UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERIA
CARRERA DE TELECOMUNICACIONES

Análisis y evaluación de la red inalámbrica de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo para determinar el nivel de seguridad mediante herramientas de software libre

Trabajo de Titulación para optar al título de:
Ingeniero en Telecomunicaciones

Autor:
Myrian Janeth Rochina Rochina

Tutor:
MgSc. José Luis Jinez Tapia

Riobamba, Ecuador. 2024

DECLARATORIA DE AUTORÍA

Yo, **Myrian Janeth Rochina Rochina**, con cédula de ciudadanía **0202286357**, autora del trabajo de investigación titulado: **Análisis y evaluación de la red inalámbrica de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo para determinar el nivel de seguridad mediante herramientas de software libre**, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autora de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 13 de mayo de 2024.

Myrian Janeth Rochina Rochina

C.I: 0202286357

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

En la Ciudad de Riobamba, a los 09 días del mes de abril de 2024, luego de haber revisado el Informe Final del Trabajo de Investigación presentado por el estudiante **MYRIAN JANETH ROCHINA ROCHINA** con CC: **0202286357**, de la carrera **de TLECOMUNIACIONES** y dando cumplimiento a los criterios metodológicos exigidos, se emite el **ACTA FAVORABLE DEL INFORME FINAL DEL TRABAJO DE INVESTIGACIÓN** titulado **"ANÁLISIS Y EVALUACIÓN DE LA RED INALÁMBRICA DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO PARA DETERMINAR EL NIVEL DE SEGURIDAD MEDIANTE HERRAMIENTAS DE SOFTWARE LIBRE"**, por lo tanto se autoriza la presentación del mismo para los trámites pertinentes.

Firmado electrónicamente por:
JOSE LUIS JINEZ TAPIA

Mgs. José Luis Jinez Tapia
TUTOR(A)

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **ANÁLISIS Y EVALUACIÓN DE LA RED INALÁMBRICA DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO PARA DETERMINAR EL NIVEL DE SEGURIDAD MEDIANTE HERRAMIENTAS DE SOFTWARE LIBRE**, presentado por **Myrian Janeth Rochina Rochina**, con cédula de identidad número 0202286357, bajo la tutoría de Mg. José Luis Jinez Tapia; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 13 de mayo de 2024.

Deysi Vilma Inca Balseca, Mgs.
PRESIDENTE DEL TRIBUNAL DE GRADO

Manuel Antonio Meneses Freire, PhD.
MIEMBRO DEL TRIBUNAL DE GRADO

Yesenia Elizabeth Cevallos Villacres, PhD.
MIEMBRO DEL TRIBUNAL DE GRADO

CERTIFICADO ANTIPLAGIO

Dirección
Académica
VICERRECTORADO ACADÉMICO

en movimiento
SGC
SISTEMA DE GESTIÓN DE LA CALIDAD

UNACH-RGF-01-04-08.15
VERSIÓN 01: 06-09-2021

C E R T I F I C A C I Ó N

Que, **ROCHINA ROCHINA MYRIAN JANETH** con CC: **0202286357**, estudiante de la Carrera de **TELECOMUNICACIONES**, Facultad de **INGENIERÍA**; ha trabajado bajo mi tutoría el trabajo de investigación titulado " **ANÁLISIS Y EVALUACIÓN DE LA RED INALÁMBRICA DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO PARA DETERMINAR EL NIVEL DE SEGURIDAD MEDIANTE HERRAMIENTAS DE SOFTWARE LIBRE**", cumple con el 4 %, de acuerdo al reporte del sistema Anti plagio **TURNITIN**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 26 de abril de 2024

JOSE LUIS JINEZ TAPIA

Mgs. José Jinez
TUTOR(A)

DEDICATORIA

A mis padres quienes con su sacrificio, amor y sabiduría me han guiado para logar uno de mis sueños. A mis hermanos por sus palabras de aliento y apoyo constante durante todas las etapas de mi vida. A mi cuñada por ser la hermana que no tuve. A mis adorados sobrinos, quienes llenan mi vida de alegría y risas. A todos ustedes con infinito amor.

Myrian

AGRADECIMIENTO

Agradezco a Dios, por darme vida y salud a lo largo de este viaje académico. A mis padres, por brindar apoyo moral y económico durante toda mi vida, mi logro también es su logro.

A mi hermano César, gracias por ser mi guía y tus consejos durante mi formación profesional. A mi hermano Joffre, gracias por tu compañía y apoyo en una ciudad lejana.

A mi tutor de tesis, quien con sus valiosos conocimientos me guio durante este proceso de culminación del trabajo de investigación.

Myrian

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Las redes inalámbricas son más vulnerables a cualquier tipo de amenazas, por que utilizan el aire como medio de transporte de datos. Existen múltiples herramientas de software libre para realizar escaneos y ataques con el fin de evaluar la red. El objetivo principal de esta investigación es analizar y evaluar la red inalámbrica de la Facultad de Ingeniería UNACH, mediante una serie de procedimientos de OSSTMM, primero se realiza el estudio de la información proporcionado por el analista de DTIC identificando las vulnerabilidades en las contraseñas que utilizan en el proceso de autenticación, se crea un escenario de pruebas combinando escenario virtual y físico, y se realiza pruebas de ataque de Fuerza Bruta y Diccionario, Denegación de Servicio y Fake/Rogue AP para medir la confidencialidad, integridad y disponibilidad, una vez obtenido los resultados se utiliza la sección de análisis de riesgo del SGSI, se determinó que el nivel de seguridad en el Bloque A es MEDIO y para el Bloque B es MEDIO. Se recomienda a los administradores de DTIC utilizar contraseñas más robustas, monitoreo constante para detectar intrusos a la red, capacitar a los usuarios e investigar medidas de seguridad actualizadas con el fin de brindar el servicio de red inalámbrico eficaz y confiable.

Palabras claves: vulnerabilidad, amenazas, confidencialidad, integridad, disponibilidad, ataques, OSSTMM, SGSI.

ABSTRACT

The main objective of this research study was to focus on wireless networks that are vulnerable to any kind of threats. Because, those use the air as a data transport medium. There are multiple free software tools to perform scans and attacks in order to evaluate the network. The main objective of this research is to analyze and evaluate the wireless network of the Faculty of Engineering UNACH, through a series of OSSTMM procedures, first we study the information provided by the DTIC analyst identifying vulnerabilities in the passwords used in the authentication process, A test scenario is created combining virtual and physical scenarios, and Brute Force and Dictionary, Denial of Service and Fake/Rogue AP attack tests are performed to measure confidentiality, integrity and availability. Once the results are obtained, the risk analysis section of the ISMS is used. It is recommended that DTIC administrators use stronger passwords, constant monitoring to detect network intruders, train users and investigate updated security measures in order to provide effective and reliable wireless network service.

Keywords: vulnerability, threats, confidentiality, integrity, availability, attacks, OSSTMM, ISMS.

Reviewed by:
Marco Antonio Aquino
ENGLISH PROFESSOR
C.C. 1753456134

1. CAPÍTULO I

1.1 Introducción

Una red inalámbrica es un sistema de comunicación que utiliza el estándar IEEE 802.11y sus diversas versiones incluyen mejoras en la velocidad, el alcance y la seguridad. Permite la conexión de dispositivos a través de señales de radiofrecuencia en el rango de los 2.4 GHz o 5GHz[1].

A lo largo de los últimos años se ha visto un gran avance en el desarrollo de las comunicaciones a través de redes inalámbricas por las ventajas que poseen en cuanto a la movilidad, facilidad de instalación y flexibilidad[2], ya que permiten llegar a zonas donde no es posible la implementación de la red mediante cables. Sin embargo, en este tipo de redes la seguridad ha sido una desventaja porque la señal que se propaga es incontrolable y libre[3] dando lugar a que cualquiera pueda captar la información que se está transmitiendo, poniendo en peligro la confidencialidad e integridad de la misma.

De ahí nace el interés de contar con medidas de seguridad para proteger el sistema de la red inalámbricas[4] que requiere una combinación de medidas técnicas administrativas y de concienciación. La elección de las medidas de seguridad depende de las necesidades y el entorno especifico, pero es esencial implementar un enfoque integral para proteger eficazmente los datos y los recursos de la red.

Existen múltiples herramientas de software libre disponibles que desempeñan un papel fundamental en la detección y mitigación de posibles puntos de accesos no autorizados ya sean routers, dispositivos móviles u otros dispositivos. Wireshark, Nmap, Kismet, Aircrack-ng y muchos otros, permiten a los administradores de red y profesionales de seguridad llevar a cabo escaneos exhaustivos de la red para identificar cualquier dispositivo no autorizado que pueda representar una amenaza.

La situación actual de las redes inalámbricas necesita una solución emergente con relación a la seguridad. La aplicación de medidas técnicas y monitoreo por parte de los administradores de red utilizando herramientas de software libre, sirve como una barrera sólida para abordar la problemática garantizando la confidencialidad, integridad y disponibilidad de las redes inalámbricas.

Esta investigación tiene como finalidad analizar y evaluar el nivel de seguridad de la red inalámbrica de la Facultad de Ingeniería de la UNACH, para la cual se propone un estudio basado en cuatro etapas. En la etapa 1 se estudia la topología de red inalámbrica de la Facultad de Ingeniería, en la etapa 2 se establece los controles que ha posterior servirá para evaluar la red inalámbrica, mientras que en la etapa 3 se implementa un escenario de pruebas donde se simula la red inalámbrica. Finalmente, en la etapa 4 se evalúa los controles de

seguridad aplicando los criterios de evaluación del Sistema de Gestión de Seguridad Informática (SGSI) para determinar el nivel de seguridad.

1.2 Planteamiento del problema

La seguridad es un tema de vital importancia en la era digital actual, ya que estas redes juegan un papel fundamental en la comunicación y transmisión de datos de las en diferentes ámbitos. A medida que la tecnología inalámbrica continúa avanzando, ocurre lo mismo con las amenazas y vulnerabilidades comprometiendo la seguridad y privacidad de la información. La protección de los datos confidenciales, la integridad de los recursos y la prevención de accesos no autorizados son elementos cruciales para garantizar un entorno académico seguro y confiable.

En este contexto, la falta de estudios previos sobre este tema de estudio surge la necesidad de realizar un análisis exhaustivo y una evaluación detallada de la red inalámbrica, con el objetivo de determinar su nivel de seguridad identificando y evaluando los controles de seguridad implementados. Se centrará en evaluar aspectos relevantes como los protocolos de seguridad, configuración de los dispositivos y políticas de acceso que puedan influir en la seguridad mediante el uso de herramientas de software libre ampliamente reconocidas en el ámbito de la seguridad informática.

1.3 Justificación

La red inalámbrica de Facultad de Ingeniería, al ser una red empresarial debe garantizar la confidencialidad, integridad y disponibilidad de la información que se transmite disponiendo de seguridad ya que es un punto vulnerable en este tipo de redes. Las amenazas de accesos no autorizados, ataques cibernéticos y vulnerabilidades ocurren en cualquier momento, esto desata la necesidad critica de realizar un análisis detallado y evaluación continua de la infraestructura de seguridad para la protección de estos datos sensibles de los usuarios que transitan a través de esta red. Las herramientas de software libre ofrecen ventajas de flexibilidad y es adaptable para soluciones emergentes y confiables. La investigación propuesta contribuirá con resultados sobre las vulnerabilidades en la seguridad para la cual se presentará estrategias y recomendaciones para mitigar y corregir las fallan que se presenten.

1.4 Objetivos

1.4.1 General

- Analizar y evaluar la red inalámbrica para determinar el nivel de seguridad de la Facultad de Ingeniería de la UNACH mediante herramientas de software libre.

1.4.2 Específicos

- Estudiar el diseño del diagrama de red inalámbrica mediante el análisis de la información proporcionada por DTIC y bibliografías existentes, para determinar las amenazas, riesgos y vulnerabilidades.
- Establecer los controles de seguridad que serán evaluados para determinar el nivel de seguridad.
- Implementar un escenario de pruebas con herramientas de software libre para simular la red inalámbrica proporcionado por DTIC.
- Evaluar la red inalámbrica mediante el escenario de pruebas y controles establecidos para determinar el nivel de seguridad.

2. CAPÍTULO II

2.1 Fundamento teórico

2.1.1 Estado del arte

En algunos estudios de investigación de seguridad inalámbrica, se llevan a cabo análisis y evaluaciones exhaustivas para identificar vulnerabilidades. Estos estudios emplean diversas metodologías con el objetivo de evaluar la seguridad en entornos específicos. Un elemento común en estos trabajos es la aplicación de herramientas de software libre, las cuales desempeñan un papel importante en la detección y mitigación de los riesgos que se presentan. Esta combinación resalta la importancia de evaluar la seguridad en redes inalámbricas y la importancia de utilizar recursos disponibles y de fácil acceso para fortalecer la protección de los sistemas.

