Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Creación de un sistema para mitigación de ataques tipo *Spoofing* en dispositivos y redes inalámbricas.

Ballardo Collado Ramírez

Noviembre, 2021

Declaratoria de derechos de derechos de autor

Agradecimientos

Profesor tutor Dennis Durán Céspedes:

Por permitirme y guiarme a expandir los límites de mi investigación innumerables veces y para poder obtener el mejor resultado en el proyecto, con su amplio conocimiento que tiene en esta área.

Lector Carlos Jiménez Camacho:

Le agradezco por todos los años de apoyo, consejos y guía, tanto a nivel profesional como personal para poder crecer como persona y como ingeniero y por siempre estar dispuesto a ayudar con total disposición. Muchas gracias por ayudarme a seguir en la lucha.

La familia:

Agradezco a mi Mamá y mi Papá por todo el apoyo en todo lo que podían, la paciencia y comprensión en todos los momentos que necesitaba y por impulsarme a siempre seguir adelante y ser el mejor ejemplo de cómo nunca rendirse importar las dificultades que la vida interpusiera y llegar a ser una mejor persona cada día. A mi novia Paula, por toda su paciencia durante el proceso, los innumerables consejos y todo su apoyo y amor de inicio a fin de este trabajo.

universidad cenfotec_
tecnologías digitales

Universidad Cenfotec
Carrera de Postgrado
Maestría en Ciberseguridad

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Collado Ramírez Ballardo.**

DENNIS ALONSO DURAN CESPEDES (FIRMA)

Firmado digitalmente por DENNIS ALONSO DURAN CESPEDES (FIRMA)
DN: SERIALNUMBER=CPF-01-1029-0075, SN=DURAN CESPEDES, G=DENNIS ALONSO, C=CR, OI=PERSONA FISICA, OU=CIUDADANO, CN=DENNIS ALONSO DURAN CESPEDES (FIRMA)
Razón: Soy el autor de este documento
Ubicación: la ubicación de su firma aquí
Fecha: 2021.11.04 20:01:03-06'00'
Foxit PDF Reader Versión: 11.1.0

M. Sc. Dennis Durán Céspedes
Tutor

CARLOS ENRIQUE JIMENEZ CAMACHO (FIRMA)

Firmado digitalmente por CARLOS ENRIQUE JIMENEZ CAMACHO (FIRMA)
Fecha: 2021.11.05 08:40:10 -06'00'

M. Sc. Carlos Jiménez Camacho
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)

Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA)
Fecha: 2021.11.05 11:41:10 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 04 de noviembre de 2021

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

Tabla de Contenido

Abstract

En la actualidad, cuando muchos empleados se han visto forzados a tomar una modalidad de trabajo remoto, toda la seguridad de sus redes recae en sus hogares o centros de reunión, la cual suele ser básica y fácil de evadir para un ataque de *Wifi Spoofing,* el cual imita a un AP legítimo para que los clientes se conecten de forma desapercibida. Debido a ello, en este trabajo se busca investigar los mecanismos de mitigación existentes y desarrollar un sistema que permita cubrir las vulnerabilidades descubiertas en muchos de los dispositivos existentes.

Esto se desarrolla por medio de la amplia investigación de técnicas, mecanismos, protocolos, para identificar la mejor protección a los clientes conectados a redes wifi, lo que da como resultado que solamente dispositivos con sistemas Android y Windows permiten el desarrollo de una propuesta ya para cualquier dispositivo de Apple las librerías se encuentran limitadas en casi su totalidad, por las medidas de seguridad de este y para Linux se cuenta con medidas de muy buena calidad para la mitigación de este ataque con EvilAP_Defender y Kismet. Con el nuevo sistema para la mitigación de los dispositivos Android y Windows se demuestra tener una alta efectividad para detectar y alertar al usuario final de la amenaza.

Palabras clave: Wifi Spoofing, 802.11, AP, ETA, Wifi, pentesting, Metodología de Ciencia de Diseño, alcances, limitaciones.

Capítulo 1. Introducción

1.1 Generalidades

Con la situación actual en el mundo, cuando una gran cantidad de empresas han cambiado a una modalidad de trabajo remoto, muchos de sus empleados se exponen a las medidas de seguridad con que cuenten en sus hogares, las cuales no suelen ser tan sofisticadas como en su lugar de trabajo, lo cual los expone a este tipo de ataque.

1.2 Antecedentes del problema

La necesidad de contar con accesibilidad a redes inalámbricas para muchos de los dispositivos crece exponencialmente cada año, pero las mejoras de seguridad a la tecnología y protocolos que lo soportan no han mejorado al mismo ritmo, muchas empresas deben invertir recursos adicionales para proteger dichas redes, por lo que resulta muy sencillo para atacantes en zonas públicas, como aeropuertos, cafeterías y centro comerciales robar información confidencial de empleados descuidados.

1.3 Definición y descripción del problema

La infraestructura actual en la que operan las redes inalámbricas bajo el protocolo 802.11, así como lo señalan W. Wang y H. Wang (2011), cuenta con muchas vulnerabilidades desde sus inicios en 1999, inclusive luego de ser publicadas una tras otras versiones mejoradas de dicho protocolo.

Existen soluciones de protección propietarias, las cuales ofrecen una buena gama de protección como los WIPS o equipos especializados como Cisco o Aruba, representan una inversión inicial de más de $15.000, lo que es un gasto que solo grandes empresas pueden llegar a cubrir.

Debido a esto, muchos investigadores han propuesto métodos de análisis para la detección, como lo proponen Agarwal, Biswas y Nandi (2018) por medio de la construcción de una base de datos que analiza el patrón de autenticación y desautenticación, o como el estudio de Nakhila y Zou (2015) y Nakhila y Zou (2016), por medio del análisis de los paquetes en el protocolo TCP y luego por medio del monitoreo de los canales de comunicación, pero dichos estudios, aun con porcentajes de detección altos, se realizan en un ambiente específico y controlado para las pruebas, lo que no proporciona un mecanismo de mitigación en un ámbito más amplio una vez puesto a prueba en el mundo real.

1.4 Justificación

Si bien se cuenta con propuestas para la detección de un ataque de Wifi Spoofing, como los algoritmos de detección por Nakhila y Zou (2016) y Agarwal, Biswas y Nandi (2018), estos proponen ambientes, por lo cual se busca crear una alternativa que aproveche de los aportes que esta e investigaciones como las de Kao, Yeo, Yong y Chen (2011), Sriram, Sahoo y Agrawal (2010) y Chirumamilla (2003) con análisis minucioso a los canales de comunicación de las redes inalámbricas, proporcionan una respuesta de mitigación a dispositivos que no cuenten con *hardware* y *software* especializado para el monitoreo del tráfico en la red.

Por esta razón se busca explorar por qué los mecanismos de protección disponibles no logran solventar esta falla, y en base en estas fallas poder desarrollar una solución que ofrezca mitigar esta vulnerabilidad como alternativa para ser implementada en las empresas sin la necesidad de recurrir a soluciones propietarias o de un grado de complejidad muy elevado.

Adicionalmente, en la solución que se busca crear se explora la factibilidad de poder implementarlo en los diferentes dispositivos de uso cotidiano, como lo son computadoras de escritorio, *smartphones* y tabletas de diferentes fabricantes.

1.5 Viabilidad

1.5.1 Punto de vista técnico

Desde el punto de vista técnico, el autor del proyecto cuenta con conocimientos en desarrollo de *software* en plataformas propietarias y de código abierto, además de contar con la experiencia de trabajar en el área de investigación y desarrollo del área de redes, al igual que cuenta con la experiencia obtenida como un futuro máster de Ciberseguridad y con el aporte de los estudios realizados por diversos autores como Agarwal, Biswas y Nandi (2018), los cuales proveen un análisis a los algoritmos de monitoreo de la red con gran detalle. Como otro aspecto relevante se cuenta con acceso a recursos de tecnologías propietarias para realizar varios de los análisis y pruebas propuestas en esta investigación.

1.5.2 Punto de vista operativo

Para el punto de vista operativo, al tratarse de una investigación que analiza la seguridad en los medios de comunicación inalámbricos, se estudian dispositivos de uso cotidiano y de fácil adquisición, los cuales cuentan con muchos mecanismos y librerías que facilitan su análisis, al igual que el acceso a *software* de código abierto, el cual facilita recopilar esta información, por lo cual hace viable este proyecto.

1.5.3 Punto de vista económico

Debido a que el proyecto utiliza muchos recursos de código abierto para realizar el análisis de las redes inalámbricas, y los dispositivos analizados son de uso cotidiano, el costo teórico del proyecto para desarrollarlo se determina en horas

de investigación, ya que el costo para el uso de *software* y *hardware* adicional corre por cuenta del autor del proyecto.

Usando como referencia el promedio calculado por el sitio de Glassdoor, el cual promedia el salario anual de un analista de ciberseguridad en $76,410 (ver Figura 1), el costo estimado tomando como una referencia las horas requeridas para este proyecto es de $22,815.8, como se detalla en la Tabla 2.

Figura 1. Salario de Analista de Ciberseguridad. Fuente: Glassdoor.

Tabla 1. Desglose de salario.

Salario Anual	Salario Mensual	Salario Diario	Salario por hora
$76,410	$6,367.5	$212.25	$26.53

Fuente: Elaboración propia basada de información de Glassdoor.

Tabla 2. Costo de horas consultor

Investigador	Horas Semanales	Duración TFG Meses	Duración TFG Horas	Costo promedio
Ballardo Collado	20	8	860	$22,815.8

Fuente: Elaboración propia basada de información de Glassdoor.

1.6 Objetivos

Para la definición de los objetivos se utilizará la Taxonomía de Bloom, ya que esta cuenta con una escalabilidad para definir los objetivos desde lo más sencillo hasta lo más complejo, para confeccionar una manera efectiva de mitigación, que es lo que busca la presente investigación.

1.6.1 Objetivo general

Crear un sistema para la mitigación de ataques tipo *Spoofing* en redes inalámbricas, analizando los mecanismos, herramientas y protocolos existentes para lograr mitigarlos en su mayor parte, y así ofrecer un mecanismo de protección adicional hacia los diferentes dispositivos de los usuarios dentro o fuera de una red empresarial.

1.6.2 Objetivos específicos

- Identificar los procesos y mecanismos actuales para proteger a los empleados fuera de sus empresas de ataques tipo *Spoofing*.
- Explicar el motivo por el cual esta amenaza se mantiene presente y representa un riesgo para las organizaciones que cuentan con sus empleados fuera de sus sedes.
- Ensayar, con las herramientas y técnicas de penetración más recientes, la deficiencia de las medidas de mitigación existentes.
- Examinar la efectividad y fallas de todas las opciones estudiadas para ser clasificadas por su capacidad de mitigación y así recomendarlas para su uso a los empleados que se encuentran en modalidad de trabajo remoto.

1.7 Alcances y limitaciones

1.7.1 Alcances

El alcance de esta investigación es delimitado por la creación de un mecanismo de mitigación ante los ataques de *Wifi Spoofing* en un ambiente controlado. La investigación cuenta con una primera etapa en la cual se evaluará qué tan alta es la vulnerabilidad de los dispositivos existentes ante esta amenaza, una segunda etapa en la cual se realizará el desarrollo de varias pruebas para determinar la efectividad de los mecanismos de defensa accesibles para todos los usuarios y, por último, una tercera etapa donde se desarrolla el sistema para ofrecer una nueva medida para mitigar este tipo de ataque.

1.7.2 Limitaciones

Este proyecto de investigación cuenta con la limitación de no corregir los protocolos existentes para la mitigación de ataques de *Spoofing*, todo esto bajo un escenario de pruebas controladas que simulará las condiciones de los escenarios del mundo real, de forma que no deberá afectar ningún otro mecanismo previamente existente en el mercado.

De la misma forma, se cuenta con las limitantes de los sistemas de los diferentes clientes que se pueden ver limitados por restricciones de sus fabricantes para poder utilizar los recursos internos para los protocolos de Wifi u otros medios de configuración que sean necesarios modificar para poder implementar una solución.

1.8 Marco de referencia organizacional y socioeconómico

En la actualidad, el uso de redes inalámbricas consta como un medio básico para el acceso a internet, y negar el acceso supone una violación de los derechos humanos definida por las Naciones Unidas (United Nations, 2016), por lo cual

resulta indispensable proveer mejores mecanismos de seguridad que fomenten la integridad, confidencialidad y disponibilidad para los usuarios.

De la misma forma que lo denotan Dong, Han, Petropulu y Poor (2008), la necesidad de proveer una capa de seguridad física hacia las comunicaciones inalámbricas requiere de cooperación de todos los ámbitos tecnológicos, para buscar mitigar el acceso de terceros a los canales privados sin consentimiento de las partes, lo cual demuestra la necesidad de proveer más y mejores mecanismos de protección de los canales de comunicación de internet.

1.9 Estado de la cuestión

En el área de las redes inalámbricas hay un esfuerzo mundial para mejorar y volver más seguro este medio de comunicación que ahora se encuentra presente en muchos o casi todos los dispositivos tecnológicos. Debido a esto es necesario recopilar estudios y avances en el área que sean relevantes para fundamentar y desarrollar la investigación, por lo que se procede a hacer su identificación, selección y análisis.

1.9.1 Planificación de la revisión

En esta etapa se formula una pregunta concreta y bien definida del tema de investigación, ya que se realiza la búsqueda de las fallas y los mecanismos existentes que proveen una protección parcial o total al conjunto de vulnerabilidades presentes en esta tecnología, con el objetivo de conocer el desarrollo y avances que existen, además de las posibles debilidades que aún persisten con el fin de no se estén duplicando estudios o sistemas ya desarrollados en otras investigaciones o tecnologías.

1.9.1.1 Formulación de la pregunta

En la formulación de la pregunta se busca poder delimitar el alcance de la búsqueda de información y de la investigación para hallar respuestas y las soluciones que mejor contribuyan a este trabajo de investigación y así poder fundamentar las bases que establezcan los requerimientos para poder definir la propuesta de mitigación por desarrollar.

1.9.1.1.1 Foco de la pregunta

Es necesario para esta investigación ahondar en los aspectos técnicos al más bajo nivel que hace posible el funcionamiento de los protocolos de comunicación inalámbrica, para entender su eficacia en el proceso y cómo estos aún cuentan con las vulnerabilidades necesarias para poder definir el alance del requerimiento para la propuesta de mitigación.

1.9.1.1.2 Amplitud y calidad de la pregunta

Se define en esta sección la pregunta de investigación que se busca responder de manera concisa con base en el problema por mitigar, por lo que se realiza un listado de los términos relevantes para la búsqueda de información que ayude a exponer las fallas y los eventos de nuestro interés. Así se define las medidas por utilizar para medir el efecto para el cual se busca diseñar la propuesta de mitigación por desarrollar.

1. Problema

Los avances en la tecnología han facilitado que muchos dispositivos utilicen redes inalámbricas como su medio de comunicación, lo que facilita los medios para las empresas para fin de que sus empleados trabajen de forma más rápida y eficiente; esto al mismo tiempo habilita las opciones para atacar dichos aparatos y debido a que el proceso o protocolos de comunicación que facilitan esta tecnología

cuentan con las vulnerabilidades necesarias para poder engañar a estos dispositivos a conectarse a redes inalámbricas falsas o suplantadas -conocido como *Wifi Spoofing*-, esto abre los peligros a los que tanto los usuarios como las empresas se exponen. Por ello la presente investigación se enfoca en estudiar las fallas que permiten esto, los trabajos para contrarrestarlo y los escenarios en los cuales aún es necesario mitigar estas fallas por medio del desarrollo de un nuevo sistema.

2. Pregunta

Con base en la definición anterior del problema, se realiza la pregunta de investigación:

¿Existen actualmente soluciones o mecanismos que ayuden a proteger los diferentes dispositivos de más uso por las personas y las empresas ante el ataque de *Wifi Spoofing*?

3. Palabras clave y sinónimos

Para realizar la búsqueda de documentos y posibles trabajos de investigación que previamente han estudiado las fallas y medidas de mitigación que facilitan el ataque de *Wifi Spoofing*, se realiza un listado de las palabras claves para poder ser utilizadas en esta búsqueda, muchas de estas palabras están en el idioma inglés ya que gran parte de las publicaciones existentes se encuentren en este idioma, como se puede ver en la Tabla 3.

Tabla 3: Listado de Palabras

Palabra	Equivalente en inglés
Wifi	Wifi
Engañar	Spoofing
Gemelo Malvado	Evil Twin
Debilidad	Weakness
Inalámbrico	Wireless
Protocolo	Protocol
Red	Network
Solicitud de Sonda	Probe request
Desautenticación	Deauthentication
Ataque	Attack
Enrutador	Router
Defensa	Defense

Fuente: Elaboración propia.

4. Intervención

Ver los resultados de los mecanismos actuales para la mitigación o protección ante las vulnerabilidades existentes de los protocolos de comunicación inalámbrica.

5. Control

Se cuenta con una base de información básica estudiada durante la carrera, por lo cual se empieza con los dispositivos y protocolos de comunicación utilizados en las redes inalámbricas.

6. Efectos

Se espera poder obtener la documentación por medio de las búsquedas realizadas para poder entender las fallas que habilitan las vulnerabilidades existentes y los mecanismos y esfuerzos realizados a la fecha para mitigar este problema.

7. Medida de salida

Con la documentación encontrada se revisará su calidad en sitios web que permiten el poder clasificar esto mismo.

8. Población

La población correspondería a los dispositivos de uso común por los empleados en las empresas, con capacidades de comunicación inalámbrica, como lo son las computadoras, teléfonos inteligentes y tabletas.

9. Aplicación

Esta investigación puede ser de utilidad para empresas o administradores de red en las empresas que busquen poder conocer este ataque y requieran poder utilizar un mecanismo de mitigación existente o el desarrollado en este trabajo.

10. Diseño experimental

En el diseño experimental se hace un análisis y clasificación de los estudios resultantes con base en la calidad que su contenido y relevancia que aportan para la investigación, para de esta forma garantizar que se cuenta con el material de mayor relevancia para este trabajo dentro del rango de lo estudiado para poder desarrollar la nueva propuesta de mitigación del ataque en estudio.

1.9.1.2 Selección de fuentes

En esta sección se especifica las fuentes para la identificación de los estudios primarios que serán utilizados en este trabajo de investigación.

1.9.1.2.1 Definición del criterio de selección de fuentes

El criterio principal para la selección de las fuentes en general toma en cuenta diversos aspectos como la popularidad del trabajo, además de la fuente donde se publica, también se considera la relevancia y detalle con que cuente la documentación.

1.9.1.2.2 Lenguaje de estudio

En este estudio se utiliza en su mayoría el idioma inglés para realizar las búsquedas relacionadas con el tema, ya que mucha de la documentación técnica y trabajos existentes se encuentran en este idioma.

1.9.1.2.3 Identificación de fuentes

En esta sección se describe la selección de las fuentes para la documentación primaria y se realiza una descripción de cómo se ejecutarán las búsquedas.

1. Método de selección de fuentes

El método de selección de fuentes se basa en el reconocimiento con que se cuente en el área de tecnología de los protocolos de comunicación inalámbrica, ante la publicación de documentos y proyectos de investigación.

2. Cadena de búsqueda

Las cadenas de búsqueda que se utilizan los términos en combinación de *OR* y de *AND*. (*Evil twin attack defense*) *AND* (*Deauthentication Attack*) ((802.11w) *OR* (802.11) *OR (Management Frame Protection*)) *AND (Build your own router*) *AND* (*Wifi Probe Request*) *AND* (*Network defense*).

3. Lista de fuentes

Dado que en el área de la tecnología la entidad conocida como IEEE es la que se encarga de analizar, regular y publicar todos lo relacionado con los estándares de tecnología y que, para efectos de esta investigación, son los responsables de la creación, cambios y mejoras a los protocolos de comunicación de redes inalámbricas se utiliza como fuente: IEEE Digital Library.

1.9.1.2.4 Selección de fuentes después de la evaluación

Para poder refinar la lista de fuentes como resultado de las cadenas de búsqueda y la calidad que estos resultados arrojan, el aspecto por considerar es la calidad de la información que estos proveen.

1.9.1.2.5 Comprobación de las fuentes

En este momento no se cuenta con un criterio experto para la selección precisa entre las fuentes, se escogen las más utilizadas según la fuente de publicación, dado que estos documentos pasan por un proceso de selección y evaluación para ser publicados en la IEEE.

1.9.1.3 Selección de los estudios

Ahora, ya definidas las fuentes, se define cuáles de los trabajos recuperados en los resultados de las búsquedas se podrán incluir en el análisis final.

1.9.1.3.1 Definición del criterio de inclusión y exclusión de estudios

Se utiliza los criterios definidos en la Tabla 4 para incluir o excluir los documentos de la búsqueda, de manera que los artículos resultantes serán los incluidos.

Tabla 4: Criterios de inclusión y exclusión de estudios

Pregunta de investigación	Término principal para criterio de inclusión	Criterio de Exclusión
¿Existen actualmente soluciones o mecanismos que ayuden a proteger los diferentes dispositivos de más uso por las personas y las empresas ante el ataque de *Wifi Spoofing*?	*Wifi, Evil Twin, 802.11, 802.11w, Probe, Defense, Handshake, RAP, WIPS, Wireless, OpenWRT, Security, MFP*	• Documentos de análisis de red que no tengan relación con la mitigación del ataque. • Documentos sobre las vulnerabilidades que se enfoquen solo en buenas prácticas de los usuarios finales. • Estudios que se enfoquen en solo el estudio del ataque de denegación de servicio. • Trabajos que busquen solo proteger el canal de comunicación de los datos.

Fuente: Elaboración propia.

1.9.1.3 Definición de tipos de estudio

La definición de los tipos de estudio se relaciona con la pregunta de investigación, lo cual se define en la Tabla 5 para determinar los requisitos de los artículos de interés.

Tabla 5: Tipos de estudio

Pregunta de investigación	¿Quién?	¿Qué?	¿Cómo?	¿Dónde?
¿Existen actualmente soluciones o mecanismos que ayuden a proteger los diferentes dispositivos de más uso por las personas y las empresas ante el ataque de *Wifi Spoofing*?	Dispositivos que usen protocolos de comunicación inalámbrica.	Vulnerabilidades, fallas en protocolos.	Detección, Prevención	En redes inalámbricas, enrutadores, empresas.

Fuente: Elaboración propia.

1.9.1.3 Procedimiento para la selección de los estudios

Para la selección de los estudios se realizó el siguiente proceso por cada una de las fuentes y así determinar las más relevantes:

1. Realizar la búsqueda de manera general o de forma avanzada en las fuentes seleccionadas.
2. Con base en la cantidad de resultados obtenidos, utilizar las cadenas de búsqueda aplicables y así obtener resultados de interés que satisfagan los criterios de inclusión.
3. Si aun al realizar el paso anterior, en la lista de resultados la cantidad es mayor a 50, aplicar filtros o cadenas adicionales para excluir resultados, como ver los rangos de fechas de los estudios.
4. Evaluar los resultados restantes y aplicar criterios de exclusión que se encuentren en el *Abstract* y las *keywords* de los artículos.
5. Seleccionar los resultados obtenidos más relevantes para la fuente seleccionada y repetir el mismo proceso para las otras fuentes.

1.9.2 Ejecución de la revisión

Se presentará a continuación el proceso de selección llevado a cabo en la fuente seleccionada.

1.9.2.1 Ejecución de la selección en la fuente IEEE

1.9.2.1.1 Selección de estudios iniciales

Al realizar el proceso de búsqueda utilizando los parámetros ya mencionados, se encontraron cinco resultados al aplicar los métodos de exclusión propuestos, específicamente los artículos que no se enfocaran en solo proteger los datos, sino que aportaran mecanismos de protección o consecuencias de las vulnerabilidades, excluyendo investigaciones sobre el análisis de los ataques de denegación de servicio (DoS) o denegación de servicio distribuida (DDoS), como se detalla en la Tabla 6.

Tabla 6: Estudios encontrados en IEEE

n.º	Título	Autores	Año	URL
1	An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks.	Agarwal, M., Biswas, S. & Nandi, S.	2018	https://doi.org/10.1007/s10776-018-0396-1
2	User-side Wi-Fi evil twin attack detection using random wireless channel monitoring	O. Nakhila and C. Zou	2018	https://doi.org/10.1109/CCNC.2015.7157983
3	Weakness in 802.11w and an improved mechanism on protection of management frame	Wang, W., & Wang, H	2011	https://doi.org/10.1109/WCSP.2011.6096780
4	Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests	A. Di Luzio, A. Mei and J. Stefa	2016	https://doi.org/10.1109/INFOCOM.2016.7524459
5	An OpenWRT solution for future wireless homes	C. E. Palazzi, M. Brunati and M. Roccetti	2010	https://doi.org/10.1109/ICME.2010.5583223

Fuente: Elaboración propia.

1.9.2.1.2 Evaluación de la calidad de los estudios

Debido a que las fuentes fueron obtenidas de una organización altamente reconocida, se asume que se superan los filtros y evaluaciones necesarios para ser considerables confiables.

1.9.2.1.3 Revisión de la selección

La selección de estos estudios primarios se ha realizado por medio de una revisión de los *Abstract* y del contenido de cada uno de los artículos, los cuales fueron ordenados con base en la relevancia que aportan a la investigación.

1.9.2.1.4 Extracción de información

De los estudios primarios que cumplen todos los requisitos se extrae la información y su índice bibliográfico, para cada una de las fuentes seleccionadas:

Tabla 7. Extracción fuente 1

Repositorio	**IEEE Digital Library**
Título	An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks.
Publicación	Int J Wireless Inf Networks 25, 130–145 (2018).
Autores	Agarwal, M., Biswas, S. & Nandi, S.
Referencia	Agarwal, M., Biswas, S., & Nandi, S. (2018*). An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks. International Journal of Wireless Information Networks.* Obtenido de Springer:

	https://doi.org/10.1007/s10776-018-0396-1
Resumen	En esta investigación se evalúa cómo la capa MAC del protocolo 802.11 es vulnerable a varios ataques de seguridad como denegación de servicio, ataque de desautenticación, ataques de alimentación, punto de acceso no autorizado (RAP), entre los cuales se enfocan en el de Evil Twin Attack (ETA), el cual es una forma de RAP que clona la dirección MAC y el BSSID de un punto de acceso inalámbrico (AP) existente para que los clientes se conecten sin saberlo creyendo que están conectados a un AP genuino, al cual un atacante espía e intercepta la comunicación para redirigir a los clientes a sitios maliciosos o robar las credenciales de los clientes.
Aspectos por destacar	Aquí se evalúan métodos existentes para detectar el ETA, como mantener listas blancas, parchear AP / cliente, soluciones basadas en tiempo, modificaciones de protocolo, monitoreo en el tiempo del protocolo TCP, los cuales requieren configuración y mantenimiento extensos, con problemas de escalabilidad y compatibilidad y cambios en protocolos, por lo que los autores proponen crear r un patrón de anomalías para un IDS, eventualmente comportándose bajo el esquema de WIDS que aborde la mayoría de problemas con los mecanismos de detección existentes, esta investigación además cuenta con altos índices bibliográficos.

Fuente: Elaboración propia.

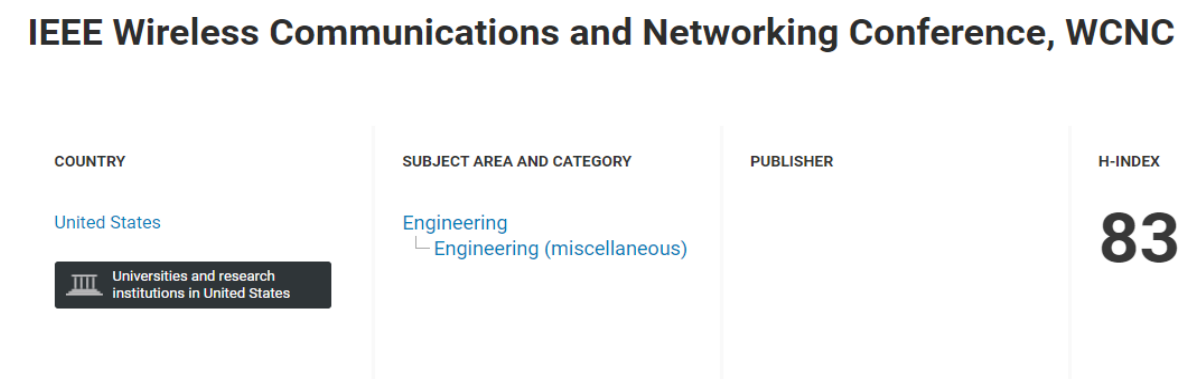

Figura 2. Índice bibliográfico 1 de Agarwal, Biswas y Nandi (2018). Generado de Scimago Journal & Country Rank

Figura 3: Índice bibliográfico 2 de Agarwal, Biswas y Nandi (2018). Generado de Scimago Journal & Country Rank

Tabla 8. Extracción fuente 2

Repositorio	**IEEE Digital Library**
Título	User-side Wi-Fi evil twin attack detection using random wireless channel monitoring
Publicación	MILCOM 2016 - 2016 IEEE Military Communications Conference, Baltimore, MD, USA, 2016, pp. 1243-1248
Autores	O. Nakhila and C. Zou

Referencia	O. Nakhila and C. Zou. (2016). "*User-side Wi-Fi evil twin attack detection using random wireless channel monitoring," MILCOM 2016 - 2016 IEEE Military Communications Conference, Baltimore, MD, USA.* Obtenido de IEEE: https://doi.org/10.1109/CCNC.2015.7157983.
Resumen	En este artículo se plantea cómo el acceso gratuito a Internet inalámbrico es un servicio disponible en la mayoría de las cafeterías, restaurantes de comida rápida y aeropuertos para sus clientes, se realiza por lo general a redes wifi inseguras, por lo que resulta sencillo para un atacante engañar a un cliente inalámbrico por medio de un punto de acceso no autorizado (RAP) simulando la MAC y el BSSID del AP legítimo, para el ataque del hombre en el medio (MitM), incluso por medio de la denegación de servicio (DoS). Para mitigar esto se presenta un esquema de detección del lado del cliente en tiempo real para detectar el ataque ETA al monitorear múltiples canales de wifi en un orden aleatorio en busca de paquetes de datos específicos enviados por un servidor dedicado en Internet y así identificar claramente si un AP específico es un RAP. Aunque esta referencia no cuenta con información de cuartiles, sí cuenta con un índice de un buen nivel.
Aspectos por destacar	Se analizan los escenarios en el mundo real y como medida de protección se establece un esquema para el monitoreo de las redes dentro del perímetro.

Fuente: Elaboración propia.

Figura 4. Índice bibliográfico 1 de Nakhila y Zou (2016). Generado de Scimago Journal & Country Rank

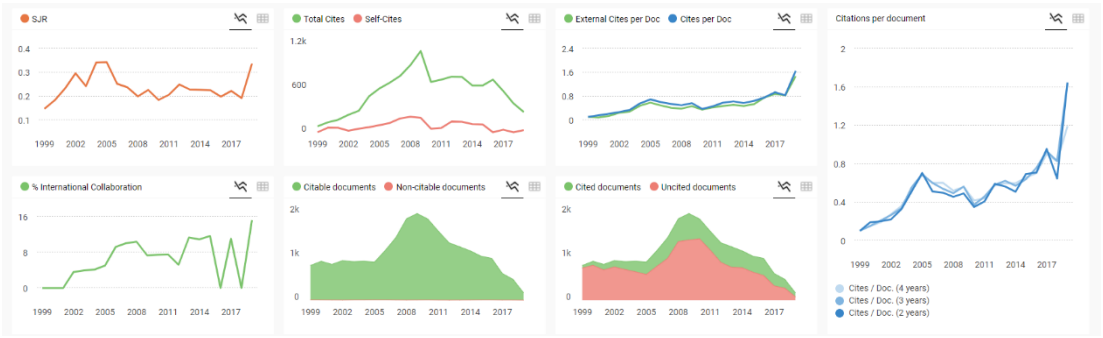

Figura 5. Índice bibliográfico 2 de Nakhila y Zou (2016). Generado de Scimago Journal & Country Rank.

Tabla 9. Extracción fuente 3

Repositorio	**IEEE Digital Library**
Título	Weakness in 802.11w and an improved mechanism on protection of management frame.
Publicación	2011 International Conference on Wireless Communications and Signal Processing (WCSP), 1–4

Autores	Wang, W., & Wang, H.
Referencia	Wang, W., & Wang, H. (2011). *Weakness in 802.11w and an improved mechanism on protection of management frame. 2011 International Conference on Wireless Communications and Signal Processing (WCSP).* Obtenido de IEEE: https://doi.org/10.1109/WCSP.2011.6096780
Resumen	Este artículo plantea cómo la seguridad de la WLAN bajo el estándar 802.11 que fue liberado en 1999 utilizando WEP (privacidad equivalente cableada) para proporcionar confidencialidad de datos para la WLAN, abrió la puerta a un nuevo conjunto de vulnerabilidades. Para esto exponen como IEEE libera el 802.11i que proporciona una RSN (Robust Security Network) para reemplazar el WEP, donde se establece el estándar actual para comunicación que utiliza *Four-Way Handshake* y Group Key Handshake, que se usa para cifrar y proporcionar integridad de datos a la trama de datos, el cual aún contaba con muchas vulnerabilidades. Por ello, IEEE establece el 802.11w, que fue fortalecido como una enmienda al 802.11i, este proporciona un mecanismo para proteger los marcos de administración y control, es utilizado actualmente por diversos WIPS, este aun ve situaciones en las que el 802.11w no puede desempeñar un papel eficaz para proporcionar suficiente protección a los marcos. Todas las situaciones se basan en los ataques conocidos al 802.11i y cada uno refleja un aspecto de la debilidad de 802.11w.

Aspectos por destacar	Aquí se expande el porqué se dan las vulnerabilidades actuales que presenta el protocolo de comunicación y los intentos para poder proveer una capa de protección. Este artículo no cuenta con un índice bibliográfico alto, pero provee un alto y detallado contexto del porqué de esta investigación.

Fuente: Elaboración propia.

Figura 6. Índice bibliográfico 1 de Wang, y Wang (2011). Generado de Scimago Journal & Country Rank.

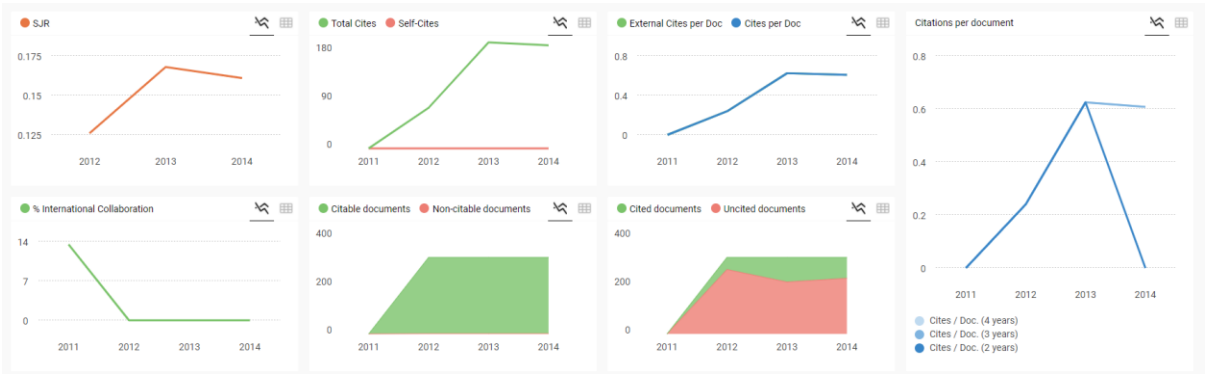

Figura 7. Índice bibliográfico 2 de Wang, y Wang (2011). Generado de Scimago Journal & Country Rank.

Tabla 10: Extracción fuente 4

Repositorio	**IEEE Digital Library**
Título	Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests
Publicación	IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA, 2016, pp. 1-9
Autores	A. Di Luzio, A. Mei and J. Stefa
Referencia	A. Di Luzio, A. Mei and J. Stefa. (2016*). "Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests," IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA.* Obtenido de IEEE: https://doi.org/10.1109/INFOCOM.2016.7524459.
Resumen	Como parte de las vulnerabilidades del protocolo 802.11, este explica cómo teléfonos inteligentes y otros dispositivos wifi encendido realizan periódicamente intentos de conexión a AP conocidos por medio de *WiFi probe requests*, el cual contiene la dirección MAC del dispositivo de envío y BSSID del AP conocido. Esta información referente al protocolo se envía de forma clara y, si se captura, puede ayudar a descubrir información y patrones importantes de las personas y la naturaleza humana que no tienen nada que ver con la tecnología, por lo cual en este artículo

	presenta la idea de aprovechar los *Wifi probe requests* para estudiar los usuarios de varios conjuntos de datos disponibles públicamente.
Aspectos por destacar	Provee el contexto de los mecanismos y protocolos de comunicación ante el ataque en estudio y por qué se mantienen muchas de las vulnerabilidades actuales. Este artículo cuenta con una clasificación un poco baja, pero con contenido aún relevante para esta investigación.

Fuente: Elaboración propia

2016 2nd IEEE International Conference on Computer and Communications, ICCC 2016 - Proceedings

COUNTRY	SUBJECT AREA AND CATEGORY	PUBLISHER	H-INDEX
United States Universities and research institutions in United States	Computer Science Computer Networks and Communications Hardware and Architecture Engineering Safety, Risk, Reliability and Quality		8

PUBLICATION TYPE	ISSN	COVERAGE	INFORMATION
Conferences and Proceedings	-	-	Homepage

Figura 8. Índice bibliográfico 1 de Di Luzio, Mei y Stefa (2016). Generado de Scimago Journal & Country Rank.

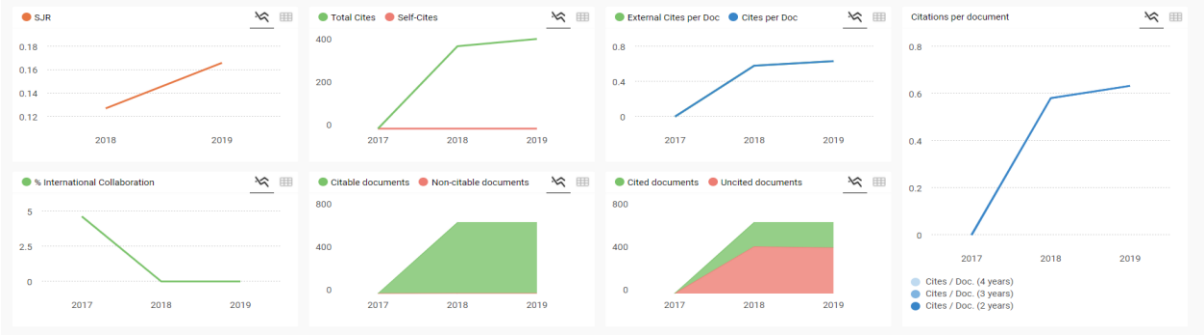

Figura 9. Índice bibliográfico 2 de Di Luzio, Mei y Stefa (2016). Generado de Scimago Journal & Country Rank.

Tabla 11. Extracción fuente 5

Repositorio	**IEEE Digital Library**
Título	An OpenWRT solution for future wireless homes
Publicación	IEEE International Conference on Multimedia and Expo, Singapore, 2010, pp. 1701-1706
Autores	C. E. Palazzi, M. Brunati and M. Roccetti
Referencia	C. E. Palazzi, M. Brunati and M. Roccetti. (2010). *"An OpenWRT solution for future wireless homes," 2010 IEEE International Conference on Multimedia and Expo, Singapore.* Obtenido de IEEE: https://doi.org/10.1109/ICME.2010.5583223.
Resumen	En este artículo se estudia que para servicios digitales futuros para usuarios domésticos y de oficina será indispensables por

	medio de la conectividad inalámbrica, por lo que el empleo de protocolos y puntos de acceso (AP) regulares no permitirá una coexistencia eficiente, por ello en este trabajo se presenta un prototipo de AP capaz de garantizar una entrega de datos rápida y fluida para flujos en tiempo real mientras se mantiene un alto rendimiento para aplicaciones basadas en TCP basado en el sistema operativo OpenWRT, para dar forma de manera adecuada al tráfico de red en tránsito, incluso proveer una capa más compleja de protección para ataques de *Phishing* o DoS. Este artículo cuenta con una referencia parcialmente buena en sus índices.
Aspectos por destacar	En este estudio se parte de las consecuencias de las vulnerabilidades, por lo que se facilita un mecanismo o dispositivo alternativo para poder administrar las redes inalámbricas de manera profesional y a bajo costo.

Fuente: Elaboración propia.

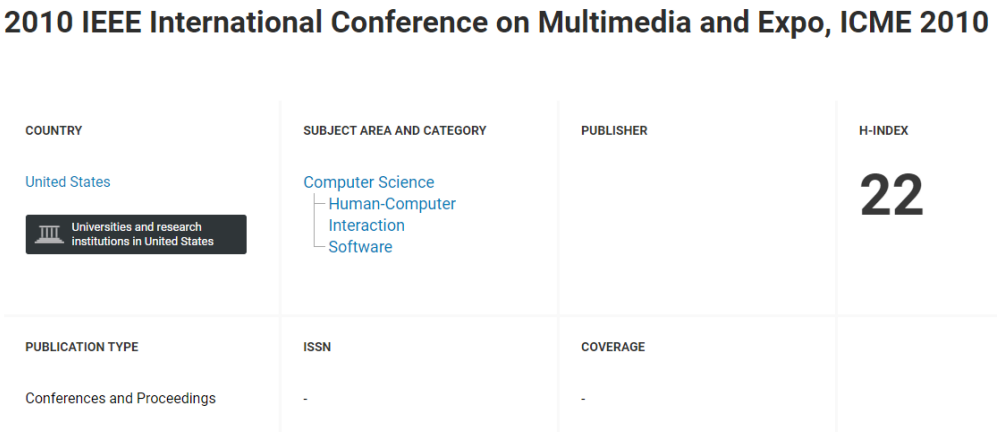

Figura 10. Índice bibliográfico 1 de Palazzi, Brunati y Roccetti (2010). Generado de Scimago Journal & Country Rank.

