UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TÍTULO DEL TRABAJO DE TITULACIÓN

ANÁLISIS DE SEGURIDAD MEDIANTE TÉCNICAS DE CIBERSEGURIDAD EN REDES INALÁMBRICAS 802.11 PARA MITIGAR ATAQUES INFORMÁTICOS EN AMBIENTE CONTROLADO

AUTOR

González Balón Ricardo Rubén

MODALIDAD: EXAMEN COMPLEXIVO

Previo a la obtención del grado académico en

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

Lsi. Daniel Quirumbay Yagual.

Santa Elena, Ecuador

Año 2024

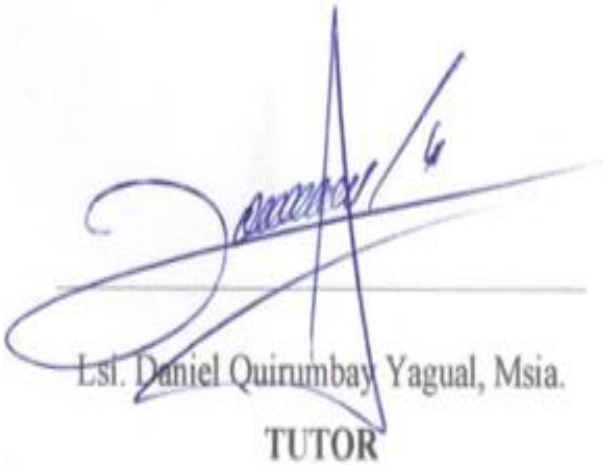
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino, Mgt.

DIRECTOR DE LA CARRERA



Lsi. Daniel Quirumbay Yagual, Msia.

TUTOR

Ing. Jaime Orozco Iguasnia, Mgt

DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez, Mgt

DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por GONZÁLEZ BALÓN RICARDO RUBÉN, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 25 días del mes de junio del año 2024

TUTOR

Firmado electrónicamente por:
DANIEL IVAN
QUIRUMBAY YAGUAL

Lsi. Daniel Quirumbay Yagual, Msia.

UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **González Balón Ricardo Rubén**

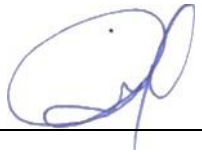
DECLARO QUE:

El trabajo de Titulación, Análisis de seguridad mediante técnicas de ciberseguridad en redes inalámbricas 802.11 para mitigar ataques informáticos en ambiente controlado previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 25 días del mes de junio del año 2024

EL AUTOR



Ricardo Rubén González Balón

UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado análisis de seguridad mediante técnicas de ciberseguridad en redes inalámbricas 802.11 para mitigar ataques informáticos en ambiente controlado, presentado por el estudiante, GONZÁLEZ BALÓN RICARDO RUBÉN fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 2%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS
magister

TI_RICARDO_RUBEN_GONZALEZ_BALON

2%
Textos sospechosos

2% Similitudes
2% similitudes entre comillas
< 1% entre las fuentes mencionadas
< 1% Idiomas no reconocidos

Nombre del documento: TI_RICARDO_RUBEN_GONZALEZ_BALON.pdf
ID del documento: 239fec24e11e1ccb883ad89a8b7889424d75b54d
Tamaño del documento original: 3,53 MB

Depositante: DANIEL IVAN QUIRUMBAY YAGUAL
Fecha de depósito: 21/6/2024
Tipo de carga: interface
fecha de fin de análisis: 21/6/2024

Número de palabras: 16.200
Número de caracteres: 112.133

Ubicación de las similitudes en el documento:

TUTOR

Firmado electrónicamente por:
DANIEL IVAN QUIRUMBAY YAGUAL

Lsi. Daniel Quirumbay Yagual, Msia.

UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

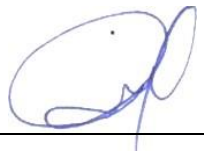
Yo, **GONZÁLEZ BALÓN RICARDO RUBÉN**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del trabajo de titulación con fines de difusión pública, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 25 días del mes de junio del año 2024

EL AUTOR



Ricardo Rubén González Balón

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a Dios por darme la fortaleza y la perseverancia necesarias para llegar a este momento tan importante en mi vida. Gracias por guiarme y ayudarme a superar todas las adversidades que se me han presentado en el camino, permitiéndome así alcanzar una de mis metas más anheladas.

Asimismo, quiero agradecer a mis amados padres, Miguel González Caiche y Lourdes Balón Panchana, por su apoyo incondicional y su orientación a lo largo de mi formación académica. Gracias por estar siempre ahí para mí, por brindarme su atención y ser ese soporte fundamental en mi vida.

Por último, quiero expresar mi profundo agradecimiento a todos los profesores que han contribuido a mi desarrollo académico, compartiendo generosamente sus conocimientos y experiencias, y guiándome para lograr culminar con éxito mi formación. Gracias por haber sido parte de este importante logro en mi vida.

Ricardo Rubén, González Balón

DEDICATORIA

Con gran alegría y gratitud, dedico este trabajo a mis amados padres Miguel González Caiche y Lourdes Balón Panchana, ustedes han sido el pilar fundamental en mi vida, brindándome su incondicional amor, apoyo y guía a lo largo de mi formación.

Extiendo esta dedicatoria a toda mi familia, a mis seres queridos y a todas las personas que han formado parte de este trayecto. Gracias especialmente a María Jimena Suárez Tomalá por su cariño, sus palabras de aliento y por haber estado presentes en cada uno de mis logros. Su presencia y su apoyo han sido fundamentales para poder cumplir con esta meta tan importante en mi vida.

Este trabajo es para ustedes, quienes han sido un pilar inquebrantable en mi camino. Espero que este logro los llene de orgullo y satisfacción, pues sin su amor y respaldo, nada de esto hubiera sido posible.

Ricardo Rubén, González Balón

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La seguridad de las redes inalámbricas se ha convertido en una preocupación importante para nuestra sociedad en entornos tecnológicos. A medida que se incrementa el uso de los dispositivos móviles ha aumentado, así mismo lo hacen las conexiones inalámbricas para transmitir información crítica, y es vital el resguardo de los datos e información que circula por estas redes. Esta investigación presenta un robusto análisis de seguridad en redes 802.11 a través de la aplicación de la metodología PTES orientada a la ciberseguridad con el objetivo de detener los ataques cibernéticos que comprometen los datos a través de la violación de la confidencialidad, integridad y disponibilidad de estos, los efectos y causas detrás de los ataques cibernéticos a las redes inalámbricas y las debilidades y vulnerabilidades de los protocolos de seguridad.

Adicionalmente, se emplearán técnicas sofisticadas de hacking ético que permiten proteger la seguridad de las redes. Se utilizarán los escenarios de pruebas y simulaciones en el estudio de caso para determinar cuál de las técnicas, ataques y herramientas es más eficaz para su implementación. También en base a los resultados, se formularán la mejores recomendaciones y guías para la mejora de la seguridad de las redes 802.11 y la minimización de los riesgos de su ataque.

Palabras claves: ciberseguridad, ataques informáticos, redes inalámbricas, 802.11.

ABSTRACT

The security of wireless networks has become an important concern for our society in technological environments. As the use of mobile devices has increased, so have wireless connections to transmit critical information, and safeguarding the data and information that circulates through these networks is vital. This research presents a robust security analysis in 802.11 networks through the application of the PTES methodology oriented to cybersecurity with the objective of stopping cyber attacks that compromise data through the violation of confidentiality, integrity and availability of these , the effects and causes behind cyber attacks on wireless networks and the weaknesses and vulnerabilities of security protocols.

Additionally, sophisticated ethical hacking techniques will be used to protect the security of the networks. The test scenarios and simulations in the case study will be used to determine which of the techniques, attacks and tools are most effective for implementation. Also based on the results, the best recommendations and guides will be formulated to improve the security of 802.11 networks and minimize the risks of their attack.

Keywords: cybersecurity, computer attacks, wireless networks, 802.11.

INTRODUCCIÓN

El contexto de las redes inalámbricas este estudio de análisis es basado en los estándares principales 802.11, estos son conocidas como Wifi, esta tecnología se ha convertido en una herramienta que ofrece confort a los usuarios con sus dispositivos en ámbitos comunicación inalámbrica. En general, estas redes presentan desafíos e incertidumbres por lo que son considerados en ámbitos de seguridad algo importante, en la mayoría de los casos son vulnerables y son vulnerables a tipos de ataques cibernéticos.

Como mencionamos anteriormente esta investigación se centra en realizar un análisis de tipo auditoria en seguridad en redes inalámbricas, así mismo la utilización de técnicas en ciberseguridad en ambientes controlados y seguros con ayuda de las máquinas virtuales. El objetivo de este trabajo de investigación es evaluar, analizar e identificar vulnerabilidades en los protocolos de comunicación inalámbrica, de lo cual propone estrategias efectivas como el del desarrollo de informe de recomendaciones para mitigar los riesgos y reforzar la protección de la información que circula a través de estas redes.

Basado en un enfoque metodológico se dará cumplimiento con el estándar de pruebas de penetración PTES, se procederá mediante una interacción previa, recopilación de información, modelado de amenazas, análisis de vulnerabilidad, explotación, post explotación y reporte. Estos permitirán comprender una manera puntual los puntos débiles de los protocolos de seguridad, las causa detrás de esta investigación fue principales por la falta seguridad en la construcción de las contraseñas o claves de acceso. Desde cualquier punto de vista de los ataques efectuados a las redes inalámbricas pueden ser consideradas graves por lo que pueden poner en riesgo la confidencialidad, integridad y disponibilidad de la información.

La evaluación de seguridad en este ámbito controlado se volvió importante y fundamental para reducir e identificar vulnerabilidades de una manera anticipada, esto permitirá salvaguardar diversos riesgos que comúnmente son asociados a los ciberataques en ambientes inalámbricas.

CAPÍTULO 1. FUNDAMENTACIÓN

1.1 ANTECEDENTES DEL PROYECTO

Las redes inalámbricas comúnmente se la denomina wifi, se ha vuelto importante para diversos entornos como en negocios, hogares y sobre todo en espacios públicos, esta convivencia con la tecnología se ha convertido en soluciones de conectividad adaptada a las necesidades de las personas, no obstante, se han generado preocupaciones en que tan seguras son las redes inalámbricas porque estas presentan vulnerabilidades en comparación con las redes alámbricas, surge la necesidad de darle una garantía en seguridad a las redes inalámbricas es surgido por lo que existe diversos ataques cibernéticos que por lo general son expuestas, como ataques de fuerza bruta, atauques de diccionario e inclusos aplicación de ingeniería social[1].

Mediante el uso del internet se abre un abanico lo cual hace que aparezcan nuevas tendencias tecnológicas tanto en el ámbito de seguridad y social de lo cual hace que tengamos una mayor facilidad en nuestras vidas en diferentes ámbitos, pero a su vez el internet y las comunicaciones tienen sus ventajas y desventajas por lo que hay que considerar técnicas y métodos con el fin de poder conocer este tipo, forma o manera en la que trabajan los ciberdelincuentes[2].

Es de suma importancia tratar este tipo de acciones que realizan los ciberdelincuentes indispensablemente de que ataque informático realicen, por lo que cada ataque es considerado critico por el robo de datos personales, así mismo se considera el aspecto legal para quienes roban o hacen mal uso de la información de usuarios[3].

El artículo científico tecnológico "*Análisis de rendimiento de redes inalámbricas asistidas por RIS en presencia de errores de fase imperfectos"* indica que, en un ambiente de posibles amenazas, por lo que los dispositivos con sensores que trasmiten datos en donde podrían ser aprovechados por los delincuentes informáticos planeando ataques informáticos podrían dañar la reputación de las empresas y de los usuarios[4].

La tesis *"Análisis de vulnerabilidad en la red LAN usando herramientas de hacking ético para una empresa de la provincia de Santa Elena"* en el ámbito de las tecnologías, la información y los datos están en constante evolución por lo que las empresas tanto privadas como públicas deben considerar proteger los sistemas de seguridad de los ataques informáticos, en el momento de que los usuarios navegan en internet los posibles ataques podrían ser de diferentes formas y aplicando métodos por lo que pude poner en riesgos información como por ejemplos claves de usuarios e incluso credenciales, el objetivo de este estudio es poder proporcionar información a los usuarios de las amenazas más comunes que podrían presentarse en el momento de que algún usuario navega por una red privada o pública[5].

Por otro lado, la tesis *"Análisis De Vulnerabilidades De La Red Inalámbrica Para Mitigar La Inseguridad De Ataque Informáticos"* nos dice en la actualidad se recomienda tener las redes inalámbricas seguras por motivo que amenazas cibernéticas que están cada día evolucionando obligando a las empresas y a los usuarios a tomar en consideraciones políticas básicas en la que permitan minimizar ataques de carácter informático[6].

Es necesario tener conocimientos de cómo y cuáles son los ataques más frecuentes de los ciberdelincuentes con el fin de poder contrarrestar o tratar de impedir que las personas tengan algún tipo de altercado con este tipo de situación, cabe mencionar muchos de los ataques de robo de información es usada con fines a dañar la integridad social y emocional tanto a la persona u organización[7].

Los temas antes citados con fundamentación teórica son de gran ayuda para la realización de este presente proyecto, la mayoría tienen distintas formas de realizar o de proceder en la ejecución del mismo, pero todos conllevan a alcanzar el mismo objetivo que es tratar de mitigar ataques informáticos[8].

1.2 DESCRIPCIÓN DE PROYECTO

Al no estar vigente algún tipo de información clara y precisa a este tipo de conectividad inalámbrica wifi que afronte la seguridad de los datos, se ve muy comprometido la integridad de los datos y sobre todo la falta de compromiso por parte de las organizaciones, por la falta de tiempo en poder detectar anomalías que

conlleven incidentes tanto en el robo de información, así como otros percances informáticos por lo que no hay una respuesta inmediata es por este motivo que surge la necesidad de exponer un control y manejo en los ámbitos de ciberseguridad, realizado mediante la metodología PTES de lo cual consta de una estructura con bases de prueba de inteligencia con herramientas tecnológicas y técnicas orientadas a poder valorar o estimar la seguridad de las redes inalámbricas[9].

Las prácticas de test de penetración están plenamente relacionadas en ambientes en donde existen una mayor relevancia en incidentes informáticos, por lo que se puede conocer mediante un análisis que tanto es la efectividad o el nivel de daño que podrían ocasionar estos tipos de ataques. Por ende, el estudio de técnicas de seguridad debe ser preciso y que además por medio de buenas prácticas, se pretende disminuir la brecha que podrían existir en la seguridad en las redes wifi, este proyecto se lo realizará mediante una metodología PTES (Penetration Testing Excecution Standard) de lo cual cuenta con las siguientes fases que contendrá este proyecto[10].

FASE 1: INTERACCIÓN PREVIA

Definir alcance del proyecto:

- Identificar que las redes 802.11 serán objeto de análisis.
- Especificar el tipo de ataque.

Recursos:

- Identificar hardware, software y herramientas de ciberseguridad.

Acuerdos y permisos:

- Obtener autorizaciones y permisos.

FASE 2: RECOLECCIÓN DE INFORMACIÓN

- Recopilación de información
- Conectividad inalámbrica
- Debilidades más comunes a las redes.
- Entorno tecnológico

FASE 3: MODELADO DE AMENAZAS

- Investigación sobre ataques y amenazas en redes.
- Determinación de facilidad de explotación.

FASE 4: ANÁLISIS DE VULNERABILIDADES

- Detección, actividad, debilidades de cobertura, cifrado de red.
- Identificaciones de redes inalámbricas ocultas

FASE 5: EXPLOTACIÓN

- Fuerza bruta
- Descifrar contraseñas

FASE 6: POST- EXPLOTACIÓN

- Evaluar el alcance del ataque
- Evaluar acciones que se podrían realizar
- Búsqueda de información personal

FASE 7: INFORME

- Análisis de la seguridad de la red
- Técnicas utilizadas
- Recomendaciones para una mayor seguridad

1.3 OBJETIVOS

1.3.1 OBJETIVOS GENERAL

Elaborar un análisis a los protocolos de seguridad a redes wifi con el fin de disminuir ataques informáticos que atenten con la privacidad de los datos personales mediante técnicas de ciberseguridad.

1.3.2 OBJETIVOS ESPECÍFICOS

- Comparar las vulnerabilidades de los protocolos de comunicación inalámbrica 802.11 para determinar el nivel de riesgo siguiendo el enfoque PTES.
- Evaluar mediante el estándar PTES la efectividad de las herramientas de hacking ético en el descifrado de contraseñas en redes inalámbricas.

- Desarrollar un informe de análisis de protección y recomendaciones en redes inalámbricas basada en la seguridad de la información.

1.4 JUSTIFICACIÓN

Es primordial y necesario saber que la seguridad en las redes inalámbricas de conectividad wifi tiene sus riesgos por lo que se exponen los datos e información crucial para las personas que se conectan a este tipo de redes, muy pocas personas tienen el conocimiento del posible riesgo que toman a establecer una conexión de sus dispositivos móviles o portátiles a dichas redes, gracias a este trabajo de investigación se podrá disminuir amenazas y a soluciones de vulnerabilidad, además es necesario tener conciencia sobre lo que es la seguridad informática[11].

Por lo cual nace esta investigación con el único propósito de evaluar y analizar, vulnerabilidades que posiblemente presenten los protocolos de seguridad en redes inalámbricas, además de poder alertar sobre ataques informáticos y posibles intrusos dado que sus objetivos es poder vulnerar la seguridad[12].

Esta presente investigación tendrá una relevancia social que involucró a los dueños y administradores de redes inalámbricas por lo que verán beneficios en las tecnologías dando una mejor seguridad de los datos y además vigilancia sobre usuarios no reconocidos en la red. Además de implicar pruebas de penetración, análisis de redes y tráfico de datos, es de mucha importancia social por lo que involucra proteger información y privacidad, dichas medidas son indispensables para poder disminuir riesgos de ataques de ciberdelincuentes[13].

Con esta investigación obtendremos nuevos conocimientos en la que aseguremos la información que circulan en las redes, esto servirá como base para posteriores estudios investigativos, este proyecto también engloba a realizar procedimientos de buenas prácticas que incorpore técnicas de aplicación de hacking ético que ayuden a evaluar la seguridad de las redes y por lo consiguiente evaluar el nivel de incidencia, poder disminuir y solucionar amenazas que podrían realizar los ciberdelincuentes, así mismo tener beneficios como minimizar algún tipo de riesgo de delito informático, proteger datos privados que se podrían filtrar[14].

En la actualidad las redes inalámbricas no son lo suficiente seguros a menos que exista una configuración adecuada de los equipos, es por esos que se considera realizar un análisis exhaustivo sobre los diferentes escenarios sobre la problemática, se pretende crear ambientes virtuales lo cual nos permitirá evaluar la seguridad de la red y además de los protocolos de conectividad con el fin de garantizar a los usuarios la seguridad de sus datos cuando se navegue por una red, se considera dar solución de una manera sencilla y esencial para gestionar el correcto uso de las comunicaciones inalámbricas y la seguridad de la información[15].

El objetivo es proporcionar confianza, integridad y seguridad a las redes de conectividad inalámbrica, este estudio permite mejorar la seguridad y conocer sobre nuevas formas de ataques informáticos más comunes, evaluar mediante técnicas de seguridad informática, medir el grado de efectividad que podría ocasionar ciertos ataques, además identificar algunos puntos débiles en el proceso de análisis de seguridad[16].

OBJETIVOS DEL PLAN DE CREACIÓN DE OPORTUNIDADES

La presente propuesta está direccionado al plan de creación de oportunidades, haciendo énfasis al eje relevante, en la cual detalla lo siguiente[17]:

EJE SEGURIDAD INTEGRAL

Objetivo 6: Garantizar el derecho a la salud integral, gratuita y de calidad.

Política 6.1-A8: Ampliar la cobertura de servicios para atender a las localidades rurales, especialmente aquellas ubicadas en sitios alejados con baja conectividad a los centros urbanos.

Objetivo 10.- Garantizar la soberanía nacional, integridad territorial y seguridad del Estado.

Política 10.1: Fortalecer al estado para mantener la confiabilidad, integridad y disponibilidad de la información frente a amenazas provenientes del ciberespacio y proteger su infraestructura crítica.

1.5 ALCANCE DEL PROYECTO

La propuesta de análisis de seguridad de a redes inalámbricas por medio de técnica de ciberseguridad, permitirá realizar un análisis profundo al momento de monitorear anomalías en este tipo de redes de fácil acceso, es por eso que mediante ambientes de simulación en máquinas virtuales que sean puestas a posibles vulnerabilidades con el fin de poder exponer dichas brechas de seguridad en conectividades inalámbricas wifi[18].

El desarrollo de esta investigación se la realizará usando la metodología PTES, se detallará cada actividad que tendrá la investigación por lo cual tendremos una visión clara y precisa, en esta primera fase de recolección de información nos centraremos en el levantamiento de información en donde la información recolectada se trata sobre los protocolos y estándares conocer las debilidades, amenazas y vulnerabilidades comunes que podrían presentar las redes inalámbricas, en la segunda fase de análisis de vulnerabilidades analizaremos mediante herramientas de hacking ético a las redes inalámbricas, este tipo de análisis será de tipo auditoría, el resultado de esto es conocer información de la red como, nombre de la red, si la red es visible o de configuración oculta, el canal de frecuencia en que trabaja, además la intensidad de señal que emite la red entre otras características[19].

En esta tercera fase se procederá mediante simulación experimental técnicas de ciberseguridad sobre algunas categorías orientadas a estudios, además proceder a diseñar ámbitos y escenarios en donde se ejecutarán pruebas en donde poder analizar las amenazas posibles que se presenten en cada ámbito con entornos simulados, en donde evaluaremos el tiempo que tarda el ciberdelincuente en realizar el ataque[20].

En esta cuarta y quinta fase se presentan diferentes formas y métodos de explotación que tiene como objetivo tener un mayor privilegio, es decir acceder a la red mediante un ataque especifico fuerza bruta o denominado ataque de diccionario, es por eso que la información que podamos recopilar en la fase anterior, analizar de una manera más detallada con el fin de poder obtener datos de diferentes ambientes post- explotación mediante análisis de técnicas[21].

En las últimas fases se realizará un informe con los resultados que se han obtenido mediante los análisis de la fase de explotación y post explotación, en donde se realiza la explicación de los diferentes escenarios los procesos realizados, dando resultados, recomendaciones y observaciones de todas las practicas experimentales que se realizó en la presente investigación[22].

