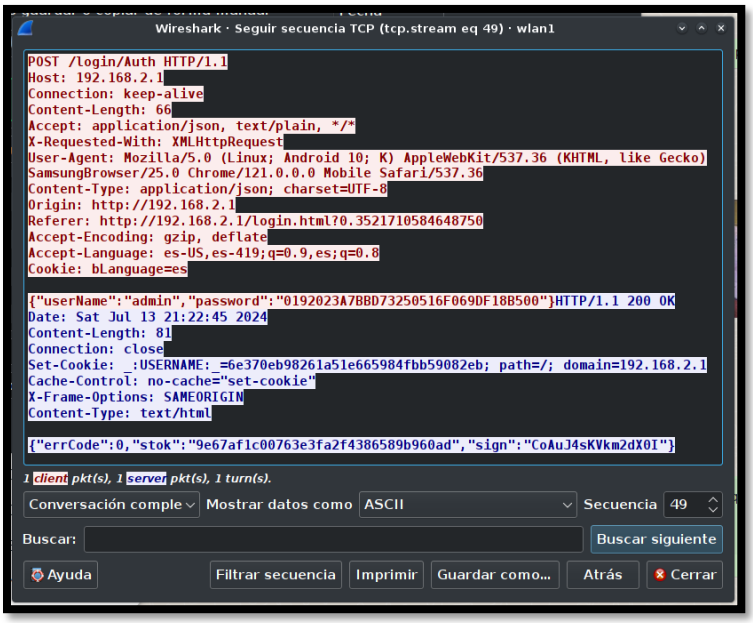


Figura 40: Ataque men in the middle a WPA2 por 2da Vez.