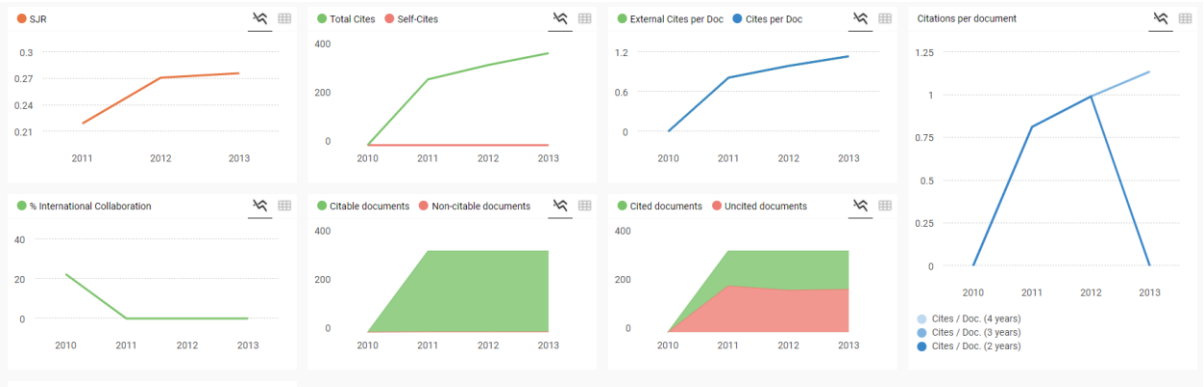

Figura 11. Índice bibliográfico 2 de Palazzi, Brunati y Roccetti (2010). Generado de Scimago Journal & Country Rank.

1.9.3 Resumen de los resultados

En resumen, respecto a los hallazgos, se puede destacar el hecho de que desde los inicios de la implementación del protocolo 802.11 para redes wifi, ha estado abierto a una gran serie de vulnerabilidades, las cuales van desde la forma en que se comunica con el AP destino, hasta la forma en que escanea los AP disponibles para conexión, lo cual revela la información sobre los dispositivos para eventualmente aprovechar el uso de un ETA para un MitMA y así robar información, credenciales o explotar las vulnerabilidades adicionales con las que pueda contar el dispositivo.

En cuanto a los mecanismos actuales para proveer un nivel de protección a los clientes inalámbricos, a nivel de protocolos se puede contar con el 802.11w, el cual protege al AP y a los clientes del wifi ante ataques de desautenticación, al proveer llaves criptográficas para proteger la comunicación y el proceso de *Four-Way Handshake*, esto es implementado en muchos de los WIPS en redes corporativas, pero no se encuentra ampliamente disponible para AP de uso común en áreas como hogares o empresas pequeñas, lo que deja aún a los clientes desprotegidos al momento de conectarse a internet por medio de estos wifi, el cual

incluso en sistemas de código abierto como OpenWRT cuenta con deficiencias en dicho protocolo, las cuales aún están revisión.

Agarwal, Biswas y Nandi (2018) y Nakhila y Zou (2016) proponen analizar los canales de comunicación con los AP para determinar si se han violentado los llamados del *Four-Way Handshake*, del cual hace provecho de la vulnerabilidad junto con los marcos de control y administración para el ataque de ETA, en el que sus algoritmos tienen una tasa de detección muy alta, pero se basan en escenarios muy específicos en el que se cuentan con más de un AP con un BSSID con las mismas características, y para el caso de un RAP implementado de la recolección de datos de un ataque de *Wifi probe request*, no va a poder detectar el ataque de *Spoofing*, por lo cual es claro que esta vulnerabilidad no se encuentra completamente cubierta o mitigada en todos los escenarios actuales.

Capítulo 2. Marco Conceptual

Con base en los conceptos más relevantes encontrados en el estado de la cuestión se ha generado la siguiente nube de conceptos, esto se extrae como parte del resumen realizado de todos los artículos mencionados.

Figura 12. Nube de conceptos. Elaboración propia. Generado de https://www.nubedepalabras.es/

Con base en la Figura 12, se presentarán los conceptos con mayor mención y que tienen más relevancia en esta investigación. Para estos se han categorizando los conceptos en grupos respecto a la función o significado que representan para este proyecto y en el mundo real.

2.1 Conceptos sobre el contenido

Actualmente el ataque de *Wifi Spoofing* hace provecho de diversas vulnerabilidades a través de todo el protocolo que provee de acceso inalámbrico a internet en todos los dispositivos (celulares, tabletas, *laptop*, etc.).

Además, se cuenta con diferentes mecanismos de defensa o mitigación, los cuales cubren diferentes aspectos de este ataque. Como consecuencia esto expone

a los usuarios en sus hogares o centros de reunión y a empleados fuera del ambiente seguro de sus empresas a diversos tipos de ataques, todo esto como parte de la relación entre los conceptos (ver Figura 13).

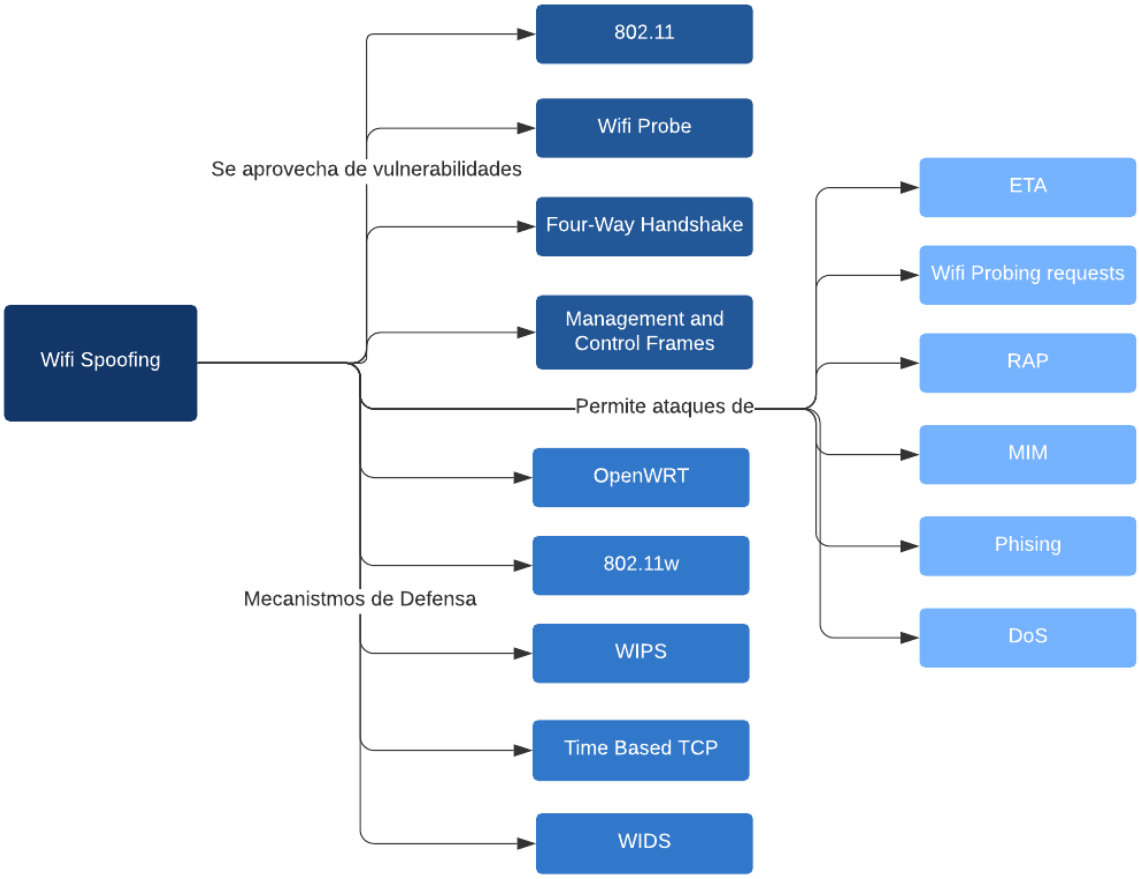

Figura 13. Diagrama sobre conceptos relacionados al ataque *Wifi Spoofing.* Fuente: Elaboración propia.

2.2 Vulnerabilidades

Las vulnerabilidades descritas a continuación se encuentran identificadas como las que abren la posibilidad para poder explotar y perpetuar el ataque de *Wifi Spoofing*, cada una de ellas se expone a continuación.

2.2.1 802.11

Este es el nombre de una familia de estándares para la comunicación inalámbrica establecido por IEEE-SA Standards Board (1999), por medio del modelo

para las comunicaciones inalámbricas que desde sus inicios presentó vulnerabilidades una tras otra.

Para solventar eso, IEEE libera 802.11i para establecer el *Four-Way Handshake*, el cual proporcionaba integridad de datos a la trama de datos, sin embargo, todavía cuenta con muchas vulnerabilidades, en los marcos de administración están desprotegidos, con lo que IEEE crea el protocolo 802.11w como una mejora al 802.11i, el cual proporciona un mecanismo para proteger las tramas de administración, pero este mecanismo no está presente en todos los puntos de acceso y en sus inicios no todos los dispositivos tenían soporte para él.

2.2.2 *Wifi Probe*

Todos los teléfonos inteligentes, por medio de su interfaz de wifi, periódicamente intentan conectarse a puntos de acceso inalámbricos conocidos a los que el usuario se ha conectado en el pasado, esto por medio de solicitudes de tramas inalámbricas especiales que contienen la dirección MAC y el nombre del punto de acceso o enrutador conocido, para poder encontrar y así conectarse automáticamente a un nuevo punto de acceso conocido.

Esta información se envía completamente clara y puede ser capturada por cualquier persona con el equipo adecuado puede ayudar a descubrir información y tendencias de las personas (Oliveira, Schneider, Souza, J. D, y Shen, 2019).

2.2.3 *Four-Way Handshake*

Introducido en 2004 por IEEE el protocolo 802.11i, el cual proporcionaba RSN (*Robust Security Network*) para reemplazar el WEP, este protocolo (ver Figura 14) funciona de forma que el cliente envía una solicitud de autenticación al AP, este

devuelve una respuesta de autenticación, luego el cliente envía una solicitud de asociación al AP, el cual envía una respuesta de asociación al cliente.

Si todos los cuatro pasos anteriores tienen éxito, se dice que el cliente se ha autenticado y asociado con éxito. Cada cliente que se conecta al AP necesita completar con éxito este apretón de manos de cuatro vías.

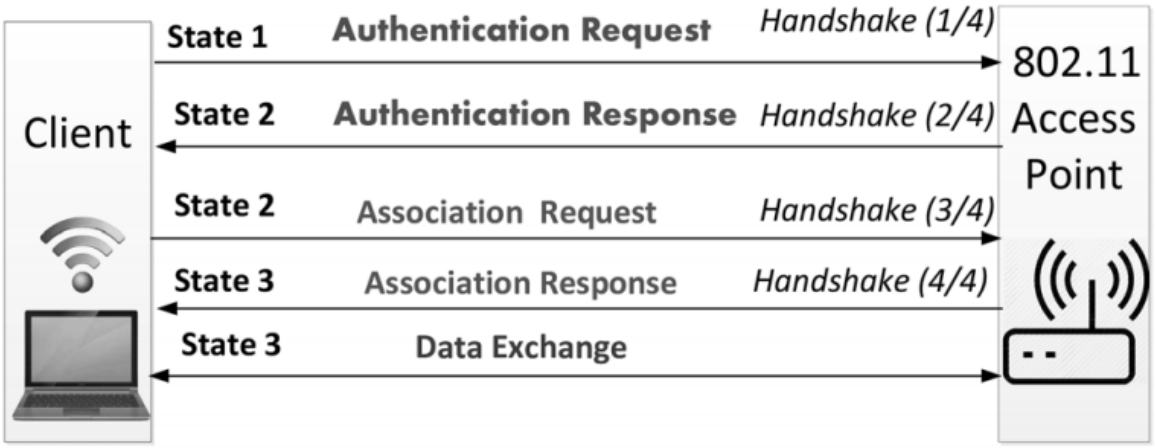

Figura 14: *Diagrama Four-Way Handshake*. Fuente: Agarwal, Biswas y Nandi, (2018).

Este proceso está expuesto dado que un atacante puede enviar solicitudes en medio de esta comunicación para desautenticar a los clientes o incluso robar datos del mismo proceso.

2.2.4 *Management and Control Frames*

Estas son las tramas que componen 802.11 para la comunicación del *Four-Way Handshake*, estos marcos de gestión y control son vitales para el establecimiento, el mantenimiento y el cierre de la conexión con el cliente, estos datos contienen la información que se intercambiará con el punto de acceso.

En el protocolo 802.11 se tiene WEP (*Wired Equivalent Privacy*), WPA (*Wifi Protected Access*) y WPA2 como mecanismos de cifrado, cada uno de los mecanismos encripta solo tramas de datos, pero los marcos de administración y

control viajan en texto plano, lo que los hace vulnerables a la suplantación de identidad. Todos estos marcos son utilizados en el *Four-Way Handshake*, explicado previamente, son vulnerables a la suplantación de identidad (Agarwal, Biswas, y Nandi, 2018).

2.3 Ataques

Los ataques aquí descritos son varias de las opciones resultantes al explotar muchas o todas las vulnerabilidades anteriormente descritas, cada una de estas se describe a continuación.

2.3.1 ETA

Cuando un cliente o dispositivo con capacidades inalámbricas regresa a una red utilizada previamente, las herramientas de administración de red tienden a intentar volver a conectarse automáticamente a una de estas redes por medio de un sondeo activo de los dispositivos, todo esto sin que el usuario tenga noción de este proceso.

De esta reasociación automática se aprovecha el ataque de gemelos maligno (*Evil Twin Attack*), en el que un atacante configura un punto de acceso con la misma identidad (SSID) y dirección MAC de los puntos de acceso confiables y utilizados previamente por el cliente, para luego aprovechar que se encuentra dentro de la misma red del atacante para explotar diversos nuevos ataques (Gonzales, Bauer, Lindqvist, McCoy y Sicker, 2010).

2.3.2 *Wifi Probe requests*

Si bien este mecanismo funciona para que los diferentes dispositivos con capacidades de conexión inalámbricas se conecten a puntos de acceso inalámbricos conocidos, como esta información puede ser leída por cualquier

persona pues se envía completamente clara, esto puede ayudar a descubrir información y tendencias de las personas, como el estudio de Di Luzio, Mei y Stefa (2016), que la utilizó para descubrir información y desanonimizar el origen de los participantes gracias a estos datos disponibles públicamente de los dispositivos, que contienen escenarios de relevancia relacionados con la religión en toda la ciudad, nacional e internacional y así descubrir con gran precisión la procedencia de las multitudes en diferentes eventos.

2.3.3 RAP

Definido como punto de acceso deshonesto por sus siglas en inglés *Rogue Access Point*, es el término que se le da al punto de acceso que se encuentra suplantando a uno legítimo, con el fin de escuchar los datos de los clientes que han sido obligados a conectarse a este wifi para eventualmente robar o utilizar algún otro tipo de ataque hacia las víctimas (Nakhila y Zou, 2016).

2.3.4 MitM

Este tipo de ataque, conocido como hombre en el medio (*Man-in-the-Middle*) requiere que el atacante se coloque entre dos partes que se encuentren comunicando mientras creen que se están comunicando entre sí de manera directa y segura, para que el atacante pueda luego monitorear y posiblemente cambiar el contenido de los mensajes, o hacer la redirección de datos a otros canales para ser almacenados (ENISA, 2016).

2.3.5 *Phishing*

El ataque de *phishing* es un medio para engañar a víctimas potenciales para que divulguen información confidencial, como credenciales, datos bancarios o tarjetas de crédito, por medio de ingeniería social, esto generalmente toma la forma

de correo SPAM, sitios web maliciosos, mensajes de correo electrónico o mensajes instantáneos, que parecen provenir de una fuente legítima, como un banco o una red social (ENISA, 2016).

2.3.6 DoS

Este es un ataque de denegación de servicio (DoS), sucede ocurre cuando los usuarios legítimos de un sistema o aplicación no pueden acceder a los sistemas de información, dispositivos o cualquier otro recurso de red debido, esto sucede cuando dicha denegación de servicio se logra al inundar el *host* o la red objetivo con tráfico hasta que el objetivo no puede responder o simplemente se bloquea, lo que impide el acceso de usuarios legítimos (CISA, 2009).

Estos ataques, en el contexto de esta investigación, se encuentran cuando por medio de la combinación de los ataques de RAP y ETA, se puede llegar a denegar el servicio a los clientes legítimos de una red, causando dicha denegación de servicio.

2.4 Mecanismos de defensa

Los mecanismos de defensa para el ataque de *Wifi Spoofing* cubren diferentes vulnerabilidades de las cuales se aprovecha este, por lo cual cada método de protección o defensa protege o provee una capa de seguridad específica que es necesario aclarar.

2.4.1 OpenWRT

Este es un sistema operativo basado en Linux dirigido a dispositivos embebidos, el cual proporciona un sistema totalmente libre de la selección y configuración de la aplicación proporcionada por el proveedor, que permite personalizar el dispositivo mediante el uso de paquetes para adaptarse a cualquier

aplicación como el marco para crear una aplicación sin tener que crear un *firmware* completo a su alrededor, esto para los usuarios significa tener la posibilidad de una personalización completa de los puntos de accesos de formas nunca imaginadas (OpenWrt Project, 2005).

2.4.2 802.11w

Este es un protocolo para la seguridad que utiliza un mecanismo mejorado, denominado *Temporary Safe Tunnel* (TST), combina la criptografía de clave pública y el sistema de almohadilla de un solo uso. Dado que se diseñó meticulosamente, su costo es lo suficientemente bajo, provee mecanismos que brindan protección a las tramas de unidifusión y las tramas de difusión / multidifusión, que también otorga un método denominado BIP (Protocolo de integridad de difusión / multidifusión), para proporcionar integridad a las tramas de difusión / multidifusión (Wang, y Wang, 2011).

2.4.3 WIPS

Como lo indica su nombre en inglés -*Wireless Intrusion Prevention System*-, es un sistema para la prevención de intrusos en las redes inalámbricas, el cual debe brindar protección contra ataques de DoS, *spoofing* de direcciones MAC, monitoreo de tráfico, protección para proporcionar comunicaciones seguras entre cada sensor y servidor para evitar la manipulación por parte de un atacante, entre otras funciones más a nivel de prevención de ataques (Department of Homeland Security Cybersecurity Engineering, 2017).

2.4.4 WIDS

Este mecanismo de defensa, como su nombre en inglés lo indica -*Wireless Intrusion Detection System*-, es un sistema para la detección de intrusos en las redes inalámbricas.

Este sistema debe poder detectar y clasificar dispositivos wifi móviles como iPads, iPods, iPhones, Android, conectados a la red para monitorear su actividad, ser capaz de detectar y bloquear múltiples AP desde un solo dispositivo sensor a través de múltiples canales inalámbricos para su clasificación (Department of Homeland Security Cybersecurity Engineering, 2017).

2.4.5 *Time Based* TCP

Este método, propuesto por Nakhila, Dondyk, Amjad y Zou (2015), presenta un nuevo método de detección del lado del cliente para descubrir ETA al utilizar una puerta de enlace diferente a la legítima, el cual toma la conexión SSL / TCP a un servidor web remoto arbitrario para evitar el mensaje engañoso del atacante y tratar de detectar el cambio de la dirección IP pública de la puerta de enlace cambiando de un AP a otro en medio de la conexión SSL / TCP.

Capítulo 3. Marco Metodológico

3.1 Tipo de investigación

Como es presentado en los objetivos de este trabajo, el proyecto consiste en evaluar los mecanismos de protección actual ante ataques de tipo *Wifi Spoofing* y de la misma manera confeccionar un sistema que mitigue las vulnerabilidades no cubiertas actualmente, por lo que debido a esto esta investigación corresponde a la investigación aplicada.

Es necesario investigar si los mecanismos de protección actual pueden mitigar este conjunto de vulnerabilidades que hacen posible efectuar el ataque de

Wifi Spoofing, debido a la necesidad de las empresas al trasladar a muchos de sus empleados de la seguridad de sus instalaciones a la seguridad con que cuenten en sus hogares o centros de elección. Esta vulnerabilidad ha sido estudiada por diferentes ingenieros, pero bajo escenarios y circunstancias muy específicas y controladas, por lo que en este caso se busca crear un sistema para la mitigación que permita cubrir este riesgo a la seguridad en la mayor cantidad de dispositivos.

3.2 Alcance investigativo

Con base en el contexto en el cual se fundamenta esta investigación, se consideran los siguientes tipos:

Exploratoria

De acuerdo con Vargas (2004), las investigaciones de este tipo "tienen por objeto esencial familiarizar al investigador con un tema que no ha abordado antes, novedoso o escasamente estudiado" (p. 92); para esta investigación sí se cuenta con estudios minuciosos respecto al tema de cada una de las vulnerabilidades individuales, pero no de forma conjunta ante todas las vulnerabilidades, de lo cual toma ventaja el ataque de *Spoofing* en redes inalámbricas para explotar todas las fallas existentes y tener éxito.

Descriptiva

Este tipo de investigación, como es definido por Vargas (2004), "busca especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis" (p. 92). Como es descrito en esta investigación, se realiza un análisis de la naturaleza de muchas de las vulnerabilidades y características, entre muchos más puntos, no solo de los dispositivos, sino de los estándares a los cuales se ven

apegados y así facilitar a un atacante el poder cubrir su alcance en un rango más amplio.

Explicativa

Haciendo nuevamente referencia a Vargas (2004), este tipo de investigaciones “Pretenden explicar por qué ocurre un fenómeno y en qué condiciones se da éste, o por qué se relacionan dos o más variables” (p. 93), esta investigación busca determinar por qué aún se cuenta con muchas de las vulnerabilidades que otorgan las condiciones para abrir paso al ataque de *Wifi Spoofing.*

3.3 Enfoque

Conforme a la naturaleza de esta investigación, se tiene que presentar un enfoque alternativo. Naranjo (2020) plantea “Para subsanar las deficiencias de ubicar el enfoque de investigación fuera del paradigma pragmático, el autor utiliza a satisfacción el enfoque alternativo” (p. 7). Para esto, se describe cómo los objetivos se relacionan en las tres dimensiones fundamentales establecidas en este enfoque.

La primera dimensión parte desde el punto de vista ontológico, como es expresado por Gruber (1993) “lo que existe es exactamente aquello que puede ser representado” (p. 8), y como es definido por Naranjo (2020): “En Informática se entiende por ontología un conjunto de términos básicos y relaciones entre ellos” (p. 8), por lo cual, al considerar dichas definiciones, este trabajo presenta las ontologías o la conceptualización de las áreas vulnerables en los protocolos de conexión que utiliza la tecnología de wifi, así como la relación que tienen los ataques para poder ejecutar un ataque de *Wifi Spoofing*, como se muestra relacionado en la Figura 15.

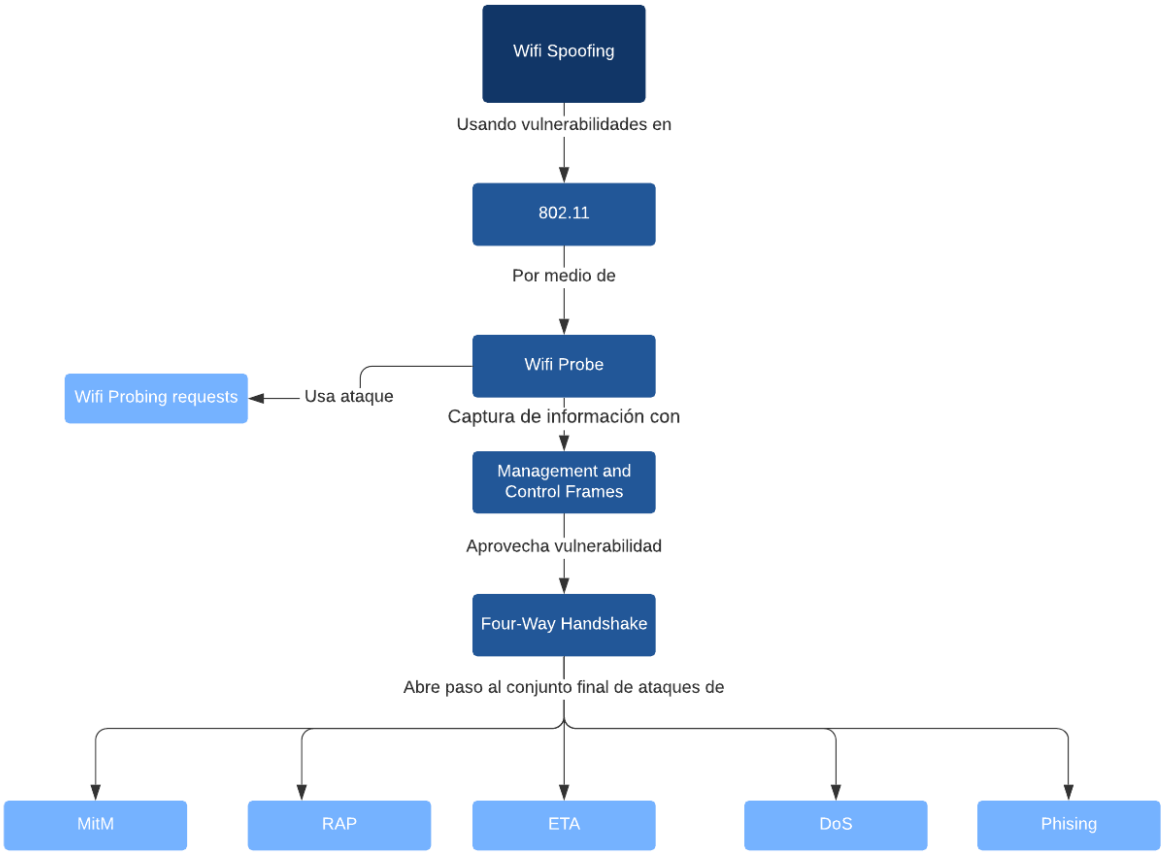

Figura 15. Ontología del conjunto de vulnerabilidades y ataques. Fuente: Elaboración propia.

Desde el punto de la dimensión epistemológica, partiendo de Naranjo (2020), “deberá explicar si asume una postura de observación o de involucramiento con el fenómeno” (p. 8), debido a que se busca evaluar la eficacia de los métodos de protección actuales y confeccionar un sistema nuevo que ayude a mitigar este conjunto de vulnerabilidades que abren paso a este ataque, es necesario tomar la postura de observación e involucramiento en el fenómeno para poder alcanzar los objetivos propuestos.

La última dimensión en este caso es la axiológica, nuevamente citando el concepto de Naranjo (2020), “se refiere a la escala de valores de lo que se va a medir, para evitar el uso de buzzwords” (p. 8)., se busca el poder clasificar y

comprender la eficacia de los mecanismos actuales y el nuevo sistema propuesto para determinar la precisión de acuerdo con las siguientes escalas.

Los fines para este trabajo, en la Figura 15 se describen los rubros en los cuales se evaluará en los capítulos 5 y 6, para determinar la efectividad y precisión de los modelos para la mitigación de ataques de *Wifi Spoofing*. Además, es necesario resaltar que muchos de los modelos y mecanismos actuales para la mitigación de muchas de estas vulnerabilidades se realizan bajo ambientes controlados, por lo que a pesar de que proveen altos resultados, estos se limitan al ambiente preestablecido de los investigadores, por lo cual no se puede definir un conceso general que clasifique la efectividad por igual de todos mecanismos existentes.

Tomando como base parte del modelo de eficacia propuesto por Agarwal et al., 2018), se define un modelo de medida para cada uno de los métodos propuestos de mitigación existentes y el implementado por este proyecto, el cual calculará por número de ejecuciones la cantidad de detecciones exitosas en cada una y definirá un porcentaje de detección, el cual clasifica estos porcentajes como mitigación deficiente a un 60% o menos, a más del 60% y menos de 85% como mitigación promedio y a más de un 85% como mitigación eficiente.

Tabla 12: Criterios para evaluación de eficiencia.

Rubro	Criterio
Método	Método de mitigación utilizado en la evaluación.
Instancias lanzadas	Cantidad de instancias inicializadas

	para esta ejecución.
Instancias detectadas	Cantidad de las instancias inicializadas que fueron detectadas.
Porcentaje de detección	Porcentaje de detección en relación con la cantidad de instancias lanzadas a las detectadas.
Clasificación de detección	Clasificado en 50% <= mitigación deficiente, 60% >= y <= 85% mitigación promedio y 85%> mitigación eficiente.

Fuente: Elaboración propia.

3.4 Diseño

Debido a la naturaleza que tienen muchas investigaciones de ingeniería, la metodología suele orientarse más a una de tipo constructiva o aplicada en vez de una pura, por lo cual Simon (1996) insiste en la importancia de la diferenciación entre las ciencias naturales y las ciencias de lo artificial.

Por ello, se plantea utilizar la metodología de ciencia de diseño para esta investigación, la cual se encuentra conformada por tres ciclos, el ciclo de relevancia, el ciclo de rigor y el ciclo de diseño. En esta metodología, la herramienta más importante es la investigación y búsqueda de información para la construcción de un artefacto en un contexto.

Dado al escenario de esta investigación, el artefacto corresponde al sistema por desarrollar para poder brindar una capa adicional de mitigación a los diferentes dispositivos que utilizan los usuarios para ejecutar las diversas funciones que ejercen en sus trabajos, sea computadoras, teléfonos o tabletas inteligentes.

Con base en esta investigación el contexto se define como la vulnerabilidad ante el ataque de *Spoofing* en redes inalámbricas, lo que respecta a los ciclos definidos en esta metodología se establece a continuación.

Para aplicar el ciclo de relevancia, se estudiará la efectividad de los métodos actuales para la protección de las vulnerabilidades que permiten llevar a cabo el ataque de *Wifi Spoofing* junto a las necesidades del mercado y de cómo se debería implementar el sistema para entender mejor los requerimientos y requisitos de este.

En el ciclo de rigor, se requiere tener una búsqueda constante de información de las necesidades identificadas, tomando en cuenta muchas de las soluciones anteriores a estas, como referencias, y todo el conocimiento técnico para poder ser utilizado en el siguiente ciclo.

Por último, con el ciclo de diseño, utilizando todo el conocimiento recopilado y estudiado en los ciclos anteriores, se procede a construir una solución posible ante el problema estudiado, además se evalúa, por medio de los mecanismos establecidos en el enfoque, si esto representa un aporte a la mitigación del ataque de *Wifi Spoofing*.

La metodología de ciencia de diseño se puede evidenciar en el esquema de la Figura 15.

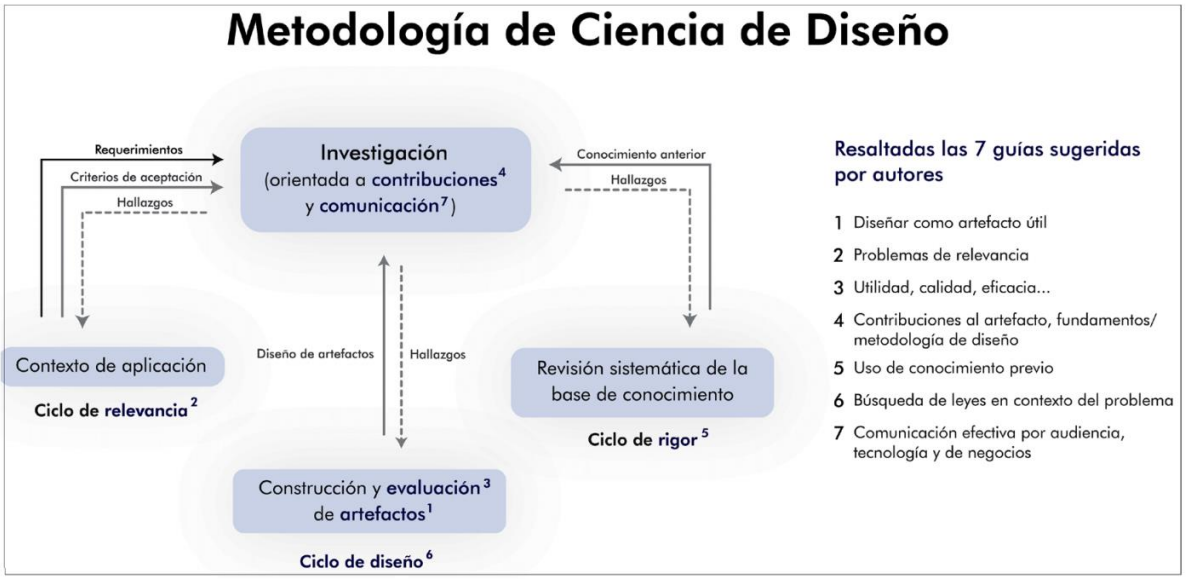

Figura 16. Ciclos de la ciencia de diseño. Fuente: Sandoval, Carvajal, Vásquez, & Zeledón, Naranjo, (2019).

3.5 Población y muestreo

Por la naturaleza de esta investigación, no se cuenta con una población significante como punto de partida para recolectar datos, ya que el foco del proyecto se encuentra en los análisis estadísticos utilizados en los siguientes capítulos relacionados con los resultados de las pruebas respecto a la solución propuesta.

3.6 Instrumentos de recolección de datos

En los instrumentos de recolección de datos se utilizan técnicas de observación para conseguir datos “crudos” relevantes a la vulnerabilidad, en el que en la primera fase se estudia la efectividad del ataque ante la configuración actual de los diferentes dispositivos.

En una segunda fase, se estudian los mecanismos actuales al alcance de cualquier persona, para determinar si la mitigación que estos diferentes medios proveen de manera individual puede detener o pausar varios de los ataques que permiten llevar a cabo el *Wifi Spoofing*.

Esta técnica de observación será llevada a cabo por medio de las herramientas y técnicas de penetración existentes utilizadas en laboratorios, las cuales, además de ser utilizadas en escenarios reales, lanzarán pruebas concretas ante los mecanismos de mitigación estudiados y propuestos.

3.7 Técnicas de análisis de información

Se realiza un diagrama de causa-efecto, que muestra las principales causas que dan paso al ataque de *Wifi Spoofing*, denotando en cada una de las espinas los detalles relevantes de cada causa, lo cuales provienen de las causas más probables ante la incidencia final, esto permitirá sacar conclusiones para poder aportar una respuesta de mitigación para tener más control sobre el problema estudiado en esta investigación.

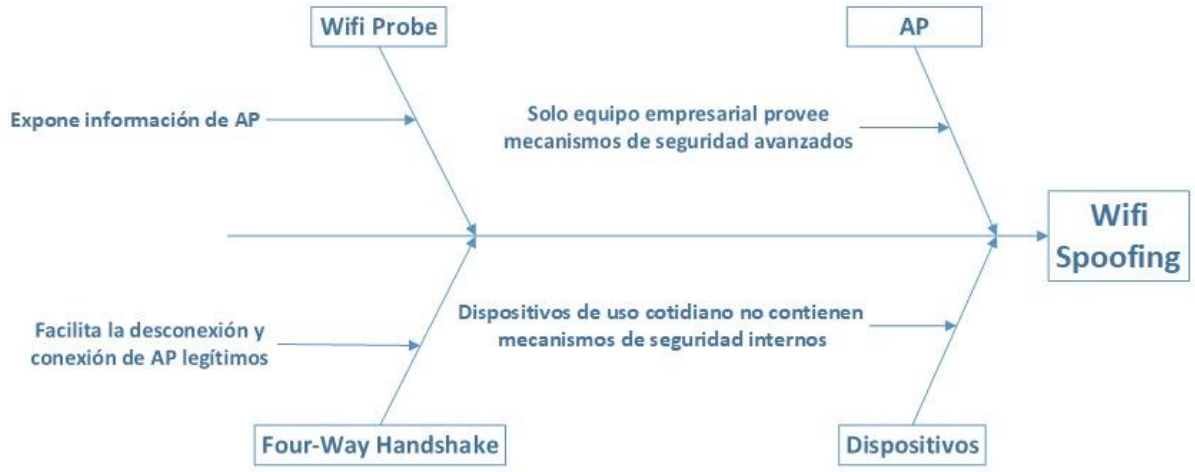

Figura 17. Diagrama de Causa-Efecto. Fuente: Elaboración propia.

3.8 Estrategia de desarrollo de la propuesta

Para el desarrollo de la propuesta se utilizará una metodología Agile para el desarrollo del sistema de mitigación, ya que proporciona un modelo de trabajo flexible para poder solventar problemas de forma más rápida.

Las herramientas para poder desarrollar esta solución toman en consideración los tres sistemas operativos y los dos dispositivos móviles más populares o de mayor uso en el mercado.

Con los sistemas operativos se toma que para Windows se plantea una solución desarrollada en .Net. De la misma manera, en el caso de los dispositivos móviles, para Android se desarrollará la propuesta por medio de Android SDK con Android Studio.

Capítulo 4. Análisis del Diagnóstico

Para poder establecer las bases de la investigación, y como se indica en la metodología de ciencia de diseño que fue seleccionada, los lineamientos de los ciclos de relevancia y rigor ayudarán a poder definir cuáles serán los requerimientos necesarios para el desarrollo de un nuevo sistema de mitigación para los ataques de *Spoofing* en redes inalámbricas, es necesario estudiar el alcance del ataque en los diferentes dispositivos a los cuales tienen acceso los empleados para poder desempeñar sus labores, ya sea computadoras, teléfonos inteligentes o tabletas.

De igual manera, bajo dichos lineamientos de la metodología es necesario analizar y probar los mecanismos actuales para la mitigación del ataque de *Spoofing* que se encuentran al alcance de los usuarios o de medianas y pequeñas empresas sin la necesidad de incurrir en un alto costo para añadir una capa adicional de seguridad a su entorno.

Como último paso se necesita realizar un diagnóstico de las capacidades de desarrollo con que cuenta cada entorno donde fueron desarrollados los diferentes dispositivos, como se establece en el ciclo de rigor, lo cual llevará a poder definir los últimos detalles necesarios para construir nuestro artefacto -como lo define la metodología de ciencia de diseño-, el cual corresponde a la propuesta de solución.

4.1 Definición de laboratorio

Para iniciar nuestro estudio es necesario establecer las herramientas para realizar los laboratorios de pruebas (*Pentesting*), al igual que todos los aspectos técnicos necesarios de que constituyen a los escenarios de los laboratorios.

4.1.1 Definición de protocolos

Como punto de partida, es necesario primero establecer detalles que se mencionarán continuamente en los diferentes laboratorios y dispositivos. Por ello, como se ve en la Tabla 13, en el espectro de las redes inalámbricas wifi, la evolución de este protocolo, lo cual va de la mano con la compatibilidad que tienen los diferentes dispositivos por utilizar en los laboratorios, ya que es necesario dejar claro que cada versión tiene retrocompatibilidad con el protocolo anterior, pero por obvias razones no todos los dispositivos tienen compatibilidad con todos los protocolos de wifi que prosiguen.

Tabla 13. Protocolos de wifi

Nombre común	Protocolo	Frecuencia	Velocidad máxima de datos
WiFi 1	802.11b	2.4 GHz	11 Mbps
WiFi 2	802.11a	5 GHz	54 Mbps
WiFi 3	802.11g	2.4 GHz	54 Mbps
WiFi 4	802.11n	2.4 o 5 GHz	450 Mbps
WiFi 5	802.11ac wave1	5 GHz	866.7 Mbps
WiFi 5	802.11ac wave2	5 GHz	1.73 Gbps
WiFi 6	802.11ax	2.4 o 5 GHz	2.4 Gbps

Fuente: Intel (2021).

4.1.2 Definición de enrutadores (*routers*)

El siguiente conjunto por definir para la base del laboratorio corresponde a los enrutadores (*routers*), los cuales serán utilizados para poder establecer todas las diferentes pruebas base y así llegar a poder determinar la estabilidad y seguridad que proveen a los diferentes dispositivos o clientes, con la configuración de fábrica en la cual fueron vendidos y que el usuario final utiliza, para lo cual se detalla la lista en la Tabla 14.

Tabla 14. Lista de enrutadores (*routers*) de laboratorios

Nombre de *Router*	**Protocolos**
Nexxt Nebula 150	802.11 b/g/n
Raspberry Pi 3B+ OpenWRT	802.11 b/g/n/ac
ASUS RT-AC-1200	802.11 a/b/g/n/ac
Verizon FIOS G3100	802.11 a/b/g/n/ac/ax
TP-Link AX1800 Dual Band	802.11 a/b/g/n/ac/ax

Fuente: Elaboración propia.

4.1.3 Definición de redes inalámbricas

Como parte de los laboratorios, con estos enrutadores se define un conjunto de diferentes redes inalámbricas para cubrir los diferentes protocolos con los distintos tipos de encriptación disponibles, los cuales no solo serán utilizados para probar la compatibilidad de los dispositivos clientes por conectarse a estas redes, sino que también serán utilizados para explotar las vulnerabilidades una vez ensayado el ataque en los diferentes laboratorios, y para replicar la efectividad del nuevo sistema de mitigación propuesto en esta investigación, por lo cual, como se

lista detalladamente en la Tabla 15, se utilizarán las diferentes redes inalámbricas a lo largo de todo el proceso de pruebas de esta investigación.

