UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
COMPUTACIÓN

Trabajo de titulación previo a la obtención del título de:
Ingenieros en Ciencias de la Computación

TEMA:
ESTADO DEL ARTE UTILIZANDO MAPEO SISTEMÁTICO DE SEGURIDAD DE REDES DOMÉSTICAS WIFI EN FAMILIAS ECUATORIANAS

AUTORES:
CYNTHIA VALERIA MAZA GONZALEZ
FABIÁN GUSTAVO ROCHINA MANOBANDA

TUTOR:
MSC. MANUEL RAFAEL JAYA DUCHE

Quito, noviembre del 2021

CESIÓN DE DERECHOS DE AUTOR

Nosotros Cynthia Valeria Maza Gonzalez, Fabián Gustavo Rochina Manobanda, con documento de identificación No 1750188854 y No 0250114337, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación intitulado ESTADO DEL ARTE UTILIZANDO MAPEO SISTEMÁTICO DE SEGURIDAD DE REDES DOMÉSTICAS WIFI EN FAMILIAS ECUATORIANAS, mismo que ha sido desarrollado para optar por el título de: INGENIEROS EN CIENCIAS DE LA COMPUTACIÓN, en la Universidad Politécnica Salesiana, quedado la Universidad facultada por ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hacemos entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

……..	……..
Cynthia Valeria Maza Gonzalez	Fabián Gustavo Rochina Manobanda
1750188854	0250114337

Quito, noviembre del 2021

Declaratoria de coautoría del docente tutor

Yo declaro que bajo mi dirección y asesoría fue desarrollado el articulo académico, con el tema: ESTADO DEL ARTE UTILIZANDO MAPEO SISTEMÁTICO DE SEGURIDAD DE REDES DOMÉSTICAS WIFI EN FAMILIAS ECUATORIANAS realizado por Cynthia Valeria Maza Gonzalez y Fabián Gustavo Rochina Manobanda, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerado como trabajo final de titulación.

Quito, noviembre 2021

Manuel Rafael Jaya Duche
C.I:1710631035

ESTADO DEL ARTE UTILIZANDO MAPEO SISTEMÁTICO DE SEGURIDAD DE REDES DOMÉSTICAS WIFI EN FAMILIAS ECUATORIANAS

STATE OF THE ART USING SYSTEMATIC SECURITY MAPPING OF HOME WIFI NETWORKS IN ECUADORIAN HOUSEHOLDS

Cynthia Maza Gonzalez [1], Fabián Rochina Manobanda [2], Rafael Jaya Duche[3],

Resumen

El presente artículo tiene como objetivo construir un estado de arte utilizando mapeo sistemático sobre la seguridad de redes domesticas Wi-Fi. El documento propuesto presenta los tipos de ataques, protocolos, estándares, vulnerabilidades, recomendaciones y herramientas encontradas en esta área de investigación. Para el desarrollo de este trabajo se utilizaron dos metodologías que son: Mapeo sistemático que permitieron conocer las frecuencias de estudios, revistas, conferencias, autores e idiomas entre los años 2017 a 2021 y por otra parte la revisión de la literatura permitió interpretar y consolidar los estudios relevantes recolectadas en el mapeo sistemático. Se identificaron un total de 95 estudios de mayor relevancia distribuidos de las siguientes manera IEEE Xplore 37, ProQuest 11, ScienceDirect 14, Scopus 20 y Web of Science 13, todas en idioma inglés. Además de encontrar los estudios en los repositorios oficiales estos fueron presentados y publicados en 37 revistas y 41 conferencias. Por otra parte, se identificaron vulnerabilidades de: Factor Humano 19, Hardware 5 y Software 28. Se encontraron 45 protocolos y 21 estándares, también se hallaron 72 ataques de entre activos y pasivos. Además de 33 herramientas para ejecutar ataques y 45 para contrarrestarlas. Finalmente, de los estudios recolectados se encontró un enfoque mayoritario hacia las empresas que a los hogares con un 95% y 5% respectivamente en el tema de estudio.

Palabras clave: Mapeo Sistemático, Revisión Sistemática Literaria, Seguridad, Vulnerabilidades, Ataques, Wi-Fi.

Abstract

The present article aims to build a state of the art using a systematic mapping on the security of home Wi-Fi networks. The proposed document presents the types of attacks, protocols, standards, vulnerabilities, recommendations and tools found in this research area. For the development of this work, two methodologies were used, which are: Systematic mapping that allowed to know the frequencies of studies, journals, conferences, authors and languages between the years 2017 to 2021 and, on the other hand, the review of the literature allowed interpret and consolidate the relevant studies collected in the systematic mapping. A total of 95 more relevant studies were identified, distributed as follows: IEEE Xplore 37, ProQuest 11, ScienceDirect 14, Scopus 20 and Web of Science 13, all in English. In addition to finding the studies in the official repositories, they were presented and published in 37 journals and 41 conferences. On the other hand, vulnerabilities of: Human Factor 19, Hardware 5 and Software 28 were identified. 45 protocols and 21 standards were found, 72 attacks were also found between active and passive. In addition to 33 tools to execute attacks and 45 to counter them. Finally, of the collected studies, a majority approach was found towards companies than towards households with 95% and 5% respectively on the subject of study.

Keywords: Systematic Mapping, Systematic Literature Review, Security, Vulnerabilities, Attacks, Wi-Fi.

[1] Estudiante de Ingeniería en Ciencias de la Computación – Universidad Politécnica Salesiana, Egresado – UPS – sede Quito. Autor para correspondencia: cmazag@est.ups.edu.ec

[2]Estudiante de Ingeniería en Ciencias de la Computación – Universidad Politécnica Salesiana, Egresado – UPS – sede Quito. Autor para correspondencia: frochina@est.ups.edu.ec

[3] Magister en redes de Información y Conectividad, Ingeniero en Electrónica y Telecomunicaciones, Profesor de Ingeniería en Ciencias de la Computación – UPS - sede Quito. Email: mjaya@ups.edu.ec

1. Introducción

De acuerdo con [1], en los próximos años pueden existir más de 7 mil millones de dispositivos inalámbricos, los cuales podrían ser vulnerables a los peligros que existen en el Wi-Fi. Uno de los principales problemas en las redes inalámbricas domesticas es la falta de seguridad en el proceso de comunicación y el cifrado de datos donde los mecanismos de autenticación y control deben asegurar la identidad del usuario.

Las redes inalámbricas fueron publicadas en Suiza en los años 1979 de resultados de experimentos por ingenieros de IBM [2], años más tarde en 1997 empezaron el proceso de estandarización en la IEEE (del inglés *Institute of Electrical and Electronics Engineers*) donde se publicó el origen del estándar 802.11 que ofrecen velocidades y bandas de frecuencias diferentes, estos estándares de seguridad permiten tres modos de autenticación: i) abierta no utiliza ninguna clave para acceso hacia la red, ii) clave compartida donde hacen uso de la misma contraseña todos los usuarios para conectarse al punto de acceso, iii) basadas en puertos mediante métodos EAP (del inglés *Extensible Authentication Protocol*) para ello utilizan un servidor de autenticación como el RADIUS donde las claves de los usuarios son individuales [3]. A pesar de las seguridades que ofrece los estándares de la IEEE en el 2019 se identificó que el 77% de las empresas financieras mundialmente detectaron varios ataques con una alta probabilidad de éxito [1]. Según estudios sobre la seguridad en las redes inalámbricas que fueron realizados en diferentes países como Bolivia, México, Uruguay, Argentina, Canadá, España y entre otros se determinó que, de 905 redes, donde el 41.33% disponen de algún sistema de cifrado, mientras que el 58.37% carecen de cifrado. En Ecuador y en especial en la cuidad de Quito se determinó que el 93% de redes Wi-Fi son vulnerables a ataques maliciosos [4]. En base a estadísticas presentado por el autor se puede decir que las seguridades en las redes inalámbricas es un campo por explorar en nuestro país.

En la actualidad a las redes inalámbricas las encontramos en todos los lugares como en hogares, empresas, instituciones educativas, entre otras. Pero la falta conocimiento y la falta de interés en el tema de seguridades son las principales motivaciones para abordar el tema de estudio propuesto. El objetivo principal del desarrollo del estudio es dar a conocer a los lectores las vulnerabilidades y seguridades que actualmente son estudiadas.

El resto del artículo se encuentra organizado de la siguiente manera: la sección dos detalla los métodos y materiales utilizadas para la elaboración del estado de arte como son el mapeo sistemático y la revisión de la literatura donde se fusionan en tres etapas y finalmente las conclusiones se presentan en la sección tres.

2. Materiales y Métodos

2.1. Materiales

Según [5] en 2019 un 45.5% de la población tienen acceso a internet en los hogares en comparación del 2018 que fue del 37.2%, otro incremento se dio en el uso de computadoras portátiles que fue del 4%. El aumento del acceso a la tecnología trae consigo dos temas importantes: i) Las seguridades en [6] y [7] definen como la disciplina que se encarga de diseñar reglas, procedimientos y técnicas con el propósito de proteger la información y la privacidad, de tal manera que sea segura y confiable, ii) Vulnerabilidad en [8] define como una "*característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotado por una amenaza*". Seguridad de redes domésticas: En [9] define como la protección de la comunicación en el hogar entre los dispositivos y el intercambio de información hacia el internet, estos dispositivos pueden ser las laptops, smartphone, cámaras, router, smartwatch, entre otros y [10] menciona que "*la seguridad de la red doméstica es esencial para la protección de la privacidad de los usuarios*".

2.2. Métodos

Con la finalidad de obtener un estado del arte actualizado se utilizó el método Mapeo sistemático (del inglés SM, *Systematic Mapping*) según [11] es una técnica de búsqueda de información y extracción de estudios seleccionados exhaustivamente y orientados a un área de investigación especifica. Revisión de literatura sistemática (del inglés SLR, *Systematic Literature Review*) [12] es una técnica que utiliza los estudios relevantes del SM para evaluar, interpretar y consolidar resultados de estudios primarios. El trabajo de [13] proporcionan literatura científica donde se identifican metodologías, técnicas y herramientas; así como también se obtiene el registro de literatura orientada a cada actividad de la ingeniería de requisitos de software. De manera que se obtienen las bases necesarias para realizar el estudio de investigación orientado a "*vulnerabilidades de redes Wi-Fi domesticas*". El proceso que tendrá esta investigación comprende de tres etapas: i) La definición del protocolo está conformado de: Definición de pregunta de investigación SM y SLR, Alcance de la revisión, Criterios de inclusión y exclusión, Conducta de búsqueda. ii) La ejecución de la búsqueda se conforma de: Selección de estudios primarios, Definición de criterios de análisis, Criterios para la revisión Sistemática iii) La Discusión de resultados se conforma de: Resultados.

Base de datos: BD, **Términos de Búsqueda:** TB, **N. Estudios encontrados por base de datos:** NEBD, **N. Estudios seleccionados con EndNote:** NEEDN **N. Estudios seleccionados de la Literatura Sistemática:** NELS, **N. Estudios descartados:** NED

2.3. Etapa 1: Definiciones del protocolo

2.3.1. Preguntas de investigación para SM:

1. ¿Cuántos artículos se han anunciado en los últimos 5 años?
2. ¿Cuáles son las revistas y conferencias más utilizadas en los últimos cinco años?
3. ¿Cuáles son los autores que han aportado más de un artículo en los últimos cinco años?
4. ¿En qué idiomas se produce la investigación sobre seguridad y vulnerabilidades en redes Wi-Fi?

