ANÁLISIS DE LOS PROTOCOLOS DE SEGURIDAD INALÁMBRICA IMPLEMENTADAS EN LAS REDES WIFI EN LA CIUDAD DE BOGOTÁ

JEIMY TATIANA PEREZ GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

ANÁLISIS DE LOS PROTOCOLOS DE SEGURIDAD INALÁMBRICA IMPLEMENTADAS EN LAS REDES WIFI EN LA CIUDAD DE BOGOTÁ

JEIMY TATIANA PEREZ GARCÍA

Proyecto de investigación para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director de trabajo de grado
Edgar Mauricio López Rojas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, marzo 2022

DEDICATORIA

Primero quiero agradecer a Dios por darme siempre la fortaleza y el entusiasmo para seguir adelante, a pesar de los retos que se presentan en el camino, aunque muchas veces sentía que estaba a punto de rendirme halle en él la valentía y el coraje para seguir adelante.

Agradezco a mis padres y hermanos por alentarme siempre a conseguir mis objetivos y por inspirarme a dar siempre lo mejor posible de mí; para compartir mis éxitos como suyos y llenarles de orgullo. Le dedico este triunfo a mi madre por siempre ser una fuente de inspiración; por haber sido una mujer valiente, dedicada y trabajadora, que siempre nos inundó con su cálido amor y a la que siempre llevo en mis pensamientos y en mi corazón.

También quiero agradecer a Camilo por ser guía y un excelente mentor en diferentes aspectos de mi vida, por siempre confiar en mis habilidades, potenciar mi conocimiento, apoyarme en una carrera llena de retos y por su amor incondicional.

AGRADECIMIENTOS

Agradezco a cada uno de los tutores y directores de curso que me han ayudado a llegar hasta este punto al compartir su valiosa experiencia, conocimiento y profundo entusiasmo por cada una de las ramas de la ingeniería de sistemas y de la ciberseguridad de las que pude aprender. Gracias por su profesionalismo y entendimiento ante las adversidades e inquietudes que presentamos como alumnos; nos inspiran a ser mejores personas y esperamos ser los mejores profesionales posibles en honor a sus enseñanzas.

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

AMENAZA: una amenaza es cualquier tipo de peligro, que puede dañar o robar datos, crear una interrupción o causar un daño en general. Algunos ejemplos comunes de amenazas son el código malicioso (o malware), el phishing, las violaciones de datos e incluso los empleados deshonestos (o insiders).

ANTENA WIFI: una antena es un dispositivo que irradia ondas de radio cuando se le suministra energía eléctrica, o un dispositivo que convierte las ondas de radio en energía eléctrica. Las antenas a veces se crean intencionadamente para ser usadas como una antena de un router inalámbrico.

AUTENTICACIÓN: es el proceso de reconocimiento de la identidad de un usuario. Es un mecanismo de asociar una solicitud entrante con un conjunto de credenciales de identificación. Las credenciales proporcionadas se comparan con las de un archivo de una base de datos de información del usuario autorizado en un sistema operativo local o en un servidor de autenticación**.**

BEACON: es un paquete de difusión enviado por el router que sincroniza la red inalámbrica. Un beacon es necesario para recibir información sobre el router, incluyendo, pero no limitado a SSID y otros parámetros. Es simplemente la frecuencia con la que el router emite la información.

CRACKER: Un cracker es un individuo que realiza cracking, o el proceso de irrumpir en un ordenador o en un sistema de red. Un cracker puede llevar a cabo el cracking por actividades maliciosas, por lucro, por determinadas intenciones o causas no lucrativas, o simplemente por un reto.

CIBERATAQUE: es un conjunto de acciones llevadas a cabo por agentes maliciosos,

que intentan obtener acceso no autorizado, robar datos o causar daños a ordenadores, redes informáticas u otros sistemas informáticos. Un ciberataque puede ser lanzado desde cualquier lugar. El ataque puede ser realizado por un individuo o un grupo que utiliza una o varias tácticas, técnicas y procedimientos.

CIFRADO: es el método por el cual la información se convierte en un código secreto que oculta su verdadero significado. La ciencia de cifrar y descifrar información se llama criptografía. Los datos no cifrados se denominan texto plano y los datos cifrados, texto cifrado. Las fórmulas utilizadas para codificar y descodificar los mensajes se denominan algoritmos de encriptación o cifrado.

CONFIDENCIALIDAD: garantiza que los datos intercambiados no sean accesibles a usuarios no autorizados. Los usuarios pueden ser aplicaciones, procesos, otros sistemas o personas. A la hora de diseñar un sistema, deben existir mecanismos de control adecuados para imponer la confidencialidad, así como políticas que dicten lo que los usuarios autorizados pueden y no pueden hacer con los datos.

DISPONIBILIDAD: garantiza que los sistemas, las aplicaciones y los datos estén disponibles para los usuarios cuando los necesiten. El ataque más común que afecta a la disponibilidad es la denegación de servicio en la que el atacante interrumpe el acceso a la información, al sistema, a los dispositivos o a otros recursos de la red.

FIRMWARE: es un software que se escribe directamente en el hardware. Funciona sin pasar por una API, sistema operativo o los controladores del dispositivo, entregando las instrucciones que el dispositivo necesita para comunicarse con otros dispositivos o realizar diversas tareas, así como la funcionalidad básica esperada.

INTEGRIDAD: es la capacidad de garantizar que un sistema y sus datos no han sufrido modificaciones no autorizadas. La protección de la integridad protege no sólo los datos, sino también los sistemas operativos, las aplicaciones y el hardware para que no sean

alterados por personas no autorizadas.

ISP: o proveedor de servicios de internet, es una empresa que permite acceder a internet desde casa, normalmente con una suscripción mensual.

KALI LINUX: es una distribución basada en Debian y desarrollada por Backtrack muy reconocida y usada en el mundo de la seguridad dado que cuenta con muchas herramientas que son útiles para analistas de seguridad y expertos en pruebas de penetración.

MALWARE: es el nombre colectivo para una serie de variantes de software malicioso, incluyendo virus, ransomware y spyware. El malware consiste en un código desarrollado por ciber atacantes, diseñado para causar grandes daños a los datos y sistemas o para obtener acceso no autorizado a una red.

MODEM DE INTERNET: es una pequeña caja que conecta los dispositivos a Internet mediante cables. Un módem actúa como traductor digital, tomando una señal de información de las líneas de cable, fibra o teléfono y haciéndola accesible a su ordenador por medio de cable ethernet o de señal inalámbrica WiFi.

MODO PROMISCUO: es un tipo de modo operativo de redes informáticas en el que los adaptadores de red que operan en este modo pueden acceder a todos los paquetes de datos de la red y verlos.

PRUEBA DE CONCEPTO: Una prueba de concepto o PoC es un ejercicio en el que el trabajo se centra en determinar si una idea puede convertirse en realidad. Una prueba de concepto sirve para determinar la viabilidad de la idea o para verificar que la idea funcionará como se ha previsto.

RECONOCIMIENTO ACTIVO: el footprinting activo consiste en recoger información interactuando directamente con el objetivo. Con este tipo de footprinting existe la posibilidad de que el objetivo se dé cuenta de la recolección de información.

RECONOCIMIENTO PASIVO: El footprinting pasivo consiste en recoger información sin interactuar directamente con el objetivo. En este caso el reconocimiento no debe ser detectado por el objetivo.

REDES INALÁMBRICAS: Una red inalámbrica es una red informática que utiliza conexiones de radiofrecuencia entre los nodos de la red. Las redes inalámbricas son usadas tanto en hogares como en empresas. La gente suele asumir que todo lo inalámbrico es Wi-Fi, pero no es así. Hay muchos tipos diferentes de redes inalámbricas en toda una gama de tecnologías como Bluetooth, ZigBee, LTE, 5G, mientras que Wi-Fi es específico del protocolo inalámbrico definido por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) en la especificación 802.11 y sus enmiendas.

RIESGO: es una combinación de la probabilidad de amenaza y el impacto de una vulnerabilidad. En otras palabras, el riesgo es la probabilidad de que un agente de amenaza explote con éxito una vulnerabilidad.

SHELL: es un entorno en el que podemos ejecutar nuestros comandos, programas y scripts. Hay diferentes shells, al igual que hay diferentes sistemas operativos. Cada diferente de shell tiene su propio conjunto de comandos y funciones reconocidos.

SSID: es el término técnico para el nombre de una red Wi-Fi. Cuando se configura una red inalámbrica, se le da un nombre para distinguirla de las demás redes cercanas.

SNIFFING: es un proceso de monitoreo y captura de todos paquetes de datos que pasan por una red determinada. Los sniffers son utilizados por el administrador de la red o del sistema para supervisar y solucionar el tráfico de la red. Aunque los ciber atacantes

utilizan los sniffers para capturar paquetes de datos que contengan información sensible como contraseñas, información de cuentas, etc.

VISTUMBLER: es un software que permite mapear y visualizar los puntos de acceso que te rodean basándose en los datos inalámbricos y GPS recogidos.

VULNERABILIDAD: es una debilidad en el hardware, el software, del personal o los procedimientos, que puede ser explotada por los actores de la amenaza para lograr sus objetivos. Las vulnerabilidades pueden ser físicas o lógicas.

WARDRIVING: es la metodología que le permite a las personas buscar redes WiFi conduciendo en un vehículo en movimiento, a menudo utilizando un dispositivo GPS para registrar la ubicación de las redes inalámbricas que encuentran. Luego, suben estos datos a sitios web específicos que procesan la información para crear mapas digitales de las redes del barrio. Esto no es un acto malintencionado, ni es ilegal. De hecho, hubo polémica cuando Google admitió la recopilación de datos de WiFi mientras tomaba imágenes de vídeo e información de geolocalización para crear su aplicación Street View, pero la acción en sí no se consideró una violación ilegal de la privacidad.

WEP: es un algoritmo de seguridad introducido para proporcionar confidencialidad a los datos de las redes inalámbricas. La Privacidad Equivalente al Cable o WEP se introdujo como parte del estándar 802.11, ratificada en 1997. Como solución inicial, su objetivo era evitar los ataques Man-in-the-Middle, lo que consiguió durante un tiempo.

WIFI: es la tecnología que permite a un PC, un portátil, un teléfono móvil o una tableta conectarse a alta velocidad a Internet sin necesidad de una conexión física por cable. Wi-Fi es un término que fue acuñado por una empresa de branding en 1999 como un nombre que se recordaría fácilmente, debido a su similitud con el entonces conocido término "hi-fi".

WPA: es un protocolo de seguridad diseñado para crear redes inalámbricas seguras. Es similar al protocolo WEP, pero ofrece mejoras en el manejo de las claves de seguridad y en la forma de autorizar a los usuarios. Para que una transferencia de datos cifrada funcione, los dos sistemas al principio y al final de una transferencia de datos deben utilizar la misma clave de cifrado o descifrado.

WPA2: es el método de seguridad añadido a WPA para las redes inalámbricas que proporciona una mayor protección de los datos y control de acceso a la red. Proporciona a los usuarios de Wi-Fi de empresas y consumidores un alto nivel de garantía de que sólo los usuarios autorizados pueden acceder a sus redes inalámbricas.

WPA3: fue lanzado en junio de 2018, es el sucesor de WPA2. El objetivo de desarrollar WPA3 era mejorar WPA en términos de simplicidad de uso y mayor fuerza en el cifrado. Esta versión mejora a WPA2 con funciones de autenticación y cifrado más robustas, y una solución al fallo incorporado en WPA2, KRACK. También incluye funcionalidades para simplificar, y asegurar mejor, la conexión de dispositivos wifi IoT.

XGPS: es un cliente de prueba para gpsd con una interfaz. Muestra la información actual de posición, tiempo y velocidad del GPS y las ubicaciones de los satélites accesibles.

RESUMEN

Las personas se enfrentan cada día a retos más diversos con el uso de internet. El auge de nuevas tecnologías, dispositivos y el crecimiento del tiempo en la navegación en internet a causa de la pandemia ha generado que no solo haya personas con mayor acceso a la información, sino que también los ciberdelincuentes puedan aprovechar su deficiente conocimiento del tema para tomar provecho y efectuar cualquier tipo de ataque.

Este documento contiene la información relacionada a la investigación de los tipos de protocolo de seguridad que usan las redes inalámbricas en Bogotá usando la técnica de WarDriving, una cuantificación de dichos protocolos y una explicación de estos; así como de los ciberataques y consecuencias que podrían llegar a asumir al usar protocolos débiles de seguridad en sus conexiones de internet.

De esta forma se permiten generar recomendaciones que puedan ser usadas por todo tipo de usuarios de redes inalámbricas de conexión a internet, para ayudar a minimizar la probabilidad de que ese riesgo se materialice por medio de la concientización de usuarios y la muestra de los posibles ciberataques en entornos controlados al usar estos protocolos inseguros.

Palabras claves: redes inalámbricas, WarDriving, protocolos de seguridad inalámbrica, WEP, WPA, WPA2, WPA3.

ABSTRACT

People face more diverse challenges every day with the use of the Internet. The rise of new technologies, devices and the growth of time spent surfing the Internet due to the pandemic has generated that not only people have greater access to information, but also cybercriminals can take advantage of their poor knowledge of the subject to take advantage and carry out any kind of attack.

This document contains information related to the investigation of the types of security protocols used by wireless networks in Bogota using the WarDriving technique, a quantification of these protocols and an explanation of these, as well as cyberattacks and consequences that could be assumed when using weak security protocols in their wireless Internet connections.

In this way, it is possible to generate recommendations that can be used by all types of users of wireless networks connecting to the Internet, to help minimize the likelihood of this risk materializing by raising awareness of users and showing the possible cyber-attacks in controlled environments when using these insecure protocols.

Keywords: wireless networks, wardriving, wireless security protocols, WEP, WPA, WPA2, WPA3

INTRODUCCIÓN

Actualmente las conexiones inalámbricas, específicamente las conexiones definidas en la IEEE 802.11x o popularmente conocidas como redes WiFi, se han convertido en parte esencial de las comunicaciones en múltiples entornos. Es así como se encuentran redes WiFi en restaurantes, bibliotecas, aeropuertos, bancos y muchos lugares más; sin embargo, no se puede hablar de conexiones sin involucrar a los dispositivos de los usuarios finales donde hoy en día prácticamente todo puede estar conectado a la red; el Internet de las Cosas (IoT) como nueva tecnología de interconexión de dispositivos ha hecho que la vida cotidiana esté interconectada con múltiples servicios.

Hoy en día es prácticamente imposible imaginar un mundo sin conexiones a la red ya que sería muy difícil, por no decir imposible realizar muchas de las actividades que hacen que el mundo se mueva hoy en día; por ejemplo, piense que sin los servicios de red muchas operaciones bancarias no se podría realizar o por ejemplo no sería tan fácil llevar el funcionamiento de las empresas debido a la pandemia por COVID-19 que obligó a que todo el mundo se incluyera en el teletrabajo y la oficina en casa para seguir trabajando y mantener las operaciones globales.

Aunque las tecnologías WiFi no son nuevas para nadie, ya que se han implementado desde hace más de 30 años gracias a la creación del IEEE802.11, la evolución de estas redes ha traído consigo cambios relacionados con sus mecanismos de seguridad desde que se vulneró el protocolo WEP, de ahí el lanzamiento de WPA, WPA2 y otras versiones que finalmente se liberaron sin ser completadas y siguieron desplegando vulnerabilidades en todas las infraestructuras donde se utilizan las redes WiFi.

Una red WiFi con contraseña no es garantía de seguridad; así se ha demostrado en múltiples pruebas de concepto en donde un ciberdelincuente podría comprometer fácilmente la seguridad de una red y por tanto toda la información que circula por ella.

Por otro lado, las redes WiFi están vinculadas a otros dispositivos de red que tienen conectados múltiples dispositivos no inalámbricos como servidores, impresoras, redes VolP en el caso de entornos corporativos y dispositivos como televisores, sistemas de CCTV, alarmas y otros en entornos domésticos. Por todo ello, existen múltiples técnicas de recopilación de información sobre objetivos inalámbricos para muchos ciberataques; sin embargo, es posible hacer uso de estas técnicas para hacer una revisión de las configuraciones más comunes y de las implementaciones erróneas de las redes Wifi con el fin de proporcionar metodologías de mitigación y recomendaciones para los usuarios que hacen uso de este tipo de redes prestadas o públicas.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Desde la invención del WiFi se han venido exponiendo al público diferentes tipos de protocolos de seguridad para proteger las conexiones. Los protocolos de seguridad de las redes inalámbricas son aquellos con los cuales se logra proteger, cifrar los datos y el tráfico que viajan por la red mientras estamos conectados a una red inalámbrica. Desde 1997 hasta la actualidad se han publicado 4 protocolos diferentes en los que encontramos WEP, WPA, WPA2 y WPA3 cada uno con distintas características y cualidades, pero con la particularidad que su desarrollo no fue lo suficientemente profundo como para garantizar que ningún ciberdelincuente pueda acceder a ella.

La primera norma IEEE para el Wi-Fi se publicó en 1997 y se conoce como IEEE 802.11. Tenía grandes deficiencias, ya que el rendimiento máximo era de 2 Mbps. En 1999 se introdujeron dos modificaciones en la norma original. 802.11a funcionaba en la banda de 5 GHz y utilizaba OFDM, mientras que 802.11b seguía en la banda de 2,4 GHz y utilizaba DSSS.

La OFDM se ha adoptado en el ámbito de la Wi-Fi, con estándares como 802.11a, 802.11n y 802.11ac, entre otros. También se ha elegido para el estándar de telecomunicaciones celulares LTE / LTE-A, y además ha sido adoptado por otros estándares como WiMAX y muchos más. La multiplexación por división de frecuencias ortogonales también se ha adoptado para una serie de estándares de radiodifusión, desde la radio digital DAB hasta los estándares de difusión de vídeo digital, DVB. También se ha adoptado para otros sistemas de radiodifusión, como la Radio Digital Mundial, que se utiliza para las bandas de onda corta y media larga. Aunque la multiplexación por división de frecuencias ortogonales (OFDM) es más complicada que las formas anteriores de formato de señal, ofrece algunas ventajas claras en términos de transmisión de datos, especialmente cuando se necesitan altas velocidades de datos junto con anchos de banda relativamente amplios.

El espectro ensanchado de secuencia directa (DSSS) es una forma de transmisión de espectro ensanchado que utiliza códigos de propagación para distribuir la señal en un ancho de banda mayor del que normalmente se necesitaría. Es una forma de transmisión que se parece mucho al ruido blanco en el ancho de banda de la transmisión. Sin embargo, una vez que se recibe y se procesa con los códigos de descodificación correctos, es posible extraer los datos necesarios. Cuando se transmite una señal de espectro ensanchado DSSS, la señal de datos requerida se multiplica con lo que se conoce como un flujo de datos de propagación o código de chip. El flujo de datos resultante tiene una velocidad de datos superior a la de los propios datos.

La principal diferencia entre DSSS y OFDM se da en un entorno de radio frecuencia congestionado o limitado. Como el DSSS transmite el mayor número posible de bits a la vez, corre el riesgo de que parte de la transmisión se interrumpa en tránsito si la radio frecuencia no es la ideal. En cambio, OFDM sacrifica un poco de rendimiento para transmitir los datos en esos paquetes de múltiples portadoras que permiten el reensamblaje o la retransmisión en caso de fallo. Por ejemplo, si se utiliza un transporte de carga extragrande para transportarla, funciona bien siempre que la autopista no tenga ningún obstáculo como carriles estrechos, trochas o pasos elevados cortos. Si se divide la carga en un mayor número de camiones más pequeños, se puede asegurar que parte de la carga llegue, aunque las condiciones como un trancón o un derrumbe impidan que llegue todo el envío. El hecho es que OFDM se utiliza para 802.11n y superiores, por lo que parece ser el que cumple de una mejor manera con los estándares del mercado actual.

A pesar de ser superior en muchos aspectos, 802.11a nunca alcanzó el nivel de éxito comercial de 802.11b debido al precio. 802.11.b era más barato y se adoptó como estándar de facto. Últimamente es más común ver routers inalámbricos tri-modales con 802.11n y 802.11b/g. 802.11a no está obsoleto en sí mismo, sino que es otro ejemplo de cómo el aspecto comercial de la tecnología supera el rendimiento.

Otras características importantes desde el despliegue de la 802.11b son:

- 802.11b:
  - Aumento de la velocidad de datos a 11 Mbps.
  - El ancho de banda de 22 MHz proporciona 3 canales no solapados en el rango de frecuencias de 2,400 GHz a 2,4835 GHz.
- 802.11d:
  - Mejoras del estándar 802.11a y 802.11b que permite el roaming global.
- 802.11e:
  - Mejora del estándar 802.11 que incluye funciones de calidad de servicio (QoS). La calidad de servicio hace referencia a cualquier tecnología que gestione el tráfico de datos para reducir la pérdida de paquetes, la latencia y el jitter en una red. Controla y gestiona los recursos de la red estableciendo prioridades para determinados tipos de datos en la red.
  - Facilita la priorización de las transmisiones de datos, voz y vídeo.
- 802.11g:
  - Amplía la velocidad máxima de datos de los dispositivos WLAN que operan en la banda de 2,4 GHz, de forma que permite la interoperabilidad con los dispositivos 802.11b.
  - Utiliza la modulación OFDM.
  - Funciona hasta 54 megabits por segundo (Mbps), con velocidades de retroceso que incluyen las velocidades "b".
- 802.11h:
  - Mejora del estándar 802.11a que resuelve los problemas de interferencias.
  - Selección dinámica de frecuencia (DFS).
  - Control de potencia de transmisión (TPC).
- 802.11i:
  - Mejora del estándar 802.11 que ofrece seguridad adicional para las aplicaciones WLAN.

    - Define un cifrado, una autenticación y un intercambio de claves más potentes; así como, opciones para el almacenamiento en caché de claves y la pre-autenticación.
- 802.11j
    - Ampliaciones reglamentarias japonesas de la especificación 802.11a
    - Gama de frecuencias de 4,9 GHz a 5,0 GHz.
- 802.11k:
    - Mediciones de recursos radioeléctricos para redes que utilizan especificaciones de la familia 802.11.
- 802.11m:
    - Mantenimiento de las especificaciones de la familia 802.11.
    - Correcciones y modificaciones de la documentación existente.