CAPÍTULO 2. MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1 MARCO CONCEPTUAL

RC4.- Es un algoritmo esquematizado antiguo y obsoleto su funcionalidad era mediante un cifrado simétrico, opera con un operador lógico OR, que va de byte a byte mediante procesos secuenciales de mensajes que varía según claves dinámicas este algoritmo se caracteriza por su facilidad, simplicidad y eficiencia, su seguridad es cuestionada por recibir diversos ataques[23].

PSK. – Sus siglas en inglés (Pre shared key) o clave previamente compartida con los dispositivos para que este tipo de conexión y la comunicación sea segura y estable, cuenta con un protocolo WPA que es una manera de autenticación entre la red y los dispositivos móviles así mismo garantiza la confidencialidad y la disponibilidad de los usuarios[24].

WEP. – Sus siglas en inglés (Wired Equivalent Privacy), la seguridad inalámbrica de este protocolo es obsoleto además utiliza un bajo nivel de seguridad, así mismo se considera alto en nivel de vulnerabilidad, este protocolo su característica era proporcionar un alto nivel de seguridad igual o similar a una red cableada, funcionaba con claves estáticas hexadecimal de 64 o 128 bits[25].

WPA. – Sus siglas en inglés (Wi-Fi Protected Access) funciona mediante la gestión de claves de seguridad y la autenticación de usuarios, utilizando avanzados métodos para verificar la identidad de cada dispositivo conectado, este protocolo incluye integridad en sus mensajes con el objetivo de detectar paquetes que si son o no alterados o modificados[26].

WPA2.- Sus siglas en inglés (Wi-Fi Protected Access 2) es la versión mejorada de WPA, es complicado realizarle un ataque y tener resultados positivos, funciona mediante el cifrado de datos con AES (Advanced Encryption Standard) es un sistema aprobado por el gobierno de los Estados Unidos[27].

PMK. – (Pairwise Master Key o Clave Maestra de Pareja) el PMK proporciona por medio de claves un proceso de autenticación única además de que es esencial para proporcionar una conexión segura y eficaz entre el usuario y el punto de acceso AP,

garantiza la confidencialidad y la integridad de los datos que se transmiten en la red inalámbrica[28].

MIC. –(Message Integrity Check o Comprobación de Integridad de Mensajes) Es un código de integridad que utilizan los mensajes es importante para verificar la autenticidad de los datos transmitidos, Esta función es crucial para mantener la seguridad y la confiabilidad de la comunicación en redes inalámbricas, ya que ayuda a detectar posibles intentos de intrusión o manipulación de datos durante la transmisión inalámbrica[29].

CCMP. – (Protocolo de modo de contador con cifrado de bloque encadenado y código de autenticación de mensaje) utiliza un algoritmo de cifrado basado en una clave y algoritmo de autentificación que permiten la protección de los datos en la red, es esencial para detectar manipulaciones o suplantaciones de datos en la red, además de que este algoritmo proporciona una seguridad robusta en dichas redes inalámbricas[30].

BEACON FRAMES. – Son envíos de paquetes hacia un punto de acceso la misma que contiene información sobre la red Wi-Fi, permitiendo a que los dispositivos cercanos puedan identificar el SID, detectar el nivel de señal y la cercanía entre otras características emitidas por la red, lo cual facilita la movilidad y la conectividad[31].

KRACK. – "Key Reinstallation Attacks" o "Ataques de Reinstalación de Clave", Es considerado un ataque crítico que compromete gravemente la seguridad de las redes WPA2/AES mediante reinstalación de claves o de cifrado, se basa en explotar la debilidad del handshake lo que permite a los atacantes acceder y espiar el tráfico de la red sin considerar conocer algún tipo de contraseña[32].

TKIP. - es un protocolo de seguridad con mayor seguridad a WEP, TKIP estos aspectos importantes que son clave para una mejor protección de los datos mediante la autentificación de cuatro vías de lo cual realiza una verificación para el cliente en el sitio de acceso wifi con una misma clave, vector de inicialización utiliza una longitud de 48 bits, el mismo que hace posible que la clave de acceso sea modificada[33].

AES. – sus siglas en inglés (Advanced Encryption Standard o Estándar de Cifrado Avanzado) fue creado con el objetivo de para mitigar incidencias o acciones prohibidas, cuenta con un cifrado en bloques, simetría y longitud en sus claves mayor a 128 bits y también trabaja con el algoritmo Rijndael que es un cifrado de tipo bloques seguro y eficiente[34].

Handshake. –utiliza procesos de autentificación que involucra al cliente en la manera de como verificar datos correctos lo cual garantiza una conexión confiable y segura, también podemos referirnos a los protocolos que utilizan para establecer una conexión que involucra la verificación de la identidad de los dispositivos[35].

WLAN. – sus siglas en inglés (Wireless Local Area Network) su manera de comunicación la realiza de manera inalámbrica los dispositivos se pueden conectar mediante una red wifi, lo que permiten la conexión inalámbrica de los dispositivos a través de ondas de radiofrecuencia, lo que brinda movilidad a los usuarios al eliminar la necesidad de cables físicos[36].

LAN. – sus siglas en inglés (Local Area Network), considerada como una red de comunicación que permite la conexión de dispositivos en un lugar limitado, utiliza una conexión de una manera cableada entre los dispositivos, estas redes permiten a los dispositivos comunicarse entre sí, compartir información y recursos, y acceder a Internet de forma local, además que proporciona altas velocidades de transferencia de datos, baja latencia, mayor seguridad, facilidad de instalación y mantenimiento[37].

2.2 MARCO TEÓRICO

2.2.1 ¿QUÉ ES LA CIBERSEGURIDAD?

Ciberseguridad es considera como prácticas a defender de las computadoras, dispositivos móviles entre otros en diferentes ámbitos, también se la conoce como la seguridad de la información electrónica o seguridad de tecnología de la información, es considerada aplicable a ciertas categorías orientadas a esta rama de la ciberseguridad como, por ejemplo, seguridad en redes, aplicaciones y seguridad de la información[38].

Así mismo la ciberseguridad se la denomina y es considerada como la seguridad informática respectivamente seguridad de la información electrónica, por otro lado, es una forma de proteger contra ataques informáticos de personas llamadas ciberdelincuentes[39].

La ciberseguridad cuenta con diferentes objetivos, detallados a continuación:

a. Garantizar la confidencialidad
b. Mantener una disponibilidad
c. Preservar la integridad

2.2.2 ¿QUÉ SON LAS REDES INALÁMBRICAS 802.11?

Las redes inalámbricas 802.11 hacen referencias a estándares y de protocolos de comunicación IEEE, utilizan tecnología de wifi lo cual permite la transmisión de información y de datos mediante señales de frecuencias con múltiples dispositivos sin necesidad de tener medios físicos. Estas redes operan en diferentes bandas de frecuencia como 2.4 GHz y 5 GHz esto permite alcanzar grandes coberturas y velocidades[40].

2.2.3 ATAQUES INFORMÁTICOS EN REDES

Las comunicaciones y las tecnologías han logrado que una gran cantidad de computadoras o dispositivos móviles puedan establecer comunicación entre ellas, como ejemplo práctico podríamos poner a una institución trabajando de una manera activa con la utilización de herramientas tecnológicas envíen información a diferentes destinatarios. Ataques a un grupo de usuarios o a una institución podría ser devastador y peligroso por lo que ocasionaría que se interrumpan servicios que son esenciales para la red[41].

Por lo general las redes inalámbricas wifi son propensos a múltiples ataques como Denegación de Servicios, este ataque puede tener diferentes consecuencias como: falsificación de direcciones o de inundación IP, esto podría controlar un sin números de quipos o dispositivos que estén conectados a la red logrando que los equipos estén o permanezcan en modo botnet o zombis[42].

2.2.4 VULNERABILIDADES EN REDES INALÁMBRICAS

Las redes inalámbricas cuentan con muchas ventajas, una de ellas y como principal que es la movilidad, por lo que no depende de algún medio físico como lo es la conectividad por cable. Estas redes no están explícitamente ligado a una ubicación estática fija por lo que la transmisión puede rotar dependiendo de los límites de conectividad permitidos por los equipos de transmisión[43]. El internet se ha actualizado hoy en día existe el internet móvil el mismo que permite que varios dispositivos puedan acceder a este tipo de redes privadas o públicas, pero así mismo existen amenazas a estas redes por lo que afectaría considerablemente[44].

2.2.5 ANÁLISIS DE SEGURIDAD

El análisis de seguridad en redes inalámbricas implica una evaluación de manera sistemática que involucra controles para la identificación de vulnerabilidades y la implementación de medidas de mitigación incluyendo otros factores. Esto podría incluir el uso de herramientas útiles para procesos de escaneo, análisis de tráfico, pruebas de penetración[45].

2.2.6 TÉCNICAS DE CIBERSEGURIDAD

Existen muchas técnicas de ciberseguridad y se las pueden aplicar en el contexto de las redes inalámbricas para abordar los desafíos de importantes de seguridad. Estas incluyen el uso de técnicas de control de acceso, autenticación, detección cifrado y prevención de intrusos, así como técnicas avanzadas de análisis de tráfico o de correlación de eventos[46].

2.2.7 AMBIENTE CONTROLADO

Estos tipos de ambiente permiten la evaluación de la seguridad en redes inalámbricas permitiendo realizar pruebas y análisis de manera más segura y controlada, sin afectar la estabilidad de la red. Esto facilita la validación de controles de seguridad e identificación de vulnerabilidades y sobre todo la implementación de medidas que permiten mitigación sin riesgos que afecte a la red local[47].

2.2.8 ATAQUE DE FUERZA BRUTA

Un ataque de fuerza bruta consiste en probar pruebas a todas las posibles combinaciones de caracteres, claves o contraseñas que podrían existir para tratar de acceder a la red. Este ataque se centra en intentar todas las posibilidades hasta dar con la correcta, por lo que puede ser muy efectivo, pero también extremadamente lento y agotar los recursos[48].

2.2.9 ATAQUE DE DICCIONARIO

Es un ataque que, a diferencia de la fuerza bruta, utiliza un listado previamente generado que se pudo haber realizado de una manera automática o manual en la contiene palabras, frases o combinaciones comunes lo que permitiría adivinar las contraseñas. El método prácticamente es basado a la información de mucha persona por lo que suelen utilizar contraseñas que son palabras o combinaciones comunes, lo que las hace más vulnerables a este tipo de ataques[49].

2.3 METODOLOGÍA DE PROYECTO

Esta investigación contempla análisis de tipo de estudio explicativo, por lo que hace énfasis a realizar un estudio enfocado a las redes de comunicación inalámbrica, engloba aspectos importantes en la cual servirá de mucho en base a un análisis de técnicas de seguridad informática en la detección de anomalías en la red y tener un enfoque cualitativo sobre la investigación recopilada, está presente investigación se la realizará mediante referencias bibliográficas fundamentadas de otros trabajos que tengan relevancias y que esté acorde a la propuesta de investigación planteada para su posterior ejecución[50].

2.3.1 METODOLOGÍA DE INVESTIGACIÓN

METODOLOGÍA O ESTUDIO DIAGNÓSTICO

Este tipo de estudio toma como referencia a investigaciones que engloben todos los conocimientos necesarios y esenciales con el fin de poder determinar el lugar o sitio en donde se encuentre el tipo de problema o situación anómala, para poder realizar un soporte en el momento de realizar alguna toma de decisiones sobre el estudio[51].

METODOLOGÍA O ESTUDIO EXPLORATORIO

Una metodología exploratoria se rige en una visión completa de las cosas que están sucediendo o la forma de interpretar información de una manera aproximativa, con respecto a una determinada situación, este tipo de estudio exploratorio se la utiliza cuando se ha seleccionado el tema poco investigado, además que el objetivo de este método es explorar, descubrir nuevas investigaciones es decir preparar el camino para futuras investigaciones, que para nuestro caso en el ámbito de ciberseguridad[52].

2.3.2 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Se detallará a continuación de manera clara y puntuada las técnicas e instrumentos para la recolección de información.

TÉCNICAS

Técnica de observación documental

La técnica de observación documental es recurrir a información escrita de datos de otras investigaciones, además se consideran como mediciones producidas por el observador, esta técnica tiene propósitos exploratorios adaptable de acuerdo con el investigador, además de que el observador se rige a las normas de una sociedad lo que equivale a poder reconocer y aceptar límites de la investigación[53].

INSTRUMENTOS

Ficha de observación[54].

VARIABLE

- Tiempo que le toma al ciberdelincuente en poder burlar la seguridad aplicando técnicas de seguridad informática.

Se medirá el tiempo en la ejecución mediante herramientas de hacking ético, por lo que no existe un tiempo estimado para la realización de estos procesos.

2.3.3 METODOLOGÍA DE DESARROLLO

PTES es una metodología muy conocida e implementada para un test de penetración informática por lo que involucra estudios experimentados con el fin de brindar un análisis seguro. Por ende, este proyecto seguirá la metodología que cuenta con las siguientes fases mencionadas[55].

Figura 1. Fases de las etapas PTES

Con la información recolectada de los estándares y protocolos, además podremos tratar de aplicar que clase de ataque o herramienta de hacking adecuado para el posterior análisis de vulnerabilidad, en esta fase se analiza las vulnerabilidades posibles que podría tener la red, es decir información necesaria para poder aplicar alguna técnica u herramienta de hacking ético, con estos conocimientos de la red podríamos comprometer a las redes de tipo inalámbricas[56].

La fase de explotación implica explorar cada brecha posible con el fin de encontrar algún acceso personal y confidencial, es decir conocer contraseñas e incluso conocer información de los dispositivos que se conectan a la red y por ende saber a quién pertenece cada dispositivo, también esta fase casi no es necesario aplicarla por lo que consiste en lograr obtener credenciales e información confidencial de suma importancia[57].

En esta última fase se elabora un informe en donde se detallan las conclusiones de todas las prácticas que se realizaron, además de detallar novedades de los resultados técnicos, además de realizar recomendaciones de seguridad a estos tipos de conectividad de manera pública[58].

2.4 MARCO LEGAL

2.4.1 LEY ORGANICA DE PROTECCION DE DATOS PERSONALES

La ley orgánica del Ecuador establece lo siguiente sobre la protección de los datos personales los mismos que son relacionados con el presente proyecto investigativo[59].

Art. 9.-Interés legítimo. -Cuando el tratamiento de datos personales tiene como fundamento el interés legítimo:

a) Únicamente podrán ser tratados los datos que sean estrictamente necesarios para la realización de la finalidad.

b) El responsable debe garantizar que el tratamiento sea transparente para el titular.

c) La Autoridad de Protección de Datos puede requerir al responsable un informe con (sic) de riesgo para la protección de datos en el cual se verificará si no hay amenazas concretas a las expectativas legítimas de los titulares y a sus derechos fundamentales.

CAPÍTULO II (PRINCIPIOS)

j) Seguridad de datos personales. -Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto.

TRANSFERENCIA O COMUNICACIÓN Y ACCESO A DATOS PERSONALES POR TERCEROS

Art. 33.-Transferencia o comunicación de datos personales**.** -Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario, cuando la transferencia se encuentre configurada dentro de una de las causales de legitimidad establecidas en esta Ley, y se cuente, además, con el consentimiento del titular.

Se entenderá que el consentimiento es informado cuando para la transferencia o comunicación de datos personales el responsable del tratamiento haya entregado información suficiente al titular que le permita conocer la finalidad a que se destinarán sus datos y el tipo de actividad del tercero a quien se pretende transferir o comunicar dichos datos.

Art. 35.-Acceso a datos personales por parte de terceros. -No se considerará transferencia o comunicación cuando el acceso a datos personales por un tercero sea necesario para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido a datos personales en estas condiciones debió hacerlo legítimamente.

El tratamiento de datos personales realizado por terceros deberá estar regulado por un contrato, en el que se establezca de manera clara y precisa que el encargado del tratamiento de datos personales tratará únicamente los mismos conforme las instrucciones del responsable y que no los utilizará para finalidades diferentes a las señaladas en el contrato, ni que los transferirá o comunicará ni siquiera para su conservación a otras personas.

Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la autoridad de protección de datos personales.

El tercero será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente Ley.

Art. 37.-Seguridad de datos personales. -El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos.

SEGURIDAD DE DATOS PERSONALES

El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y

permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales.

Art. 40.-Análisis de riesgo, amenazas y vulnerabilidades. -Para el análisis de riesgos, amenazas y vulnerabilidades, el responsable y el encargado del tratamiento de los datos personales deberán utilizar una metodología que considere, entre otras:

1) Las particularidades del tratamiento;

2) Las particularidades de las partes involucradas; y,

3) Las categorías y el volumen de datos personales objeto de tratamiento.

Art. 41.-Determinación de medidas de seguridad aplicables. -Para determinar las medidas de seguridad, aceptadas por el estado de la técnica, a las que están obligadas el responsable y el encargado del tratamiento de los datos personales, se deberán tomar en consideración, entre otros:

1) Los resultados del análisis de riesgos, amenazas y vulnerabilidades;

2) La naturaleza de los datos personales;

3) Las características de las partes involucradas;

4) Los antecedentes de destrucción de datos personales, la pérdida, alteración, divulgación o impedimento de acceso a los mismos por parte del titular, sean accidentales e intencionales, por acción u omisión, así como los antecedentes de transferencia, comunicación o de acceso no autorizado o exceso de autorización de tales datos.

El responsable y el encargado del tratamiento de datos personales deberán tomar las medidas adecuadas y necesarias, de forma permanente y continua, para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas las que conlleven un alto riesgo para los derechos y libertades del titular, de conformidad con la normativa que emita la Autoridad de Protección de Datos Personales.

Art. 46.-Notificación de vulneración de seguridad al titular. -El responsable del tratamiento deberá notificar sin dilación la vulneración de seguridad de datos

personales al titular cuando conlleve un riesgo a sus derechos fundamentales y libertades individuales, dentro del término de tres días contados a partir de la fecha en la que tuvo conocimiento del riesgo.

1. Cuando el responsable del tratamiento haya adoptado medidas de protección técnicas

organizativas o de cualquier otra índole apropiadas aplicadas a los datos personales afectados por la vulneración de seguridad que se pueda demostrar que son efectivas;

2. Cuando el responsable del tratamiento haya tomado medidas que garanticen que el riesgo para los derechos fundamentales y las libertades individuales del titular, no ocurrirá; y,

3. Cuando se requiera un esfuerzo desproporcionado para hacerlo; en cuyo caso, el responsable del tratamiento deberá realizar una comunicación pública a través de cualquier medio en la que se informe de la vulneración de seguridad de datos personales a los titulares.

La procedencia de las excepciones de les numerales 1 y 2 deberá ser calificada por la Autoridad de Protección de Datos, una vez informada esta tan pronto sea posible, y en cualquier caso dentro de los plazos contemplados en el Artículo 43.

2.4.2 CÓDIGO ORGÁNICO INTEGRAL PENAL “COIP”

El COIP busca unificar y modernizar la legislación penal ecuatoriana, incorporando nuevos tipos delictivos, reformando el sistema penitenciario, regulando la responsabilidad de las personas jurídicas y optimizando los procesos penales[60].

Art. 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

Art. 179.- Revelación de secreto**. -** La persona que, teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación

pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.

Art. 190.- Apropiación fraudulenta por medios electrónicos. - La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

Art. 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Art. 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una

transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

Art. 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. – La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas

proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

Art. 500.- Contenido digital. - El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí. En la investigación se seguirán las siguientes reglas:

1. El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses.

2. Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.

3. Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.

Por lo general se debe conocer las leyes necesarias para poder realizar cualquier tipo de acción que podría se dañina, siempre se debe tener en cuenta estos aspectos legales tanto para el tratamiento de los datos, siempre se debe realizar estas acciones mediante solicitudes para que el usuario o cualquier persona sepa de las acciones que se podrían estar realizando, siempre se debe considerar el permiso legal sobre cualquier acción.

CAPITULO 3. PROPUESTA

3.1 OBJETIVO 1: COMPARAR LAS VULNERABILIDADES DE LOS PROTOCOLOS DE COMUNICACIÓN INALÁMBRICA 802.11 PARA DETERMINAR EL NIVEL DE RIESGO SIGUIENDO EL ENFOQUE PTES.

3.1.1 FASE 1 Y FASE 2

3.1.2 FASE 1.- INTERACCIÓN PREVIA

Interacción Previa de la metodología PTES (Penetration Testing Execution Standard) tiene como objetivo establecer un entendimiento mutuo entre el equipo de pruebas de penetración y el cliente. Durante esta fase, se llevan a cabo actividades clave como los objetivos y el alcance de las pruebas, la recopilación de información relevante.

3.1.3 VERSIONES DE WIFI BASADO EN EL ESTÁNDAR IEEE 802.11

Estas normas o estándares especifican las características de la capa física y de acceso al medio (MAC) de las redes WLAN[61].

802.11: es un estándar original de las redes LAN inalámbricas, fue originado en 1997, trabaja en las frecuencias de 2.4 GHz y 5 GHz, tiene una tasa de velocidad muy baja de hasta 2mbps.

802.11a: fue establecido en el año de 1999, opera en la banda 5 GHz y tiene una velocidad de hasta 54 Mbps, es mejor en términos de velocidad y capacidad.

802.11b: también fue creado en 1999, opera en una banda de frecuencia de 2.4 GHz con velocidades de máximas de hasta 11 Mbps.

802.11g: trabaja en un rango de frecuencia de 2.4 GHz con velocidades de 54 Mbps, además de ser compatible con el 802.11b por lo que trabaja en la misma frecuencia a diferencia que posee una mayor velocidad y rendimiento.

802.11n: tiene mejores velocidades y alcance, opera en las bandas de frecuencia de 2.4 GHz y 5 GHz alcanzando velocidad de hasta 600 Mbps, utiliza una tecnología denominada MIMO (Multiple Input Multiple Output).

802.11ac: trabaja en una frecuencia de 5GHz, utiliza la tecnología MIMO, tiene velocidades mejoradas y sobre todo admite dispositivos que operan en frecuencias de 2.4 GHz.

802.11ad: fue lanzado en el año 2012, opera en la banda de frecuencia a 60 GHz y alcanza velocidades de 6,7 Gbps su desventaja es que su alcance es muy limitado a 3.3 metros.

802.11ah: Se lo conoce como Wifi Halow trabaja en frecuencias muy debajo de 1GHz, su principal función fue crear redes de rango extendido y que a su vez consuma menos energía.

802.11ax: Es conocido como WLAN de eficiencia alta, busca mejorar el rendimiento del despliegue y ofrecer velocidades de hasta 10 Gbps.

La metodología PTES (Penetration Testing Execution Standard) proporciona una estructura para evaluar el nivel de riesgo de las vulnerabilidades en los protocolos de comunicación inalámbrica, integrando la importancia de la organización internacional FIRST (Forum of Incident Response and Security Teams) en la respuesta y seguridad de incidentes. Así mismo CVSS (Common Vulnerability Scoring System) como una herramienta esencial para evaluar la gravedad de las vulnerabilidades[62].