Tabla 15. Redes inalámbricas utilizadas en laboratorios

Wireless	Seguridad
Open2.4GHz_b/g/n	Ninguna
Nexxt150_2.4GHz_b/g/n	Mixto WPA/WPA2 - PSK
Open5GHZ_ac	Ninguna
AsusAC1200-5GHZ_ac	WPA2-Personal
Open5GHz_ac/ax	Ninguna
Verizon5GHZ_ac/ax	WPA2
Open5GHz_ax	Ninguna
TPLinkAX1800_5GHz_ax	WPA/WPA2-Personal
TPLinkAX1800_2.4GHz	WPA/WPA2-Personal
TPLinkAX1800_5GHz_ax	WPA2/WPA3-Personal
TPLinkAX1800_2.4GHz	WPA2/WPA3-Personal

Fuente: Elaboración propia.

4.1.4 Definición de teléfonos inteligentes

Ahora con los varios de los detalles técnicos que conforman el laboratorio ya establecido, es necesario definir los diferentes dispositivos por utilizar en dichos laboratorios y pruebas, en el primer grupo tenemos el de teléfonos inteligentes, para poder definir o identificar hechos tales como el fabricante o si el tipo de sistema operativo favorece o no los aspectos de seguridad que se buscan explotar o mejorar con esta investigación. Como se lista en la Tabla 16, se utilizará la siguiente

variedad de teléfonos para poder realizar las pruebas en los diferentes laboratorios y por consiguiente, de ser posible, el nuevo sistema de mitigación por desarrollar como resultado de lo investigado.

Tabla 16. Teléfonos Inteligentes utilizados en laboratorios

Teléfono	Sistema	Protocolos
Galaxy S20 FE 5G	Android 11	802.11 a/b/g/n/ac/ax
IPhone SE	iOS 14.6	802.11 a/b/g/n/ac/ax
Samsung A20s	Android 10	802.11 b/g/n
Samsung Galaxy S4	Android 4.4.2	802.11 a/b/g/n/ac
Samsung Galaxy J3	Android 5.1.1	802.11 b/g/n
Huawei NMO-L22	Android 6	802.11 b/g/n
One Plus 1	Android 6	802.11 a/b/g/n/ac

Fuente: Elaboración propia.

4.1.5 Definición de tabletas inteligentes

En el siguiente conjunto de dispositivos se incluye una lista de tabletas inteligentes, el cual es un poco más reducido ya que la mayoría de los dispositivos a la disposición de las pruebas tenían las mismas características, pero aun así fueron incluidos como parte del proceso de investigación y recolección de datos.

Tabla 17. Tabletas inteligentes utilizadas en laboratorios

Tableta	Sistema	Protocolos
Konka	Android 9.1	802.11 b/g/n
AOC	Android 4.1.1	802.11 b/g/n
Linsay	Android 4.1.1	802.11 b/g/n
Sankey	Android 4.1.1	802.11 b/g/n

iPad Pro	14.5.1	802.11 a/b/g/n/ac

Fuente: Elaboración propia.

4.1.6 Definición de computadores

Como último conjunto de dispositivos para conformar el laboratorio de pruebas están las computadoras, las cuales representan los dispositivos más importantes en la investigación ya que son los de mayor empleo para cualquier usuario, así como para los empleados de las empresas. Se utilizan computadoras en los sistemas operativos más utilizados y recientes en el mercado, que cubran todos los protocolos disponibles para poder obtener los resultados más precisos y así poder llegar a definir la mejor propuesta de solución.

Tabla 18. Computadoras utilizadas en laboratorios

PC	Sistema	Protocolos
HP ProBook	Kali Linux 2021.2	802.11 b/g/n
MacBook Air	BigSur	802.11 b/g/n/ac
Acer es1-411	Windows 10	802.11 b/g/n
MSI Leopard 8RF	Windows 10	802.11 b/g/n/ac
Gigabyte A1	Windows 10	802.11 b/g/n/ac/ax

Fuente: Elaboración propia.

4.2 Análisis de herramientas de *Pentesting*

Es necesario definir el conjunto de herramientas con las que se llevará a cabo no solo los ataques a los dispositivos previamente listados, sino también las herramientas con las que monitoreará o forzará los diferentes mecanismos de protección y protocolos configurados en todos los aparatos por ser evaluados, además de proveer visibilidad a las capacidades y tecnologías a las que un posible atacante tiene acceso.

4.2.1 *Wifi Pineapple*

Esta es una de las herramientas más poderosas y flexibles disponibles en el mercado para realizar auditorías de seguridad en redes inalámbricas, esto gracias a la combinación de *hardware* y *software* de los diferentes módulos que toma ventaja para explotar los protocolos 802.11 (ver ilustración de Figura 18).

Figura 18: Wifi Pineapple. Fuente: Hak5 (2021).

Para conceptos de esta investigación el enfoque estará en cuatro módulos específicos que proveerán todas las evidencias y herramientas para evaluar la seguridad de los dispositivos en la recopilación de información antes y durante un ataque. Para esto, como se observa en la Figura 19, el primer módulo por utilizar es el de “Recon”, el cual corresponde a la fase de reconocimiento de las redes y dispositivos en los alrededores, esto permitirá escanear por intervalos de tiempo, en canales de frecuencia de 2.4GHz, 5GHz o ambos al mismo tiempo y producirá un reporte de cada red y los dispositivos conectados a ellas, esto gracias a ciertas fallas en los protocolos de comunicación que permiten recolectar esta información.

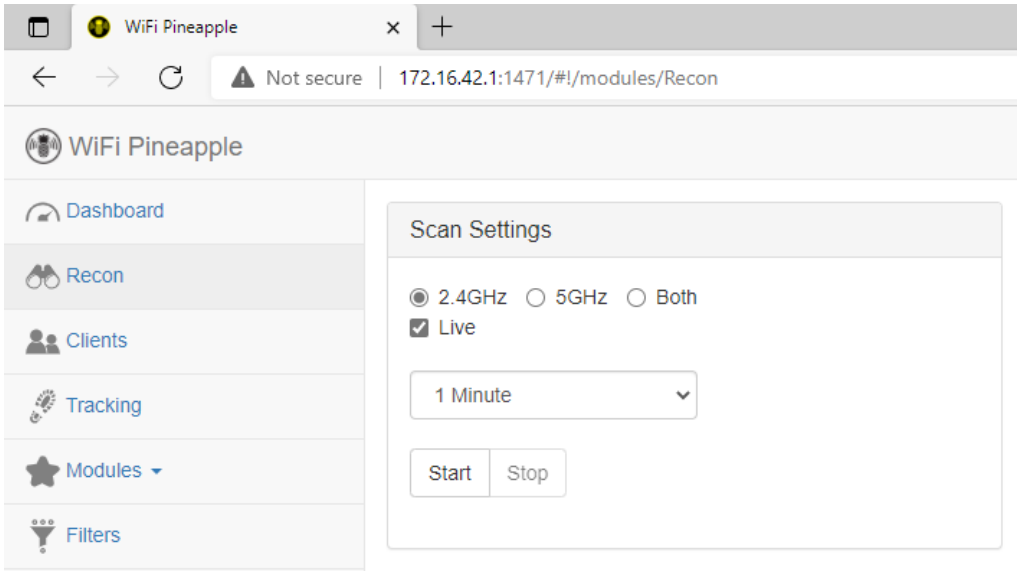

Figura 19. Wifi Pineapple, Módulo Recon. Fuente: Elaboración propia.

El segundo módulo es el de “PineAP”, así como se observa en la Figura 20, es el que permitirá realizar diferentes repuestas, así como recolección de datos, aquí es donde se habilita el modo de monitoreo de todo el dispositivo, al igual que varias casillas de chequeo que para efectos de esta investigación y los laboratorios tienen relevancia.

La primera opción por detallar es la de *Capture SSIDs to Pool*, se describe como “cuando está habilitado, el rastreador guardará los datos SSID de las solicitudes de sonda capturadas en el grupo SSID” (Hak5, 2021, p.1), esto significa que al estar habilitado se capturan los llamados de búsqueda con nombre en texto plano que envían los diferentes dispositivos en busca de una red inalámbrica que conocen o han estado conectados previamente, esto va a ser guardado en la piscina o listado de SSIDs para ser luego explotado.

La segunda opción relevante es la de *Beacon Response*, esta indica en términos generales que cuando se habilita, las solicitudes o *Probe Requests* capturados, con los SSIDs o nombres de las redes inalámbricas que los dispositivos clientes están buscando, serán únicamente transmitidas de vuelta a los mismos que

la enviaron, para que de esta forma no sea visible para otros dispositivos que no son el objetivo.

La tercera opción de relevancia es la de *Broadcast SSID Pool*, esta opción es la que una vez seleccionada se encargará de que todos los SSID capturados sean retransmitidos con el fin de que los clientes que los enviaron intenten conectarse de manera desapercibida a la red falsa o *Spoofed Wifi*, lo que representa el fin de las pruebas.

Se tienen dos opciones más que también son importantes, para los intervalos de transmisión, que corresponden a la opción de *Beacon Response Interval* y a la opción debajo de esta para *Broadcast SSID Pool*, estas opciones darán paso a que al aumentar los intervalos a un nivel más agresivo, los clientes objetivo sean inundados con nuestra transmisión, de manera que se vean aislados de cualquier otra red, y así aumentar las posibilidades de que se conecten a las redes falsas que están siendo publicadas en el ataque.

Por último, dentro de las opciones de este segundo módulo, están las de *Source MAC* y *Target MAC*, estos detalles, una vez escaneado el entorno de redes inalámbricas en las que nos encontramos, permitirán poder clonar o falsificar la dirección MAC, con el fin de ocultar nuestra identidad, o bien para generar un ataque de *Evil Twin* clonando las propiedades exactas de una red legítima.

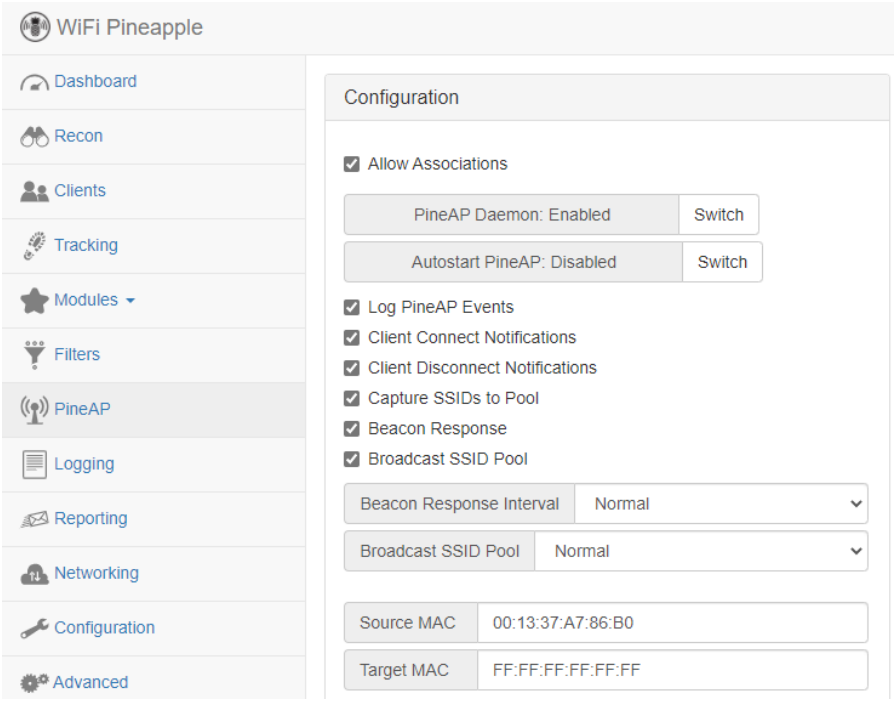

Figura 20. Wifi Pineapple, Módulo PineAP. Fuente: Elaboración propia.

El tercer módulo es el de *Filters*, como se observa en la Figura 21, este módulo permitirá filtrar clientes o redes a los cuales se quiera denegar o habilitar el acceso, esto ayudará para evitar que otros clientes intenten conectarse a la red falsa o bien para solo permitir la opción de conexión a los dispositivos objetivo en nuestros laboratorios.

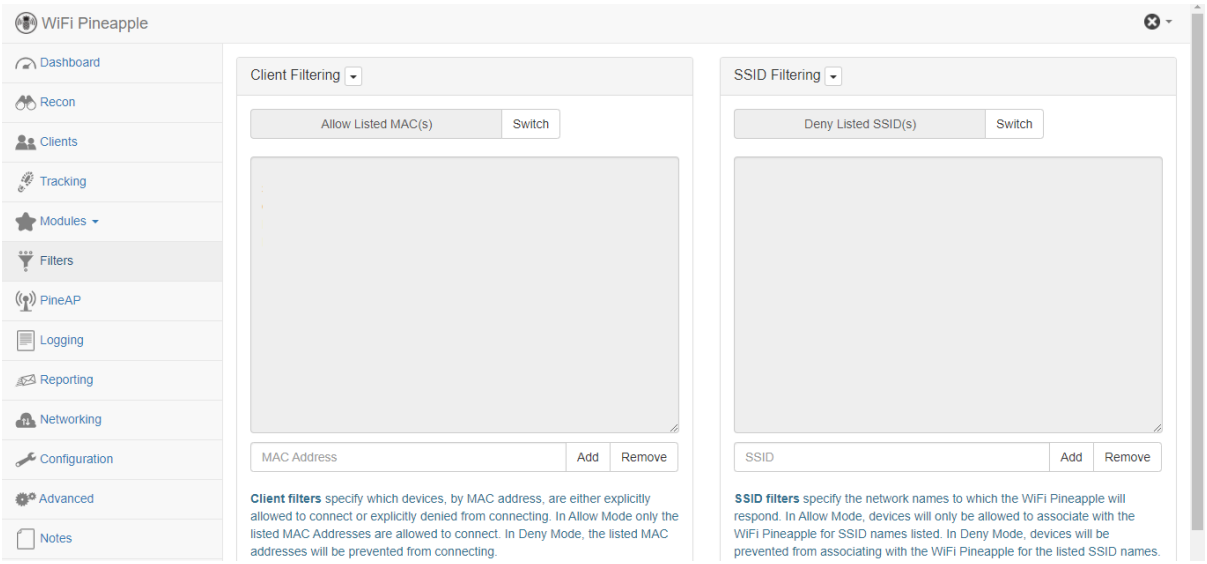

Figura 21. Wifi Pineapple, Module Filter. Fuente: Elaboración propia.

El cuarto y último módulo por especificar es el de *Logging*, este -como se aprecia en la Figura 22-, provee la información en detalle que ha sido capturada de los clientes a los cuales se tiene como objetivo, pero de la misma manera se puede llegar a capturar por defecto la información de cualquier dispositivo que esté haciendo escaneos, proporcionando *Probe Requests* de las redes inalámbricas que está buscando para conectarse.

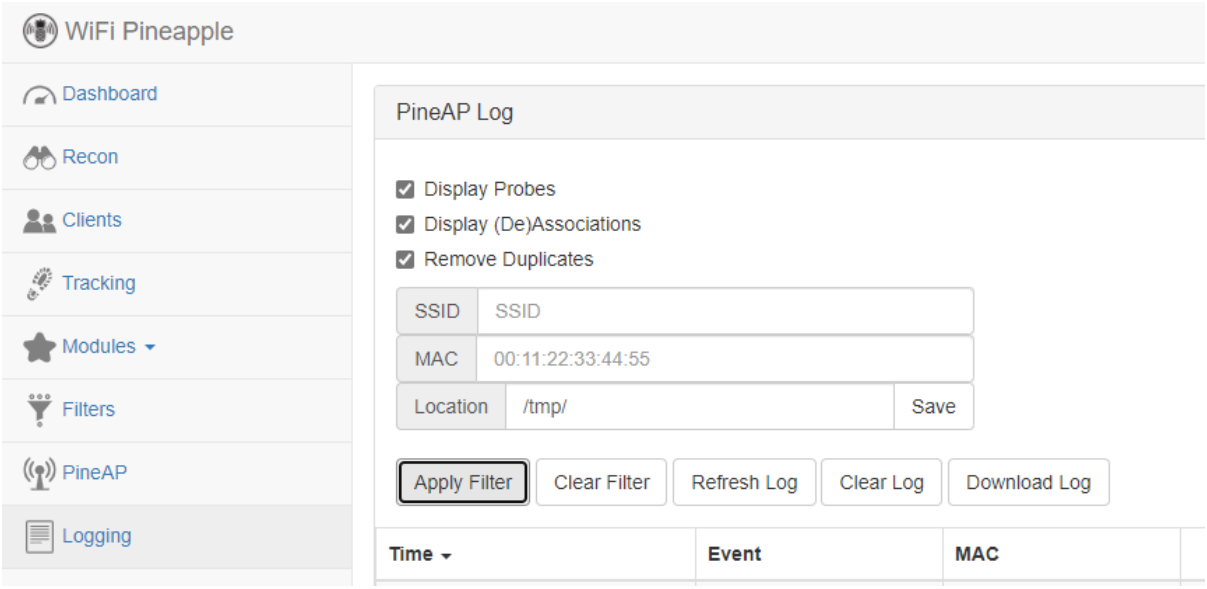

Figura 22. Wifi Pineapple, Módulo *Logging*. Fuente: Elaboración propia.

4.2.2 *Kali Linux*

Esta herramienta o sistema operativo es de los más conocidos en el área de auditorías de seguridad y de *Pentesting* (Offensive Security, 2021), ya que cuenta con una amplia gama de herramientas de código abierto ya previamente configurada y lista para su uso al alcance del usuario.

En este sistema el foco de la investigación está primero en el dispositivo AWUS1900 (ver Figura 23), el cual es un adaptador USB de red inalámbricas compatible con los protocolos 802.11a/b/g/n/ac, como característica indispensable para la investigación permite ser utilizado en modo de monitoreo e inyección de

paquetes, además de contar con alto alcance de señal, lo cual es indispensable para nuestros laboratorios.

Figura 23. Kali Linux, Módulo AWUS1900. Fuente: Alfa Network Inc. (2021)

Por último, la otra herramienta indispensable para nuestra investigación, que se encuentra en Kali Linux, es Airgeddon (ver Figura 24), esta herramienta cuenta con un conjunto de funciones que permiten el monitoreo de las redes al alcance, ataques de denegación de servicio para realizar desautenticación de los clientes en el laboratorio, al igual que para realizar el ataque de *Evil Twin* y así clonar cualquier red legítima.

La mayor ventaja de esta herramienta son las funciones de monitoreo de la red y clientes, al igual que la capacidad para realizar ataques de denegación de servicio en el laboratorio y así comprobar la viabilidad del estudio.

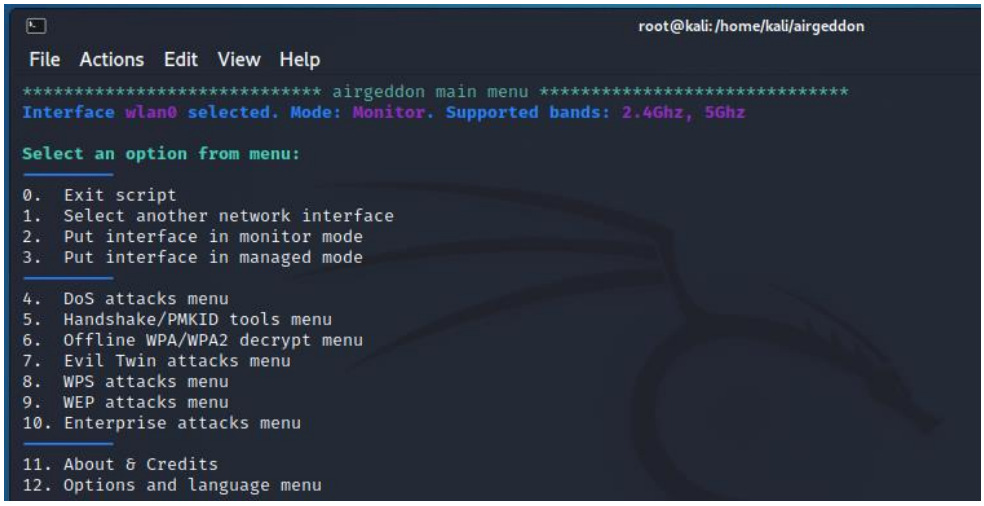

Figura 24. Kali Linux, Módulo Airgeddon. Fuente: Elaboración propia.

4.2.3 Reloj Desautenticador

Este dispositivo, como se muestra en la Figura 25, consiste en un reloj construido para ser utilizado como un kit de desarrollo con el fin de realizar varios ataques hacia redes y dispositivos inalámbricos, por medio del chip ESP8266 (DSTIKE, 2021), el cual permite realizar funciones de monitoreo en inyección de paquetes.

Figura 25. Reloj Desautenticador. Fuente: DSTIKE (2021)

Este reloj representa una herramienta más para los laboratorios, ya que permitirá poder atacar los dispositivos por evaluar, con el fin de generar una

denegación de servicio distribuida (DDoS) al ser utilizado en conjunto a las demás herramientas.

4.3 Análisis de vulnerabilidad

Establecidos ya el escenario y los diferentes dispositivos, al igual que las técnicas por utilizar para los laboratorios y la recolección de datos, se puede iniciar las pruebas de cada uno en los diferentes escenarios.

4.3.1 Análisis y *pentesting* de teléfonos inteligentes

Para el análisis de los teléfonos inteligentes listados en la Tabla 7 se ha segmentado el laboratorio en cuatro pruebas aisladas, en la primera se analiza los celulares en los protocolos de wifi del 1 al 4 en una frecuencia de los 2.4GHz.

En una segunda prueba se realiza el análisis de los protocolos de wifi del 1 al 5, pero esta vez de la frecuencia de 5GHz hacia los dispositivos aún compatibles en este escenario.

Por último, se realiza dos laboratorios más bajo la frecuencia de los 5GHz, pero esta vez es para probar los protocolos, primero de Wifi 5 como modo de compatibilidad de Wifi 6, y por último solo de Wifi 6 como modo nativo para documentar el alcance del ataque, al igual que los resultados con los dispositivos.

4.3.1.1 Redes 2.4GHz con 802.11 b/g/n

En este laboratorio, al ser el inicial, se ha definido la primera red de inalámbrica de pruebas (ver Tabla 7) con contraseña y la seguridad máxima que nos otorga este enrutador como se denota en la Figura 26.

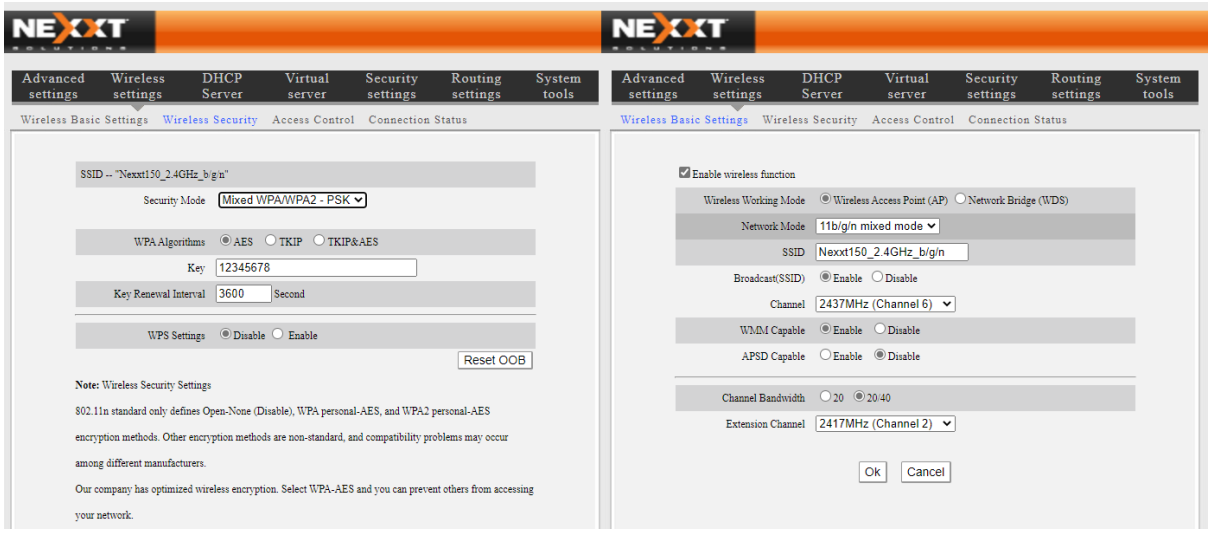

Figura 26. Redes 2.4GHz, Configuración enrutador. Fuente: Elaboración propia.

Al definir esta red inalámbrica y realizar el ataque de denegación de servicio, uno por uno a los teléfonos conectados, realizan un intento de conexión a la red falsa o clonada, no logran autenticarse ya que estas envían la contraseña al *Wifi Pineapple*, que en un escenario real la desconoce en primera instancia, debido a esto queda claro que los dispositivos no van a lograr caer en este ataque, por lo cual se identifica que esta es una ventaja para el dispositivo.

En el siguiente escenario con el mismo enrutador se crea una red abierta, esto quiere decir que no tiene o solicita contraseña a los clientes que quieran conectarse, práctica común en algunos centros de reunión o eventos. Esta red, como fue definida en la Tabla 6, corresponde a la red Open2.4GHz_b/g/n.

Como se mencionó, el teléfono fue conectado a esta red abierta para que quedara almacenada en su lista de redes conocidas, luego de esto, se vuelve a configurar el enrutador con la primera red y con la misma contraseña y se procede a realizar el escaneo, analizando el primer teléfono, en este caso el Samsung Galaxy S4 y se ejecutarnos el ataque de *Deauth*, como se muestra en la Figura 27.

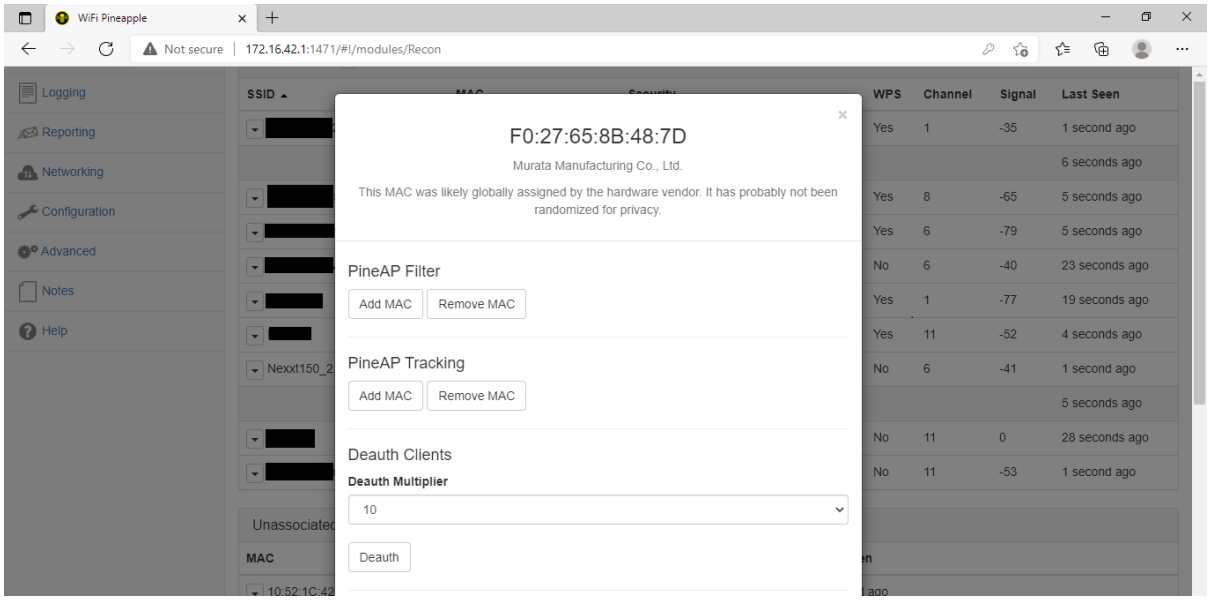

Figura 27. Redes 2.4GHz, Análisis primer teléfono. Fuente: Elaboración propia.

Al realizar un ataque para desautenticarlo e intentar poder capturar *Probe Request* que delatarían que otra red está buscando nuestro teléfono, como se evidencia en la Figura 28, efectivamente se ha podido capturar exitosamente el intento de buscar la red abierta creada con anterioridad.

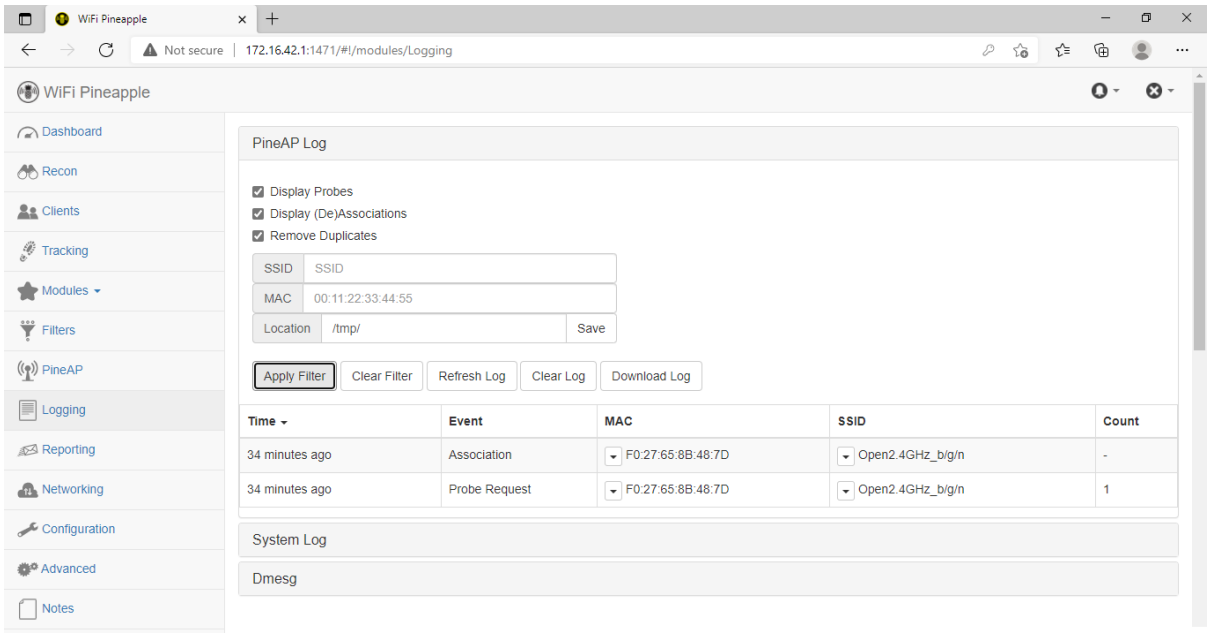

Figura 28. Redes 2.4GHz, *Probe Request* de primer teléfono. Fuente: Elaboración propia.

Como se tiene configurado al *Wifi Pineapple* para que capture este tipo de paquetes para luego transmitir la red falsa, durante esta fase también se han capturado las solicitudes de todos los demás aparatos, por lo cual, ya que se ha logrado el cometido, es necesario eliminar de la piscina de SSID estas otras redes para evitar que algún otro dispositivo no se conecte a las redes falsas, como se muestra en la Figura 29.

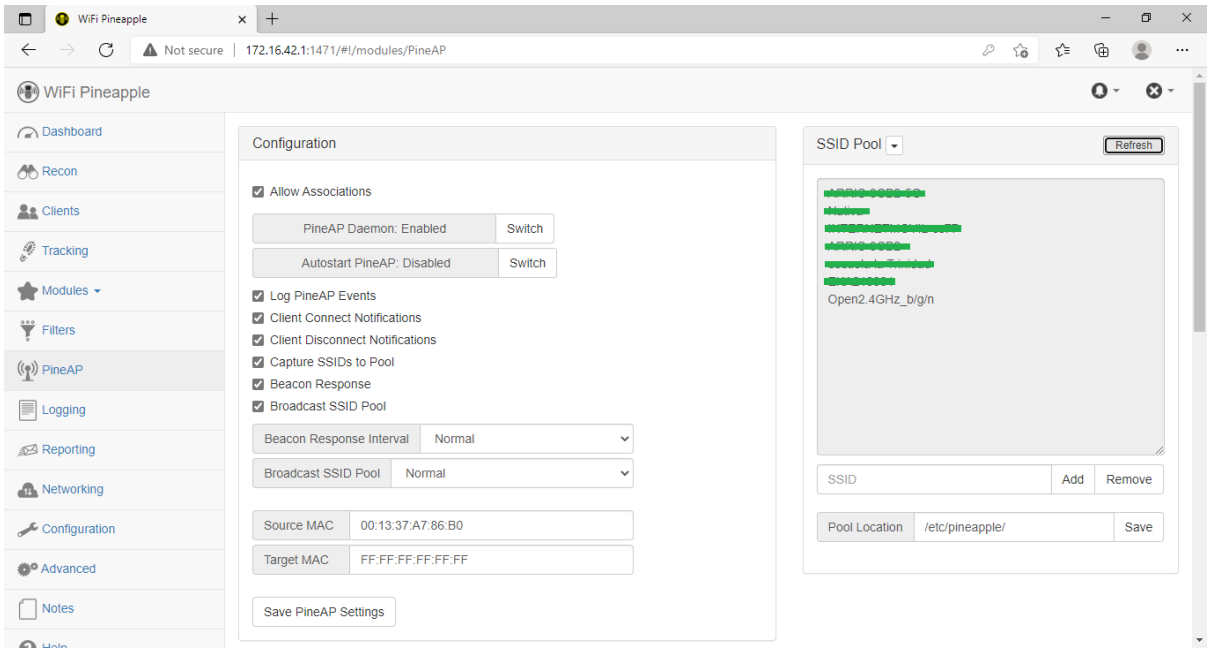

Figura 29. Redes 2.4GHz, emisión de red falsa. Fuente: Elaboración propia.

Como último paso en la prueba, ahora que se está transmitiendo la red falsa, solo se necesita realizar un ataque de denegación de servicio al teléfono para que intente conectarse a la red, lo cual resulta exitoso, como se evidencia en la Figura 30.

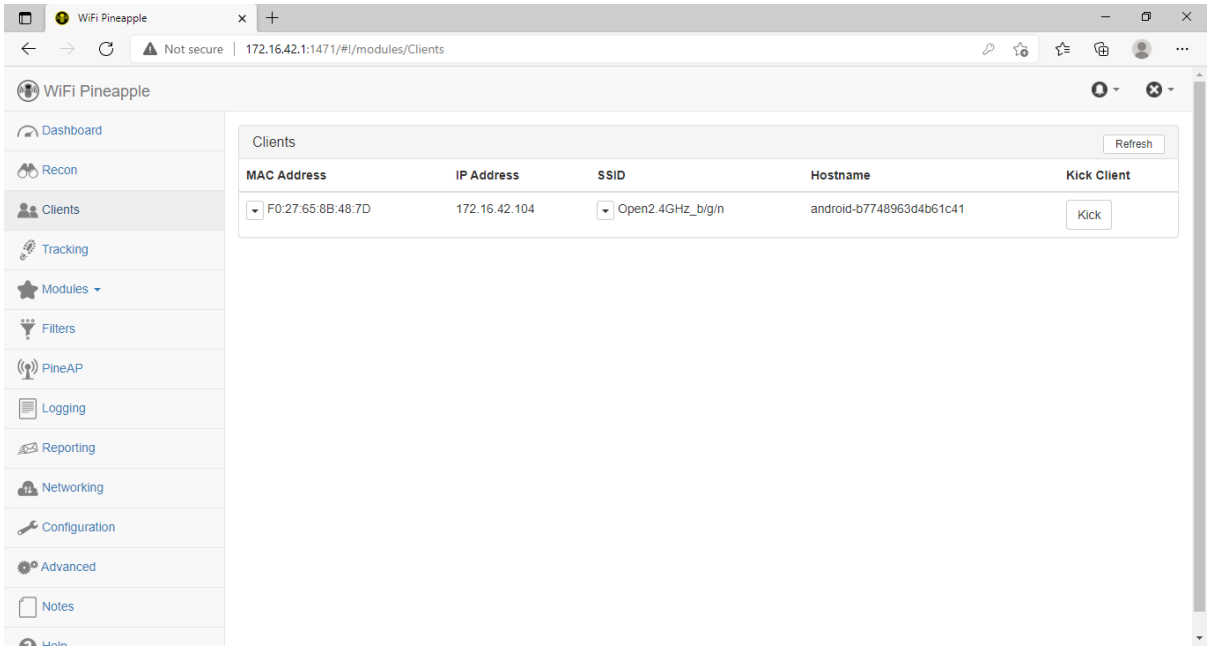

Figura 30. Redes 2.4GHz, ataque exitoso de primer teléfono. Fuente: Elaboración propia.

Una vez identificado que este es el escenario en el cual los teléfonos son engañados en conectarse a la red falsa, al reproducir este mismo escenario en el resto de teléfonos se puede evidenciar que todos se conectan automáticamente a la red al ser aislados por medio del ataque de denegación de servicio, como resultado, en la Figura 31 todos los dispositivos sucumben al ataque.

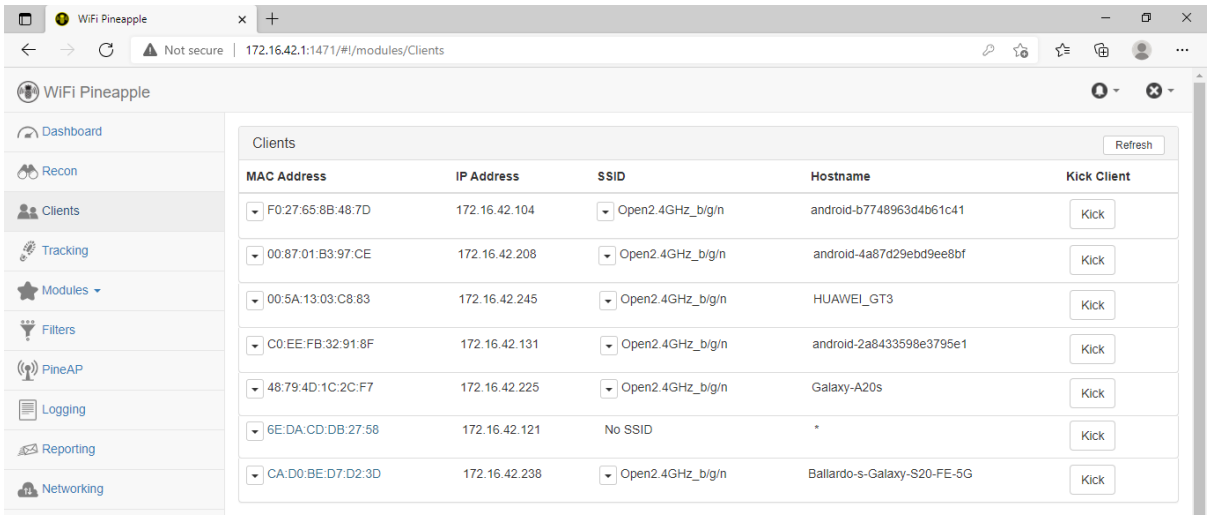

Figura 31. Redes 2.4GHz, ataque con éxito total. Fuente: Elaboración propia.

4.3.1.2 Redes 5GHz con 802.11 ac

Con el escenario por explotar ya definido y con los pasos claros, se procede a realizar el mismo experimento en un escenario con redes de Wifi 5 para evidenciar la vulnerabilidad con protocolos más recientes. Para esto, en el enrutador ASUS RT-AC-1200 se recreará una red segura con contraseña y otra abierta, pero esta nueva abierta estará en el rango y protocolos de 5GHz o 802.11ac, como se muestra la configuración en la Figura 32.