La última de las especificaciones técnicas que se han añadido al estándar es la 802.11n, que utiliza la tecnología MIMO (multiple input / multiple output) y un canal de radiofrecuencia más amplio. También proporciona un mecanismo denominado agregación de tramas para reducir el tiempo entre transmisiones. Las tecnologías WLAN actuales requieren que la estación emisora solicite el canal, envíe un paquete, libere el canal y vuelva a solicitarlo para enviar el siguiente paquete. Con la agregación de tramas, una vez que una estación solicita el canal y tiene la autoridad para transmitir, puede transmitir una serie de tramas sin tener que liberar el canal y recuperar la autoridad para cada trama. Con 802.11n, el rendimiento de los datos en bruto alcance los 600 Mbps, es decir, más de 10 veces el rendimiento de 802.11g.

Aunque el IEEE comenzó a trabajar en 802.11n en 2004, los avances en la validación de la especificación se vieron paralizados por los grupos de proveedores que competían entre sí. El borrador 1 de la norma se publicó en 2006 y los equipos "pre-N" estuvieron disponibles poco después. El borrador 2 se aprobó en 2007. Los equipos "pre-N" han demostrado una velocidad de datos de hasta 540 Mbps, con tasas típicas de entre 100 y

200 Mbps. Se espera que las velocidades de datos aumenten a medida que aumente la experiencia con la norma.

Usar protocolos de seguridad inalámbrica obsoletos o vulnerables puede traer consecuencias muy graves para cualquier infraestructura dado que se convierten en blancos fáciles para ataques de ciberdelincuentes, teniendo en cuenta que al burlar el protocolo de conexión y lograr la conexión se estaría dentro de la infraestructura del cliente y consecuente a ello se puede mapear la red, acceder a recursos compartidos y ejecutar escalamientos horizontales o verticales de privilegios en donde se puede llegar a comprometer cualquier tipo de sistema.

La principal motivación para la ejecución de esta investigación precede a varios eventos de seguridad informática en especial, la Ekoparty. La Ekoparty es una de las conferencias de seguridad informática y hacking más importantes del habla hispana y la más grande en Latinoamérica, es celebrada en Argentina y en donde la técnica de WarDriving tiene una participación muy activa y además tiene gran valor académico; allí se interactúa con distintas herramientas, métodos y aplicaciones para ejecutar dicho reconocimiento; como lo dice su nombre el evento es una fiesta de entusiastas por la seguridad informática pero en dichos eventos sólo se realiza el reconocimiento y teniendo en cuenta el impacto y la poca disponibilidad de información con respecto a la técnica y el alcance que podría tener un ciberdelincuente con dicha información se ha encontrado la motivación a realizar un análisis más profundo y detallado de esta técnica pero desde Bogotá, en donde no sólo se obtenga una estadística sino que con más detalle se logre realmente dimensionar todas las posibles consecuencias y pérdidas que se podrían tener al no tener presente un elemento tan cotidiano como la conexión inalámbrica a internet y la seguridad de su conexión.

El WarDriving es una técnica de la cual no se tiene información sobre un origen en específico, pero uno de los términos de los cuales se cree su origen es por una película lanzada en 1983 llamada “WarGames” en donde un joven pensando que estaba en un

video juego se logró infiltrar en un sistema gubernamental y evito una guerra mundial; también se cree que se originó de otra técnica llamada WarDialing muy practicada entre los años 80’s y 90’s, en donde se hacían llamadas aleatorias y de forma automática hasta encontrar módems conectados en donde se pudiera acceder a las conexiones con otros computadores.

Aunque la práctica no es tan popular en muchas partes del mundo, hay quienes la practican para hacer como en esta investigación, recopilación de datos para sensibilizar a los usuarios u otros que la usan para apoyar a ciberdelincuentes, en donde cuentan con una serie de símbolos y dibujos que les permiten comunicar entre si las características de la red para que otras personas que lo vean también puedan conocer que está pasando sin necesidad de volver hacer el reconocimiento.

Se espera dar claridad por medio de cifras sobre el estado general de Bogotá sobre los protocolos de seguridad usados en sus redes inalámbricos, para dar un temprano aviso sobre el estado, los riesgos y las recomendaciones que les permitan evitar incidentes de seguridad más graves.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo disminuir los incidentes de seguridad informática derivados del uso de protocolos de redes inalámbricas inseguros en los dispositivos de conexión WiFi en la ciudad de Bogotá?

2 JUSTIFICACIÓN

El Internet ha acercado cada vez a la humanidad a herramientas más avanzadas que permiten la interconexión con personas de todas partes del mundo; esto trae una infinidad de ventajas, pero sin el conocimiento ni la tecnología adecuada podría tener como consecuencia un incidente de seguridad critico desde un ataque con malware como Ransomware o una Botnet, hasta ataques más elaborados como una APT en un entorno corporativo.

Es por ello por lo que no solo se debe prestar atención a contraseñas seguras o mantener actualizado el Sistema Operativo sino también es importante cuidar de los dispositivos que se usan para lograr la conexión a internet.

El desarrollo de este proyecto de investigación permitirá conocer el estado de seguridad de los dispositivos de conexión inalámbrica dentro de la ciudad de Bogotá, las ventajas o desventajas consecuentes al uso de los diferentes protocolos, los riesgos a los que se exponen con el uso de protocolos de seguridad deficientes u obsoletos; así como, las recomendaciones que le permitirán a las organizaciones mejorar su defensa ante cualquier tipo de ataque. También permitirá que los expertos en seguridad tomen conciencia sobre los riesgos de usar dispositivos con tecnología obsoleta y sepan como remediarlo de forma temprana.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar el estado de seguridad de las redes inalámbricas con base en los protocolos de seguridad usados en distintas zonas geográficas de la ciudad de la Bogotá usando escenarios controlados que permitan exponer con el uso de exploits las diferentes vulnerabilidades a las cuales pueden estar expuestos los usuarios.

3.2 OBJETIVOS ESPECÍFICOS

- Recopilar la información relacionada a las redes inalámbrica disponibles en distintas zonas geográficas de Bogotá y de los protocolos de seguridad usados con la técnica del WarDriving
- Analizar y organizar los datos recopilados para identificar los protocolos de seguridad de las redes inalámbricas más utilizados y las vulnerabilidades derivadas a los protocolos
- Identificar mediante el uso de escenarios controlados las vulnerabilidades de los distintos protocolos realizando explotación de estos y explicando las posibles amenazas al usar los protocolos inseguros u obsoletos en las redes
- Recomendar distintas opciones que permitan mitigar los riesgos de las redes vulnerables. Con el fin de que personas expertas y no expertas cuenten con la información necesaria para evitar explotaciones a raíz del uso de protocolos inseguros en redes inalámbricas

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Con base a la temática de estudio y a los antecedentes evidenciados con respecto el problema generado por usar redes inalámbricas de conexión a internet obsoletas o con protocolos inseguros; mientras que desde 1969 se da por fecha de inicio a la creación de los primeros pinos de lo que conocemos hoy como internet y que en su inicio fue nombrado ARPAnet[1], seguidos de toda la evolución desde ser una red únicamente con fines militares a volverse finalmente una tecnología al alcance de millones de usuarios

[1] *(IONOS. ARPANET: Los primeros pasos de Internet.)*

para hacer búsquedas en línea y ejecutar tareas de diferentes tipos. En 1997 se lanzó públicamente lo que se conoce hoy como wifi al mundo y según la memoria colectiva no es sino hasta aproximadamente el año 2005 o 2006 en que las redes inalámbricas de conexión a internet llegan a Colombia; simplemente con esa observación podemos darnos cuenta de que en materia de tecnologías, dispositivos y seguridad informática nuestro país no ha sido pionero y ha tardado en ponerse a la vanguardia en estos asuntos. Es por ello por lo que no es sorprendente darse cuenta de que en diferentes sectores de la ciudad capital puedan encontrarse dispositivos de conexión inalámbrica obsoletos o con protocolos inseguros; cuando aún existen zonas apartadas de la ciudad en donde no llega la conexión o el servicio es paupérrimo.

Según la Asociación Colombiana de Ingenieros de Sistemas: "*durante la pandemia, (marzo- noviembre 2019) donde se registró un incremento superior al 98% en ciberataques, con más de 32 mil reportes de noticias criminales presentadas ante la Fiscalía General de la Nación*"[2]; con ello podemos ver que es muy importante que expertos en seguridad informática analicen minuciosamente las causas por los cuales pueden estarse efectuando dichos ciberataques. A pesar de que existen técnicas muy avanzadas para la ejecución de malware y ciberataques, en muchos casos se tiende a olvidar los puntos claves y se dan por obvias tareas tan sencillas como solicitar a un ISP la actualización de su hardware. Es muy importante recordar que no sólo basta con una seguridad perimetral o por capas en las compañías, sino que sin la concientización del usuario final que se conecta desde su casa a raíz de la pandemia, se está generando una brecha de seguridad muy extensa dando por hecho que el usuario tiene sus tecnologías y dispositivos actualizados cuando no se le ha dado la capacitación y advertencia sobre el uso de estos.

Aunque el WarDriving no esté catalogado como un ataque un delito ya que su funcionalidad en sí misma es recolección de datos en forma pasiva, sí existen

[2] *(ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS. Cifras de ciberseguridad en Colombia prenden alarmas al cierre del 2020.)*

procedimientos y normas que protegen a los usuarios de los posibles ataques a los que pueden exponerse al tener y usar conexiones inalámbricas inseguras u obsoletas. En Colombia se cuenta con la ley 1273 de 2009[3], que cuenta básicamente las generalidades y penalizaciones al cometer delitos informáticos; allí podríamos ver las posibles consecuencias legales y penales que debería asumir un ciber delincuente al aprovechar la información recolectada para ejecutar uno o varios ataques que le permitan obtener información privilegiada, sensible o no autorizada sobre la red afectada y toda la información que viaja en ella.

4.2 MARCO CONCEPTUAL

Aquí se encuentra una descripción de los conceptos relacionados a la temática de estudio que rodea al WarDriving y a los posibles ataques que se pueden dar tras el aprovechamiento ilegitimo de los datos recopilados:

- **Troyano:** Un troyano es un tipo de código o software malicioso que parece legítimo pero que puede tomar el control de su ordenador. Un troyano está diseñado para dañar, interrumpir, robar o, en general generar alguna otra acción dañina en los datos o en la red.

- **Rootkits:** Los rootkits son un tipo de malware que está diseñado para permanecer oculto en su ordenador. Los rootkits dan a los ciberdelincuentes la capacidad de controlar remotamente su ordenador.
- **C&C:** Un servidor de comando y control es un ordenador controlado por un atacante o ciberdelincuente que se utiliza para enviar comandos a sistemas comprometidos por el malware y recibir datos robados de una red objetivo.
- **Gusano**: Un virus gusano es un programa malicioso que se autorreplica y que puede propagarse por una red sin ayuda humana.
- **Phishing:** La suplantación de identidad es un método para tratar de obtener

[3] (*CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009.*, 2009)

información personal mediante correos electrónicos y sitios web engañosos.

- **Ransomware:** El ransomware es una forma de malware que cifra los archivos de la víctima. El atacante pide un rescate a la víctima para restaurar el acceso a los datos previo pago.
- **WEP:** es un algoritmo de seguridad introducido para proporcionar confidencialidad a los datos de las redes inalámbricas. La Privacidad Equivalente al Cable se introdujo como parte del estándar 802.11.[4] Uno de los rasgos más característicos es su clave de 10 o 26 dígitos hexadecimales, es decir, 40 o 104 bits. La red inalámbrica, por definición, transmite datos en toda un área dentro de su alcance a través de ondas de radio. Por ello, los datos transmitidos por una WLAN pueden ser fácilmente interceptados. En otras palabras, otros usuarios pueden "oír" las conversaciones privadas, adquirir archivos confidenciales y demás que se transmiten a través de una red inalámbrica. WEP pretendía añadir una capa de seguridad a la red inalámbrica ofreciendo una fuerte encriptación a los datos. De este modo, los datos serán irreconocibles para todo el mundo excepto para el receptor previsto.
- **WPA:** es un protocolo de seguridad diseñado para crear redes inalámbricas seguras. Es similar al protocolo WEP, pero ofrece mejoras en el manejo de las claves de seguridad y en la forma de autorizar a los usuarios. Para que una transferencia de datos encriptada funcione, los dos sistemas al principio y al final de una transferencia de datos deben utilizar la misma clave de cifrado o descifrado. Mientras que WEP proporciona a cada sistema autorizado la misma clave, WPA utiliza el protocolo de integridad de clave temporal (TKIP), que cambia dinámicamente la clave que utilizan los sistemas. Esto evita que los intrusos creen su propia clave de cifrado para que coincida con la que utiliza la red segura. WPA también implementa algo llamado Protocolo de Autenticación Extensible (EAP) para autorizar a los usuarios. En lugar de autorizar los ordenadores basándose únicamente en su dirección MAC, WPA puede utilizar otros métodos para verificar la identidad de cada ordenador. Esto hace

[4] Este fue el estándar original creado en 1997 para las redes inalámbricas. Sólo ofrecía una velocidad de transmisión de datos de 2 Mbps en la frecuencia de 2,4 Ghz, que era demasiado lenta para la mayoría de las aplicaciones.

más difícil que los sistemas no autorizados puedan acceder a la red inalámbrica.

- **WPA2:** Abreviatura de WiFi Protected Access 2, WPA2 es el método de seguridad añadido a WPA para las redes inalámbricas que proporciona una mayor protección de los datos y control de acceso a la red. Proporciona a los usuarios de Wi-Fi de empresas y consumidores un alto nivel de garantía de que sólo los usuarios autorizados pueden acceder a sus redes inalámbricas. Basado en el estándar IEEE 802.11i, WPA2 proporciona seguridad de nivel gubernamental al implementar el algoritmo de cifrado AES, que cumple con la norma FIPS 140-2 del Instituto Nacional de Normas y Tecnología (NIST), y la autenticación basada en 802.1x. Hay dos versiones de WPA2: WPA2-Personal y WPA2-Enterprise. WPA2-Personal protege el acceso no autorizado a la red utilizando una contraseña de configuración. WPA2-Enterprise verifica los usuarios de la red a través de un servidor. WPA2 es compatible con WPA.
- **WPA3:** fue lanzado en junio de 2018, es el sucesor de WPA2, que los expertos en seguridad describen como "roto". El objetivo de desarrollar WPA3 era mejorar WPA en términos de simplicidad de uso y mayor fuerza criptográfica. Al igual que su predecesor, se presenta en ediciones Personal y Enterprise, pero esta versión mejora a WPA2 con funciones de autenticación y cifrado más robustas, y una solución al fallo incorporado en WPA2, KRACK. También incluye funcionalidades para simplificar, y asegurar mejor, la conexión de dispositivos wifi IoT.

4.3 MARCO HISTÓRICO

Respecto a la problemática de estudio existen antecedentes de investigaciones realizadas en Colombia con respecto al uso de metodologías de recopilación de redes inalámbricas como la usada en este proyecto: “Wardriving”; sin embargo, su fecha de publicación excede el periodo de 5 años por lo cual no es pertinente su citación en esta investigación. Teniendo en cuenta otros aspectos como los protocolos de seguridad inalámbrica como el WEP, WPA, WPA2 o WPA3, al igual que en el punto anterior no existen puntos de referencia de origen local que puedan ser usadas bajo el mismo contexto por lo cual no se citaran en esta investigación.

Si se tiene en cuenta investigaciones de carácter internacional donde se puedan obtener puntos de referencias sobre las preocupaciones de la industria mundial en torno a la seguridad de redes inalámbricas y sus protocolos, podemos acercar nuestra vista hacia la investigación *"Exploring Wardriving Potential in the Ecuadorian Amazon for Indirect Data Collection"*[5], en donde al igual que esta investigación, se le brinda protagonismo y se le entrega importancia al Wardriving como un proceso de recolección de datos fiable y de gran aporte para registrar datos de las redes inalámbricas; aunque en esa investigación el enfoque no es tecnológico sino mayormente demográfico y social; el instrumento de recolección de datos es el mismo, lo que nos permite ratificar que día a día esta metodología sigue tomando protagonismo por su efectividad y no compromete los sistemas, sino que toma información que esta expuesta sin necesidad de explotarla para poder tener estadísticas e información en tiempo real sobre las redes a explorar.

4.4 ANTECEDENTES O ESTADO ACTUAL

Aunque en la actualidad en Bogotá contamos con múltiples iniciativas y grandes multinacionales que promueven el desarrollo de la ciudad en muchos aspectos aún contamos con muchas brechas de conectividad; según boletín trimestral más reciente, del segundo trimestre de 2021 de TI y las comunicaciones: *"…al segundo trimestre de 2021, Colombia superó los 8,2 millones de accesos fijos a internet. Esto representa que en promedio al día 1.700 accesos fijos a internet durante el segundo trimestre del año. En 2020, el país contaba con 7,8 millones de accesos, mientras que para el 2019 había siete millones de acceso. El crecimiento de los accesos a internet estuvo soportado principalmente por el segmento residencial, en donde al segundo trimestre hubo 7,63 millones de acceso, y en el segmento corporativo hubo 0,59 millones."*[6]

Esto nos da una perspectiva general de las dificultades y retrasos que para la época aún tenemos, con escases de acceso a elementos y herramientas que algunos ya

[5] (*SANTOS, Fabián, PESANTES, Pablo y BONILLA-BEDOYA, Santiago. Exploring Wardriving Potential in the Ecuadorian Amazon for Indirect Data Collection, 2021)*
[6] (*DIARIO LA REPUBLICA. PASTRAN, Alejandro, Colombia superó los 8,2 millones de accesos fijos a internet en segundo trimestre, 2021, noviembre 12*.)

consideramos esenciales y cotidianos como el internet. La brecha no es únicamente de acceso sino de manutención y garantías para obtener siempre los mejores servicios y posibilidades dentro de las tecnologías disponibles; en un país que desde la pandemia su gran mayoría se ha trasladado a una metodología de teletrabajo y que según datos del Ministerio del trabajo ha tenido un crecimiento de más del 80% en todo el país, es vital que no sólo dentro de las organizaciones encuentren con las mejores prestaciones, sino que se creen políticas que promuevan que el de los hogares sean iguales.

4.5 MARCO LEGAL

Desde que expertos informáticos iniciaron su carrera de exploración al mundo del hacking se han venido incorporando leyes que soporten a la legislación colombiana en los casos donde se compruebe que el acceso es ilegal y no autorizado. En Colombia la normativa que se encarga de regular estas acciones se llama Ley 1273 de 2009[7] y que trata de los tipos penales relacionados a elites informáticos y la protección de la información y de datos; en donde se puede encontrar las diferentes penalizaciones a los posibles ataques informáticos que pueda ocasionar un aprovechamiento indebido de una recolección de datos como la que se ocasiona en el WarDriving, a continuación, se encontrarán algunas de las más relevantes para el caso mencionado:

Artículo 269B: en donde se penaliza la **Obstaculización ilegítima de sistema informático o red de telecomunicación** e indica que quien, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

[7] (*Ley 1273 de 2009* | Congreso de la república, 2009)

Artículo 269C: en donde se penaliza la **Interceptación de datos informáticos** e indica que quien, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269E: en donde se penaliza el **Uso de software malicioso** e indica que quien, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: en donde se penaliza la **Violación de datos personales** e indica que quien sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269H: Allí se explican las **Circunstancias de agravación punitiva**, en donde las penas imponibles de acuerdo con los artículos descritos en este título se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1) Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2) Por servidor público en ejercicio de sus funciones.
3) Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4) Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5) Obteniendo provecho para sí o para un tercero.
6) Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7) Utilizando como instrumento a un tercero de buena fe.
8) Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Artículo 269I: en donde se penaliza el **Hurto por medios informáticos y semejantes** e indica que quien, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

4.6 DISEÑO METODOLOGICO

Se hará uso de señales Wi-Fi recopiladas aleatoriamente por la ciudad de Bogotá como población objetivo; en donde, se aplicará la técnica de escaneo de redes llamada WarDriving.

La técnica Wardriving recopila la data de las redes inalámbricas mediante el uso de distintos dispositivos de escaneo para lograr la mayor cantidad de recolección de información, estos dispositivos pueden ser: antenas WiFi, computadores, dispositivos móviles como tabletas y smartphones, que usarán el software Wigle o Kismet para interpretar y almacenar dichas señales WiFi para su posterior análisis y uso dentro de la investigación en curso.

En la tabla 1, presentada a continuación, se describe el detalle del diseño metodológico que ha sido usado y aplicado al desarrollo de este proyecto.

Tabla 1 Diseño metodológico

Diseño	
Tipo de investigación	• Investigación aplicada tecnológica • Investigación descriptiva
Procedimientos	Para la investigación se empleará el diseño investigativo basado en la recopilación, análisis y presentación de datos que permita entender la problemática explicada y la descripción cuantitativa de esta.
Población y muestra	
Población	Redes inalámbricas al alcance de las antenas y dispositivos dispuestos para el escaneo en algunas zonas de frecuente tráfico de Bogotá.
Muestra	Redes inalámbricas WiFi que se puedan identificar y analizar, para entender la seguridad de los protocolos de las redes en Bogotá.

Fuente: Elaboración propia

5 DESARROLLO DE LOS OBJETIVOS

5.1 RECOPILAR INFORMACIÓN RELACIONADA A LAS REDES INALÁMBRICAS DISPONIBLES EN DISTINTAS ZONAS GEOGRÁFICAS DE BOGOTÁ Y DE LOS PROTOCOLOS DE SEGURIDAD RECOPILADOS CON LA TÉCNICA DEL WARDRIVING

Para iniciar con la recopilación de los datos de las redes inalámbricas es necesario tener claro los elementos que se deben usar para ejecutar cualquier tarea relacionada con WarDriving, por lo que a continuación se encontrará una explicación de cada uno de ellos:

- **Vehículo:** es natural pensar que la técnica del WarDriving contempla únicamente un vehículo particular como opción para desplazarse por diferentes espacios geográficos dentro de la ciudad; sin embargo, con la evolución de la técnica y la disposición de instrumentos cada vez más pequeños para realizar el análisis es posible contemplar otros tipos de vehículos para trasladarse. En algunos casos se encuentran buses camuflados con temáticas en donde se desplazan grupos de estudiantes o personas que están aprendiendo sobre el tema para hacerlo más dinámico, en otros se puede realizar en motos, en bicicletas y realmente en cualquier tipo de transporte de preferencia siempre cuando pueda llevar consigo los instrumentos para realizar el análisis.
- **Equipos de escaneo:** en este caso es importante contar con las herramientas que permitan detectar las diferentes redes inalámbricas que se encuentren en el entorno. La forma más usual de hacerlo es con antenas wifi que permitan obtener un mayor alcance de resultados por la potencia que manejan sus antenas, otra forma es mediante el uso de dispositivos móviles; por ejemplo, los smartphone ya cuentan con sus propias antenas y que se pueden comprobar cuando se está buscando redes wifi para conectarse a un hotspot (Un hotspot es un lugar físico donde la gente puede acceder a Internet, normalmente mediante Wi-Fi, a través de una red de área local inalámbrica con un router conectado a un proveedor de servicios de Internet) y aparece un listado de redes disponibles, en definitiva el alcance de recepción es mucho menor al de una antena wifi pero también es útil y es un buen inicio para quien no cuenta con más recursos.
- **Software**: en los casos donde se usan antenas wifi es necesario tener el software que logre interpretar la información que reciben las antenas para ello hay varias opciones gratuitas en el mercado y Open Source para distintos sistemas operativos para estas tareas; por ejemplo, Kali Linux o Windows.
- **Espacio Geográfico:** para este punto es importante fijar los alcances y cuál es el objetivo del reconocimiento de las redes inalámbricas de esta forma podrán obtener objetivos más claros y no gastar tiempo en toma de datos que no sean

necesarias en este caso el espacio geográfico serán zonas aleatorias de la ciudad de Bogotá.