2.3.2. Preguntas de investigación para SLR:

1. ¿Cuáles son las características de una red Wi-Fi vulnerable?
2. ¿Cuáles son los protocolos y estándares que mayormente son utilizados?
3. ¿Cuáles son los programas de ataques más utilizadas que se emplearon?
4. ¿Cuáles son los programas más utilizados para contrarrestar los ataques informáticos?

Para el desarrollo de la investigación se consideraron las bases de datos más conocidas por ser accesibles y disponer de parámetros de búsqueda avanzada: *Scopus, Web of Science, ScienceDirect, IEEE Xplore y ProQuest*.

2.3.3. Alcance de la revisión

PICOC es una estrategia que ayuda definir el ámbito de la revisión para que se puedan responder las preguntas de investigación y seleccionar los términos de búsqueda [14]. Mediante el cual se identificaron términos de búsqueda, como se puede visualizar en la Tabla 1.

Tabla 1: Componentes claves de Picoc

Criterio	Descripción
Population (P): ¿Quién?	Seguridad y vulnerabilidades en redes Wi-Fi.
Intervention(I):¿Qué?, ¿Cómo?	Técnicas, métodos y procesos de protocolos de seguridad.
Comparison (C): ¿Con qué comparar?	Estudios con herramientas que identifican vulnerabilidades y soluciones.
Outcomes (O):¿Qué se busca conseguir/mejorar?	Conseguir mejorar la seguridad de las redes Wi-Fi.
Context (C):¿En qué tipo de organización y bajo qué circunstancias?	Revisar los estudios existentes sobre la seguridad y vulnerabilidades en redes Wi-Fi.

Mediante los componentes identificados en PICOC, permitió extraer las primeras terminologías referentes al tema de estudio, con el cual se procedieron a realizar búsquedas de palabras claves en los artículos relacionados con el tema en el buscador de Google Académico, esto permitió identificar las terminologías, como se puede visualizar en la Tabla 2 que sobresalen para armar la cadena de búsqueda a base de pruebas y error por medio de las interacciones en el buscador antes mencionado en donde se escogieron 10 artículos al azar y si 8 llegaban a tener un aporte significativo a la investigación significaba que la cadena de búsqueda estaba lista para usarse en las bases de datos.

Tabla 2: Términos de búsqueda

Prioridad	Palabras	Similares
1	Network wireless	Wi-Fi, WLAN
2	Attacks	MITM, SSID, Spoofing, DoS
3	Wireless vulnerability	Weakness
4	Wireless security	Protocols, 802.11

Y como resultado se obtuvo la siguiente cadena de búsqueda primaria: (Network wireless OR Wi-Fi OR WLAN) AND (attacks OR MITM OR SSID OR spoofing OR DoS) AND (wireless vulnerability OR weakness) AND (Wireless security OR protocols OR 802.11).

Cada artículo encontrado en la búsqueda automatizada se analizará con el fin de decidir si debe incluirse o excluirse considerando su título, resumen y palabras clave. Las discrepancias en la selección se resolverán por consenso después de revisar el articulo completo [15].

2.3.4. Criterios de inclusión

- **CISM1:** Se incluye artículos que tengan información del título, autor, revista de publicación, idioma, año, BD, tipo de referencia, doi y problema.
- **CISM2:** Son elegibles todas las publicaciones científicas que tengan relación con información acerca de vulnerabilidades y seguridades que existen en la red.
- **CISM3:** Son incluidos estudios en idiomas: inglés y español.
- **CIRLS1:** Se incluye información que contenga ataques, vulnerabilidades, herramientas de ataques o seguridad, protocolos, estándares, métodos, sugerencias para la red.

2.3.5. Criterios de exclusión

- **CESM1:** Se excluyen estudios que tengan como investigación los siguientes criterios: discusión, comentarios o resúmenes sobre prototipados en relación con redes inalámbricas, prototipados móviles y sensores.
- **CESM2:** Se excluyen estudios irrelevantes o con poca información acerca de vulnerabilidades y seguridades que existen en la red.
- **CERSL1:** Se excluyen estudios que no aporten de información o contengan criterios como: sensores, vehículos, móviles, prototipos, entre otros.

2.3.6. Conducta de la búsqueda

Para llevar a cabo la selección de artículos primarios se realizan los siguientes filtros de revisión:

Primer filtro

- **Título y Resumen:** Se examinaron títulos de estudios en diferentes bases de datos, además del resumen en donde se revisó que tenga consistencia con la investigación realizada

Segundo filtro

- **Texto completo:** Después de que los estudios pasen por el primer filtro se procederá a leer y analizar el texto completo.

2.4. Etapa 2: Ejecución de la búsqueda

En esta etapa se realiza la selección de los estudios primarios y la definición de los criterios de análisis.

Tabla 3: Cantidad de estudios

BD	TB	NEBD	NEEDN	NED	NELS
Scopus	Network wireless OR Wi-Fi OR WLAN AND attacks OR MITM OR SSID OR spoofing OR DoS AND wireless vulnerability OR weakness AND Wireless security OR protocols OR 802.11 AND NOT sensor AND NOT prototypes AND NOT mobile	175	23	3	20
Web of Science	Network wireless OR Wi-Fi OR WLAN And attacks OR MITM OR SSID OR spoofing OR DoS And wireless vulnerability OR weakness And Wireless security OR protocols OR 802.11 NOT sensor NOT prototypes NOT mobile	111	24	10	13
ScienceDirect	(Wi-Fi) AND (attacks OR DoS AND wireless vulnerability) AND (protocols OR 802.11) NOT sensor NOT prototypes	104	22	8	14
IEEE Xplore	((Wireless OR Wi-Fi OR 802.11 OR WLAN OR Wireless Connection) AND (Attack OR MITM OR spoofing OR DoS OR vulnerability OR weakness wireless Networks OR CVE) AND (security OR Cybersecurity wireless OR protocols OR prevention wireless security OR confidentiality OR integrity OR availability OR WPA OR WPA2 OR WPA3) AND (techniques OR methods OR tools OR scanning) NOT (sensor OR prototypes OR bluetooth OR mobile OR 802.15))	616	50	9	37
ProQuest	(Network wireless OR Wi-Fi OR WLAN) AND(attacks OR MITM OR SSID OR spoofing OR DoS) AND (wireless vulnerability OR weakness) AND (Wireless security OR protocols OR 802.11) NOT (sensor OR prototypes OR mobile)	286	30	17	11
Total:		**1292**	**149**	**47**	**95**

2.4.1. Selección de estudios primarios

Mediante la cadena de búsqueda, se realizó la investigación en cada una de las bases de datos haciendo uso de la búsqueda avanzada se agregaron los operadores lógicos como *AND, OR* y *NOT*, además se hicieron usos de los paréntesis para agrupar y aplicar prioridad. Con los NEBD se procedieron a descargar las citas y los resumes. Antes de proceder a revisar los resúmenes de los artículos se realizó un proceso de filtrado de resúmenes haciendo uso de la herramienta EndNote versión X9.3.3 donde se utilizó las palabras claves de mayor impacto de la cadena de búsqueda, con los NEEDN se procedieron a revisar los resúmenes en busca de información relacionado al tema de estudio, se procede a pasar al segundo filtrado en donde se leerá todo el artículo. Los resultados pueden ser observados en la Tabla 3.

2.4.2. Definición de criterios de análisis

Para el análisis de cada NEEDN, se definieron criterios de inclusión: CIRSL1 y exclusión CERSL1 para evaluar y comparar los trabajos entre sí, con el fin de obtener resultados favorables enfocados a la seguridad en la red Wi-Fi, estos son: Año: Se indica el año de las publicaciones para identificar si hubo alguna evolución en ese tiempo. Tipo de publicación: Artículos científicos de revista y conferencias. Tipo de propuesta: Cualquier articulo encontrado se clasifica de acuerdo si propone o discute algún tipo de metodología, métodos, técnicas o herramientas que ayude a reducir las vulnerabilidades en las redes Wi-Fi.

2.4.3. Criterios para SRL

Se lleva a cabo la revisión de los artículos seleccionados tomando en cuenta los criterios de inclusión y exclusión mencionados. Para la clasificación de información de los estudios obtenidos se propuso la siguiente taxonomía en base a [16], la cual se observa en la Figura 1.

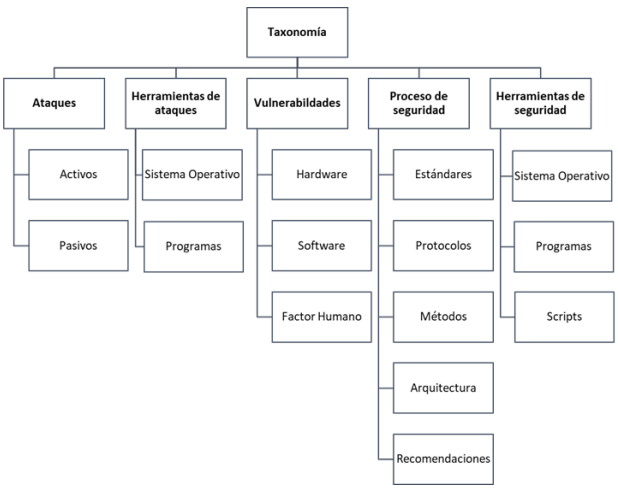

Figura 1: Taxonomía

Ataques: Son diferentes métodos para descubrir, atacar e interceptar una red inalámbrica, los cuales se pueden diferenciar en dos grupos: i) Activos: Estos se caracterizan por acciones que tratan de penetrar la infraestructura, e incluso de establecerse en la red de forma permanente por motivos de sabotajes, robo de información o despliegue de malware, entre otros, los cuales producen cambios en información y recursos del sistema. ii) Pasivos: En este caso es un ataque no invasivo ya

que no afecta a la infraestructura, pero monitoriza que puede almacenar o transmitir, incluso información que es directamente pública [17].

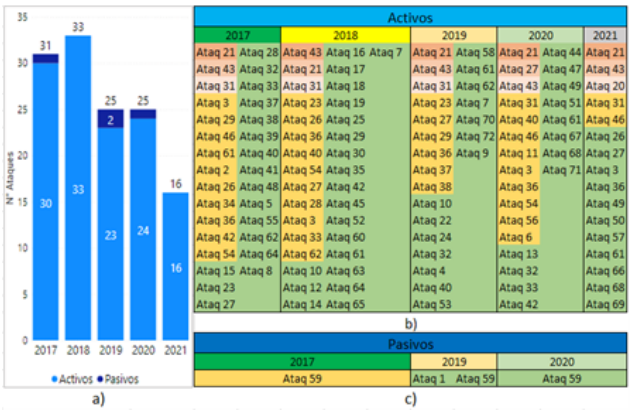

Figura 2: a) N. de Ataques activos y pasivos, b) Matriz de ataques activos, c) Matriz de ataques pasivos

Al momento de realizar la revisión literaria, proporcionó información de diferentes ataques los cuales se encuentran organizados en la Figura 2. Donde se puede visualizar que existen más ataques activos que pasivos, los cuales han sido más frecuentes en el año 2018. Como se observa en la Matriz de ataques pasivos se visualiza que han utilizado tres veces el ataque Sniffing (Ataq 59): Se utiliza para capturar el tráfico de una red inalámbrica, además de información sobre las conexiones y equipos por medio de la herramienta *"sniffer"*. Y una sola vez el ataque. Análisis de tráfico (Ataq 1): Observa los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello la herramientas *"sniffer"* [18] [19], como se puede visualizar en la Tabla 4.