El estudio propuesto por[5], con el tema Análisis de las vulnerabilidades del protocolo de seguridad WPA y WPA2 en redes inalámbricas, se centra en evaluar la vulnerabilidades de los protocolos de seguridad antes mencionados utilizando una metodología de hacking ético en la cual se realiza cuatro fases: reconocimiento, escaneo, obtención de acceso y elaboración de informe, identificando 5 vulnerabilidades cada uno con propuestas de solución buscando garantizar la seguridad de la red y dispositivos[5].

El presente estudio realizado por [6], utiliza Acrylic Wi-Fi y OpenVAS junto con la Metodología abierta de evaluación de seguridad inalámbrica con sus siglas en inglés (OWISAM) para realizar un exhaustivo análisis de vulnerabilidades en la red inalámbrica de la Empresa Punto de Vista. Este enfoque permitió diagnosticar amenazas cibernéticas, identificar carencias en la seguridad de la red, ausencia de políticas de seguridad y falta de actualizaciones críticas para la protección de la información[6]. Como resultado, se propuso un plan de remediación, enfocado en establecer medidas de seguridad, monitoreo constante, y autenticación estricta para limitar el acceso a usuarios autorizados.

Finalmente, en otra investigación, se aplicó el Manual de metodología de pruebas de seguridad de código abierto con sus siglas en inglés (OSSTMM) en el Ministerio de Inclusión Económica y Social, esta metodología proporciona una estructura planificada para la ejecución y verificación de la seguridad informática[7]. Sus secciones, como el análisis de seguridad, las pruebas de seguridad inalámbrica y de telecomunicaciones, incluyen módulos específicos para sondeo, identificación de servicios y sistemas, y búsqueda de vulnerabilidades en la red. La aplicación de esta metodología en conjunto con herramientas de software libre como Nmap, OpenVAS y otras herramientas disponibles en Kali Linux, ha permitido realizar un diagnóstico exhaustivo de la red, revelando fallos en el ámbito de la seguridad[7].

2.1.2 Amenazas y Vulnerabilidades de redes WLAN

Al hacer uso de redes inalámbricas en cualquier lugar está expuesto a varias amenazas las cuales afecta el correcto funcionamiento de la red. Aquí algunas se presenta algunas amenazas.

- Intercepción de Datos: Utiliza herramienta de software y hardware que permite hacer un barrido de tráfico de un usuario en tiempo real y captura todo el flujo de datos de un equipo[8].
- Ataques de fuerza bruta: Hace uso de todas las contraseñas posibles y averigua las claves criptográficas del acceso a la red wifi[9].
- Ataques de Denegación de servicio: Inhabilita o satura el uso de un sistema o una maquina con el fin de bloquear el servicio normal[10].
- Ataques de Suplantación de Identidad: Intercepta la comunicación entre dos dispositivos conectados a una red, sin autorización, con el objetivo de escuchar información sensible o suplantar identidad de alguna de las partes[11].

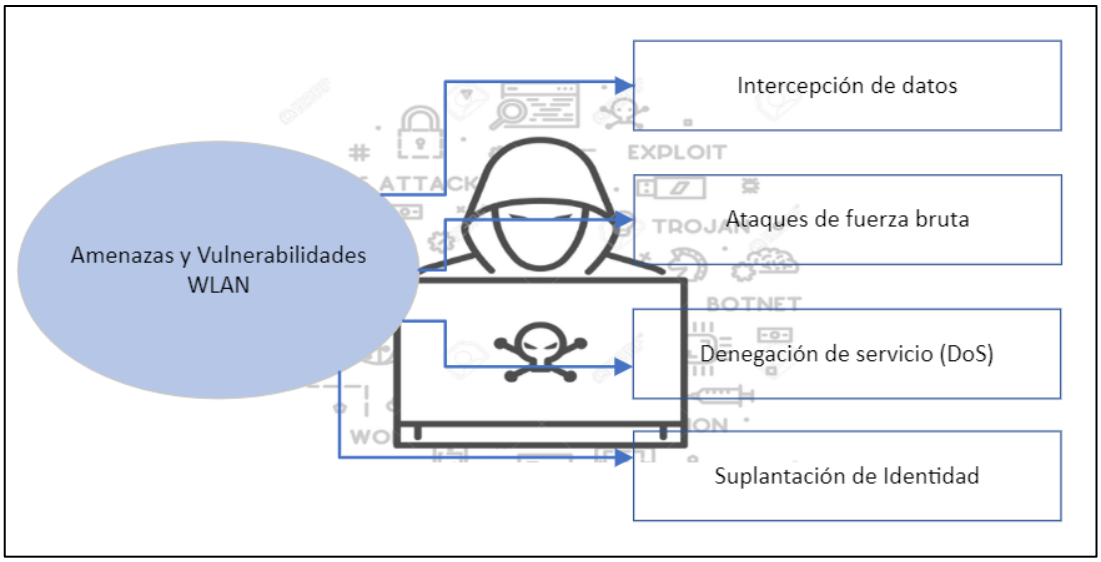


Fig. 1 Amenazas y Vulnerabilidades.
Fuente: Autor.

2.1.3 Configuración de seguridad de redes WLAN

Dentro de la estructura organizativa de una empresa, es fundamental contar con una configuración de seguridad claramente establecida y documentada con el objetivo de asegurar la protección necesaria para preservar la privacidad de la información. Para lograr un nivel de seguridad alto, es esencial implementar medidas específicas como:

- Diseño y gestión de la arquitectura de seguridad.
- Autenticación.
- Distinción de clientes internos y externos.
- Configuración estandarizada.
- Registro de actividad de usuarios.

- Monitorización.
- Auditorias de seguridad[10].

2.1.4 Herramientas de Software libre para seguridad en redes

- OpenVAS: Es un escáner de vulnerabilidades a gran escala, tiene capacidades que incluyen pruebas autenticadas y no autenticadas que realiza con un potente leguaje de programación para implementar pruebas de vulnerabilidades[12].
- Kismet: Es una herramienta de captura de paquetes, WIDS, wardriver y rastreador de código abierto para WI-FI con una interfaz de usuario moderna y completa basado en web[13].
- Nmap: Es una herramienta de línea de comandos de Linux de código abierto que se utiliza para escanear direcciones IP y detectar los equipos que se encuentran en la red, servicios que ofrecen y sistemas operativos que ejecutan[14].
- Aircrack: es un programa que sirve para crackear claves capturando paquetes encriptados, airodump-ng utiliza varios tipos de ataque para descubrir la clave WEP combinando ataques de fuerza bruta y diccionario[15].

2.1.5 Metodologías de evaluación de seguridad

- OWISAM (Metodología abierta de evaluación de la seguridad inalámbrica): Esta metodología de seguridad define un total de 64 controles técnicos, agrupados en 10 categorías, que especifican un conjunto de pruebas necesarias para garantizar una auditoría de seguridad exitosa en una infraestructura inalámbrica[16].
- OSSTMM (Manual de metodología de pruebas de seguridad de código abierto): es una metodología completa para probar, analizar y medir la seguridad operativa con el objetivo de construir las mejores defensas de seguridad posibles de su organización[17]. Proporciona una guía exhaustiva para llevar a cabo evaluaciones de seguridad en distintas áreas, como seguridad física, de red, de aplicaciones y sistemas operativos. Este manual, a lo largo del tiempo ha logrado adaptarse a los cambios en las amenazas y tecnologías de seguridad, ofreciendo una herramienta de gran utilidad para profesionales que buscan evaluar mediante un rango o valor los controles de seguridad y detectar posibles vulnerabilidades[17].

2.1.6 Triada CID

La triada CID se refiere a confidencialidad, integridad, disponibilidad, estos principios constituyen la base para el desarrollo de sistemas de seguridad informática con el fin de encontrar vulnerabilidades y métodos para crear soluciones factibles que ayudan a las organizaciones a gestionar y mitigar riesgos[18].

2.1.7 Confidencialidad

Se asegura que los datos y recursos de la red se mantengan de forma privada, es decir, el acceso a la información debe ser restringido mediante el cifrado y las políticas de control de acceso a los usuarios maliciosos o no autorizados[19].

2.1.8 Integridad

Previene la modificación de los datos garantizando la veracidad y exactitud de la información mediante cifrado y certificados digitales que verifiquen la autenticidad de los usuarios[18], [19].

2.1.9 Disponibilidad

La información debe estar disponible y accesible cuando el usuario requiera evitando la interrupción del servicio[18]. Las organizaciones utilizan copias de seguridad y duplicación de servicios cuando el sistema primario haya dejado de cumplir su función[18], [19].

2.1.10 Servidor Radius

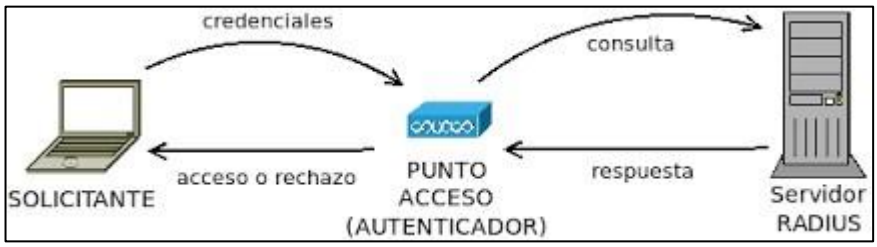


Fig. 2. Servidor Radius
Fuente: [20]

RADIUS (Servicio de Usuario de Marcación y Autenticación Remota) es un protocolo estándar de Internet que facilita la administración centralizada de autenticación, contabilidad e IP para usuarios de acceso remoto en una red distribuida[21]. Los servidores RADIUS responden a solicitudes de conexión autenticando a los usuarios y proporcionando al Dispositivo de Acceso de Red (NAS) la información de configuración necesaria para ofrecer servicios autorizados al usuario autenticado[21]. Al recibir una solicitud de autenticación, el servidor RADIUS valida la información y descifra los datos para acceder a los detalles del usuario, como nombre y contraseña, permitiendo así la prestación de servicios autorizados a través de llamadas telefónicas[21].

2.1.11 Firewall

Los firewalls se consideran como una barrera de protección o herramientas de seguridad que administran el flujo de la actividad de web[22]. En cambio, los firewalls de seguridad de red realizan la administración del tráfico y mitiga la propagación de la amenaza web[22]. También existe dispositivos firewalls que tiene como función el monitoreo del tráfico de la

red de entrada y salida, mediante un conjunto de regla de seguridad establecidos decide si bloquea o permite el tráfico de la red[23]. Un firewall puede ser hardware o software, o ambos.

En una organización uno de los Firewall más conocidos es el Fortigate, cuenta con bloqueo a nivel de aplicación para acceder a ciertos recursos y servicios. También puede realizar filtrado de contenido para bloquear el acceso a sitios web no deseados o peligrosos.

2.1.12 Base de datos

Una base de datos es una herramienta para almacenar todo tipo de información, se debe organiza mediante tablas facilitando la creación, actualización, eliminación de los datos. Cuando haya gran cantidad de información es recomendable transferir los datos a una base de datos creada con un sistema de gestión de base de datos (DBMS)[24]. Un DBMS es un software que sirve como interfaz entre la base de datos y los usuarios finales, los más populares son MySQL, Oracle Database, y Microsoft Acces[25].

2.1.13 Puntos de acceso

Es un dispositivo de red que une redes cableadas e inalámbricas. Muchos de estos dispositivos usan el estándar Wi-Fi actualmente permite operar en bandas de 2,4 Ghz, 5 Ghz y 6Ghz[26]. Los puntos de acceso comerciales cubren un área física más grande y permiten que cientos de usuarios inalámbricos accedan a la red simultáneamente[26].

2.1.14 Dispositivos inalámbricos

Los dispositivos inalámbricos utilizan señales de radiofrecuencia, infrarrojas o bluetooth para enviar y recibir información. Estos dispositivos permiten una mayor flexibilidad y facilidad de interacción. Los dispositivos que comúnmente se conectan a la red inalámbrica para acceder al internet son teléfonos inteligentes, tablets y computadoras portátiles.

3. CAPÍTULO III

3.1 Metodología

3.1.1 Tipo de Investigación

Dado que la red inalámbrica de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo fue objeto de análisis, se implicó realizar una investigación mixta, es decir una combinación de enfoques cuantitativos y cualitativos para comprender los componentes de la red, el nivel de seguridad, la topología que actualmente está implementada y las posibles vulnerabilidades.

Mediante la investigación cuantitativa se utilizó herramientas de medición y análisis estadístico para cuantificar aspectos específicos para determinar el nivel de seguridad inalámbrica. Por otra parte, la investigación cualitativa explora aspectos más subjetivos y contextuales que incluye la revisión de fuentes bibliográficas que tengan relación con la seguridad y entrevistas con administradores de red para obtener datos relevantes de la infraestructura que va ser estudiada.