En la siguiente sección se podrán encontrar los equipos de escaneo como antenas, dispositivos y el software usado durante el desarrollo de esta actividad. En la figura 1 se puede encontrar una de las antenas inalámbricas usadas para la recopilación de los datos

Figura 1 Antena WiFi Alfa

Fuente: Elaboración propia

En la figura 2 se puede encontrar una antena que a diferencia de la anterior tiene menor alcance, pero es igualmente útil para el proceso de recopilación de datos bajo la metodología de Wardriving.

Figura 2 Antena WiFi TP-Link

Fuente: Elaboración propia

Por otro lado, en la **Figura 3** se hace referencia a una antena GPS de carácter USB que también permite junto con el software tener una referencia de geo locación precisa con los datos específicos sobre la ubicación de las redes inalámbricas generando los datos de la ubicación. Luego de ello en la **Figura 4** se puede mostrar como con la ayuda del sistema de entretenimiento de un carro particular, en este caso un Renault Sandero modelo 2022; allí se puede evidenciar que en general cualquier dispositivo inteligente sin importar cual sea su propósito final; puede ser útil para el aprovechamiento de una actividad de carácter de recolección de información de redes inalámbricas por lo cual puede incentivar a personas que quieran empezar a entender un pequeño segmento de la seguridad informática cómo funcionan estas técnicas y la dimensión del alcance en el aprovechamiento de los datos que puede tener un ciberdelincuente.

Figura 3 BU-353S4 GPS USB

Fuente: Elaboración propia

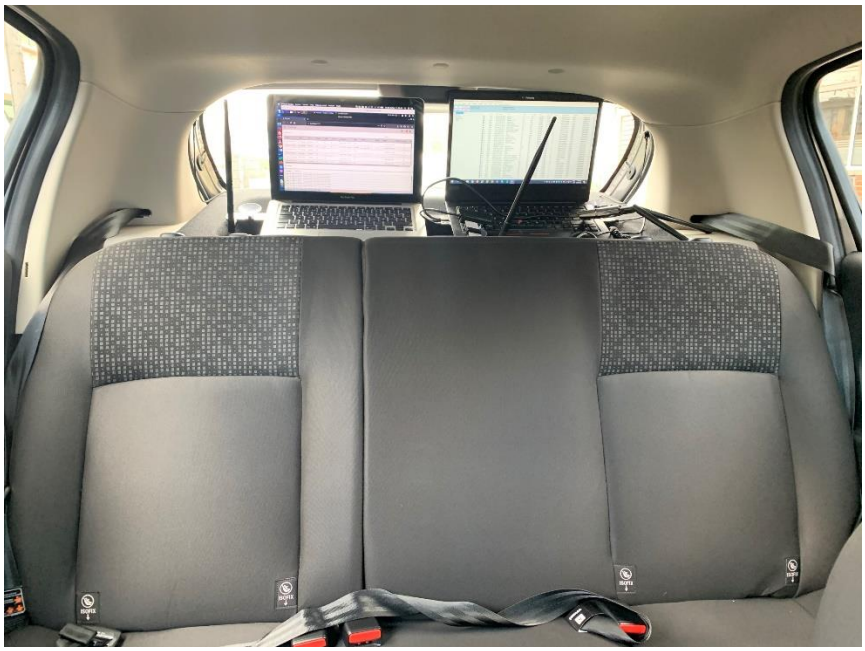
Figura 4 Renault Media NAV

Fuente: Elaboración propia

Aunque ir en automóvil particular no es la única opción disponible para hacer Wardriving en la **Figura 5** se muestra de forma grafica que no solo se limita a un teléfono celular y antenas, sino que también se pueden ubicar computadores portátiles con diferentes

antenas para obtener mas alcance y recopilar la mayor cantidad de datos posibles durante los recorridos realizados

Figura 5 Acomodación de antenas y computadores en carro



Fuente: Elaboración propia

Tras el reconocimiento de los dispositivos dispuestos para la actividad, a continuación en la **Tabla 2**, se presenta el listado completo de software y hardware que se usaron para el proceso de reconocimiento de todas las redes; así como, en el desarrollo de objetivos posteriores a esta fase; sin embargo, es importante resaltar que un ejercicio de WarDriving no se limita únicamente al uso de los recursos recomendados; sino que es a decisión, libre decisión y disponibilidad de recursos del tester, que se definen cuales puede o no usar en caso de que se desee replicar la actividad.

Tabla 2 Listado de hardware y software usado para la ejecución de pruebas

HARDWARE	SOFTWARE
MacBook Pro-13	Google Maps

Lenovo Thinkpad E480	Google Earth
Motorola Moto E4 Plus	Wigle Wifi
Alfa Wireless AWUSO36ACH	Kali Linux
TP Link USB Wireless Adapter TL-WN722N	Kismet
GlobalSat BU-353S4 GPS USB	Vistumbler
TP Link USB Wirelles Wirelles N Router TL-WR84	Wifite
Renault Media NAV Android	Aircrack-ng

Fuente: Elaboración propia

Para el ejercicio de esa actividad se utilizaron diferentes computadores portátiles con las antenas Wi-Fi expuestas anteriormente; en este caso el análisis de realizó con herramientas como Vistumbler que está especializado para sistemas operativos Windows o Kismet que está enfocado a la distribución Kali Linux. También se hizo uso de los recursos dispuestos por el vehículo, en este caso un Renault Sandero, en donde mediante el uso del centro entretenimiento del vehículo, llamado Renault Media NAV, que contiene un sistema operativo Android que también se puede utilizar para descargar aplicaciones y tomar ventaja de la antena del vehículo; es por ello que se procedió con la instalación de la aplicación Wigle WiFi la cual realiza el proceso de recopilación de información usando este tipo de dispositivos.

El proceso de recopilación de los datos se realizó durante varias semanas en donde activando el hardware y software expuesto anteriormente se realizaron desplazamientos en varias de las vías principales de la ciudad, tomando provecho de actividades cotidianas como el desplazamiento de la casa al trabajo o del trabajo a la universidad para capturar la mayor cantidad de datos posible. Con lo cual al finalizar con la recolección pasiva de dicha información; por ejemplo, la aplicación móvil Wigle permite la descarga de un archivo separado por comas “.csv” que puede usarse más adelante para analizar los datos encontrades durante el proceso de recopilación de redes.

5.2 ANALIZAR Y ORGANIZAR LOS DATOS RECOPILADOS PARA IDENTIFICAR LOS PROTOCOLOS DE SEGURIDAD DE LAS REDES INALÁMBRICAS MÁS UTILIZADOS Y LAS VULNERABILIDADES DERIVADAS A LOS PROTOCOLOS

5.2.1 Análisis y organización de los datos recopilados para la identificación de los protocolos de seguridad de redes inalámbricas de Bogotá

Tras la ejecución del escaneo realizado en el objetivo anterior, se procede con la descarga del archivo .csv generado por las herramientas de recolección de datos de redes inalámbricas y se procede a cargarlo a Excel. Donde el objetivo es organizar la información recopilada y de esta forma proceder el filtrado y categorización para identificar los protocolos de seguridad de redes inalámbricas que hayan sido detectados y continuar con su análisis.

Hay que recordar que las redes inalámbricas no hacen referencia de forma implícita a únicamente conexiones a internet; ya que existen muchos tipos de señales emitidas por otros servicios y que no tienen nada que ver con la conectividad de internet. Entre ellas tenemos las señales emitidas por Bluetooth, en donde encontramos una extensa categoría de dispositivos donde tenemos audífonos, altavoces, relojes inteligentes, entre otros wereables. Además, nos podemos encontrar con señales Bluetooth propias de otros vehículos y señales dispositivos móviles como smartphones abiertos al público; así como también, señales de dispositivos de CCTV, como cámaras de seguridad inalámbricas entre otros servicios que, aunque son menos comunes también pueden emitir información por medio de señales inalámbricas.

Al revisar los datos obtenidos nos encontramos con 968.340 señales de conexiones inalámbricas de todo tipo, detectadas durante el proceso de recopilación de datos. Todas con diferentes características, protocolos, fabricantes, modelos y procesos de autentificación. Tras ello se procede a cargar el archivo por comas obtenido en el análisis, pero como se evidencia en la **Figura 6**, al cargarlo en Google Earth para verificar las

rutas y el mapa de calor de las señales inalámbricas encontradas, nos encontramos que la aplicación no logra cargar correctamente por la gran cantidad de datos almacenados y el peso del archivo generado; así que solo se logra obtener una visual genérica de la masividad de redes inalámbricas, como se visualiza a continuación.

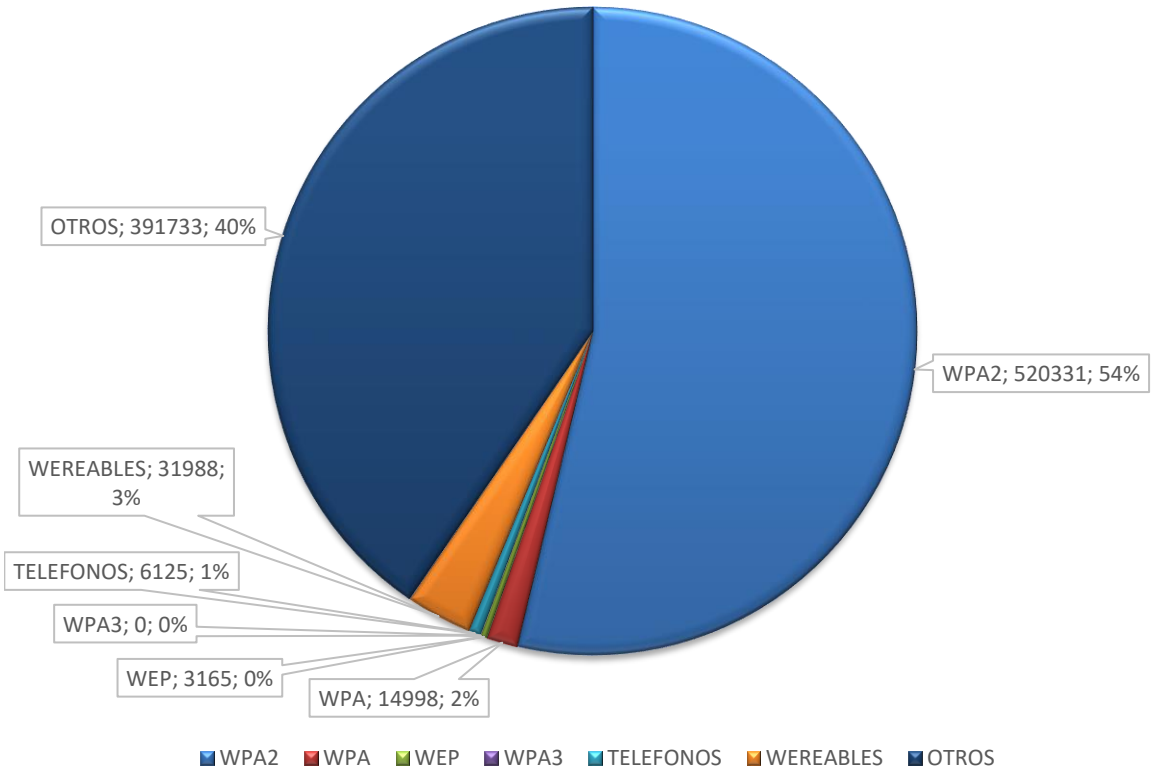
Figura 6 Bloqueo de Google Earth al cargar el archivo .csv

Fuente: Elaboración propia

Al encontrarse con dicha información se logra visualizar que no es entendible y es difícil de diferencial los datos; así que, para iniciar con el análisis de la información recopilada, se procede con la creación de gráficos cargando el archivo .csv a Microsoft Excel e iniciando con el filtrado y creación de graficas personalizadas; para entender de una forma más simple los datos que se han almacenado y los tipos de señales inalámbricos encontrados en la recolección. Al igual que con la carga de información a Google Earth, en el caso de la creación de la tabla relacionando los datos obtenidos mediante el proceso de recolección, la información es muy extensa y poco entendible para facilitarla en una sola tabla; ya que la cantidad de datos es bastante muy extensa y la lectura de las

etiquetas se hace difícil, se procede con una separación manual de los protocolos y dispositivos hallados durante la recolección para que sea mucho más claro al público tal y como se expresa en la **Figura 7.**

Figura 7 Resumen de las categorías de redes inalámbricas detectadas en Bogotá mediante reconocimiento pasivo

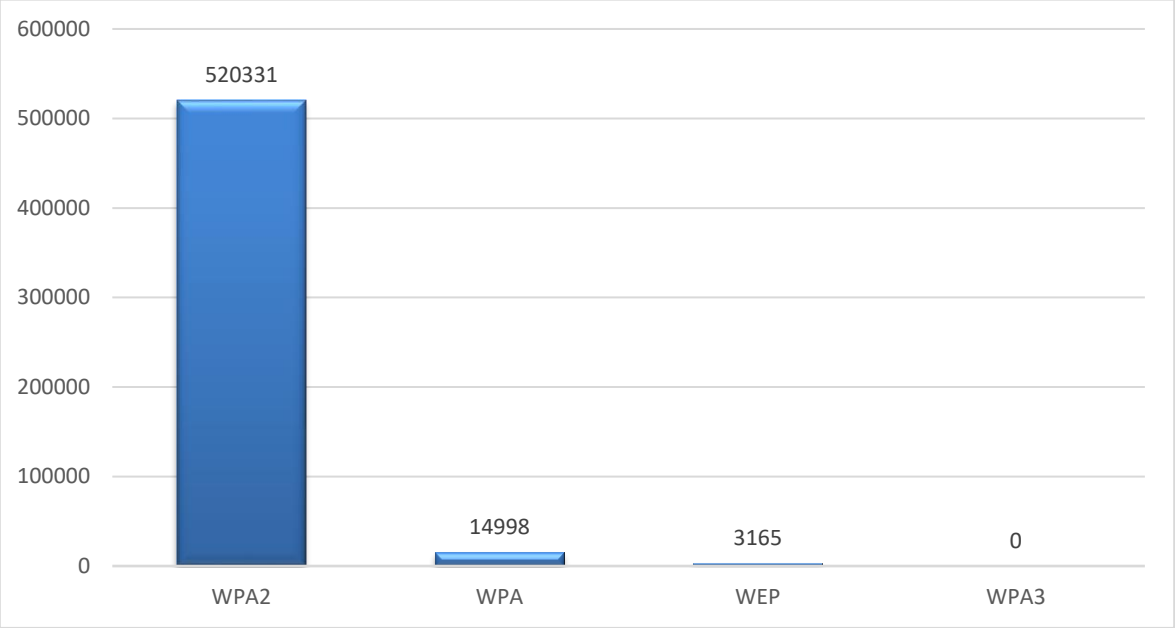


Fuente: Elaboración Propia

Tras la revisión de dicho resumen, se puede obtener una perspectiva más clara sobre los tipos de redes inalámbricas disponibles en la ciudad, pero retomando el objeto de estudio de esta propuesta investigativa, que en este caso corresponde únicamente a los protocolos de seguridad de las redes inalámbricas que nos conectan a internet.

A continuación, se sigue avanzando con el proceso de filtrado para ahondar de forma específica en los datos precisos que nos puedan aportar al desarrollo de la investigación. Es por ello por lo que se separan todas las otras redes inalámbricas encontradas, protocolos y dispositivos diferentes a los que corresponden al objeto de estudio y únicamente se relacionan los protocolos usados por las redes wifi que son WEP, WPA, WPA2 y WPA3, como se puede visualizar en la **figura 8.**

Figura 8 Protocolos de conexión inalámbrica a Internet detectados en Bogotá



Fuente: Elaboración propia

Al final de este análisis se puede concluir que:

- De las 968.340 redes inalámbricas detectadas durante el proceso de recolección de datos solo 538.494 redes corresponden a redes de conexión a internet.
- En donde, al menos 14.998 redes cuentan con protocolos de autenticación vulnerables como WPA.

- 3165 son conexiones a internet con protocolo WEP implementado, que aparte de ser obsoleto, es el protocolo más fácil de vulnerar.
- Sin contar con las vulnerabilidades de WPA2 en sus primeras versiones, en donde nos encontramos con 520.331 redes inalámbricas.

5.2.2 Análisis de las vulnerabilidades derivadas a los protocolos de conexión a Internet Inalámbricos

Al contar con los protocolos de seguridad inalámbricos detectados, se continuará con la profundización de los detalles con respecto a las vulnerabilidades, debilidades, o posibles ataques para cada uno de los protocolos descritos en la **Figura 8.**

5.2.2.1 Protocolo WEP (Wired Equivalent Privacy)

WEP utiliza el algoritmo de cifrado RC4, conocido como cifrado de flujo. Un cifrado de flujo funciona expandiendo una clave corta en un flujo de claves pseudoaleatorio infinito. El remitente cruza el flujo de claves con el texto plano para obtener el texto cifrado. El receptor tiene una copia de la misma clave y la utiliza para generar un flujo de claves idéntico. Al XOR del flujo de claves con el texto cifrado se obtiene el texto plano original.

Este modo de funcionamiento hace que los algoritmos de flujo sean vulnerables a varios ataques. Si un atacante invierte un bit en el texto cifrado, al descifrarlo se invierte el bit correspondiente en el texto plano. Además, si ciber delincuente intercepta dos textos cifrados con el mismo flujo de claves, es posible obtener el XOR de los dos textos planos. El conocimiento de este puede permitir ataques estadísticos para recuperar los textos planos. Los ataques estadísticos son cada vez más prácticos a medida que se conocen más textos cifrados que utilizan el mismo flujo de claves. Una vez que se conoce uno de los textos planos, es sencillo recuperar todos los demás.

WEP tiene defensas contra estos dos ataques. Para garantizar que un paquete no ha sido modificado en tránsito, utiliza un campo de comprobación de integridad en el

paquete. Para evitar cifrar dos textos cifrados con el mismo flujo de claves, se utiliza un vector de inicialización para aumentar la clave secreta compartida y producir una clave RC4 diferente para cada paquete.

Debilidades: El principal problema de WEP es que sólo utiliza una clave estática cuando se envían datos desde el computador. Lo cual no significaba mucho cuando recién se publicó el protocolo; sin embargo, con el paso del tiempo, los ciberdelincuentes descifraron el código detrás de las claves. Así, una vez que un cracker conoce la clave de la comunicación WiFi, puede romper el cifrado y leer los datos enviados. Ahora se pueden descargar herramientas que lo hacen automáticamente. Se configura el objetivo con el programa hacia una red con WEP habilitado y se deja activo supervisando las tramas de la red hasta encontrar el patrón y descifrar la contraseña por sí mismo. Por lo tanto, utilizar una conexión basada en WEP en estos tiempos es muy peligroso.

Una de las aplicaciones más populares para realizar este proceso es AIRCRACK-NG, esta es una suite para que la contraseña de redes inalámbricas y tienen un especial éxito con el protocolo WEP, dado que hace un análisis matemático estadístico en el cual calcula los patrones y logra descubrir la contraseña de la red inalámbrica.

5.2.2.2 Protocolo WPA “WiFi Protected Access” y WPA2

Ofrece mejoras en el manejo de las claves de seguridad y en la forma de autorizar a los usuarios con respecto a WEP. Para que una transferencia de datos cifrada funcione, los dos sistemas deben utilizar la misma clave de cifrado o descifrado al principio y al final de una transferencia de datos. Mientras que WEP proporciona a cada sistema autorizado la misma clave, WPA usa el protocolo de integridad de clave temporal o TKIP, que cambia de forma dinámica la clave que usan los sistemas. Esto impide que los intrusos creen su propia clave de cifrado para que coincida con la utilizada por la red segura. El Protocolo de Integridad de Clave Temporal “TKIP”, tal y como se define en la especificación IEEE 802.11i, aborda la parte de cifrado de la premisa de seguridad inalámbrica y se diseñó

con una restricción muy difícil ya que tenía que funcionar con el hardware existente y, por lo tanto, no podía requerir un cifrado computacionalmente avanzado.

WPA también aplica algo conocido como Protocolo de Autenticación Extensible para autorizar a los usuarios. En lugar de autorizar los computadores basándose únicamente en su dirección MAC, WPA puede usar diversos mecanismos para verificar la identidad de cada computador.

Esto hace más difícil que los sistemas no autorizados puedan acceder a la red inalámbrica. En octubre 16 de 2017 se publicó un comunicado de ICASI[8] en el que se alertó a la comunidad sobre una serie de fallos de vulnerabilidad en WPA y WPA2. Esta situación significa que la red y los dispositivos inalámbricos no eran seguros y se requerían de una acción para corregir este fallo. El fallo, conocido como KRACK, afectaba WPA y WPA2, un protocolo de seguridad ampliamente utilizado en la mayoría de los dispositivos WiFi de la época.

Es necesario recordar que los protocolos han tenido diversas actualizaciones en las cuales se han mejorado las fallas encontradas hasta crear y sacar a producción un nuevo protocolo. Un intruso podía aprovechar KRACK para inyectar malware, como un ransomware en sitios web.