Tabla 4: Ataques pasivos

Etiqueta	Nombre	Referencia
Ataq 1	Análisis de tráfico	[20]
Ataq 59	Sniffing	[20] [21] [22] [23]

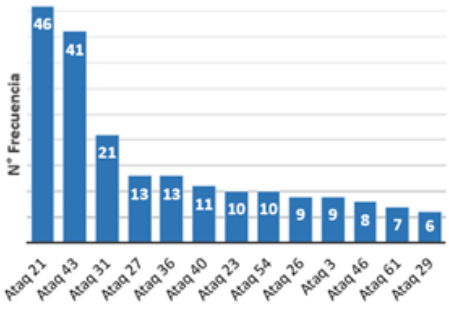

Figura 3: Ataques activos más comunes

Y en la Figura 3, se observa que existen ataques activos que se utilizan desde una vez hasta cuarenta y seis veces, sin embargo, los ataques que se describirán a continuación son en base a [18] [19] ya que se les dio mayor importancia por tener una frecuencia mayor de trece veces, los cuales son: Denial of service-DoS (Ataq 21): Es un conjunto de técnicas que su objetivo es dejar a un equipo o red informática inoperativo mediante saturaciones de peticiones hasta que no pueda atenderlas, impidiendo que pueda ofrecer servicios a sus clientes y usuarios. Man in the middle -MITM (Ataq 43): Se utiliza para supervisar la comunicación entre dos partes y falsifica los intercambios para hacerse pasar por una de ellas, este ataque es realizado utilizando la técnica de rastreo de puertos. Evil Twin (Ataq 31): Este ataque consiste en crear puntos de accesos falsos cuyo objetivo es hacer que el usuario sea redirigido a una página web falsa para que pueda iniciar sesión con su contraseña y así obtenerla fácilmente. Distributed Denial of Service-DDoS (Ataq 27): Es llevado a cabo por equipos *"zombis"*, los cuales se encargan de infectar algún virus o troyano al equipo para que puedan abrir o acceder al control remoto por parte de usuarios remotos, esto se realiza sin que el usuario se dé cuenta. Fuerza bruta (Ataq 36): Consiste en intentar averiguar o explotar todas las posibles combinaciones de contraseñas hasta encontrar la correcta, como se puede visualizar en la Tabla 5. Así mismo el anexo 1 contiene más información de la Tabla 5.

Tabla 5: Ataques activos

Etiqueta	Nombre	Referencia
Ataq 21	Denial of service-DoS	[20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] [60] [61] [62] [63]
Ataq 27	Distributed Denial Of Service-DDoS	[23] [24] [46] [55] [64] [65] [66] [67] [68] [69] [70] [71] [72]
Ataq 31	Evil Twin	[21] [26] [30] [35] [47] [48] [49] [54] [70] [73] [74] [75] [76] [77] [78] [79] [80] [81] [82] [83] [84]
Ataq 36	Fuerza bruta	[3] [23] [27] [35] [49] [54] [64] [69] [75] [85] [86] [87] [88]
Ataq 43	Man in the middle-MITM	[20] [21] [22] [24] [25] [26] [27] [29] [31] [32] [34] [35] [41] [43] [44] [48] [49] [50] [51] [53] [54] [56] [59] [60] [81] [84] [87] [89] [90] [91] [92] [93] [94]

Herramientas de ataques: Como ya se ha mencionado existen diferentes ataques activos y pasivos los cuales pueden ser implementados por herramientas de ataques según [95] son utilizados por terceras personas que quieren acceder a la red sin autorización para ello pueden utilizar: i) Sistema Operativo (S.O.): Es un conjunto de programas para el funcionamiento de otros, que sirven para utilizar en ellos herramientas tanto para realizar ataques o vulnerabilidades como herramientas de seguri-

dad, que gestionan los recursos de la computadora y controlan sus actividades. ii) Programas: Son programas que sirven para atacar a la red, está compuesto de servicios ejecutables que realizan acciones ante el sistema para vulnerar su seguridad, información, entre otros.

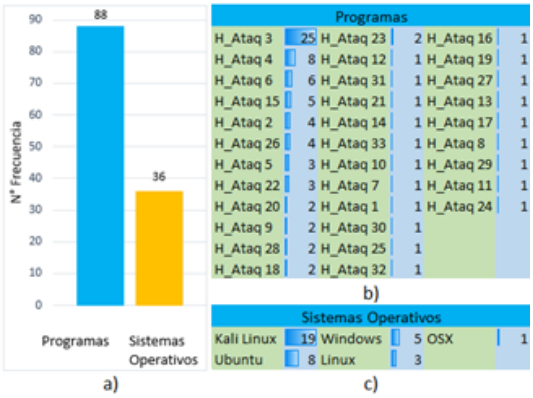

Figura 4: a) N. Herramientas de ataques (Programas y S.O.), b) Matriz de programas de ataques, c) Matriz de S.O. para ataques

Como se visualiza en la Figura 4, Matriz de programas de ataques, existen una frecuencia mayor a cinco veces los cuales son: Aircrack-ng (H_Ataq 3): Es un conjunto de herramientas que sirven para monitoreo y análisis de redes inalámbricas, descifra claves WEP y WPA. Aireplay-ng (H_Ataq 4): Sirve para inyección de paquetes y generación de tráfico. Airodump-ng (H_Ataq 6): Sirve para capturar paquetes 802.11. Ettercap (H_Ataq 15): Es una herramienta de software libre que permite analizar el tráfico que pasa por la red, poniendo en modo monitor la tarjeta de red *wireless* o *ethernet*, esto permite realizar un puente de paso que será capaz de ver conexiones tienen tus dispositivos con el router sin perder la sincronización de la conexión, como se puede visualizar en la Tabla 6. Así mismo el anexo 2 contiene más información de la Tabla 6. En el caso de los S.O. se visualiza que el más frecuente para realizar ataques es: Kali Linux: Es uno de los sistemas operativos basados en Linux con funciones para pruebas de penetración y auditorías de seguridad en red. Estas herramientas que se describieron fueron en base a [96] como se puede visualizar en la Tabla 7.

Tabla 6: Programas de ataques

Etiqueta	Nombre	Referencia
H_Ataq 3	Aircrack-ng	[28] [30] [31] [44] [47] [49] [50] [54] [57] [58] [64] [73] [76] [77] [78] [79] [85] [87] [88] [90] [92] [97] [98] [99] [100]
H_Ataq 4	Aireplay-ng	[35] [58] [73] [82] [83] [88] [101] [102]
H_Ataq 6	Airodump-ng	[30] [64] [73] [81] [82] [90]
H_Ataq 15	Ettercap	[59] [62] [65] [91] [103]

Tabla 7: Sistemas operativos para ataques y seguridad

Sistemas Operativos		
Etiqueta	**Referencias de ataques**	**Referencias de seguridad**
Kali Linux	[29] [47] [49] [50] [54] [62] [77] [80] [82] [84] [85] [91] [92] [94] [97] [98] [100] [102] [104]	[30] [64] [83]
Linux	[87] [88] [105]	[21] [37] [81]
OSX	[98]	[70]
Ubuntu	[45] [51] [56] [59] [67] [101] [106] [107]	
Windows	[46] [52] [98] [101] [108]	
Debian		[21]
Raspbian		[109]

Vulnerabilidades: En [17] concluyeron que son fallas en los sistemas, no son puertas abiertas diseñadas deliberadamente, sino errores de diseño, configuración o implementación que generan oportunidades de ataque, es decir que hacen viable una amenaza. I) Hardware: Para vulnerar un dispositivo el atacante necesita tener acceso físico, pueden producirse a través de la red o afectando al medio físico de transmisión. ii) Software: En el caso de vulnerar los programas se refiere a fallas en la programación o compilación que ejecutan las computadoras a servidores, los ataques pueden derivar en un mal funcionamiento del software, acceso a información restringida, fallos de sistema, entre otros. iii) Factor Humano: Pueden actuar contra los intereses de la organización por descontento, error, engaño o coacción.

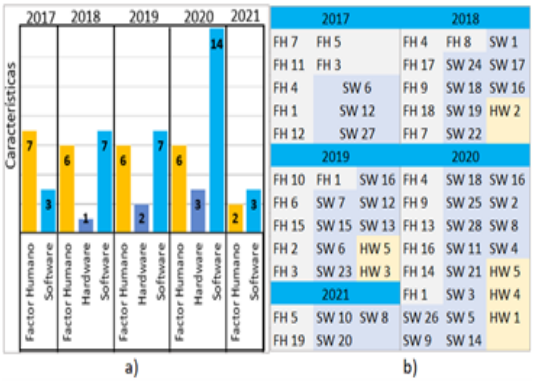

Figura 5: a) N. de vulnerabilidades, b) Matriz de vulnerabilidadesa

Como se visualiza en la Figura 5, existen vulnerabilidades que tienen una frecuencia de dos y tres veces en los últimos cinco años. Por parte de vulnerabilidades en el hardware se tiene WPS (HW 5) el cual consiste en mantener encendido esta función de acuerdo con [109] y [64]. En el caso de vulnerabilidades por software se toma en cuenta a Hole 196 SW (16) ya que tiene una repitencia de tres veces, el cual consiste en encontrar vulnerabilidades en una página web, esto suelen explotar con un *exploit man in the middle* [45]. Y por último en vulnerabilidades por factor humano: Acceso no autorizado (FH 1) consiste en que terceras personas acceden a equipos

o información sin ninguna autorización [86] [23] [72] y Configuración de red predeterminada (FH 4) que es porque los usuarios no tienen la información suficiente o hacen caso nulo ante ataques o vulnerabilidades de la red [24] [74] [86], como se puede visualizar en la Tabla 8. Así mismo el anexo 3 contiene más información de la Tabla 8.

Tabla 8: Vulnerabilidades

Etiqueta	Nombre	Referencia
Hardware		
HW 5	WPS	[64] [109]
Software		
SW 16	Hole 196	[45] [87] [106]
Factor Humano		
FH 1	Acceso no autorizado	[23] [72] [86]
FH 4	Configuración de red predeterminada	[24] [74] [86]

Proceso de Seguridad: Según [17] un proceso de seguridad ayuda a la red y usuarios a minimizar los riegos de ataques y vulnerabilidades el cual puede estar dividido en: i) Estándares: En [110] se dice que es un acuerdo en común para la comunicación entre fabricantes y ajustes de estándares en los nuevos productos que se incrementen en el mercado. ii) Protocolos: Es un conjunto de normas o un convenio que determina el formato y la transmisión de los datos. La capa n de una computadora se comunica con la capa n de otra computadora. Las normas y convenciones que se utilizan en esta comunicación se designan colectivamente protocolo de la capa *"n"*. iii) Métodos: Son medidas de corrección que permiten detectar riesgos los cuales puedan afectar a la seguridad. iv) Arquitectura: Define un esquema de áreas en la organización por el cual se establecen niveles de seguridad para cada proceso [95]. v) Sugerencias. Son criterios que se dan a conocer sobre configuraciones se pueden implementar para evitar ataques o vulnerabilidades en la red, estas pueden ser tanto para empresas y hogares.