3.1.2 Diseño de Investigación

Con el fin de tratar el problema y obtener los resultados comprensibles para analizar y evaluar la red inalámbrica se basa en un enfoque cuantitativo. Con el levantamiento de la información se detallará la topología de la red inalámbrica, dispositivos y configuraciones que están implementadas. Posteriormente, se emplearán herramientas de software libre como S.O Linux, Kali Linux, y aircrak, para llevar realizar escaneo, simulación de ataques y evaluación de la seguridad de red inalámbrica.

Los datos serán generados por el autor de la presente investigación y serán procesados utilizando métodos estadísticos y probabilísticos para obtener métricas cuantitativas que permitan evaluar el nivel de seguridad de la red y proponer posibles mejoras.

3.1.3 Proceso de Metodología

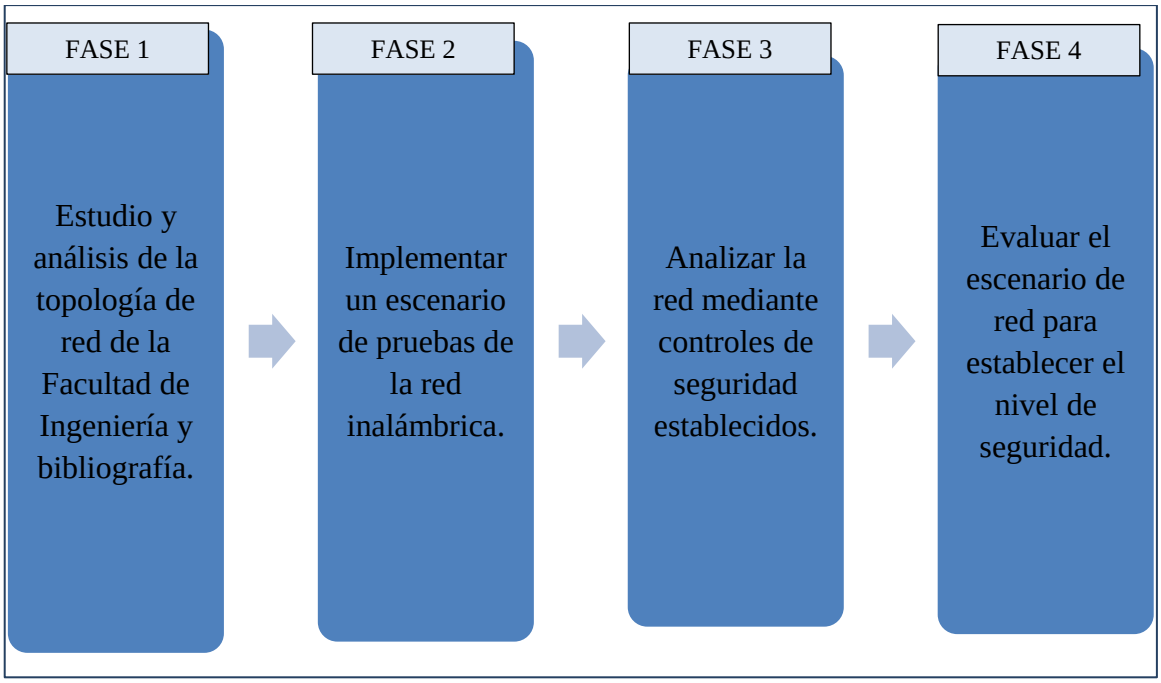


Fig. 3. Diagrama del Proceso de la Metodología.
Fuente: Autor.

3.1.3.1 Fase 1: Estudio y análisis de la topología de red, y bibliografía

Con el fin de profundizar aspectos relevantes para el análisis y evaluación de este tipo de redes, se obtiene información a través de entrevistas con administradores del Departamento de Tecnología de Información y Comunicación (DTIC) sobre la topología, dispositivos, configuraciones existentes, y políticas de seguridad. Con relación a la bibliográfica se investigará de libros, artículos científicos y trabajos de investigación relacionados con la seguridad de red inalámbrica.

3.1.3.2 Fase 2: Implementar un escenario de pruebas de la red inalámbrica

Se crea escenarios de pruebas en condiciones semejantes de la infraestructura inalámbrica para realizar un escaneo y diagnóstico de red utilizando herramientas de software libre y simulación de ataques para evaluar la resistencia de la red.

3.1.3.3 Fase 3: Analizar la red mediante controles de seguridad establecidos

Los controles que serán objetivo de análisis tienen relación con la triada CID (Confidencialidad, Integridad y Disponibilidad), aplicar estos principios proporcionan un entorno clave de la seguridad de redes con fin de proteger información y recursos de posibles amenazas.

3.1.3.4 Fase 4: Evaluar el escenario de red para establecer el nivel de seguridad

Mediante los resultados obtenidos de la fase 3 se procederá utilizar Manual de Metodología de Prueba de Seguridad de Código Abierto (OSSTMM), correspondiente a la sección de evaluación de red inalámbrica, donde indica los procedimientos a seguir para evaluar la efectividad de la infraestructura inalámbrica. Además, se utilizará el Sistema de Gestión de Seguridad de la Información (SGSI), la sección análisis de riesgo donde se calcula datos obtenidos mostrando resultados numéricos.

3.2 Población de estudio y tamaño de muestra

3.2.1 Población de estudio

La población que se considera para el análisis y evaluación de la red inalámbrica se toma en función a las variables de estudio. En este contexto, se realiza un estudio cuantitativo que implica la cantidad de ataques de Fuerza Bruta y Diccionario, Denegación de servicio, y Fake/Rogue AP que ocurren hacia los dispositivos de la red inalámbrica por lo cual hace que la población sea desconocida.

3.2.2 Tamaño de muestra

Por lo que la población es desconocida, se establece que el tamaño de muestra sea de 300 ataques sobre el escenario de pruebas.

3.3 Operacionalización de la variable

Tabla 1. Operacionalización de la variable

Variable	Descripción	Indicadores	Técnicas e Instrumentación
Independiente: Análisis de seguridad de la red inalámbrica	Análisis y evaluación de los controles de seguridad de la red inalámbrica mediante el uso de herramientas de software libre.	Controles de seguridad de red inalámbrica.	Observación- Escenario de Pruebas. Herramientas de Software Libre
Dependiente: Nivel de seguridad de la red inalámbrica.	Determinar el nivel de seguridad de red inalámbrica en base a los indicadores descritos .	· Disponibilidad de los datos · Integridad de los datos · Confidencialidad de los datos	Observación - Matriz resultante de análisis de pruebas de penetración de la red inalámbrica.

Fuente: Autor.

3.4 Métodos de análisis, y procesamiento de datos

Mediante el estudio e identificación de los dispositivos de la topología de red utiliza herramientas de Kali Linux para descubrir, escanear de vulnerabilidades, captura y análisis de tráfico, simulación de ataques a los puntos de acceso y dispositivos conectados identificando posibles vulnerabilidades, evaluando la seguridad de la configuración y proporcionando información valiosa para fortalecer la infraestructura.

3.5 Estado Actual de Red.

Mediante una entrevista con el analista de DTIC se obtiene información para el análisis de la red inalámbrica de Facultad de Ingeniería que se detalla a continuación.

Tabla 2. Información proporcionada por DTIC

Información proporcionada por DTIC	
Switch de Core	Catalyst 6500
Switch de Distribución	Catalyst 3750x
Puntos de acceso	Juniper
Nombre de red	Estudiantes Unach en Movimiento

Almacenamiento de Información de usuarios	Base de datos SICOA
Servidor de autenticación	Servidor Radius
Autenticación y Autorización	802.1x para intercambio de mensajes entre el Servidor Radius y el dispositivo de red mediante el protocolo PEAP.
Encriptación y Cifrado	AES, WPA2 Enterprise
Clase de Dirección IP	Clase B
Asignación de IP	DHCP en el switch de core
Gestión de Claves	Usuario: usuario SICOA Contraseña: número de CI.
Firewalls	Filtros de Contenido Adulto
Monitoreo y Registro	Realiza a diario para detectar y prevenir posibles amenazas de dispositivos no autorizados.
Segmentación de Red	VLANs para cada tipo de privilegios. • Estudiantes VLAN 56 con máscara de red /21 • Unach en movimiento VLAN 96 con mascara de red /20
Control de Acceso	Un dispositivo por usuario.

Fuente: Autor.

3.5.1 Levantamiento de Información

Con la recopilación de información se procede a realizar la topología de red inalámbrica. Además, con la técnica de observación directa se recopila información de la cantidad de puntos de acceso por cada piso y la ubicación de los puntos de acceso de los dos bloques de la Facultad de Ingeniería.

En la Fig. 4 se observa la topología de red, consta de la capa de Core, capa de distribución y capa de acceso. La investigación se centra únicamente en el estudio, análisis y evaluación de la capa de acceso.

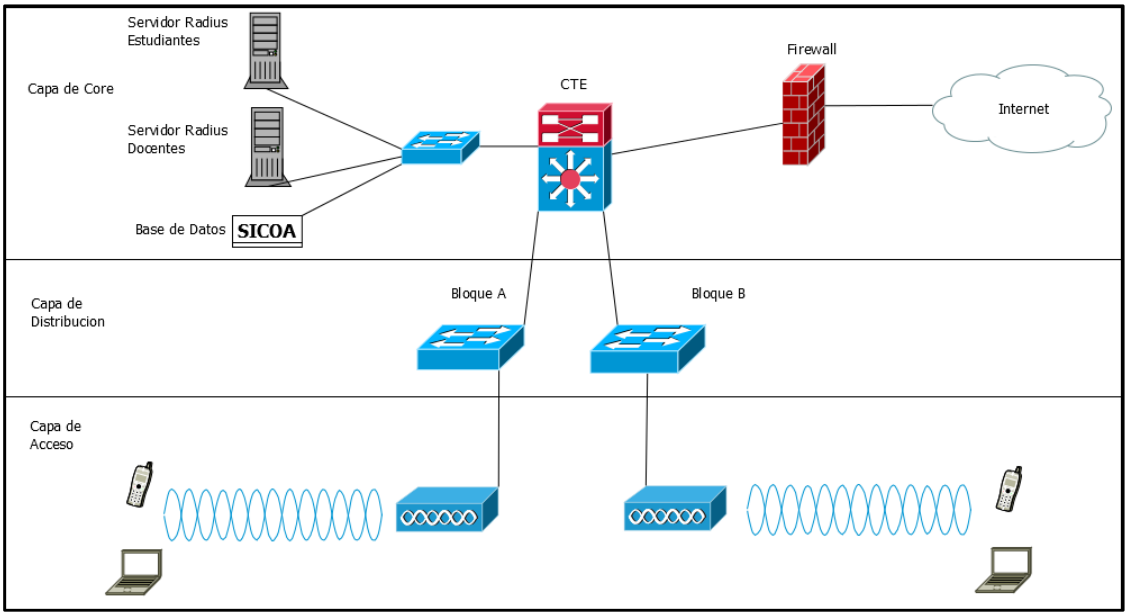


Fig. 4 Topología de Red - Facultad Ingeniería UNACH.
Fuente: Autor.

En la Tabla 3 se detalla los dispositivos que componen la infraestructura inalámbrica, marca, modelo y la cantidad de cada uno de ellos.

Tabla 3. Descripción de dispositivos de topología de red

Equipo	Marca	Modelo	Cantidad
Switch Core	Cisco	Catalyst 6500	1
Switch de Distribución	Cisco	Catalyst 3750X	2
Puntos de acceso	JUNIPER	AP JUNIPER A32 AP JUNIPER A63	22

Fuente: Autor.

3.5.1.1 Bloque A

En la Tabla 4. Se detalla la cantidad de puntos de Acceso por cada Piso del Bloque A.

Tabla 4. Cantidad de Puntos de Acceso -Bloque A

No. Planta	Puntos de Acceso
Planta 1	4
Planta 2	5
Planta 3	4
Total	13

Fuente: Autor.

En la Fig. 5 se muestra el plano y la ubicación de los puntos de acceso de la primera planta de Bloque A.