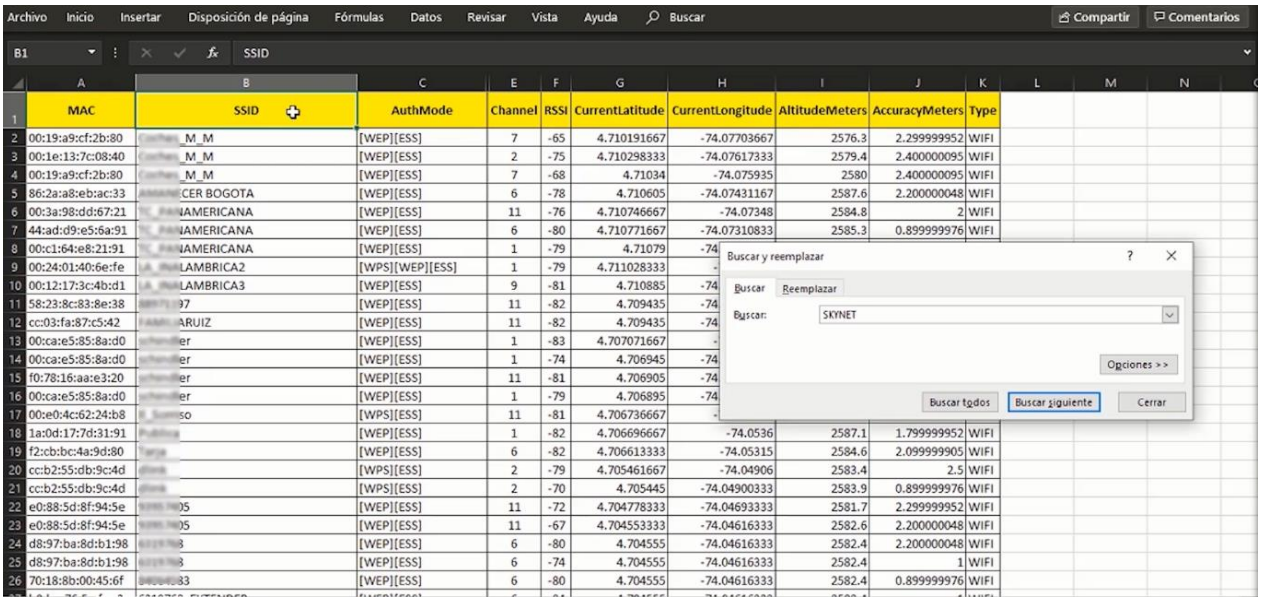
5.3. IDENTIFICAR MEDIANTE EL USO DE ESCENARIOS CONTROLADOS LAS VULNERABILIDADES DE LOS DISTINTOS PROTOCOLOS REALIZANDO EXPLOTACIÓN DE ESTOS Y EXPLICANDO LAS POSIBLES AMENAZAS AL USAR LOS PROTOCOLOS INSEGUROS U OBSOLETOS EN LAS REDES

5.3.1. PoC en entorno controlado para el protocolo WEP

[8] (Statement from the Industry Consortium for Advancement of Security on the Internet (ICASI) on the Wi-Fi Protected Access (WPA) Vulnerabilities | ICASI, 2017)

Para este ejercicio se procedió con la creación de un punto de acceso en un entorno controlado y que también fue escaneado durante la recolección de los datos presentados anteriormente. Por lo cual, en el archivo de Excel, se hace el filtrado de los SSID de las diferentes redes recopiladas hasta encontrar el SSID llamado “SkyNet” como se puede evidenciar en la **Figura 9.**

Figura 9 Búsqueda de la red inalámbrica controlada creada para la PoC



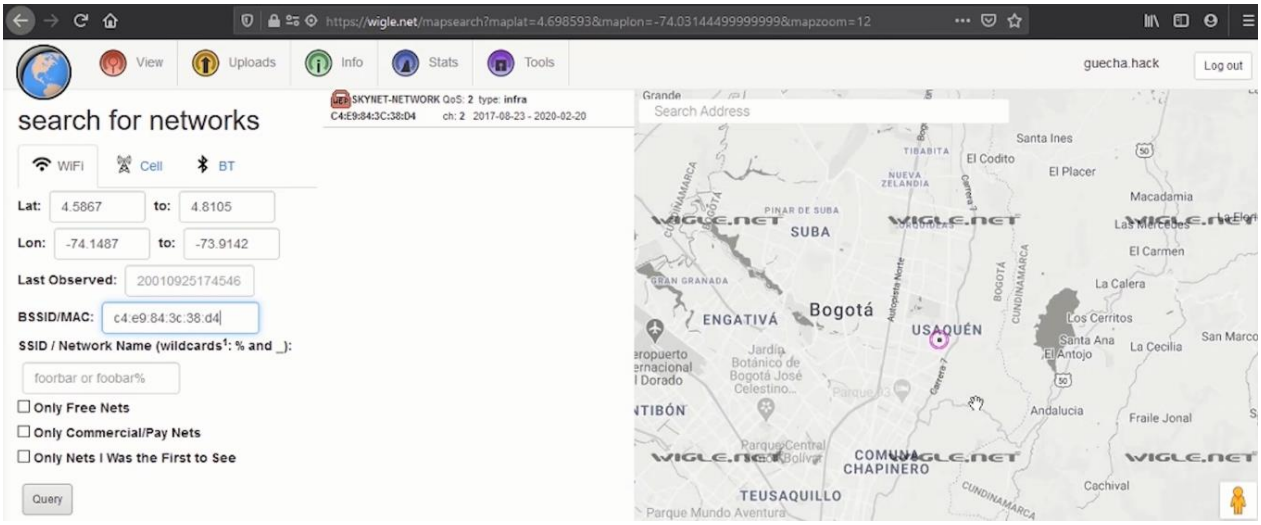
	A	B	C	E	F	G	H	I	J	K
1	MAC	SSID	AuthMode	Channel	RSSI	CurrentLatitude	CurrentLongitude	AltitudeMeters	AccuracyMeters	Type
2	00:19:a9:cf:2b:80	[illegible]_M_M	[WEP][ESS]	7	-65	4.710191667	-74.07703667	2576.3	2.299999952	WIFI
3	00:1e:13:7c:08:40	[illegible]_M_M	[WEP][ESS]	2	-75	4.710298333	-74.07617333	2579.4	2.400000095	WIFI
4	00:19:a9:cf:2b:80	[illegible]_M_M	[WEP][ESS]	7	-68	4.71034	-74.075935	2580	2.400000095	WIFI
5	86:2a:a8:eb:ac:33	[illegible]CER BOGOTA	[WEP][ESS]	6	-78	4.710605	-74.07431167	2587.6	2.200000048	WIFI
6	00:3a:98:dd:67:21	[illegible]AMERICANA	[WEP][ESS]	11	-76	4.710746667	-74.07348	2584.8	2	WIFI
7	44:ad:d9:e5:6a:91	[illegible]AMERICANA	[WEP][ESS]	6	-80	4.710771667	-74.07310833	2585.3	0.899999976	WIFI
8	00:c1:64:e8:21:91	[illegible]AMERICANA	[WEP][ESS]	1	-79	4.71079	-74			
9	00:24:01:40:6e:fe	[illegible]LAMBRICA2	[WPS][WEP][ESS]	1	-79	4.711028333	-			
10	00:12:17:3c:4b:d1	[illegible]LAMBRICA3	[WEP][ESS]	9	-81	4.710885	-74			
11	58:23:8c:83:8e:38	[illegible]97	[WEP][ESS]	11	-82	4.709435	-74			
12	cc:03:fa:87:c5:42	[illegible]ARUIZ	[WEP][ESS]	11	-82	4.709435	-74			
13	00:ca:e5:85:8a:d0	[illegible]er	[WEP][ESS]	1	-83	4.707071667	-			
14	00:ca:e5:85:8a:d0	[illegible]er	[WEP][ESS]	1	-74	4.706945	-74			
15	f0:78:16:aa:e3:20	[illegible]er	[WEP][ESS]	11	-81	4.706905	-74			
16	00:ca:e5:85:8a:d0	[illegible]er	[WEP][ESS]	1	-79	4.706895	-74			
17	00:e0:4c:62:24:b8	[illegible]so	[WPS][ESS]	11	-81	4.706736667	-			
18	1a:0d:17:7d:31:91	[illegible]	[WEP][ESS]	1	-82	4.706696667	-74.0536	2587.1	1.799999952	WIFI
19	f2:cb:bc:4a:9d:80	[illegible]	[WEP][ESS]	6	-82	4.706613333	-74.05315	2584.6	2.099999905	WIFI
20	cc:b2:55:db:9c:4d	[illegible]	[WPS][ESS]	2	-79	4.705461667	-74.04906	2583.4	2.5	WIFI
21	cc:b2:55:db:9c:4d	[illegible]	[WPS][ESS]	2	-70	4.705445	-74.04900333	2583.9	0.899999976	WIFI
22	e0:88:5d:8f:94:5e	[illegible]05	[WEP][ESS]	11	-72	4.704778333	-74.04693333	2581.7	2.299999952	WIFI
23	e0:88:5d:8f:94:5e	[illegible]05	[WEP][ESS]	11	-67	4.704553333	-74.04616333	2582.6	2.200000048	WIFI
24	d8:97:ba:8d:b1:98	[illegible]3	[WEP][ESS]	6	-80	4.704555	-74.04616333	2582.4	2.200000048	WIFI
25	d8:97:ba:8d:b1:98	[illegible]3	[WEP][ESS]	6	-74	4.704555	-74.04616333	2582.4	1	WIFI
26	70:18:8b:00:45:6f	[illegible]33	[WEP][ESS]	6	-80	4.704555	-74.04616333	2582.4	0.899999976	WIFI

Fuente: Elaboración propia

Tras realizar la búsqueda se pueden ver en los diferentes datos recopilados; en este caso se parte del SSID Skynet y seleccionamos la dirección MAC que le corresponde. Es importante resaltar que cuando se usa Wigle WiFi de forma gratuita, los datos obtenidos se comparten en una base de datos colaborativa en Wigle.net; en donde otros usuarios podrán también obtener el detalle de la información recopilada en la recolección de datos que se ha realizado de forma previa. Continuando, al obtener la dirección MAC es necesario dirigirse al sitio web de Wigle WiFi y se hace la búsqueda de la red por medio de la dirección MAC.

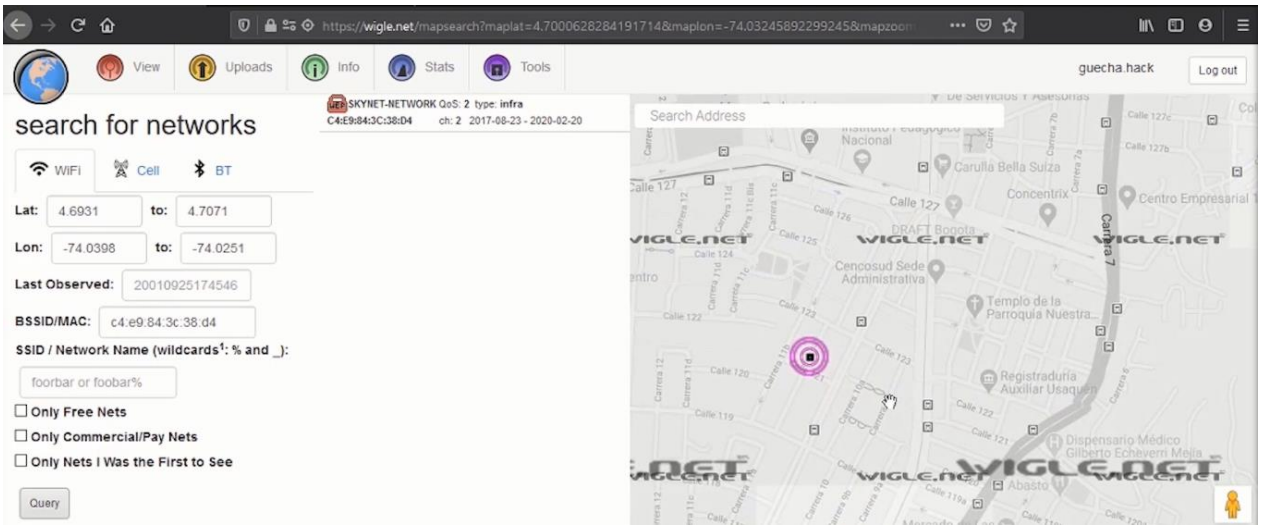
Al realizar la búsqueda como se ve en la **Figura 10**; se encontrará una aproximación de la ubicación de dicha red inalámbrica que se está buscando. Es importante resaltar, que la ubicación es aproximada y aunque sea ubicado en un punto específico, su ubicación puede variar ligeramente ya que lo que registra la aplicación es el punto desde donde fue detectado el punto de acceso por la antena, lo que indica que los factores cómo el tipo de antena usada y el alcance del punto de acceso son determinantes para encontrar una geolocalización más o menos precisa como se puede ver en la **Figura 11.**

Figura 10 Búsqueda del SSID de la PoC en wigle.net



Fuente: Elaboración propia

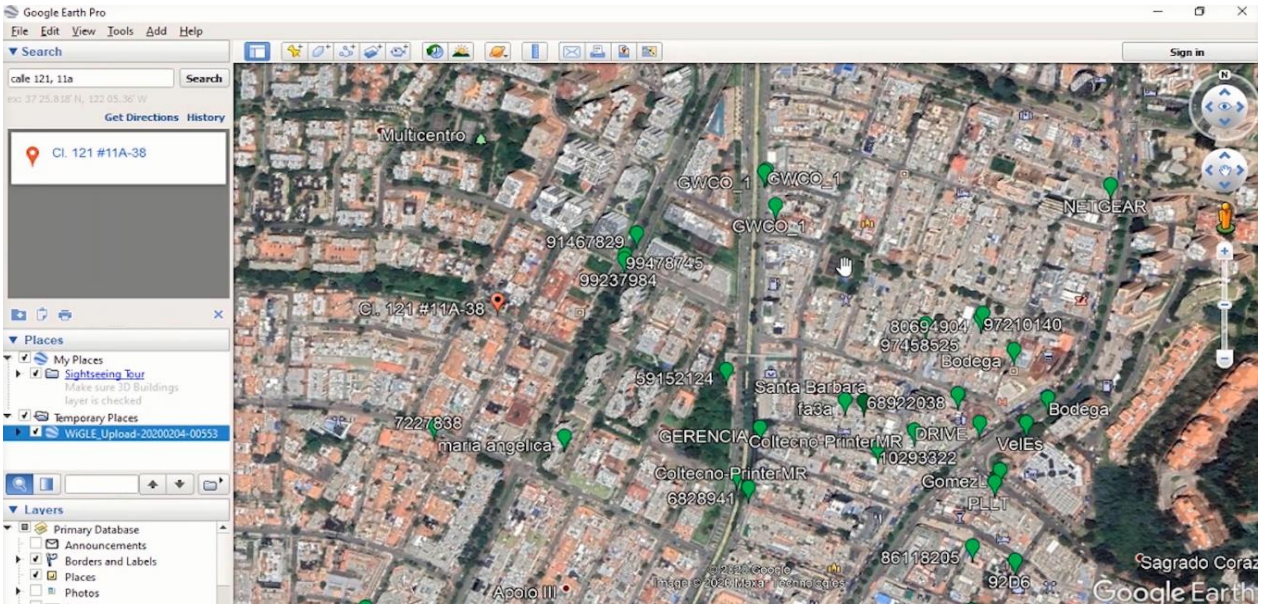
Figura 11 Vista del punto de acceso de la PoC en wigle.net



Fuente: Elaboración propia

En comparación a los datos visualizados en la figura anterior con respecto a la posición real donde se crea el punto de acceso de prueba, se puede confirmar que hay una diferencia real de 5 cuadras; ya que la ubicación del punto de acceso se encontraba sobre esa zona, pero no específicamente sobre el punto, por lo cual se puede afirmar que es bastante precisa en casos en los que el ciberdelincuente quiera retornar al punto de origen. Para continuar, cuando un ciberdelincuente se encuentra con esta situación pude escalar a hacer un reconocimiento mucho más específico de la zona para intentar efectuar un ataque; así que, en este caso se procede con hacer la búsqueda de la dirección que arroja el SSID, para determinar en primer lugar que podría verificar un delincuente con la información mencionada en cuestión. Se prosigue buscando en Google Earth o en Google Maps como se puede visualizar en la **Figura 11** y **Figura 12;** mediante la opción de Street View , en donde se puede detectar que se puede encontrar en esa zona, que tipos de edificaciones existen, cuáles son las zonas de parqueo públicas, la existencia de puestos de control o de vigilancia de conjuntos residenciales, entre otros, que le permitan al atacante crear una estrategia para pasar por inadvertido al momento de intentar efectuar un ataque a la red dispuesta.

Figura 12 Búsqueda de la dirección en Google Earth



Fuente: Elaboración propia

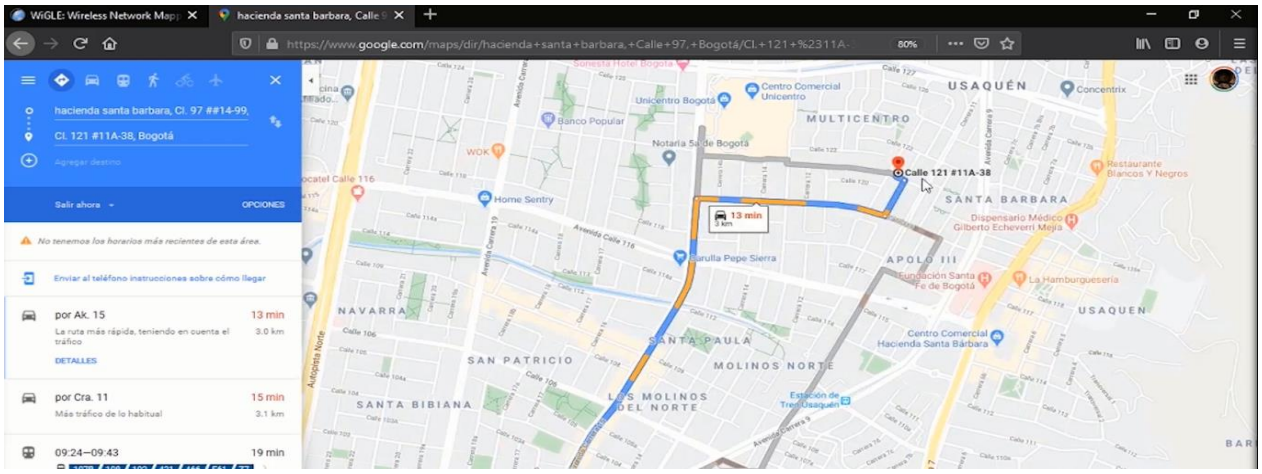
Figura 13 Búsqueda de la dirección en Google Earth con Street View

Fuente: Elaboración propia

También se puede apoyar mediante el uso de aplicaciones como Google Maps o Waze como se ve en la **Figura 14**, para comprobar la mejor ruta para llegar a ese destino o si

hay presencia de accidentes, reparaciones en la vía que impidan el tránsito, autoridad de tránsito con puestos de control, distancia al punto objetivo, etc…

Figura 14 Búsqueda de la ruta de acceso en Google Maps

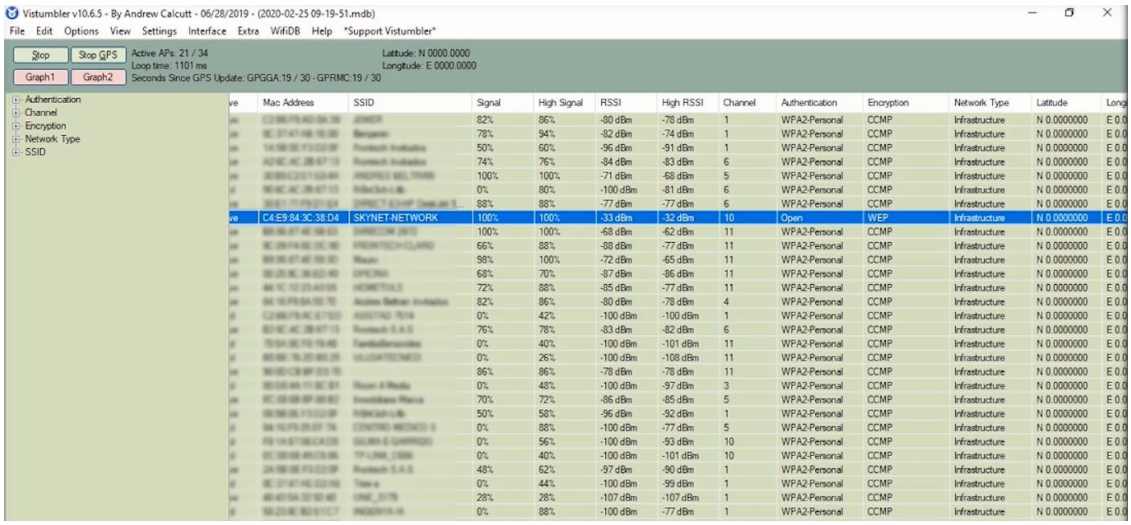


Fuente: Elaboración propia

Una vez el atacante en este caso tiene la información suficiente sobre cómo, cuándo y dónde puede atacar; el siguiente paso es dirigirse a la zona señalada esperando que, al momento de iniciar un escaneo con el software y el hardware deseado; logre detectar la red objetivo Skynet dentro de la periferia de esa zona. Para este punto de la actividad se relaciona el uso de una herramienta llamada Vistumbler, qué es ideal para las personas que cuentan con sistemas operativos Windows y que no están familiarizados con otros sistemas o plataformas.

Como se observa en la **Figura 15**, se encuentra la red objetivo dentro del análisis, y con ella trae datos en tiempo real sobre características muy específicas de la red inalámbrica como su estado, el nivel de señal actual, el canal por el cual se está comunicando, el tipo de autenticación que maneja, entre otros datos relevantes que al atacante le permiten reconocer las posibles brechas de seguridad por las cuales podría afectar esa red.