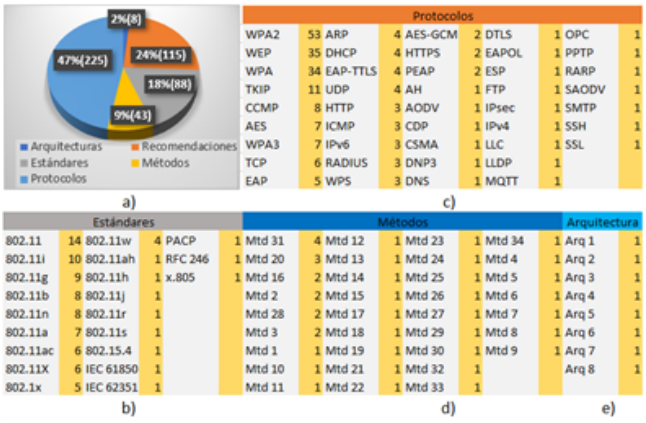

Figura 6: a) Porcentajes de los procesos de seguridad, b) Matriz de estándares, c) Matriz de protocolos, d) Matriz de métodos, e) Matriz de arquitecturas

En la Figura 6, Matriz de protocolos se observa que existen protocolos que se repiten más de once veces, los cuales se describirán en base a [111], estos son: Wi-Fi Protected Access 2 (WPA2): Es un método de encriptar redes inalámbricas más seguro hasta la fecha, ya que su algoritmo es suficientemente complejo y con suficientes precauciones y prácticas de seguridad informática se hace más complicado obtener las contraseñas rápidamente sin ataques de fuerza bruta. Wired Equivalent Privacy (WEP): Desarrollado para proporcionar un modelo de transporte seguro en redes de área local. Wi-Fi Protected Access (WPA): Aborda las debilidades de la privacidad de los datos de WEP. Temporal Key Integrity Protocol (TKIP): Es un protocolo de encriptación utilizado por el protocolo WPA, como se puede visualizar en la Tabla 9. Así mismo el anexo 4 contiene más información de la Tabla 9.

Tabla 9: Protocolos

Etiqueta	Nombre	Referencia
TKIP	Temporal Key Integrity Protocol	[20] [22] [26] [27] [35] [42] [44] [74] [78] [86] [90]
WEP / WPA	Wired Equivalent Privacy / Wi-Fi Protected Access	[3] [22] [26] [30] [32] [35] [38] [39] [40] [42] [44] [46] [50] [51] [52] [54] [64] [70] [73] [76] [77] [78] [79] [81] [85] [86] [88] [89] [90] [100] [105] [108] [109] [112] [113]
WPA2	Wi-Fi Protected Access 2	[3] [22] [25] [26] [27] [29] [31] [32] [35] [38] [42] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [57] [62] [64] [69] [73] [74] [75] [77] [78] [79] [81] [84] [86] [87] [88] [89] [90] [92] [94] [97] [99] [101] [105] [106] [107] [108] [109] [112] [113] [114] [115]

En la Figura 6, Matriz de estándares se observa que existen estándares que se frecuentan más de ocho veces, los cuales se describirán en base a [116], estos son: 802.11: Es un estándar de red inalámbrico, que define como tener una conexión entre dispositivos y redes inalámbricos, fue creador por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). 802.11i: Permite incorporar mecanismos de seguridad WLAN, ofrece una solución interoperable y un patrón robusto para asegurar datos. Corrige el sistema de cifrado incompleto WEP del 802.11b. 802.11g: Esta basado en el estándar 802.11b, es capaz de utilizar dos métodos de modulación (DSSS y OFDM). Es capaz de incrementar su velocidad de transmisión llegando hasta los 54Mbps, teniendo características parecidas a 802.11b en cuanto a distancia, nivel de consumo y frecuencia. 802.11b: Es conocido con el nombre de marca registrada Wi-Fi fidelidad inalámbrica (*Wireless Fidelity*). Es un estándar que se ha convertido la tecnología de red inalámbrica dominante que se puede utilizar ampliamente, se puede encontrar en oficinas, espacios públicos y hogares. 802.11n: Permite velocidades mínimas de 100 Mbps y tiene previsto operar en la banda

de frecuencia de los 5 GHz y esto promete rangos superiores en comparación con los estándares superiores, como se puede visualizar en la Ver Tabla 10.

Tabla 10: Estándares

Etiqueta	Referencias
802.11	[29] [34] [35] [38] [41] [42] [44] [69] [70] [73] [77] [79] [86] [90]
802.11a	[46] [51] [56] [70] [112] [113] [114]
802.11ac	[46] [51] [52] [89] [112] [113]
802.11ah	[89]
802.11b	[22] [46] [51] [56] [70] [112] [113] [114]
802.11g	[22] [46] [51] [56] [70] [109] [112] [113] [114]
802.11h	[113]
802.11i	[27] [31] [35] [42] [75] [78] [86] [90] [92] [107]
802.11j	[113]
802.11n	[22] [46] [51] [58] [70] [112] [113] [114]
802.11r	[75]
802.11s	[35]
802.11w	[28] [35] [70] [78]
802.11x	[22] [32] [42] [70] [86] [90]
802.15.4	[40]
802.1x	[3] [27] [75] [88] [94]
IEC 61850	[37]
IEC 62351	[37]
PACP	[37]
RFC 246	[75]
x.805	[20]

En la Figura 6, Matriz de métodos se observa que existen varios métodos que se frecuentan más de tres veces, los cuales se describirán en base a [117], los cuales son: Machine learning (Mtd 20): Es la práctica de usar algoritmos para analizar datos, aprender de ellos, y luego hacer una determinación o predicción sobre algo en el mundo [38]. En [118] implementan este método para ataques phishing utilizando un conjunto de datos para la detección de estos ataques. Y en [79] usan este método para detectar diferentes tipos de actividades de red maliciosas y un estudio de características basado en métodos de clasificación. Y en Neural Networks (Mtd 31): Es un modelo simplificado, que emula el procesamiento de la información. En [114] menciona que el rendimiento y la potencia de la señal WLAN se puede incrementar utilizando técnicas de *Neural Networks, Deep learning* las cuales analizan utilizando el programa *Wi-Fi Monitor*. Y en [93] se dice que el detector de ataques de hombre en el medio denominado Vesper utiliza redes neuronales llamadas autocodificadores para modelar patrones normales de los pulsos con eco y detectar cuando cambia el entorno, además es capaz de detectar ataques MITM con alta precisión sin incurrir en una sobrecarga de red mínima, consiguiendo distinguir el 70% de los dispositivos idénticos, como se puede visualizar en la Tabla 11. Así mismo el anexo 5 contiene más información de la Tabla 11.

Tabla 11: Métodos

Etiqueta	Nombre	Referencia
Mtd 20	Machine learning	[38] [79] [118]
Mtd 31	Neural Networks	[38] [93] [114]

En la Figura 6, Matriz de arquitecturas se pueden visualizar las siguientes arquitecturas que se describirán en base a [119], estos son: DGRU (Arq 1): Su objetivo es recibir un conjunto de datos para la extracción de sus características importantes que serán clasificadas por árboles para generar un vector de información [38]. Evil-Twin Frameworks (Arq 2): Según [73] ayuda a aumentar la eficiencia de una auditoría de penetración de Wi-Fi al integrar cooperativamente las diversas funciones necesarias para realizar la prueba en una sola herramienta que se centran en el análisis de vulnerabilidades en el lado del cliente y lugar. Framework 802.1X (Arq 3): se desarrolló abierto para su implementación en ambos tipos de entornos inalámbricos y LAN cableadas. Básicamente, 802.1X proporciona un modelo de acceso a la red, IEEE 802.1X La autenticación basada se implementa en WLAN a nivel empresarial [107]. MITM Frameworks (Arq 4): Sirve para realizar *pentesting* del ataque *Man in the Middle*. En [59] implementan esta arquitectura utilizando un sistemas operativo Ubuntu con Ettercap demostrando la facilidad de realizar ataque de hombre en el medio donde los objetivos son dos Hosts. MUD (Arq 5): Es un estándar del Grupo de trabajo de ingeniería de Internet (IETF) destinado a describir el comportamiento esperado del dispositivo de IoT mediante listas de control de acceso (ACL), para limitar la comunicación hacia / desde un dispositivo específico [67]. RNN (Arq 6): Conocidas como redes neuronales recurrentes son variantes de las redes neuronales. Fue utilizada para implementar la Arq1 en [38], con ayuda de *Neural Networks*. Sparse auto-encode - SEA (Arq 7): Según [36] es un algoritmo de aprendizaje automático no supervisado que agrega un término de penalización escaso a la red de codificador automático tradicional para extraer características de datos escasos. SEA extrae características de datos escasos a través de una penalización escasa para mejorar la eficiencia y precisión de la extracción de características. X.805 (Arq 8): Define la seguridad inalámbrica de extremo a extremo en siete clasificaciones, que se denominan dimensiones. Este sistema de clasificación permite una identificación clara y conveniente de las amenazas a la seguridad en una red y posibles soluciones a esos problemas [34], como se puede visualizar en la Tabla 12.

Tabla 12: Arquitecturas

Etiqueta	Nombre	Referencias
Arq 1	DGRU	[38]
Arq 2	Evil-Twin Framework	[73]
Arq 3	Framework 802.1X	[107]
Arq 4	MITM framework	[59]
Arq 5	MUD	[67]
Arq 6	RNN	[38]
Arq 7	Sparse auto-encode-SEA	[36]
Arq 8	X.805	[34]

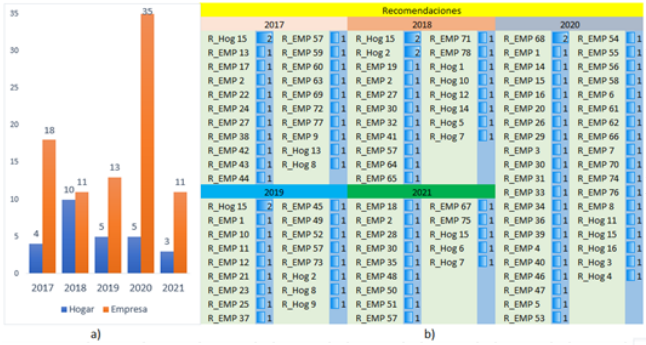

Figura 7: a) Gráfica de recomendaciones de hogares y empresas, b) Matriz de recomendaciones

En la Figura 7, se puede observar que en los ultimos cinco años existen ciertas recomendaciones que tienen una frecuencia mayor a tres, las cuales se dan para brindar seguridad a la red del hogar son: R_Hog 15: Utilizar una contraseña con más de 8 caracteres, combinación de letras mayúsculas y minúsculas, números y caracteres especiales y R_Hog 2: Actualizar el firmware de los dispositivos a la última versión. Y en el caso de las recomendaciones para empresas se tiene una frecuencia entre tres y cuatro veces las cuales son: R_EMP 57: Supervisión, monitoreo, y configuración la red para seguridad ante anomalías, R_EMP 30: Implementar mecanismos de autenticación, R_EMP 2: Asignación dinámica y configuración de direcciones MAC , como se puede visualizar en la Tabla 13. Así mismo el anexo 6 contiene más información de la Tabla 13.