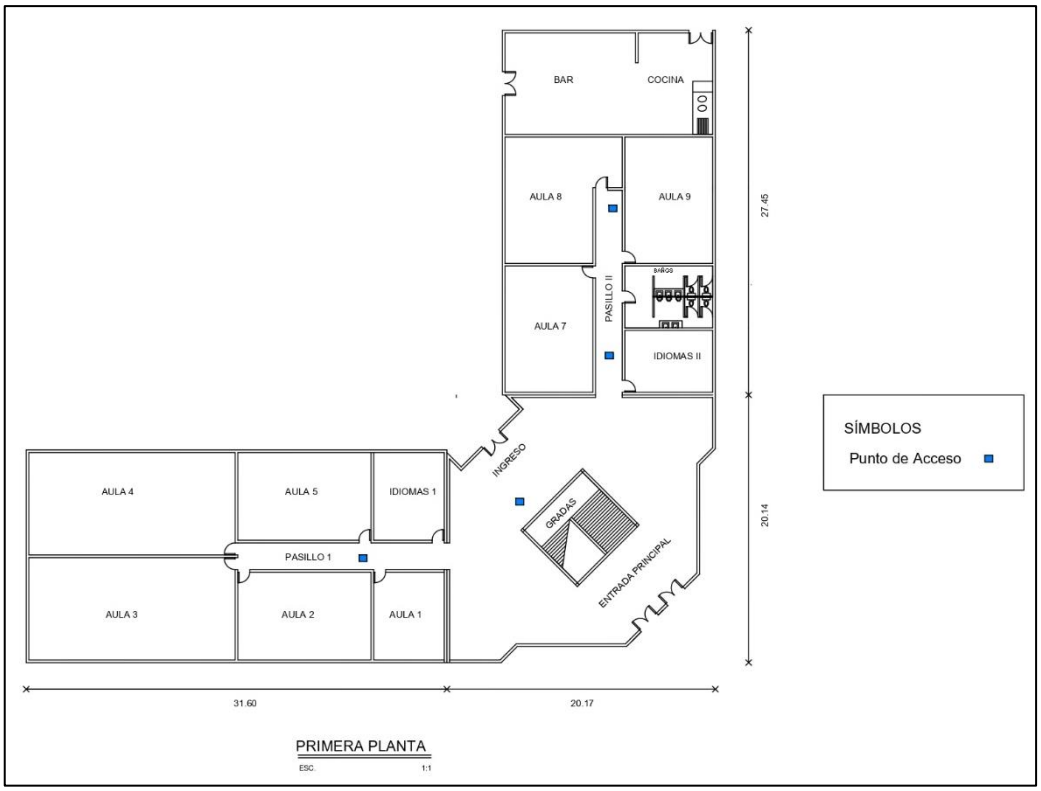


Fig. 5 Plano Primera Planta Bloque A.
Fuente: Autor.

Tabla 5. Distribución de Puntos de Acceso - Bloque A

Piso 1	Aulas
AP1	Aula1, Aula2, Aula3, Aula4, Aula5, Idiomas1
AP2	Ingreso, Entrada Principal
AP3	Aula7, Idiomas II, Baños
AP4	Aula8, Aula9, Bar, Cocina

Fuente: Autor.

En la Fig. 6 se muestra el plano y la ubicación de los puntos de acceso de la segunda planta de Bloque A.

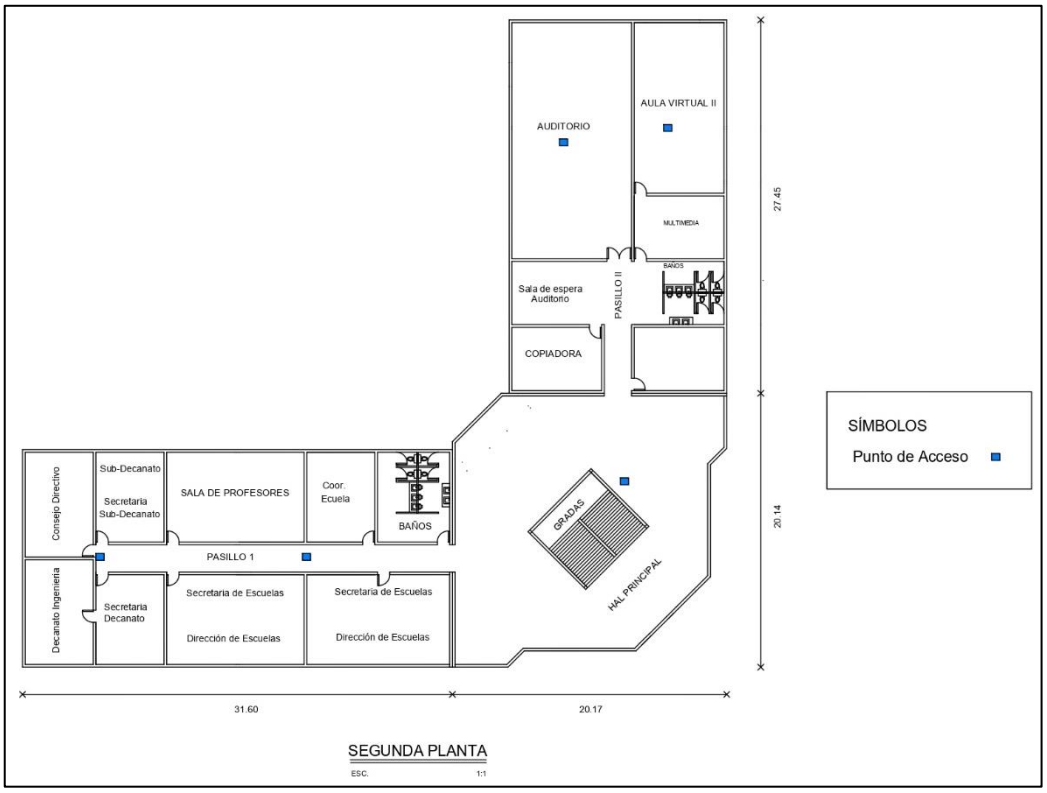


Fig. 6 Plano Segunda Planta Bloque A.
Fuente: Autor.

Tabla 6. Distribución de Puntos de Acceso - Bloque A

Piso 2	Aulas
AP1	Decanato, Sub-decanato, Dirección de Escuelas, Secretaria de Escuelas, Sala de Profesores, Consejo Directivo
AP2	Ingreso, Entrada Principal
AP3	Auditorio, Aula Virtual II, Copiadora

Fuente: Autor.

En la Fig. 7 se muestra el plano y la ubicación de los puntos de acceso de la tercera planta de Bloque A.

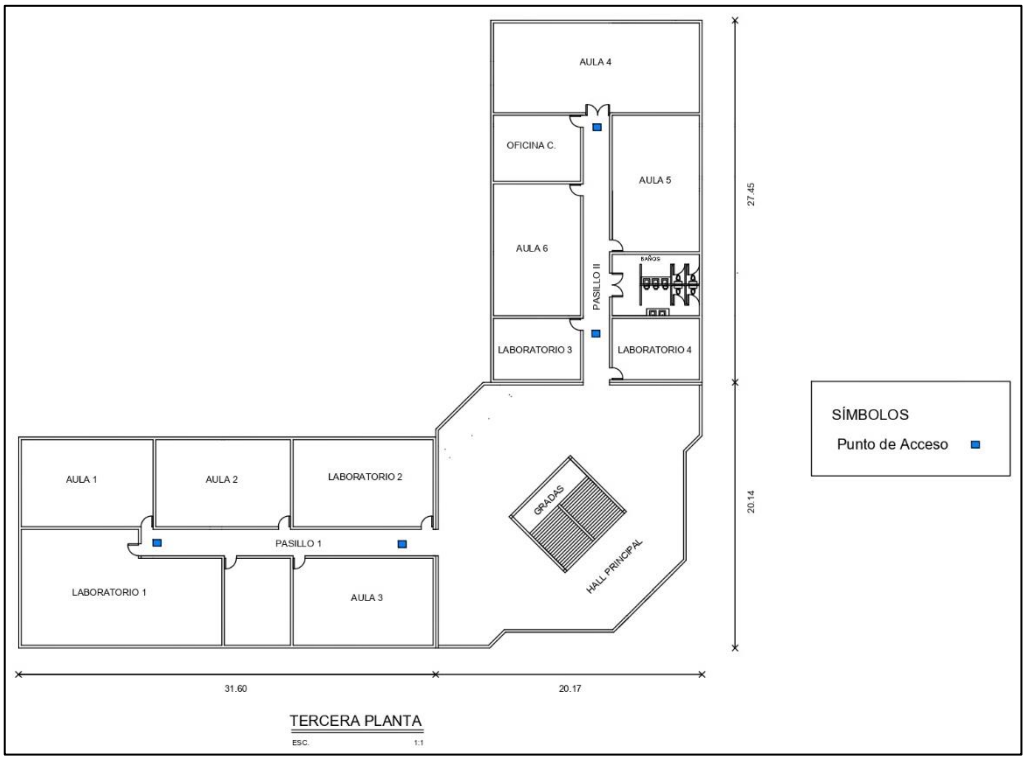


Fig. 7 Plano Tercera Planta Bloque A
Fuente: Autor.

Tabla 7, Distribución de Puntos de Acceso - Bloque A

Piso 3	Aulas
AP1	Aula1, Aula2, Laboratorio1, Oficina
AP2	Laboratorio2, Aula3, Hall Principal
AP3	Laboratorio3, Laboratorio4, Aula 8, Baño
AP4	Oficina C, Aula4, Aula5

Fuente: Autor.

3.5.1.2 Bloque B

En la Tabla 8. Se detalla la cantidad de puntos de Acceso por cada Planta del Bloque B.

Tabla 8. Cantidad de Puntos de Acceso - Bloque B

No. Planta	Puntos de Acceso
Planta 1	4
Planta 2	5
Total	9

Fuente: Autor.

En la Fig. 8 se muestra el plano y la ubicación de los puntos de acceso de la primera planta de Bloque B.

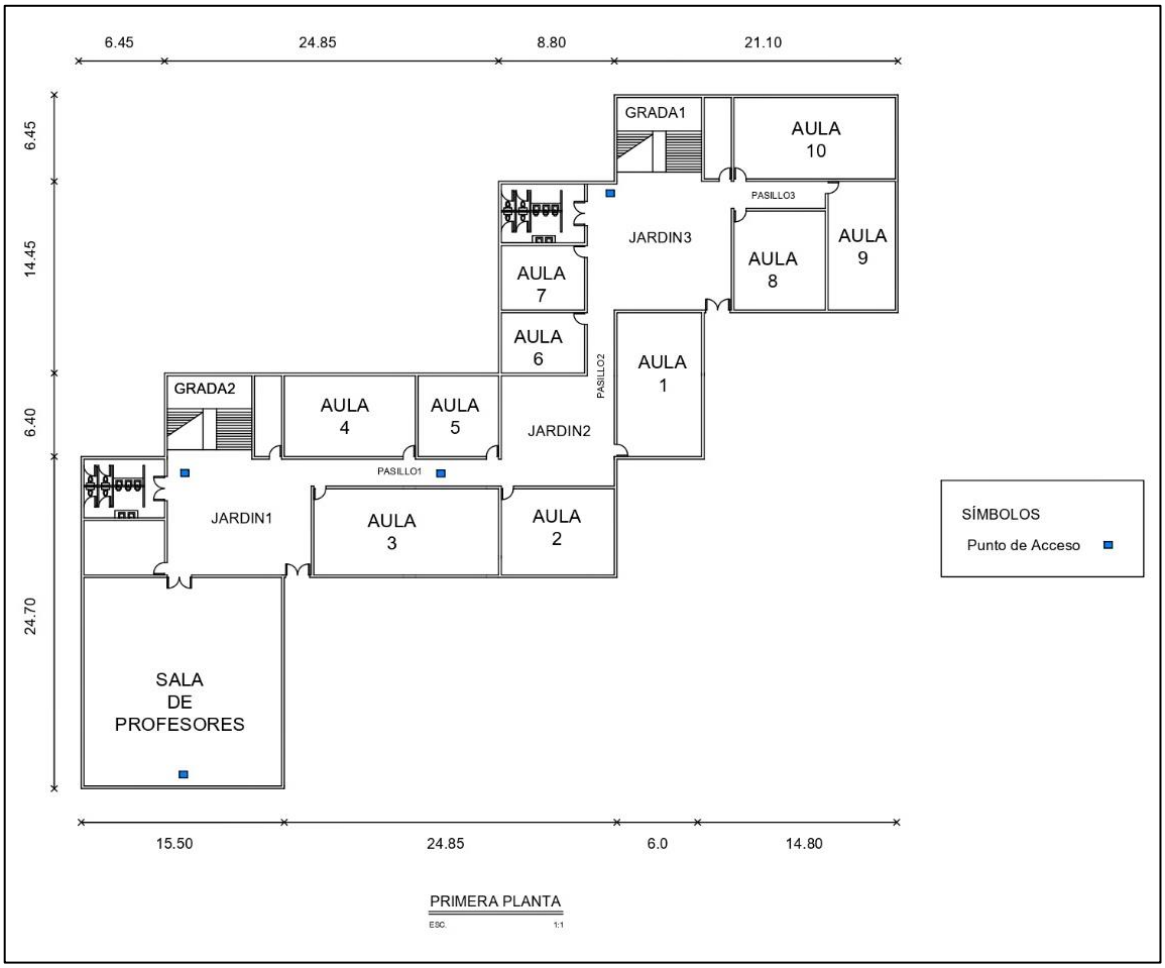


Fig. 8 Plano Primera Planta Bloque B.
Fuente: Autor.