Las vulnerabilidades van a estar dirigidas a métricas CVE (Common Vulnerabilities and expposures) y CWE (Common Weakness Enumeration), son consideradas listas de problemas de vulnerabilidades conocidas públicamente, se utilizara un sistema de valoración definido en CVSS (Common Vulnerability Scoring System) la misma que proporciona métricas que facilitan la medición, con esto se puede tener un dato para considerar el nivel de riesgo al comparar las vulnerabilidades, esto se basa en[63]:

WEP, WPA, WPA2: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Métrica:

AV (Access Vector) = Representa la complejidad del acceso = N: significa que un atacante no necesita acceso físico al sistema.

AC (Access Complexity): complejidad del ataque en explotar la vulnerabilidad = H: significa que el ataque es de alto nivel.

PR (Privileges Required) = Privilegios necesarios = N: no es necesario tener privilegios especiales para llevar a cabo el ataque.

UI (User Interaction): La vulnerabilidad requiere interacción del usuario = N: No se requiere interacción del usuario.

S (Scope): Alcance de la vulnerabilidad= U: Vulnerabilidad afecta a un solo usuario.

C (Confidentiality Impact): Impacto en la confidencialidad = H: indica un impacto alto en la confidencialidad.

I (Integrity Impact): Impacto en la integridad = H: Impacto alto en la integridad.

A (Availability Impact): Disponibilidad = H: Impacto alto en la disponibilidad.

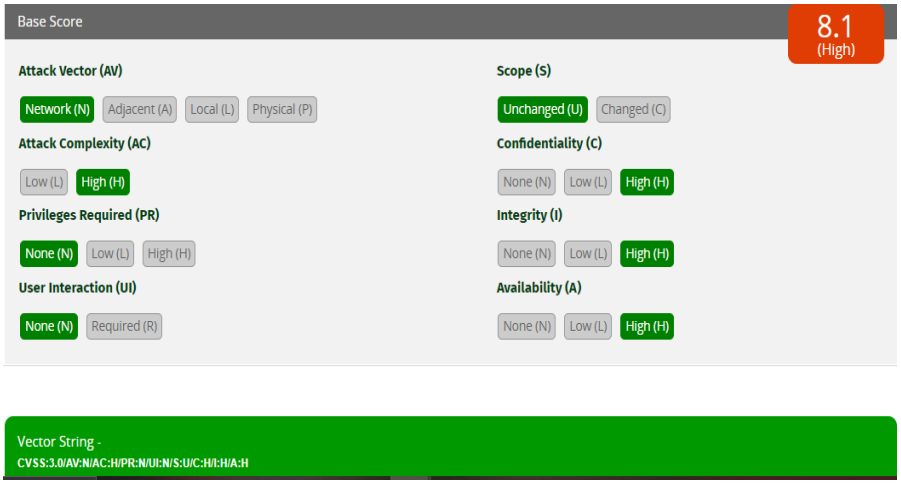


Figura 2. CVSS Protocolos de seguridad[64].

WPA3: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

Métrica:

AV (Access Vector) = Representa la complejidad del acceso = N: significa que un atacante no necesita acceso físico al sistema.

AC (Access Complexity): complejidad del ataque en explotar la vulnerabilidad = H: significa que el ataque es de alto nivel.

PR (Privileges Required) = Privilegios necesarios = N: no es necesario tener privilegios especiales para llevar a cabo el ataque.

UI (User Interaction): La vulnerabilidad requiere interacción del usuario = N: No se requiere interacción del usuario.

S (Scope): Alcance de la vulnerabilidad= U: Vulnerabilidad afecta a un solo usuario.

C (Confidentiality Impact): Impacto en la confidencialidad = L: indica un impacto bajo en la confidencialidad.

I (Integrity Impact): Impacto en la integridad = L: Impacto bajo en la integridad.

A (Availability Impact): Disponibilidad= L: Impacto bajo en la disponibilidad.

Figura 3. CVSS Protocolo de seguridad WPA3[64].

Mediante la herramienta CVSS podemos medir y calcular el nivel de impacto, nivel de riesgo y además la probabilidad de que algo ocurra en estos protocolos de seguridad, además de comparar las vulnerabilidades conocidas mediante un indicador estándar CVE lo cual es una lista de códigos y nombres estandarizados esto con el fin de nombrar las vulnerabilidades y sobre todo las exposiciones en la seguridad.

Tabla 1. Comparativa de vulnerabilidades

Protocolos de seguridad	CVE	Algoritmo	Versiones	Vulnerabilidades clave	Amenaza asociada	Impacto Potencial	Probabilidad de Ocurrencia	Nivel de Riesgo
WEP (Wired Equivalent Privacy)	CVE-2017-13077	RC4	802.11i 1997	Clave de cifrado estática y débil. Falta de autenticación de usuarios.	Ataques de diccionario para obtener la clave	Acceso no autorizado a la red	Alto	Crítico
WPA(Wi−FiProtectedAccess)	CVE-2020-24586	TKIP	802.11i 2004	Debilidades en el algoritmo TKIP	Ataques de inyección de paquetes	Acceso no autorizado a la red	Medio	Moderado
WPA2(Wi−FiProtectedAccess2)	CVE-2017-13077, CVE-2018-14526	CCMP (AES)	802.11i 2004	Vulnerabilidad KRACK (Key Reinstallation Attack)	Obtención de la clave de cifrado	Pérdida de confidencialidad e integridad de la comunicación, acceso no autorizado a la red	Alto	Alto
802.11i(WPA3)	CVE-2019-9494	SAE (Simultaneous Authentication of Equals)	802.11w-2018	Nuevas vulnerabilidades aún por descubrir |Muy Baja	Resistencia a ataques de diccionario	Impacto acotado en la confidencialidad y disponibilidad	Bajo	Bajo

Nota: Información de la investigación realizada[20].

3.1.4 CONTROLES EN CIBERSEGURIDAD DISPONIBLES PARA DISMINUIR INCIDENTES EN LOS PROTOCOLOS DE COMUNICACIÓN INALÁMBRICA 802.11

1. **Disminución de riesgos en WEP (Wired Equivalent Privacy):**

   Son protocolos más seguros como WPA2 o WPA3 en lugar de WEP.

2. **Disminución de riesgos en WPA (Wi-Fi Protected Access):**

   Actualización a WPA2 o WPA3 para aprovechar la seguridad que ofrecen sus protocolos, es favorable considerar el uso de herramientas de análisis de tráfico inalámbrico para identificar actividad sospechosa.

3. **Disminución de riesgos en WPA2 (Wi-Fi Protected Access II):**

   Actualizar a WPA3 para bajar índices de vulnerabilidades como KRACK.

4. **Disminución de riesgos en 802.11i (WPA2-Enterprise):**

   Fortalecimiento de procesos de autenticación, utilizando métodos como EAP-TLS.

5. **Disminución de riesgos en 802.11r:**

   Implementaciones de controles de red, para restringir el acceso no autorizado.

6. **Disminución de riesgos en 802.11w:**

   Implementación de la protección de tramas en la gestión según los estándares.

3.1.5 FASE 2.- RECOLECCIÓN DE INFORMACIÓN

En esta fase abarca la recolección de información y datos relevantes que nos servirá de mucho para realizar este trabajo investigativo práctico. En esta etapa de fase se trata de involucrarse en aspectos de estándares, protocolos y posibles amenazas que se podrían dar en las conectividades inalámbricas wifi, así enlistar las herramientas que contamos para desarrollar la posterior fase de vulnerabilidad.

Comparación entre una red WLAN y LAN para una mayor seguridad.

Tabla 2. Comparación entre una red WLAN y LAN
Fuente: Propia

Parámetros de Comparación	WLAN	LAN
Significa	Wireless local área Network.	Local área Network.
Tipo de conexión	Inalámbricas	Inalámbricas y Alámbricas
Costo y seguridad	Es costoso de instalar y menos seguro.	Menos costoso y más seguro
Cobertura	Grandes regiones.	Grades áreas
Rendimiento	Rendimiento alto; rendimiento es afectado por el mal tiempo.	Rendimiento aceptable y no se ve afectado por el clima
Interferencias	Fácil interferencia.	No se puede interferir fácilmente
Ejemplos	Dispositivos móviles o aparatos tecnológicos en general.	Dispositivos móviles o aparatos tecnológicos en general que cuenten con puertos de entrada a redes.

Nota: Información realizada por Autor[36].

Una de las principales ventajas de Kali Linux es su capacidad para realizar ataques a redes inalámbricas, lo que lo convierte en una herramienta esencial para las pruebas de penetración de Wi-Fi. Incluye herramientas como Aircrack-ng, que puede usarse para descifrar contraseñas de redes inalámbricas"

3.1.6 LISTA DE COMANDOS UTILIZADOS

La tabla de comandos utilizados en el sistema operativo Kali Linux para la realización de esta práctica investigativa en la fase de 3 de la metodología PTS cuenta con su respectiva descripción, para el posterior análisis de post explotación.

Tabla 3.Comandos Utilizados

COMANDOS UTILIZADOS	
Comando	Descripción
Sudo su	Cambia de una manera temporal a la cuenta a super usuario o denominado root.
cupp	Crea perfiles de contraseñas con información de la víctima.
git clone	Sirve para crear una copia local.
cupp.py	Sirve para ejecutar la herramienta cupp.
python cupp.py -i	Es la forma de iniciar un cuestionario básico sobre información de la víctima para crear un diccionario.
cat	Muestra contenido de un archivo.
crunch	Generar diccionarios de una manera personalizada.
airmon-ng	Sirve para capturar paquetes en la red.
airodum-ng	Sirve para visualizar información detallada de la red inalámbrica.
aireplay-ng	Sirve para generar tráfico en la red.
aircrack-ng	Sirve para realizar auditorías en redes.

COMANDOS UTILIZADOS	
nmcli	Sirve para controlar el estado de la red.

Nota: Información realizada según la investigación[38].

3.2 OBJETIVO 2: EVALUAR MEDIANTE EL ESTÁNDAR PTES LA EFECTIVIDAD DE LAS HERRAMIENTAS DE HACKING ÉTICO EN EL DESCIFRADO DE CONTRASEÑAS EN REDES INALÁMBRICAS.

3.2.1 FASE 3, 4, 5 Y 6

En estas fases se centrarán en cumplir con el objetivo número dos en donde se indagará las mejores herramientas de hacking ético propias del sistema operativo Kali Linux, mediante la herramienta CVSS (Common Vulnerability Scoring System) y el proceso de las fases de la metodologia PTES serán de gran ayuda para poder evaluar que tan efectivas son las herramientas para el uso de ataques de diccionario y de fuerza bruta.

3.2.2 MODELADO DE AMENAZAS

En esta fase se analiza cómo un atacante podría aprovechar las vulnerabilidades identificadas para acceder a información sobre la de la red. Este análisis considera factores como el tipo de activo afectado y la criticidad de la información, y las posibles consecuencias reputacionales o legales, ayuda a priorizar las vulnerabilidades encontradas y a determinar las medidas de seguridad más apropiadas para mitigarlas y reducir el riesgo general.

3.2.3 HERRAMIENTAS DE PROTECCIÓN TECNOLÓGICA EN EL SISTEMA OPERATIVO KALI LINUX

En la siguiente tabla se muestra una serie de herramientas de seguridad inalámbrica propia del sistema operativo Kali Linux, se realizó una comparativa de las herramientas, (ver Tabla 4 y Tabla 9) en la cual se eligió las mejores para la realización de este trabajo.

Tabla 4. Herramientas de protección tecnológica

Aircrack-ng	Esta herramienta se la puede utilizar para auditar redes wifi, además permite realizar ataques de diccionario o denominado ataque de fuerza bruta a claves WEP, WPA Y WPA2.
Kismet	Su función es detectar de redes inalámbricas así se encuentren de manera oculta, funciona con tarjetas o adaptadores que sea compatible con 802.11.
Reaver	Esta herramienta permite realizar ataques de fuerza bruta al WPS (Wifi Protected Setup) con lo que permitiría obtener contraseñas WPA/WPA2.
Bettercap	Esta herramienta versátil en el uso hacking y de monitoreo a redes, permitiendo realizar ataques MitM (Man in the Middle).
Fluxion	Esta herramienta permite automatizar procesos respectivamente a ataque de phishing contra a redes inalámbricas para obtener contraseñas.
Fern Wifi Cracker	Esta herramienta permite ver graficas sus principales ataques son de diccionario y de fuerza bruta a redes inalámbricas.
WifiPhisher	Su mismo nombre lo indica, sirve para realizar ataque de phishing y obtener acceso a las redes wifi.
Wifite	Con esta herramienta ayuda en el proceso de automatización, pudiendo realizar múltiples ataques contra redes WiFi, como ataques de diccionario, de fuerza bruta y lograr deshabilitar WPS.
Cowpatty	Esta herramienta permite realizar ataques de diccionario y fuerza bruta contra claves WPA/WPA2-PSK.

Airgeddon	Esta herramienta permite auditar la seguridad, puede realizar diversos ataques con el fin de deshabilitar WPS y poder ejecutar el ataque de diccionario.

Nota: Información realizada según la investigación[40].

La siguiente tabla muestra una perspectiva sobre los recursos que se tienen para la siguiente fase de la metodología, para eso presentamos un entorno tecnológico en donde involucra el objetivo y las características de los equipos necesarios para la ejecución de la siguiente fase.

Tabla 5. Recolección de Información (Entorno Tecnológico)

Fuente: propia

Nombre del responsable:	**Fase:**
Ricardo González Balón	**Recopilación de información**
Objetivo: Detallar los recursos de hardware y software a utilizar para la posterior fase de vulnerabilidades	
Tiempo estimado: **30 minutos**	**Nivel de complejidad** a.(bajo) b.(medio) c.(alto)
Herramientas tecnológicas utilizadas:	
Hardware:	

Equipo	Portátil DELL
Adaptador de red	Wireless Adapter 950Mbps 802.11 Velocidad de datos dinámica: 802.11b: 1,2,5,5,11 Mbps;

	802.11g: 6,9,12,18,24,32,48,54 Mbps. 802.11n: (20 MHz) MCSO-7, hasta 72 Mbps; (40 MHz) MCSO-7, hasta 150 Mbps Soporte de seguridad para 64/128 WEP, WPA, WPA2, WPAI Opera en la banda de frecuencia de 2,4 GHz
Router	ZTE ZXHN F660
Software:	
SO	Windows 10 pro
Máquina Virtual	Virtual Box 6.1 Versión
SO de prueba	Kali Linux
Versiones	Kali Linux (Kali Linux 2023.2)
Resultados: Con las herramientas de software y hardware podemos tener los recursos necesarios para una posterior fase de análisis de vulnerabilidades en redes inalámbricas wifi.	

Aquí presentamos un informe detallado sobre la red número uno en donde podemos identificar ciertas características de la red como su seguridad, autentificación, intensidad de señal etc. (ver Tabla 6)

Tabla 6. Informe de resultados red 1

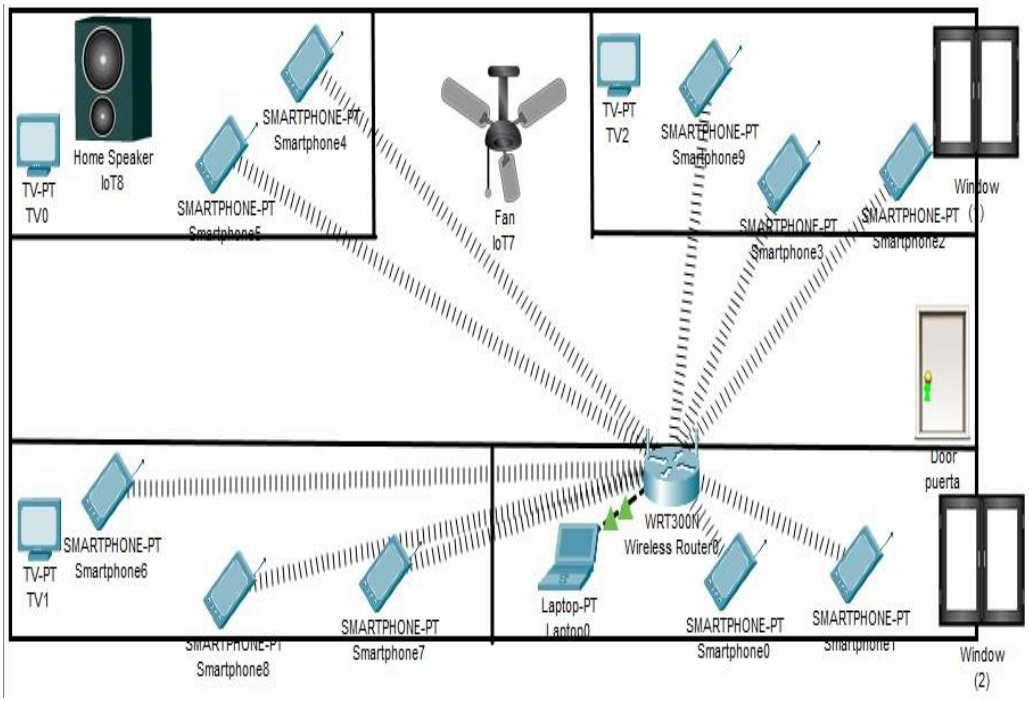
Fuente: propia

Informe de resultados	
Red 1	**Responsable**: Ricardo González

SSID: **XTRIM_GONZALEZ**		**BSSID:** B8:F0:B9:C2:95:B0	
Canal: 1	**Rate:** 130Mbit/s	**Señal**: 100 dbm	**Beacons:** 40
Seguridad: **WPA2**		**Algoritmo de cifrado**: CCMP	**Autentificación**: PSK
Ataque aplicado: Ataque de diccionario o fuerza bruta.			
Dispositivos en red: 1. **30:B1:B5:92:98:0C** 2. **4E:33:5C:E1:87:3E** 3. **B8:C3:85:10:00:3E** 4. **DC:90:88:7B:C1:02** 5. **72:59:D3:EA:52:CD** 6. **90:48:9A:F9:A8:E3** 7. **E8:68:E7:8B:63:D8** 8. **E5:DC:96:9A:CB:7B** 9. **12:47:F4:FF:84:9C** 10. **B6:14:54:3D:2C:A5**			

En esta gráfica se observa la topología de red de tipo estrella, este domicilio cuenta con una sola planta, pero con diferentes compartimientos, también observamos que cuenta con diversos dispositivos inalámbricos conectados a un solo router.

Figura 4. Topología de red tipo estrella



Fuente: propia

Aquí presentamos un informe detallado sobre la red número dos en donde podemos identificar ciertas características de la red como su seguridad, autentificación, intensidad de señal además de la cantidad de usuarios que se conectan a esta red. etc. (Ver Tabla 7)

Tabla 7. Informe de resultados red 2

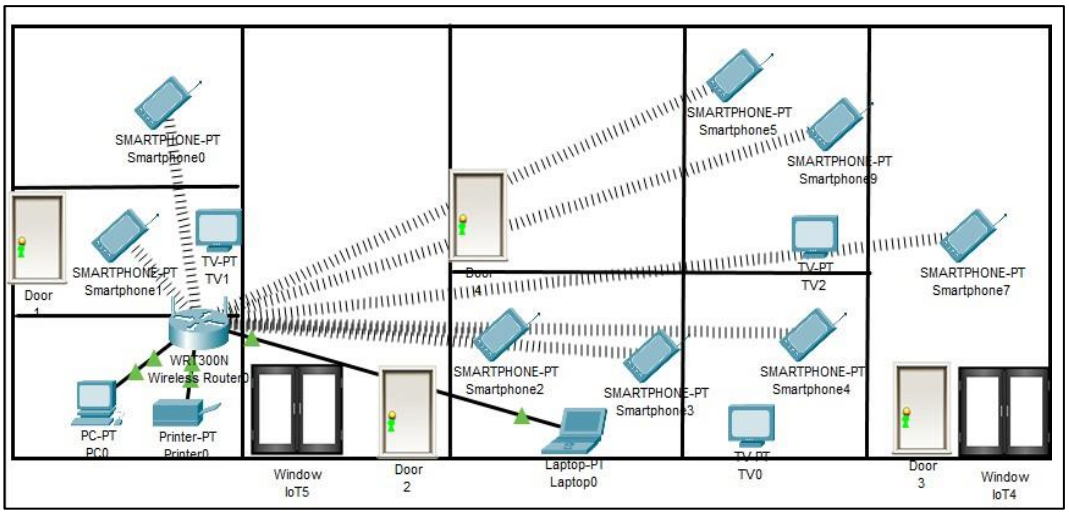
Fuente: Propia

Informe de resultados			
Redes 2	**Responsable**: Ricardo González		
SSID: SUMPATV_VERASUAREZ		**BSSID:** E0:67:B3:57:82:4A	
Canal: 6	**Rate:** 130Mbit/s	**Señal**: 62 dbm	**Beacons:** 45
Seguridad: WPA2	**Algoritmo:** CCMP		**Autentificación**: PSK
Ataque aplicado: Ataque de diccionario o fuerza bruta			

Informe de resultados
Dispositivos en red: 1. **02:E0:20:0B:AE:A3** 2. **EA:3A:19:48:FF:3B** 3. **30:A1:F4:7C:F8:AA** 4. **DC:90:88:7B:C1:02** 5. **88:9F:6F:32:6C:7E** 6. **54:FC:F0:E5:83:9A**

Figura 5. Topología de red tipo estrella

Esta gráfica observamos a una topología de red de tipo estrella, este domicilio cuenta con múltiples compartimientos en donde observamos diferentes dispositivos inalámbricos y alámbricos conectados a la red.