Tabla 13: Recomendaciones

Etiqueta	Nombre	Referencia
Hogar		
R_Hog 2	Actualizar el firmware de los dispositivos a la última versión.	[25] [50] [89]
R_Hog 15	Utilizar una contraseña con más de 8 caracteres, combinación de letras mayúsculas y minúsculas, números y caracteres especiales.	[31] [44] [64] [69] [74] [85] [86] [89]
Empresas		
R_EMP 2	Asignación dinámica y configuración de direcciones MAC.	[26] [41] [85]
R_EMP 30	Implementar mecanismos de autenticación.	[3] [71] [94]
R_EMP 57	Supervisión, monitoreo, y configuración la red para seguridad ante anomalías.	[25] [43] [85] [86]

Herramientas de seguridad: En [17] expresa que existen herramientas (programas y scripts) para la detección de ataques y vulnerabilidades las cuales se dividen en: i) Sistemas Operativos (S.O.): Es un conjunto de programas para el funcionamiento de otros, que sirven para utilizar en ellos herramientas tanto para realizar ataques o vulnerabilidades como herramientas de seguridad, que gestionan los recursos de la computadora y controlan sus actividades. ii) Programas: Sirven para proteger la privacidad de información contenida en un sistema informático. iii) Scripts: Códigos que utilizan una variante de lenguaje para evitar que un atacante pueda realizar operaciones o acceder información de los equipos [95].

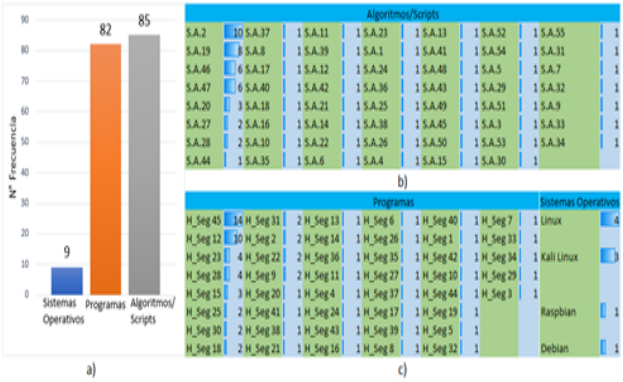

Figura 8: a) N. de Herramientas de seguridad, b) Matriz de Algoritmos/Scripts, c) Matriz de programas de seguridad, d) Matriz de S.O.

En la Figura 8, matriz de S.O. se observa que solo hay cuatro, los cuales se describirán en base a [120], estos son: Linux: Es un sistema operativo de código abierto, esto quiere decir que cualquier persona tiene licencia para modificarlo o distribuirlo sin ningún tipo de problema. Kali Linux, Debian: Es una distribución de Linux compuesta de software libre y de código abierto, desarrollado por el Proyecto apoyada por la comunidad Debian. Y Raspbian: Es un sistema operativo gratuito basado en Debian optimizado para el hardware Raspberry Pi. Un sistema operativo es el conjunto de programas básicos y utilidades que hacen que su Raspberry Pi funcione, como se puede visualizar en la Tabla 7.

En la Figura 8, matriz de programas de seguridad se observa que existen varios programas que se repiten más de cuatro veces, los cuales se describirán en base a [121], estos son: WIRESHARK (H_Seg 45): Tiene la habilidad para determinar no solamente las computadoras activas en la red objetivo, también el sistema operativo, puertos de escucha, servicios, valiéndose del uso de una combinación de comandos y acciones. IDS (H_Seg 12): Es una herramienta usada para la seguridad de sistema informáticos, detecta intrusos los cuales intentan ingresar de manera no autorizada. NMAP (H_Seg 23): Es un programa de código libre para analizar redes y crear auditorías en seguridad. Sirve para gestionar los programas de actualización de servicios o la red y actividad monitorización tiempo real, entre otros. Raspberry pi 3 (H_Seg 28): Es una placa compuesta por varios elementos como un computador en la cual se puede realizar tareas de seguridad de red [120], como se puede visualizar en la Tabla 14. Así mismo el anexo 7 contiene más información de la Tabla 14.

Tabla 14: Programas de seguridad

Etiqueta	Nombre	Referencia
H_Seg 12	IDS	[28] [33] [38] [39] [40] [41] [71] [72] [78] [87]
H_Seg 23	NMAP	[59] [76] [88] [91]
H_Seg 28	Raspberry pi 3	[49] [57] [80] [97]
H_Seg 45	WIRESHARK	[45] [52] [59] [62] [81] [91] [98] [100] [102] [103] [104] [106]

En la Figura 8, Matriz de algoritmos/scripts se observa que existen varios algoritmos que se repiten más de seis veces, los cuales se describirán en base a [122], estos son: AES (S.A.2): Según [35] es un algoritmo de cifrado de bloques que admite entre 128 y 256 claves en secuencias de 32 bits. La longitud de la llave y la longitud del bloque se eligen de forma independiente. Para [46] [50] [52] [88] [105] y [112] el mejor rendimiento se logra con WPA2 con cifrado AES, AES con TSK, CCMP y TKIP, que demuestra mediante experimentos de pruebas inalámbricas, ya que prueba que existe un bajo rendimiento al no tener las seguridades pertinentes. RC4 (S.A.19): Sistema de cifrado más utilizado por algunos protocolos para proteger el tráfico de internet. En [22] [42] [44] [51] [86] y [112] utilizan este cifrado en los protocolos WEP, WPA y TKIP para aumentar la velocidad general de comunicación en comparación de otros cifrados, además utiliza una clave de longitud de 40 a 256 bits. También contiene 24 bits para representar un vector de inicialización que se utiliza para regulación de la transmisión. CCMP (S.A.46): De acuerdo con [108] es el algoritmo más avanzado con controles y protección adicionales, este es un nuevo método para la protección de transmisiones inalámbricas. En [51] [112] definen como un protocolo que utiliza WPA. En [50] realizan un experimento en una red configurada WPA2 PSK con cifrado CCMP donde al utilizar herramientas de ataques descubre la contraseña cifrada . Y por ultimo en algoritmo TKIP (S.A.47): Utiliza la técnica de cifrado RC4 como WEP, a diferencia que antes de que el vector de inicialización entre en el proceso del algoritmo RC4, este se duplica, uno pasa por un hash junto a la clave y el otro es enviado directamente a RC4. En el caso de [46] [88] [108] y [112] realizan un experimento donde analizan el impacto sobre los diferentes mecanismos de cifrado entre ellos es TKIP el cual muestra un rendimiento bajo en comparación a los otros cifrados como AES, como se puede visualizar en la Tabla 15. Así mismo el anexo 8 contiene más información de la Tabla 15.

Tabla 15: Scripts / Algoritmos

Etiqueta	Nombre	Referencia
S.A.2	AES	[26] [35] [45] [46] [50] [52] [88] [105] [106] [112]
S.A.19	RC4	[22] [35] [42] [44] [51] [86] [108] [112]
S.A.42	ICV	[42]
S.A.47	TKIP	[46] [50] [51] [88] [108] [112] [123]

2.5. Etapa 3: Discusión de resultados

2.5.1. Resultados

Después de la recolección de datos y clasificación de la misma como respuestas a las preguntas de SM se obtienen los siguientes resultados.

1. **¿Cuántos artículos se han anunciado en los últimos 5 años?**
   Como se puede visualizar en la Figura 9, se observa que existe un decrecimiento de estudios del 2017 al 2021, siendo el 2018 el año que más artículos de relevancia existen en las bases de datos *IEEE Xplore y Scopus*.

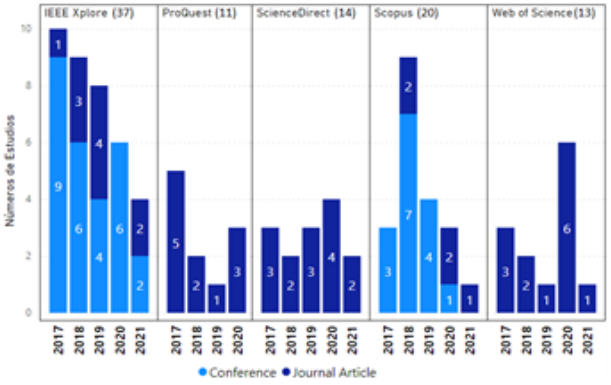

Figura 9: N. de estudios

2. **¿Cuáles son las revistas y conferencias más utilizadas en los últimos cinco años?**
   En la Figura 10, se ven las revistas y conferencias que contienen más de un artículo publicado, entre las cuales existe una frecuencia de tres veces en publicaciones de artículos de las siguientes revistas: *IEEE ACCESS, International Journal of Advanced Research in Computer Science, Procedia Computer Science, Computers Security. Y en el caso de las conferencias existe una en donde se han realizado dos publicaciones que es 2017 International Conference on Engineering Technology and Technopreneurship (ICE2T).*

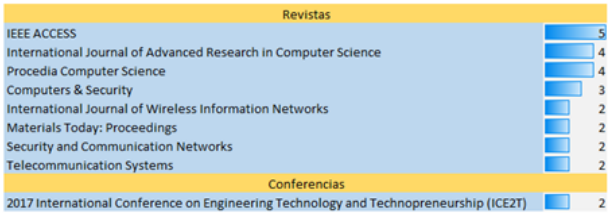

Figura 10: N. de Revistas y conferencias

3. **¿Cuáles son los autores que han aportado más de un artículo en los últimos cinco años?**
   Como visualiza en la Figures 11, en los años 2017 y 2020 se obtuvo un total de cuatro autores que han aportado con un máximo de dos artículos, los cuales son importantes al momento de aportar información.

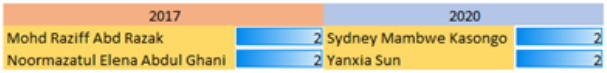

Figura 11: Autores relevantes

4. **¿En qué idiomas se produce la investigación sobre seguridad y vulnerabilidades en redes Wi-Fi?**
   En la Figura 12, se observa que todos los estudios recolectados fueron en el idioma inglés ya que en ellos existe más información.

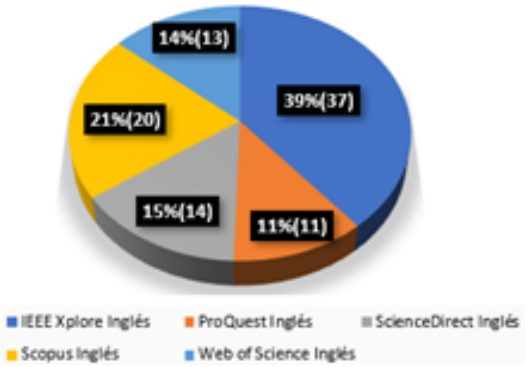

Figura 12: Idiomas de artículos por Revista

Y como respuestas a las preguntas de LSR se obtienen los siguientes resultados.

1. **¿Cuáles son las características de una red Wi-Fi vulnerable?**
   En la Figura 5, se observó tres grupos de vulnerabilidades por factores que ya se habían mencionado que son hardware, software y factor humano que entre los más comunes se obtuvo WPS (HW 5), Hole 196 (SW 16), Acceso no autorizado (FH 1) y Configuración de red predeterminada (FH 4), los cuales ya se habían aludido anteriormente.