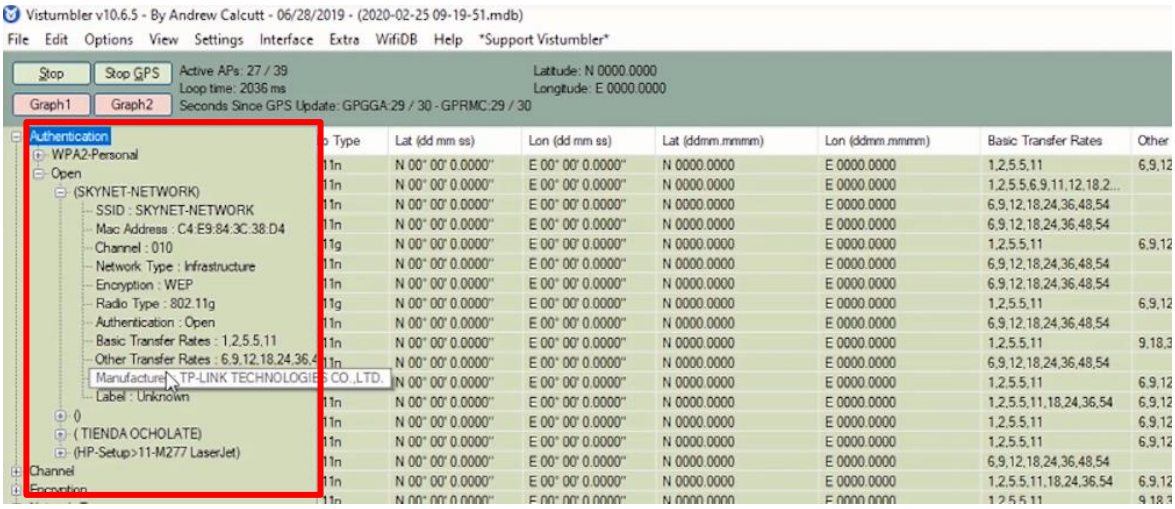
Figura 15 Búsqueda de red objetivo con Vistumbler



Fuente: Elaboración propia

Incluso como se puede ver en la **Figura 16**, es posible visualizar el fabricante del punto de acceso y su configuración, por lo cual para un atacante que encuentre el fabricante y modelo del dispositivo, sería fácil hacer una búsqueda por posibles vulnerabilidades del firmware o por configuraciones por defecto del dispositivo, que le permitan de forma más sencilla intervenir y atacar una red.

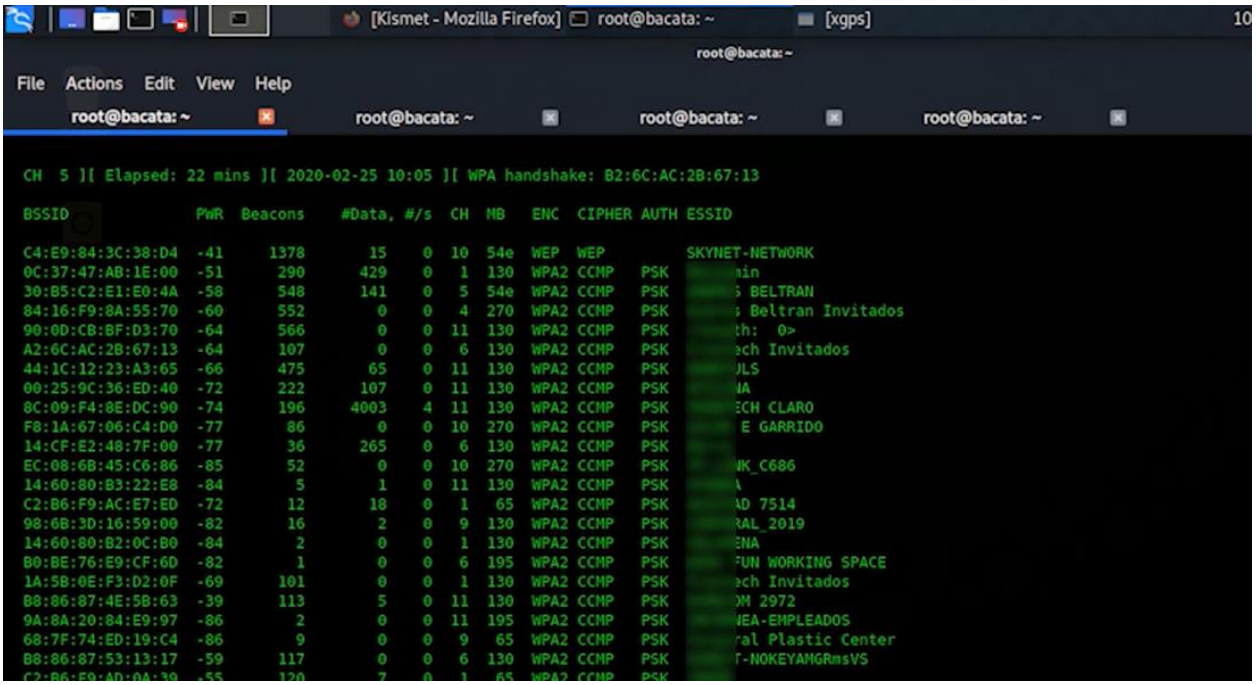
Figura 16 Detalles del punto de acceso desde Vistumbler



Fuente: Elaboración propia

Por otro lado, también se puede hacer este mismo proceso de escaneo realizado con Vistumbler anteriormente, pero directamente con la distribución Kali Linux; sin embargo, esto se escoge a elección del tester, en donde se configura la antena en modo promiscuo, allí se encontrarán los detalles de la red, del protocolo de conexión, los beacons, el cifrado que usa, etc… Tras la configuración del GPS también se tendrán datos precisos de la geo locación de los dispositivos y redes, tal y como se evidencia en las **Figura 17**.

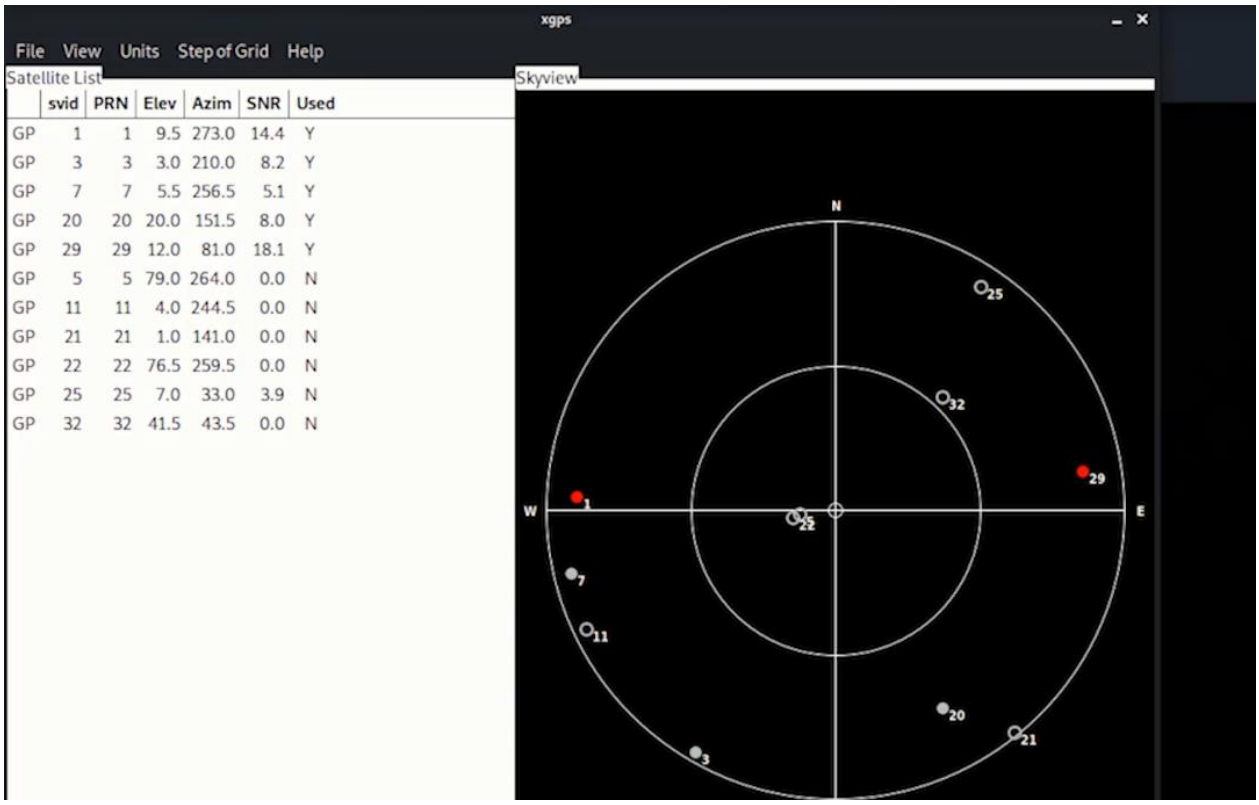
Figura 17 Antena WiFi en modo monitor en Kali Linux



Fuente: Elaboración propia

Para el arranque del dispositivo GPS, es importante verificar que el GPS este funcional y bien posicionado de tal manera que se pueden obtener datos precisos y verídicos acerca de la geo locación de las redes inalámbricas. Para comprobar su funcionamiento se debe esperar que la aplicación xgps que se está usando sobre Kali Linux, muestre los puntos de dos satélites en rojo, esto garantiza que el dispositivo que se está usando para la actividad funciona correctamente, tal y como se muestra en la **Figura 18**.

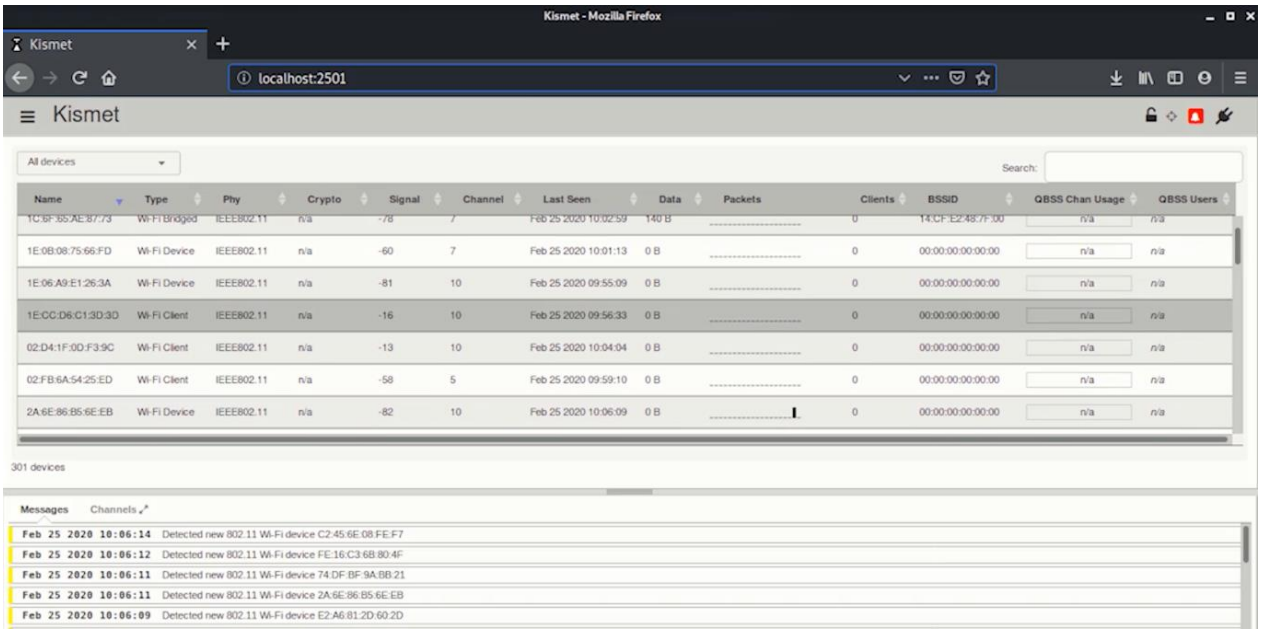
Figura 18 Verificación del estado del GPS



Fuente: Elaboración propia

Al comprobar que la antena está configurada en modo promiscuo y recibe todas las redes inalámbricas en su entorno, incluida la red inalámbrica de la PoC que se llama “Skynet” y que también el GPS está trabajando de forma correcta, se puede recabar en profundidad sobre la red objetivo con la aplicación Kismet. Kismet es una herramienta encontrada en Kali Linux. que desde su interfaz gráfica hace uso de la antena y el GPS que se ha configurado anteriormente, para hacer un análisis exhaustivo de las redes inalámbricas al alcance como se puede observar en la **Figura 19.**

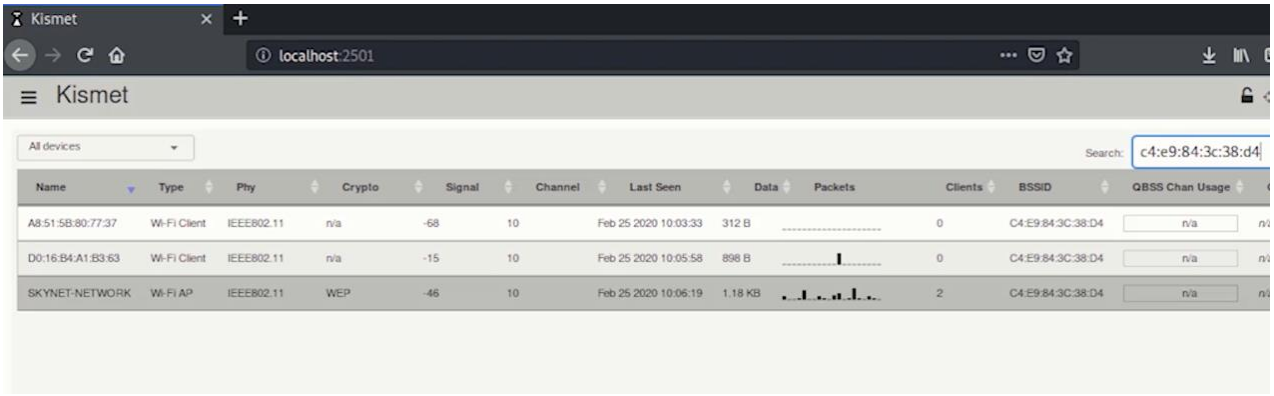
Figura 19 Dashboard de Kismet



Fuente: Elaboración propia

Al igual que con las herramientas anteriores, esta herramienta al tener interfaz gráfica tiene unas utilidades que son de gran impacto y apoyo para las actividades del tester ya que permiten filtrar y hacer búsquedas de forma sencilla; para no tener que ver punto por punto, sino que nos permite buscar una red por diferentes características, en este caso se busca la dirección mac de Skynet como se puede observar en la **Figura 20**.

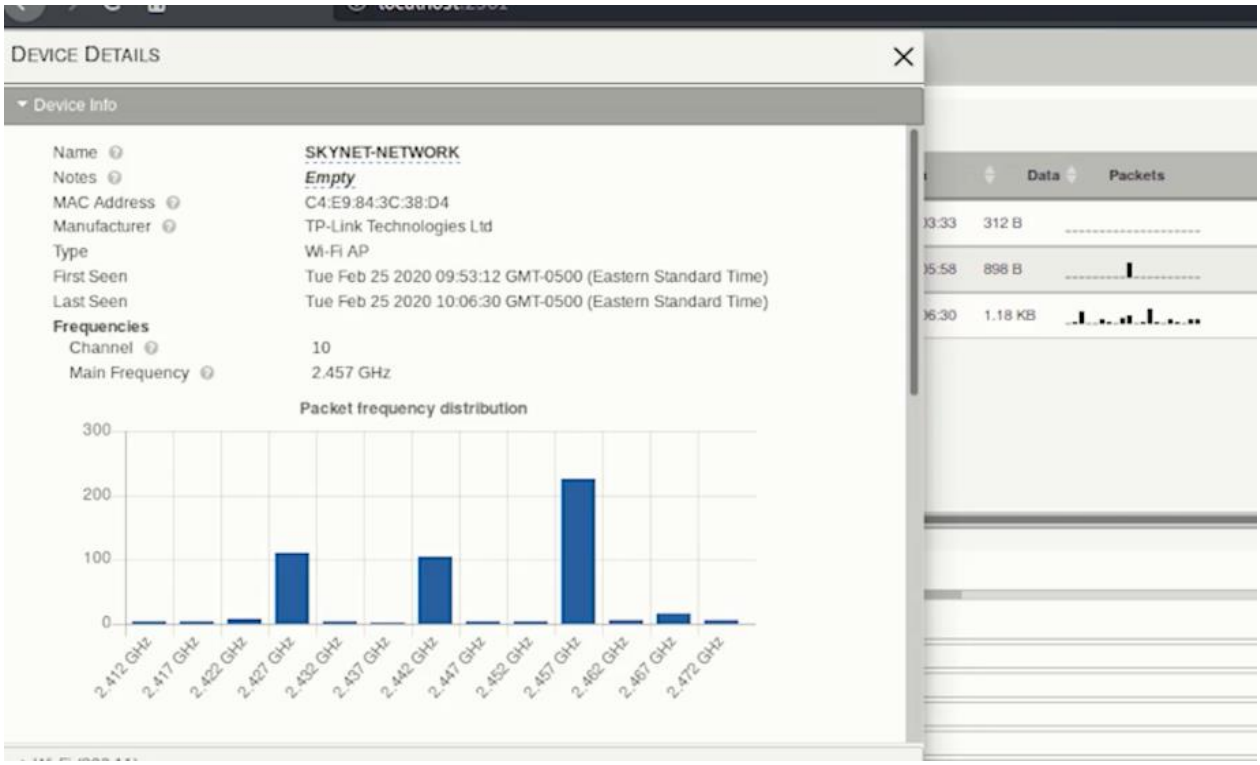
Figura 20 Búsqueda por dirección mac en Kismet



Fuente: Elaboración propia

Al igual que con Vistumbler, Kismet permite encontrar datos específicos de la red inalámbrica, que son ideales para el proceso de reconocimiento y recolección de información que pueden ser usados para un eventual ataque como se ve en la Figura 19. Aquí se puede ver la dirección mac, fabricante, frecuencia, protocolo, modelo del dispositivo, serial, clientes conectados al punto de acceso como se ve en la **Figura 21**; con lo que nos se verifica que con el uso de diferentes herramientas se puede obtener información más detallada y sensible que puede usarse más adelante.

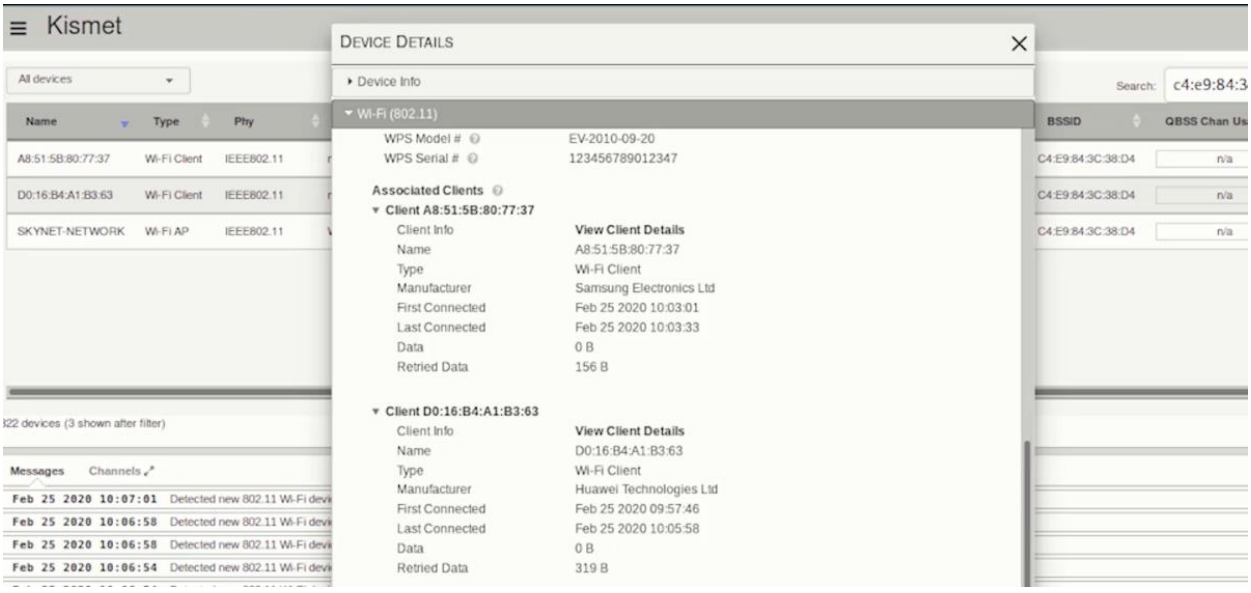
Figura 21 Búsqueda por dirección mac en Kismet



Fuente: Elaboración propia

Como se puede ver en la **Figura 23** que se encuentra a continuación; también se puede verificar de forma detallada cuales clientes están conectados al punto de acceso, lo cual genera mayor valor a la actividad ya que compromete incluso más información de los dispositivos conectados.

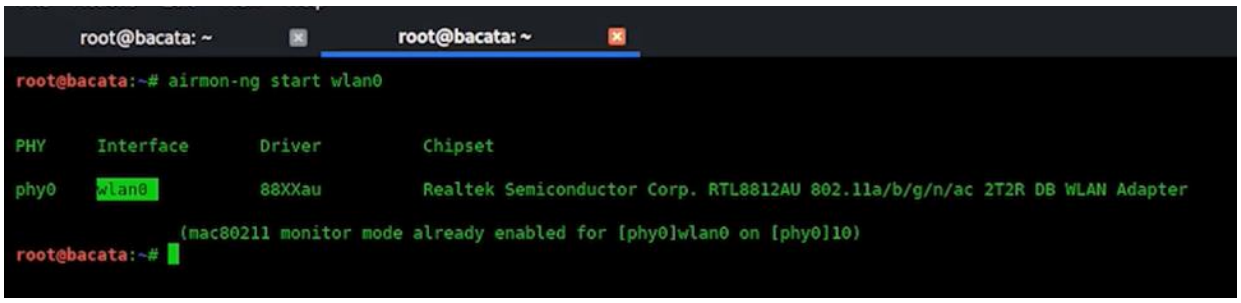
Figura 22 Clientes conectados en el punto de acceso desde Kismet



Fuente: Elaboración propia

Una vez se finaliza la etapa de reconocimiento con las herramientas seleccionadas, se debe proceder con la fase de ataque en donde se verificará el nivel de seguridad de una red inalámbrica con protocolo de seguridad WEP y con una contraseña fuerte. Inicialmente se debe configurar la antena WiFi en modo monitor, que permite más adelante realizar inyección de paquetes, tal y como lo podemos apreciar en la **Figura 23**.