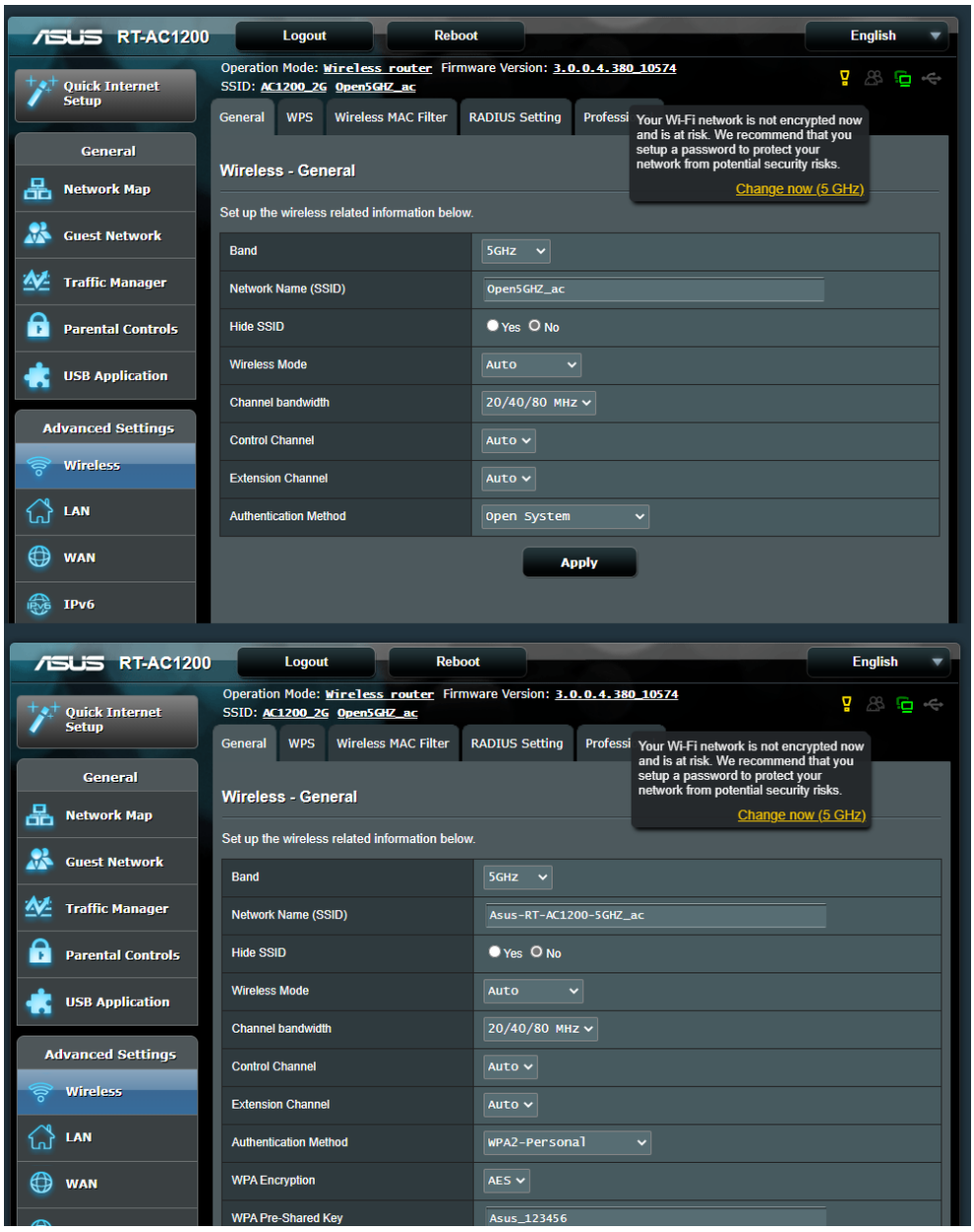

Figura 32. Redes 5GHz, Configuración enrutador. Fuente: Elaboración propia.

Con la configuración establecida, una vez que nuevamente se conectan los dispositivos a la red abierta para registrarla dentro de sus redes conocidas, y nuevamente se conecta a una red segura en este protocolo, al realizar el escaneo de los dispositivos, estos aún pueden ser identificados, como se muestra en la Figura 33.

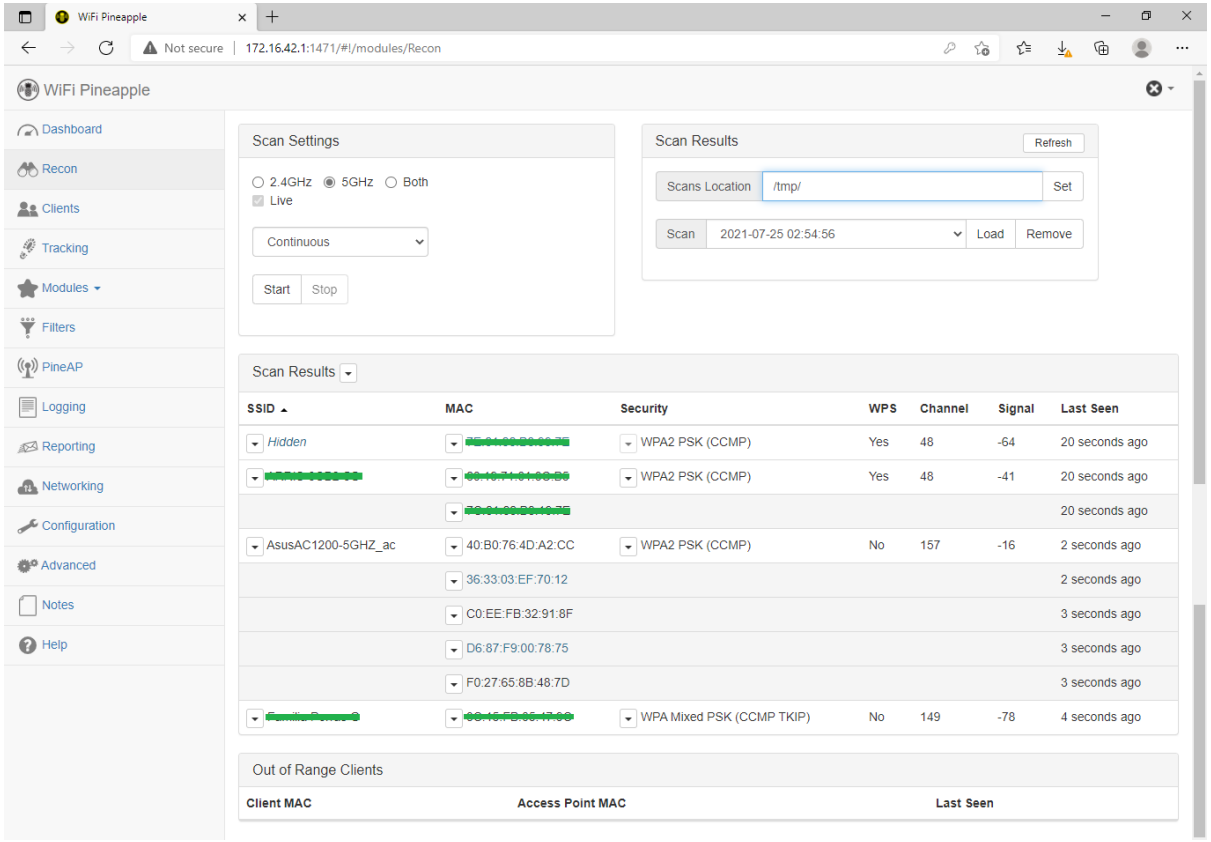

Figura 33. Redes 5GHz, Análisis de redes. Fuente: Elaboración propia.

Con lo que nuevamente, al realizar el ataque de denegación de servicio a cada uno de los teléfonos compatibles con este protocolo, como se evidencia en la Figura 34, se pudo capturar los *Probe Request*, dando a conocer que aún buscan la red abierta una vez que son aislados por medio de la denegación de servicio, por lo que este protocolo no provee ningún cambio o protección, al igual que los protocolos antecesores.

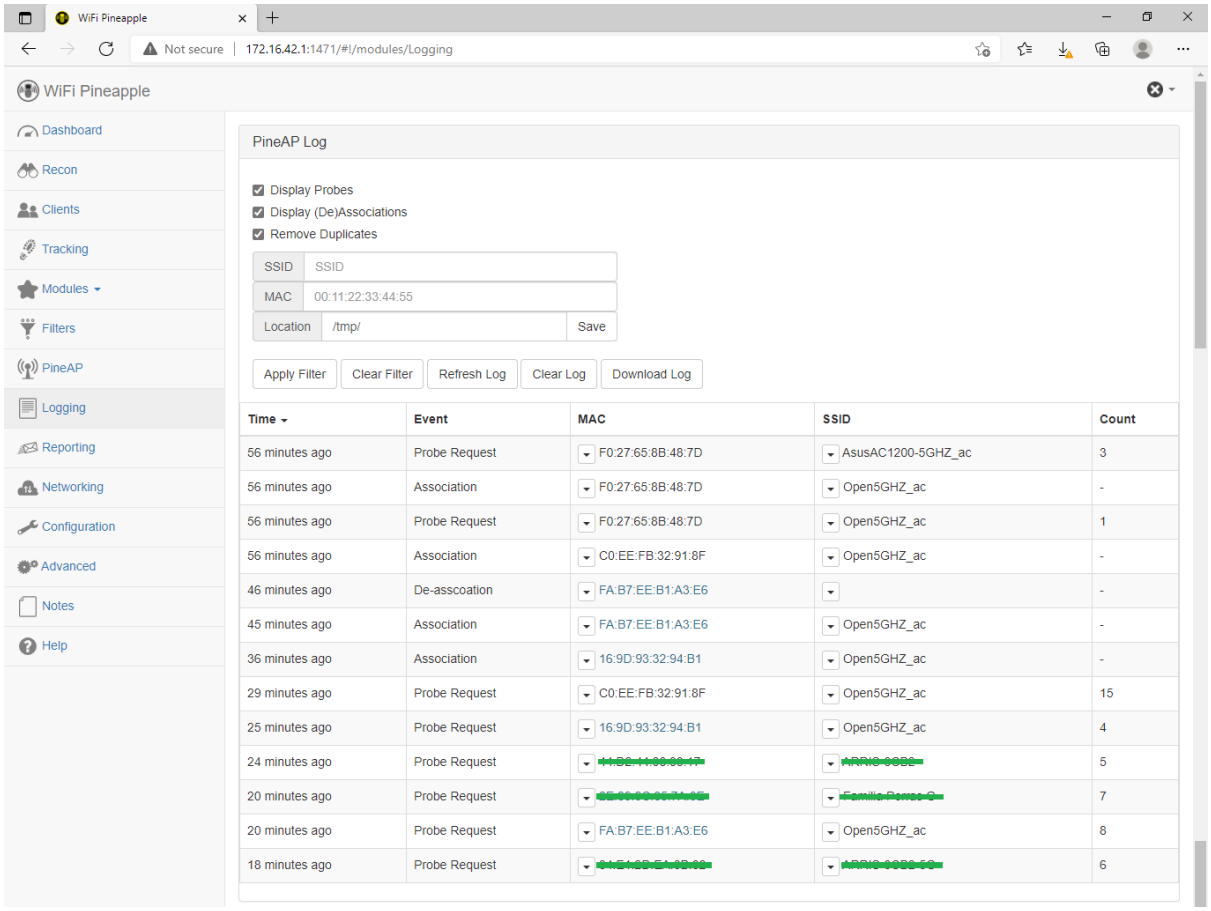

Figura 34. Redes 5GHz, *Probe Request* de teléfonos. Fuente: Elaboración propia.

Por lo que como último paso solo queda desplegar la red falsa de Open5GHZ_ac, para luego por medio de otra denegación de servicio aislar los teléfonos de la red real, con lo que nuevamente cada uno de ellos termina conectándose a la nueva red falsa, como se evidencia en la Figura 35.

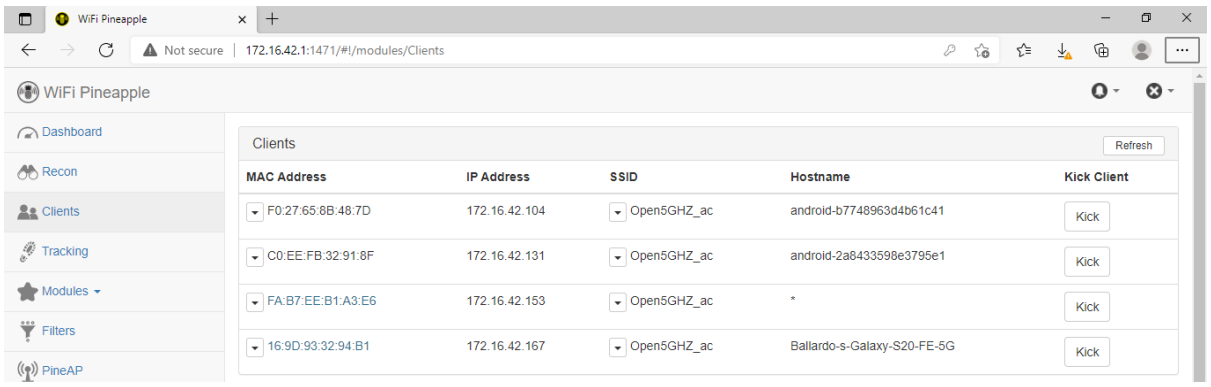

Figura 35. Redes 5GHz, ataque con éxito total. Fuente: Elaboración propia.

4.3.1.3 Redes 5GHz con 802.11 ac/ax

En esta prueba los resultados que se busca recopilar son si se cuenta con alguna mejora, diferencia o ventaja al utilizar un enrutador con soporte nativo del protocolo de Wifi 5 de 802.11ac, pero compatible con el Wifi 6 de 802.11ax por medio de actualización de *software* y no de la circuitería interna, para lo cual se utilizará el Verizon FIOS G3100, como lo demuestra la configuración que denota la Figura 36 para la red llamada Verizon5GHZ_ac/ax.

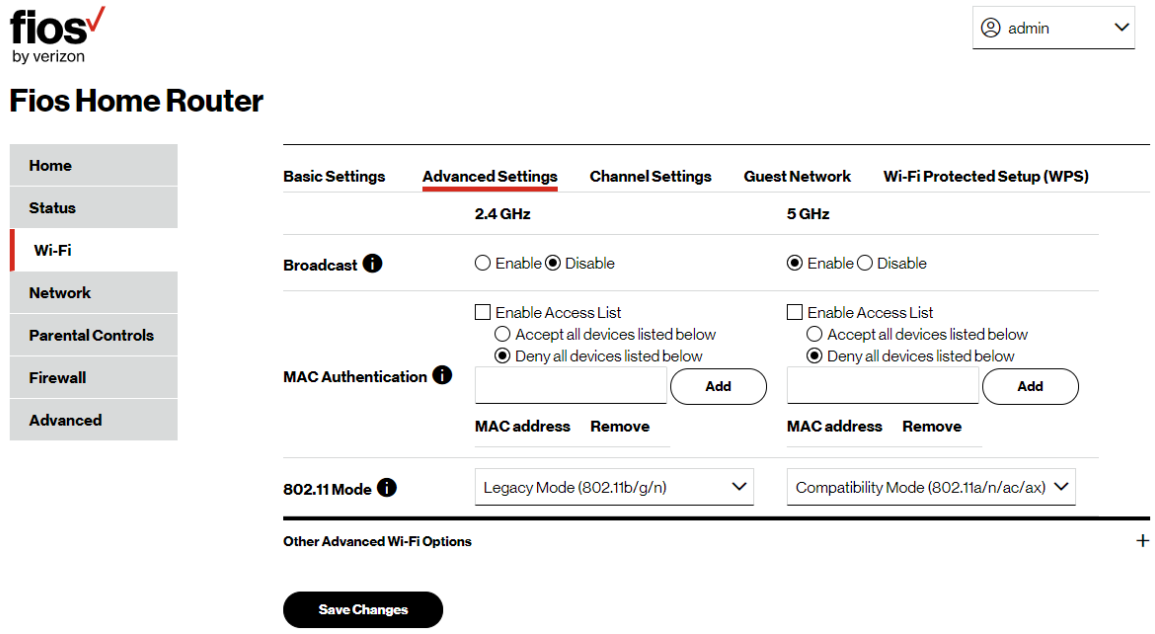

Figura 36. Redes 5GHz, en modo compatibilidad a Wifi 6. Fuente: Elaboración propia.

En esta prueba hay hallazgos interesantes, ya que además de que el enrutador está funcionando en modo de compatibilidad para el protocolo de Wifi 6, únicamente se cuenta con compatibilidad a los teléfonos Galaxy S20 FE 5G y iPhone SE, pero los teléfonos Samsung Galaxy S4 y One Plus 1 aún son compatibles para poder conectarse al enrutador, lo cual se evidencia en la Figura 37.

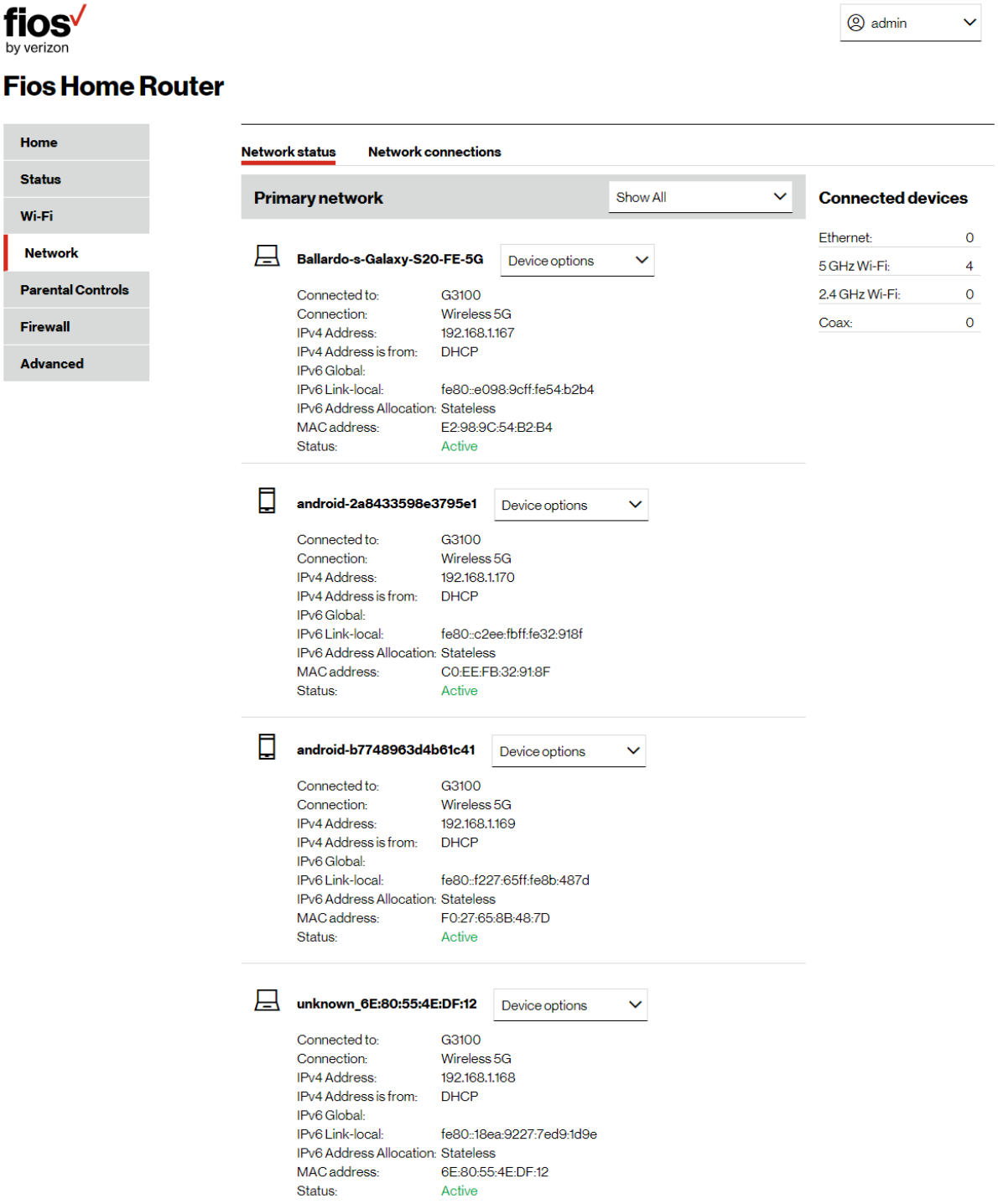

Figura 37. Redes 5GHz, modo compatibilidad de teléfonos. Fuente: Elaboración propia.

Al realizar el escaneo de reconocimiento, se encuentra que a la *Wifi Pineapple* se le dificulta encontrar e identificar el teléfono Samsung Galaxy S4, el

cual también está funcionando en modo de compatibilidad, por lo cual no se puede aislar este teléfono, como se puede ver en la Figura 37, donde solo hay tres.

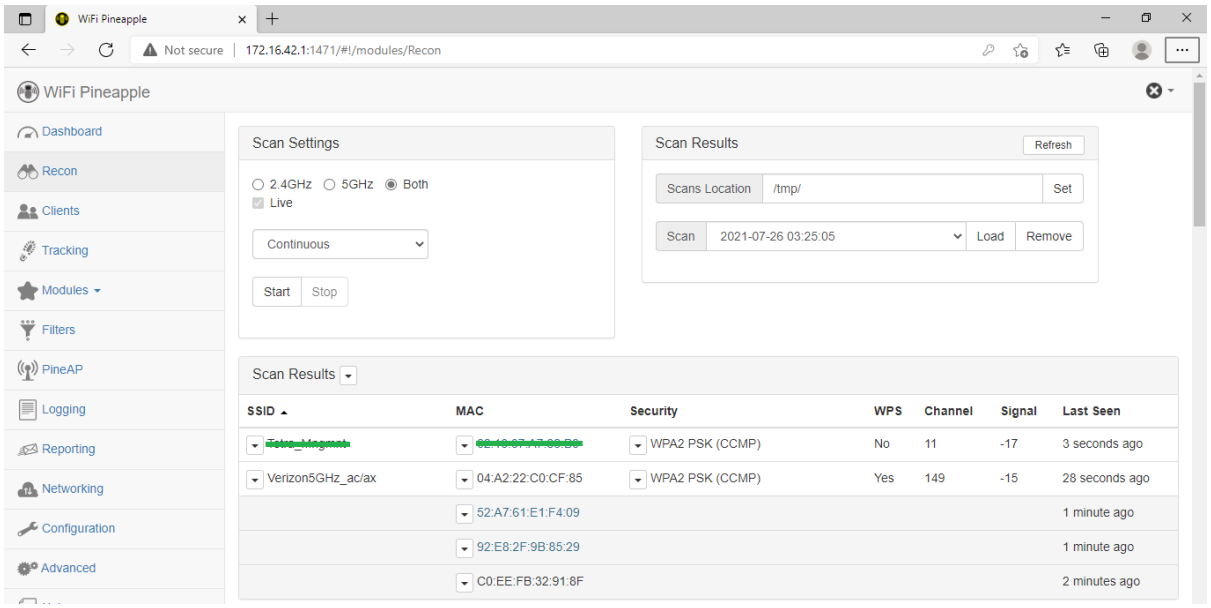

Figura 38. Redes 5GHz, modo compatibilidad, teléfono faltante. Fuente: Elaboración propia.

Para este caso se tomará ventaja de las herramientas de la *Wifi Pineapple*, y se procederá a desautenticar todo lo que se encuentre conectado a la red de prueba, como se ejemplifica en la Figura 39.

Como paso recurrente, previamente se ha creado una red abierta como en los otros laboratorios, a la cual se ha nombrado Open5GHz_ac/ax, y a la que se ha conectado cada uno de los cuatro teléfonos para que nuevamente quedara registrada entre las redes conocidas y por consiguiente por buscar una vez que se lanzara la red falsa.

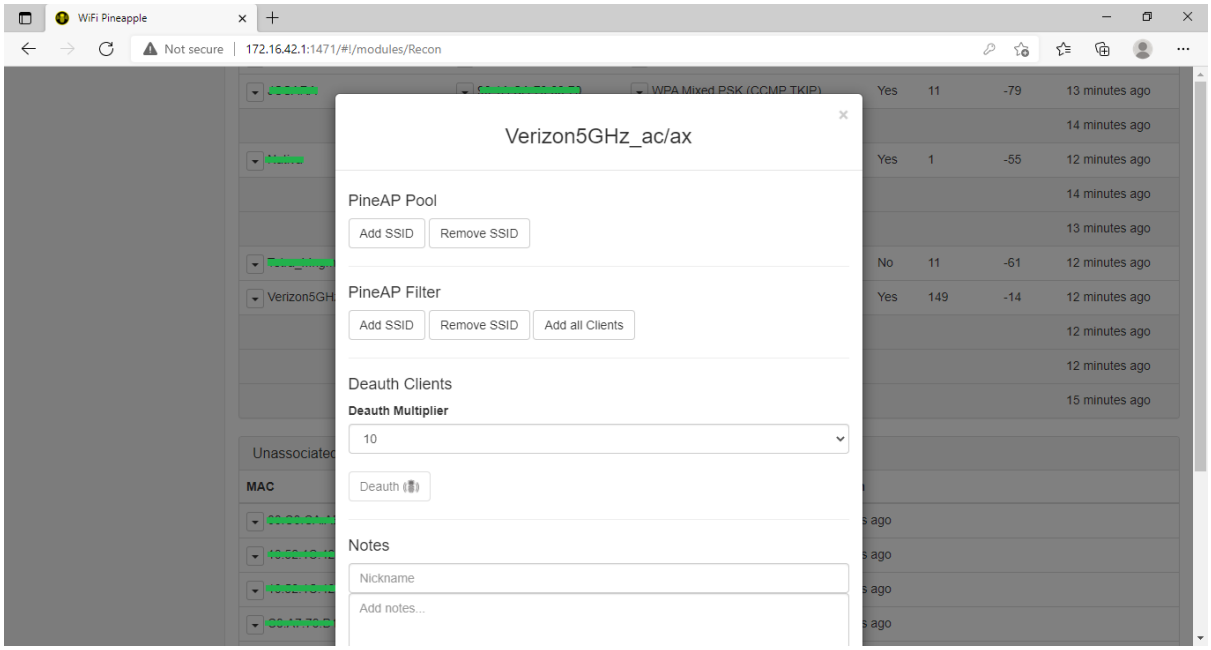

Figura 39. Redes 5GHz, modo compatibilidad, ataque hacia enrutador. Fuente: Elaboración propia.

Para este escenario se recurre a un ataque de denegación de servicio distribuido, ya que se utilizan todas las herramientas mencionadas para aislar los cuatro teléfonos de la red y desplegar la red falsa para engañarlos y llevarlos a conectarse a ella, lo cual, como se evidencia en la Figura 40, resulta ser un ataque exitoso.

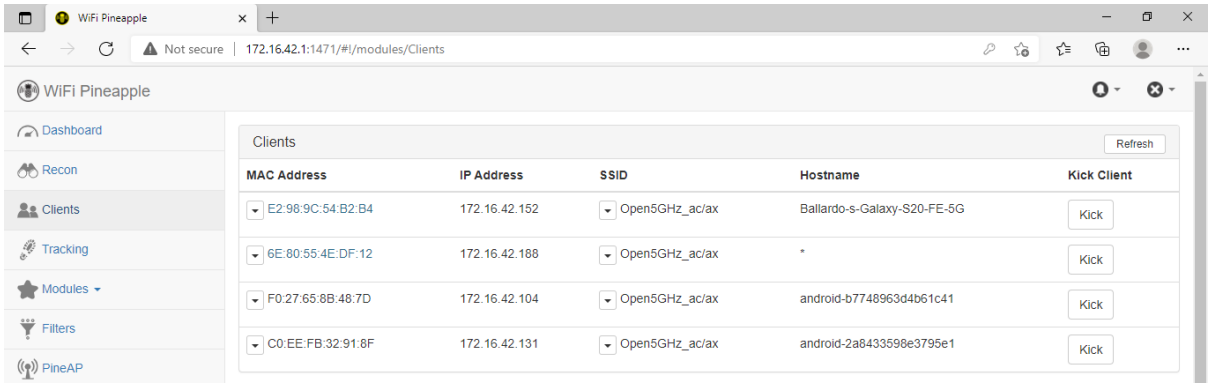

Figura 40. Redes 5GHz, modo compatibilidad, ataque exitoso. Fuente: Elaboración propia.

4.3.1.4 Redes 5GHz 802.11ax

La última prueba se realiza un enrutador con compatibilidad de fábrica con Wifi 6, pero aun con retrocompatibilidad hacia el Wifi 5, con el mismo ejercicio de los laboratorios anteriores, se configura las redes como en la Figura 41.

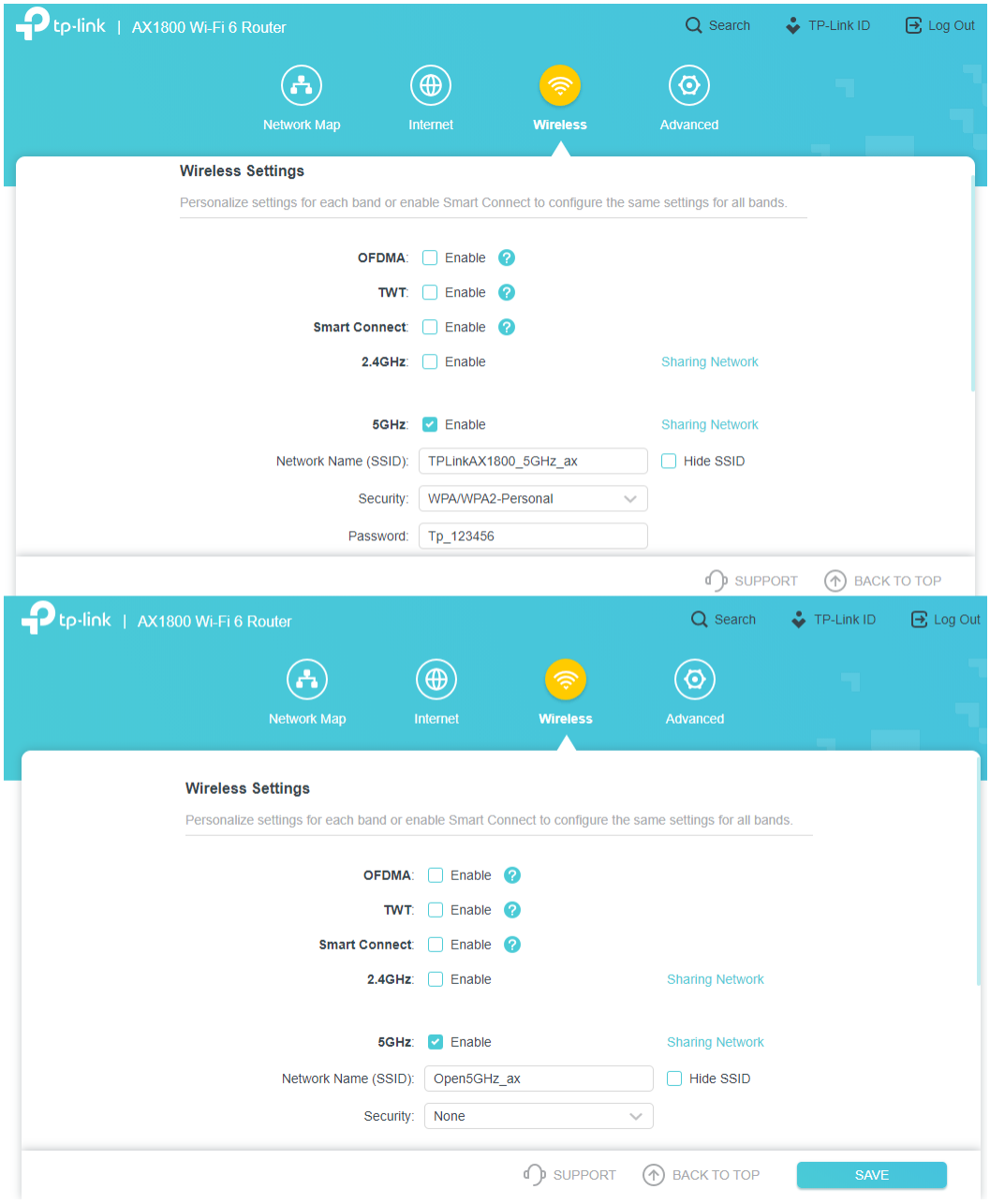

Figura 41. Redes 5GHz, Wifi 6 nativo. Fuente: Elaboración propia.

Debido al modo de retrocompatibilidad que tiene hacia el Wifi 5 con el protocolo 802.11 ac, aún se tiene que los mismos cuatro teléfonos anteriores son

capaces de conectarse a este enrutador y nuevamente se ve que al realizar el escaneo de las redes, el *Wifi Pineapple* solo puede identificar al Galaxy S20 FE 5G y al iPhone SE, como se observa en la Figura 42.

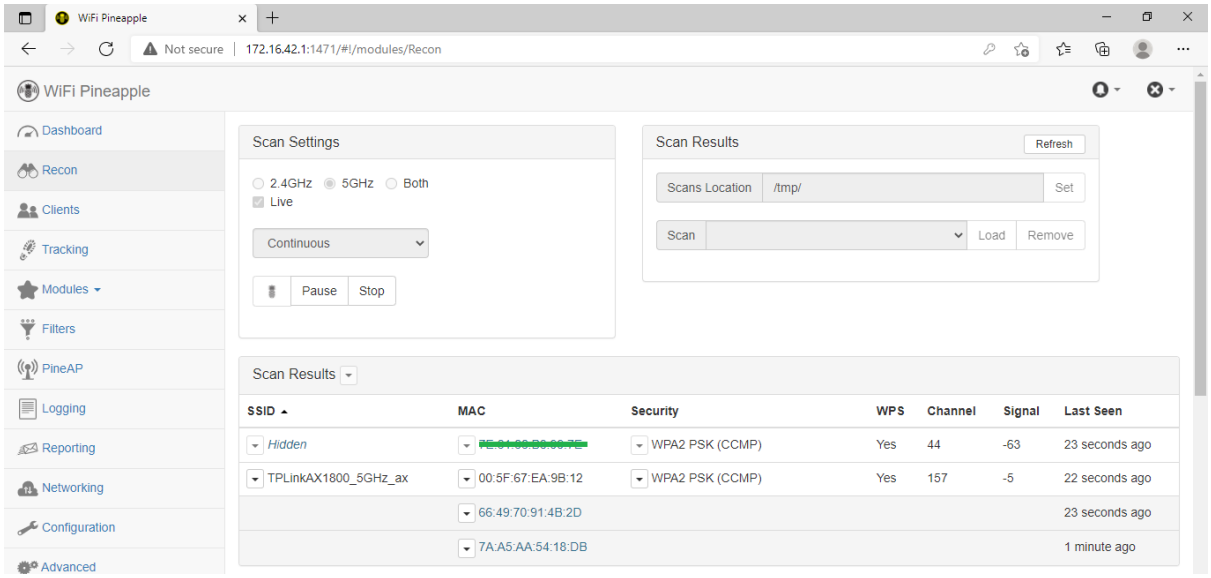

Figura 42. Redes 5GHz, Wifi 6 nativo, escaneo. Fuente: Elaboración propia.

Para ello se realiza el mismo ejercicio, se hace un ataque de desautenticación y se tiene como resultado lo que puede verse en la Figura 43, se observa que efectivamente se han capturado los *Probe Request* de los teléfonos.

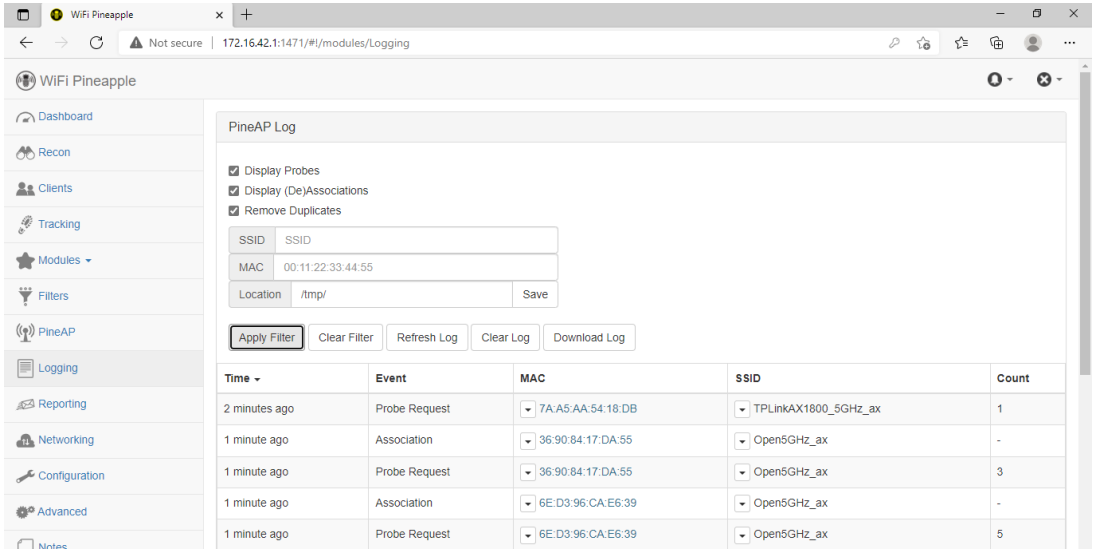

Figura 43. Redes 5GHz, Wifi 6 nativo, *Probe request* capturados. Fuente: Elaboración propia.

Ahora solo se procede a desplegar la red falsa de Open5GHz_ax, se continúa con el ataque de denegación de servicio distribuido y efectivamente uno por uno se logra que los teléfonos se conecten a la red falsa, como el resultado mostrado en la Figura 44.

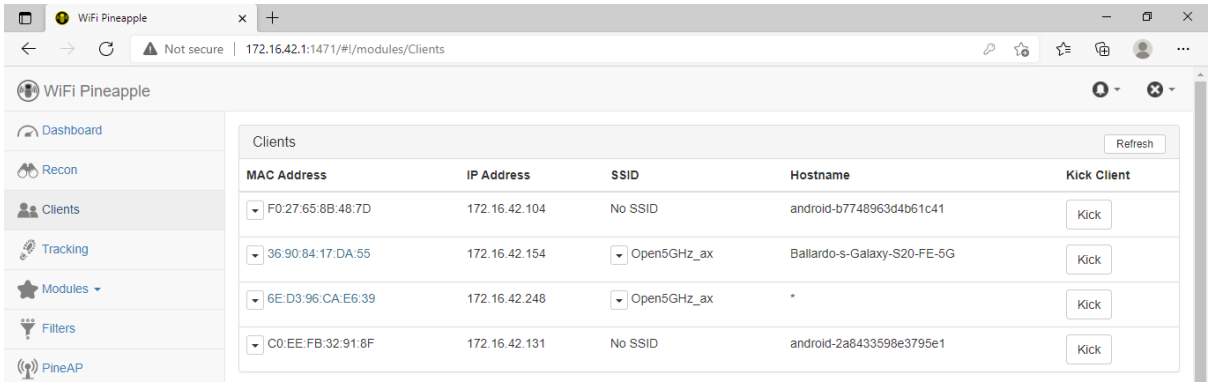

Figura 44. Redes 5GHz, Wifi 6 nativo, ataque exitoso. Fuente: Elaboración propia.

Como un resultado de este último laboratorio, al realizar las redes de prueba se encontró que el teléfono Galaxy S20 FE 5G sí era capaz de detectar y visualmente identificar que las redes originales eran del protocolo de Wifi 6, al agregar un pequeño 6 al ícono de red, como se muestra en la Figura 45.

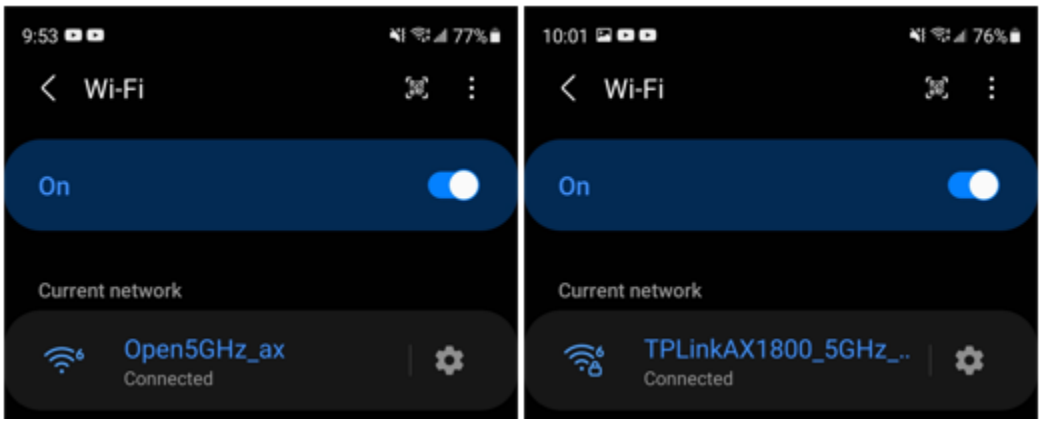

Figura 45. Redes 5GHz, Wifi 6 nativo, ejemplo Galaxy S20 FE 5G. Fuente: Elaboración propia.

Cuando el teléfono es engañado y se conecta a la red falsa, se evidencia claramente cómo la red no está usando el protocolo de Wifi 6, como se muestra en la Figura 46.

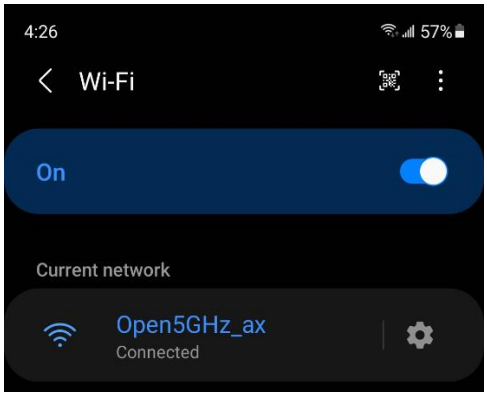

Figura 46. Redes 5GHz, Wifi 6 nativo, ejemplo Galaxy S20 FE 5G en red falsa. Fuente: Elaboración propia.

Haciendo un escaneo externo, como se detalla en la Figura 47, se evidencia que la red válida TPLinkAX1800_5GHz_ax sí se encuentra transmitiendo bajo el protocolo de 802.11ax, pero la red falsa desplegada generada por la *Wifi Pineapple* está transmitiendo bajo el protocolo 802.11g, lo que quiere decir que el teléfono no guarda dicha información de la red inalámbrica.