Tabla 9. Distribución de Puntos de Acceso - Bloque B

Piso 1	Aulas
AP1	Sala de Profesores, Oficina, Jardín1, Gradas 2, Bodega
AP2	Aula5, Aula4, Aula3, Aula2, Jardín2
AP3	Aula1, Aula6, Aula7, Baño, Jardín3
AP4	Aula8, Aula9, Aula10, Bodega, Gradas1

Fuente: Autor.

En la Fig. 9 se muestra el plano y la ubicación de los puntos de acceso de la primera planta de Bloque B.

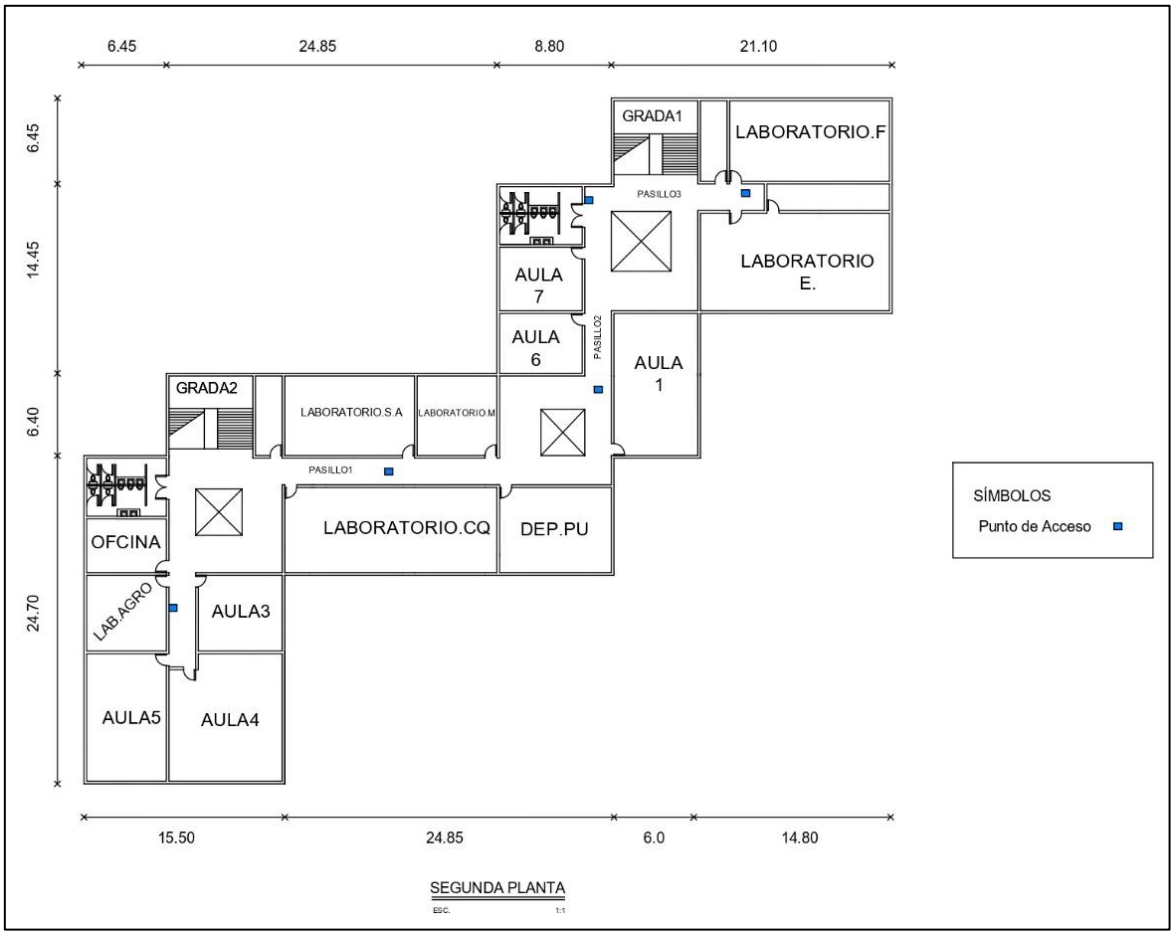


Fig. 9 Plano Segunda Planta Bloque B.
Fuente: Autor.

Tabla 10. Distribución de Puntos de Acceso - Bloque B

Piso 1	Aulas
AP1	Aula3, Aula4, Aula5, Lab. Agro, Oficina, Baños, Gradas2
AP2	Laboratorio. S.A, Laboratorio M., Laboratorio CQ, Bodega
AP3	Dep. PU., Aula1, Aula6, Aula7,
AP4	Laboratorio F., Laboratorio E., Oficina, Baños, Grada1

Fuente: Autor.

3.6 Controles de seguridad

3.6.1 Triada CID

En el proceso de evaluación del nivel de seguridad se realizará la medición de estos principios fundamentales con el objetivo de determinar la robustez y fiabilidad de la red inalámbrica. Se toma como base los tres principios fundamentales de la triada CID

- Confidencialidad
- Integridad
- Disponibilidad

4. CAPÍTULO IV

4.1 Resultados y discusión

4.1.1 Escenario de Pruebas

En el escenario de pruebas de la Fig.10 se implementa una combinación de máquinas virtuales y dispositivos físicos. El router, firewall, servidores de Radius y base de datos son parte del ambiente virtualizado, hacemos uso del software de VirtualBox que ofrecen un entorno controlado para llevar a cabo pruebas de seguridad, simulando diferentes elementos y configuraciones en la infraestructura de red. Por otra parte, los dispositivos físicos como puntos de acceso y dispositivos de usuarios reales forman parte del ambiente real.

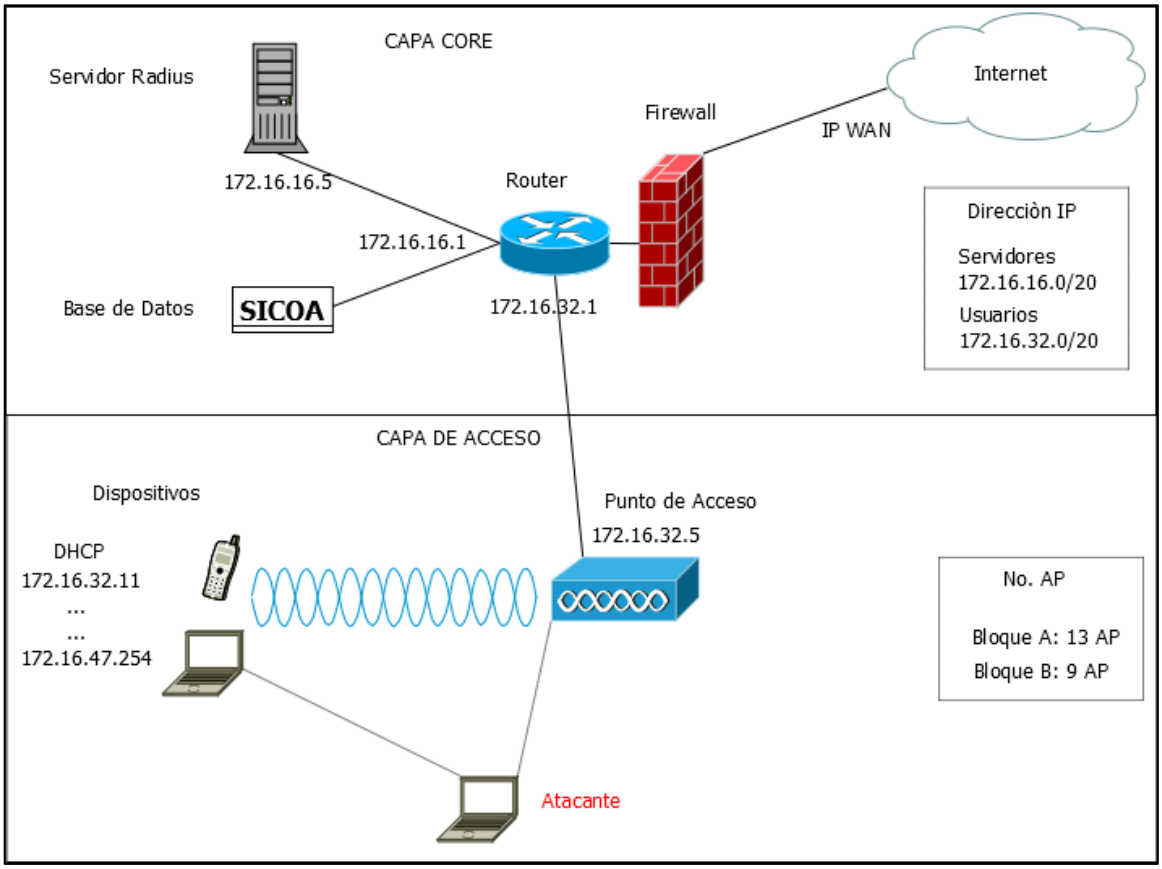


Fig. 10 Topología de escenario de Pruebas
Fuente: Autor.

La combinación de estos ambientes virtuales y físicos facilita la evaluación de la efectividad de las medidas de seguridad implementadas en un entorno más real de la red inalámbrica.

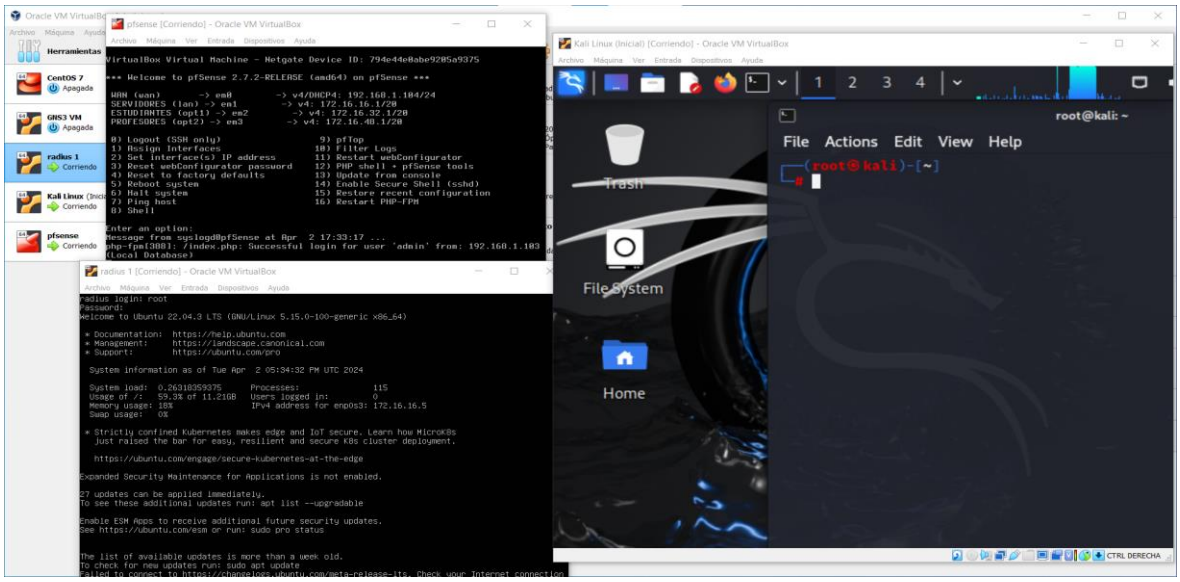


Fig. 11. Escenario Virtual.
Fuente: Autor.

Fig. 12. Escenario físico.
Fuente: Autor.

A continuación, se presenta la tabla de direccionamiento IP del escenario de pruebas.

Tabla 11. Tabla de Dirección IP del escenario de pruebas

Red		Direccionamiento IP
Firewall		172.16.16.5/20
Router		DHCP de Proveedor de Servicio (Internet)
Servidores	Radius	172.16.16.1/20
	Base de Datos SICOA	172.16.16.2/20
Punto de acceso	Estudiantes	172.16.32.1/20
	Docentes	172.16.48.1/20

Fuente: Autor.

4.2 Hardware y Software del escenario de pruebas

Para la implementación del escenario virtual y real se levantó con el siguiente hardware y software.

Tabla 12. Hardware del escenario de pruebas

Nombre	Especificaciones	Descripción
1 Laptop	Dell / Intel CORE i7 /16 GB RAM / 2.80 GHz	Computadora personal para la ejecución de ataques
Servidor Radius	VM / 2GB RAM	Servidor de autenticación Radius
Base de Datos	VM / 2GB RAM	Base de Datos SICOA
Firewall	VM / 1GB RAM	Firewall
Router	VM / 1GB RAM	Router Principal
Punto de Acceso	TP-LINK TL-WR840N	Punto de Acceso
Dispositivo inalámbrico	Redmi Note 11S Dell / Intel CORE i5 /8 GB RAM / 2.80 GHz	Dispositivos de usuario

Fuente: Autor.