Figura 23 Configuración de antena WiFi en modo monitor



Fuente: Elaboración propia

Tras hacer este procedimiento, se inicia con el uso de la suite de aircrack-ng que es la seleccionada para atacar la red Skynet con el protocolo WEP. El primer comando que se usa es airodump-ng en la antena que se ha configurado en modo monitor como se ve en la **Figura 24.**

Figura 24 Ejecución de airodump-ng en la antena en modo monitor

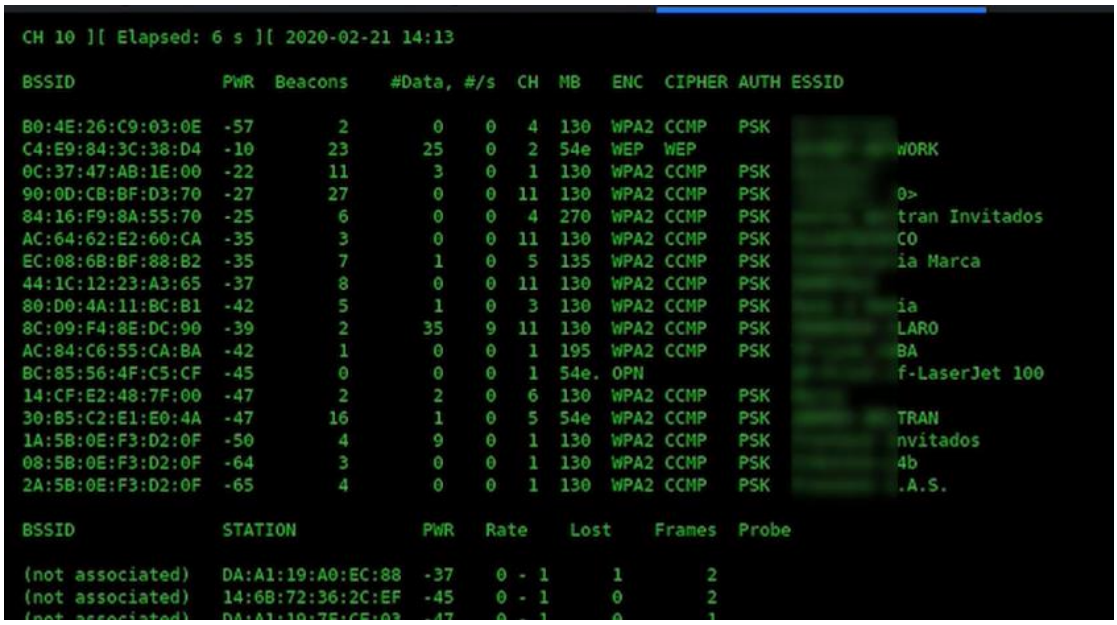
Fuente: Elaboración propia

Como indica el fabricante sobre la ejecución del comando en la línea anterior: *"…se usa para capturar paquetes wireless 802.11 y es útil para ir acumulando vectores de inicialización IVs con el fin de intentar usarlos con aircrack-ng y obtener la clave WEP. Si tienes un receptor GPS conectado al ordenador, airodump-ng es capaz de mostrar las coordenadas de los puntos de acceso que vaya encontrando.*[9]*"*; así que, la ejecución permite a grande escala ver la información de las redes inalámbricas y de los clientes asociados a cada punto de acceso.

Es por ello por lo que, como resultado de la ejecución de la antena en modo monitor se obtiene la información detallada en la **Figura 25**, en donde se obtiene la información de los routers, que en este caso a diferencia de los puntos anteriores no es obtenida con el nombre SSID, sino que lo expresa directamente con la dirección MAC de cada uno de los puntos de acceso que han sido detectados por la antena. Así mismo se puede ver otros datos como la cantidad de Beacons que están en tráfico, el canal por el cual se realiza la transmision de la data y también otros datos como el tipo de protocolo de conexión WiFi y el cifrado que utiliza dicha conexión inalámbrica.

[9] (AIRCRACK-NG ORG. Descripción Airodump-ng, 2009)

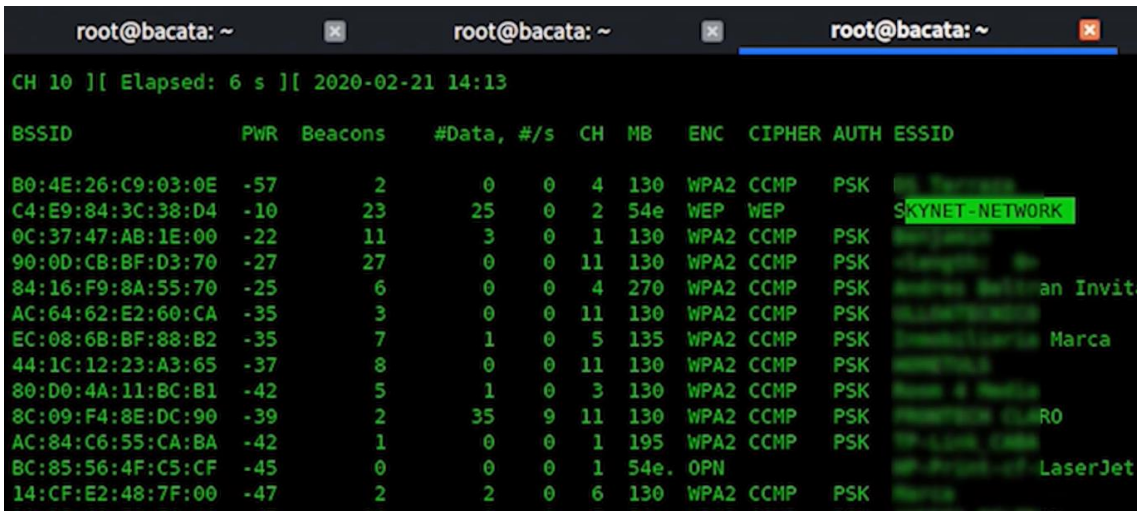
Figura 25 Configuración de antena WiFi en modo monitor



Fuente: Elaboración propia

Según la PoC que se está realizando se debe detectar la red objetivo y los datos que se necesitan para comprometerla, como se muestra a continuación en la **Figura 26**.

Figura 26 Red PoC objetivo con airodump



Fuente: Elaboración propia

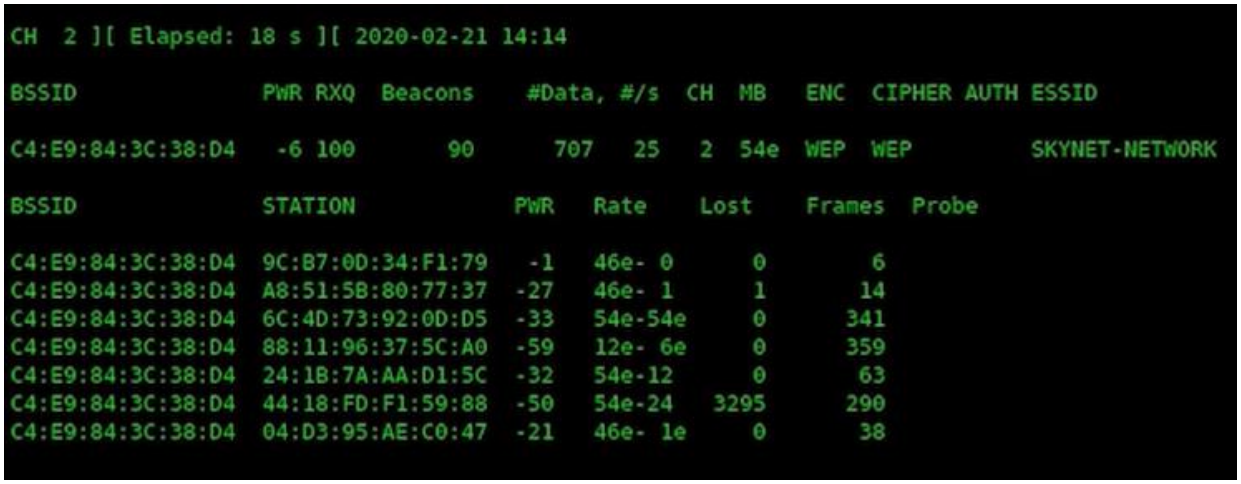
El propósito es capturar los vectores de inicio que se encuentran en el tráfico de la red para lograr descifrar la clave de la red inalámbrica. Por lo que se usa el comando *airodump-ng -bssid bssidobjetivo -c 2 -w nombredelarchivo*, en donde -c corresponde al canal que está usando la red inalámbrica para conectarse y que se puede encontrar en la **Figura 26**, al ejecutar el comando se capturan los vectores de inicio de la red y con -w se guardan los resultados en un archivo de texto, como se puede ver en la **Figura 27** en donde se ejecuta el comando explicado en este párrafo.

Figura 27 Ejecución airodump-ng para capturar vectores de inicio

Fuente: Elaboración propia

Como resultado del proceso anterior se inicia con la captura de vectores de inicio de esa red inalámbrica y se puede ver la información que va procesando en la **Figura 28** que se muestra a continuación.

Figura 28 Captura de vectores de inicio con airodump-ng

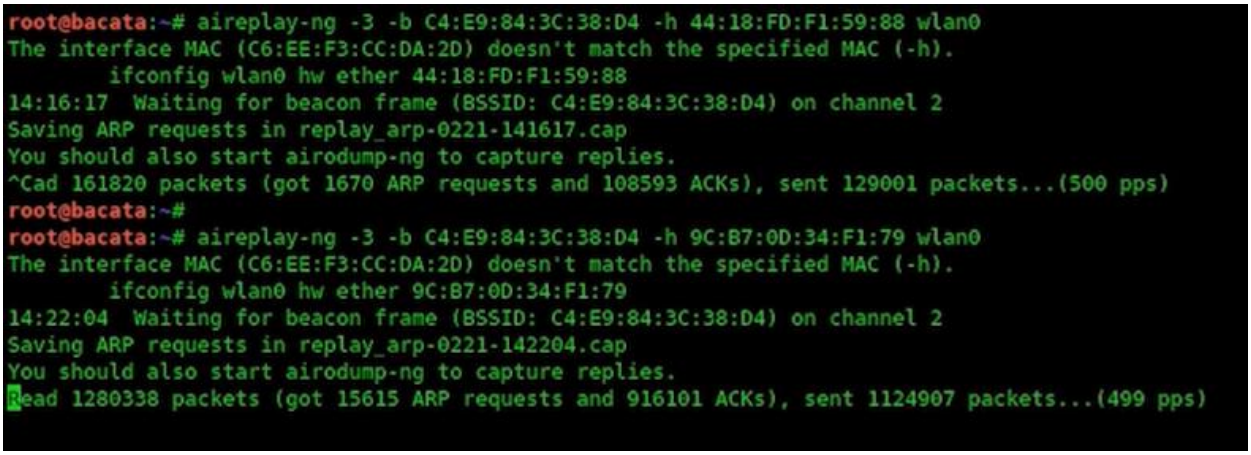


Fuente: Elaboración propia

Mientras se ejecuta el comando previo, en otro Shell de comandos, se debe ejecutar el comando ***aireplay-ng*****,** que permite inyectar paquetes. Mientras el comando previo captura los vectores de inicio, este comando permite enviar peticiones de forma masiva y a mayor número de peticiones incrementa la posibilidad de descifrar la clave.

El comando ejecutado en la PoC es *aireplay-ng -3 -b bssidobjetivo -h bssidclienteconectado*, el -3 del comando hace referencia a un ataque predeterminado de la herramienta para generar un ataque de ARP Request, esto se puede encontrar en la **Figura 29**.

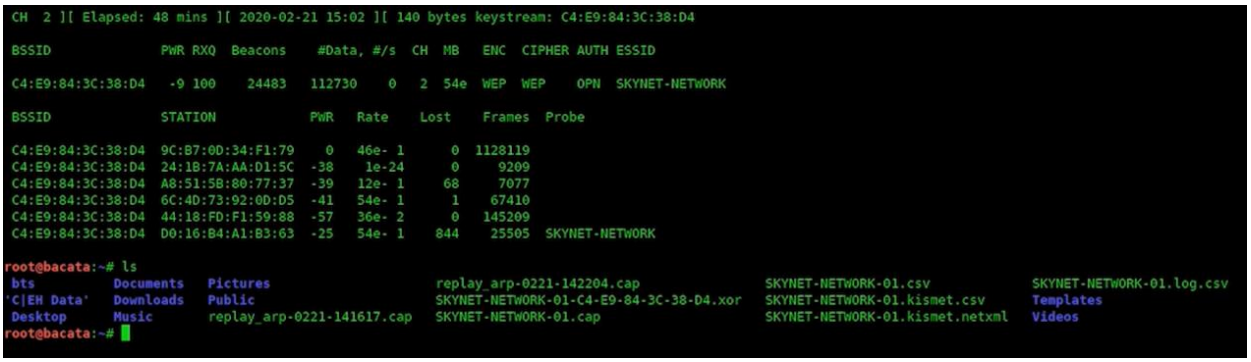
Figura 29 ARP Request con aireplay-ng



Fuente: Elaboración propia

Al generar el ataque “ARP Request” y elevar el número de peticiones al punto de acceso objetivo, aumenta el número de beacons inicial por lo cual podemos inferir que logró capturar un mayor número de vectores de inicio, esta información queda almacenada en el archivo de texto que se indicó de forma previa por medio del comando, tal y como se aprecia en la **Figura 30,** en donde se debe acceder a la ruta del sistema en donde se seleccionó que se almacenara la información para después de ello proceder a usar ese archivo de texto que creo el comando anteriormente mencionado.

Figura 30 Airodump y almacenamiento del archivo de texto con los resultados.



Fuente: Elaboración propia

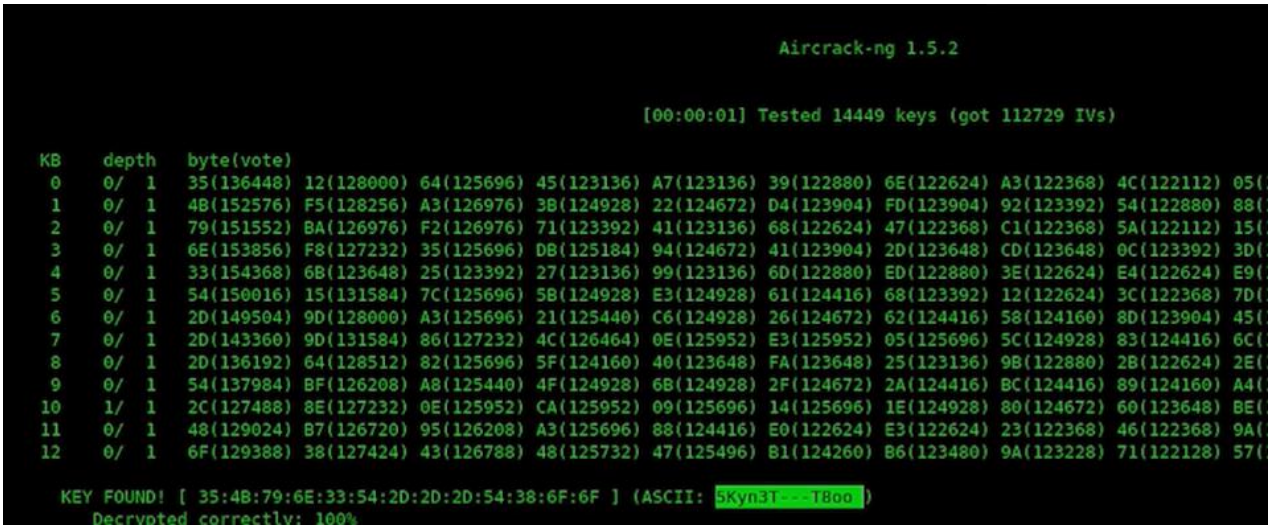
Al tener dicho archivo con los resultados que contienen los vectores de inicio resultantes a la inyección de paquetes con un ataque tipo ARP Request, se procede con la ejecución del comando y suite *aircrack-ng* que, al usar el archivo de texto dentro de su ejecución, permite descifrar la clave configurada en la red inalámbrica. En la **figura 31** se puede observar como inicia la ejecución, seleccionando el archivo de texto que se obtuvo previamente.

Figura 31 Ejecución aircrack-ng

Fuente: Elaboración propia

Después de ello se puede observar como la aplicación inicia con el ataque de fuerza bruta para obtener la contraseña de la red inalámbrica, tomando como base el resultado de la inyección de paquetes y el resultado obtenido en el archivo de vectores de inicio para ir contrastando dentro de las posibilidades cual coincide con el resultado y al final permite obtener la clave de la red inalámbrica, tal y como se evidencia en la **Figura 32**.

Figura 32 Ejecución de Aircrack-ng



Fuente: Elaboración propia

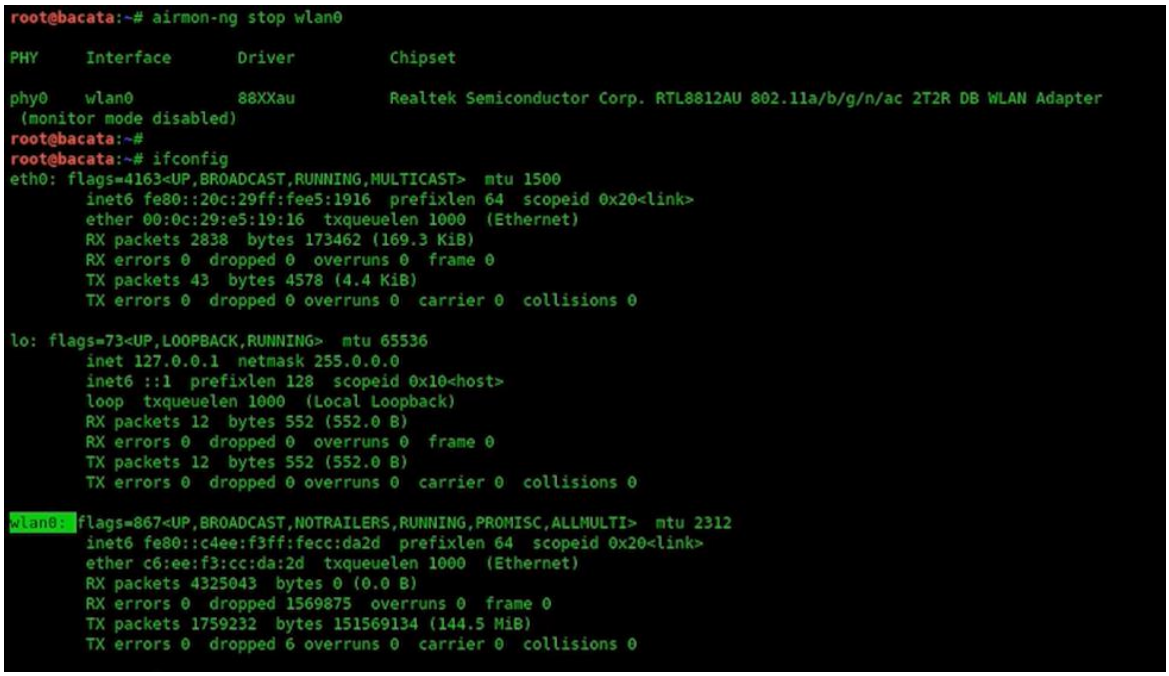
Finalmente, se obtiene la clave en texto plano que corresponde a la red inalámbrica Skynet que se ha configurado para esta PoC. Como se puede observar en la **figura 33,** a pesar de que la clave se considera una contraseña segura por la combinación de caracteres y coincide con las recomendaciones de seguridad otorgadas por grandes fabricantes; cuando el protocolo que protege la conexión inalámbrica no es seguro y es obsoleto, de nada sirve tener una clave robusta, controles costosos, ni políticas de seguridad definidas, ya que el protocolo dejara vulnerable la red y cualquier tipo de información que transite en ella; por lo que pondrá en riesgo a la compañía y su infraestructura dejando un punto vulnerable expuesto al publico y a merced de los ciber delincuentes.

Figura 33 Obtención de la clave de la red inalámbrica Skynet

Fuente: Elaboración propia

Teniendo las credenciales de la red inalámbrica, se puede intentar iniciar sesión para realizar alguna acción intrusiva adicional; así que primero, se debe desactivar el modo monitor de la antena para recobrar todas las funciones de red y reiniciar el servicio de red del sistema operativo que se está usando. Se verifica cuál es la IP asignada para comprobar cuando se realice la conexión a la red víctima, si realmente algo en la red cambia, esto se puede apreciar en la **Figura 34.**

Figura 34 Restablecimiento de la antena y las propiedades de red de Kali



Fuente: Elaboración propia

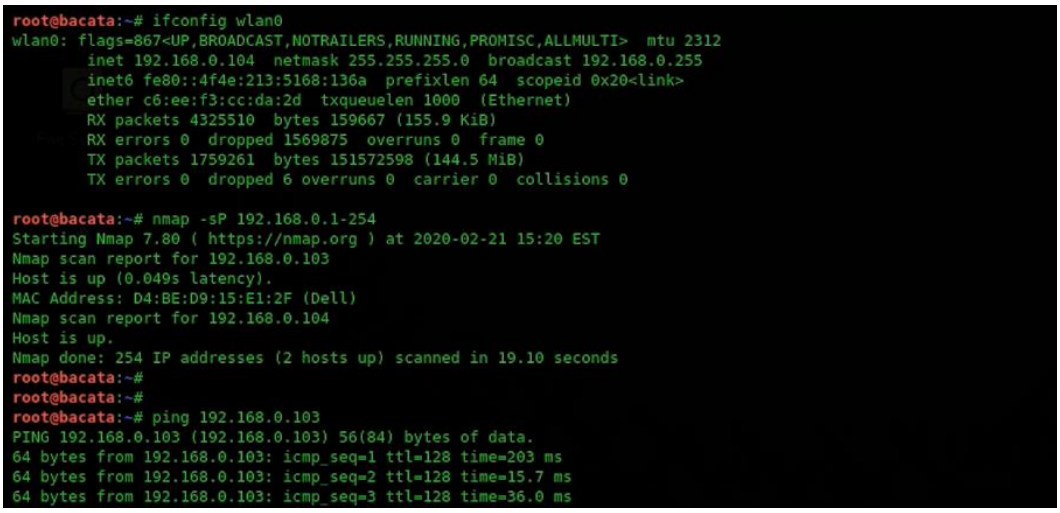
Una vez recobrado el servicio de red de la máquina virtual Kali Linux, se intenta conectar a la red inalámbrica vulnerada como se ve en la **Figura 36**, para comprobar que la contraseña realmente funcione y determinar que otras brechas se pueden encontrar dentro de la red.