Fuente: Propia

3.2.4 FASE 4.- ANÁLISIS DE VULNERABILIDAD

En esta fase analizaremos mediante herramientas de hacking ético a las redes inalámbricas, este tipo de análisis será de tipo auditoria, el resultado de esto es conocer información como por ejemplo el nombre de la red, si la red es visible o de configuración oculta, el canal de frecuencia en que trabaja, además la intensidad de señal que emite la red entre otras características. (Ver Tabla 6 y Tabla 7)

3.2.5 PROCESO DE ESCANEOS DE REDES (KISMET)

Para este análisis de vulnerabilidad vamos a utilizar la herramienta de Kali Linux llamada Kismet. Pero antes debemos realizar unos pasos que de detallan a continuación. En nuestra terminal de Kali Linux debemos activar el super usuario

para tener los permisos con el siguiente comando **sudo su**, después nos pedirá ingresar la contraseña del usuario, además debemos activar el adaptador wifi, pero antes debemos comprobar que este adaptador lo detecte a máquina virtual. A continuación, verificaremos que este activo el adaptador **iwconfig**, es necesario colocar el adaptador de red wifi en modo monitor, con el siguiente comando lograremos eso **airmon-ng start wlan0.**

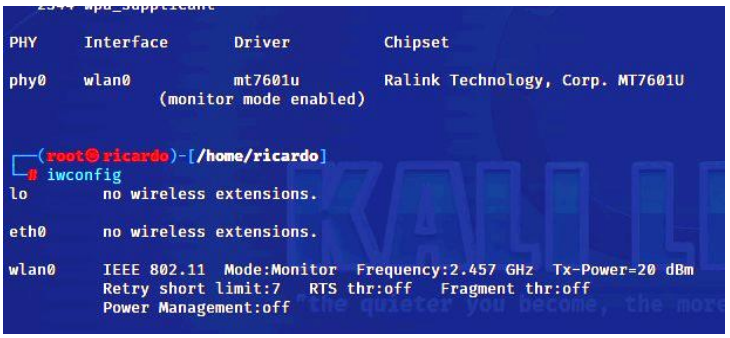


Figura 6. Activación modo monitor
Fuente: propia

Luego de habilitar estas configuraciones, procedemos a levantar el kismet en consola mediante el siguiente comando **sudo kismet**, luego aparecerá una url en donde aparecerá un local host en donde debemos abrir en el navegador.

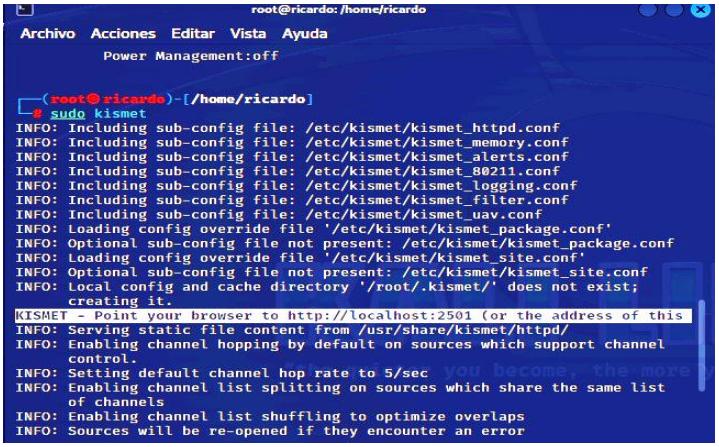


Figura 7. Http para Interfaz Kismet
Fuente: propia

A continuación, en el navegador aparecerá la interfaz web de kismet, antes de iniciar Kismet por primera vez nos en la máquina virtual Kali Linux, nos pedirá crear una cuenta en donde tendremos que colocar el usuario y una contraseña.

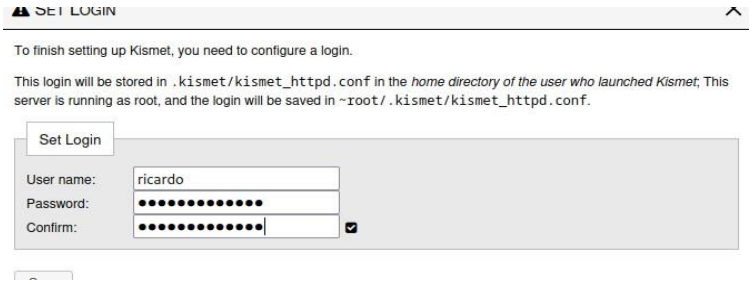


Figura 8. Creación de Usuario
Fuente: propia

Debemos indicarle a la aplicación web kismet de donde queremos tomar la información en otras palabras, donde se encuentran las antenas, anteriormente habíamos activado nuestro adaptador lo cual nos servirá para poder obtener información de las redes.

Figura 9. Activación de la tarjeta de red en Kismet
Fuente: propia

En esta gráfica observamos que nuestro adaptador de red está detectando los dispositivos es decir las señales que emiten las redes de los usuarios cercaos o lejos del punto de escaneo, en primera instancia observamos el nombre, tipo y paquetes que circulan en la red.

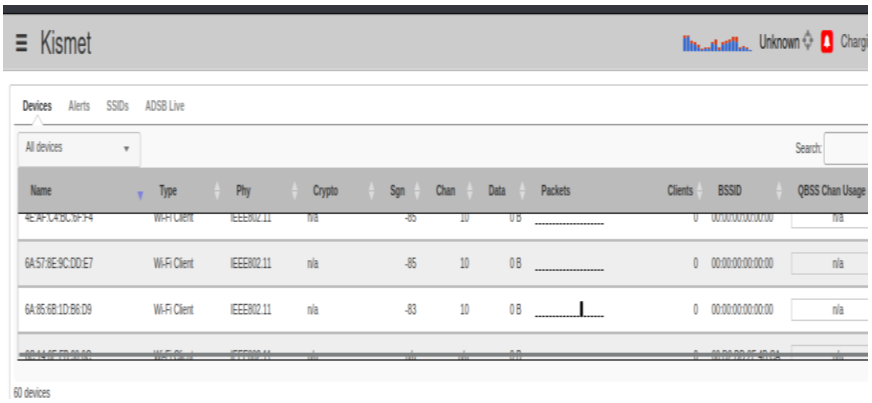


Figura 10. Detectando redes
Fuente: Propia

3.2.6 ESCANEO A REDES INALÁMBRICAS.

Escaneo número uno a la red “oculto”.

En esta gráfica observamos si existen redes ocultas, es decir que los usuarios de esa red han configurado para que esto sea posible, para saber un poco más debemos dar clic en el SSID en la que queramos ver información de la red, aunque la red sea de configuración oculto.

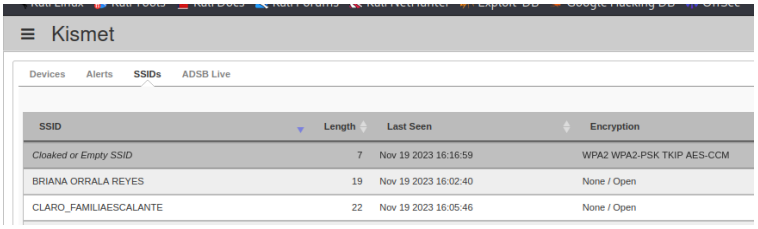


Figura 11. Identificación de red Oculta
Fuente: Propia

Dando clic, nos aparecerá la información de la red como el tipo de encriptación, la dirección MAC, el nombre del usuario, además podemos ver detalles del dispositivo. Esta red es de tipo oculta, pero podemos observar información a quien pertenece esta red.

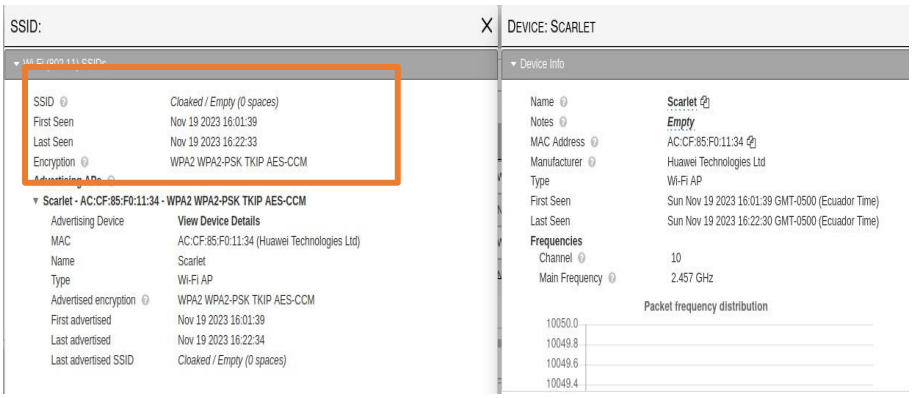


Figura 12. Información de red
Fuente: Propia

3.2.7 ESCENARIO 1 RED “XTREAM_GONZALEZ”.

En la gráfica proporciona información detallada sobre la red, incluyendo el nombre del propietario, la frecuencia de trabajo y el canal utilizado. Además, se muestra el rango de señal en el que la red está emitiendo datos, lo que permite evaluar la cobertura y la calidad de la conexión.

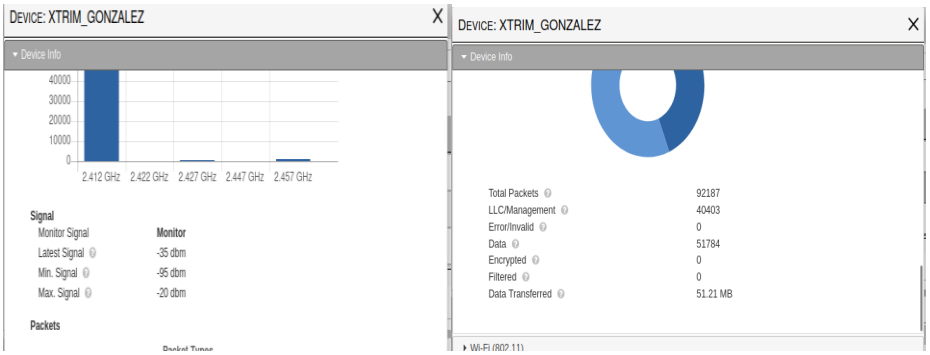


Figura 13. Datos que genera la red Wi-fi
Fuente: propia

En la siguiente imagen muestra el recuento total de paquetes generados por la red inalámbrica, lo que es crucial para evaluar el tráfico y la eficiencia de la red. Este dato es fundamental para identificar posibles congestiones, problemas de rendimiento o patrones de uso inusual.

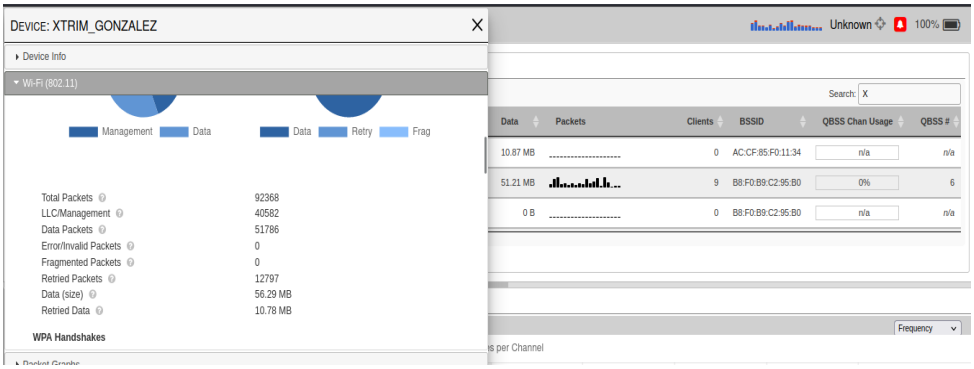


Figura 14. Paquetes que genere a red
Fuente: Propia

En la gráfica muestra una representación clara de los dispositivos conectados a la red, con un total de 10 dispositivos móviles identificados por sus direcciones IP. Esta información es fundamental para el control y la gestión de la red, ya que permite garantizar la seguridad y el rendimiento óptimos.

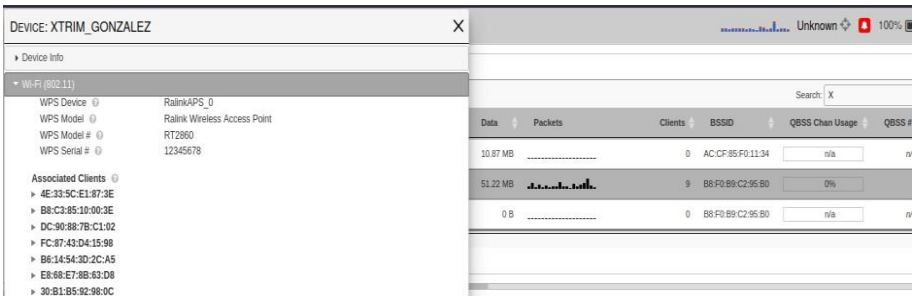


Figura 15. Dispositivos conectados a la red
Fuente: Propia

3.2.8 ESCENARIO 2 DE RED “SUMPATV_VERASUAREZ”.

Este este tipo de red, se puede observar el SSID de la red Wi-Fi, junto con otra información esencial. El SSID, o nombre de la red, es un identificador único que permite a los dispositivos conectarse a la red correcta.

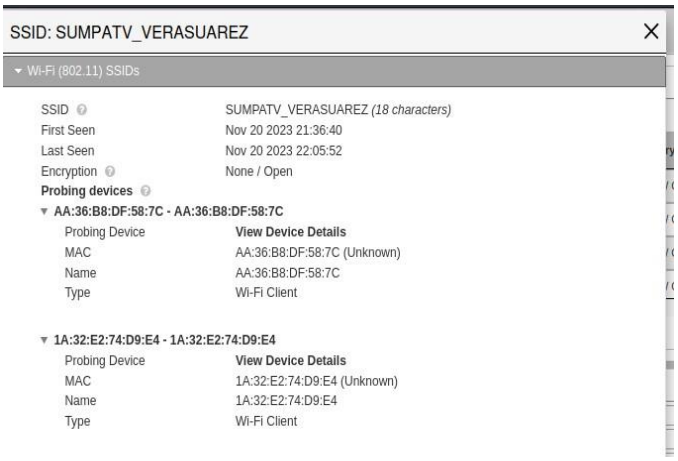


Figura 16. SSID de la red wifi
Fuente: propia

La visualización de la red permite identificar dispositivos que están sondeando la red, lo que indica intentos de conectarse a la misma. Además, se puede observar la conectividad de otras redes inalámbricas, lo que facilita la estabilidad de la conexión.

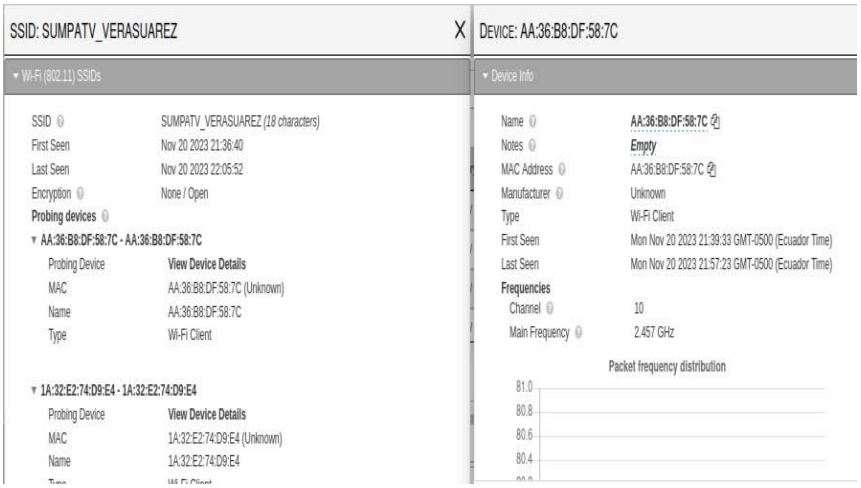


Figura 17. Dispositivos que sondean la red
Fuente: propia

La figura muestra una representación gráfica de las diferentes redes que están sondeando la red escaneada, lo que permite identificar posibles intentos de conexión no autorizados o intrusiones en la red.

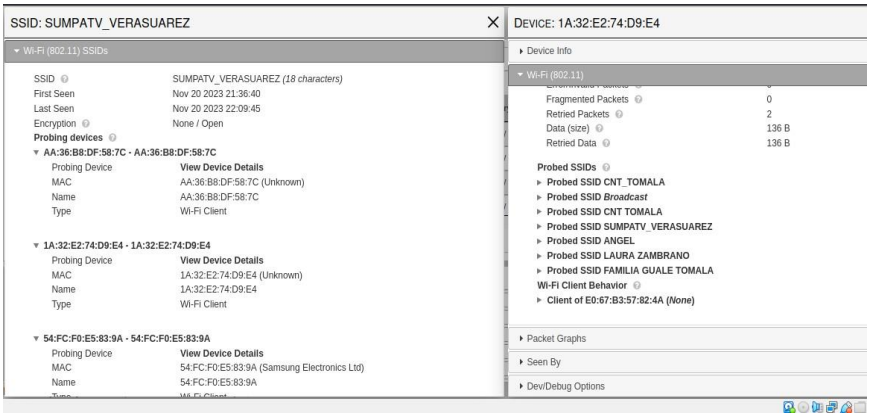


Figura 18. Redes que sondean la red
Fuente: propia

Esta tabla detalla las características de cada red y la efectividad de la herramienta Kismet en realizar el escaneo de redes e información además la utilización del adaptador de red lo cual es importante para realizar este proceso de escaneo de redes. (Ver Tabla 8)

Tabla 8. Ficha de información de vulnerabilidades
Fuente: Propia

Ficha de información de vulnerabilidades	
Nombre del responsable: **Ricardo González**	Fase: Escaneo de vulnerabilidades
Objetivo: Identificar qué tipo de seguridad tienen las redes inalámbricas, la frecuencia, la intensidad de señal entre otras características utilizando la máquina virtual Kali Linux con su herramienta integrada de Kismet.	
Tiempo estimado: 3 horas	**Nivel de complejidad** a.(bajo) b.(medio) c.(alto)
Herramientas tecnológicas utilizadas	
Hardware: **Computadora:** Dell	**Software:** Sistema Operativo Kali Linux -Kismet

Ficha de información de vulnerabilidades	
Adaptador de red: Wireless Adapter 950Mbps 802.11.	
Resultado Obtenidos:	
	Detalles encontrados
Red 1 **(oculto)**	Tiene una configuración de red oculta, pero se puede identificar el nombre de propietario, además de saber en canal trabaja y la intensidad de señal emite, además de cuantos dispositivos acceden a esta red.
Red 2 **(XTREAM_GONZALEZ)**	Esta red es visible, tienen una seguridad de encriptación adecuada, conocemos su SSID además tenemos información sobre la cantidad de usuarios que se conectan, también sabemos la intensidad de señal de emite la red.
Red 3 **(SUMPATV_VERASUREZ)**	Esta red es de tipo visible, aunque en el escaneo no se encuentra el tipo de encriptación de la red, además sabemos la intensidad de señal, los usuarios que están conectadas a la red, la frecuencia y el canal en la que se trabaja.
Resultados: Después de realizar este análisis de escaneo de vulnerabilidades de redes, los resultados obtenidos a estas redes son las siguientes, las redes tienen una seguridad de encriptación aceptable, además cada red tiene dispositivos conectados que generan datos constantemente, además una de las redes es de tipo no visible es decir que el usuario decidió mantenerlo.	

3.3 FASE 5.- EXPLOTACIÓN

3.3.1 FORMAS DE CREAR UN DICCIONARIO

3.3.2 CUPP (COMMON USER PASSWORDS PROFILER)

Existen varias formas de crear un diccionario de claves en esta fase vamos a poner en práctica de estos dos métodos, en internet existe una documentación llamada **cupp,** a continuación, se detalla el proceso.

En primer lugar, abre el navegador web predeterminado de Kali Linux como Firefox, ya en el navegador propio de Kali Linux colocamos en la barra de direcciones del navegador, escribe "“cupp descargar github”" y presiona enter.

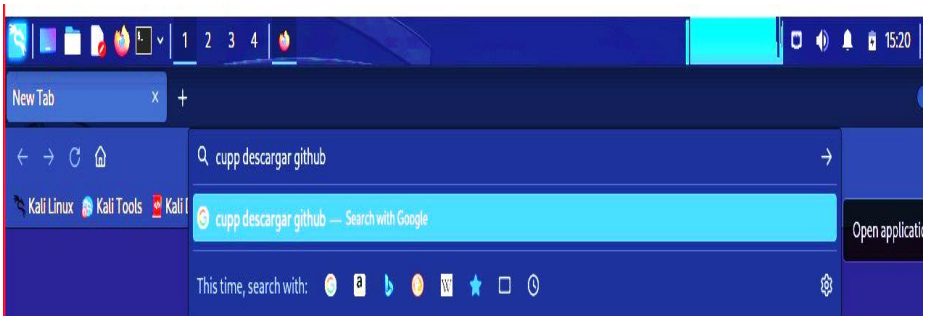


Figura 19. Cupp descargar github
Fuente: propia

Al interactuar con esta gráfica, seremos redirigidos a una nueva ventana. Para continuar, debemos hacer clic en el recuadro verde etiquetado como "code" y luego copiar el enlace proporcionado, que suele ser "https://github.com/Mebus/cupp.git"[65].

Figura 20. Copiamos el link
Fuente: propia

En esta gráfica muestra que se está iniciando el proceso de clonado de los documentos necesarios para su correcto funcionamiento, además muestra el

tamaño que ocupan los documentos. Por último, aparcera un mensaje que indica que está listo.

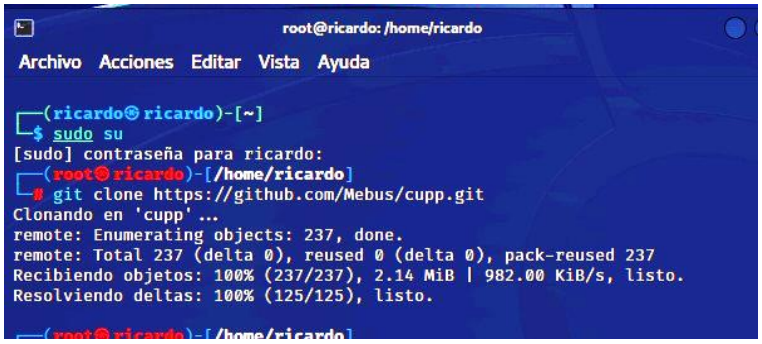


Figura 21. Finalización de la clonación
Fuente: propia

En esta gráfica muestra lo siguiente, colocamos en nuestro terminal "python cupp.py" para observar que información contiene esta herramienta en ella observamos diferentes acciones que podemos realizar.

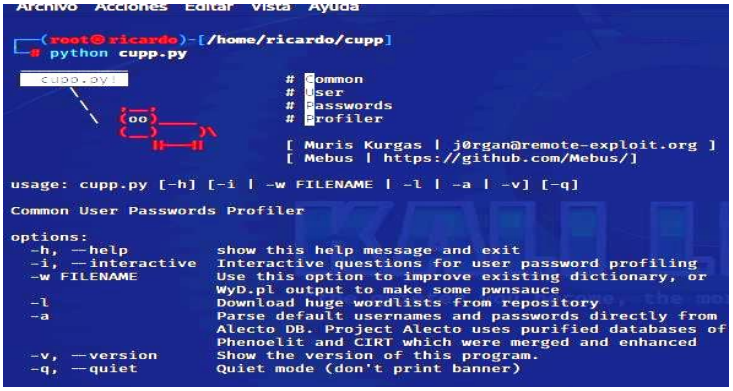


Figura 22. Python cupp.py
Fuente: propia

En esta gráfica colocamos en nuestro terminal "python cupp.py -i" esto nos servirá para contestar algunas preguntas del usuario básicas para poder generar nuestro diccionario de claves de la red que vamos atacar.