Tabla 13, Software del escenario de pruebas

Software	Descripción
Kali Linux	Distribución de Linux utilizada para ejecutar ataques sobre el escenario de pruebas.
pfSense	Distribución de FreeBSD usado para simular Firewall y Router
S.O Linux	Sistema operativo utilizado para implementar el servicio de Radius y Base de Datos
S.O Windows	Sistema operativo que utiliza el equipo de usuario en Laptop
S.O Android	Sistema operativo que utiliza el equipo de dispositivo móvil de usuario

Fuente: Autor.

4.3 Procedimiento de evaluación de OSSTMM

Para evaluar la seguridad inalámbrica utilizando OSSTMM se realiza una serie de procedimientos que se detallan a continuación

- Análisis de la red inalámbrica para identificar puntos de acceso y dispositivos de usuarios: En el escenario de pruebas mediante el uso de herramientas de Kali Linux se realiza un escaneo para identificar los SSID de los puntos de acceso y los dispositivos que están conectados a cada uno de ellos.
- Identificar los dispositivos inalámbricos: Con la herramienta de aircrack-ng se realiza un escaneo para identificar los dispositivos que están conectados al punto de acceso objetivo.
- Pruebas de seguridad para evaluar la resistencia de la red: Se realiza varios tipos de ataques al escenario para probar la resistencia de la red.
- Evaluación de la seguridad implementada: Aplicamos los controles establecidos: confidencialidad, integridad y disponibilidad.
- Generación de reporte de los hallazgos de evaluación: Se realiza tablas de acuerdo a los criterios de evaluación que se toma del SGSI a fin de determinar el nivel de seguridad en la que está la red inalámbrica de la Facultad de Ingeniería UNACH.

4.4 Ataques realizados en el escenario de pruebas

De acuerdo al tema de investigación todas las pruebas de ataques se realizarán específicamente en la capa de acceso. Con el paquete de herramientas de Aircrack-ng se detecta y recopila información relevante sobre la red inalámbrica que va ser objetivo de ataque como: ESSID corresponde al nombre de red, ECN verifica el tipo de cifrado y AUTH es el protocolo de autenticación. En la Fig. 13 se puede observar la red que va ser atacada

tiene encriptación WPA2 y autenticación MGT, quiere decir que utiliza un servidor de autenticación centralizada, los dispositivos de los usuarios se conectan a un punto de acceso e inician sesión mediante usuario y contraseña para tener acceso a la red.

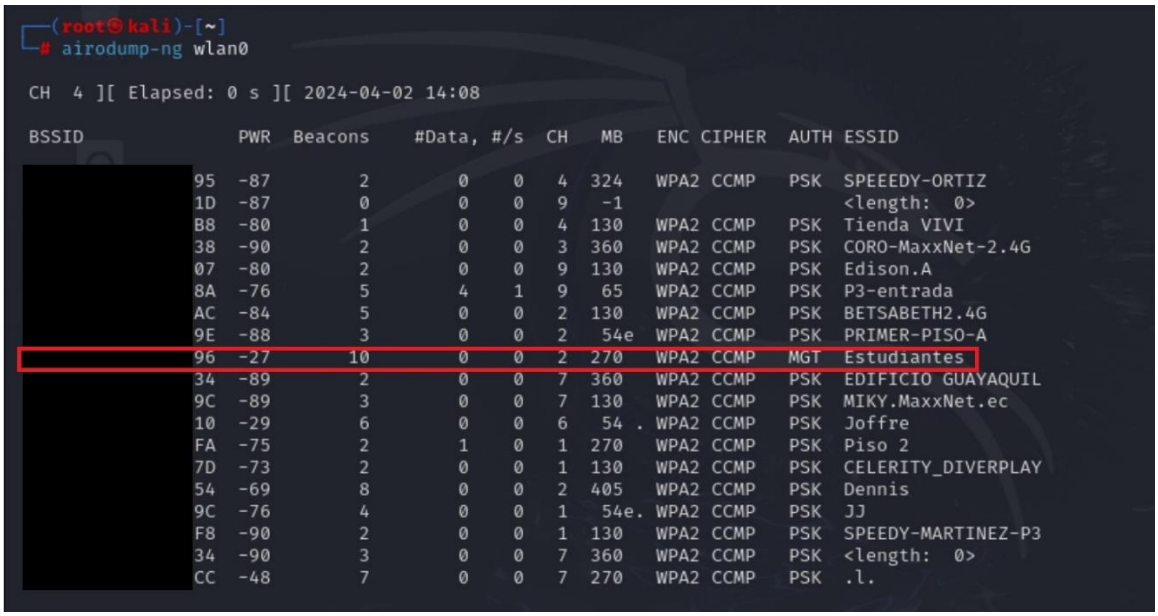


Fig. 13. Escaneo de redes inalámbricas.
Fuente: Autor.

Una vez hecho el proceso de obtener información se ejecuta ataques de Diccionario y Fuerza Bruta, Denegación de Servicio y Fake/Rogue AP.

4.4.1 Diccionario y Fuerza Bruta

Para realizar este proceso se utiliza la herramienta crunch que genera un diccionario de todas las combinaciones posibles de 0 a 9. Este diccionario generado se utiliza luego para intentar adivinar las contraseñas de los usuarios que se encuentran en la base de datos del servidor radius. El comando que se ejecuta en la Fig. 14 se genera palabras de 10 caracteres de longitud, donde @ representan posiciones que pueden ser ocupadas por cualquier número del 0 al 9 y la opción -o especifica el nombre del archivo donde se guarda las claves generadas.

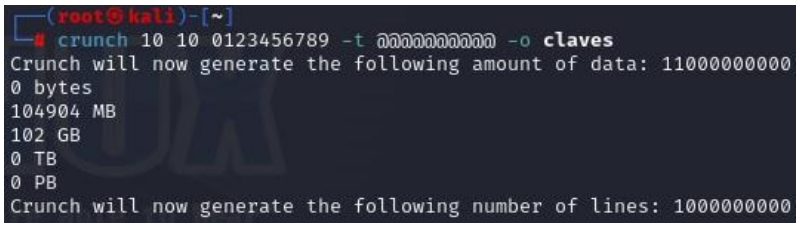


Fig. 14. Creación de Diccionario.
Fuente: Autor.

Se captura un handshake de autenticación entre un dispositivo cliente legítimo y el punto de acceso objetivo. Esto generalmente se hace mediante la desautenticación de un dispositivo ya conectado y la captura del handshake durante el proceso de reconexión.

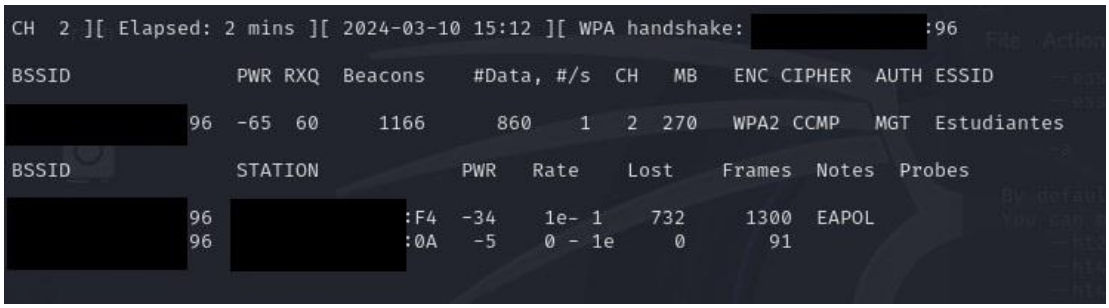


Fig. 15 Captura de handshake.
Fuente: Autor.

Una vez capturado el handshake se ejecuta el ataque para probar cada palabra que se encuentra en el diccionario generado intentando descifrar la clave.

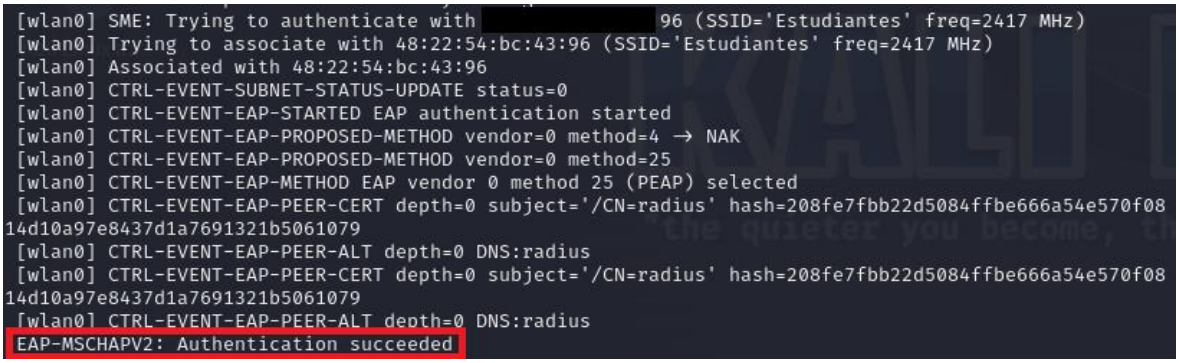


Fig. 16 Ataque Diccionario y Fuerza Bruta.
Fuente: Autor.

Mediante una combinación de diccionario y fuerza bruta, se descifra la contraseña probando la lista de claves generadas con respecto a las claves de usuarios registrados en la base de datos SICOA, descifrando con éxitos varias contraseñas. Mediante este ataque se prueba la confidencialidad e integridad, una vez obtenida el acceso a una cuenta de usuario el atacante podría acceder a toda la información del mismo es decir ocurre el acceso no autorizado, y manipulación de los datos.

4.4.2 Denegación de servicio.

Cuando se quiere realizar un ataque DoS a una red inalámbrica dejando sin servicio, se puede atacar de 2 formas:

- Ataque al punto de acceso.
- Ataque a un usuario especifico.

Se activa el modo monitor con la herramienta airmong-ng en la interfaz inalámbrica especificada que permite escuchar todo el tráfico del canal que se encuentra la red y captura todos los paquetes de datos que están en el aire, sin necesidad de estar conectado a un punto de acceso específico.

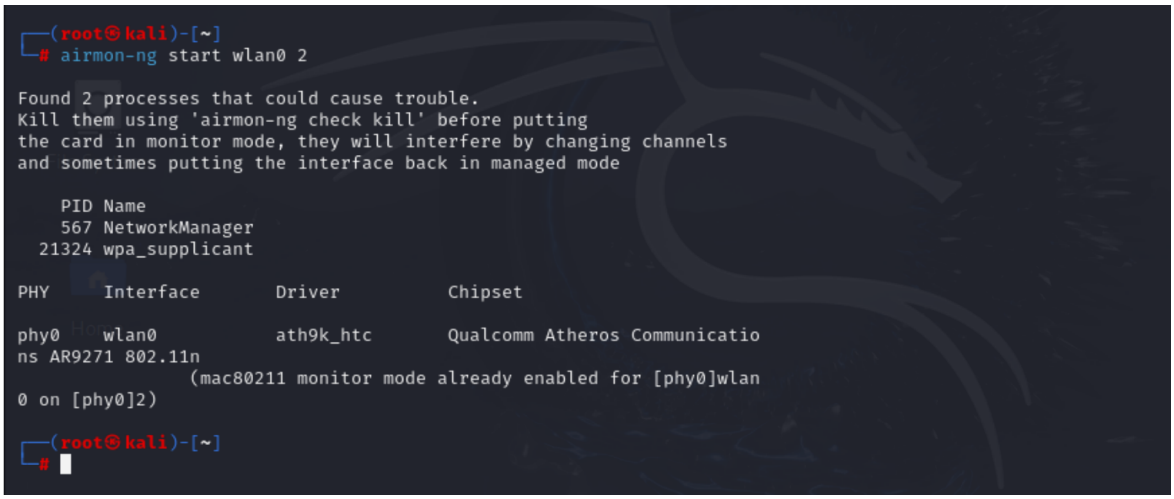


Fig. 17 Captura de paquetes
Fuente: Autor.

Con la herramienta aireplay-ng enviamos paquetes de des-autenticación a todos los usuarios que estén conectados al punto de acceso objetivo en un bucle infinito.