2. **¿Cuáles son los protocolos y estándares que mayormente son utilizados?**
   En la Figura 6, se observa que existen protocolos que se repiten más de once veces los cuales ya se habían dicho anteriormente, estos son: *Wired Equivalent Privacy* (WEP), *Wi-Fi Protected Access* (WPA), *Wi-Fi Protected Access 2* (WPA2), *Temporal Key Integrity Protocol* (TKIP). Y en el caso de los estándares que se frecuentan más de ocho veces son: 802.11, 802.11b, 802.11g, 802.11n.

3. **¿Cuáles son los programas de ataques más utilizadas que se emplearon?**
   En la Figura 4, se observan los programas de ataques que se utilizaron y como se había dicho anteriormente las más utilizadas son: *Aircrack-ng* (H_Ataq 3), *Aireplay-ng* (H_Ataq 4), *Airodump-ng* (H_Ataq 6) y *Ettercap* (H_Ataq 15).

4. **¿Cuáles son los programas más utilizados para contrarrestar los ataques informáticos?**
   En la Figura 8, se observan los programas de ataques que se utilizaron y como se había dicho anteriormente las más utilizadas son: WIRESHARK (H_Seg 45), IDS (H_Seg 12), NMAP (H_Seg 23) y Raspberry pi 3 (H_Seg 28).

3. Conclusiones

En este trabajo se ha realizado un estado del arte utilizando mapeo sistemático al igual que revisión de la literatura sistemática con el objetivo de encontrar información relacionada sobre seguridad en redes Wi-Fi domésticas. Esta investigación tomo en cuenta a estudios que fueron publicados entre los años 2017 a 2021. Se conformó de varios procesos los cuales ayudaron a clasificar estudios primarios para el mapeo sistemático con ayuda de cuatro preguntas que fueron esenciales para su clasificación. Así como para los estudios secundarios también se realizaron otras cuatro preguntas de literatura sistemática, además de tomar en cuenta la taxonomía que fue estructurada para la clasificación de la información.

A pesar de que existe diversa información sobre seguridad en redes inalámbricas se encontraron cinco artículos que hablaban directamente sobre ataques, vulnerabilidades y seguridades que puede haber en las red inalámbricas del hogar. Estos artículos son [47] [50] [67] [68] y [74] los cuales tienen varias características en común como son protocolos, vulnerabilidades, métodos, herramientas.

En el caso de las vulnerabilidades que pueden existir para las redes domesticas podemos encontrar diferentes características que son: interfaces de usuario no fiables, ausencia de registros apropiados, explotación de vulnerabilidades, ausencia de mecanismos de autenticación, *dragonblood* (robo de contraseñas) y configuración de red predeterminada. Esto indica que existen personas con falta de interés sobre la seguridad de la red, no tienen información suficiente o no son capaces de realizar una configuración adecuada para tratar de evitar estas vulnerabilidades que son las más comunes en una red Wi-Fi doméstica.

Con respecto a las soluciones que se pueden utilizar para tener una red Wi-Fi más segura es actualizar dispositivos de red o sistemas operativos, actualizar el *firmware* en la última versión y utilizar contraseñas con más de 8 caracteres, combinando letras mayúsculas, minúsculas, números y caracteres especiales. Además, se pueden emplear diferentes herramientas como *Iperf* que sirve para el diagnóstico de problemas en la velocidad de la red, en el caso de protocolos se pueden implementar AES, ICMP, UDP TKIP, DHCP, SSH, WPA y WPA2. Así como aplicar códigos *hyperledger* y scripts *Paramiko*.

Finalmente, como se pudo evidenciar no existe una estructura determinada para realizar un mapeo sistemático junto con la revisión literaria sistemática, solo existen procesos de similitud. Al revisar los estudios seleccionados por mapeo sistemático se observó que no todos tenían los parámetros necesarios para realizar una revisión sistemática, por este motivo se separaron los artículos que no contenían los parámetros necesarios para la revisión literaria sistemática con respecto a vulnera-

bilidades y seguridades en la red Wi-Fi. Además, que la mayoría de los estudios seleccionados se centraron empresas por tener un mayor grado de riesgo que los hogares.

Referencias

[1] E. Nasr, M. Jalloul, J. Bachalaany, and R. Maalouly, "Wi-fi network vulnerability analysis and risk assessment in lebanon," *MATEC Web of Conferences*, vol. 281, p. 05002, 2019. [Online]. Available: https://doi.org/10.1051/matecconf/201928105002

[2] I. P. F. A. A. Lesta, "Fundamentos y aplicaciones de seguridad en redes wlan : de la teoria a la practica," *MARCOMBO S.A.*, 2006.

[3] P. Kumar, "Issues and concerns in entity authentication in wireless local area networks (wlans)," *International Journal of Advanced Research in Computer Science*, vol. 9, no. 2, pp. 834–838, 2018. [Online]. Available: http://www.ijarcs.info/index.php/Ijarcs/article/view/5829

[4] M. C. E. Apráez, "Análisis de vulnerabilidades de la red inalámbrica para evitar la inseguridad de la información de los usuarios de la fisei de la uta." Ph.D. dissertation, UNIVERSIDAD TÉCNICA DE AMBATO, apr 2013.

[5] I. N. de Estadística y Censos, "Tecnologías de la información y comunicación-tic." [Online]. Available: https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/

[6] P. A. López, *Seguridad informática*, 07 2021.

[7] G. Urbina, *Introduccion a la seguridad informatica*. Mexico D.F: Grupo Editorial Patria, 2016.

[8] S. M. Q.-Z. y David G. Macías-Valencia, "Seguridad en informática: consideraciones," *Dominio de las Ciencias*, vol. 3, no. 3 mon, pp. 676–688, 2017. [Online]. Available: https://dominiodelasciencias.com/ojs/index.php/es/article/view/663

[9] C. A. C. . I. SECURITY. (2015) Security tip (st15-002). [Online]. Available: https://us-cert.cisa.gov/ncas/tips/ST15-002#:~:text=What%20is%20home%20network%20security,the%20internet%20within%20a%

[10] Y. kyung Lee, H. il Ju, D. woo Kim, and J. wook Han, "Home network modelling and home network user authentication mechanism using biometric information," in *2006 IEEE International Symposium on Consumer Electronics*, 2006, pp. 1–5.

[11] R. A. Khan, S. U. Khan, H. U. Khan, and M. Ilyas, "Systematic mapping study on security approaches in secure software engineering," *IEEE Access*, vol. 9, pp. 19 139–19 160, 2021.

[12] Y. Miyashita, T. Tanaka, and A. Hazeyama, "Systematic literature review regarding communication support in project-based learning of software development," 07 2018, pp. 781–782.

[13] D. Carrizo and J. Rojas, "MetodologÃas, tÃy herramientas en ingenierÃa de requisitos: un mapeo sistemÃ¡tico," *Ingeniare. Revista chilena de ingenierÃa*, vol. 26, pp. 473 – 485, 00 2018. [Online]. Available: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-33052018000300473&nrm=iso

[14] "What is a picoc?" [Online]. Available: https://cebma.org/faq/what-is-a-picoc/

[15] D. X. Jara Juárez, "Propuesta metodológica de evaluación de seguridad para aplicaciones de mobile cloud computing," Jan 1970. [Online]. Available: http://dspace.ucuenca.edu.ec/handle/123456789/28279

[16] C. J. C. Montealegre, D. N. Bayona, and Z. Ortiz Bayona, "Extensión de taxonomía y tratamiento de valores faltantes sobre un repositorio de incidentes de seguridad informática," *Ingeniería*, vol. 18, no. 1, jun. 2013. [Online]. Available: https://revistas.udistrital.edu.co/index.php/reving/article/view/4894

[17] M. I. R. Castro, G. L. F. Morán, D. S. V. Navarrete, J. E. Álava Cruzatty, G. R. P. Anzúles, C. J. Álava Mero, Ángel Leonardo Murillo Quimiz, and M. A. C. Merino, *Introducción a la seguridad informática y el análisis de vulnerabilidades*. Editorial Científica 3Ciencias, oct 2018. [Online]. Available: https://doi.org/10.17993%2Fingytec.2018.46

[18] Álvaro Gómez Vieites, "Tipos de ataques e intrusos en las redes informÁticas," *Edisa*, aug 2014.

[19] L. J. Cañon Parada, "Ataques informáticos, ethical hacking y conciencia de seguridad informática en niños." Ph.D. dissertation, 2015. [Online]. Available: https://login.unipiloto.basesdedatosezproxy.com/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cat06403a&AN=uni.34703&lang=es&site=eds-live

[20] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in internet of things," *Future Generation Computer Systems*, vol. 100, pp. 144–164, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X19304194

[21] B. Benadda, M. Elgorma, and B. Beldjilali, "Embedded beaglebone based wi-fi intrusions detector and vulnerabilities checker," 2017, cited By 2. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85018708401&doi=10.1109%2fDAT.2017.7889183&partnerID=40&md5=0b200b493f53b2830e19d4f34a97bdb0

[22] P. Jindal and B. Singh, "Quantitative analysis of the security performance in wireless lans," *JOURNAL OF KING SAUD UNIVERSITY-COMPUTER AND INFORMATION SCIENCES*, vol. 29, no. 3, pp. 246–268, JUL. [Online]. Available: https://doi.org/10.1016/j.jksuci.2014.12.012

[23] A. Pradhan and R. Mathew, "Solutions to vulnerabilities and threats in software defined networking (sdn)," *Procedia Computer Science*, vol. 171, pp. 2581–2589, 2020, third International Conference on Computing and Network Communications (CoCoNet'19). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050920312734

[24] S. Hashemi and M. Zarei, "Internet of things backdoors: Resource management issues, security challenges, and detection methods," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, 2021, cited By 1. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85092407557&doi=10.1002%2fett.4142&partnerID=40&md5=aab2c1a4bb1b788d23c77196e3dfb475

[25] F. Aftab, S. Suntu, and Z. Zhang, "Self-organized security framework for wigig wlan against attacks and threats," 2018, pp. 249–253, cited By 3. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85056377551&doi=10.1109%2fICCSN.2018.8488316&partnerID=40&md5=150918ab2d7357a254d26b370e0a7d93

[26] E. Letsoalo and S. Ojo, "Session hijacking attacks in wireless networks: A review of existing mitigation techniques," 2017, cited By 0. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85043299339&doi=10.23919%2fISTAFRICA.2017.8102284&partnerID=40&md5=07dc26370ab73d6cb128e767ea431c04

[27] M. Abo-Soliman and M. Azer, "A study in wpa2 enterprise recent attacks," vol. 2018-January, 2018, pp. 323–330, cited By 7. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046647191&doi=10.1109%2fICENCO.2017.8289808&partnerID=40&md5=7a6c27cf9d8e5c5d478a2d396e58e1dd

[28] A. Seth, S. Biswas, and A. Dhar, "De-authentication attack detection using discrete event systems in 802.11 wi-fi networks," vol. 2019-December, 2019, cited By 0. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85087272242&doi=10.1109%2fANTS47819.2019.9118100&partnerID=40&md5=2f7fbe131e0db985b9551ddf621e0749