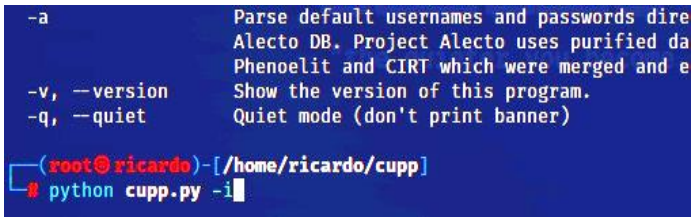


Figura 23. Python cupp.py -i
Fuente: propia

La siguiente gráfica contiene una serie de preguntas clave que nos guiarán en la creación de nuestro diccionario, además de que también se puede colocar caracteres

especiales para que haya una mejor combinación de palabras y que el diccionario sea más efectivo.

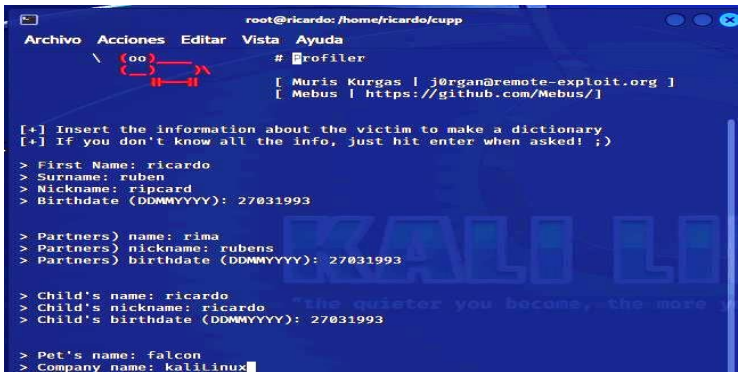


Figura 24. Preguntas claves para poder generar nuestro diccionario
Fuente: propia

En está siguiente gráfica muestra el proceso de iniciación de la creación del diccionario, el nombre que le otorgamos al archivo en este caso ricardo.txt en la cual se van a crear una combinación de 25596 palabras.

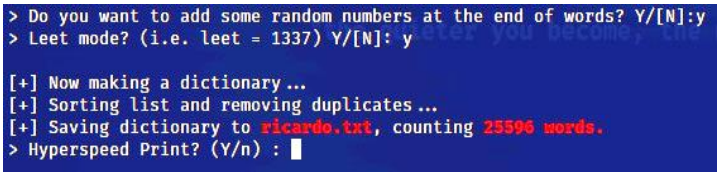


Figura 25. Creación el diccionario
Fuente: propia

En la siguiente gráfica podemos corroborar la creación de nuestro diccionario mediante el comando "ls" observamos el archivo creado ricardo.txt, podemos observar lo que contiene **el archivo mediante el siguiente comando "cat ricardo.txt".**

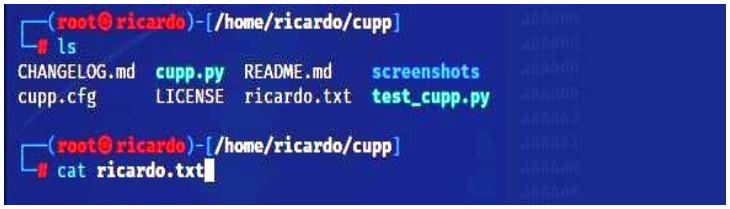


Figura 26. "cat ricardo.txt"
Fuente: propia

Estás gráfica muestra que cuando colocamos en el terminal "**cat ricardo.txt**" Observamos la cantidad de combinaciones posibles que se han creado con la

información del usuario de la red que otorgamos al inicio del cuestionario de preguntas básicas.

Figura 27. Cantidad de combinaciones
Fuente: propia

3.3.3 CRUNCH (GENERADOR DE DICCIONARIO)

Existe otra manera de poder crear un diccionario la siguiente imagen muestra que con el comando **"mkdir crunch"** en nuestro terminal colocamos "sudo su" luego de ser super usuario procedemos a colocar **"mkdir crunch"** que sirve para crear una carpeta en el directorio, después colocamos "**cruch seguido el número de palabras y número de combinaciones**"

Figura 28. Comando "mkdir crunch"
Fuente: propia

En esta gráfica muestra el número de palabras y las combinaciones que va a contener nuestro diccionario con un tamaño de datos de 96 bytes como se ve en el ejemplo: "Crunch 3 6 -p Jimena maji maria".

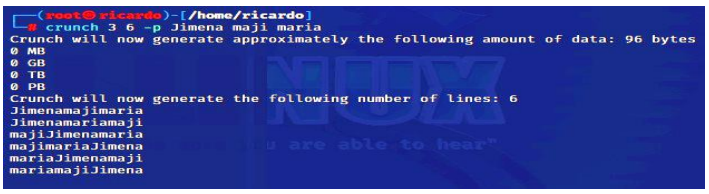


Figura 29. Crunch colocamos el número de palabras y las combinaciones

Fuente: propia

Con Crunch colocamos el número de palabras y las combinaciones como se ve en el ejemplo: **"Crunch 3 6 Jimena maji maria"** se generan una gran combinación de caracteres con las palabras escritas.

Figura 30. Número de palabras y las combinaciones
Fuente: propia

3.3.4 EVALUACIÓN EN BASE A LOS LINEAMIENTOS DEL ESTÁNDAR PTES (PENETRATION TESTING EXECUTION STANDARD)

Muy Bajo: Desempeño nulo en el criterio evaluado.

Bajo: Desempeño limitado o con dificultades significativas en el criterio evaluado.

Medio: Desempeño aceptable, mínimas limitaciones o debilidades.

Alto: Desempeño en el criterio evaluado, con pocas debilidades o limitaciones.

Muy Alto: Excelente desempeño en el criterio evaluado.

Esta escala de 1 a 10 permite cuantificar y comparar de manera sistemática el rendimiento de las diferentes herramientas de hacking ético en cada aspecto clave:

Facilidad de Uso: este criterio evalúa de una manera muy sencilla y simple, sirve para el usuario utilizar la herramienta, considerando los siguientes factores de medición:

- Interfaz
- Conocimientos técnicos
- Disponibilidad

Velocidad de Descifrado: es un criterio que evalúa la capacidad de la herramienta en descifrar contraseñas de forma rápida considerando lo siguiente:

- Métodos de ataque utilizados (fuerza bruta, diccionario, etc.)
- Rendimiento y optimización de descifrado

Tasa de Éxito: Este evalúa la efectividad de la herramienta en lograr el descifrado de contraseñas, considerando lo siguiente:

- Porcentaje de éxito en escenarios y tipos de contraseñas (composición).

Versatilidad: Este criterio evalúa tanto la capacidad de la herramienta como en adaptarse a diferentes métodos de ataque y entornos de red inalámbrica, considerando lo siguiente:

- Compatibilidad de protocolos
  (WEP, WPA, WPA2 y WPA3)
- Posibilidad de realizar otros tipos de ataques.
  (Denegación de servicio y monitoreo)
- Integración con otros sistemas y herramientas de seguridad

Puntuación General: Este último criterio representa una evaluación de manera global en sentido de la efectividad de la herramienta para el descifrado de contraseñas en estos tipos de redes inalámbricas, considerando dichos criterios antes descritos.

Este análisis de seguridad realizado en redes inalámbricas 802.11 requiere el uso especializado de herramientas que permitan el monitorizar el tráfico, detectar vulnerabilidades y realizar pruebas de penetración. Algunas de las herramientas más populares en este ámbito mencionadas y utilizadas para realizar el proceso de descifrado de claves. (Ver la Tabla 4.)

Tras evaluar estas y otras opciones, las herramientas elegidas como las mejores para el análisis de seguridad en redes 802.11 fueron Kismet y Aircrack-ng. Kismet destaca por su capacidad de detección y monitorización, mientras que Aircrack-ng sobresale en las pruebas de penetración y la evaluación de vulnerabilidades. La combinación de estas dos herramientas brinda una solución completa y efectiva para el análisis de seguridad en entornos inalámbricos. (ver Tabla 9)

Utilizando el formato CVSS:3.0 estándar, la fórmula para la herramienta de hacking ético KISMET sería la siguiente:

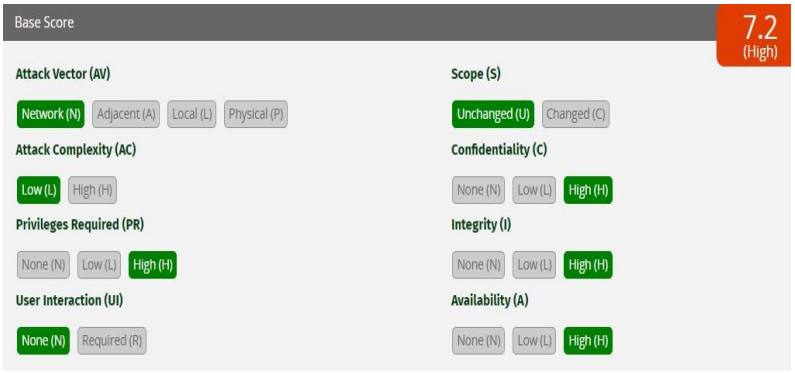


Figura 31. CVSS3 KISMET

CVSS:3.0/AV:[N]/AC:[L]/PR:[H]/UI:[N]/S:[U]/C:[H]/I:[H]/A:[H]

AV (Attack Vector): [N] – Network

KISMET es una herramienta de hacking ético que se utiliza a través de la red.

AC (Attack Complexity): [L] - Low

KISMET fácil de utilizar y no requiere un alto grado de complejidad.

PR (Privileges Required): [H] - High

Se requieren privilegios de usuario avanzados o de administrador.

UI (User Interaction): [N] - None

No requiere interacción del usuario, ya que puede ser ejecutada de forma autónoma.

S (Scope): [U] - Unchanged

No amplía el alcance del impacto más allá del componente objetivo.

C (Confidentiality Impact): [H] - High

Puede comprometer la confidencialidad de los datos y descifrar el tráfico de red.

I (Integrity Impact): [H] - High

KISMET puede permitir la modificación o el control de los datos y sistemas de la red.

A (Availability Impact): [H] – High

HERRAMIENTA DE HACKING ÉTICO AIRCRACK-NG:

CVSS:3.0/AV:[N]/AC:[L]/PR:[H]/UI:[N]/S:[U]/C:[H]/I:[H]/A:[H]

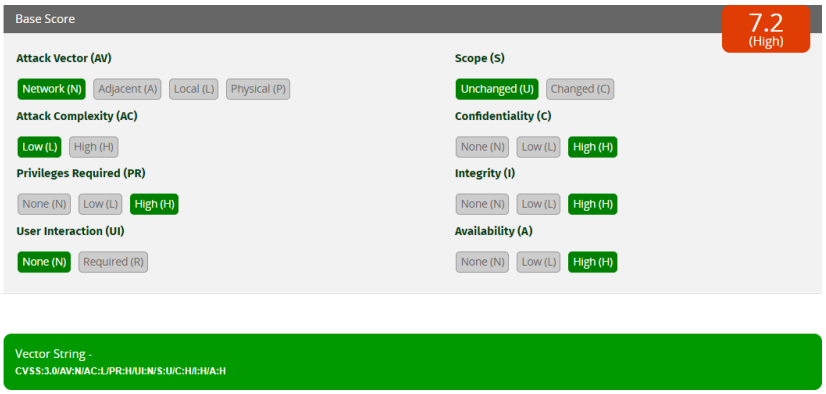


Figura 32. CVSS AIRCRACK-NG

AV (Vector de ataque): [N] - Red

Aircrack-ng es una herramienta de hacking ético que se utiliza a través de la red.

AC (complejidad del ataque): [L] - Baja

Aircrack-ng es una herramienta relativamente fácil de utilizar y no requiere un alto grado de complejidad en su explotación.

PR (privilegios requeridos): [H] - Alto

Para utilizar Aircrack-ng de manera efectiva, se requieren privilegios de usuario avanzados o de administrador.

UI (Interacción del usuario): [N] - Ninguno

Aircrack-ng no requiere interacción del usuario, ya que puede ser ejecutada de forma autónoma.

S (alcance): [U] - Sin cambios

El uso de Aircrack-ng no amplía el alcance del impacto más allá del componente objetivo.

C (Impacto de confidencialidad): [H] - Alto

Aircrack-ng puede comprometer gravemente la confidencialidad de la información al descifrar las contraseñas de redes inalámbricas.

I (Impacto de integridad): [H] - Alto

Aircrack-ng puede permitir la modificación o el control de los datos y sistemas de la red.

A (impacto en la disponibilidad): [H] - Alto

Aircrack-ng puede provocar la denegación de servicio o la indisponibilidad de los sistemas de la red.

Tabla 9. Valoración de herramientas

Herramienta	Aircrack−ng	Kismet
Vector de ataque (AV)	N	N
Complejidad de ataque (AC)	L	L
Privilegios requeridos (PR)	H	H
Interacción del usuario (UI)	N	N
Alcance (S)	U	U
Impacto de confidencialidad (C)	H	H
Impacto de integridad (I)	H	H
Impacto de disponibilidad (A)	H	H

Nota: Información realizada según la investigación[66].

3.3.5 ACTIVACIÓN DE HERRAMIENTAS

En esta gráfica muestra el primer paso que debemos realizar que es instalar el **aircrack-ng** para eso en nuestro terminal colocaremos el siguiente comando **sudo apt install aircrack-ng** de los cual indica que vamos a darle prioridad de super usuario para una correcta instalación.

Figura 33. Instalar el aircrack-ng en el terminal
Fuente: propia

En la siguiente figura mediante el comando colocado en nuestro terminar "**iwconfig"** verificamos si aparece o reconoce el computador la interfaz de nuestro adaptador de red wifi, en este caso aparece "**wlan0**" pero debemos activarlo para posteriormente usarlo.

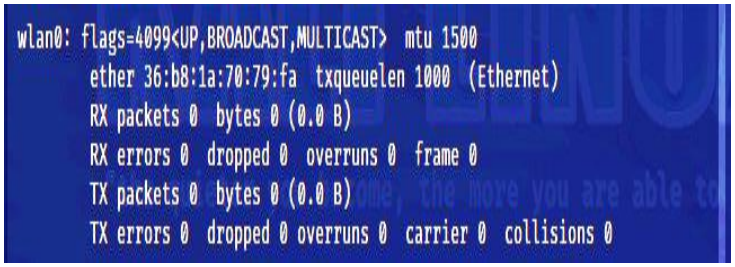


Figura 34. Interfaz de nuestro adaptador de red wifi
Fuente: propia

En esta gráfica muestra en nuestro terminal mediante el comando "**airmon-ng start wlan0"** estamos habilitando el **modo monitor** de nuestro adaptador de red wifi, lo cual es importante para continuar con el proceso, nos muestra un mensaje "**monitor mode enabled**".

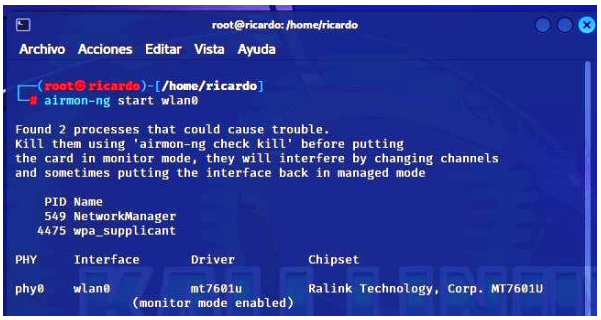


Figura 35. Habilitando el modo monitor
Fuente: Propia

En la gráfica a continuación en el terminal colocamos "**airodump-ng wlan0"** con esto estamos escaneando las redes inalámbricas que detecta nuestro adaptador de red, la gráfica muestra las redes disponibles que puede detectar.

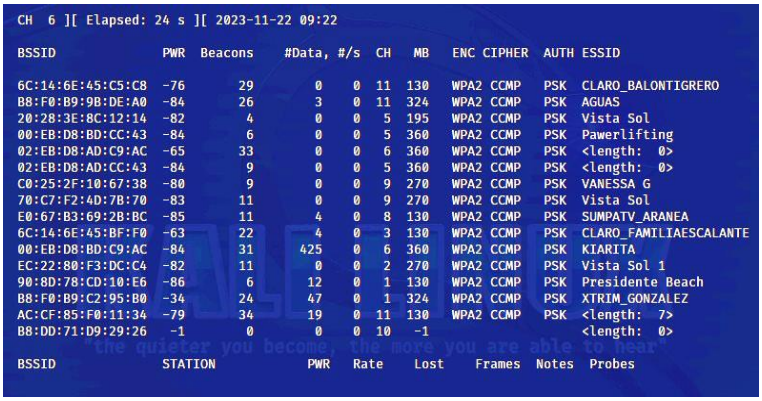


Figura 36. Escaneando las redes inalámbricas
Fuente: propia

3.3.6 ESCENARIO 2 ATAQUE DE DICCIONARIO RED_1

La siguiente gráfica ilustra el proceso de escaneo de redes inalámbricas cercanas utilizando el comando "**airmon-ng start wlan0.**". Además, muestra las redes inalámbricas detectadas por nuestro adaptador de red. Para proceder con el ataque, es necesario seleccionarla.

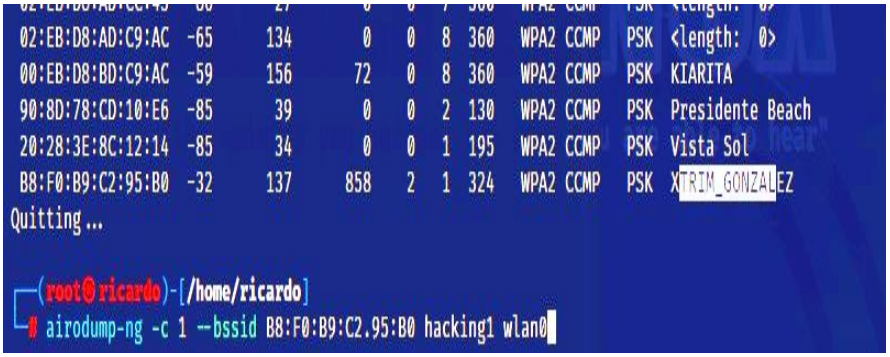


Figura 37. Selección de red.
Fuente: propia

La siguiente ilustración muestra la ejecución del comando **airodump-ng** en la ventana del terminal. Este comando se utiliza para analizar y capturar paquetes de datos de las redes inalámbricas cercanas. El comando **airodump-ng** proporciona información detallada sobre las redes detectadas, incluyendo el nombre de la red (SSID), el canal que utiliza, el tipo de seguridad, la dirección MAC de los dispositivos conectados y la potencia de la señal.

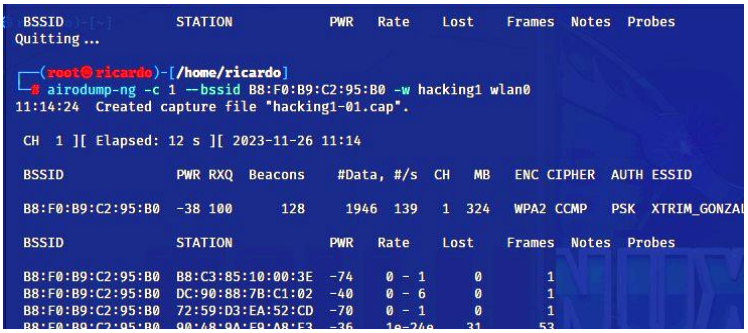


Figura 38. Airodump-ng que nos sirve para analizar y capturar paquetes
Fuente: propia

La siguiente ilustración muestra la generación de tráfico en la red inalámbrica utilizando el comando **aireplay-ng.** El comando **aireplay-ng** es una herramienta versátil que permite generar diferentes tipos de tráfico en redes inalámbricas. En el ejemplo mostrado, el comando genera paquetes de datos dirigidos al dispositivo con dirección MAC 30:B1:B5:92:98:0C en la red con BSSID B8:F0B9:C2:95:B0.

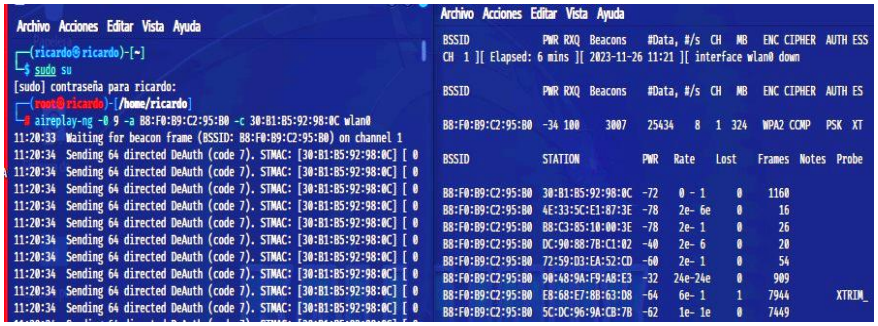


Figura 39. Aireplay-ng genera tráfico en la red
Fuente: Propia

La siguiente ilustración indica que el proceso de generación de tráfico con el comando **aireplay-ng** debe continuar hasta que se capture el **handshake** de la red objetivo. Una vez capturado el **handshake,** se puede utilizar para descifrar la clave de seguridad de la red objetivo y obtener acceso no autorizado.

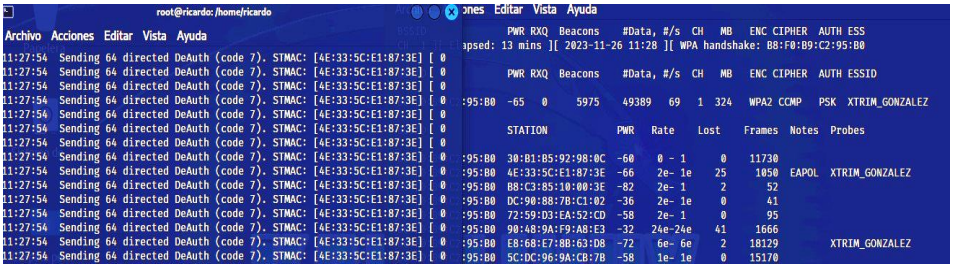


Figura 40. Capturamos el handshake
Fuente: Propia

La siguiente ilustración muestra la ejecución del comando **aircrack-ng** en la ventana del terminal para descifrar la clave de seguridad de una red inalámbrica. En el ejemplo mostrado, el comando **aircrack-ng** utiliza el **handshake** generado con el comando **aireplay-ng**, el diccionario password.txt y el archivo .cap que contiene los paquetes capturados.