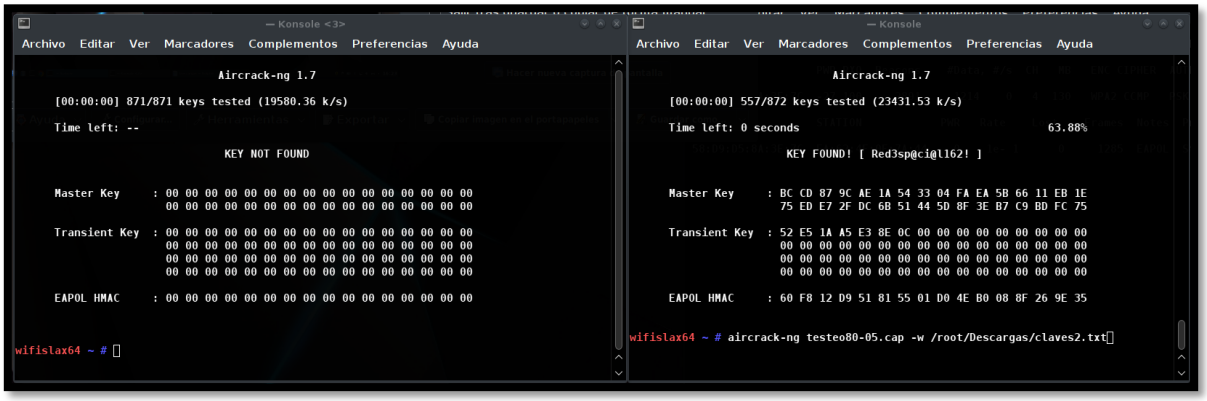


Figura 41: Ataque de desautenticacion a WPA2 por 2da vez

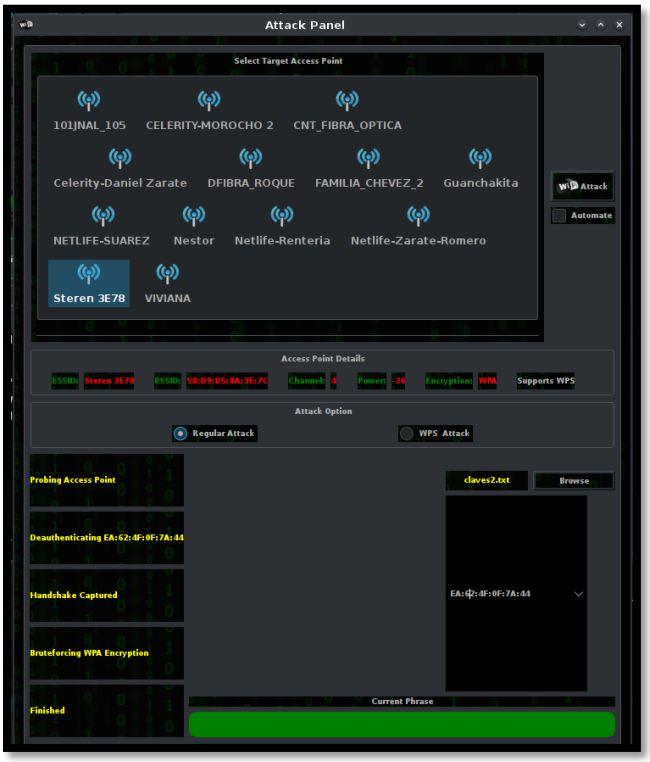


Figura 42: Ataque de Diccionario a WPA3 por 2da vez

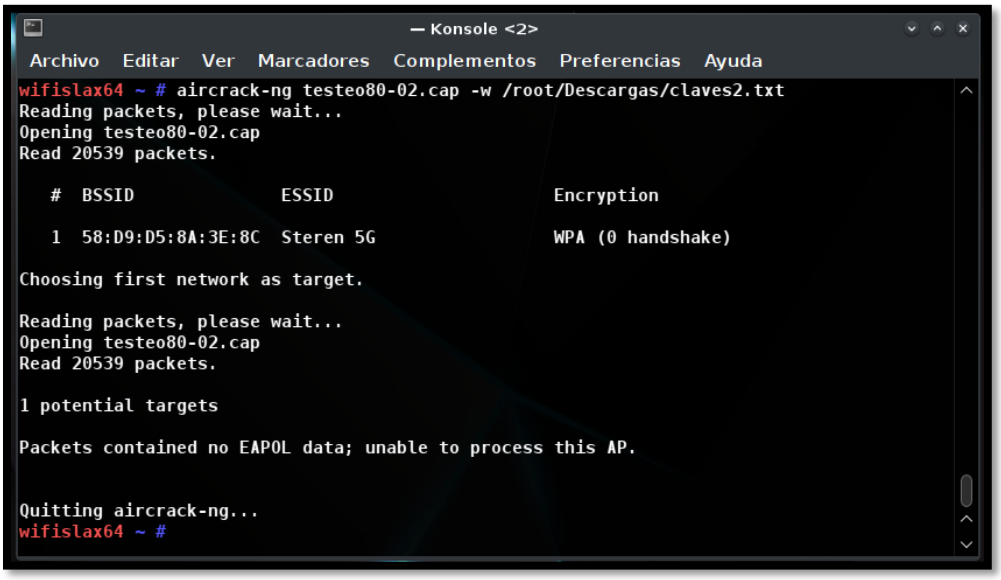


Figura 43: Ataque men in the middle a WPA3 por 2da vez

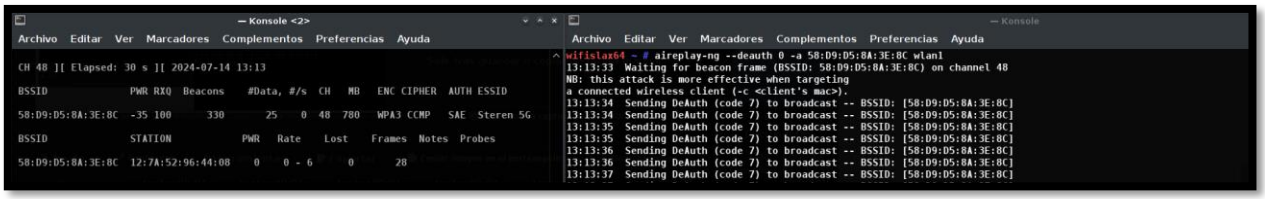


Figura 44: Ataque de desautenticacion a WPA3 por 2da vez