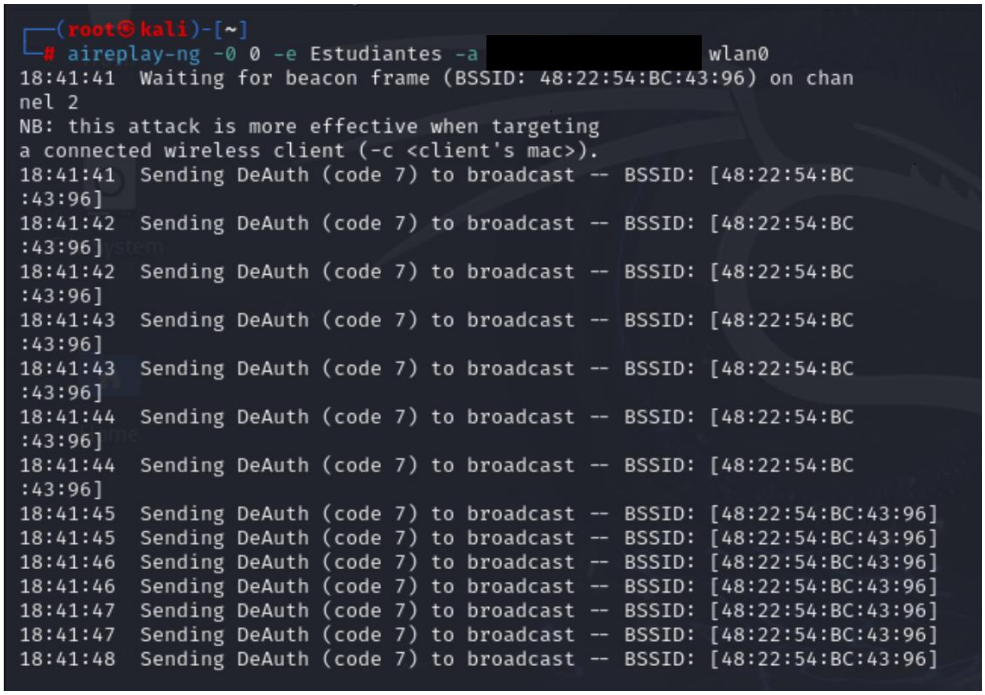


Fig. 18 Ataque al Punto de Acceso.
Fuente: Autor.

Si se requiere realizar el ataque a un usuario especifico también se puede hacer uso de aireplay-ng enviando paquetes de des-autenticación a un usuario especifico en un bucle infinito.

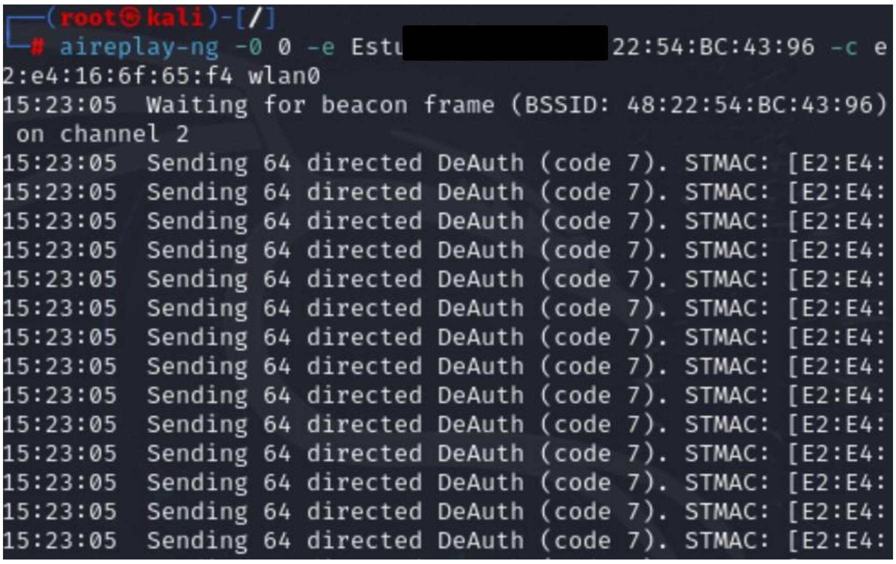


Fig. 19 Ataque a un usuario especifico.
Fuente: Autor.

Una vez que se ejecuta el ataque, automáticamente pierden la conexión el dispositivo de usuario con el punto de acceso.

Fig. 20 Ataque Denegación de Servicio.
Fuente: Autor.

Con este proceso se prueba la falla que existe con respecto a la disponibilidad porque no garantiza que los recursos de la red estén disponibles y accesibles cuando necesita los usuarios, sin interrupciones no autorizadas o tiempos de inactividad prolongados en la red inalámbrica.

4.4.3 Fake /Rogue AP

Primeramente, se identifica el Punto de Acceso que va ser atacado, obteniendo información como la MAC, SSID, y el canal que utiliza.

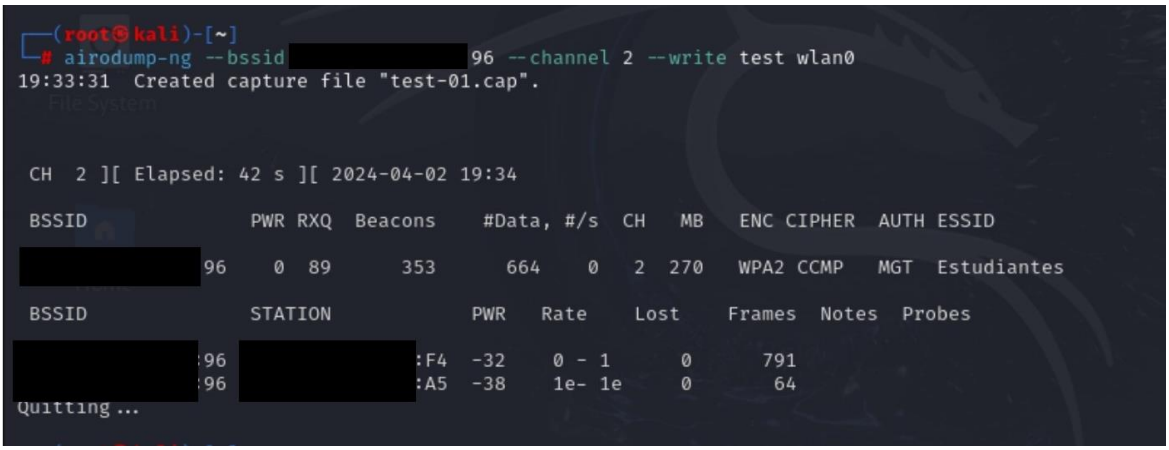


Fig. 21 Datos SSID.
Fuente: Autor.

Ejecutamos el comando aireplay-ng para des-autenticar a los clientes de forma indefinida con el fin de que ningún usuario se conecte al punto de acceso legitimo hasta terminar con el ataque.

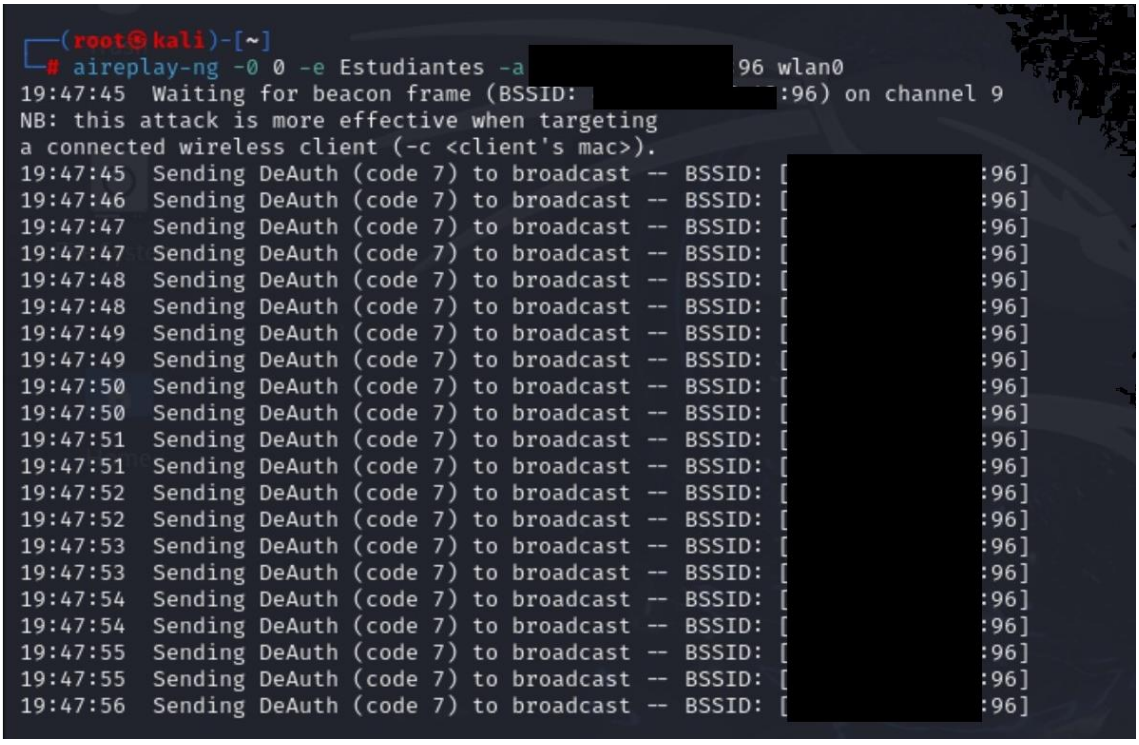


Fig. 22 Des-autenticación indefinida.
Fuente: Autor.

El software hostapd-wpe que sirve para crear puntos de acceso inalámbrico en Linux. hostapd crea el punto de acceso falso que imita al punto de acceso legítimo y wpe permite al atacante realizar ataques de suplantación de identidad contra los usuarios que intentan autenticarse en el punto de acceso falso.

```
┌──(root㉿kali)-[/etc/hostapd-wpe]
└─# hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
wlan0: interface state UNINITIALIZED→ENABLED
wlan0: AP-ENABLED
```

Fig. 23. Punto de acceso Falso
Fuente: Autor.

En la Fig. 24 se observa a los usuarios realizando la conexión al punto de acceso falso

Fig. 24 Conexión a punto de acceso falso.
Fuente: Autor.

Cuando el usuario está autenticando al punto de acceso falso, el atacante captura los paquetes y se obtiene el usuario en texto claro y la contraseña en un algoritmo de hash.

```
mschapv2: Wed Mar 13 03:02:00 2024
         username:      mrochina
         challenge:     65:18:4e:68:1d:d9:bd:96
         response:      ab:cd:ab:06:29:62:99:01:89:34:35:29:71:25
:f3:42:e3:5b:b8:37:04:40:d9:6d
         jtr NETNTLM:           mrochina:$NETNTLM$65184e681dd9bd9
6$abcdab06296299018934352971 25f342e35bb8370440d96d
```

Fig. 25 Captura de paquetes.
Fuente: Autor.

Se crea un archivo con el hash que se obtuvo para poder descifrar la contraseña.

```
┌──(root㉿kali)-[~]
└─# wordlists cat hashes.txt mrochina:$NETNTLM$65184e681dd9bd96$a
bcdab06296299018934352971 25f342e35bb8370440d96d
```

Fig. 26. Crear archivo hash.
Fuente: Autor.

Finalmente se muestra las contraseñas que se han podido descifrar a partir de los hashes proporcionados en el archivo hashes.txt

Fig. 27 Ataque Fake/Rogue AP.
Fuente: Autor.

Durante la ejecución de este ataque se captura los datos del punto de acceso legítimo, luego hacer uso de estos datos de manera no autorizada para crear otro punto de acceso falso con la finalidad de robar credenciales de los usuarios. Con este ataque se demuestra las fallas que existen en la red comprometiendo la confidencialidad e integridad de los datos.

4.5 Análisis y Evaluación de la Facultad de Ingeniería

Se realizó ataques durante 5 días, 60 ataques diarios, siendo un total de 300 ataques. Estos resultados se registran en una base de datos, 0 como ataque fallido y 1 como ataque exitoso. Del total, 100 ataques para probar Confidencialidad, 100 ataques para probar Integridad, 100 ataques para probar Disponibilidad, Por ende, se ha realizado en una escala de 1 a 10 de la siguiente manera: Bajo (>0 a <=3,2), Medio (>3,2 a <=6,8) y Alto (>6,8 a <=10), como una forma más simple de visualizar las amenazas, impactos y probabilidades tomando como referencia la tablas de criticidad emitidas por el Ministerio de Telecomunicaciones para medir la confidencialidad, integridad y disponibilidad[27], posteriormente tomar los criterios con respecto al proceso de evaluación de la red inalámbrica.

Tabla 14. Criterio para medir Confidencialidad

Confidencialidad	Criterio
Alto (>6,8 a <=10)	La divulgación no autorizada de la información tiene un efecto crítico para la red
Medio (>3,2 a <=6,8)	La divulgación no autorizada de la información tiene un efecto limitado para la red
Bajo (>0 a <=3,2)	La divulgación de la información no tiene ningún efecto para la red

Fuente: [27]

Tabla 15, Criterio para medir Integridad

Integridad	Criterio
Alto (>=6,8 a <=10)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la red
Medio (>=3,2 a <6,8)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la red
Bajo (>=0 a <3,2)	La destrucción o modificación de la información tiene un efecto leve para la red

Fuente:[27]

Tabla 16. Criterio para medir Disponibilidad

Disponibilidad	Criterio
Alto (>6,8 a <=10)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la red
Medio (>3,2a <=6,8)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la red
Bajo (>0 a <=3,2)	La interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la red

Fuente:[27]

Tabla 17. Criterio para medir amenazas

Nivel de amenazas	Criterio
Bajo(>0 a <=3,2)	La ocurrencia es menos probable.
Medio (>3,2 a <=6,8)	La ocurrencia es probable.
Alto(>6,8 a <=10)	La ocurrencia es muy probable.