Figura 41. Colocamos el airecrack-ng más el handshake generado
Fuente: Propia

La siguiente ilustración marca el inicio del proceso de ataque de diccionario contra la red objetivo. El éxito del ataque de diccionario depende de la complejidad de la contraseña y del tamaño del diccionario. En el ejemplo mostrado, el ataque de diccionario se realiza utilizando el **handshake** generado con el comando **aireplay-ng** en la ilustración anterior y el diccionario **password.txt.**

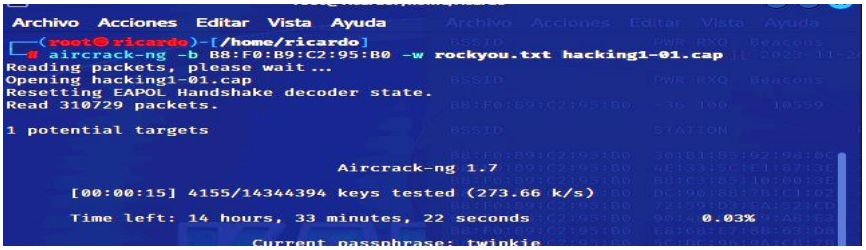


Figura 42. Proceso de ataque de diccionario
Fuente: Propia

El proceso de obtención de la clave de seguridad de la red objetivo se completó en un tiempo total de 7 horas, 3 minutos y 43 segundos. La duración del proceso puede variar significativamente dependiendo de la complejidad de la clave de seguridad, el tamaño del diccionario utilizado y la potencia de procesamiento del equipo.

Figura 43. Tiempo y obtención de contraseña
Fuente: Propia

3.3.7 ESCENARIO 2 ATAQUE DE DICCIONARIO RED_2

La siguiente ilustración muestra la ejecución del comando **airemon-ng start wlan0** en la ventana del terminal para activar el modo monitor en el adaptador de red Wifi. El comando **airemon-ng** es una herramienta que se utiliza para gestionar el modo monitor en los adaptadores de red Wifi.

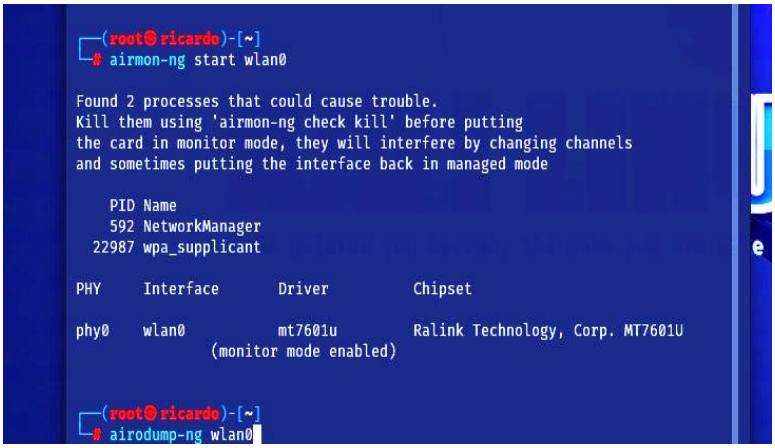


Figura 44. Airemon-ng start wlan0 para activar el modo monitor
Fuente: Propia

Cuando ya hemos seleccionado nuestra víctima en el terminal colocaremos **airodump-ng -c 1 –bssid DE:90:88:7B:41:02 -w ataque wlan0** para saber que dispositivo está conectado para generar tráfico de red.

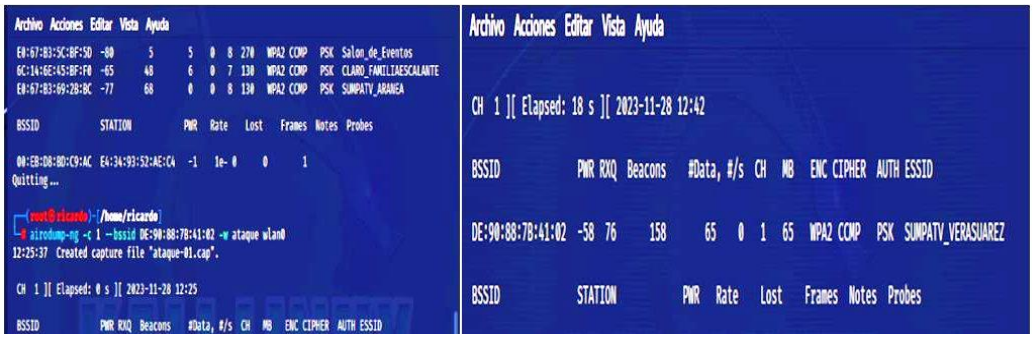


Figura 45. Dispositivo está conectado para generar tráfico de red.
Fuente: Propia

En la siguiente gráfica muestra que en otra terminal colocamos **aireplay-ng -0 9 -a DE:90:88:7B:41:02 -c 1A:32:E2:74:D9:E4** lo cual indica de que **-0 9** Indica que se enviarán 9 paquetes por segundo, **-a DE:90:88:7B:41:02** especifica la BSSID de la red objetivo, que en este caso es DE:90:88:7B:41:02 y **-c 1A:32:E2:74:D9:E4**

define la dirección MAC del cliente objetivo, que en este caso es 1A:32:E2:74:D9:E4.

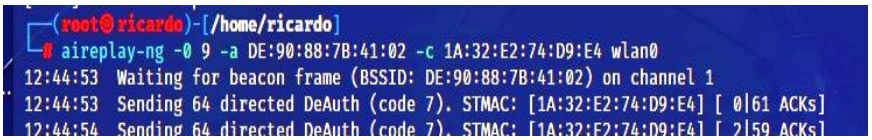


Figura 46. Ejecución de aireplay-ng
Fuente: Propia

La siguiente ilustración indica que es necesario aguardar la carga completa del **handshake** antes de continuar. Este handshake, que representa un intercambio de mensajes criptográficos entre el cliente y el punto de acceso inalámbrico.

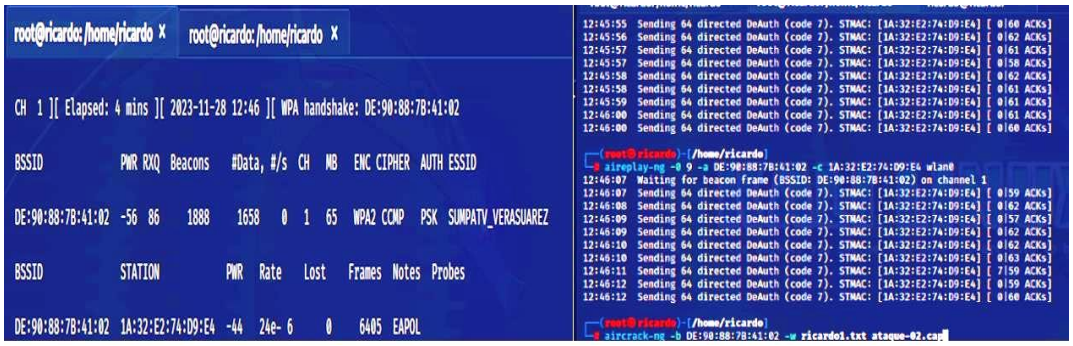


Figura 47. Esperamos hasta que cargue el handshake
Fuente: Propia

En la imagen muestra que mediante el comando colocado en nuestro terminal "**airecrack-ng -b DE:90:88:7B:41:02 -w ricardo1.txt ataque-02.cap"** y tenemos que esperar hasta que pueda encontrar la contraseña del usuario.

Figura 48. Encontramos la contraseña
Fuente: Propia

La tabla muestra los detalles de la fase de explotación, se realizó el proceso de obtención de claves mediante la creación de diccionarios construidos para cada red, utilizando información básica de los usuarios se procedió a realizar el ataque de diccionario o denominado ataque de fuerza bruta. (Ver Tabla 10)

Tabla 10. Resultados de la Fase de Explotación

Fuente: Propia

Resultados de la Fase de Explotación	
Nombre del responsable: **Ricardo González**	Fase: Explotación
Objetivo: Conocer la forma de cómo crear diccionarios para ataques de fuerza bruta o llamado ataque de diccionario, además de descifrar las contraseñas que son de seguridad débiles, fuertes y complejas.	
Tiempo estimado: **10 horas**	**Nivel de complejidad** a.(bajo) b.(medio) c.(alto)
Herramientas tecnológicas utilizadas	
Hardware: **Computadora: Dell** **Adaptador de red: Wireless Adapter 950Mbps 802.11.**	**Software:** Sistema Operativo Kali Linux
Resultado Obtenidos:	
	Detalles encontrados
Red 1 **(XTREAM_GONZALEZ)**	Esta red es tiene una configuración compleja por lo que su contraseña contiene *caracteres especiales, letras mayúsculas y números* su tiempo estimado de conseguir la contraseña de la red fue alrededor de 7 horas con 3 minutos.

Resultados de la Fase de Explotación	
Red 2 **(SUMPATV_VERASUREZ)**	Esta red tiene una configuración no tan compleja por lo que su contraseña solo contiene *números* su tiempo estimado de conseguir la contraseña de la red fue alrededor de 45 segundos, por lo que el diccionario creado fue con información básica del usuario.
Conclusiones: Después de realizar el proceso de obtención de las claves, concluimos que si la contraseña que se coloque a la red wifi tiene caracteres espaciales, números, letras etc. Se considerará una contraseña difícil de descifrar. Además, se podría considerar una recomendación a las personas no dar información relevante a otras personas por lo que podrían ser víctimas de ingeniería social y por lo consiguiente ataque de fuerza bruta o llamado de diccionario robando información.	

3.3.8 FASE 6.- POST EXPLOTACIÓN

Para estos análisis de red wifi se procedió a crear un diccionario con una cantidad significante de palabras relacionadas con información básica de la víctima, en el análisis se recabó información como el ssid, bssid, velocidad, autentificación, algoritmo de cifrado, el canal en el que trabaja, además el tiempo que tomo encontrar la respectiva clave. (Ver Tabla 6 y Tabla 7)

3.3.9 TABLA GENERAL DESCRIPCIÓN DE INFORMACIÓN DE CONTRASEÑAS

En esta tabla se muestra información como las características que contiene cada contraseña, como por ejemplo en la red 1 se consideró una contraseña de nivel alta, por lo que su grado de complejidad de lo cual solo la clase contenía caracteres alfanuméricos y su obtención de clave fue un tiempo estimado de 7 horas con 3 minutos y por último la red número 3 es considerada un nivel baja por lo que su contraseña contenía solo caracteres numéricos y su tiempo de obtención de contraseña fue de 45 segundos, es importante mencionar que el tiempo en las obtenciones de contraseñas depende de mucho del diccionario con la información del usuario.

Tabla 11. Datos Estadísticos de diccionarios

Fuente: Propia

Cantidad de palabras generadas (información)		
Redes (keys tested)		
keys tested	9.524.767/14.344.394	22.530/22.585
Tested Speed	380.51 k/s	517.67 k/s
Search Percentage	66.40%	34.12%

En conclusión, el ataque de diccionario a una red inalámbrica wifi debe involucrar datos de las personas víctimas, para crear un diccionario robusto que contiene caracteres numéricos, alfanuméricos, letras y caracteres especiales. El tiempo en tratar de encontrar la contraseña del usuario dependerá también de que tan profesional este hecho el diccionario para su posterior ataque de fuerza bruta, debemos mencionar que es ilegal este tipo de ataque y es penado por la ley.

3.4 OBJETIVO 3: DESARROLLAR UN INFORME DE ANÁLISIS DE PROTECCIÓN Y RECOMENDACIONES EN REDES INALÁMBRICAS BASADA EN LA SEGURIDAD DE LA INFORMACIÓN.

Se desarrollará un análisis basa en la protección de las redes inalámbricas y la seguridad que con esto conlleva, desde las vulnerabilidades conocidas nos centramos a evaluar para tener una posible solución en el ámbito de los protocolos de seguridad, además de proporcionar posibles recomendaciones que ayuden a proteger las claves de las redes wifi.

3.4.1 REQUERIMIENTOS

Los requerimientos funcionales y no funcionales son dos categorías importantes dentro de esta investigación. Ambos requerimientos son importantes para definir completamente las necesidades y características sobre la investigación.

Tabla 12. Requerimientos Funcionales

Código	REQUERIMIENTOS FUNCIONALES
RF-01	Detallar los componentes que conforman una red inalámbrica, como puntos de acceso y la conexión de dispositivos.
RF-02	Configuración de seguridad de los dispositivos inalámbricos.
RF-03	Identificación de vulnerabilidades conocidas tanto en estándares y protocolos de seguridad inalámbrica.
RF-04	Ejecución de escenarios de penetración para la respetiva evaluación de seguridad en redes inalámbricas.
RF-05	Uso de herramientas de detección y de monitoreo para reducir activades inusuales dentro de una red inalámbrica.
RF-06	Desarrollo de una guía sobre mitigación en ataques informáticos basados en vulnerabilidades en una red inalámbrica.
RF-07	Evaluar la efectividad de las medidas de seguridad mediante pruebas de penetración en el ambiente controlado.
RF-08	Realizar un informe de cumplimiento que documente las acciones y sobre todo recomendaciones orientadas a evaluar la seguridad.

Tabla 13. Requerimientos no Funcionales

Código	REQUERIMIENTOS NO FUNCIONALES
RNF-09	El ambiente de pruebas se la debe realizar de una manera aislada y controlado, sin afectar el rendimiento de operación normal de la red inalámbrica.
RNF-10	Todas las actividades de análisis y pruebas deben cumplir con aspectos legales y éticos.
RNF-11	En la evaluación de seguridad los procesos deben ser documentados de manera detallada y comprensible sobre los resultados obtenidos.
RNF-12	Las herramientas y técnicas utilizadas deben ser y estar respaldadas por alguna organización o comunidad orientada en la seguridad en incidentes informáticas.
RNF-13	Los informes y documentación generada deben cumplir con estándares en seguridad de la información.
RNF-14	La probable solución de seguridad debe ser escalable y adaptable a cambios futuros en la arquitectura de la red inalámbrica.
RNF-15	Las medidas de seguridad no deben afectar significativamente el desempeño y la disponibilidad de la red inalámbrica.
RNF-16	Los resultados del proyecto deben ser presentados de manera clara, concisa y con un lenguaje accesible para diferentes audiencias.

3.4.2 FASE 7

En esta etapa, se recopilan y organizan todas las evidencias recabadas durante las pruebas de penetración y las vulnerabilidades conocidas CVE con el fin de tener un análisis detallado de las pruebas de penetración realizadas. Posteriormente, se elaboró una guía basada y adaptada de un CCN CERT en donde se presentan los resultados de manera clara y concisa, incluyendo, el análisis de riesgos y recomendaciones concretas para mitigar los problemas de seguridad[66].

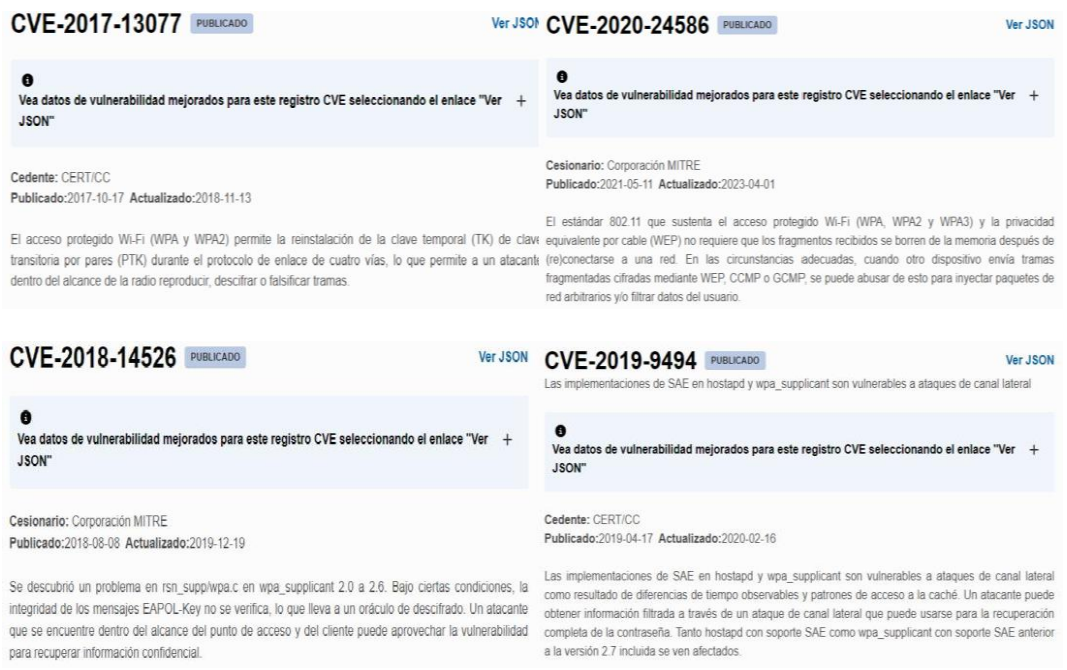


Figura 49. CVE vulnerabilidades[67].

Un CERT (Computer Emergency Response Team) es prácticamente un equipo especializado para la detección, análisis y respuesta inmediata a incidentes de seguridad informática.

Características de los CERT:

- El objetivo de los CERT es minimizar el impacto de los ataques cibernéticos y dar soluciones a sistemas afectados.
- Los CERT brindan servicios como alertas de amenazas, análisis forense y asistencia técnica en respuesta a incidentes.

¿Cuántos CERT existen?

No se registra un número exacto, además de que los CERT se pueden categorizar en diferentes niveles (nacional, gubernamental, sectorial, empresarial, etc.). Pero se estima que existen cientos de CERT en todo el mundo, cada uno de ellos adaptado a las necesidades y ámbito.

¿Por qué debemos usar CNN CERT?

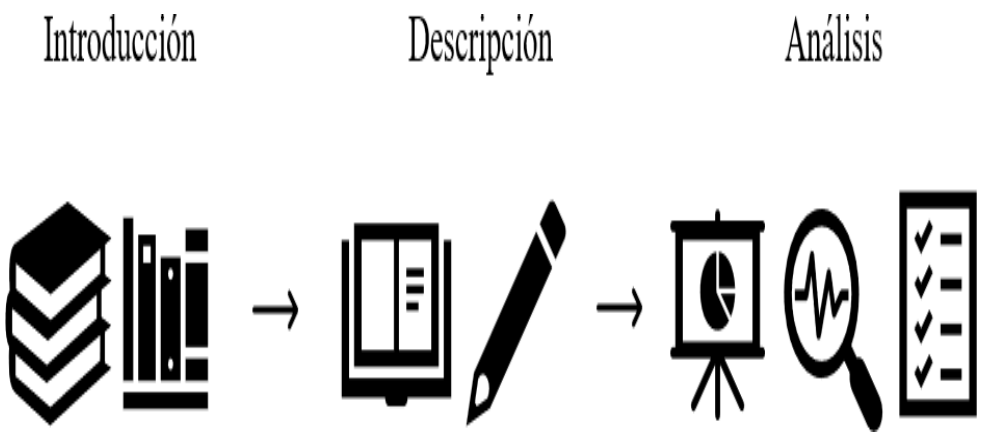
CNN CERT (Computer Network Naming CERT) es un tipo de CERT especializado en detección y mitigación de ataques basados la suplantación de identidad entre otros ataques de hacking ético.

Razones para utilizar CNN CERT:

- Monitorea constantemente para poder detectar patrones de actividad que indiquen intentos de ataques de fuerza bruta o de diccionario.
- Los CNN CERT colaboran estrechamente con otros CERT y equipos de seguridad, lo que permite una respuesta coordinada y más efectiva ante este tipo de ataques.
- Los CNN CERT pueden compartir información y recomendaciones de seguridad relacionadas con los ataques de fuerza bruta y de diccionario.

En conclusión, mientras que un CERT aborda de manera integral los incidentes de seguridad informática, un CNN CERT se especializa en la detección y mitigación de amenazas relacionadas específicamente la infraestructura de Internet.

En base a esta estructura para realizar un informe y mediante una guía CCN CERT, se modificó acorde a esta investigación con fines de obtener resultados basándose a la seguridad de las redes y mejor el cifrado de las claves de acceso a las redes inalámbricas. De esta manera, se aseguró que este informe cumpliera con los más estrictos requisitos de confidencialidad, integridad y disponibilidad de la información, alineándose a las mejores prácticas en materia de ciberseguridad.[67]



Nota: Estructura de proceso de informe

3.4.3 FASE 7.- INFORME

3.4.4 RESUMEN

I. INTRODUCCIÓN

Objetivo, alcance y metodología de estudio

Evaluar la efectividad de las medidas de seguridad implementadas en la red Wi-Fi para garantizar la confidencialidad, integridad y disponibilidad de la información transmitida.

Al someter estos sistemas a posibles vulnerabilidades en un ambiente controlado, se podrán identificar y documentar las brechas de seguridad presentes en las conectividades WiFi. Esta metodología exploratoria permitirá realizar un análisis integral y profundo, con el objetivo de mitigar los ataques informáticos identificados y fortalecer la seguridad de las redes inalámbricas.

Hallazgos clave y recomendaciones de seguridad

Se realizaron ataques de diccionario o denominado ataques de fuerza bruta, a diferentes redes con distintas claves de seguridad en donde se pudo constatar que si se coloca una contraseña más robusta tardaría la obtención de las claves, se podrían dar diversas recomendaciones en ámbitos de contraseñas en colocar caracteres especiales o establecer una seguridad superior a WPA2.

II. DESCRIPCIÓN METODOLOGÍA APLICADA

El proceso de este análisis de seguridad ha sido basado en la metodología PTES que cuenta con 7 fases de los cuales son los siguiente:

a. Interacción previa
b. Recogida de información
c. Modelado de amenazas
d. Análisis de vulnerabilidad
e. Explotación
f. Post explotación
g. Informe

3.4.5 ANÁLISIS DE LA SEGURIDAD DE LA RED

En el campo de la informática y la seguridad en las redes inalámbricas pude ser un poco complicado al principio por lo que existen diversos términos tanto técnicos como algunos conceptos complejos, la seguridad inalámbrica es importante para la correcta protección de la red. Lo siguientes términos son fundamental en la seguridad de las redes inalámbricas.

Confidencialidad: se considera la protección de información contra accesos no permitidos o no autorizados, para tener una confidencialidad segura esto se la puede garantizar mediante contraseñas seguras, un correcto cifrado de datos y restricciones a la red.

Integridad: es la manera de asegurar que la información no sea alterada durante el proceso de transmisión u almacenamiento, se puede aplicar ciertos sistemas de detección de intrusiones lo cual permitirá identificar ciertas anomalías en la red.