[29] Y. Chahid, M. Benabdellah, and A. Azizi, "Internet of things protocols comparison, architecture, vulnerabilities and security: State of the art," 2017, cited By 1. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85049613245&doi=10.1145%2f3167486.3167554&partnerID=40&md5=76a2a597649b1f1d8c6994bd6c00ee12

[30] V. Rajavel and G. Aloy Anuja Mary, "Design of wireless intrusion detection system for dos attack and malicious access point in wi-fi networks," *Journal of Critical Reviews*, vol. 7, no. 6, pp. 782–788, 2020, cited By 0. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85084202799&doi=10.31838%2fjcr.07.06.136&partnerID=40&md5=0f37d2d6af56d2062fc9c772d83b6955

[31] S. Simbana, G. Lopez, C. Tipantuna, and F. Sanchez, "Vulnerability analysis toolkit for ieee 802.11 wireless networks: A practical approach," vol. 2018-December, 2018, pp. 227–232, cited By 1. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85063221292&doi=10.1109%2fINCISCOS.2018.00040&partnerID=40&md5=412cccd799ff0d9a1377363f12f1e109

[32] Suroto, "Wlan security: Threats and countermeasures," *International Journal on Informatics Visualization*, vol. 2, no. 4, pp. 232–238, 2018, cited By 1. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85099054366&doi=10.30630%2fjoiv.2.4.133&partnerID=40&md5=e0640cfe9f36c9886ca7856ba5458029

[33] A. K. Shukla, "An efficient hybrid evolutionary approach for identification of zero-day attacks on wired/wireless network system," *WIRELESS PERSONAL COMMUNICATIONS*. [Online]. Available: https://doi.org/10.1007/s11277-020-07808-y

[34] D. Hurley-Smith, J. Wetherall, and A. Adekunle, "Superman: Security using pre-existing routing for mobile ad hoc networks," *IEEE TRANSACTIONS ON MOBILE COMPUTING*, vol. 16, no. 10, pp. 2927–2940, OCT 1. [Online]. Available: https://doi.org/10.1109/TMC.2017.2649527

[35] C. P. Kohlios and T. Hayajneh, "A comprehensive attack flow model and security analysis for wi-fi and wpa3," *ELECTRONICS*, vol. 7, no. 11, NOV. [Online]. Available: https://doi.org/10.3390/electronics7110284

[36] X. Han, Y. Liu, Z. Zhang, X. Lü, and Y. Li, "Sparse auto-encoder combined with kernel for network attack detection," *Computer Communications*, vol. 173, pp. 14–20, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366421000992

[37] L. E. da Silva and D. V. Coury, "A new methodology for real-time detection of attacks in iec 61850-based systems," *Electric Power*

Systems Research, vol. 143, pp. 825–833, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378779616303236

[38] S. M. Kasongo and Y. Sun, "A deep gated recurrent unit based model for wireless intrusion detection system," *ICT Express*, vol. 7, no. 1, pp. 81–87, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959519303224

[39] ——, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," *Computers Security*, vol. 92, p. 101752, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404820300365

[40] R. Faqihi, J. Ramakrishnan, and D. Mavaluru, "An evolutionary study on the threats, trust, security, and challenges in siot (social internet of things)," *Materials Today: Proceedings*, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214785320373430

[41] J. O. Agyemang, J. J. Kponyo, G. S. Klogo, and J. O. Boateng, "Lightweight rogue access point detection algorithm for wifi-enabled internet of things(iot) devices," *Internet of Things*, vol. 11, p. 100200, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660518301501

[42] Y. Asimi, A. Asimi, A. Guezzaz, Z. Tbatou, and Y. Sadqi, "Unpredictable cryptographic primitives for the robust wireless network security," *Procedia Computer Science*, vol. 134, pp. 316–321, 2018, the 15th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2018) / The 13th International Conference on Future Networks and Communications (FNC-2018) / Affiliated Workshops. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050918311438

[43] D. Upadhyay and S. Sampalli, "Scada (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations," *Computers Security*, vol. 89, p. 101666, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404819302068

[44] T. Mekhaznia and A. Zidani, "Wi-fi security analysis," *Procedia Computer Science*, vol. 73, pp. 172–178, 2015, international Conference on Advanced Wireless Information and Communication Technologies (AWICT 2015). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050915034705

[45] F. W. Sarjana, T. Yuliar Arif, R. Adriman, and R. Munadi, "Simple prevention of advanced stealth man-in-the-middle attack in wpa2 wi-fi networks," in *2019 International Conference on Electrical Engineering and Computer Science (ICECOS)*, 2019, pp. 349–353.

[46] S. Lepaja, A. Maraj, I. Efendiu, and S. Berzati, "The impact of the security mechanisms in the throughput of the wlan networks," in *2018 7th Mediterranean Conference on Embedded Computing (MECO)*, 2018, pp. 1–5.

[47] E. Lamers, R. Dijksman, A. van der Vegt, M. Sarode, and C. de Laat, "Securing home wi-fi with wpa3 personal," in *2021 IEEE 18th Annual Consumer Communications Networking Conference (CCNC)*, 2021, pp. 1–8.

[48] S. Kwon and H.-K. Choi, "Evolution of wi-fi protected access: Security challenges," *IEEE Consumer Electronics Magazine*, vol. 10, no. 1, pp. 74–81, 2021.

[49] A. Ilovan and B. Iancu, "Penetration testing solution for wireless networks using mobile devices," in *2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, 2018, pp. 1–6.

[50] Z. Akram, M. A. Saeed, and M. Daud, "Real time exploitation of security mechanisms of residential wlan access points," in *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 2018, pp. 1–5.

[51] P. Satam and S. Hariri, "Wids: An anomaly based intrusion detection system for wi-fi (ieee 802.11) protocol," *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 1077–1091, 2021.

[52] K. McHugh, W. Akpedeye, and T. Hayajneh, "Next generation wireless-lan: Security issues and performance analysis," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, 2017, pp. 1–7.

[53] A. Kavianpour and M. C. Anderson, "An overview of wireless network security," in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 2017, pp. 306–309.

[54] I. Hossain, M. M. Hasan, S. Faisal Hasan, and M. R. Karim, "A study of security awareness in dhaka city using a portable wifi pentesting device," in *2019 2nd International Conference on Innovation in Engineering and Technology (ICIET)*, 2019, pp. 1–6.

[55] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, and Z. Han, "Applications of economic and pricing models for wireless network security: A survey," *IEEE Communications Surveys Tutorials*, vol. 19, no. 4, pp. 2735–2767, 2017.

[56] S.-H. Choi, D.-H. Hwang, and Y.-H. Choi, "Wireless intrusion prevention system using dynamic random forest against wireless mac spoofing attack," in *2017 IEEE Conference on Dependable and Secure Computing*, 2017, pp. 131–137.

[57] E. Basan, M. Medvedev, and S. Teterevyatnikov, "Analysis of the impact of denial of service attacks on the group of robots," in *2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2018, pp. 63–638.

[58] J. Villain, V. Deniau, A. Fleury, E. P. Simon, C. Gransart, and R. Kousri, "Em monitoring and classification of iemi and protocol-based attacks on ieee 802.11n communication networks," *IEEE Transactions on Electromagnetic Compatibility*, vol. 61, no. 6, pp. 1771–1781, 2019.

[59] Sudhakar and R. K. Aggarwal, "A survey on comparative analysis of tools for the detection of arp poisoning," in *2017 2nd International Conference on Telecommunication and Networks (TEL-NET)*, 2017, pp. 1–6.

[60] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3044–3056, 2019.

[61] Y. Jie, M. Li, C. Guo, and L. Chen, "Dynamic defense strategy against dos attacks over vehicular ad hoc networks based on port hopping," *IEEE Access*, vol. 6, pp. 51 374–51 383, 2018.

[62] H. Singh and J. Singh, "Penetration testing in wireless networks," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 2213–2216, 05 2017.

[63] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, "Physical layer security schemes for mimo systems: an overview," *Wireless Networks*, 2020.

[64] N. Pimple, T. Salunke, U. Pawar, and J. Sangoi, "Wireless security - an approach towards secured wi-fi connectivity," 2020, pp. 872–876, cited By 2. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85084652655&doi=10.1109%2fICACCS48705.2020.9074350&partnerID=40&md5=0d5775e1eaec696762cd85fec5a3454c

[65] B. Pingle, A. Mairaj, and A. Javaid, "Real-world man-in-the-middle (mitm) attack implementation using open source tools for instructional use," vol. 2018-May, 2018, pp. 192–197, cited By 3. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85057086896&doi=10.1109%2fEIT.2018.8500082&partnerID=40&md5=fa314f766971d35c2377d21e01a491ce

[66] R. Vishwakarma and A. K. Jain, "A survey of ddos attacking techniques and defence mechanisms in the iot network," *TELECOMMUNICATION SYSTEMS*, vol. 73, no. 1, pp. 3–25, JAN. [Online]. Available: https://doi.org/10.1007/s11235-019-00599-z

[67] S. M. Sajjad, M. Yousaf, H. Afzal, and M. R. Mufti, "emud: Enhanced manufacturer usage description for iot botnets prevention on home wifi routers," *IEEE ACCESS*, vol. 8, pp. 164 200–164 213, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.3022272

[68] Y. Tushir, B.and Dalal, B. Dezfouli, and Y. H. Liu, "A quantitative study of ddos and e-ddos attacks on wifi smart home devices," *IEEE INTERNET OF THINGS JOURNAL*, vol. 8, no. 8, pp. 6282–6292, APR 15. [Online]. Available: https://doi.org/10.1109/JIOT.2020.3026023

[69] Z. Belghazi, N. Benamar, A. Addaim, and C. A. Kerrache, "Secure wifi-direct using key exchange for iot device-to-device communications in a smart environment," *FUTURE INTERNET*, vol. 11, no. 12, DEC. [Online]. Available: https://doi.org/10.3390/fi11120251

[70] H. Mahini and S. M. Mousavirad, "Wifi intrusion detection and prevention systems analyzing: A game theoretical perspective," *INTERNATIONAL JOURNAL OF WIRELESS INFORMATION NETWORKS*, vol. 27, no. 1, pp. 77–88, MAR. [Online]. Available: https://doi.org/10.1007/s10776-019-00474-3

[71] M. I. Al-Ghamdi, "Effects of knowledge of cyber security on prevention of attacks," *Materials Today: Proceedings*, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214785321029941

[72] A. Aldaej, "Enhancing cyber security in modern internet of things (iot) using intrusion prevention algorithm for iot (ipai)," *IEEE Access*, pp. 1–1, 2019.