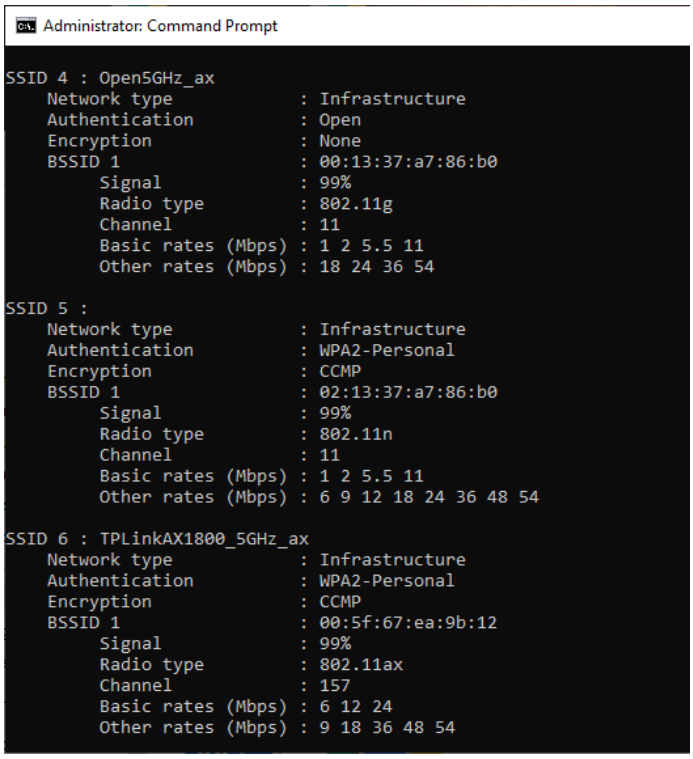

Figura 47. Redes 5GHz, Wifi 6 nativo, escaneo externo. Fuente: Elaboración propia.

4.3.2 Análisis y *pentesting* de tabletas inteligentes

En el análisis para las tabletas, dado que la mayoría cuenta con el sistema operativo de Android 4.1.1, el resultado fue el mismo que en los escenarios de los teléfonos probados bajo la misma versión, pero aún es necesario probar la tableta con Android 9.1 y el iPad Pro para documentar algún cambio.

4.3.2.1 Redes 2.4GHz 802.11 b/g/n

Dado que la única variable de la que no se tiene registro es la tableta Konka, la cual es compatible únicamente con los protocolos 802.11 b/g/n, se ha reproducido el mismo escenario que los laboratorios previos, conectándolo a la red abierta Open2.4GHz_b/g/n y luego a la verdadera, como se demuestra en la Figura 48.

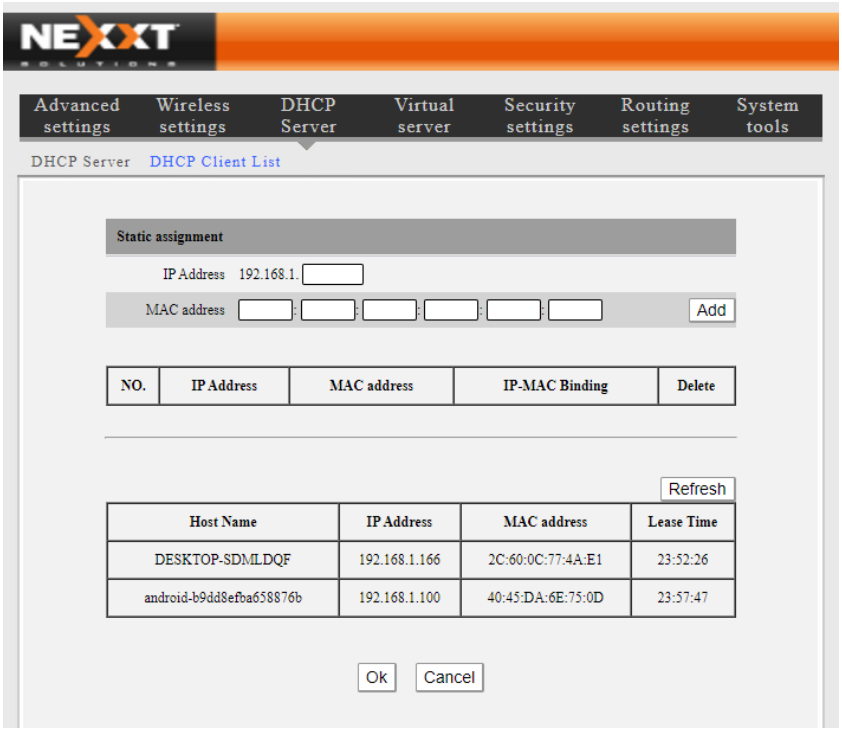

Figura 48. Tableta en 2.4GHz, conectada a enrutador valido. Fuente: Elaboración propia.

Nuevamente, al realizar el ataque de desautenticación por medio de la denegación de servicio previamente ejecutada en los laboratorios anteriores, se

puede ver que sin ninguna resistencia esta tableta se ha conectado a la red falsa, como se muestra en la Figura 49.

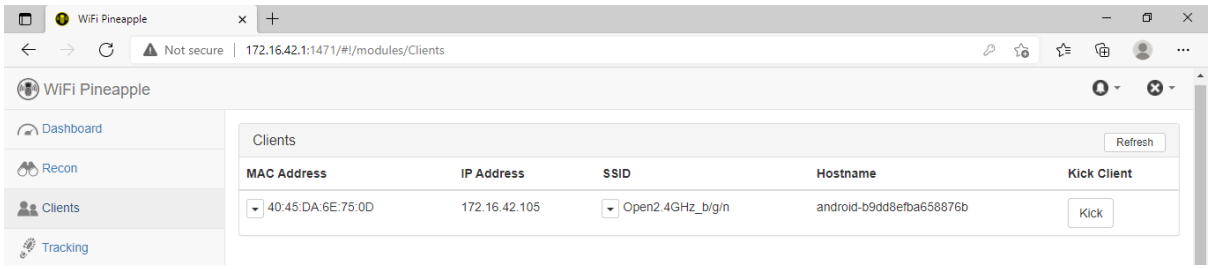

Figura 49. Tableta en 2.4GHz, atacada con éxito. Fuente: Elaboración propia.

Esto demuestra que aún se mantienen las mismas vulnerabilidades encontradas en los sistemas Android de los teléfonos inteligentes.

4.3.2.2 Redes 5GHz 802.11 ac/ax

Para esta última prueba, y dado que el iPad cuenta con soporte al protocolo 802.11ac, se va a realizar la prueba directamente con el enrutador TPLink AX1800 Dual Band, para probar si al contarse con sistema operativo de iOS 14.5.1 se posee alguna medida de seguridad.

Para esto se ha replicado el mismo escenario que los laboratorios anteriores y se ha configurado una red abierta Open5GHz_ax para que quede dentro de la lista de redes conocidas del iPad, y luego una red protegida legítima, la TPLinkAX1800_5GHz_ax que se ha utilizado en los escenarios previos, al que se deja el dispositivo conectado y listo para ser atacado, como se observa en la Figura 50.

En esta prueba se ha realizado el ataque nuevamente, para desautenticar por medio de una denegación de servicio distribuido (DDoS) para engañar al iPad a conectarse a la red falsa.

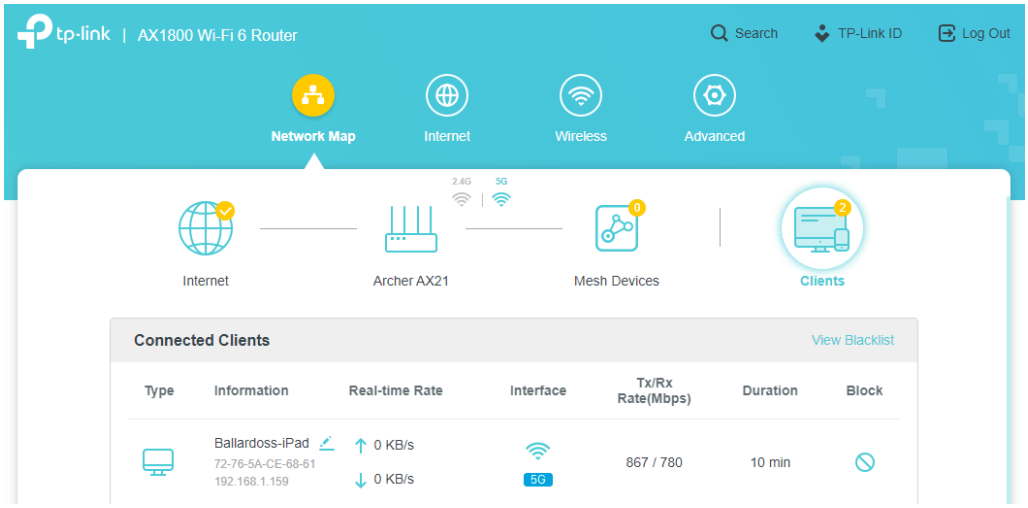

Figura 50. Redes 5GHz, iPad en red válida. Fuente: Elaboración propia.

Como se ha observado previamente con el iPhone, el iPad de igual forma ha caído víctima del ataque, lo cual deja en evidencia que este cuenta con las mismas vulnerabilidades en el sistema, como se aprecia en la Figura 51 y se confirma en la Figura 52.

Figura 51. Redes 5GHz, iPad atacado con éxito. Fuente: Elaboración propia.

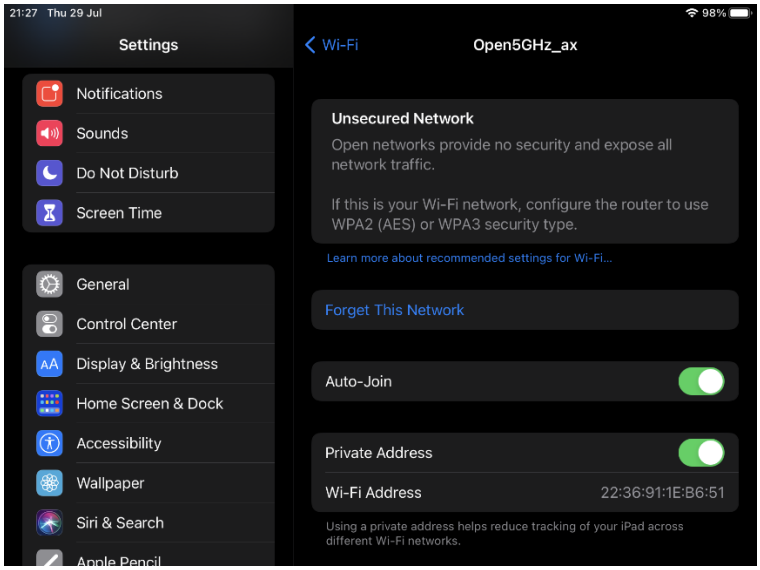

Figura 52. Redes 5GHz, iPad prueba de ataque exitoso. Fuente: Elaboración propia.

4.3.3 Análisis y *pentesting* de computadoras

En este siguiente conjunto de laboratorios se tiene la prueba más importante, ya que las computadoras son de los dispositivos de uso más común y por eso servirán para determinar en su mayor parte los requerimientos para una propuesta de solución.

Para obtener el mejor conjunto de resultados, en primer lugar se estudia este ataque en los equipos bajo el protocolo 802.11 b/g/n como la prueba base que definirá su comportamiento en los siguientes protocolos, pero en este caso se añade un escenario adicional, donde se incluye una computadora con una tarjeta inalámbrica con soporte nativo de fábrica para Wifi 6, con el fin de determinar si al utilizar el equipo más reciente en el mercado va a incorporar algún factor determinante utilizado en los últimos estándares de la tecnología inalámbrica, con lo que se procede a dichas pruebas para obtener los últimos resultados y de esta manera definir los requerimientos finales para la construcción de la solución propuesta.

4.3.3.1 Redes 2.4GHz 802.11 802.11 b/g/n

En este laboratorio de pruebas y experimentación se utilizará nuevamente el mismo modelo de los escenarios anteriores y se creará la red abierta Open2.4GHz_b/g/n, a la cual se conectarán todas las computadoras para que quede guardada en su lista de redes conocidas, para luego, nuevamente en la red Nexxt150_2.4GHz_b/g/n dejar conectados los equipos para lanzar el ataque de reconocimiento y luego la red falsa para intentar que los dispositivos se conecten al ser aislados de la red válida.

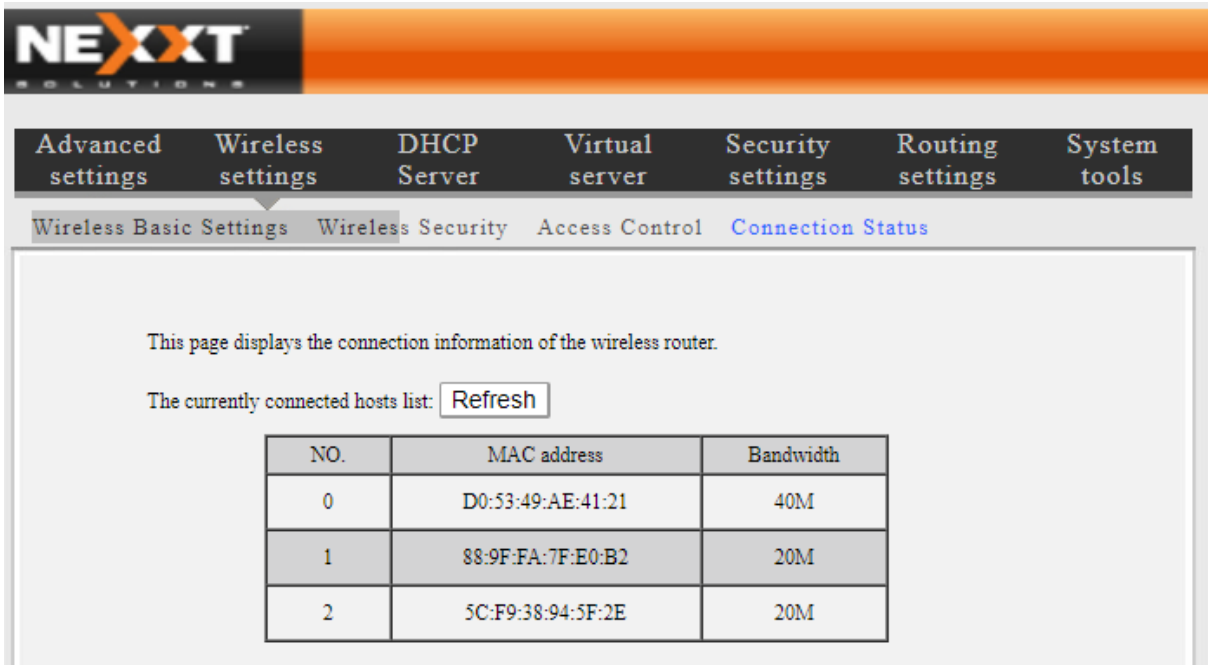

Figura 53: Redes 2.4GHz, computadoras conectadas. Fuente: Elaboración propia.

Como se aprecia en la Figura 53, se tiene conectadas a la red válida las computadoras HP ProBook, Acer es1-411 y MacBook Air, al realizar un escaneo con el *Wifi Pineapple*, como se observa en la Figura 54, las tres han sido detectadas correctamente, lo cual las deja al alcance del siguiente paso, que corresponde al ataque.

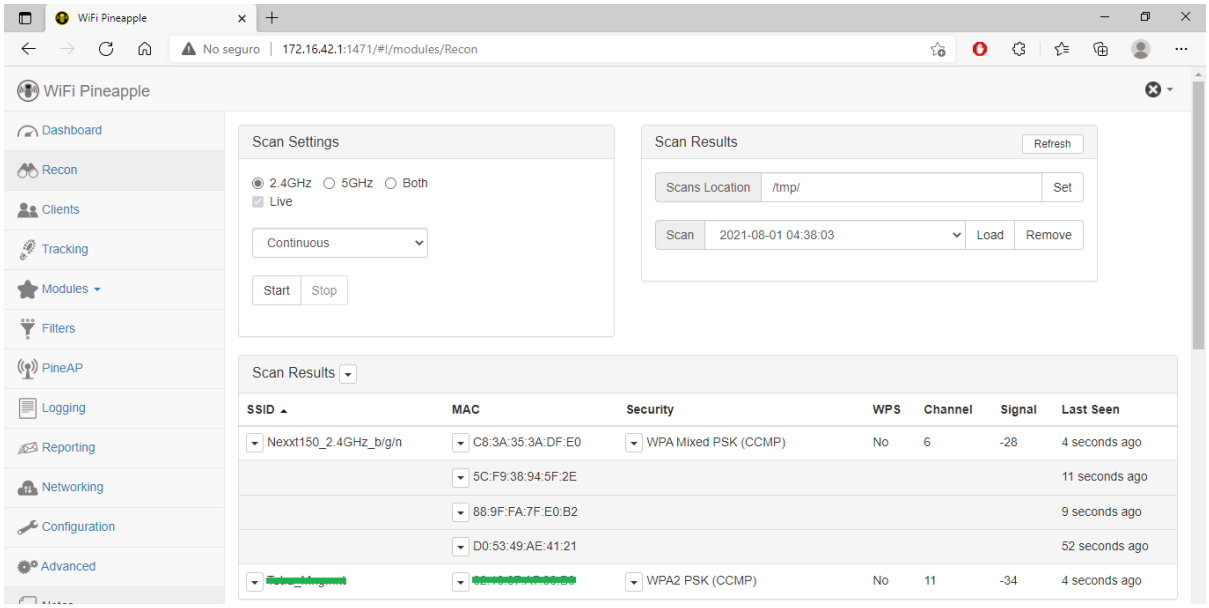

Figura 54. Redes 2.4GHz, computadoras escaneadas. Fuente: Elaboración propia.

Al lanzar el ataque de desautenticación a los equipos, por medio de una denegación de servicio distribuida (DDoS), hasta aislarlas de la red válida, se tiene como resultado en la Figura 55, cómo todas las computadoras se han conectado a la red falsa desplegada con el ataque, por lo cual se sientan las mismas bases o comportamiento visto en los dispositivos y laboratorios anteriores.

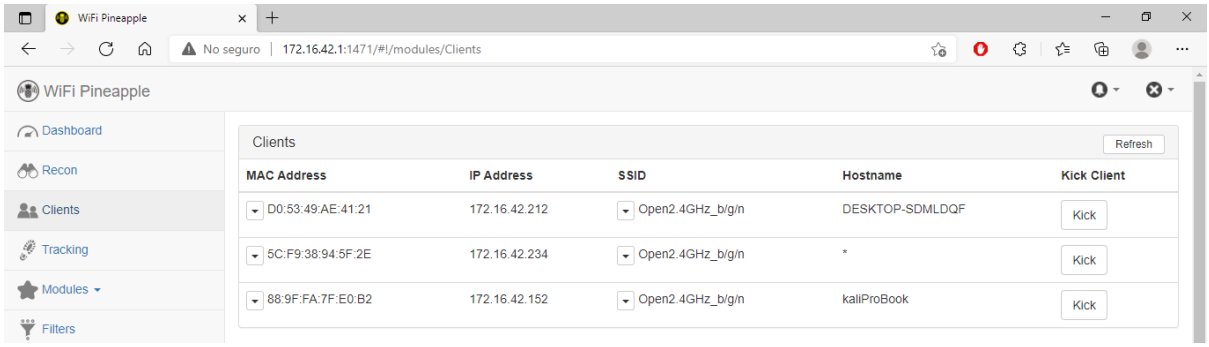

Figura 55. Redes 2.4GHz, computadoras atacadas con éxito. Fuente: Elaboración propia.

Este es un avance importante en la recolección de información para eventualmente construir la solución, para lo cual se evidencia en las Figuras 56, 57

y 58 que las mencionadas direcciones MAC corresponden a la de nuestro laboratorio.

Figura 56. Redes 2.4GHz, MacBook Air. Fuente: Elaboración propia.

Como muestra la Figura 56, nuevamente, a pesar de que se cuenta con un sistema operativo diferente, aún se encuentra vulnerable al ataque.

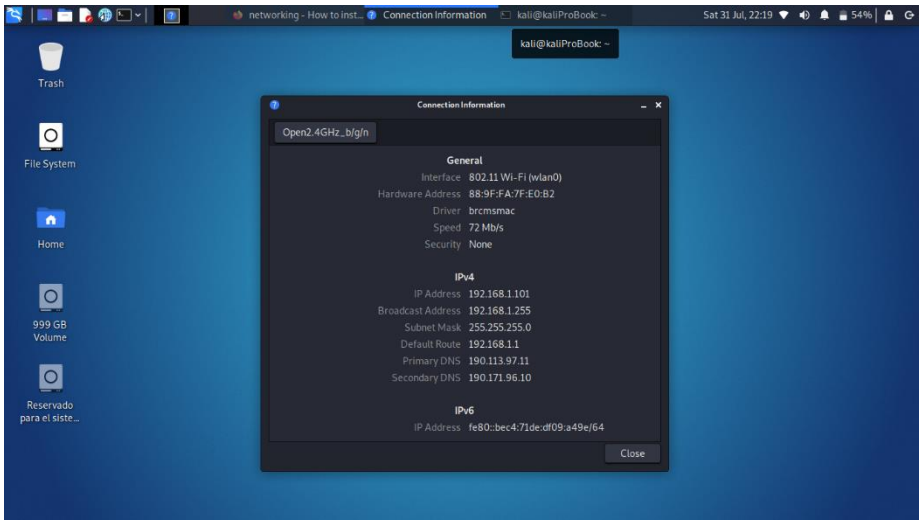

Figura 57. Redes 2.4GHz, Kali Linux. Fuente: Elaboración propia.

El caso con la Figura 57, se evidencia que, aunque la computadora cuente con un sistema operativo Linux, no se encuentra exenta del ataque en estudio.

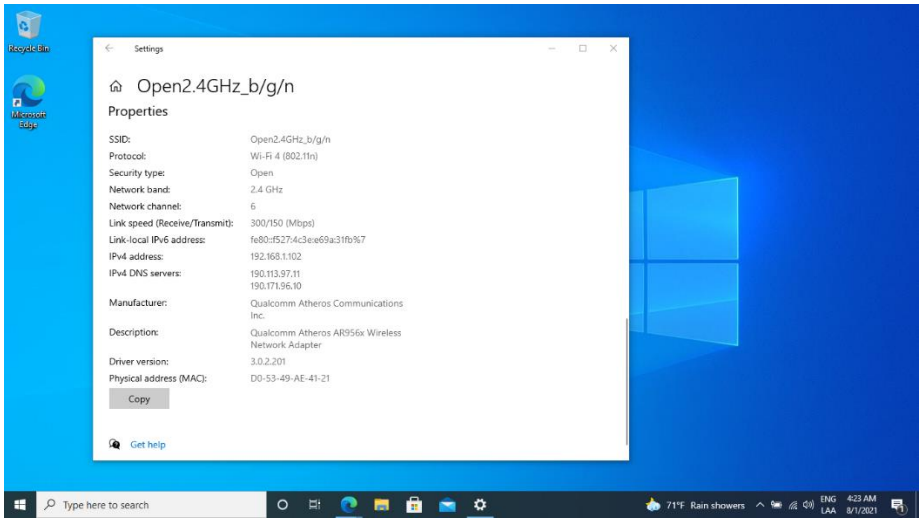

Figura 58. Redes 2.4GHz, Acer es1-411. Fuente: Elaboración propia.

Por último, en el equipo con Windows, se observa que son los mismos resultados evidenciados en todos los demás dispositivos, por lo que esto define ya el camino hacia el diseño de la propuesta de solución.

4.3.3.2 Redes 2.4GHz 802.11 b/g/n con chip ax

En este caso, al ser uno aislado del resto, se evalúa si hay alguna ventaja de seguridad al tener el equipo con los últimos estándares de comunicación, como se muestra en la configuración de nuestro equipo en la Figura 59.

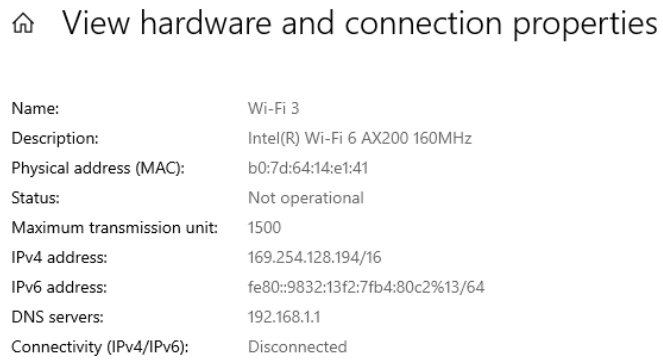

Figura 59. Redes 2.4GHz, computadora Wifi 6 nativa. Fuente: Elaboración propia.

Nuevamente se configura el mismo laboratorio que en las iteraciones pasadas y la red abierta Open5GHZ_ac, a la cual conectamos el equipo para que la

guarde como una de las redes conocidas, y nuevamente se habilita la red válida TPLinkAX1800_2.4GHz, se deja conectado en espera del ataque, como se muestra en la Figura 60.

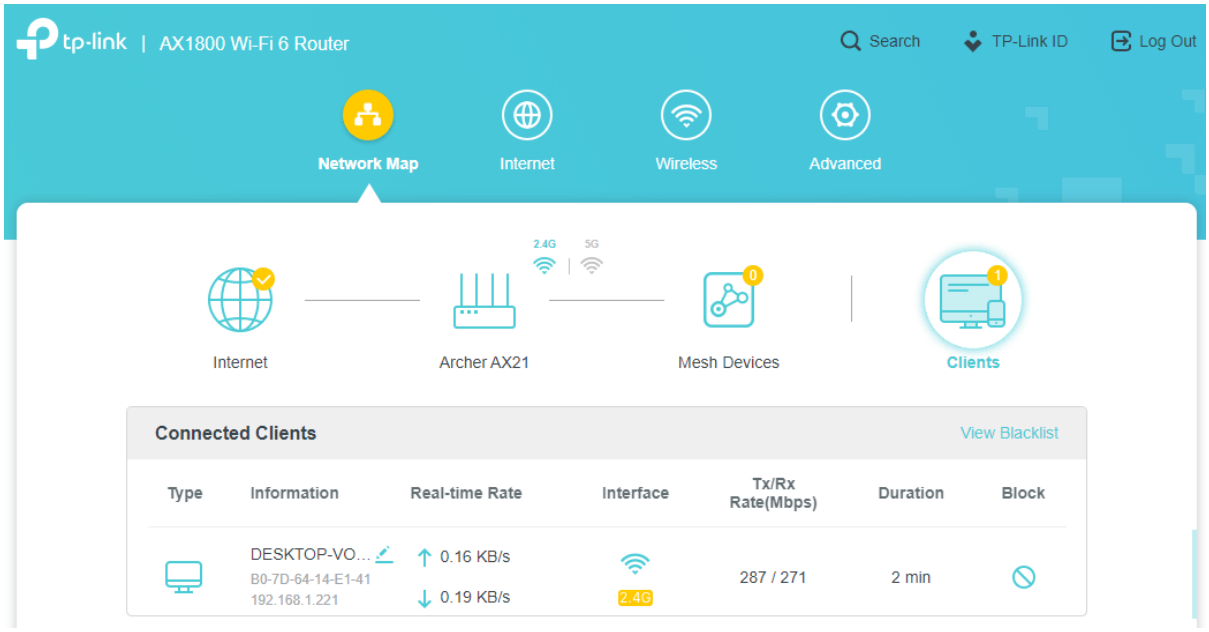

Figura 60. Redes 2.4GHz, computadora Wifi 6 conectada a red válida. Fuente: Elaboración propia.

Cuando se realiza el escaneo de las redes disponibles con el *Wifi Pineapple,* puede verse que no tiene problemas en encontrar e identificar nuestro equipo de prueba, como se muestra en la Figura 61.

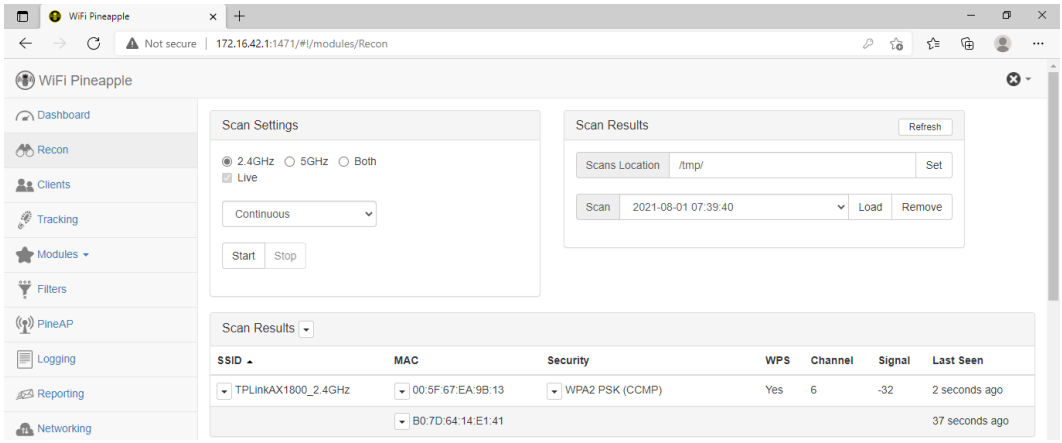

Figura 61. Redes 2.4GHz, computadora Wifi 6 escaneada. Fuente: Elaboración propia.

Para fines de documentar todos los detalles relevantes, se puede ver en la Figura 62 como una vez al lanzar el ataque de desautenticación, se está en la capacidad de evidenciar que el equipo efectivamente se conecta a la red falsa, dando por concluido este laboratorio.

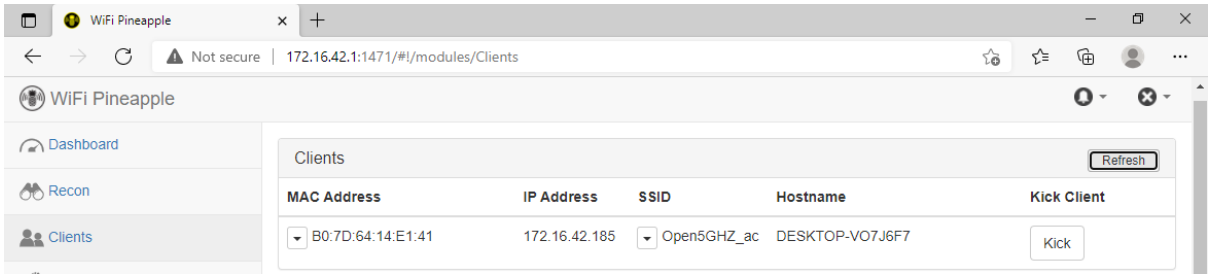

Figura 62. Redes 2.4GHz, computadora con Wifi 6 atacada exitosamente. Fuente: Elaboración propia.

4.3.3.3 Redes 5GHz 802.11 ac/ax

De vuelta a protocolos más recientes, en este laboratorio se analizará por última vez a la MacBook Air, pero esta vez contra una red de 5GHz en el enrutador TPLink AX1800 Dual Band y así registrar algún cambio en los resultados, para lo cual se conecta el equipo a la red Open5GHz_ac/ax para que la guarde en sus

redes conocidas y nuevamente se conecta a la red válida TPLinkAX1800_5GHz_ax a la espera del ataque como se muestra en la Figura 63.

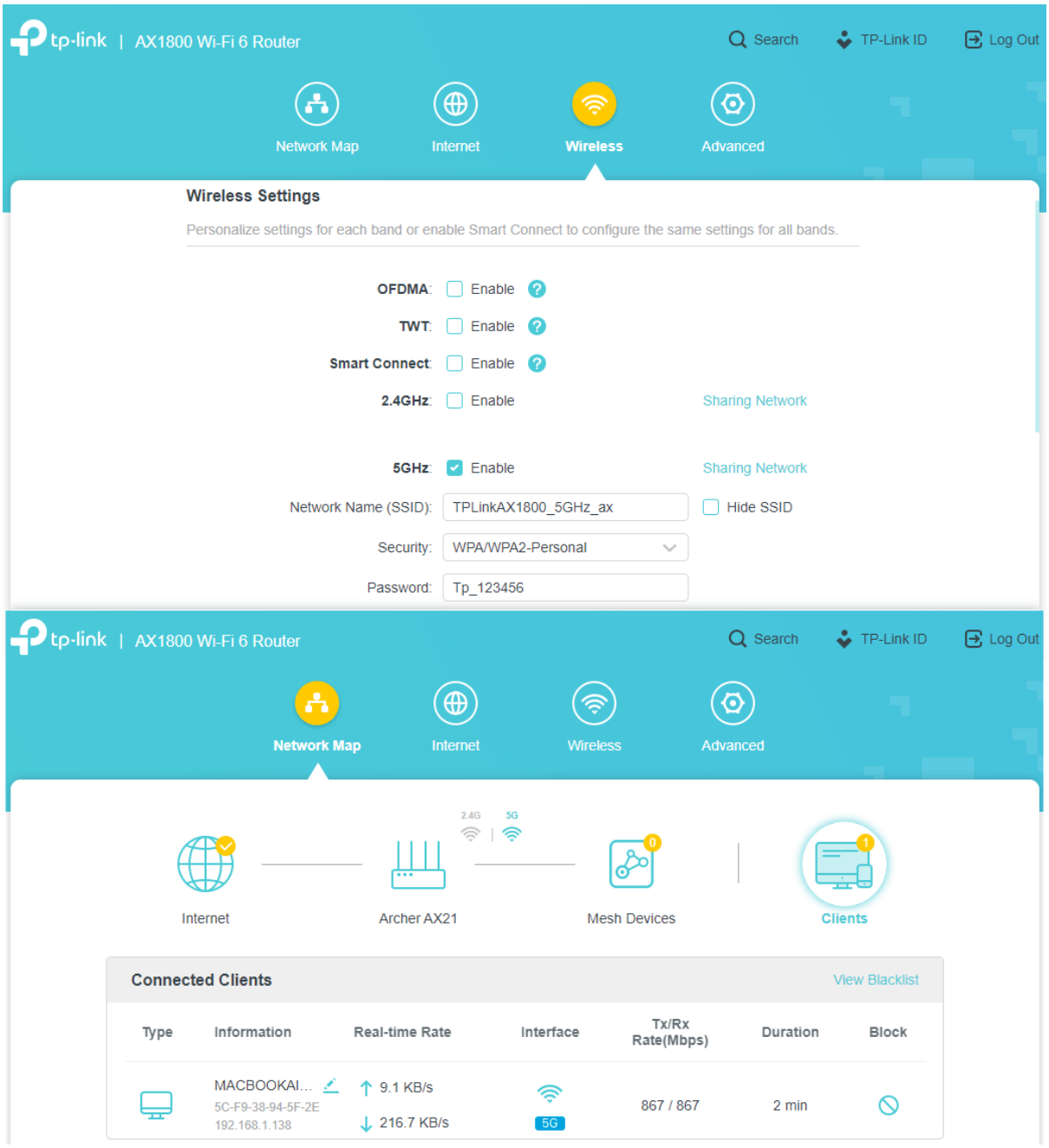

Figura 63. Redes 5GHz, en enrutador de Wifi 6 con cliente MacBook Air. Fuente: Elaboración propia.

Ya con el escenario listo, se procede a realizar el escaneo de las redes inalámbricas y como se evidencia en la Figura 64, fue identificada sin problema alguno.

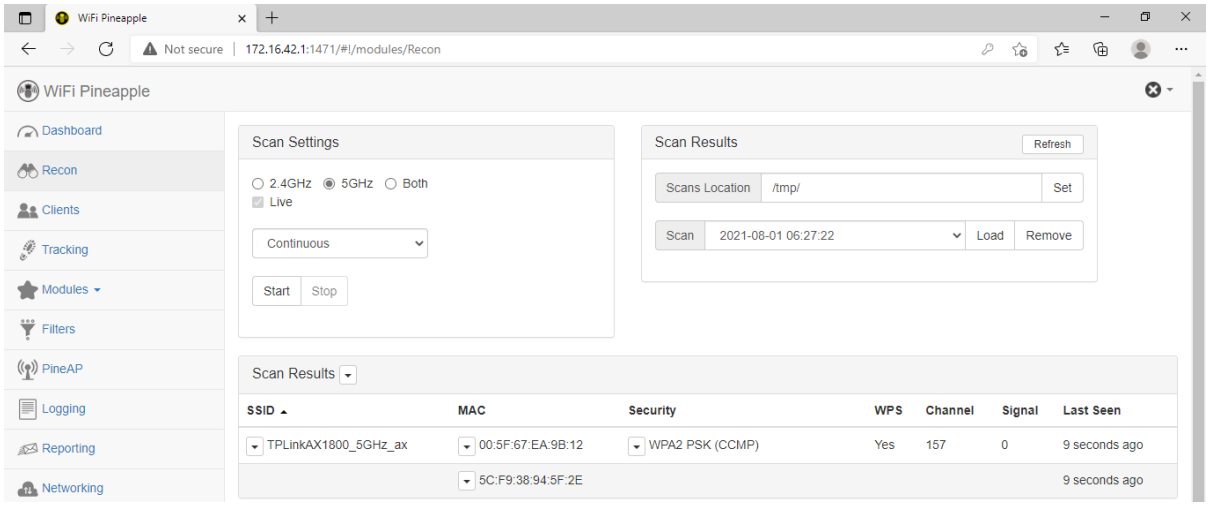

Figura 64. Redes 5GHz, en enrutador de Wifi 6, escaneo de cliente MacBook Air. Fuente: Elaboración propia.

De la misma manera, una vez iniciado el ataque de desautenticación por medio de DoS para aislar al equipo, como se muestra en la Figura 65, aún somos capaces de capturar los *Probe Request* como en otros escenarios.

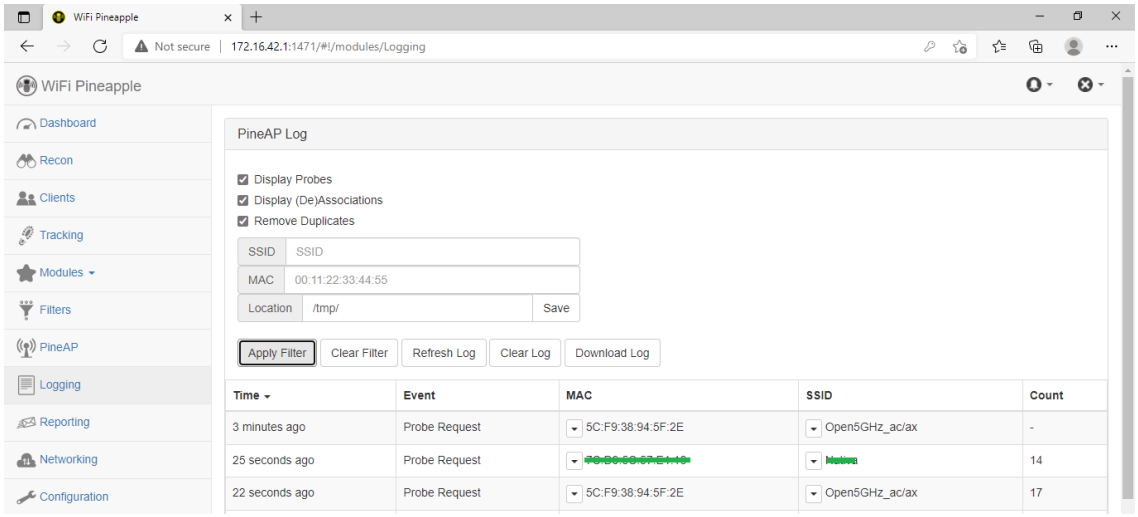

Figura 65. Redes 5GHz, en enrutador de Wifi 6, captura de *Probe Request* de MacBook Air. Fuente: Elaboración propia.

Con lo que, por último al desplegar la red falsa y continuar con el ataque de DoS y aislar al equipo de la red válida, se puede evidenciar en la Figura 66 que nuevamente el equipo se conecta sin problema aparente a la red falsa.

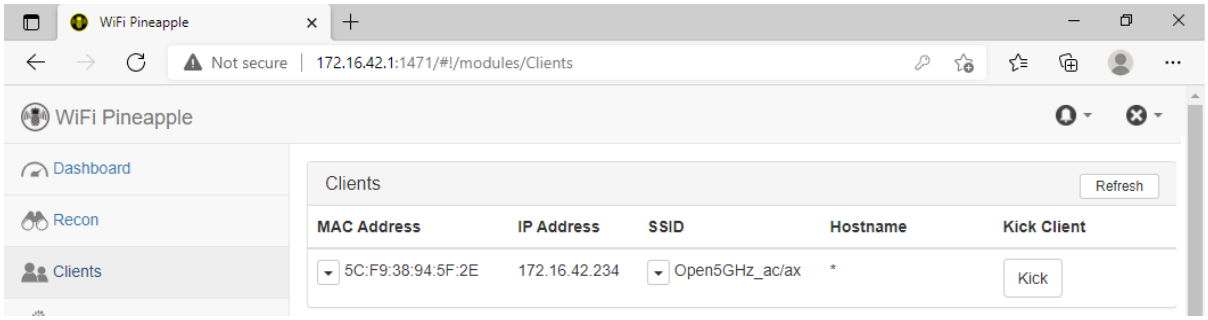

Figura 66. Redes 5GHz, en enrutador de Wifi 6, con MacBook Air atacado exitosamente. Fuente: Elaboración propia.

4.3.3.4 Redes 5GHz 802.11ax

En esta última prueba se tiene el escenario final en el que se aprovecha las capacidades del enrutador TPLink AX1800 Dual Band para habilitar de manera única el funcionamiento del protocolo 802.11ax de Wifi 6 para ser comparado contra la única computadora y dispositivo que cuenta con compatibilidad nativa para este protocolo.

Para iniciar la configuración del laboratorio, nuevamente la red abierta Open5GHz_ax, a la que se conecta el equipo, para luego conectarlo a la red válida TPLinkAX1800_5GHz_ax, como se muestra en la Figura 67, esperando ser atacado como parte de las pruebas de este último laboratorio.