Disponibilidad: quiere decir que los recursos e información de la red deben estar obligados a estar disponibles para los usuarios en sus requerimientos, se pude tener una mayor disponibilidad implementando ciertas medidas para mejorar la estabilidad de la red en cualquier momento que el usuario acceda a estos recursos.

Análisis de seguridad basado en los principales pilares de la seguridad informática, confidencialidad, integridad y disponibilidad.

Tabla 14. Análisis de Seguridad

Fuente: Propia

Análisis de seguridad				
Tipo de prueba			Ataque de diccionario o fuerza bruta	
Número de ataque			3	
Tiempo total de duración del (los) ataque(s)			10 horas	
Confidencialidad				
Análisis de redes			Red 1	Red 2
Seguridad (protocolos)			WPA2	WPA2
WEP	WPA	WPA2		

Análisis de seguridad				
Cambio del SSID y contraseña por defecto			✓	✓
Restricción de acceso a la red			✓	✓
Ocultar SSID			x	x
Integridad				
Análisis de redes			Red 1	Red 2
Utilización de contraseñas robustas			Alta	Baja
Alta	Media	Baja		
Desactivación WPS			x	x
Actualización firmware del router			x	x
Disponibilidad				
Análisis de redes			Red 1	Red 2
Cableado de dispositivos			✓	✓
Ubicación adecuada del router			✓	✓
Monitore y mantenimiento			✓	x

III. Análisis de vulnerabilidades en redes inalámbricas 802.11

3.4.6 ANÁLISIS DESCRIPCIÓN DE VULNERABILIDADES

Muchos usuarios conectados

En está gráfica muestra a esta red fue identificada con un SSID oculto lo que significa que no es visible cuando un dispositivo quiere acceder a ella, pero se recopilo información importante sobre a quién pertenecía esta red y cuantos usuarios tiene conectado. (Ver Figura 15)

En está gráfica observamos que en esta red no tenía su SSID de manera oculto lo que significa que cualquier persona puede ver la red mediante su dispositivo, se

recopilo información sobre su tipo de cifrado, usuarios conectados entre otros datos importantes. (Ver Figura 17)

En esta grafica muestra que la red tiene sus SSID de forma visible, además de contener el nombre del proveedor de servidos de internet, el tipo de encriptación es abierto y durante la prueba se detectaron dispositivos conectados a la red. (Ver Figura 16)

3.4.7 ANÁLISIS DE CONTRASEÑAS ENCONTRADAS

En la ilustración se pude apreciar la herramienta que ayuda en la automatización para encontrar la contraseña de la red 1, muestra datos como el tiempo que tomo encontrar la clave, el número de palabras que contiene el diccionario y la velocidad de búsqueda. (Ver Figura 43)

En la ilustración se pude apreciar la herramienta que ayuda en la automatización para encontrar la contraseña de la red 2, muestra datos como el tiempo que tomo encontrar la clave, el número de palabras que contiene el diccionario y la velocidad de búsqueda. (Ver Figura 48)

3.4.8 ANÁLISIS DE CIFRADO DE RED

En está gráfica muestra información como el nombre, dirección MAC, el tipo de red entre otros aspectos importantes y que sirve de mucho para un posterior ataque o análisis a redes inalámbricas.

Figura 50. Información sobre la red
Fuente: Propia

En está gráfica muestra información sobre la red como por ejemplo que el SSID cuenta con veinticuatro caracteres, además podemos observar aspectos importantes como el tipo de encriptación y dispositivos conectados en la red.

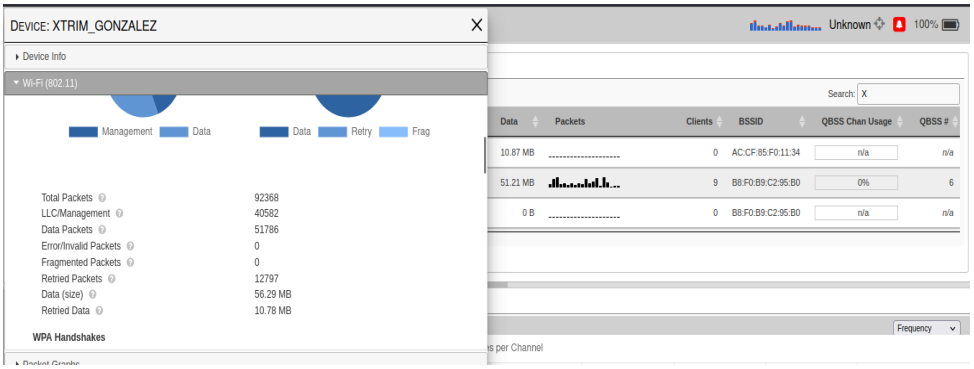


Figura 51. Aspectos importantes el tipo de encriptación y dispositivos en red
Fuente: Propia

En está gráfica muestra información sobre la red, en donde hay aspectos importantes el tipo de encriptación que al parecer el programa lo detecta como abierto, pero utilizando otros métodos se obtuvo el tipo de cifrado y dispositivos conectados en red.

Figura 52. Tipo de encriptación no se puede apreciar
Fuente: Propia

IV. ANÁLISIS DE PRUEBAS DE INTRUSIÓN

TÉCNICAS UTILIZADAS PARA APLICAR ATAQUE DE DICCIONARIO.

La creación de diccionarios puede combinarse para realizar ataques de fuerza bruta, se pude utilizar información obtenida para a través de la ingeniería social para la creación de diccionarios personalizados que podrían incluir palabras o frases

relacionadas a la víctima seleccionada, para eso con ayuda de algunas herramientas se procedió a realizar este ataque.

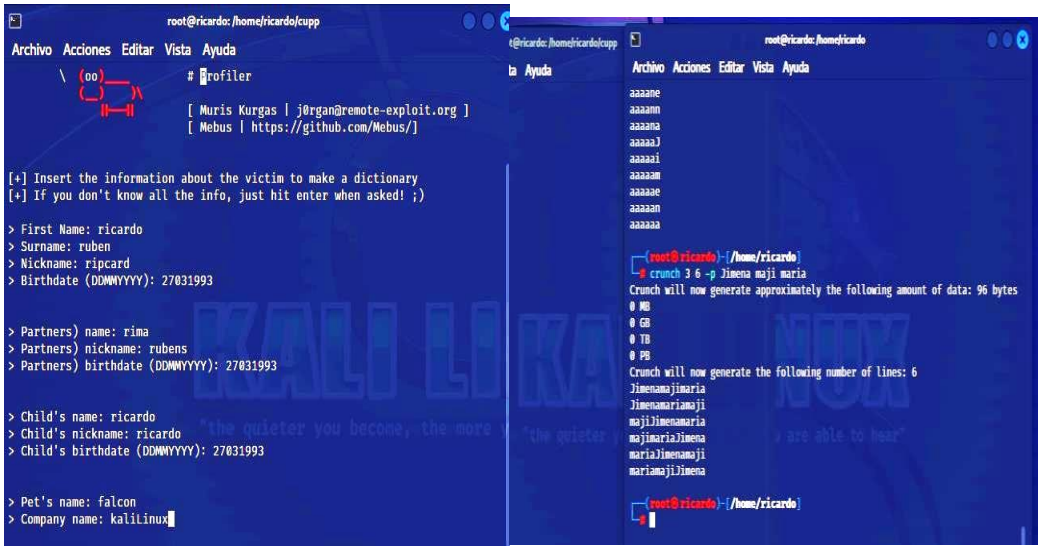


Figura 53. Creación de diccionarios
Fuente: Propia

3.4.10 ATAQUE DE FUERZA BRUTA O DE DICCIONARIO.

Este método se la denomina cracking, consiste en averiguar una clave o contraseña probando un sin número de combinaciones posibles de un diccionario, para este procedimiento se realizó con programas que automatizan estos procesos, el posible éxito de este ataque de diccionario dependerá de que tan alta complejidad este formado la contraseña, si este tipo de clave son simples, si tiene nombre de personas o de lugares tienen un alto grado de susceptibilidad a este tipo de ataque

V. ANÁLISIS DE INFORME DE RESULTADOS

En esta tabla proporcionamos información importante y nuestro comentario sobre el análisis de seguridad realizada sobre la situación actual en la que se encuentran las redes inalámbricas.

Tabla 15. Informe de problemas e inconvenientes
Fuente: Propia

Informe de problemas e inconvenientes		
Debilidad	Situación actual	Comentario del analista
Cifrado débil	La seguridad de las redes	Es recomendable optar por un

Informe de problemas e inconvenientes		
	no se ven tan comprometidas por lo que el tipo de cifrado que utilizan es medianamente seguro en alguno de los casos.	mejor cifrado en redes inalámbricas como es el AES (Advanced Encryption Standard)
Configuración predeterminada	Existe configuración predeterminada pero esencial en ámbito de seguridad.	No se recomienda tener una configuración predeterminada por lo que podría ser propenso a ciertos ataques de Hacking ético.
Falta de autentificación	Una de las redes se la configuro para sin restricciones a la red, solo como tipo de prueba para identificar las cantidades de personas que se podrían conectar.	Observado en el escaneo de la res el uso adecuado de cifrado de autenticación en la red, lo que ayuda a garantizar la confidencialidad y la integridad de los datos transmitidos.
Contraseñas débiles	Algunas redes analizadas y descifradas no poseen una robustes en sus contraseñas es decir que una de las redes posee clave de tipo solo numérico.	Los usuarios podrían mejorar sus contraseñas incluyendo símbolos especiales y mejorando la longitud de los caracteres.
Falta de educación del usuario	Ninguno de los usuarios aplicada alguna medida de seguridad tanto en aspectos físico como en la red.	Es necesario tener algún tipo de conocimientos en el ámbito de las redes y el hacking ético.

Informe de problemas e inconvenientes		
Falta de monitoreo de la red	Ninguna de las redes ha sido monitoreada.	Es recomendable realizar monitoreo en las redes, existen aplicaciones que ayudan de mucho a detectar intrusos en la red inalámbrica.
Uso de dispositivos obsoletos	Una de las redes utiliza router antiguo por lo que disminuye aspectos de fluides en la red afectando la disponibilidad, integridad y confidencialidad.	En el sentido de dispositivos podría haber dispositivos que no dan la garantía basándose en la disponibilidad, integridad y confidencialidad.

VI. RECOMENDACIONES FINALES

Recomendaciones para mejorar la seguridad en las redes inalámbricas.

Objetivo

Proponer recomendaciones necesarias y útiles para mejorar la protección de los datos de los usuarios en redes wifi.

Método

Este respectivo informe fue elaborado mediante una revisión bibliográfica y práctica con respecto a la seguridad wifi.

Resultados

Las comunicaciones y las redes wifi utilizan una forma muy conveniente y popular al acceder al internet, no obstante, son vulnerables a diversos ataques que ponen en riesgo la información de los usuarios.

Para mejorar la seguridad en una red wifi, se podrían seguir las siguientes recomendaciones:

- Se recomienda proporcionar información a los usuarios con conceptos básicos de seguridad en la creación de claves.

- Tener una clave que tenga al menos 10 a 12 caracteres.
- No relacionar información personal en las contraseñas como por ejemplo nombre de algún familiar, fecha de nacimiento, o alguna palabra que se encuentre en el diccionario.
- Crear una clave diferente para cada servicio que el usuario use.
- Es importante actualizar las contraseñas constantemente en cierto lapso de tiempo con el fin de garantizar la seguridad de los datos.
- No se debe compartir contraseñas por medio de servicios de mensajería como por ejemplo correos electrónicos o mensajes de texto.
- Es recomendable tener las claves en un archivo de texto, no almacenado en la nube.
- Aprender a memorizar contraseñas de una manera segura utilizando técnicas de memorización de patrones en el teclado esta técnica depende de una memoria visual que tenga el usuario.
- Realizar escaneos cada cierto tiempo para detectar patrones inusuales en la red.
- Desactivar la visibilidad del SSID.

Recomendaciones generales que van orientadas a la seguridad de las redes inalámbricas como lo es la confidencialidad, integridad y disponibilidad.

Tabla 16. Recomendaciones para mejorar la seguridad en redes wifi

Fuente: Propia

Confidencialidad	Integridad	Disponibilidad
Utilización de cifrado fuerte, mediante configuración en el enrutador con el cifrado WPA2 personal.	Activar el filtro de direcciones MAC ayuda a mantener la seguridad de los dispositivos conectados. Esto permite que los dispositivos autorizados participen y preserven la integridad de la red, evitando así	Optar por un router moderno con el fin de mejorar la cobertura y sobre todo la señal.

	accesos no permitidos de otros equipos.	
Mantener el firmware del enrutador actualizado, es recomendable para disminuir vulnerabilidades.	Utilizar contraseñas robustas en el enrutador con combinaciones de letras, números y caracteres especiales.	Ubicación adecuada del router, recomendable colocarlo en un lugar alto tratando de reducir los obstáculos para que ondas electromagnéticas puedan expandirse.
Desactivación del WPS, es una de las principales causas para que los ciberdelincuentes realicen ataques en especial de fuerza bruta.	Utilizar un firewall, lo cual permitirá bloquear el tráfico no autorizado y prevenir intrusos.	Se recomienda controlar la cantidad de ventanas abiertas con el fin de evitar colapso en la red.

CONCLUSIONES

- Tras aplicar el enfoque PTES se llevó a cabo la comparación de las vulnerabilidades comunes de los protocolos de seguridad wifi, este tipo de análisis logramos identificaron debilidades significativas y puntuales en protocolos antiguos como WEP y WPA lo que representa un alto riesgo para la seguridad de la red. Los protocolos más recientes, como WPA2 y WPA3, presentan mejoras en seguridad y sobre todo resistencia a ataques, reduciendo el nivel de riesgo en comparación con protocolos obsoletos.
  Las alternativas WPA2 y WAP3 permitirán disminuir el riesgo el mismo que se asocia a las redes inalámbricas, mejorando la seguridad en aspectos de confidencialidad, integridad y disponibilidad.
- Mediante el uso del estándar PTES, evaluamos que tan efectivas son las herramientas de hacking ético en el descifrado de contraseñas en redes Wi-Fi, esto permitirá identificar vulnerabilidades en la autenticación de las redes inalámbricas. Así mismo se demostró la importancia de utilizar contraseñas seguras y robustas con la finalidad de disminuir los ataques de descifrado o de fuerza bruta.
- Este informe de recomendaciones se basa y se fundamenta en los principios básicos de la seguridad de la información, es importante por parte de los usuarios o administradores de red implementar medidas se seguridad en redes para salvaguardar la información que circula por la red, además este informe se considera destacables por su enfoque en la seguridad inalámbrica y sobre todo en el tipo de cifrado y como tener contraseñas robustas.

RECOMENDACIONES

- Por lo general es importante realizar de protocolos obsoletos como WEP y WPA a los WPA2 o WPA3 que son más seguros por lo que su propósito es de mitigar los riesgos de seguridad y confidencialidad de los datos en redes inalámbricas. La actualización tanto a nivel de software y hardware brindan esa seguridad de buscar esas posibles amenazas que dañen la integridad de la red, esto garantizará en todos los aspectos tener una solución a la seguridad.
- Implementación de contraseñas seguras es una opción para disminuir riesgo algún ataque de descifrado, con combinaciones complejas de caracteres, utilizar autenticación adecuada para blindar la seguridad de las contraseñas y prevenir ataques de fuerza bruta. Es aconsejable que las contraseñas deben incluir combinaciones de números, caracteres especiales, letras mayúsculas y minúsculas, y por lo general evitar frases, fechas, nombres o palabras comunes o información.
- Optar por la guía propuesta en el informe e implementando medidas de protección e incluso se debe estar al tanto de las actualizaciones y vulnerabilidades en este ámbito de la ciberseguridad. Podemos incluir funcionalidades que son básicas para detectar el tráfico de red y que además de generar informes que son de vital importancia por lo que ayudara a identificar y a solucionar a incidentes de seguridad basadas en redes inalámbricas.

BIBLIOGRAFÍA

[1] F. Z. Chriki, “Sistema de detección de intrusiones en el entorno de ciberseguridad en redes,” Jul. 2022, Accessed: May 09, 2023. [Online]. Available: https://upcommons.upc.edu/handle/2117/373045

[2] C. A. Arney and X. Wang, “Active Snort Rules and the Needs for Computing Resources: Computing Resources Needed to Activate Different Numbers of Snort Rules,” *RIIT 2016 - Proceedings of the 5th Annual Conference on Research in Information Technology*, p. 54, Sep. 2016, doi: 10.1145/2978178.2978189.

[3] B. Adrián. Merino Lluay, “Estudio y evaluación del rendimiento de las técnicas MIMO y BEAMFLEX para diseño de una red inalámbrica para el campus norte de la Universidad Nacional de Chimborazo,” Sep. 2022, Accessed: Jun. 06, 2023. [Online]. Available: http://dspace.unach.edu.ec/handle/51000/9716

[4] M. Bilim, “Performance Analysis of RIS-Assisted Wireless Networks in the Presence of Imperfect Phase Errors,” *AEU - International Journal of Electronics and Communications*, p. 154923, Sep. 2023, doi: 10.1016/J.AEUE.2023.154923.

[5] L. C. Suárez Panchana, “Análisis de vulnerabilidad en la red Lan usando herramientas de hacking ético para una empresa de la provincia de Santa Elena,” Jun. 2022, Accessed: Sep. 10, 2023. [Online]. Available: https://repositorio.upse.edu.ec/handle/46000/7727

[6] C. DE Tecnologías La Información Proyecto De Titulación Previo A La Obtención Del Título De, “UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ FACULTAD DE CIENCIAS TÉCNICAS”.

[7] C. J. Amaguaña Aguilar, “Herramientas de seguridad defensiva y ofensiva para redes lorawan : desarrollo de un prototipo de módulo de análisis de

tráfico basado en wireshark para detección de ataques de denegación usando inspección de tramas lorawan que provea una capa de integración api rest.," 2022, Accessed: Jun. 06, 2023. [Online]. Available: http://bibdigital.epn.edu.ec/handle/15000/23416

[8] J. I. Castillo Mendoza, "Análisis de los sistemas de detección de intrusos (IDS) Open Source y Software Propietario.," 2022, Accessed: Sep. 10, 2023. [Online]. Available: http://dspace.utb.edu.ec/handle/49000/12548

[9] J. M. González González Mentor and N. Torres Batista, "Uso de las Técnicas Del Hacking Ético para la Reducción de Amenazas de Ciberseguridad," 2023, doi: 10.18535/ijecs/v6i4.42.

[10] F. Z. Lidanta, A. Almaarif, and A. Budiyono, "Vulnerability Analysis of Wireless LAN Networks Using Penetration Testing Execution Standard: A Case Study of Cafes in Palembang," *8th International Conference on ICT for Smart Society: Digital Twin for Smart Society, ICISS 2021 - Proceeding*, Aug. 2021, doi: 10.1109/ICISS53185.2021.9533216.

[11] T. Cubillo, D. Tutor, B. Navarro, V. Juan Cotutor, and P. Cámara, "Aplicación de técnicas de Deep Learning en un Sistema de Detección de Intrusos con tráfico de red relacionado con la Dark Web," Sep. 2022, Accessed: May 30, 2023. [Online]. Available: https://riunet.upv.es/handle/10251/185219

[12] H. Guzmán Moreno and Presencial, "Hacking Wireless Usando Parrot y un Adaptador Inalámbrico," Nov. 2022, Accessed: Jun. 18, 2024. [Online]. Available: http://repository.unipiloto.edu.co/handle/20.500.12277/12302

[13] M. Paspuel, "Hack de Redes Wireless con Aircrack-ng," *NEXOS CIENTÍFICOS - ISSN 2773-7489*, vol. 2, no. 2, pp. 16–20, Dec. 2018, Accessed: Oct. 09, 2023. [Online]. Available: https://nexoscientificos.vidanueva.edu.ec/index.php/ojs/article/view/20/155

[14] E. De, I. Electrónica, E. N. Telecomunicaciones, Y. Redes, A. Alejandro, and P. Caluña, "Aplicación de hacking ético para la determinación de vulnerabilidades de acceso a redes inalámbricas WiFi.," 2011, Accessed:

Oct. 09, 2023. [Online]. Available: http://dspace.espoch.edu.ec/handle/123456789/1726

[15] I. En, S. De Información, A. De Vulnerabilidad, Y. Propuesta, D. E. Aseguramiento, and D. E. La, "Análisis de vulnerabilidad y propuesta de aseguramiento de la seguridad de la información en la infraestructura tecnológica de la Empresa 'Internet Los Ríos,'" 2024, Accessed: Mar. 23, 2024. [Online]. Available: http://dspace.utb.edu.ec/handle/49000/15669

[16] W. L. S. Álava, A. R. Rodríguez, X. L. A. Ávila, and O. M. Cornelio, "Redes inalámbricas, su incidencia en la privacidad de la información," *Journal TechInnovation*, vol. 1, no. 2, pp. 104–109, Jul. 2022, doi: 10.47230/JOURNAL.TECHINNOVATION.V1.N2.2022.104-109.