[73] A. Esser and C. Serrao, "Wi-fi network testing using an integrated evil-twin framework," 2018, pp. 216–221, cited By 2. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85059990050&doi=10.1109%2fIoTSMS.2018.8554388&partnerID=40&md5=9ee56264d9aaae6ede8a47fe6752e062

[74] D. Fehér and B. Sándor, "Effects of the wpa2 krack attack in real environment," 2018, pp. 239–242, cited By 7. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85057969520&doi=10.1109%2fSISY.2018.8524769&partnerID=40&md5=6800e81b05095cc7e6ed3231feedfbda

[75] M. Abo-Soliman, "Enterprise wlan security flaws current attacks and relative mitigations," 2018, cited By 0. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85055248869&doi=10.1145%2f3230833.3230836&partnerID=40&md5=a37f61c7e8dd2b3f6c17b936defcc21c

[76] K. Sinchana, C. Sinchana, H. Gururaj, and B. Sunil Kumar, "Performance evaluation and analysis of various network security tools," 2019, pp. 644–650, cited By 0. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85081158121&doi=10.1109%2fICCES45898.2019.9002531&partnerID=40&md5=80a0ab24228217552b2602e4c5365438

[77] M. Agarwal, S. Biswas, and S. Nandi, "An efficient scheme to detect evil twin rogue access point attack in 802.11 wi-fi networks," *International Journal of Wireless Information Networks*, vol. 25, no. 2, pp. 130–145, 2018, cited By 14. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85044515390&doi=10.1007%2fs10776-018-0396-1&partnerID=40&md5=2291b8b96eb1c169a577626109cd020d

[78] A. D. A, A. K. Mohan, and S. M, "Wireless security auditing: Attack vectors and mitigation strategies," *Procedia Computer Science*, vol. 115, pp. 674–682, 2017, 7th International Conference on Advances in Computing Communications, ICACC-2017, 22-24 August 2017, Cochin, India. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050917319853

[79] A. Rizzi, G. Granato, and A. Baiocchi, "Frame-by-frame wi-fi attack detection algorithm with scalable and modular machine-learning design," *Applied Soft Computing*, vol. 91, p. 106188, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1568494620301289

[80] E. Al Neyadi, S. Al Shehhi, A. Al Shehhi, N. Al Hashimi, M. Qbea'H, and S. Alrabaee, "Discovering public wi-fi vulnerabilities using raspberry pi and kali linux," in *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*, 2020, pp. 1–4.

[81] S. A. Noman, M. Qasaimeh, R. Al-Qassas, and H. A. Noman, "Mitigating evil twin attacks in wireless 802.11 networks at jordan," *International Journal of Computer Science Issues (IJCSI)*, vol. 14, no. 1, pp. 60–68, 01 2017.

[82] V. Modi and C. Parekh, "Detection analysis of evil twin attack in wireless network," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 774–777, 05 2017.

[83] Q. Lu, H. Qu, Y. Ouyang, and J. Zhang, "Slfat: Client-side evil twin detection approach based on arrival time of special length frames," *Security and Communication Networks*, vol. 2019, p. 10, 2019.

[84] A. Bartoli, E. Medvet, and F. Onesti, "Evil twins and wpa2 enterprise: A coming security disaster?" *Computers Security*, vol. 74, pp. 1–11, 2018.

[85] H.-J. Lu and Y. Yu, "Research on wifi penetration testing with kali linux," *Complexity*, vol. 2021, 2021, cited By 0. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85102282168&doi=10.1155%2f2021%2f5570001&partnerID=40&md5=0655b6ab271204f826981c7e8c82ba2c

[86] R. Kalnins, J. Purins, and G. Alksnis, "Security evaluation of wireless network access points," *APPLIED COMPUTER SYSTEMS*, vol. 21, no. 1, pp. 38–45, MAY. [Online]. Available: https://doi.org/10.1515/acss-2017-0005

[87] I. Ghafir, K. G. Kyriakopoulos, F. J. Aparicio-Navarro, S. Lambotharan, B. Assadhan, and H. Binsalleeh, "A basic probability assignment methodology for unsupervised wireless intrusion detection," *IEEE Access*, vol. 6, pp. 40 008–40 023, 2018.

[88] H. Huang, Y. Hu, Y. Ja, and S. Ao, "A whole-process wifi security perception software system," in *2017 International Conference on Circuits, System and Simulation (ICCSS)*, 2017, pp. 151–156.

[89] H. Valchanov, J. Edikyan, and V. Aleksieva, "An empirical study of wireless security in city environment," 2019, cited By 0. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85073344344&doi=10.1145%2f3351556.3351563&partnerID=40&md5=65fc563f0ee795c24de9171b26cb9ac7

[90] M. Vondracek, J. Pluskal, and O. Rysavy, "Automated man-in-the-middle attack against wi-fi networks," *JOURNAL OF DIGITAL FORENSICS SECURITY AND LAW*, vol. 13, no. 1, pp. 59–80, 2018.

[91] A. Idiyatullin and P. E. Abdulkin, "A research of mitm attacks in wi-fi networks using single-board computer," in *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, 2021, pp. 396–400.

[92] J. Noh, J. Kim, and S. Cho, "Secure authentication and four-way handshake scheme for protected individual communication in public wi-fi networks," *IEEE Access*, vol. 6, pp. 16 539–16 548, 2018.

[93] Y. Mirsky, N. Kalbo, Y. Elovici, and A. Shabtai, "Vesper: Using echo analysis to detect man-in-the-middle attacks in lans," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1638–1653, 2019.

[94] T. Perković, A. Dagelić, M. Bugarić, and M. Čagalj, "On wpa2-enterprise privacy in high education and science," *Security and Communication Networks*, 2020.

[95] M. Olvera, *Fundamentos de computacion para ingenieros*. City: Larousse - Grupo Editorial Patria, 2000.

[96] M. J. García Álvarez, "Diagnóstico de vulnerabilidad de la infraestructura de telecomunicaciones facultad de ingeniería industrial de la universidad de guayaquil." Ph.D. dissertation, UNIVERSIDAD DE GUAYAQUIL FACULTAD DE INGENIERÍA INDUSTRIAL DEPARTAMENTO ACADÉMICO DE GRADUACIÓN, may 2017.

[97] K. Juhász, V. Póser, M. Kozlovszky, and A. Bánáti, "Wifi vulnerability caused by ssid forgery in the ieee 802.11 protocol," in *2019 IEEE 17th World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, 2019, pp. 333–338.

[98] R. Singh and S. Kumar, "A comparative study of various wireless network monitoring tools," in *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, 2018, pp. 379–384.

[99] M. R. Abd Razak, T. A. T. Aziz, and N. E. A. Ghani, "The performance of wi-fi protected access 2 on 2.4ghz wlan network," in *2017 International Conference on Engineering Technology and Technopreneurship (ICE2T)*, 2017, pp. 1–6.

[100] J. Pokorny, R. Fujdiak, M. Kovanda, M. Strajt, and J. Hosek, "Traffic analysis of ieee 802.11 on physical layer by using software defined radio," in *2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, 2020, pp. 78–81.

[101] A. Abdelrahman, H. Khaled, E. Shaaban, and W. S. Elkilani, "Detailed study of wlan psk cracking implementation," in *2020 15th International Conference on Computer Engineering and Systems (ICCES)*, 2020, pp. 1–6.

[102] S. Raj and N. K. Walia, "A study on metasploit framework: A pen-testing tool," in *2020 International Conference on Computational Performance Evaluation (ComPE)*, 2020, pp. 296–302.

[103] R. Bijral, A. Gupta, and S. S. Lalit, "Study of vulnerabilities of arp spoofing and its detection using snort," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 2074–2077, 05 2017.

[104] B. Van Leeuwen, J. Eldridge, and V. Urias, "Cyber analysis emulation platform for wireless communication network protocols," in *2017 International Carnahan Conference on Security Technology (ICCST)*, 2017, pp. 1–6.

[105] T. Aziz, M. R. Abd Razak, and N. E. A. Ghani, "The performance of different ieee802.11 security protocol standard on 2.4ghz and 5ghz wlan networks," in *2017 International Conference on Engineering Technology and Technopreneurship (ICE2T)*, 2017, pp. 1–7.

[106] J. Guo, M. Wang, H. Zhang, and Y. Zhang, "A secure session key negotiation scheme in wpa2-psk networks," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, 2020, pp. 1–6.

[107] P. Kumar and D. Kumar, "A secure n-secret based client authentication protocol for 802.11 wlans," *Telecommun Syst*, p. 259–271, 2020.

[108] A. V. Anastasia, S. V. Zareshin, I. S. Rumyantseva, and V. G. Ivanenko, "Analysis of security of public access to wi-fi networks on moscow streets," in *2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 2017, pp. 105–110.

[109] H. Valchanov, J. Edikyan, and V. Aleksieva, "A study of wi-fi security in city environment," vol. 618, no. 1, 2019, cited By 0. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85076086492&doi=10.1088%2f1757-899X%2f618%2f1%2f012031&partnerID=40&md5=f42e15e8f7de806ec8d9551b36e398a4

[110] A. Tanenbaum, *Redes de computadoras*. Mexico: Pearson Educacion, 2003.

[111] C. H. Suárez, I. Páez, and D. A. G. Ramírez, "Modelo AHP-VIKOR para handoff espectral en redes de radio cognitiva," *Revista Tecnura*, vol. 19, no. 45, p. 29, jul 2015. [Online]. Available: https://doi.org/10.14483%2Fudistrital.jour.tecnura.2015.3.a02

[112] P. K. Pant, "The impact of sgi and rts/cts in wlan throughput," in *2020 International Conference on Intelligent Engineering and Management (ICIEM)*, 2020, pp. 207–211.

[113] C. L. Leca, "Overview of romania 802.11wireless security statistics," *EAI Endorsed Transactions on Security and Safety*, vol. 4, no. 12, 12 2017.

[114] P. Dhere, P. Chilveri, R. Vatti, V. Iyer, and K. Jagdale, "Wireless signal strength analysis in a home network," in *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, 2018, pp. 1–5.

[115] L. Antipova and A. Borisov, "Development and research self-organizing network based on protocol ieee 802.11 wi-fi," in *2019 International Science and Technology Conference "EastConf"*, 2019, pp. 1–4.

[116] A. C. O. O. y Wilson Medardo Pancho Males, "Análisis y diseño de una wlan 802.11," Ph.D. dissertation, Escuela Politécnica Nacional Facultad de Ingeniería en Sistemas Informáticos y de Computación (FIS), sep 2006.

[117] A. F. Khatiboun, "Machine learning en ciberseguridad," Ph.D. dissertation, Universidad Abierta de Cataluña, jun 2019.

[118] A. K. Ghazi-Tehrani and H. N. Pontell, "Phishing evolves: Analyzing the enduring cybercrime," *VICTIMS & OFFENDERS*, vol. 16, no. 3, pp. 316–342, APR 3. [Online]. Available: https://doi.org/10.1080/15564886.2020.1829224

[119] J. G. Otero and L. M. Galán, "Arquitectura de seguridad para la comunicación de agentes," *Dialnet*, 2019.

[120] C. M. Alonso, "Seguridad informática en el sistema operativo linux en sus diversas distribuciones aplicadas a las tecnologías de la información." 1992-08-28. [Online]. Available: https://repository.unad.edu.co/handle/10596/40342

[121] M. E. Narváez Portillo, "Análisis de la distribución kali linux, su aplicación en la configuración de un sistema detector de intrusiones y la validación del sistema en la red de datos de la sede sur de quito de la universidad politécnica salesiana," B.S. thesis, 2015.

[122] H. D. S. Losada, "Comparación de métodos criptograficos para la seguridad informática," Ph.D. dissertation, UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD ESCUELA DE CIENCIAS BÁSICAS DE TECNOLOGÍA E INGENIERÍA. ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA, 2019.

[123] A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "Cyber-physical attack vulnerabilities in manufacturing quality control tools," *QUALITY ENGINEERING*, vol. 32, no. 4, pp. 676–692, OCT 1. [Online]. Available: https://doi.org/10.1080/08982112.2020.1737115