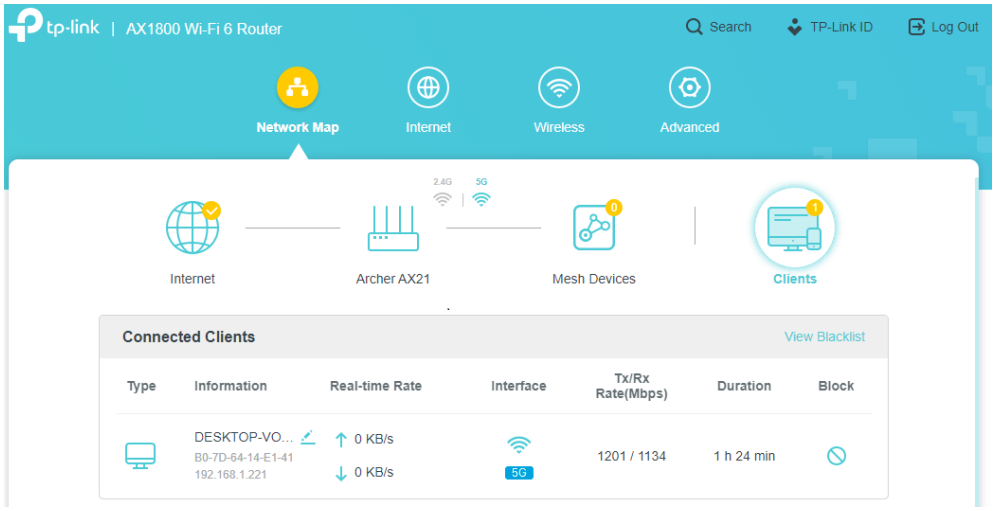

Figura 67. Redes 5GHz, Wifi 6 nativo en cliente y enrutador. Fuente: Elaboración propia.

En primer lugar, se corrobora, como se aprecia en la Figura 68, que la máquina cuenta con la capacidad y compatibilidad del protocolo 802.11ax y que, además, está conectada a la red válida bajo el mismo protocolo.

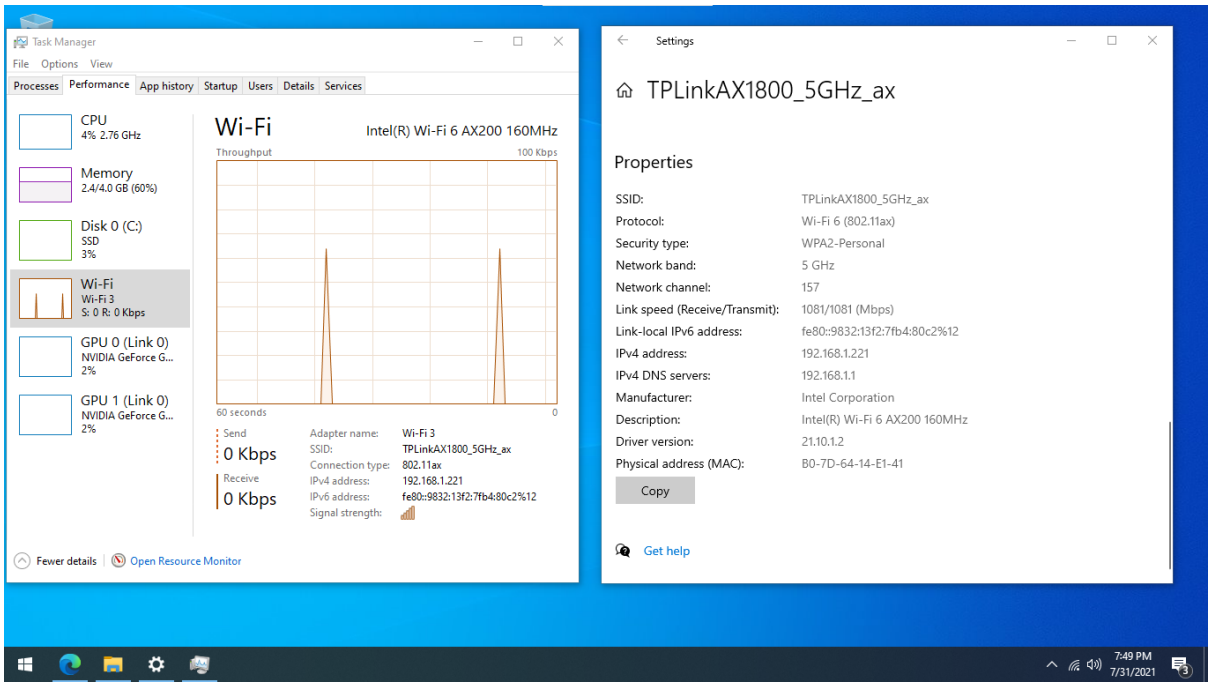

Figura 68: Redes 5GHz, Wifi 6 nativo, configuración de maquina cliente. Fuente: Elaboración propia.

Una vez iniciado el escaneo, e incluso luego de varios intentos, de realizar el escaneo de la red e inclusive de enviar un ataque de desautenticación al enrutador, para utilizar ese segundo vector de ataque, no se ha podido capturar el estado real con el *Wifi Pineapple,* como se muestra en la Figura 69, en cambio se ve que describe la máquina como un cliente no asociado o no conectado a ninguna red, lo que no es correcto.

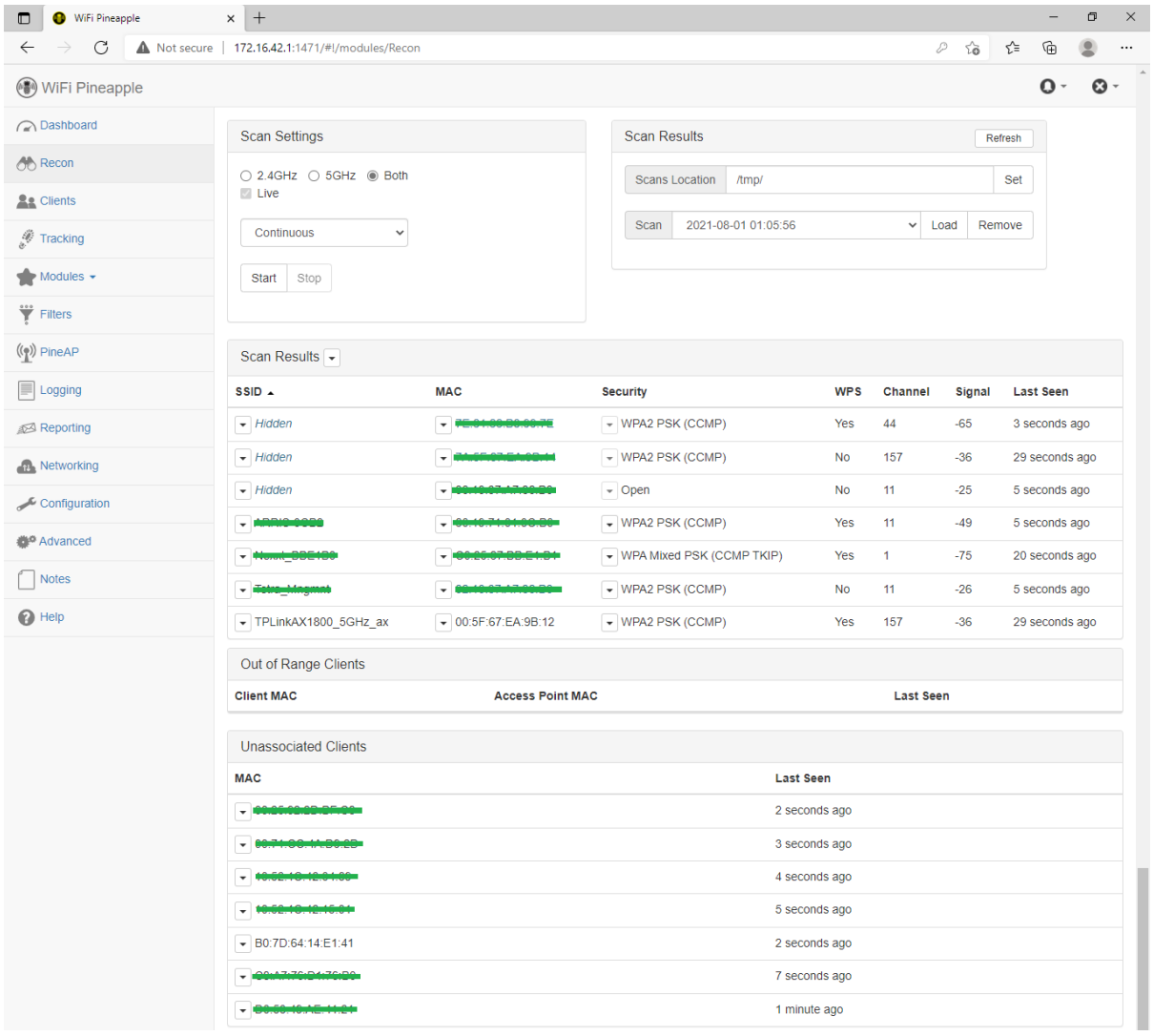

Figura 69. Redes 5GHz, Wifi 6 nativo, problema de captura de red de cliente. Fuente: Elaboración propia.

Debido a que no se tiene respuesta en el escenario usual, se presenta la necesidad de realizar el análisis de manera manual, para eso se utilizará la

herramienta Airgeddon y el adaptador USB AWUS1900 de alto alcance para monitorear la red, lo cual requirió la espera de una gran cantidad de tiempo, como se observa en la Figura 70.

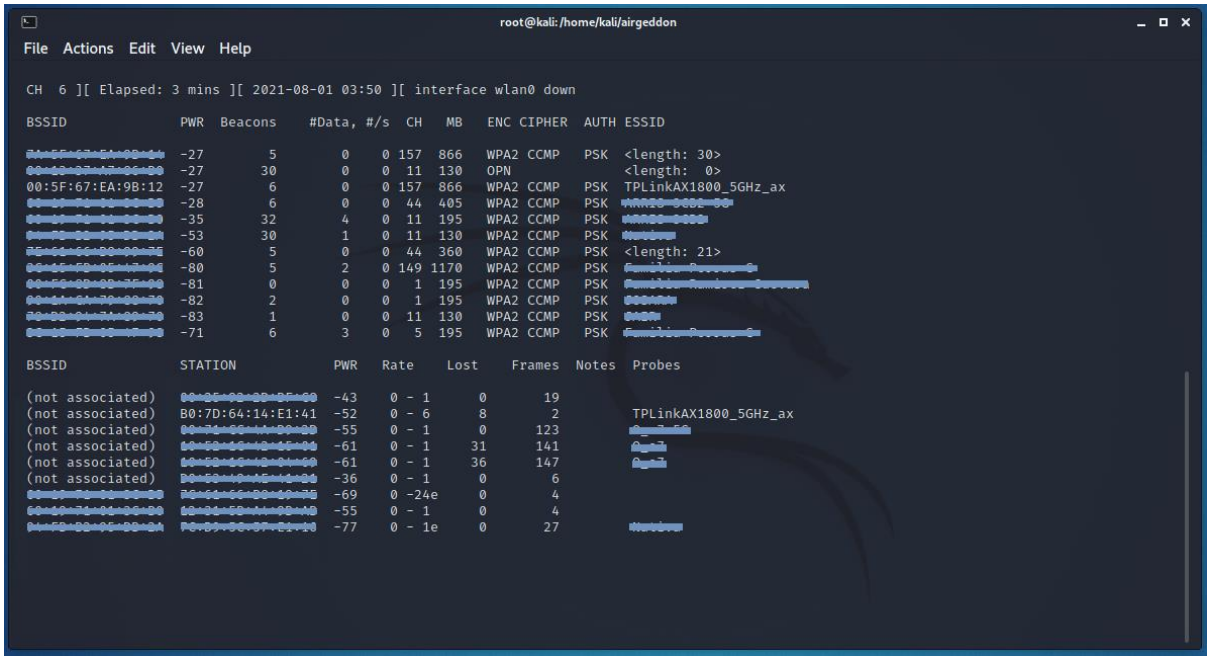

Figura 70. Redes 5GHz, Wifi 6 nativo, análisis con Airgeddon. Fuente: Elaboración propia.

Aunque se ha podido capturar un trazo de un *Probe Request*, se ve que una vez que se monitorea solo el canal de la red válida no se logra capturar nuevamente, por lo cual a la hora de proceder a enviar un ataque de desautenticación no se obtiene respuesta de que se haya podido realizar, como se muestra en la Figura 71, a pesar de los innumerables intentos.

De este último resultado se puede deducir que, efectivamente, al tener tanto el enrutador como el cliente en un protocolo más moderno, quedan aislados de las herramientas de ataque y análisis, las cuales son solo compatibles hasta el protocolo 802.11ac de Wifi 5, por consiguiente, no son capaces de alcanzar la comunicación efectuada en el espectro de 802.11ax.

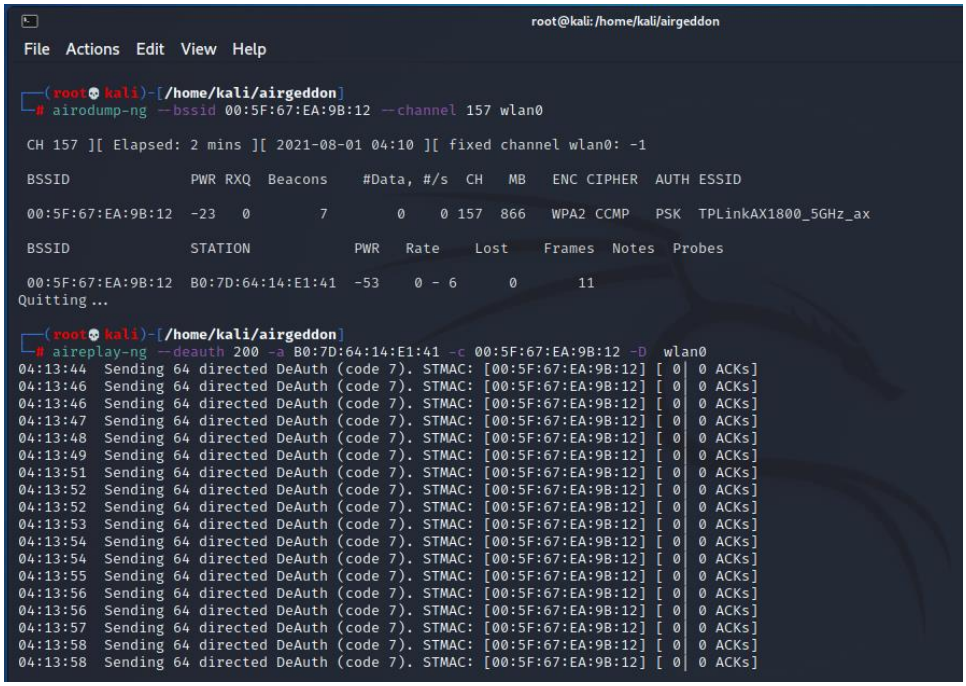

Figura 71. Redes 5GHz, Wifi 6 nativo, análisis Airgeddon e intento de desautenticación. Fuente: Elaboración propia.

4.4 Mecanismos de mitigación

Para poder determinar el alcance de la propuesta de solución es necesario poder establecer si se existen los medios o sistemas que provean una capa de protección para el ataque de *Wifi Spoofing*, por lo cual es ideal evaluar los mecanismos de mitigación existentes y de acceso a cualquier usuario, para determinar si existe o no la necesidad de desarrollar la propuesta de solución que puede cubrir los diferentes sistemas o productos en el mercado.

Como resultado se evalúan tres áreas donde se ha buscado tener un mecanismo de protección, la primera es a nivel de protocolos integrados en los estándares de comunicación de los protocolos de redes inalámbricos.

En el segundo nivel están los sistemas especializados de detección, conocido por sus siglas en inglés IDS, los sistemas de detección de intrusos, los cuales son capaces de monitorear la red en los alrededores y determinar si hay algún tipo de

acción o ataque siendo ejecutado, con el fin de alertar al o a los administradores de dicho sistema.

Como último nivel se evaluarán los mecanismos de encriptación, los cuales proveen protección a los medios de comunicación en el medio inalámbrico entre el cliente y el punto de acceso o enrutador.

Para esto a continuación se evalúa cada uno de los niveles de mitigación mencionados y se pondrá a prueba su efectividad utilizando las diferentes herramientas de *pentesting* ante los mecanismos más utilizados o más conocidos en cada nivel.

4.4.1 Diagnóstico de OpenWRT y 802.11w

En el primer caso se evaluará la efectividad para mitigar el ataque en estudio a nivel de los protocolos existentes, para esto se realiza el estudio del protocolo 802.11w (IEEE, 2021), el cual fue ratificado en 2009 por IEEE con el fin de introducir una manera de proteger contra los ataques de desautenticación y desasociación.

A pesar de ser un protocolo creado desde el 2009, no se encuentra disponible en los enrutadores o puntos de acceso comercial, pero sí de uso empresarial, por lo cual para poder investigar sus propiedades se utiliza el sistema de OpenWRT, este es un

> … sistema operativo Linux destinado a dispositivos integrados. En lugar de intentar crear un único firmware estático, OpenWrt proporciona un sistema de archivos totalmente escribible con administración de paquetes. Esto lo libera de la selección y configuración de aplicaciones proporcionadas por el proveedor y le permite personalizar el dispositivo mediante el uso de paquetes para adaptarse a cualquier aplicación. Para los desarrolladores, OpenWrt es el marco para construir una aplicación sin tener que construir un

> firmware completo a su alrededor; para los usuarios, esto significa la capacidad de personalización completa, para usar el dispositivo de formas nunca imaginadas. (OpenWrt Project, 2005)

Gracias a este sistema es posible configurar este protocolo para su uso, el cual es compatible para ser instalado en diferentes dispositivos, para ello se ha utilizado un Raspberry Pi 3 B+ (Figura 73), al cual se le instalará y configurará este sistema para las pruebas con 802.11w.

Figura 72. Mitigación 802.11w, Raspberry Pi 3 B+. Fuente: Elaboración propia.

Con el Raspberry Pi con OpenWRT instalado, se procede a realizar la configuración básica del dispositivo, el acceso a la red, la puerta de enlace y la actualización de las librerías y paquetes para las pruebas.

Una vez que estas tareas son completadas es necesario habilitar la configuración o propiedades de red inalámbricas para que puedan ser utilizadas.

En el sistema en el Raspberry Pi solo se puede habilitar redes de Wifi 4 o de Wifi 5, dadas las capacidades del dispositivo, así que para las pruebas se utilizará la

red inalámbrica OpenWRT bajo el protocolo de Wifi 5 802.11ac, como se muestra en la Figura 73.

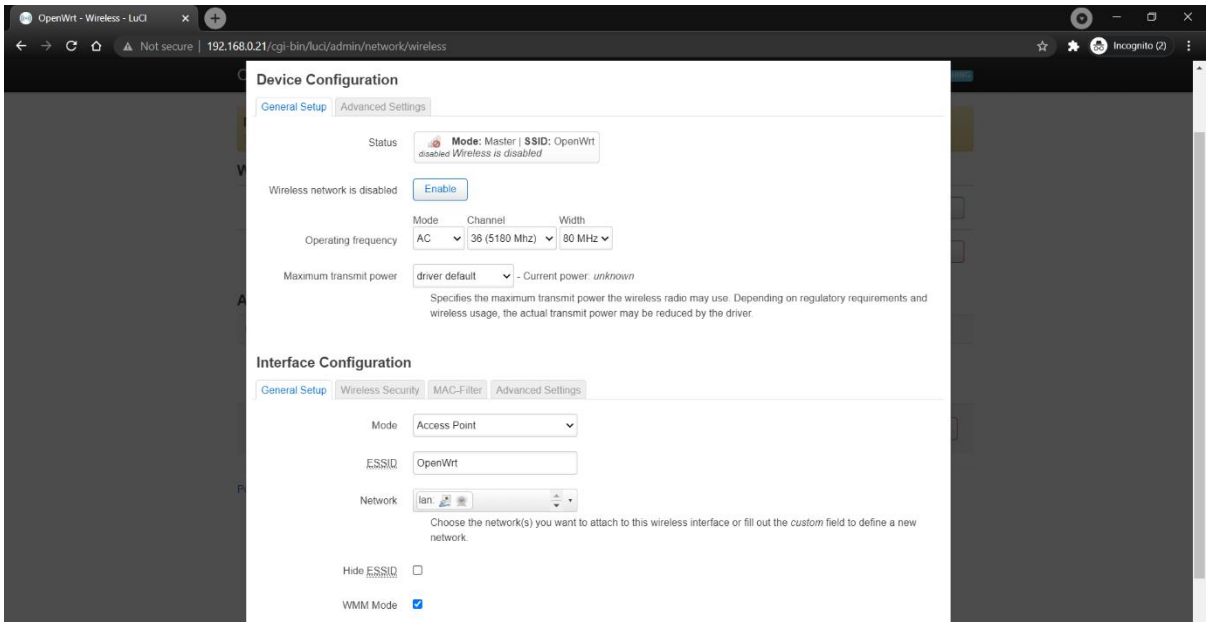

Figura 73. Mitigación 802.11w, configuración Wifi OpenWRT. Fuente: Elaboración propia.

Con estos detalles listos, el siguiente paso es habilitar el protocolo 802.11w en la nueva red inalámbrica, para eso se establece la opción como requerida para la configuración de 802.11w *Management Frame Protection* como se muestra en la Figura 74, dejando la red lista para las pruebas.

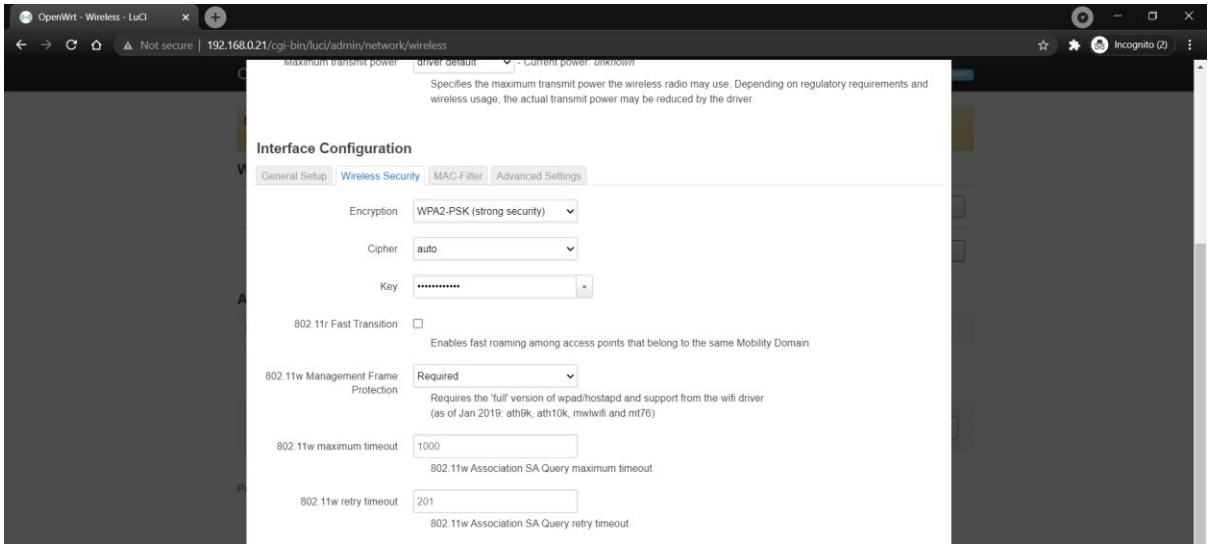

Figura 74. Mitigación 802.11w, protocolo habilitado. Fuente: Elaboración propia.

En cuanto se habilita este protocolo, se presenta cierto inconveniente, en solo uno nuestros dispositivos, la computadora MSI Leopard 8RF, ya que el resto del equipo a disposición no es compatible con este protocolo, lo cual se comprobaba desde el hecho de desplegar mensajes hasta simplemente pedir nuevamente la contraseña sin ser capaz de conectarse exitosamente a la red, así como se muestra en la Figura 75.

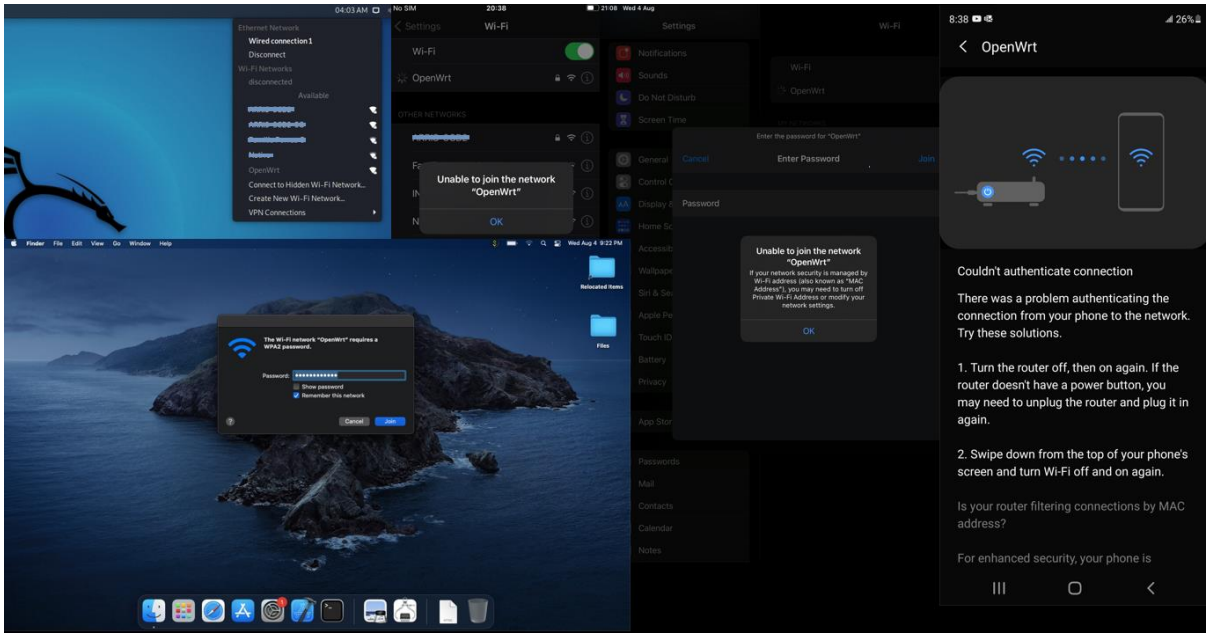

Figura 75. Mitigación 802.11w, problema de compatibilidad. Fuente: Elaboración propia.

Al contar con solo la computadora MSI Leopard 8RF con compatibilidad a este protocolo, se procede a iniciar las pruebas. Una vez conectado a esta red, se evidencia que funciona sin problema como cualquier otro tipo de red inalámbrica, por lo cual se inicia el ataque para evaluar la efectividad de este sistema de protección. Como se puede evidenciar en la Figura 76, se puede identificar sin problema que el computador está conectado a esta red por medio del escaneo del *Wifi Pineapple*.

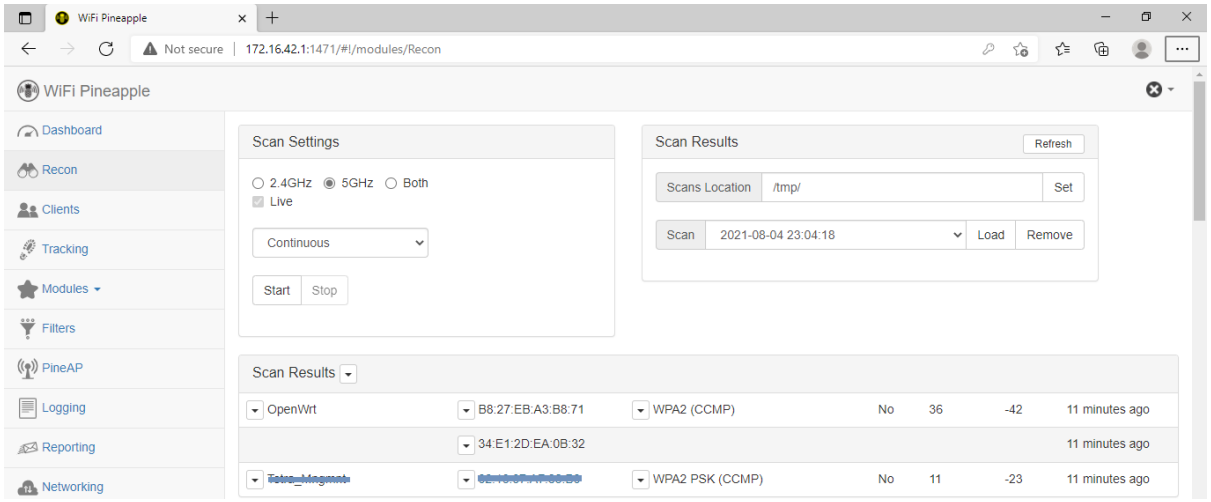

Figura 76. Mitigación 802.11w, escaneo *Wifi Pineapple*. Fuente: Elaboración propia.

Evidenciado que está al alcance para ser atacado, una vez iniciado el DoS y DDoS para identificar si este protocolo efectivamente cuenta con protección, como resultado se tiene que sí es posible desautenticarlo, y como se ve en la Figura 77, se pudo incluso capturar el *Probe Request* del equipo sin problema alguno.

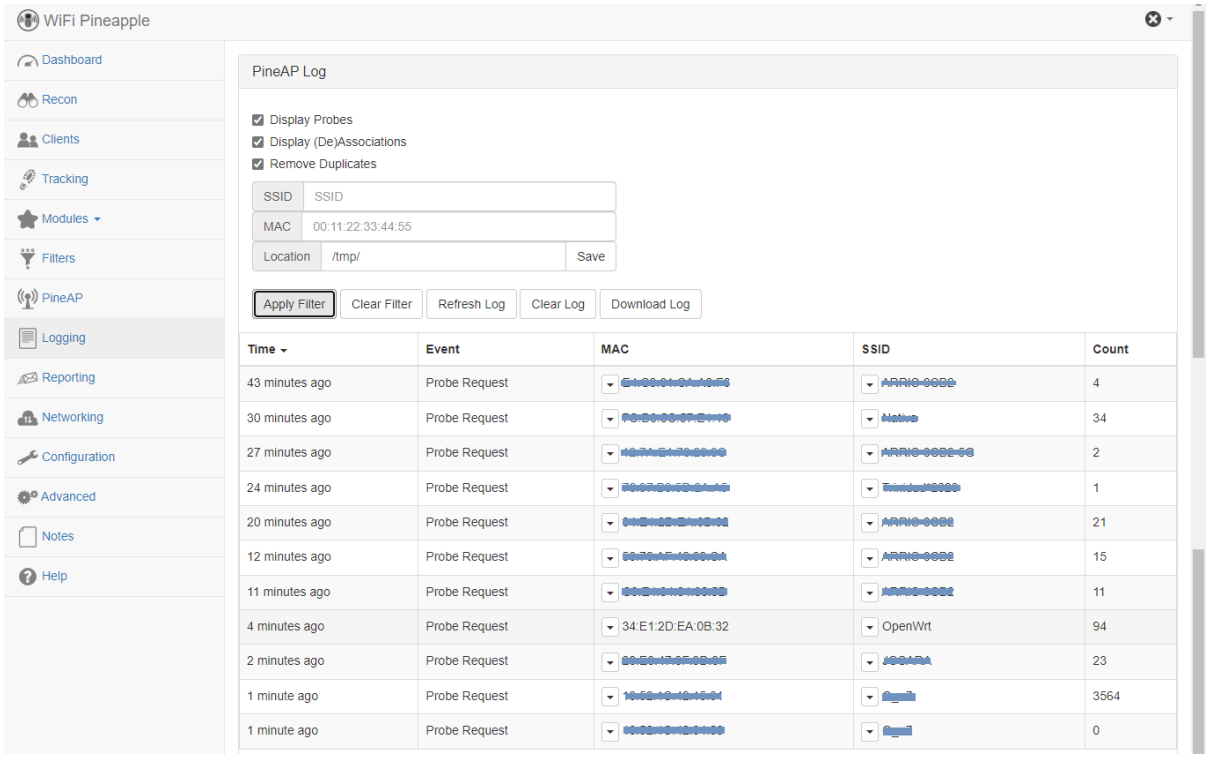

Figura 77. Mitigación 802.11w, Probe *Wifi Pineapple*. Fuente: Elaboración propia.

Al encontrar que el ataque sí funciona, en todas las ocasiones, incluso para reproducir el escenario completo y hacer que la computadora se conecte a una de las redes falsas, se da la necesidad de analizar el tráfico que existe entre el enrutador y la computadora para estudiar si todas las condiciones, tanto del protocolo como del ataque, son reales.

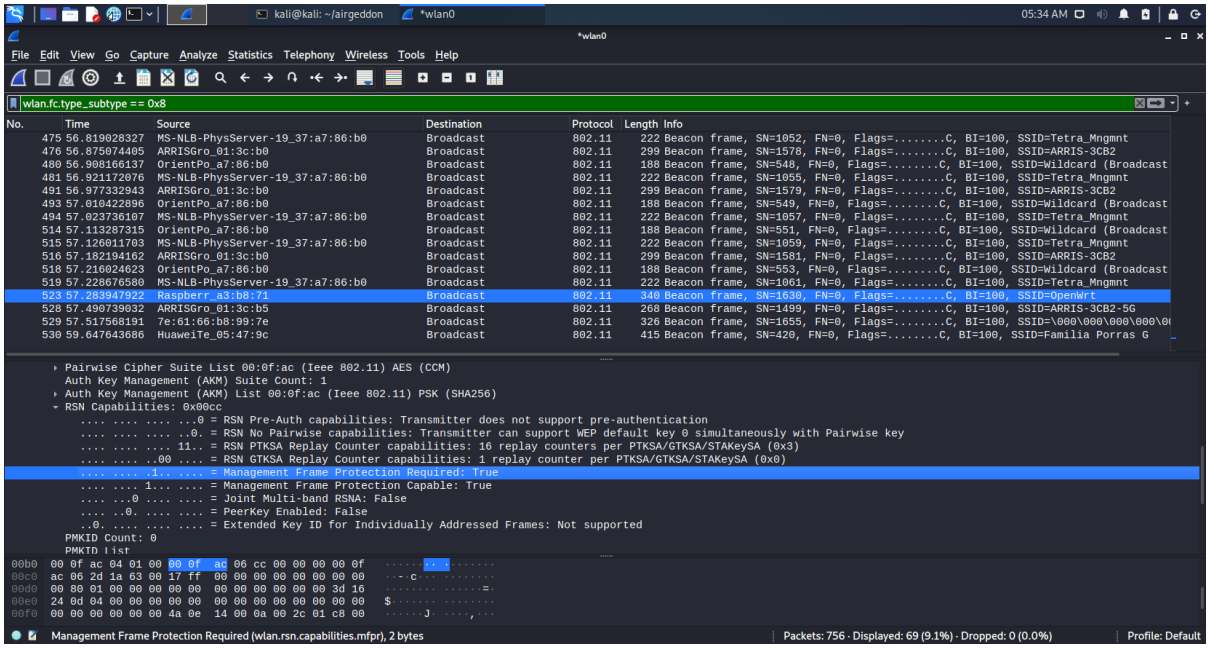

Figura 78. Mitigación 802.11w, análisis de red. Fuente: Elaboración propia.

Par esto, se realiza un análisis profundo de la comunicación, por lo que, así como se aprecia en la Figura 78, se inicia analizando la comunicación del enrutador Raspberry Pi con OpenWRT. Al revisar el encabezado de los paquetes de comunicación sí cuenta con protección de 802.11w habilitada, como se muestra en la propiedad *Management Frame Protection Required* y la *Management Frame Protection Capable*, ambas son verdaderas, lo cual confirma que el protocolo se encuentra activo y funcionando como es esperado, por lo cual se recurre a confirmar si los paquetes de comunicación al realizar el ataque evidencian la efectividad observada.

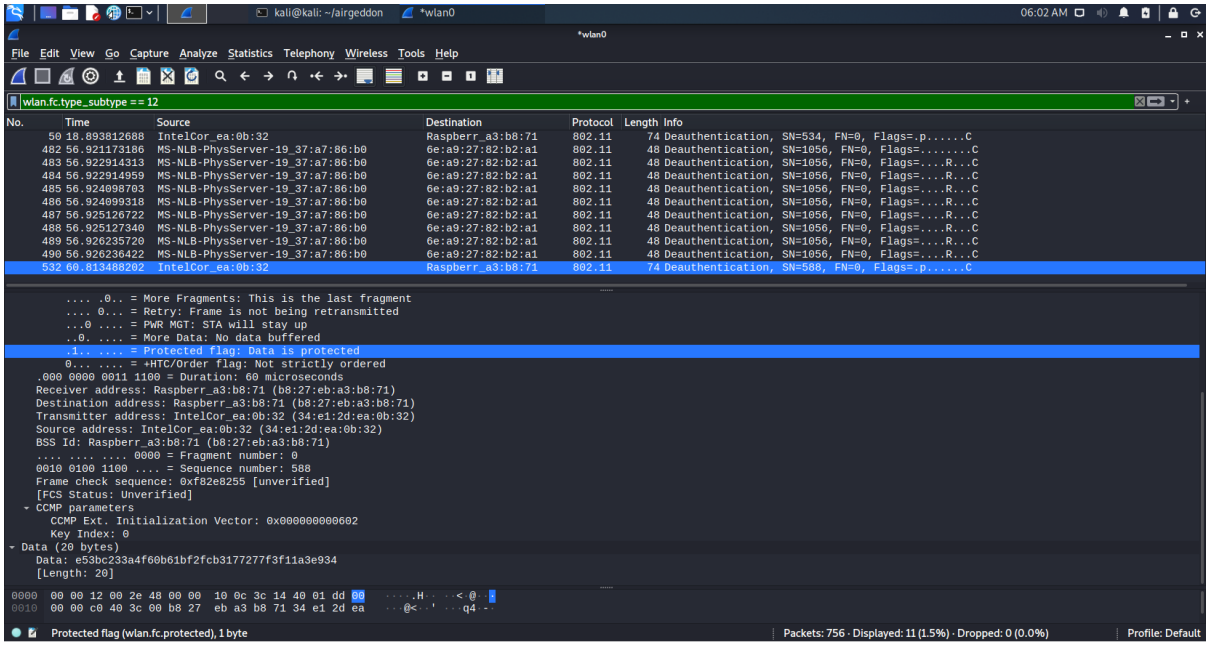

Figura 79. Mitigación 802.11w, análisis de ataque. Fuente: Elaboración propia.

Analizando los paquetes del ataque, como se observa en la Figura 79, se deja en evidencia que efectivamente el ataque está dirigido al Raspberry Pi con OpenWRT, y que corresponde a una desautenticación del equipo como resultado del ataque. Además de esto, al investigar las propiedades del paquete de comunicación, se ve que efectivamente este está protegido, visto en la propiedad *Protected flag*, como es de esperar como resultado de la comunicación.

Este resultado indica que no se cuenta con una total protección para los ataques de desautenticación que eventualmente serían usados para forzar al cliente a conectarse a la red falsa, pero este último análisis muestra que a pesar de que este protocolo no protege para el fin de esta investigación, sí protege el contenido de la información que viaja del cliente hacia el enrutador, lo cual añade una capa de protección, pero no para los fines de este trabajo o la propuesta de solución.

4.4.2 Diagnóstico de IDS

En este análisis, se tiene que existen varios sistemas de detección de intrusos de código abierto y sin costo alguno al alcance de cualquier usuario, aunque es necesario comentar que en su mayoría se requiere un conocimiento técnico para poder ser instalados y posteriormente configurados para su uso.

Para esto se selecciona el IDS llamado Kismet, el cual es “detector de dispositivos, rastreador, herramienta de control y plataforma WIDS (sistema de detección de intrusiones inalámbricas)” (Kismet, 2021, p. 1).

La ventaja de este sistema es que viene preinstalado y configurado en las versiones más recientes de Kali Linux, lo cual facilita su uso en general para el usuario final. Para esto solo es necesario abrir la herramienta, seleccionar la tarjeta de red inalámbrica que posea capacidades de monitoreo y con esto ya se tiene el IDS activo y funcionando, como se muestra en la Figura 80.