[17] "Plan de Creación de Oportunidades 2021-2025 – Secretaría Nacional de Planificación." Accessed: Oct. 09, 2023. [Online]. Available: https://www.planificacion.gob.ec/plan-de-creacion-de-oportunidades-2021-2025/

[18] F. Antonio Salinas Valencia and I. Miguel Angel Zúñiga Sanchez, "Análisis de vulnerabilidad de la red wifi, del Departamento de TICS del GAD Municipal del cantón Baba," 2021, Accessed: Jun. 20, 2023. [Online]. Available: http://dspace.utb.edu.ec/handle/49000/9514

[19] C. DE Tecnologías La Información Proyecto De Titulación Previo A La Obtención Del Título De, "ANÁLISIS DE VULNERABILIDADES DE LA RED INALÁMBRICA PARA MITIGAR LA INSEGURIDAD DE ATAQUE INFORMÁTICOS," Jan. 2023, Accessed: Sep. 15, 2023. [Online]. Available: http://repositorio.unesum.edu.ec/handle/53000/4798

[20] "Análisis a la seguridad de los activos tecnológicos de red de la Empresa Seguros Comerciales Bolívar S.A." Accessed: Sep. 25, 2023. [Online]. Available: https://repository.unad.edu.co/handle/10596/56392

[21] L. P. MERCHAN ALAY, "POTENCIACION DE LA RED INALAMBRICA PARA EL MEJORAMIENTO DEL SERVICIO DE INTERNET DE LA UNIDAD EDUCATIVA 'DR. JOSÉ VILIULFO

CEDEÑO SÁNCHEZ,’” Mar. 2024, Accessed: Mar. 23, 2024. [Online]. Available: http://repositorio.unesum.edu.ec/handle/53000/6362

[22] C. A. Castro Vasquez, “Pruebas de penetración e intrusión,” Jul. 2019, Accessed: May 11, 2024. [Online]. Available: http://repository.unipiloto.edu.co/handle/20.500.12277/6273

[23] L. G. Torres Vargas, “Red wifi basada en la metodología top - down para mejorar la comunicación de datos en el instituto nacional de estadística e informática – Pucallpa,” 2017, Accessed: Oct. 09, 2023. [Online]. Available: https://repositorio.uap.edu.pe/xmlui/handle/20.500.12990/7626

[24] “Estudio de seguridad en las bases de datos, mediante metodologías de Pen Test, Ethical Hacking en la Secretaria de Hacienda Municipal de Los Patios.” Accessed: Oct. 09, 2023. [Online]. Available: https://repository.unad.edu.co/handle/10596/21194

[25] B. Guamán and J. Alexander, “Análisis de riesgo en redes wifi aplicando técnicas de hacking ético,” 2019, Accessed: Oct. 09, 2023. [Online]. Available: http://dspace.udla.edu.ec/handle/33000/10769

[26] F. Pablo, R. Navarro, A. Jesús, N. Urbaneja, J. Francisco, and C. García, “Análisis teórico y experimental sobre seguridad en redes Wi-Fi,” Nov. 2014, Accessed: Oct. 09, 2023. [Online]. Available: https://riuma.uma.es/xmlui/handle/10630/8409

[27] R. R. Asaad, “Penetration Testing: Wireless Network Attacks Method on Kali Linux OS,” *Academic Journal of Nawroz University*, vol. 10, no. 1, pp. 7–12, Feb. 2021, doi: 10.25007/AJNU.V10N1A998.

[28] “Análisis a la seguridad de los activos de información tecnológicos de la Empresa ECOMIL SAS, bajo la metodología PTES.” Accessed: Sep. 25, 2023. [Online]. Available: https://repository.unad.edu.co/handle/10596/57306

[29] C. Práctico, “UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN MODALIDAD: EXAMEN COMPLEXIVO".

[30] K. Sood *et al.*, "Performance Evaluation of a Novel Intrusion Detection System in Next Generation Networks," *IEEE Transactions on Network and Service Management*, 2023, doi: 10.1109/TNSM.2023.3242270.

[31] Wlan, "TRABAJO DE FIN DE CARRERA TÍTULO DEL TFC: Criptoanálisis práctico de WEP y WPA sobre".

[32] R. Fabian Patiño Hinojosa Bryan Alexis Pozo Vallejo and V. Emma Soria Maldonado Quito -Ecuador, "Análisis de rendimiento del estándar 802.11ax aplicando OFDMA mediante software de simulación," 2022, Accessed: Apr. 29, 2024. [Online]. Available: http://dspace.ups.edu.ec/handle/123456789/22768

[33] B. P. Huerta and R. Jhoel, "Evaluación de técnicas de hacking ético para analizar la seguridad informática de la municipalidad distrital de los Olivos, Lima," *Repositorio Institucional - USS*, 2022, Accessed: Apr. 29, 2024. [Online]. Available: http://repositorio.uss.edu.pe//handle/20.500.12802/9377

[34] B. C. Celis, J. Abelardo, B. O. Romero, A. Jhonatan, M. A. Urrutia, and C. William, "Evaluación del desempeño de protocolos de seguridad para combatir ataques en redes inalámbricas wi-fi," *Repositorio Institucional - USS*, 2022, Accessed: Nov. 11, 2023. [Online]. Available: http://repositorio.uss.edu.pe//handle/20.500.12802/10055

[35] "HashCatch: Capturar Handshakes en Redes WiFi Cercanas » EsGeeks." Accessed: May 28, 2024. [Online]. Available: https://esgeeks.com/hashcatch-capturar-handshakes-redes-wifi/

[36] A. Khalajmehrabadi, N. Gatsis, and D. Akopian, "Modern WLAN Fingerprinting Indoor Positioning Methods and Deployment Challenges," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 3, pp. 1974–2002, Jul. 2017, doi: 10.1109/COMST.2017.2671454.

[37] B. W. Abeysundara and A. E. Kamal, “High-speed local area networks and their performance,” *ACM Computing Surveys (CSUR)*, vol. 23, no. 2, pp. 221–264, Jun. 1991, doi: 10.1145/103724.103726.

[38] “¿Qué es la ciberseguridad?” Accessed: May 11, 2024. [Online]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[39] “Análisis y evaluación de la virtualización de redes Inalámbricas con SDN - hdl:11349/28678.” Accessed: Mar. 23, 2024. [Online]. Available: https://repository.udistrital.edu.co/handle/11349/28678

[40] V. Gaitán, G. Tutor, P. Serrano Yáñez-Mingot, C. Jesús, and B. Cano, “Monitorización y análisis del tráfico en redes inalámbricas 802.11.” 2017. Accessed: May 28, 2024. [Online]. Available: https://hdl.handle.net/10016/27611

[41] “Secrets of a Super Hacker : The Knightmare : Free Download, Borrow, and Streaming : Internet Archive.” Accessed: May 11, 2024. [Online]. Available: https://archive.org/details/Secrets_of_a_Super_Hacker/page/n13/mode/2up?view=theater

[42] L. Á. Ramos Ayuque and D. Torres Landeo, “Servidor Radius en el control de acceso a la red inalámbrica de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica.” Universidad Nacional de Huancavelica, Nov. 17, 2021. Accessed: Mar. 23, 2024. [Online]. Available: https://repositorio.unh.edu.pe/handle/UNH/4906

[43] R. I. Salinas Vasquez, “Análisis de las vulnerabilidades del protocolo de seguridad WPA y WPA2 en redes inalámbricas.,” Sep. 2023, Accessed: Nov. 11, 2023. [Online]. Available: https://repositorio.upse.edu.ec/handle/46000/10300

[44] J. Manuel and M. Molina, “Seguridad en redes inalámbricas 802.11,” *Sistemas y Telemática*, vol. 2, no. 3, pp. 13–28, Jul. 2004, doi: 10.18046/SYT.V2I3.934.

[45] J. Pablo and O. Delgado, “Análisis de seguridad y calidad de aplicaciones (Sonarqube),” 2015, Accessed: Jun. 01, 2024. [Online]. Available: https://openaccess.uoc.edu/handle/10609/43263

[46] A. Villanueva Orea, “Técnicas avanzadas de ciberseguridad para entornos de teletrabajo,” Dec. 2020, Accessed: Jun. 01, 2024. [Online]. Available: https://riunet.upv.es/handle/10251/157713

[47] “Cámara de ambiente controlado.” Accessed: Jun. 01, 2024. [Online]. Available: https://repository.upb.edu.co/handle/20.500.11912/3647

[48] J. Larenas and A. Rosero, “Medusa herramienta para realizar ataques de fuerza bruta,” *NEXOS CIENTÍFICOS - ISSN 2773-7489*, vol. 4, no. 2, pp. 27–31, Dec. 2020, Accessed: Jun. 01, 2024. [Online]. Available: https://nexoscientificos.vidanueva.edu.ec/index.php/ojs/article/view/34/159

[49] A. F. Yánez Tapia, “Ataque de diccionario mediante el análisis y recolección de datos de las redes sociales.” 2023. Accessed: Jun. 01, 2024. [Online]. Available: https://repositorio.puce.edu.ec/handle/123456789/42686

[50] M. C. en Roberto Hernández Sampieri, C. Fernández Collado, D. Pilar Baptista Lucio, and M. de la Luz Casas Pérez, “METODOLOGÍA DELA INVESTIGACIÓN,” 1991.

[51] R. Hernández Sampieri, C. Fernández Collado, D. María del Pilar Baptista Lucio, and S. Méndez Valencia Christian Paulina Mendoza Torres, “Con la colaboración de”.

[52] M. Torres, K. Paz, and F. G. Salazar, “Métodos de recolección de datos para una investigación,” 2019, Accessed: Oct. 09, 2023. [Online]. Available: http://148.202.167.116:8080/xmlui/handle/123456789/2817

[53] F. De *et al.*, “Aplicación de la metodología OSSTMM para la seguridad de la red inalámbrica de la Universidad Técnica del Norte mediante herramientas de Kali Linux,” Jun. 2019, Accessed: Oct. 09, 2023. [Online]. Available: http://repositorio.utn.edu.ec/handle/123456789/9357

[54] E. L. Cayambe López, "'Desarrollo de una ficha integral para la empresa Impactex con el fin de optimizar y facilitar el proceso de producción," 2024, Accessed: Jun. 18, 2024. [Online]. Available: https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/41140

[55] A. Sorribas Segura, "Definición de una metodología para el análisis informático forense en entornos IoT," Sep. 2022, Accessed: Sep. 25, 2023. [Online]. Available: https://riunet.upv.es/handle/10251/186198

[56] "Penetration Testing Execution Standard (PTES) | Cyberzaintza." Accessed: May 28, 2024. [Online]. Available: https://www.ciberseguridad.eus/ciberpedia/marcos-de-referencia/penetration-testing-execution-standard-ptes

[57] "The Penetration Testing Execution Standard." Accessed: May 28, 2024. [Online]. Available: http://www.pentest-standard.org/index.php/Main_Page

[58] "Penetration Testing Execution Standard (PTES) | Minery Report S.L." Accessed: May 28, 2024. [Online]. Available: https://mineryreport.com/ciberseguridad/glosario/conceptos-generales/termino/penetration-testing-execution-standard-ptes/

[59] "Ley de Protección de Datos Personales en Ecuador - Russell Bedford EC." Accessed: Apr. 21, 2024. [Online]. Available: https://russellbedford.com.ec/ley-de-proteccion-de-datos-personales-en-ecuador/

[60] "COIP – Servicio Nacional de Contratación Pública." Accessed: Apr. 28, 2024. [Online]. Available: https://portal.compraspublicas.gob.ec/sercop/cat_normativas/coip

[61] D. Trabajo and D. E. Titulación, "Análisis comparativo del desempeño del estándar IEEE 802,11ac respecto al IEEE 802.11n a través de simulación numérica apoyada por software," 2015, Accessed: Jun. 01, 2024. [Online]. Available: http://dspace.ups.edu.ec/handle/123456789/10181

[62] “Common Vulnerability Scoring System SIG.” Accessed: Jun. 01, 2024. [Online]. Available: https://www.first.org/cvss/

[63] “CVE Website.” Accessed: Jun. 01, 2024. [Online]. Available: https://www.cve.org/

[64] G. Gori, L. Rinieri, A. Melis, A. Al Sadi, F. Callegati, and M. Prandini, “A Systematic Analysis of Security Metrics for Industrial Cyber–Physical Systems,” *Electronics 2024, Vol. 13, Page 1208*, vol. 13, no. 7, p. 1208, Mar. 2024, doi: 10.3390/ELECTRONICS13071208.

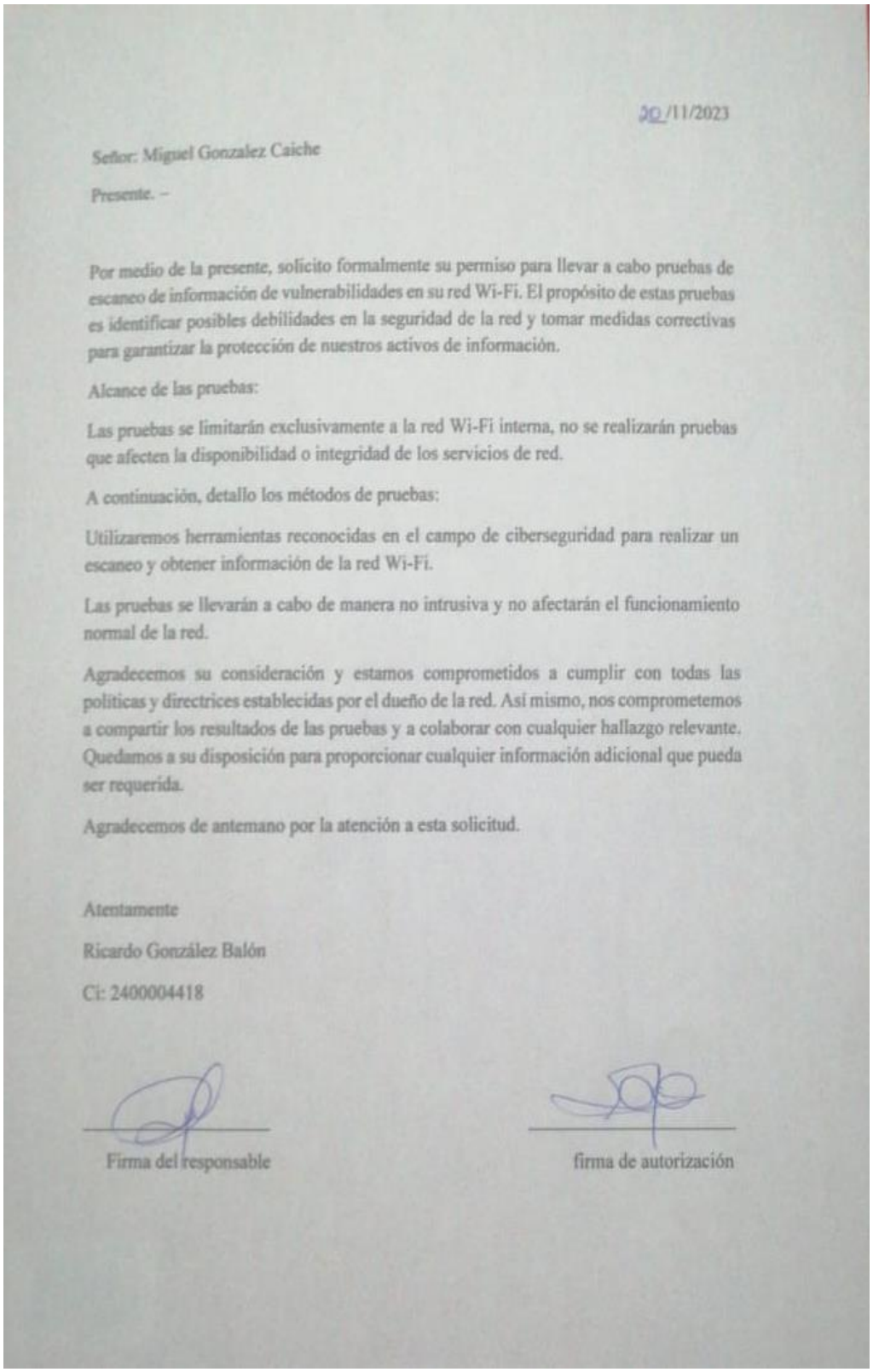
[65] “GitHub - Mebus/cupp: Common User Passwords Profiler (CUPP).” Accessed: Jun. 18, 2024. [Online]. Available: https://github.com/Mebus/cupp

[66] D. Sanz Esteban, “Análisis de la aplicabilidad de las Recomendaciones para métodos de evaluación y examen en remoto del CCN-CERT y su aplicabilidad en el ámbito universitario,” *La Ley privacidad, ISSN-e 2659-8698, Nº. 8 (Abril-junio 2021), 2021*, no. 8, p. 10, 2021, Accessed: Jun. 06, 2024. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=8098213&info=resumen&idioma=ENG

[67] Borja. Pareja García, J. M. Gracia De Castro, and P. De. Pitta Simoes, “Gestión de crisis de compliance ante un ciberincidente : estudio de diferentes estrategias de comunicación para reducir el impacto reputacional,” *Compliance y lucha contra la corrupción en España, Portugal e Iberoamérica*, pp. 103–125, 2021.

ANEXOS

Anexo (solicitudes de permisos a usuarios propietarios de la red)



20 /11/2023

Señor: Miguel Gonzalez Caiche

Presente. –

Por medio de la presente, solicito formalmente su permiso para llevar a cabo pruebas de escaneo de información de vulnerabilidades en su red Wi-Fi. El propósito de estas pruebas es identificar posibles debilidades en la seguridad de la red y tomar medidas correctivas para garantizar la protección de nuestros activos de información.

Alcance de las pruebas:

Las pruebas se limitarán exclusivamente a la red Wi-Fi interna, no se realizarán pruebas que afecten la disponibilidad o integridad de los servicios de red.

A continuación, detallo los métodos de pruebas:

Utilizaremos herramientas reconocidas en el campo de ciberseguridad para realizar un escaneo y obtener información de la red Wi-Fi.

Las pruebas se llevarán a cabo de manera no intrusiva y no afectarán el funcionamiento normal de la red.

Agradecemos su consideración y estamos comprometidos a cumplir con todas las políticas y directrices establecidas por el dueño de la red. Así mismo, nos comprometemos a compartir los resultados de las pruebas y a colaborar con cualquier hallazgo relevante. Quedamos a su disposición para proporcionar cualquier información adicional que pueda ser requerida.

Agradecemos de antemano por la atención a esta solicitud.

Atentamente

Ricardo González Balón

Ci: 2400004418

Firma del responsable

firma de autorización

20/11/2023

Señora: Vanessa Suárez Tomalá

Presente. –

Por medio de la presente, solicito formalmente su permiso para llevar a cabo pruebas de escaneo de información de vulnerabilidades en su red Wi-Fi. El propósito de estas pruebas es identificar posibles debilidades en la seguridad de la red y tomar medidas correctivas para garantizar la protección de nuestros activos de información.

Alcance de las pruebas:

Las pruebas se limitarán exclusivamente a la red Wi-Fi interna, no se realizarán pruebas que afecten la disponibilidad o integridad de los servicios de red.

A continuación, detallo los métodos de pruebas:

Utilizaremos herramientas reconocidas en el campo de ciberseguridad para realizar un escaneo y obtener información de la red Wi-Fi.

Las pruebas se llevarán a cabo de manera no intrusiva y no afectarán el funcionamiento normal de la red.

Agradecemos su consideración y estamos comprometidos a cumplir con todas las políticas y directrices establecidas por el dueño de la red. Así mismo, nos comprometemos a compartir los resultados de las pruebas y a colaborar con cualquier hallazgo relevante. Quedamos a su disposición para proporcionar cualquier información adicional que pueda ser requerida.

Agradecemos de antemano por la atención a esta solicitud.

Atentamente

Ricardo González Balón

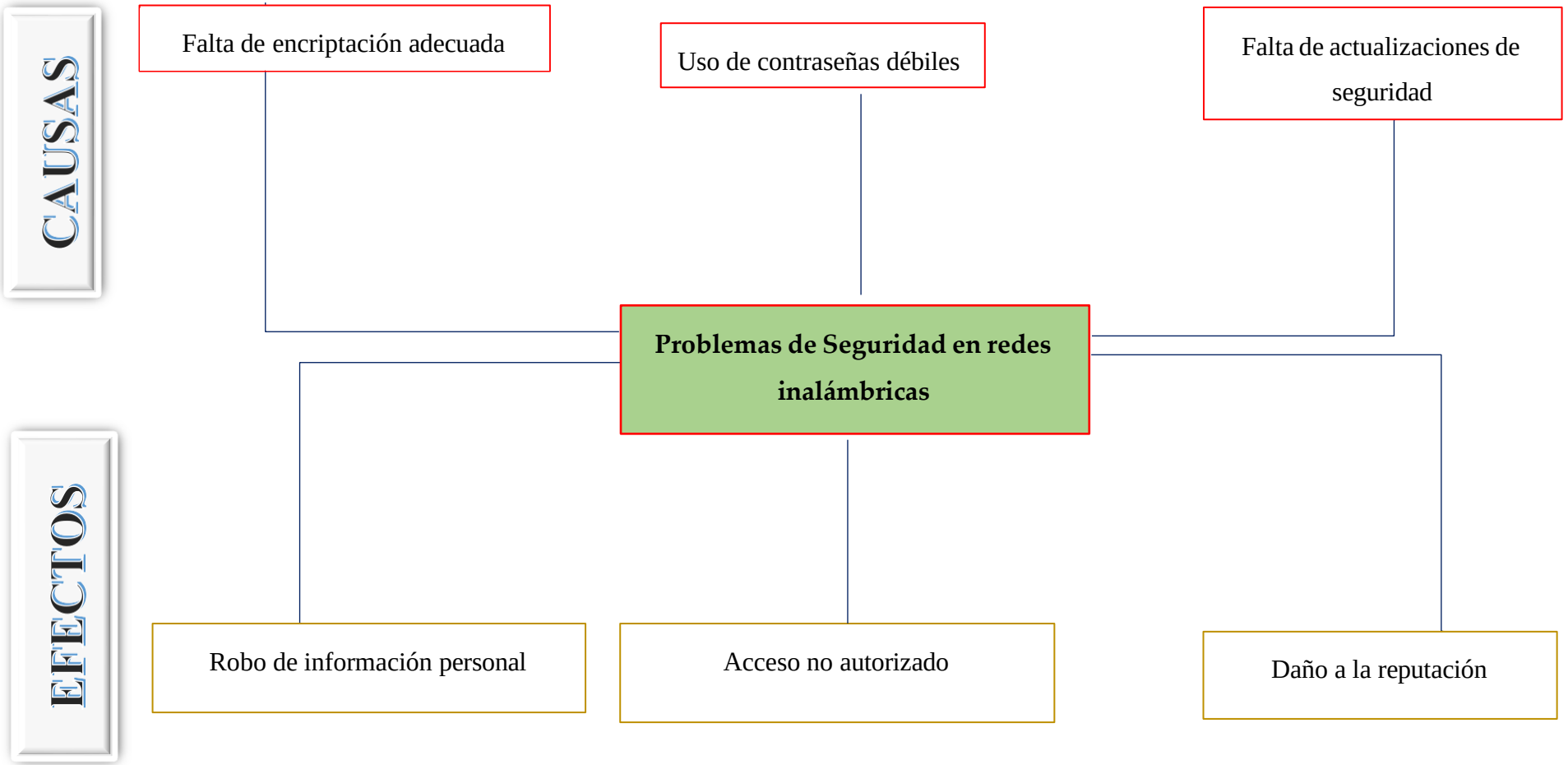
Ci: 2400004418

Firma del responsable

firma de autorización

FICHA DE OBSERVACIÓN

Nombre del responsable: **Ricardo González Balón**	**Fase:** **Escaneo**
Objetivo:	
Tiempo estimado:	Nivel de complejidad a.(bajo) b.(medio) c.(alto)
Herramientas tecnológicas utilizadas	
Hardware:	
Software:	
Técnicas:	
Resultados:	


CAUSAS
Falta de encriptación adecuada
Uso de contraseñas débiles
Falta de actualizaciones de seguridad
Problemas de Seguridad en redes inalámbricas
EFECTOS
Robo de información personal
Acceso no autorizado
Daño a la reputación