Figura 35 Conexión a la red inalámbrica victima con la clave descifrada

Fuente: Elaboración propia

Como se aprecia en la **Figura 36** al momento de iniciar la sesión en la red victimizada ejecutar en la shell de Kali Linux, el comando ifconfig para verificar cuál es la IP asignada tras la conexión a la red víctima; donde se puede evidenciar que la IP ha cambiado completamente al entorno en el que se ha realizado la conexión. una vez dentro de la red se pueden ejecutar otros comandos como el de reconocimiento del segmento de red con nmap y allí se puede encontrar un dispositivo conectado de marca Dell. Asimismo, se puede ejecutar ping para ver si hay conectividad a esa máquina tal y como se referencia en la **Figura 36.**

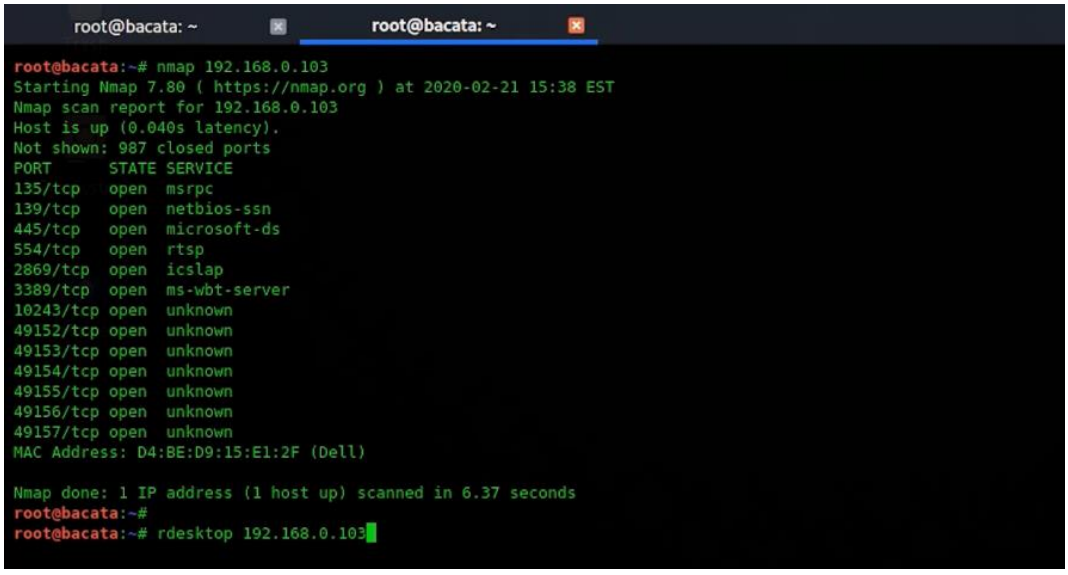
Figura 36 Comprobaciones iniciales tras conectarse a la red victima



Fuente: Elaboración propia

Al comprobar que hay conectividad con otra máquina dentro de la red, otra vez con la ayuda del comando **nmap** se hace un reconocimiento de este dispositivo para verificar qué servicios o puertos se encuentran abiertos que puedan ser de utilidad para el atacante y seguir escalando dentro de la red tal y como se observa en la **Figura 37**.

Figura 37 Ejecución de nmap para descubrir puertos y servicios

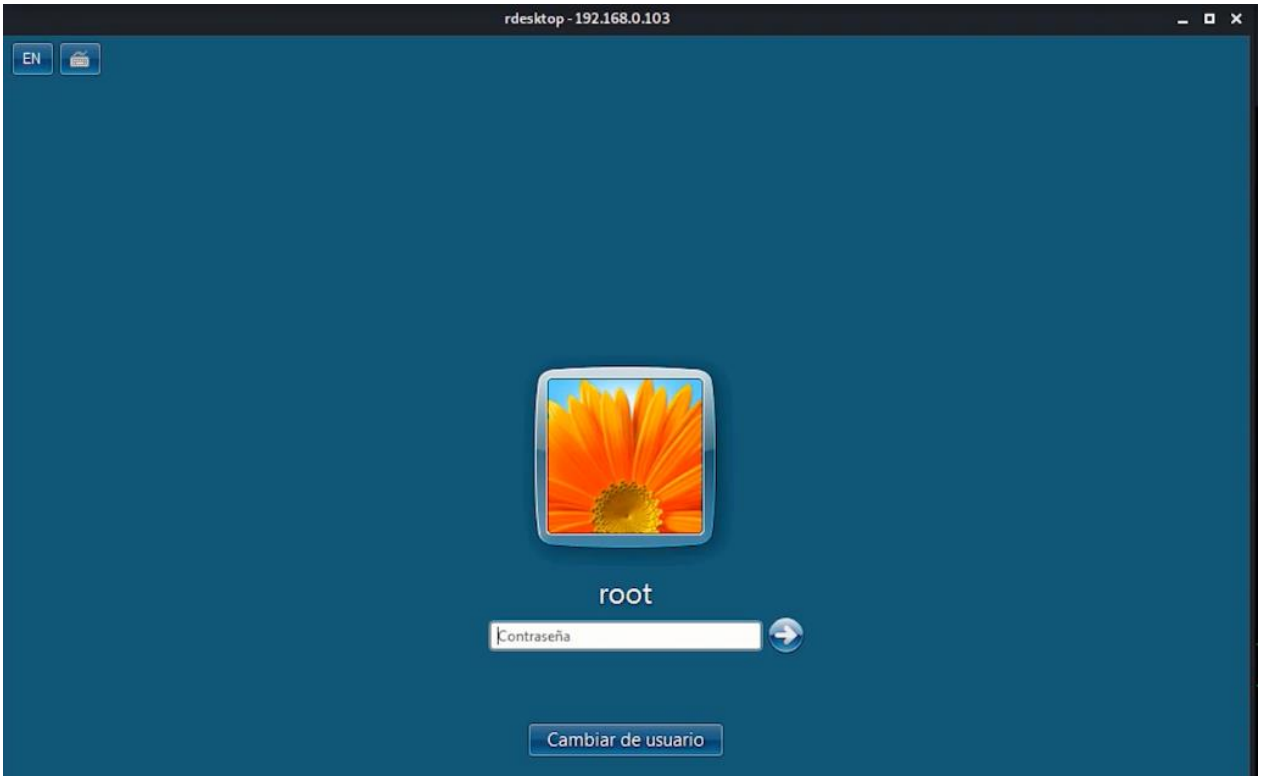


Fuente: Elaboración propia

Cómo se encuentra en la **Figura 37**, se puede ver que tras el descubrimiento de puertos se encuentran varios abiertos y que son críticos para cualquier red o compañía, ya que permitiría fácilmente que ciber delincuente vulnere la seguridad de la red y por ende pueda generar daño mediante el aprovechamiento de los recursos o la información que se encuentren allí.

Cómo se puede observar el puerto para las conexiones de Escritorio Remoto de Windows o RDP se encuentra abierto, así que es evidente que se ha logrado encontrar un sistema operativo Windows y un dispositivo Dell. Aprovechando esta información en la **Figura 38,** se procede a intentar generar una conexión remota a esa máquina expuesta dentro de la red vulnerada y se puede ver como se logra acceder a la ventana de inicio de sesión de ese servidor.

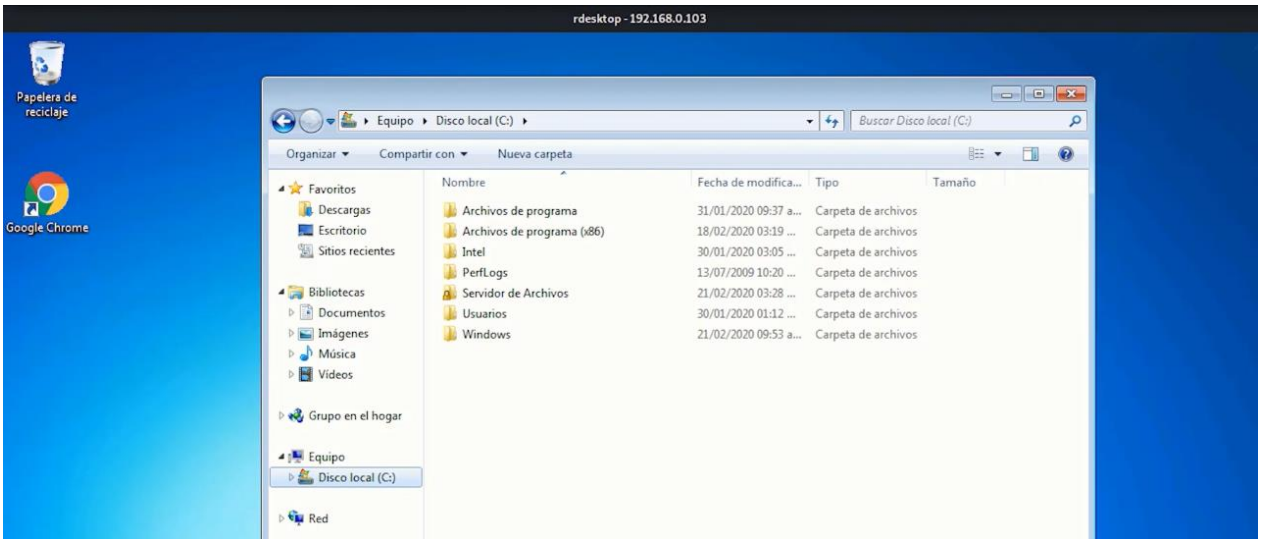
Figura 38 Conexión RDP desde Kali hacia un servidor Windows de la red victima



Fuente: Elaboración propia

Al ver que hay un usuario configurado con un nombre por defecto o que está en la lista de los usuarios comunes de un sistema operativo, una de las primeras actividades a realizar es probar también con contraseñas por defecto o comunes de los sistemas para verificar que se pueda acceder sin generar algún ataque específico; así que, en la **Figura 39** se puede verificar que tras probar con diferentes claves comunes y registradas en diferentes reportes de claves por defecto vulnerables, se logra concretar un acceso al sistema operativo víctima.

Figura 39 Acceso a la máquina conectada a la red victima



Fuente: Elaboración propia

Desde el momento en el que se tuvo el acceso a la red inalámbrica, el ciberdelincuente se encuentra dentro de la red de la víctima por lo cual se podría ejecutar una infinidad de otros ataques; sin embargo, al lograr acceder directamente a un equipo o un servidor que esté conectado a esa red, es mucho más sencillo para un atacante hacer un escalamiento horizontal o vertical dentro de la red víctima, o incluso generar un daño mayor para la compañía o usuario, robando sus credenciales, los datos de sus tarjetas de crédito, los accesos a sus plataformas, instalando código malicioso dentro de la máquina, secuestrando sus datos para luego pedir un rescate, entre infinidad de opciones que pueden ejecutar tras haber logrado el acceso al equipo.

5.4. RECOMENDAR DISTINTAS OPCIONES QUE PERMITAN MITIGAR LOS RIESGOS DE LAS REDES VULNERABLES CON EL FIN DE QUE PERSONAS EXPERTAS Y NO EXPERTAS CUENTEN CON LA INFORMACIÓN NECESARIA PARA EVITAR EXPLOTACIONES A RAÍZ DEL USO DE PROTOCOLOS INSEGUROS EN REDES INALÁMBRICAS

Es importante verificar con atención los dispositivos de conexión a internet que proveen los proveedores ISP, que son usados tanto en las compañías como en los hogares, se debe poner especial atención al protocolo de seguridad que tiene la conexión a internet y el estándar de conexión que utilizan. Se debe verificar que no sea obsoleto o vulnerable, en caso de que así sea se debe solicitar al fabricante su actualización o cambio el dispositivo con el fin de evitar que sea víctima de un ciberataque a causa de esto.

Se recomienda el uso dispositivos de conexión inalámbrica que se encuentren bajo la especificación 802.11n y el protocolo de conexión inalámbrica WPA3. WPA3 es una versión actualizada y más segura del protocolo Wi-Fi Protected Access para asegurar las redes inalámbricas. WPA3 introduce nuevas mejoras de seguridad que dificultan la intrusión en las redes mediante la adivinación de las contraseñas; también hace imposible descifrar los datos capturados en el pasado; es decir, antes de que se descifrara la clave o contraseña de la red. Cuando la alianza Wi-Fi anunció los detalles técnicos de WPA3 a principios de 2018, su comunicado de prensa transmitía cuatro características principales:

- **Un nuevo handshake más seguro para establecer conexiones:** llamado Autenticación simultánea de iguales (SAE). Cuando un dispositivo intenta conectarse a una red Wi-Fi protegida por contraseña, los pasos de suministro y verificación de la contraseña se realizan mediante un handshake de 4 vías. En WPA2, esta parte del protocolo era vulnerable a los ataques KRACK: En un ataque de reinstalación de clave, el atacante engaña a la víctima para que reinstale una clave ya utilizada. Esto se consigue manipulando y reproduciendo los mensajes

del handshake. Cuando la víctima reinstala la clave, los parámetros asociados, como el número de paquete de transmisión incremental y el número de paquete de recepción; es decir, el contador de repeticiones, vuelven a su valor inicial. Básicamente, para garantizar la seguridad, una clave sólo debe instalarse y utilizarse una vez. Incluso con las actualizaciones de WPA2 para mitigar las vulnerabilidades de KRACK, WPA2-PSK puede ser descifrado. Incluso hay guías de cómo hackear las contraseñas de WPA2-PSK.

WPA3 soluciona esta vulnerabilidad y mitiga otros problemas al utilizar un mecanismo de intercambio de información diferente para autenticarse en una red Wi-Fi: la autenticación simultánea de iguales, también conocida como intercambio de claves Dragonfly. Las ventajas del intercambio de claves Dragonfly son el secreto hacia adelante y la resistencia al descifrado fuera de línea.

- **Resistente al descifrado sin conexión:** Una vulnerabilidad del protocolo WPA2 es que el atacante no tiene que permanecer conectado a la red para adivinar la contraseña. El atacante puede esnifar y capturar el handshake de 4 vías de una conexión inicial basada en WPA2 cuando está cerca de la red. Este tráfico capturado puede utilizarse fuera de línea en un ataque basado en diccionario para adivinar la contraseña. Esto significa que, si la contraseña es débil, es fácil de romper. De hecho, las contraseñas alfanuméricas de hasta 16 caracteres pueden descifrarse con bastante rapidez en las redes WPA2.

  WPA3 utiliza el sistema de intercambio de claves Dragonfly, por lo que es resistente a los ataques de diccionario. Esto se define de la siguiente manera: La resistencia al ataque de diccionario significa que cualquier ventaja que pueda obtener un adversario debe estar directamente relacionada con el número de interacciones que realice con un participante honesto del protocolo y no a través del cálculo. El adversario no podrá obtener ninguna información sobre la contraseña, excepto si una única suposición de una ejecución del protocolo es

correcta o incorrecta. Esta característica de WPA3 protege las redes en las que la contraseña de red -es decir, la clave pre compartida (PSDK)- es más débil que la complejidad recomendada.

- **Secreto hacia adelante:** Las redes inalámbricas utilizan una señal de radio para transmitir información o paquetes de datos, entre un dispositivo cliente (por ejemplo, un teléfono o un portátil) y el punto de acceso inalámbrico. Estas señales de radio se emiten abiertamente y pueden ser interceptadas o "recibidas" por cualquier persona que se encuentre en las proximidades. Cuando la red inalámbrica está protegida mediante una contraseña, ya sea WPA2 o WPA3, las señales se cifran para que un tercero que las intercepte no pueda entender los datos.

  Sin embargo, un atacante puede grabar los datos que intercepta. Y si es capaz de adivinar la contraseña en el futuro, lo que es posible mediante un ataque de diccionario en WPA2, puede utilizar la clave para descifrar el tráfico de datos registrado en el pasado en esa red. WPA3 proporciona secreto hacia adelante. El protocolo está diseñado de forma que, incluso con la contraseña de la red, es imposible que un atacante espíe el tráfico entre el punto de acceso y otro dispositivo cliente.

- **Cifrado inalámbrico oportunista (OWE):** Descrito en el documento técnico (RFC 8110), el OWE es una nueva función de WPA3 que sustituye a la autenticación "abierta" de 802.11, muy utilizada en puntos de acceso y redes públicas. La idea clave es utilizar un mecanismo de intercambio de claves Diffie-Hellman para cifrar toda la comunicación entre un dispositivo y un punto de acceso. La clave de descifrado de la comunicación es diferente para cada cliente que se conecta al punto de acceso. Así, ninguno de los otros dispositivos de la red puede descifrar esta comunicación, incluso si la esnifan. Esta ventaja se denomina protección de datos individualizada: el tráfico de datos entre un cliente y un punto de acceso está

"individualizado", de modo que, aunque otros clientes puedan husmear y registrar este tráfico, no pueden descifrarlo.

Una gran ventaja de OWE es que no sólo protege las redes que requieren una contraseña para conectarse; también protege las redes abiertas "no seguras" que no requieren contraseña, por ejemplo, las redes inalámbricas de las bibliotecas. OWE proporciona a estas redes un cifrado sin autenticación. No es necesario ni el aprovisionamiento, ni la negociación, ni las credenciales: simplemente funciona sin que el usuario tenga que hacer nada, ni siquiera saber que su navegación es ahora más segura.

OWE no protege contra los puntos de acceso (AP) "fraudulentos", como los honeypot AP o los evil twins, que intentan engañar al usuario para que se conecte con ellos y robarle información. Otra advertencia es que WPA3 admite, pero no obliga el cifrado no autenticado. Es posible que un fabricante obtenga la etiqueta WPA3 sin implementar el cifrado no autenticado. La función se llama ahora Wi-Fi CERTIFIED Enhanced Open, por lo que los compradores deben buscar esta etiqueta además de la de WPA3 para asegurarse de que el dispositivo que compran admite el cifrado no autenticado.

WPA3 usa cifrado de 128 bits en el modo WPA3-Personal (192 bits en WPA3-Empresa). WPA3 también sustituye el intercambio de claves pre compartidas (PSK) por la autenticación simultánea de iguales, una forma más segura de realizar el intercambio inicial de claves a diferencia de WPA2 que utiliza el estándar AES. La especificación final sólo impone el nuevo handshake, pero algunos fabricantes aplicarán también las demás características.

Se sabe que los puntos de acceso y redes inalámbricas son de uso constante tanto para los usuarios de confianza es decir aquellos que pertenecen a la compañía o que viven en los hogares; pero también es común encontrar usuarios invitados que se conectan de

forma frecuente y nunca se tiene una revisión o actualización de estos usuarios. Así vamos a qué se debe cambiar de forma frecuente la clave de conexión a la red inalámbrica, configurando una contraseña segura que conste de minúsculas, mayúsculas, números, caracteres especiales y una longitud recomendada de más de 12 caracteres; con el fin de evitar que pueda ser vulnerada de forma fácil y de garantizar que la red se encuentra lo más segura posible de intrusos.

Siempre que sea posible se debe actualizar los dispositivos y los sistemas operativos a los cuáles tengamos acceso, ya que esto es una garantía de recibir nuevas configuraciones y herramientas de seguridad por parte de los fabricantes que en caso de un descuido serán de gran utilidad para evitar que por fallos de actualización seamos vulnerados.

Es común encontrar que en los entornos comparativos haya recursos compartidos dentro de los diferentes servidores y dispositivos para ejecutar diferentes labores rutinarias de la compañía; sin embargo, es vital que si en la compañía o en el lugar en donde nos encontramos existe una configuración de este tipo, se verifiquen los permisos de cada carpeta compartida y únicamente se limiten a los usuarios o recursos que los necesitan.

También se pueden contar que en las compañías se requiera del uso del escritorio remoto y aunque no es la opción más recomendada, en caso de que sea necesario evitar para la compañía lo ideal sería usar un sistema de doble autentificación para añadir un nivel de seguridad extra a las conexiones y evitar intrusos en la organización; también se recomienda cambiar los puertos comunes de los servicios expuestos; de esta manera al ciber delincuentes le será más difícil encontrar un vector de ataque.
Para los casos de conexiones a escritorio remoto, es importante poder usar un sistema de doble autenticación.

6. CONCLUSIONES

Al finalizar con el desarrollo de esta actividad se logró verificar que el estado de seguridad en las redes inalámbricas de la ciudad de Bogotá, se encuentra en un estado deficiente y que requiere especial atención para el desarrollo de las empresas; teniendo en cuenta los hallazgos presentados en donde gran parte de las señales de WiFi WEP y WPA2 basándonos en el SSID de la red corresponden a redes corporativas de pequeñas y medianas empresas de diferentes sectores de la industria local y nacional.

Se ha evidenciado que cada día existen más proyectos de impacto TIC y de inclusión en el mundo de la informática; así que es importante empezar a tenerlos en cuenta para un correcto y competitivo avance dentro del mundo de la tecnología, de la ciberseguridad y de las compañías frente a normativas. Ya que desde los últimos años se ha venido exigiendo cada vez más un nivel de calidad optimo dentro de las compañías, que salvaguarden la integridad, la confidencialidad y la disponibilidad de la información como con la normativa presentada por la ISO 27001. Según los hallazgos se pudo notar con datos estadísticos que las redes inalámbricas son una potencial fuente de riesgos en todos los entornos y han estado desatendidas; por lo que, es necesario y primordial no dejar a un lado la seguridad en las redes inalámbricas así en muchos casos sea desestimada porque no se ha considerado importante o de impacto; bien sea por desconocimiento de las posibles consecuencias y que pueden resultar en pérdidas de información y el enfrentamiento de diferentes consecuencias a varios niveles para los actores que intervienen.

Según lo estudiado y aunque en la teoría se sabe que redes inalámbricas con protocolos de seguridad como WEP, WPA y WPA2 no son seguros y gracias al desarrollo de esta investigación pudimos confirmar de forma práctica cómo podría ser el actuar de un delincuente y que tan grave podría llegar a ser un ataque por el aprovechamiento de uno de estos protocolos en cualquier red inalámbrica que los use. Los especialistas han creído

que estas redes ya no son usadas en ningún entorno, pero es importante resaltar que gracias al desarrollo de este proyecto pudimos identificar de forma cuantitativa; de una población objetivo, las cifras específicas y porcentajes relacionados a cada uno de los protocolos de seguridad de redes inalámbricas; lo cual nos deja en una postura más acertada al intentar implementar al hablar académicamente sobre datos más precisos y exactos que nos permitan continuar con una investigación de protocolos de seguridad de conexiones inalámbricas hacia internet.