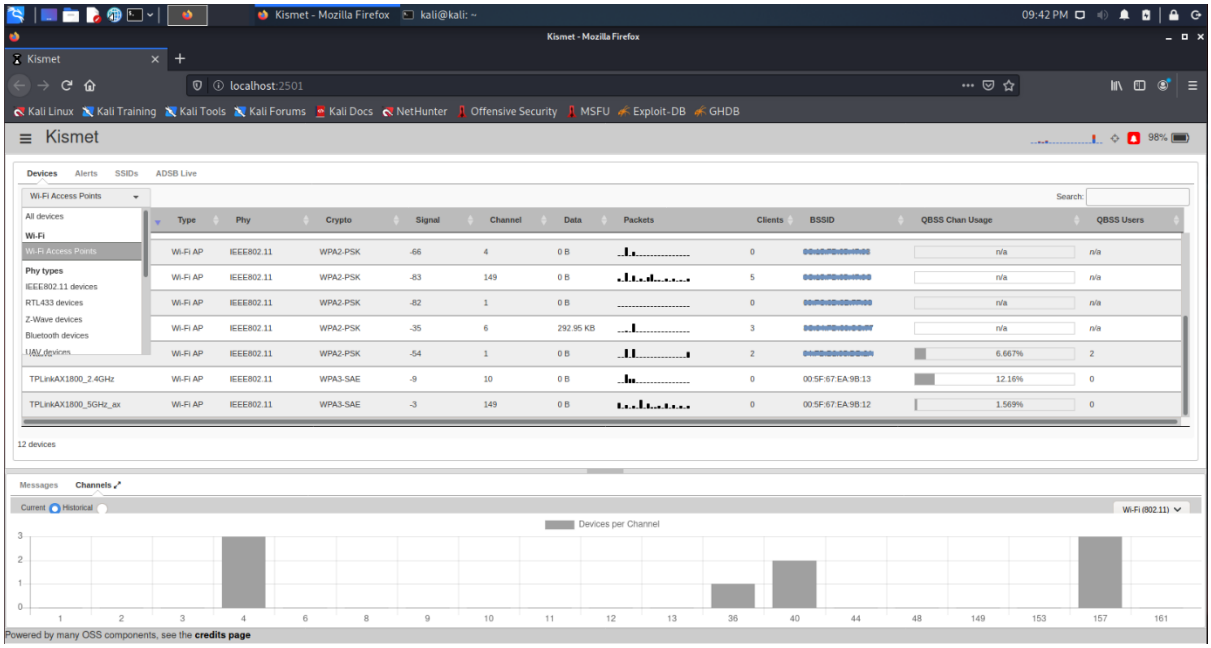

Figura 80. Diagnóstico IDS, Kismet. Fuente: Elaboración propia.

Con este sistema listo, únicamente habilitando las redes falsas utilizadas en los laboratorios, como se evidencia en la Figura 81, se tiene que el sistema ha

identificado dichas redes como un posible ataque de *Wifi Spoofing*, lo cual demuestra la efectividad de esta plataforma IDS, ya que esta detecta no solo que nuestras redes falsas provienen del mismo dispositivo con la misma MAC, sino que también detecta como parte del ataque del *Wifi Pineapple*, el cual cambia el canal en el cual transmite a las redes falsas para así poder captar a las posibles víctimas en caso de tener alguna restricción en los canales.

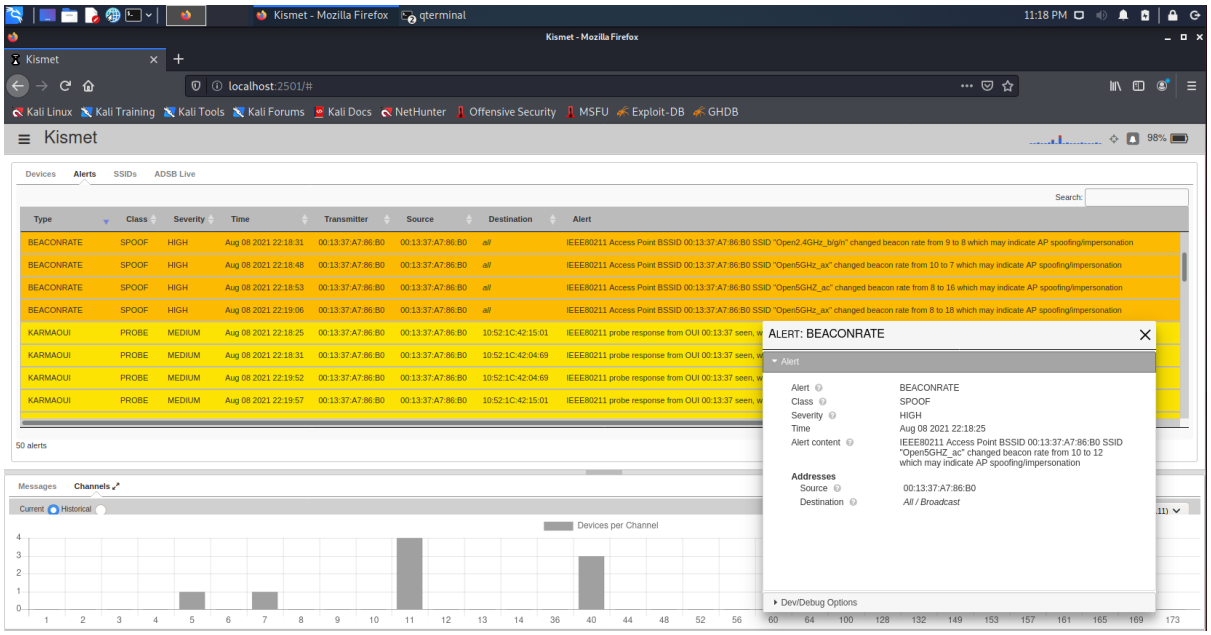

Figura 81. Diagnóstico IDS, primera captura de Kismet. Fuente: Elaboración propia.

Con el primer escenario exitoso, solo queda probar el ataque de desautenticación por medio de un DDoS. Como se aprecia en la Figura 82, Kismet exitosamente alerta que hay un ataque siendo ejecutado en ese momento, el tipo de ataque y su fuente.

Es más que claro que este sistema funciona perfectamente como se esperaría, lo cual se considera más adelante en esta investigación.

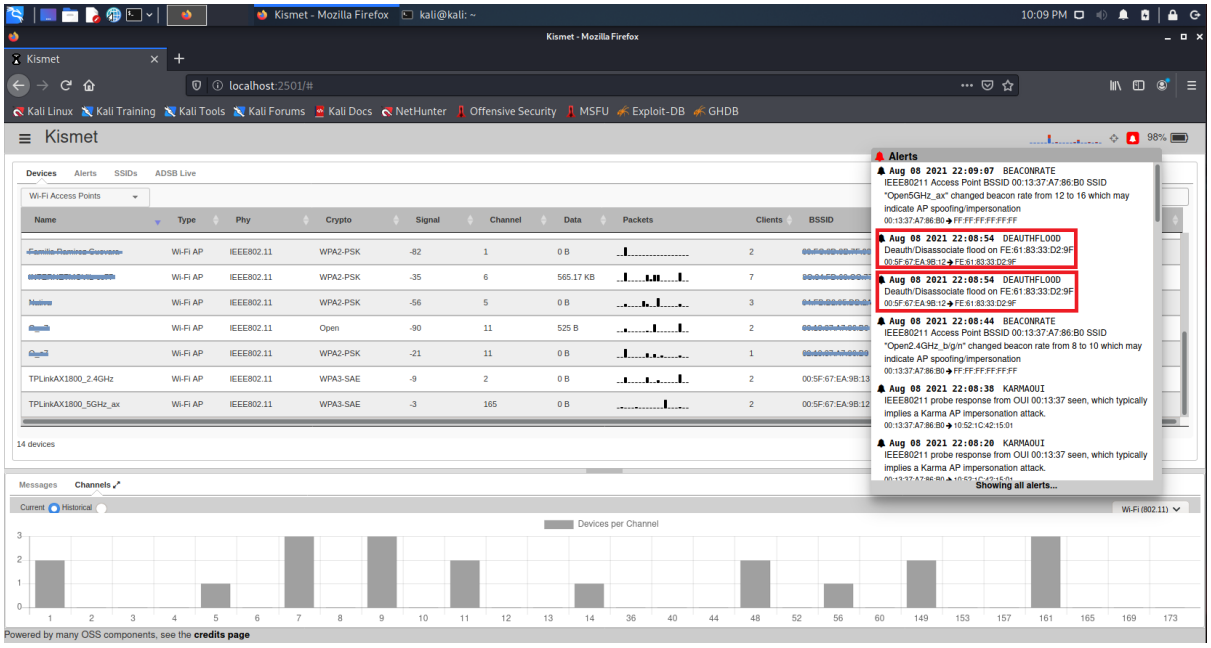

Figura 82. Diagnóstico IDS, Kismet alerta de ataque. Fuente: Elaboración propia.

4.4.3 Diagnóstico de encriptación WPA3

En el último nivel, lo que queda por evaluar es el nuevo modelo de encriptación, que es el WPA3, este provee a las personas y empresas

> …aumento en la protección de la información que se mueve a través de redes Wi-Fi por medio de la familia de tecnologías Wi-Fi Protected Access®. Las funciones de seguridad del acceso protegido Wi-Fi evolucionan constantemente para incluir protecciones más sólidas y nuevas prácticas de seguridad a medida que cambia el panorama de la seguridad. (Wi-Fi Alliance, 2021)

Además de ser el último modelo para la encriptación, en las mejoras de este nuevo sistema se cuenta con tres mejoras de interés para la investigación: “Utiliza los métodos de seguridad más recientes, rechace los protocolos heredados obsoletos, requiera el uso de marcos de administración protegidos (PMF)” (Wi-Fi Alliance, 2021, p. 1), lo cual protegería la comunicación de la red para evitar las

desconexiones al proteger los marcos de comunicación, y además provee protección a la contraseña del enrutador.

Para esta prueba se tiene que el enrutador TPLink AX1800 Dual Band, es el único al cual se le puede habilitar este nuevo modelo de encriptación, por lo cual se habilita WPA3 para las redes de 2.4GHz y 5GHz, como se muestra en la Figura 83.

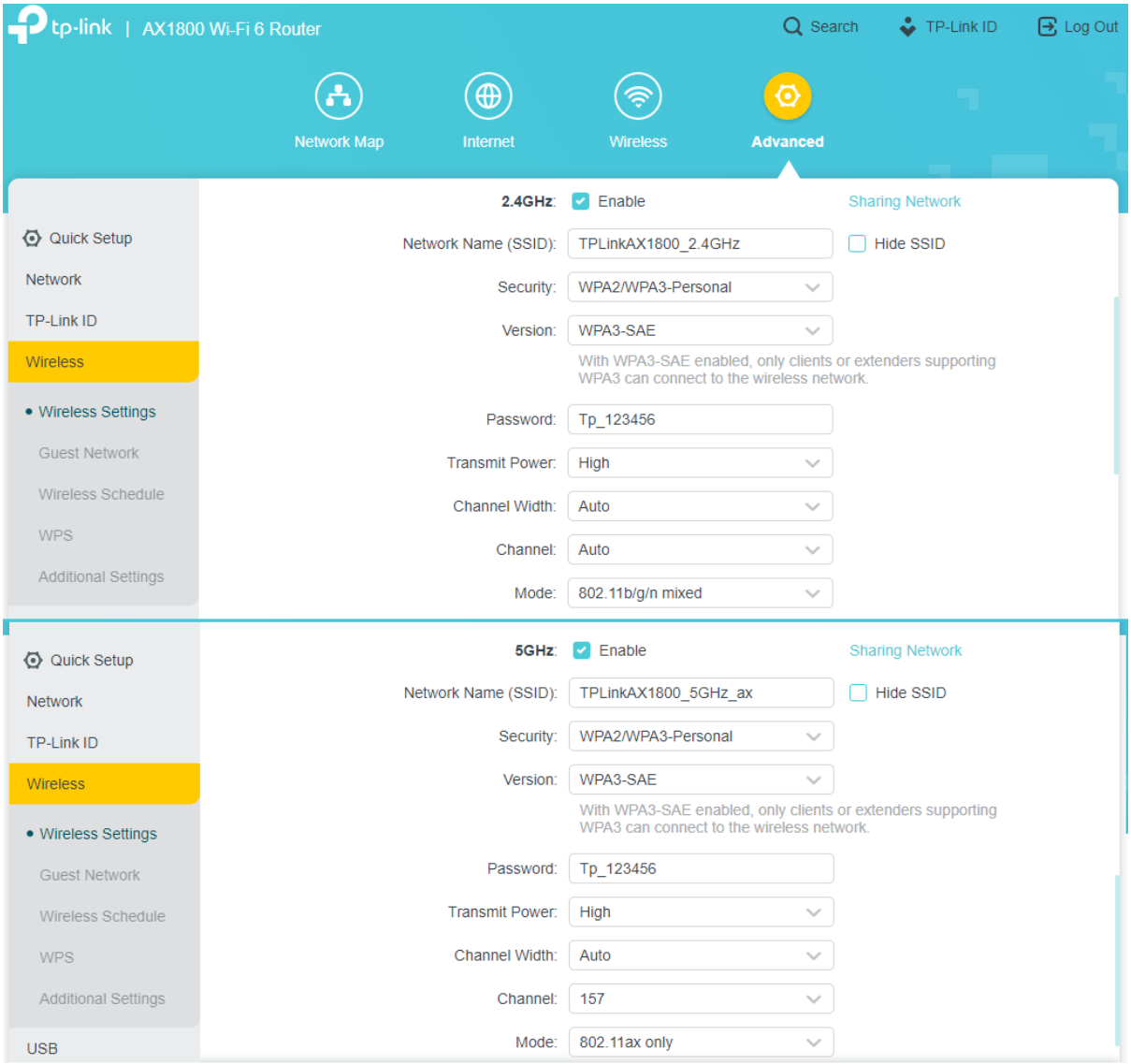

Figura 83. Diagnóstico WPA3, configuración enrutador. Fuente: Elaboración propia.

Como es de esperarse, no todos los dispositivos cuentan con la compatibilidad para este modelo de encriptación de redes inalámbricas, ya que muchos, aunque estuvieran conectados a estas redes previamente en otros

laboratorios, al habilitar el WPA3 muchas de estas botaban su conexión y por ende cualquier otro intento de volver a conectarse. Como se muestra en la Figura 84, los dispositivos iban desde mensajes de error al realizar el intento, hasta mostrar la red con problemas e incluso quedarse en un ciclo de intentos sin éxito alguno.

Figura 84. Diagnóstico WPA3, errores de intento de conexión. Fuente: Elaboración propia.

En este escenario aún se tiene los teléfonos iPhone SE y Galaxy S20 FE 5G, así como se evidencia en la Figura 84, ya que son de los pocos de última generación entre los dispositivos utilizados en este laboratorio, en los que además de ser de los pocos compatibles con Wifi 6 en el mercado, cuentan con la mayor compatibilidad a los protocolos de red más recientes en el mundo de la tecnología, por lo cual serán los únicos puntos de evaluación para esta última prueba.

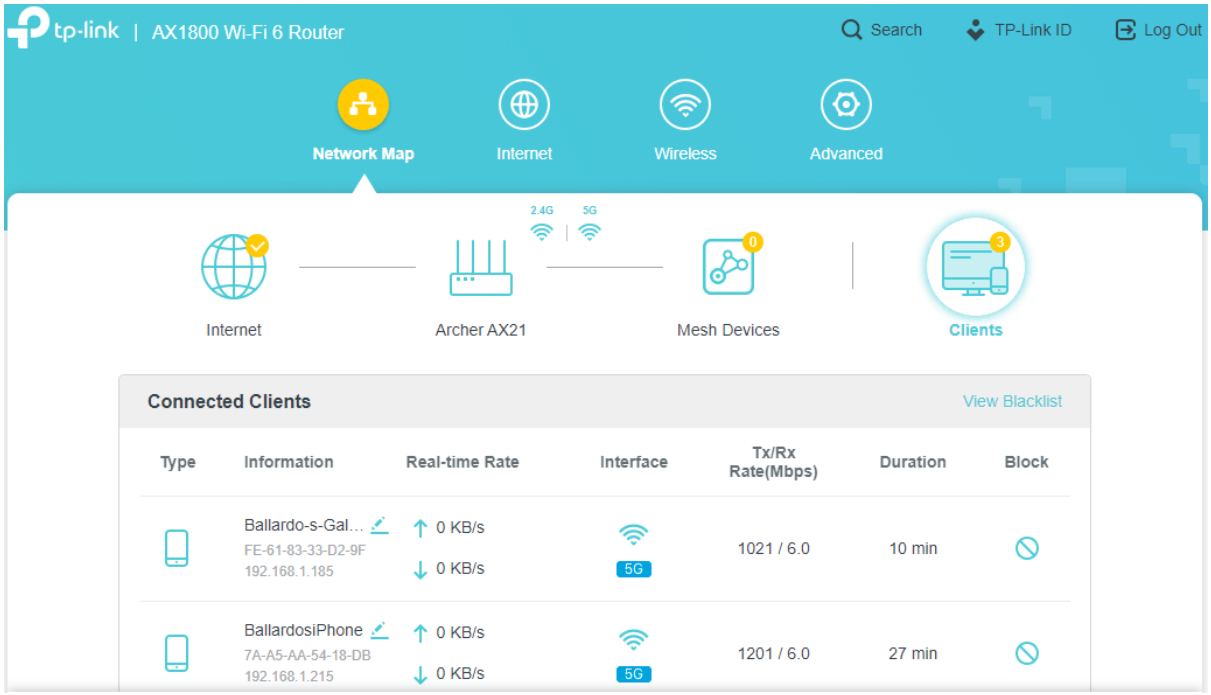

Figura 85. Diagnóstico WPA3, teléfonos compatibles. Fuente: Elaboración propia.

Con el escenario del laboratorio definido, se puede iniciar el ataque a los teléfonos conectados a la red con encriptación WPA3, por lo que se iniciamos el escaneo de la red, y como se muestra en la Figura 86, se puede identificar sin problema o inconveniente alguno, como sucedió en otros laboratorios, tanto el enrutador como los teléfonos son identificados en la red correcta.

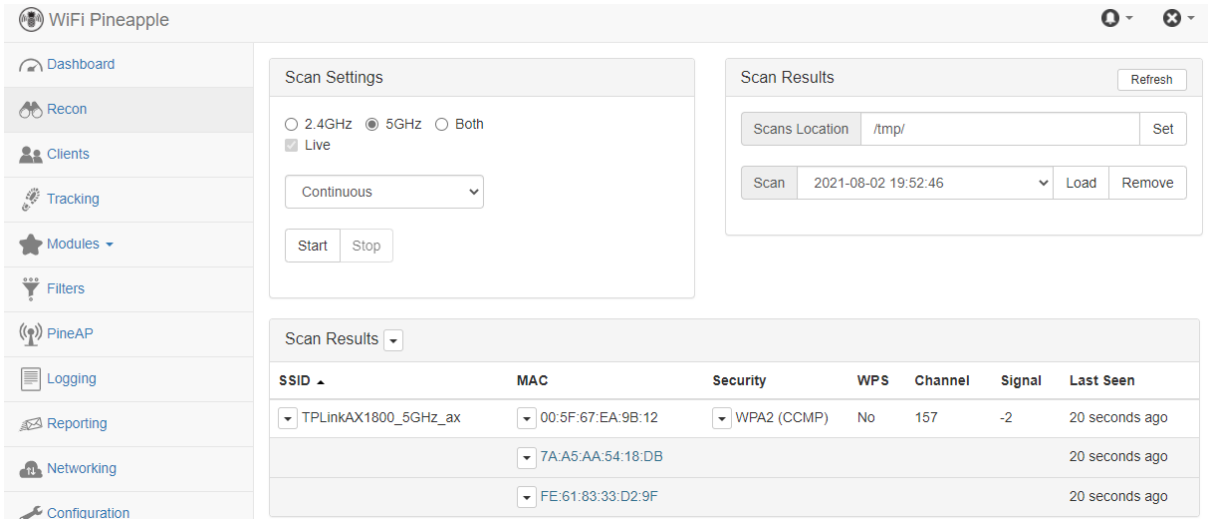

Figura 86: Diagnóstico WPA3, escaneo de red. Fuente: Elaboración propia.

Sin embargo, hay que resaltar el hecho de que según el *Wifi Pineapple*, la seguridad es WPA2, al intentar confirmar este detalle en los teléfonos (Figura 87), se tiene que al menos para el iPhone SE no se encuentra dentro de las opciones de las propiedades de la red inalámbrica el tipo de seguridad utilizada, en cambio en el Galaxy S20 FE 5G, sí se puede determinar que el teléfono identifica la red con seguridad de WPA3, lo cual puede ser un problema del *Wifi Pineapple* para identificar este nuevo modelo de encriptación.

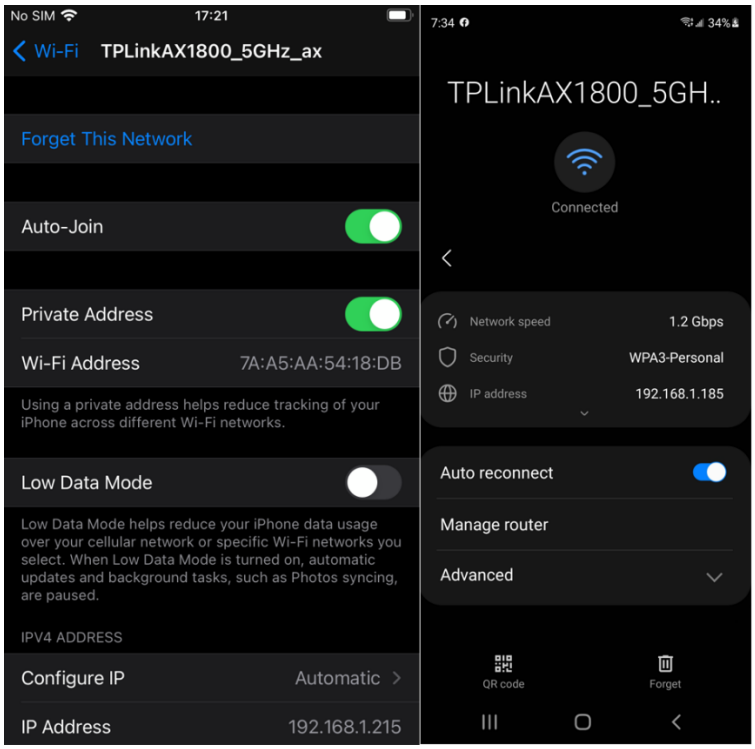

Figura 87. Diagnóstico WPA3, verificación de teléfonos conectados. Fuente: Elaboración propia.

Solo queda ejecutar el ataque, en comparación con el resto de laboratorios fue necesario establecer el mecanismo de emisión de la red falsa en el modo más agresivo, como se muestra en la Figura 88, al igual que utilizar el ataque de desautenticación en modo DDoS para forzar el aislamiento de los teléfonos de la red válida.

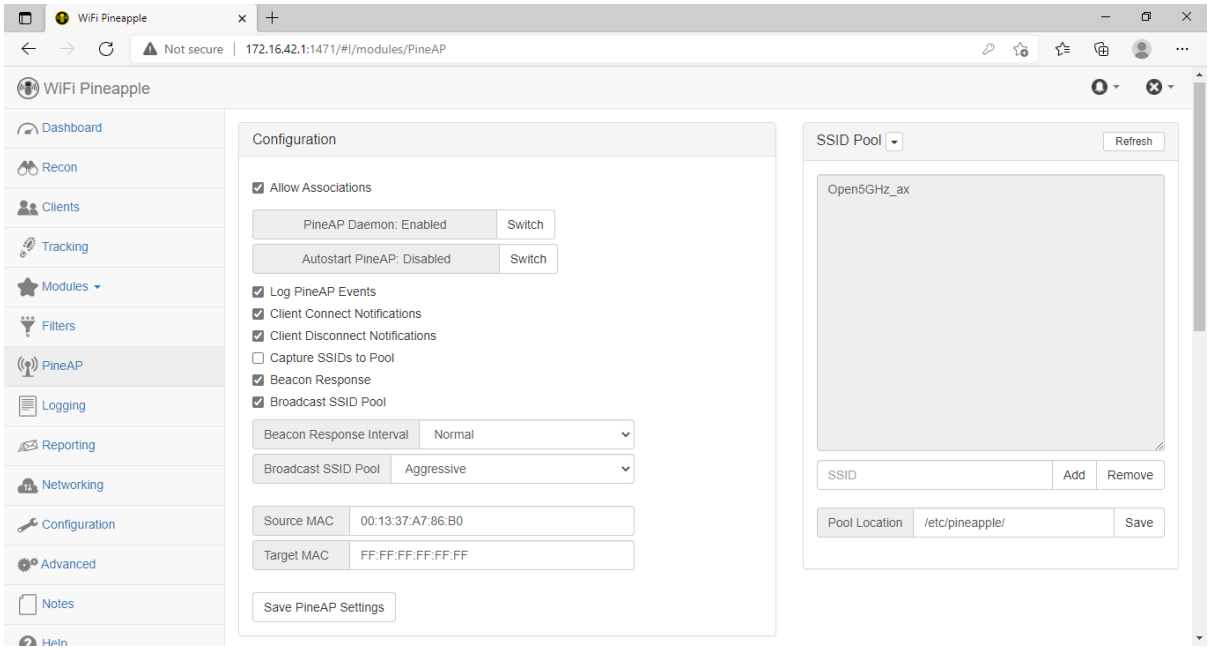

Figura 88. Diagnóstico WPA3, ataque agresivo a teléfonos. Fuente: Elaboración propia.

Al realizar este ataque por un periodo más prolongado que en otras ocasiones, se observa que efectivamente, como se detalla en la Figura 89, el ataque ha sido exitoso y los teléfonos se ven forzados a conectarse a la red falsa, dando por concluidas las pruebas de este último mecanismo de mitigación.

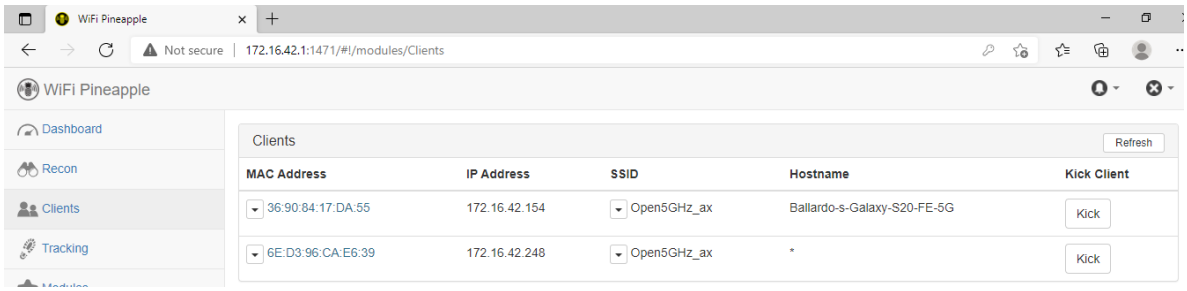

Figura 89. Diagnóstico WPA3, ataque exitoso a teléfonos. Fuente: Elaboración propia.

4.5 Análisis de herramientas de desarrollo

Ya que se cuenta con los escenarios evaluados, es necesario establecer si es posible desarrollar una propuesta de solución para mitigar el ataque en estudio,

por lo cual se analiza si cada uno de los ambientes o sistemas operativos que utilizan los dispositivos evaluados en los laboratorios, permiten o facilitan las herramientas para la construcción del nuevo sistema en cuestión.

4.5.1 Análisis de Android

Este sistema es de los más conocidos y utilizados por muchos de los teléfonos inteligentes hoy en día, por lo cual es necesario evaluar si es posible avanzar con una propuesta de solución, para lo cual se busca evaluar si se tiene acceso en modo de desarrollador a obtener información de la red inalámbrica a la cual se encuentra conectado el dispositivo, con todos los atributos posibles de la misma cuenta.

De igual forma es necesario tener acceso para poder obtener la información de las redes en los alrededores al alcance del dispositivo con todos los mismos atributos que estas tienen para poder analizarlo en la propuesta de solución.

Para esto se evalúa la documentación de desarrollo oficial para Android, el cual efectivamente tiene las capacidades necesarias para poder ser utilizadas en la propuesta de desarrollo, pero también detalla que desde versiones de Android 9, “Cada app en primer plano puede realizar cuatro búsquedas en un período de 2 minutos. Esto permite un pico de actividad de búsquedas en poco tiempo” (Android Developers, 2021, p. 1).

Con esto el tiempo de escaneo de redes es reducido en la cantidad por tiempo, y además de esto, para versiones de Android 11 en adelante es necesario que los usuarios otorguen permisos de localización a la aplicación para poder acceder a la información que se necesita, esto se debe a medidas de seguridad implementadas para que aplicaciones no deseadas no accedan a esta información sensible sin el consentimiento y sin el permiso del usuario.

4.5.2 Análisis de iOS y MacOS

En el siguiente análisis se evalúa el mismo escenario, en el cual se requiere determinar si las herramientas para desarrollo otorgan permisos en estos sistemas y así poder escanear las redes al alcance de estos dispositivos, al igual de las propiedades de la red inalámbrica en la que se encuentran conectados.

En este sistema, las librerías y el lenguaje y herramientas de desarrollo son los mismos para todos sus dispositivos (iPhone, MacBook, iPad, etc.), por lo cual, al evaluar las librerías y su capacidad, se encuentra que sí se tiene acceso a la información de la red inalámbrica a la cual el dispositivo se encuentra conectado, pero no para acceder a las redes de los alrededores al alcance del dispositivo.

Esto se debe a un cambio en la política de seguridad para poder restringir el acceso a las redes al alcance de los dispositivos, el cual fue introducido en iOS 8 (Apple Inc., 2017) sin embargo, proveen acceso a una librería especial que sí lo permite al inscribirse como desarrolladores oficiales, proceso que, además del llenado de un formulario, debe ser revisado y aprobado por la empresa.

Aun con el permiso para poder utilizar esta librería (Apple Inc., 2011) se cuenta con limitaciones así como se detalla al investigar las propiedades de cada una de sus funciones en las librerías de código, es posible de obtener la información de las redes al alcance del dispositivo, pero únicamente cuando el usuario se dirige y abre la configuración de red, ya que por código no se permite hacer escaneos de manera dinámica, limitando y asegurando que el usuario sea el único que inicie esta acción para ser capturada por el código.

4.5.3 Análisis de Windows

Con el análisis del sistema operativo de Windows, este posee una gran variedad de librería para el desarrollo de aplicaciones que provean acceso a la

información de red inalámbrica a la que se encuentra conectado el equipo, al igual que la posibilidad de poder acceder a la información de las redes inalámbricas en las cercanías, sin embargo, cuenta con varias reglas.

En primer lugar, una de sus librerías más documentadas y utilizadas para el escaneo de redes inalámbricas se encuentra en proceso de no ser soportada en futuras versiones de este sistema, podría ser reemplazada por una librería nueva, lo cual quedaría a elección de los desarrolladores de este sistema, debido al ciclo de vida y soporte de su API (Microsoft, 2021).

Aun con esta aclaración, y sin tomarlo en cuenta como una restricción de alto impacto para esta investigación, es bueno aclarar aún se cuenta con capacidad para poder acceder a la configuración de los diferentes adaptadores o dispositivos conectados al equipo, está la tarjeta de red inalámbrica, la cual también puede proporcionar acceso a esta información utilizando comandos de red especiales en el sistema.

Adicionalmente, debido al constante cambio y actualización de este sistema, es requisito tener el ambiente de desarrollo actualizado a la última versión disponible de este sistema ya que “aplicaciones de Windows solo pueden ejecutar la misma versión de destino mínima compilada del sistema operativo (SO) o superior” (Microsoft, 2021, p. 1), lo cual debe de ser tomado en cuenta por cualquier desarrollador para este sistema.

4.5.4 Análisis de Linux

En este último sistema, caracterizado por ser uno de los sistemas de código abierto y con una gran comunidad de desarrolladores que comparten información y librerías de código para poder ser utilizado, es un hecho que no se cuenta con un soporte total de todos los fabricantes. Esto se debe a que es un hecho comúnmente

conocido para cualquier usuario de Linux que la compatibilidad hacia dispositivos es compleja, ya que no todos los fabricantes liberan o permiten acceso a las librerías de código de sus dispositivos, lo cual para esta investigación corresponde a la compatibilidad con las tarjetas de red inalámbricas.

Es un tema por considerar cuidadosamente, ya que este rige las capacidades de desarrollo o monitoreo de cualquier sistema o aplicación que intente realizar esta operación en un equipo con este sistema, pero no restringe las capacidades en caso de requerir desarrollar una solución con esta necesidad.

Analizando las diversas comunidades de código abierto para identificar los mejores métodos para obtener información de la red inalámbrica a la cual se encuentra conectado el equipo, al igual que la información de las redes al alcance del dispositivo, muchos desarrolladores utilizan como base y recomiendan usar como producto final la aplicación llamada EvilAP_Defender (GitHub, 2016), la cual encapsula muchas librerías y la compatibilidad con muchas de las marcas y diferentes fabricantes de tarjetas de red inalámbricas, para poder realizar escaneos de red de una forma más rápida y eficiente, además de proveer acceso a otro tipo de llamados y acciones hacia los dispositivos de red.

Capítulo 5. Propuesta de Solución

Como resultado de toda la evaluación realizada en el capítulo anterior, es posible poder sentar las bases para el desarrollo de nuestra propuesta de solución, además de que, de la misma forma, se establecen límites en los diferentes dispositivos a los cuales se les realizo la evaluación.

Dados los resultados y las pruebas realizadas, es necesario establecer, en primer lugar, que no es posible desarrollar una solución para los dispositivos desarrollados por Apple Inc., implementada como medida de seguridad.

Como segundo resultado para la propuesta de solución, para los equipos que utilizan sistemas operativos Linux se cuenta con muchas opciones para la protección y mitigación del ataque de *Wifi Spoofing*, por lo cual no será incluido en propuesta de solución por desarrollar.

Una vez descartados los dispositivos en los sistemas o ambientes de desarrollo mencionados, queda como resultado elaborar una propuesta de solución para los dispositivos que cuentan con los sistemas Android y Windows.

Para esto es necesario establecer los requerimientos o hallazgos en las pruebas, por lo cual, iniciando con la topología del laboratorio, como se aprecia en la Figura 90, se pone en una posición compleja a propuestas como el Time Based TCP (Nakhila, Dondyk, Amjad y Zou, 2015), ya que los dispositivos de ataque se encuentran dentro de la misma red, escenario que no está muy lejos de la realidad dependiendo de dónde se pueda encontrar un atacante, lo que es similar para la propuesta de Agarwal, Biswas, & Nandi (2018), al utilizar equipo con capacidades de monitoreo de bajo nivel, ya que se debe implementar la solución con las capacidades y limitantes técnicas de los dispositivos en estos sistemas Android y Windows.

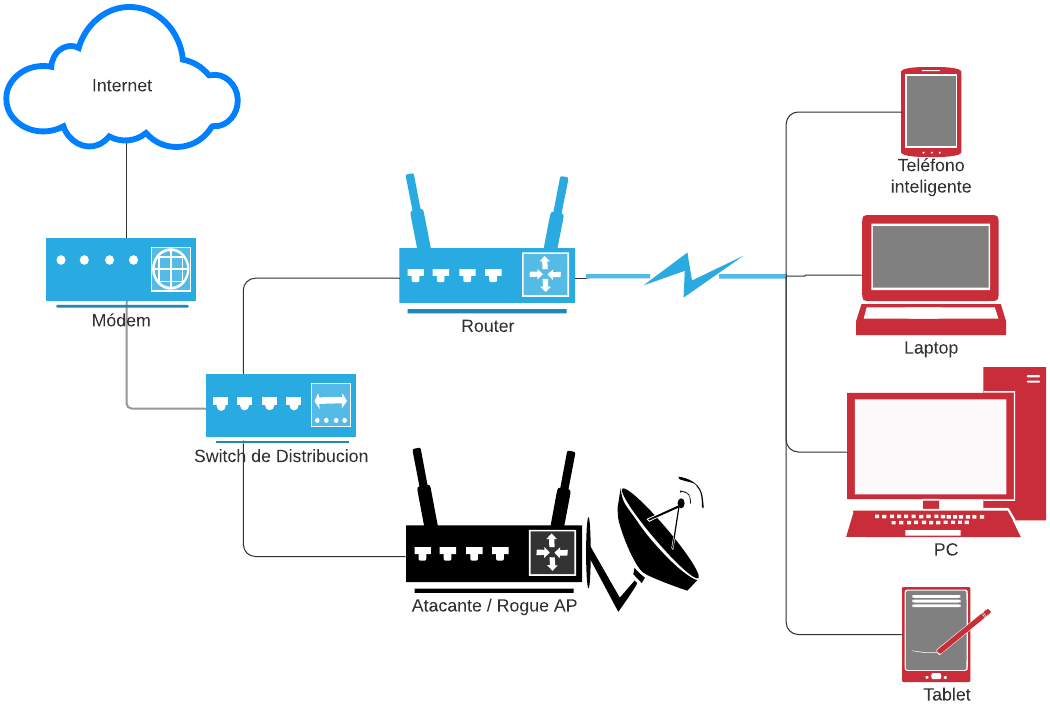

Figura 90. Topología de los laboratorios. Fuente: Elaboración propia.

Esto lleva las capacidades de los dispositivos, así que, como fue presentado, tanto equipos con Windows, como los teléfonos inteligentes con Android cuentan con las capacidades de proporcionar información sobre la red actual a la que se encuentran conectados, al igual que las redes dentro de su rango de alcance.

Para poder establecer el alcance de la propuesta, se lista en la Tabla 19 se muestran los hallazgos más relevantes para poder construir la solución.

Tabla 19: Propuesta de solución, hallazgos relevantes

n.º	Hallazgo Relevante
1	El ataque de *Wifi Spoofing* no funciona con redes inalámbricas que originalmente poseían contraseña.
2	Los dispositivos no guardan información sobre qué protocolos proveía la red válida original.
3	Únicamente las redes abiertas a las que los dispositivos conocían son las

	que el ataque aprovecha para engañar a los dispositivos a conectarse.
4	El dispositivo atacante suele tener la misma dirección MAC para muchas de las redes falsas que despliega durante el ataque.
5	No se almacena la frecuencia con la que la red original existe, por lo cual las redes falsas se despliegan con los protocolos más antiguos para tener completa compatibilidad con cualquier dispositivo.
6	El ataque sucede de forma desapercibida para el usuario, incluso una vez que el dispositivo se conecta a la red falsa.
7	Mientras se pueda capturar las redes conocidas que buscan los dispositivos, una vez que se vean en necesidad de escanear las redes aledañas, van a transmitir los nombres de las redes que buscan.
8	Debe cumplir con los requerimientos de desarrollo seguro para evitar que la propuesta sea comprometida por algún otro tipo de ataque.

Fuente: Elaboración propia.

Con base en estos hallazgos, se puede definir que el sistema por desarrollar para la mitigación de este ataque debe ser capaz de escanear las redes al alcance del dispositivo, luego evaluar si encuentra una red duplicada con el mismo nombre y la dirección MAC idéntica, y por último, alertar al usuario de redes sin seguridad o abiertas a todo público, lo cual representa un riesgo de seguridad para el usuario, ya que aunque no sea un ataque siendo ejecutado, es necesario alertar que conectarse a este tipo de redes no es seguro.

Además de esto, cabe destacar que se debe adherir a los estándares de MASVS (Owasp, 2021), los cuales para conceptos de esta propuesta cumplirán el MASVS-L1, el cual solicita el apegarse a los lineamientos de seguridad que el dispositivo solicite o mantenga, lo que quiere decir que no se debe forzar la

adquisición de la información necesaria para la ejecución de nuestra aplicación. De la misma forma específica, el código desarrollado debe ser de calidad, lo que significa que cualquier información sensible no debe ser expuesta, motivo por el cual la aplicación no almacenará ningún tipo de dato en una base de datos, ya que cualquier análisis será realizado en tiempo real.

Ahora, una vez definidos los requerimientos en el que la propuesta de solución para mitigar este tipo de ataques debe ser desarrollada, se puede realizar la implementación en cada una de las plataformas seleccionadas.

5.1 Propuesta de solución de Android

En esta propuesta, se desarrolla un sistema tomando la limitante que de la versión de Android 10 en adelante es necesario que el usuario final habilite los permisos de localización a la aplicación para que esta pueda realizar las opciones de escaneo.

El desarrollo de este sistema de mitigación se desarrolló como un *background service*, lo cual quiere decir que la aplicación, aunque se encuentre en funcionamiento, no necesita o interfiere con el uso del dispositivo al usuario.

Este sistema se aprovecha de las tareas de red usuales del dispositivo Android para que una vez que este escanee las redes en los alrededores, esta información sea capturada por la aplicación y en el caso de encontrar alguna de las anomalías descritas en los requerimientos, enviará una notificación al usuario para mantenerlo alerta o para que tome alguna acción al respecto.

Para evaluar y calificar la efectividad de la solución se ha realizado la evaluación mostrada en la Tabla 20, donde se evalúa la efectividad para detectar redes inseguras y alertar al usuario.

Tabla 20: Propuesta de solución, evaluación redes inseguras en Android

Rubro	Criterio
Método	Análisis de redes inseguras
Instancias lanzadas	5
Instancias detectadas	4
Porcentaje de detección	90%
Clasificación de detección	Mitigación eficiente

Fuente: Elaboración propia.

Esta calificación se debe a que las capacidades del dispositivo de detectar todas las redes son reducidas, en los escenarios de prueba lanzados no se pudo detectar todas, sin embargo, si detectó y notificó al usuario de las restantes, como se aprecia en la Figura 91.

Como siguiente punto por evaluar, la aplicación es capaz de detectar si luego de ser lanzado el ataque de DoS para desautenticarlo de la red válida y forzar al dispositivo a conectarse a una de las redes falsas, el sistema es capaz de alertar al usuario que se ha conectado a una red insegura y aconseja desconectarse de ella.