Este trabajo nos ha permitido tener un espectro más claro y dar una visibilidad al problema planteado para intentar llegar a la mayor cantidad de población que requiera esta información y que no tenga la pesquisa precisa con respecto a las redes que usa o porque el uso de estas mismas puede llegar a ser tan controversial y nocivo para una red y para una compañía.

7. RECOMENDACIONES

Al implementar una investigación donde el WarDriving sea la metodología recolección de datos es importante tener en cuenta que el recolector no se debe limitar únicamente a las herramientas expuestas durante la ejecución de esta investigación, sino que dependiendo de sus necesidades se puede ajustar a herramientas nuevas son metodologías diferentes. Es muy importante tener en cuenta que los datos recolectados dentro de esta investigación son únicamente usados para carácter académico y no para fines maliciosos. Así que su único propósito es informar y advertir para evitar futuros incidentes de ciberseguridad y generar conciencia dentro de las compañías y administradores de las redes.

Se recomienda hacer especial énfasis dentro de las organizaciones sobre los dispositivos que se usan para conectar a los usuarios a internet, así como los protocolos que intervienen para el cifrado, comunicación y conexión externa hacia la red. Es importante que esto sea puesto en práctica por personal capacitado e idóneo; con profundos conocimientos de ciberseguridad y networking para evitar errores en la implementación y vulnerabilidades por desconocimiento de la actividad que se ha programado.

A pesar de contar con dispositivos de última generación es importante tener en cuenta cualquier actualización que tenga el software y el firmware, ya que estas contienen mejoras de funcionamiento y de opciones de seguridad que ha detectado el fabricante. Con esto se garantiza cubrir vulnerabilidades conocidas y así disminuir la probabilidad de ser víctima de un ciber ataque. Sin embargo; es necesario que el especialista siempre se encuentre en un continuo proceso de capacitación que garantice que esta persona este actualizado ante cualquier posible vulnerabilidad de día cero. Así mismo, es importante tener en cuenta que las configuraciones por defecto como puertos, protocolos, usuarios, contraseñas y portales de inicio de sesión, son uno de los primeros recursos que agotan los cibercriminales por lo que es de vital importancia proceder con una personalización de los recursos para evitar que estas configuraciones sean aprovechadas.

8. BIBLIOGRAFÍA

AIRCRACK-NG ORG. [Sitio web]. Airodump-ng [Consultado: 21 de abril 2022]. Disponible en: https://www.aircrack-ng.org/doku.php?id=es:airodump-ng

AKRAM, Zeeshan, MUHAMMAD Anwaar Saeed, y MARRIAM Daud. Wardriving and its Application in Combating Terrorism [En línea]. 2018. [Consultado: 21 de mayo de 2022]. ISBN 978-1-5386-4427-0. Disponible en: https://ieeexplore.ieee.org/document/8442035/

ARBAUGH,William y UNIVERSIDAD DE MARYLAND. Wireless Security Is Different. [en línea]. 2003, 01 septiembre. Volumen 36. [Consultado: 21 de abril 2022]. Disponible en: https://www.computer.org/csdl/magazine/co/2003/08/r8099/13rRUxZRbv5

ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS. [Sitio web]. Cifras de ciberseguridad en Colombia prenden alarmas al cierre del 2020. [Consultado 21 de marzo de 2022]. Disponible en: https://acis.org.co/portal/content/noticiasdelsector/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020

ATLURI, Sidharth, y REVANTH,Rallabandi. Deciphering WEP, WPA, and WPA2 Pre-Shared Keys Using Fluxion. [En línea]. 2021. [Consultado: 21 de mayo de 2022]. ISBN 978-1-5386-4427-0. Disponible en: https://link.springer.com/chapter/10.1007/978-981-16-0878-0_37

BENO, Richard, y RON Poet. Hacking Passwords that Satisfy Common Password Policies: Hacking Passwords. [En línea]. 2020. [Consultado: 21 de mayo de 2022]. ISBN 9781450387514 Disponible en: https://dl.acm.org/doi/10.1145/3433174.3433616

BLACK BOX CORPORATION. [Sitio web]. The Evolution of 802.11. [Consultado 21 de marzo de 2022]. Disponible en: https://www.bboxservices.com/resources/blog/bbns/2018/04/30/802.11-wireless-standards-explained

CANO, Jeimy. Ciberataques en Colombia ¿Está Colombia preparada para uno? [en línea]. 2022. [Consultado: 21 de mayo 2022]. Disponible en: https://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/

CASA EDITORIAL EL TIEMPO. ¿Colombia está preparada para repeler ataques cibernéticos? [En línea]. 2022. Disponible en: https://www.eltiempo.com/politica/gobierno/ataque-cibernetico-en-elecciones-gobierno-explica-medidas-en-colombia-657962

CONGRESO DE LA REPÚBLICA. [Sitio web]. Ley 1273 de 2009. [Consultado 21 de marzo de 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

DAULAY, Muhammad. ANALISIS WEP, WPA, WPA2, PADA ACCESS POINT. [En línea]. 2019. [Consultado: 21 de mayo de 2022]. Disponible en: http://repository.uir.ac.id/1775/

DIARIO LA REPUBLICA. PASTRAN, Alejandro. [Sitio web]. 2021, noviembre 12. Colombia superó los 8,2 millones de accesos fijos a internet en segundo trimestre. [Consultado: 21 de marzo de 2022]. Disponible en: https://www.larepublica.co/economia/colombia-supero-los-82-millones-de-accesos-fijos-a-internet-en-el-segundo-trimestre-3261097

DOMINGUEZ, Luis y VARELA, Carlos. Redes Inalámbricas. [en línea]. 2002. Universidad de Valladolid [Consultado: 21 de marzo 2022]. Disponible en: https://www.blyx.com/public/wireless/redesInalambricas.pdf

ECURED. Seguridad en redes inalámbricas. [en línea]. [Consultado: 21 de mayo 2022]. Disponible en: https://www.ecured.cu/Seguridad_en_redes_inal%C3%A1mbricas

FERNANDEZ, Lorena. Cómo funciona la escalada de privilegios y cómo protegernos [en línea]. 2020. [Consultado: 21 de mayo 2022]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/escalada-privilegios-que-es-funcionamiento/

FIRST ORGANIZATION - ICASI. [Sitio web]. Statement from the Industry Consortium for Advancement of Security on the Internet (ICASI) on the Wi-Fi Protected Access (WPA) Vulnerabilities. 2017, octubre 16. [Consultado 21 de marzo de 2022]. Disponible en: https://www.icasi.org/wi-fi-protected-access-wpa-vulnerabilities/

GCFGlobal. Seguridad en internet: Seguridad en redes wifi. [en línea]. 2020. [Consultado: 21 de mayo 2022]. Disponible en: https://edu.gcfglobal.org/es/seguridad-en-internet/seguridad-en-redes-wifi/1/

GOMEZ, Álvaro. Enciclopedia de la Seguridad Informática. Grupo Editorial RA-MA, 2011. ISBN 8499643949, 9788499643946

GONZALEZ, Georgina. The 25 most common passwords. [en línea]. 2022. [Consultado: 21 de mayo 2022]. Disponible en: https://www.beckershospitalreview.com/cybersecurity/the-25-most-common-passwords.html

GONZÁLEZ-MARRÓN, David, PÉREZ-HERNÁNDEZ, Iridian, MARQUÉZ-CALLEJAS, Alejandro y BADILLO-PAREDES, Leonardo. Análisis de vulnerabilidades en redes

inalámbricas instaladas en diversos municipios del Estado de Hidalgo. [en línea]. 2017, septiembre. [Consultado: 21 de abril 2022]. Disponible en: https://www.ecorfan.org/spain/researchjournals/Tecnologia_Informatica/vol1num2/Revista_de_Tecnologia_Informatica_V1_N2_5.pdf

GUERRERO-SANCHEZ, Andres Camilo y PEREZ-GARCIA, Jeimy Tatiana. Bogotá Wardriving (Spanish). [en línea]. 2020, octubre 1. [Consultado: 21 de abril 2022]. Disponible en: https://www.youtube.com/watch?v=_ehjol02UAs

IEEE 802.11. [Sitio web]. The Working Group Setting the Standards for Wireless LANs. [Consultado: 21 de marzo de 2022]. Disponible en: https://www.ieee802.org/11/

INDIRA, Reddy y V. Srikant. Review on Wireless Security Protocols WEP, WPA, WPA2 & WPA3. [En línea]. 2019. ISSN 2456-3307. Disponible en: https://doi.org/10.32628/CSEIT1953127

IONOS. [Sitio web]. ARPANET: Los primeros pasos de Internet. [Blog]. [Consultado 21 de marzo de 2022]. Disponible en: https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/arpanet-los-inicios-de-internet/

KUMAR, Vishal, TIWARI, Akhil, TIWARI, Pawan, GUPTA, Ashish y SHRAWNE, Seema. [Sitio web]. Vulnerabilities of Wireless Security protocols WEP and WPA2. [Consultado: 21 de marzo de 2022]. Disponible en: https://dl.irstu.com/wp-content/uploads/Download/Education/Book/Network/Network%20Security/WEP-WPA-Article/Vulnerabilities%20of%20Wireless%20Security%20protocols.pdf

LASHKARI, Arash Habibi, DANESH, Mir Mohammad Seyed y SAMADI, Behrang. [Sitio web]. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). 2009, 2vol IEEE International Conference on Computer Science and Information Technology, 48-52. [Consultado: 21 de marzo de 2022]. ISBN 978-1-4244-4519-6. Disponible en: https://doi.org/10.1109/ICCSIT.2009.5234856

LI, Jikai, ZEIGLER, Ethan, HOLLAND, Thomas, PAPAMICHAIL, Dimitris, GRECO, David, GRABENTEIN, Joshua, y LIANG Daan. [En línea]. 2020. ISBN 978-3-030-45690-0. Disponible en: https://link.springer.com/chapter/10.1007/978-3-030-45691-7_77

LOUNIS, K. y ZULKERNINE, M. WPA3 Connection Deprivation Attacks. [En línea]. 2020, pág. 164-176. [Consultado: 21 de marzo de 2022]. ISBN 978-3-030-41567-9, 978-3-030-41568-6. Disponible en: https://doi.org/10.1007/978-3-030-41568-6_11

MARÁCZI, Máté. Wardriving in Eger. [En línea]. 2019. ISBN 978-1-7281-0686-1. Disponible en: https://ieeexplore.ieee.org/document/9111489/authors#authors

MONSALVE-PULIDO, Julián Alberto, APONTE-NOVOA, Fredy Andrés y CHAPARRO-BECERRA, Fabián. Security analysis of a WLAN network sample in Tunja- Boyacá-

Colombia.pdf. [en línea]. 2014, mayo 2. [Consultado: 21 de marzo 2022]. Disponible en: http://www.scielo.org.co/pdf/dyna/v82n189/v82n189a28.pdf

OUGHTON, Edward J., KUSUMA, Julius, PEYRONEL, Thibault y CROWCROFT Jon. [En línea]. 2021. Disponible en: https://arxiv.org/abs/2101.06301v2

PACHÓN, Camila. 2021. Los Ciberataques más famosos del 2021 en Colombia y el mundo [En línea]. 2021. Disponible en: https://www.nsit.com.co/los-ciberataques-mas-famosos-del-2021-en-colombia-y-el-mundo/

PANDA SECURITY MEDIACENTER. [Sitio web]. Wardriving: ¿What Is It + How Can You Detect It?. 2020, noviembre 13. [Consultado 21 de marzo de 2022]. Disponible en: https://www.pandasecurity.com/en/mediacenter/security/wardriving/

PAUS, Lucas. [Sitio web]. Wardriving, ¿un censo digital de redes Wi Fi? [Consultado 21 de marzo de 2022]. Disponible en: https://www.welivesecurity.com/la-es/2017/01/06/wardriving-censo-digital/

PEREZ-VAQUERO, Carlos. [Sitio web]. El delito tecnológico del wardriving. 2014, diciembre 30. [Consultado 21 de marzo de 2022]. Disponible en: https://cpvaquero.blogspot.com/2014/12/el-delito-tecnologico-del-wardriving-en.html

POLOCHE-ZABALA, Miguel Angel. Evadiendo Protocolos de Cifrado Wep, Wpa y Wpa2 En Ambientes Reales, Implicaciones y Contramedidas. [En línea]. 2018. Disponible en: https://repository.udistrital.edu.co/handle/11349/13485

QUIÑONEZ-SOLÓRZANO, Jorge Andrés y PALOMEQUE-CRESPO, Isamar Adriana. Auditoria de seguridad de redes inalámbricas con encriptación wep, wpa y wpa2 utilizando la placa de arduino wifi-jammer y la metodología owisam para la empresa Importecell ubicado en el Cantón el Triunfo perteneciente a la provincia del Guayas. [En línea]. 2018. Disponible en: http://repositorio.ug.edu.ec/handle/redug/32560

RANCHAL, Juan. Razer Synapse y los privilegios de administrador en Windows. [En línea]. 2021. Disponible en: https://www.muyseguridad.net/2021/08/24/razer-synapse-administrador/

REVISTA SEMANA. El año de los ciberataques en Colombia, estas son las alarmantes cifras. [En línea]. 2022. Disponible en: https://www.semana.com/economia/empresas/articulo/el-ano-de-los-ciberataques-en-colombia-estas-son-las-alarmantes-cifras/202125/

RODRÍGUEZ-CORREA, Jose Ramiro. Wi-me: sistema de medición de seguridad de redes inalámbricas con protocolo wep, wpa y wpa2 utilizando wardriving, wireless penetration testing y otras herramientas en un sector del distrito de víctor larco herrera -

trujillo. [en línea]. 2019. [Consultado: 21 de abril 2022]. Disponible en: http://repositorio.uss.edu.pe//handle/20.500.12802/6255

RODRIGUEZ-GIJÓN, Mariano. GISAT. Análisis de redes inalámbricas en la ciudad de Cuenca mediante Wardriving. [en línea]. 2016. [Consultado: 21 de abril 2022]. Disponible en: https://ruidera.uclm.es/xmlui/handle/10578/11596

SANTOS, Fabián, PESANTES, Pablo y BONILLA-BEDOYA, Santiago. Exploring Wardriving Potential in the Ecuadorian Amazon for Indirect Data Collection [En línea]. 2021. Disponible en: 10.1088/1755-1315/690/1/012054.

SOPHOS. Seguridad para redes inalámbricas sincronizada. [En línea]. 2021. Disponible en: https://www.sophos.com/es-es/products/secure-wifi

THEORETISCHE, Fachgebiet, TERM, Summer, INFORMATIK, Fachbereich, DARMSTADT, Tu y TEWS, Erik. Attacks on the WEP protocol. [en línea]. 2007. [Consultado: 21 de abril 2022]. Disponible en: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.420.5739&rep=rep1&type=pdf

ZAIDAN, Doaa Talib. Analyzing Attacking Methods on Wi-Fi Wireless Networks Pertaining (WEP, WPA-WPA2) Security Protocols. [En línea]. 2021. ISSN: 2303-4521 Disponible en: http://pen.ius.edu.ba/index.php/pen/article/view/2545

ZHAO, Yurong. Wireless Network Security Status in Oulu: War-Driving. [En línea]. 2019. Disponible en: http://jultika.oulu.fi/Record/nbnfioulu-201906212615

9. ANEXO

9.1. RESUMEN ANALITICO ESPECIALIZADO

Fecha de Realización:	22/09/2022
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Título:	Análisis de los protocolos de seguridad inalámbrica implementadas en las redes wifi en la ciudad de Bogotá
Autor(es):	Perez Garcia, Jeimy Tatiana
Palabras Claves:	WarDriving, WEP, WPA, WPA2, WPA3
Descripción:	Las personas se enfrentan cada día a retos más diversos con el uso de internet. El auge de nuevas tecnologías, dispositivos y el crecimiento del tiempo en la navegación en internet a causa de la pandemia ha generado que no solo haya personas con mayor acceso a la información, sino que también los ciberdelincuentes puedan aprovechar su deficiente conocimiento del tema para tomar provecho y efectuar cualquier tipo de ataque. Este documento contiene la investigación de los tipos de protocolo de seguridad que usan las redes inalámbricas en Bogotá mediante el uso de la técnica de WarDriving, una cuantificación los protocolos y una explicación de estos; así como, los riesgos de seguridad a los que se encuentran expuestos los usuarios por la explotación de las redes a causa del uso de protocolos de seguridad deficientes en las conexiones WiFi y cuáles son las contramedidas que se pueden tener en cuenta para evitar que los ciberdelincuentes tengan éxito.
Fuentes bibliográficas destacadas: AIRCRACK-NG ORG. [Sitio web]. Airodump-ng [Consultado: 21 de abril 2022]. Disponible en: https://www.aircrack-ng.org/doku.php?id=es:airodump-ng ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS. [Sitio web]. Cifras de ciberseguridad en Colombia prenden alarmas al cierre del 2020. [Consultado 21 de marzo de 2022]. Disponible en:	

<table>
<tr><td colspan="2">https://acis.org.co/portal/content/noticiasdelsector/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020
BLACK BOX CORPORATION. [Sitio web]. The Evolution of 802.11. [Consultado 21 de marzo de 2022]. Disponible en: https://www.bboxservices.com/resources/blog/bbns/2018/04/30/802.11-wireless-standards-explained
CONGRESO DE LA REPÚBLICA. [Sitio web]. Ley 1273 de 2009. [Consultado 21 de marzo de 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
GUERRERO-SANCHEZ, Andres Camilo y PEREZ-GARCIA, Jeimy Tatiana. Bogotá Wardriving (Spanish). [en línea]. 2020, octubre 1. [Consultado: 21 de abril 2022]. Disponible en: https://www.youtube.com/watch?v=_ehjol02UAs
IEEE 802.11. [Sitio web]. The Working Group Setting the Standards for Wireless LANs. [Consultado: 21 de marzo de 2022]. Disponible en: https://www.ieee802.org/11/</td></tr>
<tr><td>Contenido del documento:</td><td>En el documento se especifica el procedimiento que se debe tener en cuenta si una persona quiere hacer reconocimiento de redes IEEE 802.11.x que se encuentren en una zona determinada por medio del uso de la técnica WarDriving. En donde se indican las diferentes alternativas que se pueden tener en cuenta, software y hardware para llevar a cabo el reconocimiento.
Tras la recopilación de estos datos, se deben presentar de manera organizada para enumerar y cuantificar los tipos de señales inalámbricas detectadas y los protocolos de seguridad detectados en las redes IEEE 802.11x, de esta manera con cifras reales, entender cuál es el panorama actual en la ciudad con respecto a la seguridad en redes inalámbricas y el uso de los diferentes tipos de redes y protocolos.
Una vez listados los diferentes protocolos y tipos de redes, se procede con el análisis de las vulnerabilidades que se derivan del uso de los diferentes protocolos obsoletos que se encuentran activos por la ciudad, de esta manera enumerar las diferentes fallas y posibles consecuencias que podrían generarse en las redes que hacen uso de estos protocolos.</td></tr>
</table>

	Se encuentra una demo en la que se muestra como IEEE 802.11 más obsoleta se puede vulnerar mediante el uso de diferentes herramientas en Kali Linux; teniendo en cuenta que, a pesar de ser obsoleta se encuentran más de 3000 redes inalámbricas en la ciudad de Bogotá. Finalmente se ofrecen las recomendaciones que pueden ayudar a mitigar estos ataques, en donde se pueden encontrar el uso de redes IEEE 802.11 con el protocolo WPA3; así como, otras recomendaciones relacionadas a buenas prácticas como el uso de autenticación multifactor.
Marco Metodológico:	Se hará uso de señales Wi-Fi recopiladas aleatoriamente por la ciudad de Bogotá como población objetivo; en donde, se aplicará la técnica de escaneo de redes llamada WarDriving. La técnica Wardriving recopila la data de las redes inalámbricas mediante el uso de distintos dispositivos de escaneo para lograr la mayor cantidad de recolección de información, estos dispositivos pueden ser: antenas WiFi, computadores, dispositivos móviles como tabletas y smartphones, que usarán el software Wigle o Kismet para interpretar y almacenar dichas señales WiFi para su posterior análisis y uso dentro de la investigación en curso. El tipo de investigación se considera como: Investigación aplicada tecnológica e Investigación descriptiva. Para la investigación se empleará el diseño investigativo basado en la recopilación, análisis y presentación de datos que permita entender la problemática explicada y la descripción cuantitativa de esta. La población son las redes inalámbricas al alcance de las antenas y dispositivos dispuestos para el escaneo en algunas zonas de frecuente tráfico de Bogotá.
Conceptos adquiridos:	Conocimiento sobre las diferentes actualizaciones y la importancia de la norma IEEE 802.11. Las vulnerabilidades y principales ciberataques relacionados al uso de protocolos

	de seguridad débiles en las redes inalámbricas. El uso de la suite de Aircrack-ng para hacer auditorias de redes WiFi. Datos estadísticos sobre los tipos de redes que se encuentran en la ciudad.
Conclusiones:	Al finalizar con el desarrollo de esta actividad se logró verificar que el estado de seguridad en las redes inalámbricas de la ciudad de Bogotá, se encuentra en un estado deficiente y que requiere especial atención para el desarrollo de las empresas; teniendo en cuenta los hallazgos presentados en donde gran parte de las señales de WiFi WEP y WPA2 basándonos en el SSID de la red corresponden a redes corporativas de pequeñas y medianas empresas de diferentes sectores de la industria local y nacional. Se ha evidenciado que cada día existen más proyectos de impacto TIC y de inclusión en el mundo de la informática; así que es importante empezar a tenerlos en cuenta para un correcto y competitivo avance dentro del mundo de la tecnología, de la ciberseguridad y de las compañías frente a normativas. Ya que desde los últimos años se ha venido exigiendo cada vez más un nivel de calidad optimo dentro de las compañías, que salvaguarden la integridad, la confidencialidad y la disponibilidad de la información como con la normativa presentada por la ISO 27001. Según los hallazgos se pudo notar con datos estadísticos que las redes inalámbricas son una potencial fuente de riesgos en todos los entornos y han estado desatendidas; por lo que, es necesario y primordial no dejar a un lado la seguridad en las redes inalámbricas así en muchos casos sea desestimada porque no se ha considerado importante o de impacto; bien sea por desconocimiento de las posibles consecuencias y que pueden resultar en pérdidas de información y el enfrentamiento de diferentes consecuencias a varios niveles para los actores que intervienen.