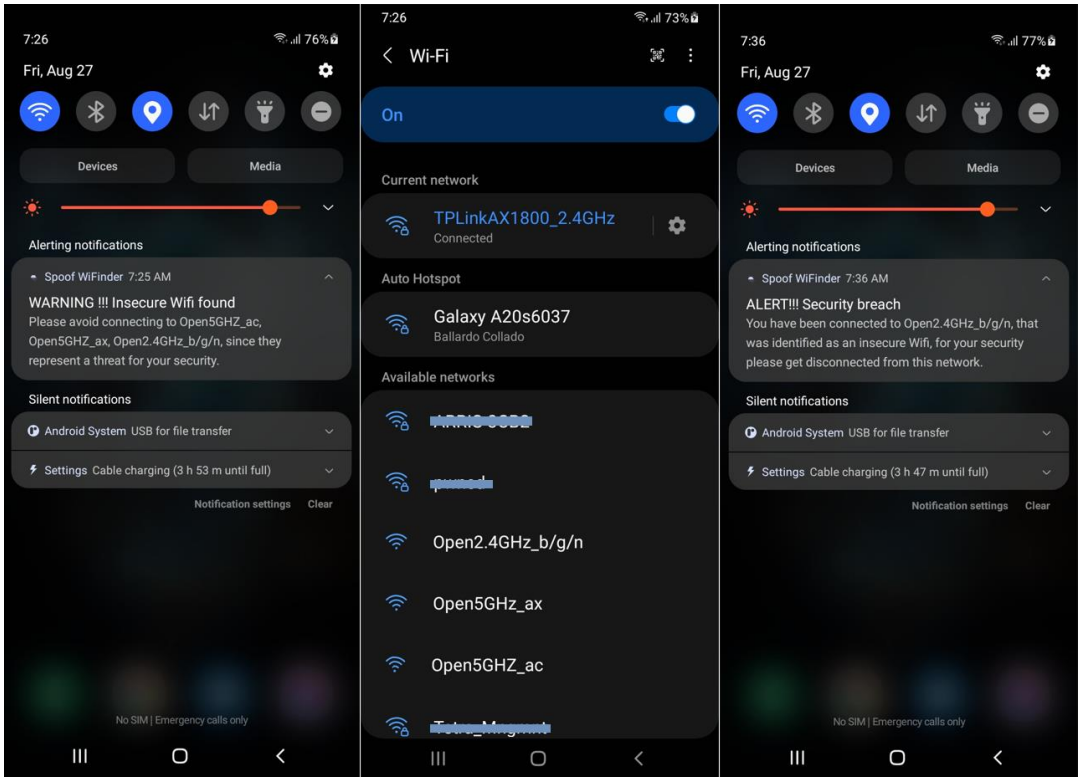

Figura 91. Propuesta de solución, detección de redes inseguras Android. Fuente: Elaboración propia.

Para la siguiente evaluación, como se observa en la Tabla 21, se realizan las pruebas para la detección de redes clonadas, gemelas o conocidas como *Evil Twin*.

Tabla 21: Propuesta de solución, evaluación redes gemelas o clonadas en Android.

Rubro	Criterio
Método	Detección de red gemela o clonada
Instancias lanzadas	5
Instancias detectadas	5
Porcentaje de detección	100%
Clasificación de detección	Mitigación eficiente

Fuente: Elaboración propia.

En este escenario, la detección es muy precisa ya que debido a que la información es exacta a la de una red activa válida, es completamente factible identificar dos redes idénticas, así como se observa en el ejercicio realizado en la Figura 92.

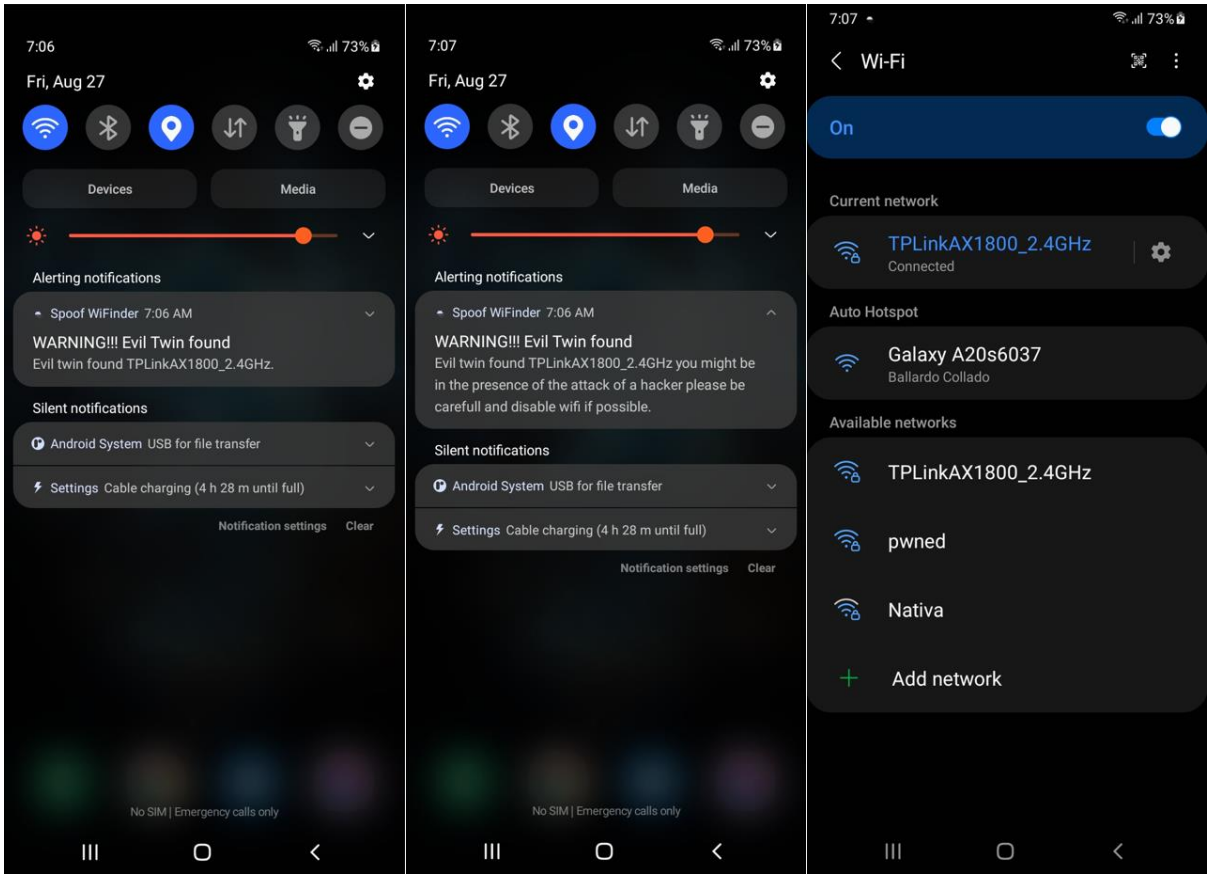

Figura 92. Propuesta de Solución, detección de *Evil Twin* en Android. Fuente: Elaboración propia.

5.2 Propuesta de solución de Windows

En el desarrollo de esta propuesta para la mitigación de la propuesta de esta investigación, se desarrolla una aplicación que nuevamente sea capaz de analizar las redes en las cercanías para poder detectar una posible amenaza o un riesgo como tal para la seguridad del usuario.

Para esta aplicación se realiza el desarrollo de otro *background service*, el cual tiene la limitante que se apega a los periodos de escaneo del sistema Windows, para no forzar alguna de las medidas de seguridad implementadas.

Sin embargo, debido al diseño del mismo sistema, este se encuentra en una tarea constante de estar conectado a la red inalámbrica que cuente con la mejor señal y que esté en sus alrededores, de manera que no es necesario realizar un escaneo constante y de lo contrario no violar las prácticas de desarrollo seguro de MASVS.

Por ello, ya sea porque el sistema lance un escaneo voluntario o en el peor de los casos que el equipo sea desconectado de forma voluntaria o involuntaria de la red inalámbrica con la que mantenía conexión, este evento va a alertar nuestro sistema y por consiguiente, alertar al usuario.

De la misma manera que con la aplicación anterior, se evalúa la efectividad del sistema de mitigación para analizar las redes inseguras que se encuentre en las cercanías del equipo, como se detalla en la Tabla 22.

Tabla 22: Propuesta de solución, evaluación redes inseguras Windows.

Rubro	Criterio
Método	Análisis de redes inseguras
Instancias lanzadas	5
Instancias detectadas	5
Porcentaje de detección	100%
Clasificación de detección	Mitigación eficiente

Fuente: Elaboración propia.

Este resultado se debe a que, en el caso de Windows, se cuenta con una mejor recepción de redes inalámbricas en los alrededores, por lo cual es capaz de

detectar todas la redes inseguras o abiertas sin encriptación, de forma que alerta al usuario de la presencia de dichas redes, al igual que es capaz de detectar que el dispositivo ha sido conectado a una de estas, independientemente de si es de forma voluntaria o involuntaria como resultado de un ataque de desautenticación para forzarlo a conectarse a una red falsa, como se observa en la Figura 93.

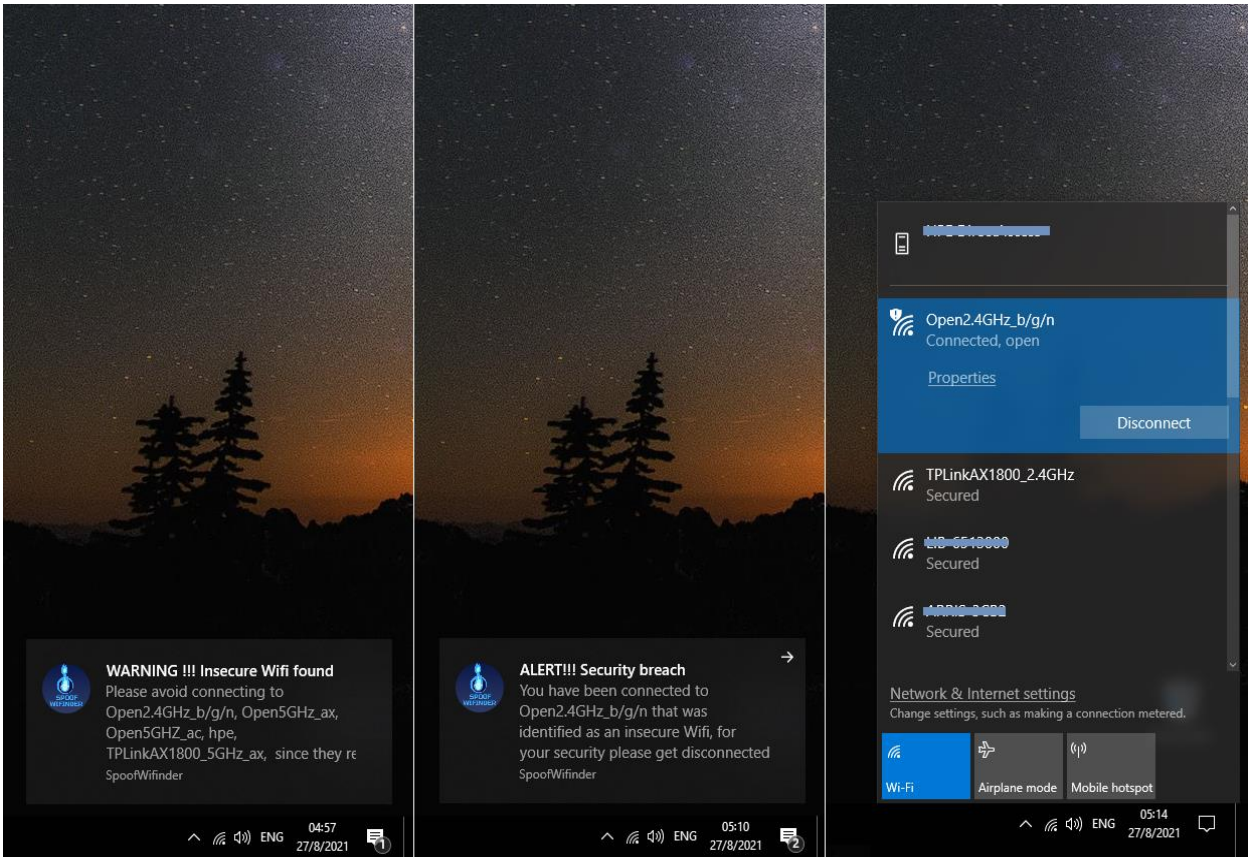

Figura 93. Propuesta de solución, detección de redes inseguras Windows. Fuente: Elaboración propia.

Como ultimo escenario, se evalúa la capacidad de la aplicación para poder detectar redes clonadas, gemelas o como se mencionaba un *Evil Twin.* El resultado altamente exitoso se documenta en la Tabla 23 a continuación.

Tabla 23: Propuesta de solución, evaluación redes gemelas o clonadas en Windows

Rubro	Criterio
Método	Detección de red gemela o clonada
Instancias lanzadas	5
Instancias detectadas	5
Porcentaje de detección	100%
Clasificación de detección	Mitigación eficiente

Fuente: Elaboración propia.

Como se mencionó en el escenario con el sistema Android, debido a que detectar una red clonada es relativamente sencillo ya que utiliza los mismos parámetros que una red válida, el poder identificara es completamente posible, como se evidencia en la Figura 94.

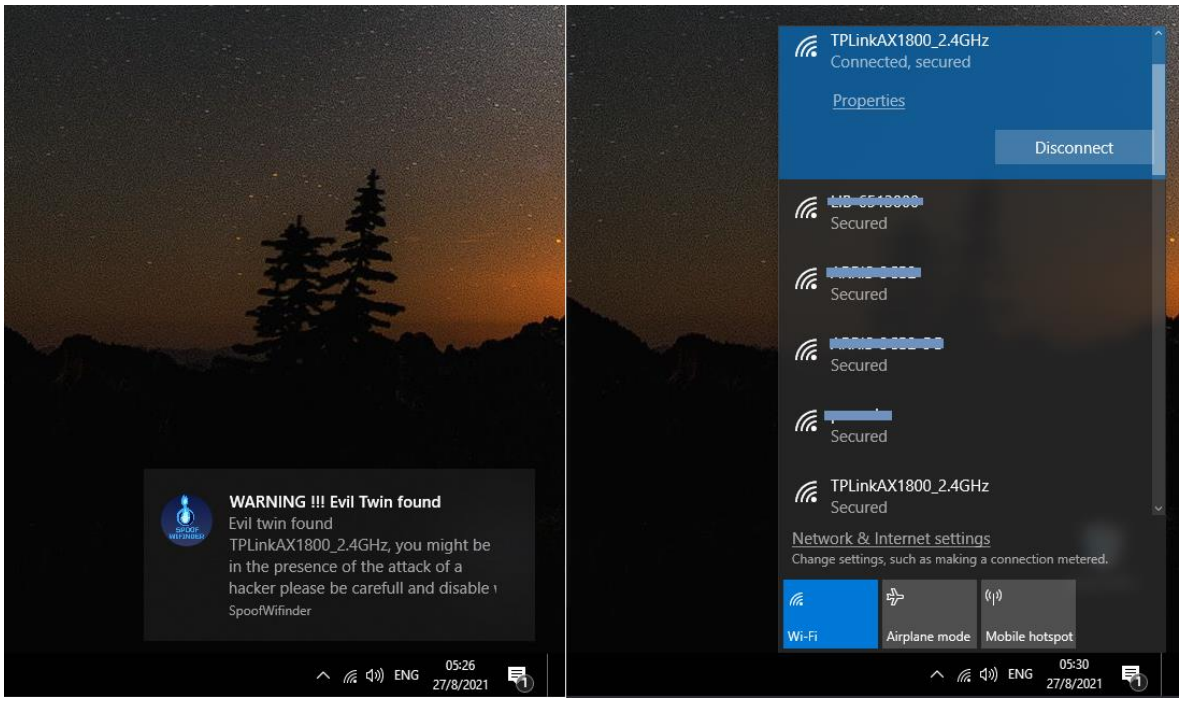

Figura 94. Propuesta de solución, detección de *Evil Twin* en Windows. Fuente: Elaboración propia.

Capítulo 6. Conclusiones y Recomendaciones

En este último capítulo se presentan las conclusiones conforme a los objetivos planteados, al igual que algunas recomendaciones que podrían tomarse en cuenta para mejorar este tipo de investigación.

6.1 Conclusiones

Conclusiones del objetivo 1: Identificar los procesos y mecanismos actuales para proteger empleados fuera de sus empresas de ataques tipo *Spoofing*.

Este objetivo fue alcanzado y se concluye:

- El poder identificar y evaluar los diferentes métodos que se encuentran disponibles para poder proveer una capa de protección o al menos mitigación para empleados fuera de sus empresas o bien cualquier usuario, requirió realizar un estudio detallado para poder determinar qué escenarios era necesario evaluar ya que en muchos casos correspondía a una solución propietaria de alguna empresa que ofrecía sus servicios.
- Se requirió estudiar y entender todo el proceso desde un bajo nivel hasta el nivel de usuario para poder identificar los mecanismos y quiénes eran responsables por el funcionamiento de las comunicaciones de redes inalámbricas y así poder identificar los puntos claves donde se podía investigar para encontrar un sistema o método existente que proveyera protección o alguna forma de mitigación para el conjunto de.
- El estudio del funcionamiento total de las comunicaciones inalámbricas dio a conocer que existen muchos intentos para proveer una mitigación exitosa, como el desarrollo del protocolo de 802.11w , el cual buscaba proteger la comunicación de los clientes de redes inalámbricas, los sistemas IDS, que funcionan como una capa intermedia de monitoreo

para identificar amenazas, el cual demostró una efectividad excelente en su función, o bien con los protocolos de seguridad o encriptación de las redes, como con el más reciente método de WPA3, que a pesar de las mejoras, no resulto exitoso para el fin de esta investigación.

Conclusiones del objetivo 2: Explicar el motivo por el cual esta amenaza se mantiene presente y representa un riesgo para las organizaciones que cuentan con sus empleados fuera de sus sedes.

Este objetivo fue alcanzado y se concluye:

- Como se demostró en los laboratorios elaborados, las capas de comunicación en todo el espectro de comunicación de redes inalámbricas de 802.11, hasta el hecho de que las prácticas del usuario final abran el portillo para explotarlas, presenta un alto riesgo para las organizaciones que necesiten proteger la integridad, confidencialidad y disponibilidad de sus equipos e información.
- El motivo, desde el punto de vista de los protocolos, se debe a que los dispositivos para poder comunicarse con el enrutador por medio de los *Probe Request* emiten la sonda de búsqueda de la red conocida en texto claro, la cual puede ser captada por cualquier observador con las herramientas de monitoreo accesibles a todo público.
- De la misma manera, el hecho de que el protocolo de *Four-way Handshake* no cuenta con un mecanismo para rechazar cualquier llamado de desautenticación que no provenga del enrutador valido, y que pueda ser aprovechado por un atacante es un factor decisivo no solo para que

sea engañado para conectarse a una red falsa, sino también para ser víctima de un ataque de DoS o DDoS.

Conclusiones del objetivo 3: Ensayar con las herramientas y técnicas de penetración más recientes la deficiencia de las medidas de mitigación existentes. Este objetivo fue alcanzado y se concluye:

- Como parte del proceso de investigación para determinar la efectividad de la mitigación de los ataques que daban paso al *Wifi Spoofing* ese escenario fue el punto clave, ya que debido a la cantidad de vulnerabilidades presentes en cada una de las capas es posible para un atacante tomar ventajas del dispositivo o la mala práctica del usuario de conectarse previamente a alguna red abierta o sin encriptación alguna.
- Parte de este proceso se evidenció al evaluar la efectividad del protocolo 802.11w, cuyo único objetivo es proteger los canales de comunicación entre el enrutador y el cliente, el cual sí protegió el contenido de los datos de la transmisión como fue evidenciado en la captura de la comunicación, pero a pesar de que este protocolo estaba activo tanto para nuestro único equipo compatible como para nuestro enrutador Raspberry Pi con el sistema OpenWRT, el éxito que tuvo el ataque de desautenticación fue evidenciado de la misma manera, por lo cual solo se puede decir que el protocolo no es capaz de proteger el canal de comunicación para evitar ser desautenticado o que el cliente conectado presente algún problema ya que es una clara evidencia que de funcionar correcta y efectivamente, este protocolo estaría habilitado sin lugar a duda en todos y cada uno de los dispositivos evaluados en los laboratorios.

- En último lugar se evaluaron los mecanismos de última generación para la encriptación de la comunicación inalámbrica con WPA3. El motivo de que cada nuevo modelo de encriptación provea una capa de seguridad adicional es proteger la contraseña que se comparte entre el enrutador y el cliente en el proceso de conexión, y como objetivo adicional -como lo detalla su documentación- proteger todos los canales de comunicación, pero nuevamente al realizar el ataque, que resulta exitoso, se observa que los dos únicos dispositivos compatibles con este nuevo mecanismo, se evidencia que al monitorear los paquetes de comunicación, de nuevo ambas partes cuentan con este mecanismo habilitado, pero no otorga protección alguna para nuestro fin.
- Esto pone de manifiesta que las herramientas de *pentesting*, desde la más sencilla de todos, el reloj desautenticador, tienen una alta efectividad, en el caso de este último es un bajo costo de adquisición, pero de una alta efectividad en sus labores, esto sin dejar de lado que el caso de Kali Linux, la cual es una herramienta completamente accesible y que cuenta de manera preconfigurada con una gran cantidad de herramientas listas para ser ejecutadas.
- La herramienta con mayor valor para la investigación es el *Wifi Pineapple*, el cual representa una inversión mínima y abre las puertas para un nuevo mundo de ataques, ya que esta herramienta encapsula en una interfaz gráfica todas las herramientas de ataque que posteriormente requerían un mayor conocimiento técnico para poder ser ejecutadas, lo cual facilita el trabajo para cualquier auditor de seguridad, pero al mismo tiempo facilita lo mismo a un posible atacante.

Conclusiones del objetivo 4: Examinar la efectividad y fallas de todas las opciones estudiadas para ser clasificadas por su capacidad de mitigación y así recomendarlas para su uso a los empleados que se encuentran en modalidad de trabajo remoto. Este objetivo fue alcanzado y se concluye:

- Como resultado, se tiene que el sistema desarrollado efectivamente provee una buena opción de mitigación, ya que no solo es capaz de realizar un escaneo de las redes que representen una posible amenaza, sino que también promueve orientar al usuario final para evitar conectarse a redes inseguras o, en el peor de los casos, que se vea en el escenario de un *Evil Twin*, para que tome la medida de apagar el wifi de su dispositivo, aunque una de las fallas para esta propuesta no es el sistema en sí, sino el hecho que para los dispositivos desarrollados por Apple Inc., no se tuviera un acceso más adecuado a la necesidad, por lo que para estos dispositivos no se pudo habilitar el programa.
- La otra forma de mitigación que mostró eficiencia es el sistema IDS o WIDS de Kismet, el cual, además de venir previamente preconfigurado en todas las versiones recientes de Kali Linux, está ya programado para detectar todos los ataques de uso común que eventualmente permiten abrir paso al *Wifi Spoofing*, por lo que es altamente recomendado, pero con la falla de que esta herramienta es útil y de fácil acceso para administradores de red, lo que deja por fuera a todo usuario final o sin el conocimiento técnico mínimo para implementar y aprovechar las capacidades de este sistema para protegerse.
- La última conclusión, la cual es cuestión de tiempo antes de que pierda su ventaja de mitigación, es el escenario con el Wifi 6, no es el hecho de que

el protocolo provea una capa de seguridad, sino que debido a lo reciente que es este protocolo, las herramientas para realizar el *pentesting* o los ataques tenían compatibilidad hasta el protocolo de 802.11ac, conocido como Wifi 5, por lo cual como se demostró en los laboratorios, estas herramientas no pudieron detectar u operar bajo este nuevo espectro, por lo consiguiente quedando inmune a los ataques, por lo que sí se encuentran protegidos estos dispositivos, pero conforme este nuevo estándar sea más comercializado, el poder tener equipos o dispositivos que puedan atacarlos es solo un asunto de tiempo.

Conclusión del objetivo general: Crear un sistema para la mitigación de ataques tipo *Spoofing* en redes inalámbricas analizando los mecanismos, herramientas y protocolos existentes para lograr mitigarlos en su mayor parte, y así ofrecer un mecanismo de protección adicional hacia los diferentes dispositivos de los usuarios dentro o fuera de una red empresarial.

El poder alcanzar el fin de nuestro objetivo requirió un arduo estudio, desde los niveles de comunicación más bajos hasta el mismo usuario para poder determinar y entender qué era necesario para poder desarrollar el mejor mecanismo de mitigación, todo este proceso tuvo como requisito claro el explorar, probar y explotar todas las vulnerabilidades existentes, incluso hasta de los medios de protección que disponibles, teniendo que ser puesto a prueba con todas las herramientas de libre acceso o que necesitaran incurrir en algún costo.

Gracias a todo el empeño puesto en esta investigación, se pudo obtener un resultado satisfactorio para los dispositivos Android y Windows que permitió desarrollar una propuesta adicional para la mitigación.

En el caso de los equipos desarrollados por Apple Inc., al establecer una capa de seguridad para evitar que se pueda acceder a las propiedades de redes inalámbricas, dejan por fuera la posibilidad de poder implementar el nuevo mecanismo, lo que en contraparte, se ve para los sistemas basados en Linux, ya se cuenta con un gran avance para la protección de este y muchos más ataques.

Es necesario resaltar que uno de los resultados más interesantes de este trabajo de investigación es el hecho de cómo las herramientas de ataque cada vez proporcionan acceso a mecanismos sofisticados de una manera “amigable” de uso, facilitando en gran medida el trabajo a un analista de seguridad, pero dejando abierto el hecho que pueda ser aprovechado por alguien con fines no éticos.

6.2 Recomendaciones

Se presentan a continuación varias recomendaciones surgidas de la experiencia obtenida en esta investigación, desde un punto de vista técnico, a un nivel de usuario final.

- Dentro de las recomendaciones técnicas es necesario resaltar que, para cualquier desarrollador en cualquier plataforma, es necesario investigar las capacidades de la plataforma en que se desee desarrollar antes de iniciar el proceso, de lo contrario puede verse en medio de la propuesta de desarrollo y llegar a un punto donde se desee utilizar cierta funcionalidad, la cual no esté disponible o se encuentre bloqueada para ese sistema en específico; esto con el fin de evitar incurrir en un gasto innecesario de equipo técnico o dispositivos.
- De la misma manera, es recomendable investigar a fondo todo proyecto que ya haya sido desarrollado, para evitar un retrabajo o simplemente para apoyarse en la documentación o recomendaciones que este provea,

lo cual puede servir de base para la construcción o mejora de una nueva propuesta.

- Las sesiones o laboratorios de pruebas, de ser posible, deben ser ejecutados en un ambiente lo más aislado posible del mundo exterior, ya que al realizar análisis de redes inalámbricas se queda expuesto a los dispositivos en las cercanías, ya que es usual que se encuentre algún dispositivo con capacidad de conexión a wifi, el cual inunde los canales de comunicación, o en este caso más específico con el envío masivo de *Probe Request*, de forma que no solo dificulta la captura de los resultados esperados, sino que satura a los equipos de análisis y por consiguiente, a todo el laboratorio.
- Al elegir el equipo de red para las pruebas es recomendable que se evalué correctamente las capacidades o protocolos en los cuales este funciona, ya que se evidenció que uno de los enrutadores, a pesar de que el fabricante aseguraba que era compatible con los últimos protocolos de redes inalámbricas, al adquirir el dispositivo este requería una actualización de *firmware*, la cual no era permitida para ser realizada fuera de los Estados Unidos, ya que solo se podía ejecutar dentro de esa área de cobertura como una medida de seguridad para ellos.

Capítulo 7. Reflexiones Finales

La interrogante que llevó al planteamiento de este trabajo de investigación, fue la inquietud del autor de poder poner en práctica los conocimientos, no solo adquiridos en esta especialidad, sino en toda la carrera profesional, de manera que se viera forzado a investigar y aprender desde los medios de comunicación actual que utiliza la tecnología, los mecanismos de *pentesting*, que muchos profesionales

utilizan día a día para poder diagnosticar certeramente una falla en un sistema o ambiente.

En la misma medida, se buscaba poder aprender de los sistemas actuales para entender los vectores de ataque de los que se aprovechan los atacantes al explotar la gran cantidad de vulnerabilidades que a pesar de que están presentes en los dispositivos de uso cotidiano, no se está consciente de ellas y nos encontramos expuestos sin estar enterados.

También con el presente trabajo, se buscaba poder formar y entender la mentalidad y habilidad de un atacante para vulnerar a toda costa un objetivo, para que poder lograr la contraparte y encontrar una forma de contrarrestar dichas acciones de la mejor forma posible.

Finalmente, como un último objetivo de este trabajo de investigación se buscaba poder tomar todas las herramientas y experiencia de programador para aplicarlas bajo medidas de seguridad, es decir, aplicando las medidas de desarrollo seguro, ya que muchas de las fallas en los sistemas que eventualmente son vulnerados, se dan porque se enfocan en proveer una solución final y no en proteger el sistema y el proceso hasta llegar a la solución, por lo cual poder aplicar una de estas metodologías fue una meta y reto personal alcanzado.

Capítulo 8. Trabajos a Futuro

- Como una mejora para esta propuesta para la mitigación, se recomienda analizar si en versiones futuras de los diferentes entornos de desarrollo se muestran mejoras, como el caso de los dispositivos de Apple Inc., los cuales en su versión actual cuentan con las limitaciones de desarrollo ya mencionadas, por lo cual en futuras versiones de sus librerías se podría

ver la opción de acceder a los datos necesarios para analizar y escanear redes inalámbricas dentro del alcance del dispositivo.

- También para estos mismos dispositivos, dentro de la comunidad de desarrolladores se cuenta con librerías privadas, no oficiales y prohibidas para el uso oficial por el fabricante, que permiten realizar las operaciones de escaneo y recolección de datos de las redes inalámbricas al alcance del dispositivo, pero esto, de ser evaluado, rompería la práctica de MASVS para el desarrollo seguro, ya que con este medio estaría violentando las medidas de seguridad por defecto del sistema. Habría que evaluar si la ganancia de utilizar esta opción justifique el no acoplarse a las prácticas de desarrollo seguro.
- Una medida para considerar es el uso de la aplicación de EvilAP_Defender, ya que incluye mecanismos de defensa y de contra ataque contra un posible atacante, de aprovechar las librerías y métodos que ofrece se podría desarrollar un sistema más robusto que proteja a los usuarios.
- Una última recomendación es buscar explotar el potencial de Kismet, ya que se encontraron estudios donde por medio de la integración de ELK (Elasticsearch, Logstash y Kibana) podría alcanzar los sistemas de notificación y reporteo de los sistemas IDS más sofisticados y costosos del mercado.

Glosario

8

802.11
Es el estándar de protocolos de una familia de normas inalámbricas creada por el Institute of Electrical and Electronics Engineers · 1

A

AP
Access Point, o punto de acceso, se conoce como el enrutador o puerta de enlace a internet o subredes · 20

D

DDoS
Ataque de denegación de servicio distribuido, se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino. · 83

DoS
Denial of Service, de los ataques más utilizados para desestabilizar sistemas informáticos para la denegación de un servicio por medio de la sobrecarga de llamados a un objetivo. · 22

I

IDS
Intrusion Detection System o sistema de detección de intrusiones, es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red · 20

IEEE
Instituto de Ingenieros Eléctricos y Electrónicos, es una asociación mundial de ingenieros dedicada a la normalización y el desarrollo en áreas técnicas. · 24

M

MAC
Significa *Media Access Control* (Control de acceso a medios). Es un identificador único para las interfaces de red. · 20

MASVS
Movie AppSec Verification Standard, es una metodología que se puede utilizar para establecer un nivel de confianza en la seguridad de las aplicaciones móviles. · 121

O

Owasp
Open Web Application Security Project, es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el *software* sea inseguro. · 117

P

Pentesting
Es una abreviatura formada por dos palabras del idioma inglés, *penetration* y *testing* y es una práctica o técnica que consiste en atacar diferentes entornos o sistemas con la finalidad de encontrar y prevenir posibles fallos. · 1

*Probe Reque*st
Es una solicitud de sondeo por parte de un dispositivo hacia una red inalámbrica cuando se realiza un "escaneo activo", mediante el cual envían tramas de solicitud en cada canal del espectro inalámbrico, estas solicitudes existen para que los enrutadores envíen información sobre sí mismos. · 30

R

RAP
Acrónimo para *Rogue Access Point*, que se define como un enrutador falso · 20

S

Spoofing
Palabra del idioma Inglés que significa suplantación, engaño , etc. · 1

W

WIDS
: *Wireless Intrusion Detection System* es una tecnología desarrollada para proteger y gestionar las infraestructuras wifi de ataques y accesos no autorizados. · 20

Wifi
: Es una abreviación de *Wireless Fidelity* para nombrar un conjunto de protocolos y *hardware* de red inalámbrica · 1

WIPS
: *Wireless Intrusion Prevention System* es un término de la industria del wifi que se refiere a la prevención de amenazas de wifi. · 2

Referencias

Agarwal, M., Biswas, S., & Nandi, S. (2018*). An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks. International Journal of Wireless Information Networks.* Obtenido de Springer: https://doi.org/10.1007/s10776-018-0396-1

ALFA Network Inc. (2020). *AWUS1900*. Obtenido de Alfa Network Inc.: https://www.alfa.com.tw/products/awus1900

Android Developers (2021). *Descripción general de la búsqueda de Wi-Fi.* Obtenido de Google Developers: https://developer.android.com/guide/topics/connectivity/wifi-scan?hl=es-419

Apple Inc. (2017). *Technical Q&A QA1942: IOS Wi-Fi Management APIs*. Obtenido de Apple Inc.: https://developer.apple.com/library/archive/qa/qa1942/_index.html

Apple Inc. (2021). *NEHotspotHelper* | *Apple Developer Documentation*. Obtenido de Apple Inc: https://developer.apple.com/documentation/networkextension/nehotspothelper

Chirumamilla, M. K. (2003). *Agent based intrusion detection and response system for wireless LANs. In: Proceedings of IEEE International Conference on*

Communications. Obtenido de IEEE: https://doi.org/10.1109/ICC.2003.1204225

CISA. (2009). *Understanding Denial-of-Service Attacks* | CISA. Obtenido de CISA: https://us-cert.cisa.gov/ncas/tips/ST04-015

Constantin, L. (2015). *This tool can alert you about evil twin access points in the area.* Obtenido de InfoWorld: https://www.infoworld.com/article/2905725/this-tool-can-alert-you-about-evil-twin-access-points-in-the-area.html

Department of Homeland Security Cybersecurity Engineering. (2017). *A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family).* Obtenido de US CISA: https://us-cert.cisa.gov/sites/default/files/publications/A_Guide_to_Securing_Networks_for_Wi-Fi.pdf.

Di Luzio, A., Mei, A. and Stefa, J. (2016*). "Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests," IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA.* Obtenido de IEEE: https://doi.org/10.1109/INFOCOM.2016.7524459.

DSTIKE. (2021). *Deauther Watch V2*. Obtenido de DSTIKE: https://dstike.com/products/dstike-deauther-watch-v2

Enisa. (2015). *Passive WIFI Surveillance and Access Point Hijacking*. Obtenido de Enisa: https://www.enisa.europa.eu/publications/info-notes/passive-wifi-surveillance-and-access-point-hijacking

Enisa. (2016). *Man-in-the-Middle*. Obtenido de Enisa: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/man-in-the-middle

Enisa. (2016). *Phishing/Spear phishing*. Obtenido de Enisa: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing

GitHub. (2016). *moha99sa/EvilAP_Defender Wiki*. Obtenido de GitHub: https://github.com/moha99sa/EvilAP_Defender

Glassdoor. (2021). *Salary: Cyber Security Analyst.* Obtenido de Glassdoor: https://www.glassdoor.com/Salaries/cyber-security-analyst-salary-SRCH_KO0,22.htm

Gonzales, H., Bauer, K., Lindqvist, J., McCoy, D. and Sicker, D. (2010*). "Practical Defenses for Evil Twin Attacks in 802.11*". 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL, USA. Obtenido de IEEE: https://doi.org/10.1109/GLOCOM.2010.5684213.

Gruber, T. R. et al. (1993), *"*A translation approach to portable ontology specifications," *Knowledge acquisition, vol. 5, no. 2.* Obtenido de ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S1042814383710083

Hak5. (2021). *About the WiFi Pineapple*. Obtenido de Hak5: https://docs.hak5.org/hc/en-us/articles/360010471394-About-the-WiFi-Pineapple

IEEE 802.11. (1999). *Standard for Information Technology—Telecommunications and information exchange between systems—Local and Metropolitan Area*

networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Obtenido de IEEE: https://standards.ieee.org/standard/802_11-1999.html

IEEE. (2021). *802.11w-2009—IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Protected Management Frames.* (s/f). Obtenido de IEEE: https://standards.ieee.org/standard/802_11w-2009.html

Intel. (2021). *Diferentes protocolos de Wi-Fi y velocidades de datos*. Obtenido de Intel Asistencia: https://www.intel.la/content/www/xl/es/support/articles/000005725/wireless/legacy-intel-wireless-products.html

Kao, K., Yeo, T., Yong, W. and Chen, H. (2011). A location-aware rogue AP detection system based on wireless packet snifng of sensor APs. In: *Proceedings of the 2011 ACM Symposium on Applied Computing, SAC '11,* New York, USA. Obtenido de ACM: https://dl.acm.org/doi/10.1145/1982185.1982195

Kismet. (2021). *Kismet*. Obtenido de Kismet: https://www.kismetwireless.net/

Lun Dong, Z. Han, A. P. Petropulu and H. V. Poor. (2008). "Secure wireless communications via cooperation," 2008 46th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA. Obtenido de IEEE: https://doi.org/10.1109/ALLERTON.2008.4797687.

Microsoft. (2021). *Known Issue – Unable to deploy apps when targeting Windows 10, version 1809 (Windows 10 1809 SDK (17763), October 2018 release.).* Obtenido de Microsoft: https://social.msdn.microsoft.com/Forums/sqlserver/en-US/d6d5980d-ec6d-4fc1-9eaa-5bb20f23c600/known-issue-8211-unable-to-deploy-apps-when-targeting-windows-10-version-1809-windows-10-1809?forum=Win10SDKToolsIssues

Microsoft. (2021). *Modern Apps—Build a Wi-Fi Scanner in the UWP.* Obtenido de Microsoft: https://docs.microsoft.com/en-us/archive/msdn-magazine/2016/july/modern-apps-build-a-wi-fi-scanner-in-the-uwp

Nakhila, O. and Zou, C. (2016). "*User-side Wi-Fi evil twin attack detection using random wireless channel monitoring," MILCOM 2016 - 2016 IEEE Military Communications Conference, Baltimore, MD, USA.* Obtenido de IEEE: https://doi.org/10.1109/CCNC.2015.7157983.

Nakhila, O., Dondyk, E. Amjad, M. F. and Zou, C. (2015). *"User-side Wi-Fi Evil Twin Attack detection using SSL/TCP protocols,"* 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA. Obtenido de IEEE: https://doi.org/10.1109/CCNC.2015.7157983.

Naranjo, L. (2020). Investigación en Informática: el enfoque alternativo*. Revista Technology Inside by CPIC.* Obtenido de CPIC: https://cpic-sistemas.or.cr/revista/index.php/technology-inside/article/view/35

Offensive Security. (2021). *Kali Linux Features*. Obtenido de Kali Linux: https://www.kali.org/features/

Oliveira, L., Schneider, D., Souza, J. D., & Shen, W. (2019). *Mobile Device Detection Through WiFi Probe Request Analysis*. IEEE Access, 7. Obtenido de IEEE: https://doi.org/10.1109/ACCESS.2019.2925406

OpenWrt Project. (2005). *OpenWrt/LEDE project*. Obtenido de OpenWrt: https://openwrt.org/

Owasp. (2021). *Using the MASVS.* Obtenido de: https://mobile-security.gitbook.io/masvs/0x03-using_the_masvs

Palazzi, C. E., Brunati, M. and Roccetti, M. (2010). *"An OpenWRT solution for future wireless homes," 2010 IEEE International Conference on Multimedia and Expo, Singapore.* Obtenido de IEEE: https://doi.org/10.1109/ICME.2010.5583223.

Sandoval, S. R., Carvajal, H. V., & Zeledón, L. N. (2019). Adaptación de la metodología de ciencia de diseño en el desarrollo de luminarias. T*ecnología Vital.* Obtenido de Tecnología Vital: https://revistas.ulatina.ac.cr/index.php/tecnologiavital/article/view/252

Simon, H. (1996). *The Sciences of the Artificial*. London: The Mit Press. Obtenido de: https://rauterberg.employee.id.tue.nl/lecturenotes/DDM110%20CAS/Simon-1969%20The_Sciences_of_the_Artificial_3rd_ed.pdf

Sriram, V., Sahoo, G. and Agrawal, K. (2010). *Detecting and eliminating rogue access points in IEEE-802.11 WLAN—A multi-agent sourcing methodology. In: Advance Computing Conference (IACC), 2010 IEEE 2nd International.* Obtenido de IEEE: https://doi.org/10.1109/IADCC.2010.5422999.

United Nations. (2016). *General Assembly "Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development.".* Obtenido de United Nations: https://doi.org/10.1163/2210-7975_HRD-9970-2016149

Vargas, A. I. (2004). GUÍA PARA ELABORAR UNA PROPUESTA DE INVESTIGACIÓN. *Revista Educación* 29(0379-7082), 92. Obtenido de Revista Educación: revistas.ucr.ac.cr/index.php/educacion/article/viewFile/2241/2200

Wang, W., & Wang, H. (2011). *Weakness in 802.11w and an improved mechanism on protection of management frame.* 2011 International Conference on Wireless Communications and Signal Processing (WCSP). Obtenido de IEEE: https://doi.org/10.1109/WCSP.2011.6096780

Wi-Fi Alliance. (2021). *Discover Wi-Fi Security*. Obtenido de Wi-Fi Alliance: https://www.wi-fi.org/discover-wi-fi/security