Fuente: [27]

Tabla 18. Criterio para medir vulnerabilidad

Nivel de vulnerabilidad	Criterio
Bajo(>0 a <=3,2)	La medida de seguridad es adecuada
Medio (>3,2 a <=6,8)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable.
Alto(>6,8 a <=10)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza.

Fuente:[27]

Como inicialmente el número de ataques era 100 para cada uno de los indicadores, entonces hacemos una relación a la escala 10 para realizar los cálculos correspondientes.

Tabla 19. Criterio de evaluación con respecto a los ataques

Criterio de Evaluación	**Escala de 100**	**Escala de 10**
Bajo	>=0 a <= 32 ataques exitosos	>=0 a <= 3,2 ataques exitosos
Medio	>32 a <=68 ataques exitosos	>3,2 a <=6,8 ataques exitosos
Alto	>68 a <=100 ataques exitosos	>6,8 a <=10 ataques exitosos

Fuente: Autor.

El análisis de riesgo se hace de manera conjunta para el bloque A y bloque B de la Facultad de Ingeniería debido a que existe las mismas amenazas y vulnerabilidad expuestas en la Tabla 20.

Tabla 20. Análisis de Riesgo

Análisis de Riesgo		
Nombre de Activo	Amenazas	Vulnerabilidades
Puntos de accesos, Dispositivos de usuarios	Intercepción de datos	Cifrado vulnerable para ciertos tipos de ataque.
	Interrupción de servicio	Falta de medidas de mitigación de ataques DOS.
	Acceso no autorizado	Contraseñas débiles.

Fuente: Autor.

Teniendo en cuenta las calificaciones en las tablas anteriores, al realizar la multiplicación, obtenemos un rango de valores para el riesgo del (>=0 a <=320) es riesgo bajo, (>320 a <=680) es riesgo medio, (>680 a <=1000) es riesgo alto como se muestra en la Tabla 21 para el cálculo del resultado final de la Facultad de Ingeniería.

Tabla 21. Criterio de evaluación de riesgo

Nivel de Riesgo	
>=0 a <=320	El riesgo es Bajo
>320 a <=680	El riesgo es Medio
>680 a <=1000	El riesgo es Alto

Fuente: Autor.

4.5.1 Análisis y Evaluación de Bloque A

4.5.1.1 Análisis e interpretación de resultados de la variable Independiente

Con tamaño de muestra n=300 y porción de éxitos X= 201. La proporción de la muestra es $p = \frac{X}{n} = \frac{201}{300} = 0.67$, para Z= 1.96 para el 95% de confianza. Calculamos el intervalo de confianza.

$$IC = p \pm 1.96\sqrt{\frac{0.67(1-0.67)}{100}}$$

$$IC = 0.67 \pm 0.0921$$

Por lo tanto, el intervalo de confianza de los ataques exitosos sería aproximadamente entre 0.5778 (57.78%) y 0.7621 (76.21%). Es decir, hay un 95% de confianza de que la verdadera proporción de ataques exitosos en la población general este dentro del rango.

Tabla 22. Ataques ejecutados Bloque A

	Ataques ejecutados	**Ataques exitosos**	**Ataques fallidos**	**Intervalo de confianza 95%**
Cantidad	300	201	99	Entre 0,5778 y 0,7621
Porcentaje	100%	67%	33%	Entre (57,78%) y (76,21%)

Fuente: Autor

Se ha realizado 300 ataques en el escenario de pruebas, obteniendo 201 ataques éxitos y 99 ataques fallidos.

A continuación, se presenta una gráfica de los porcentajes de los ataques éxitos y ataques fallidos para la presente investigación

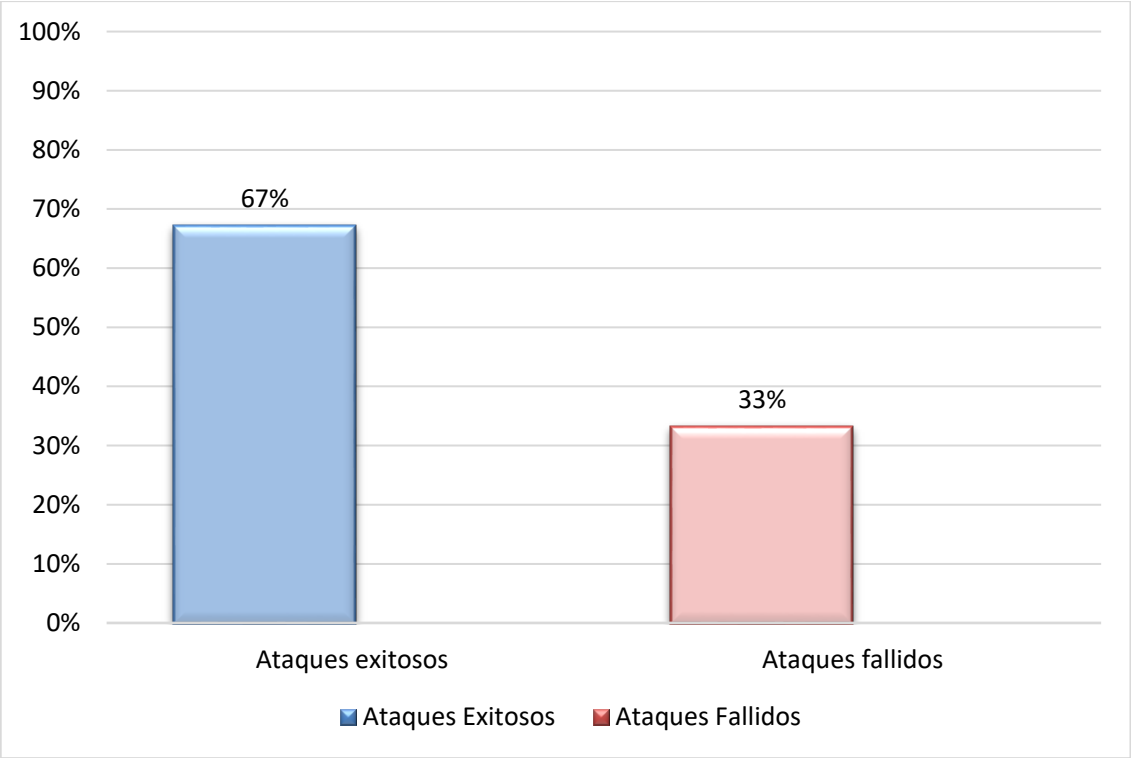


Fig. 28 Porcentaje de ataques en el Bloque A.

Se ejecutaron la cantidad de 300 ataques que representan el 100% obteniendo 67% ataques exitosos y 33% ataques fallidos en el Bloque A.

4.5.1.2 Análisis e interpretación de resultados de la variable Dependiente

Tabla 23. Ataques para medir los controles establecidos Bloque A

	Ataques ejecutados	Ataques exitosos	Ataques fallidos
Confidencialidad	100	69	31
Integridad	100	57	43
Disponibilidad	100	75	25

Fuente: Autor.

Para medir los controles que previamente se establecieron se realiza la cantidad 100 ataques para cada uno de ellas, además, se describe el número de ataques exitosos y fallidos.

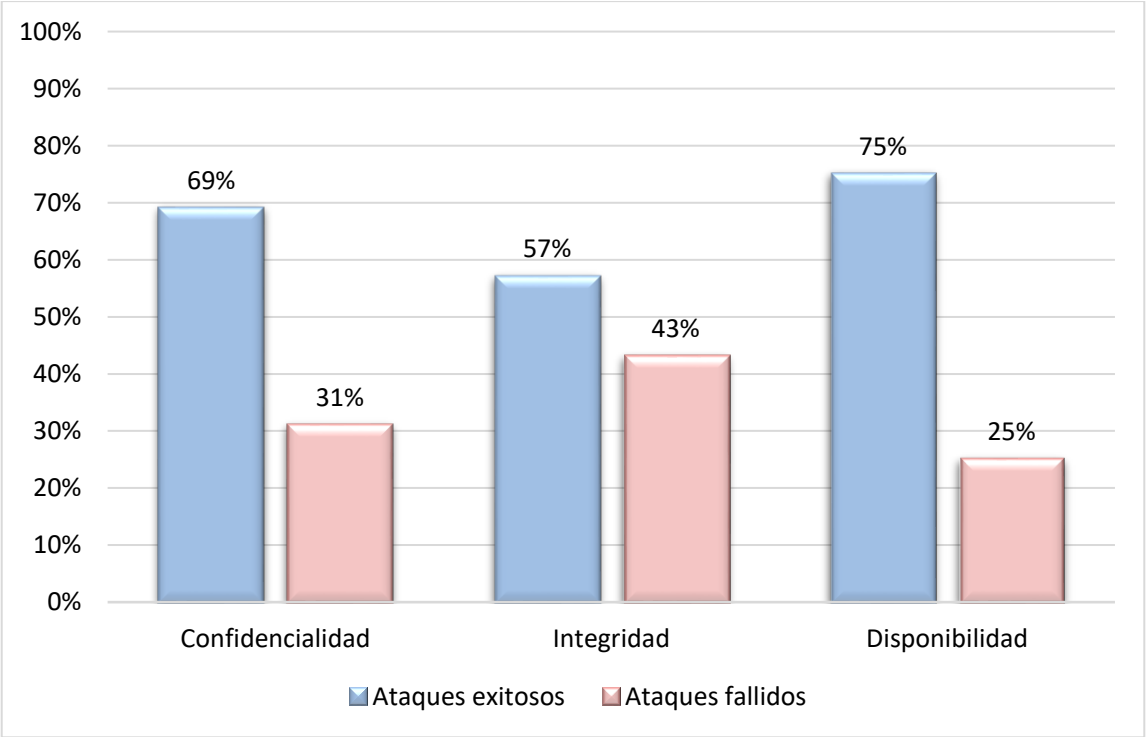


Fig. 29 Porcentaje de ataques de los controles Bloque A.

En la Fig.29 se observa el porcentaje de los ataques exitosos y fallidos para medir el nivel de seguridad mediante los controles establecidos, 69% de ataques exitosos y 31% de ataques fallidos en confidencialidad, 57% de ataques exitosos y 43% de ataques fallidos en integridad, y 75% de ataques exitosos y 25% de ataques fallidos en disponibilidad.

De acuerdo a los resultados que se obtiene en la tabla anterior se evalúa en una escala de 10 determinando la criticidad que corresponde.

Tabla 24. Evaluación de los controles de Seguridad Bloque A

Controles	Ataques exitosos	Criticidad
Confidencialidad	6,9	Alto
Integridad	5,7	Medio
Disponibilidad	7,5	Alto

Fuente: Autor.

Tomando los resultados de la Tabla 24 se calcula la valoración de activos y posterior el nivel de riesgo.

$$\text{Valoración de Activos} = \frac{\text{Confidencialidad} + \text{Integridad} + \text{Disponibilidad}}{3}$$

$$\text{Valoración de Activos} = \frac{6{,}9 + 5{,}7 + 7{,}5}{3} = 6{,}7$$

$$\text{Nivel de Riesgo} = \text{VA(CID)} * \text{Nivel de amenaza} * \text{Nivel de Vulnerabilidad}$$

$$\text{Nivel de Riesgo} = 6{,}7 * 7 * 7 = 328{,}3$$

4.5.2 Análisis y Evaluación de Bloque B

4.5.2.1 Análisis e interpretación de resultados de la variable Independiente

Con tamaño de muestra n=300 y porción de éxitos X= 223. La proporción de la muestra es $p = \frac{X}{n} = \frac{223}{300} = 0.74$, para Z=1,96 para el 95% de confianza. Calculamos el intervalo de confianza.

$$IC = p \pm 1.96\sqrt{\frac{0.74(1-0.74)}{100}}$$

$$IC = 0.74 \pm 0.03245$$

Por lo tanto, el intervalo de confianza de los ataques exitosos sería aproximadamente entre 0.7075 (70.75%) y 0.7724 (77.24%). Es decir, hay un 95% de confianza de que la verdadera proporción de ataques exitosos en la población general cae dentro del rango.

Tabla 25. Ataques ejecutados Bloque B

	Ataques ejecutados	Ataques exitosos	Ataques fallidos	Intervalo de confianza 95%
Total	300	223	77	Entre 0.7075 y 0,7724
Porcentaje	100 %	74.33 %	25.67 %	Entre (70.75%) y (77.24%)

Fuente: Autor.

Durante la ejecución de pruebas de penetración se ejecutaron la cantidad de 300 ataques que representan el 100% obteniendo 223 ataques exitosos y 77 ataques fallidos en el Bloque B.

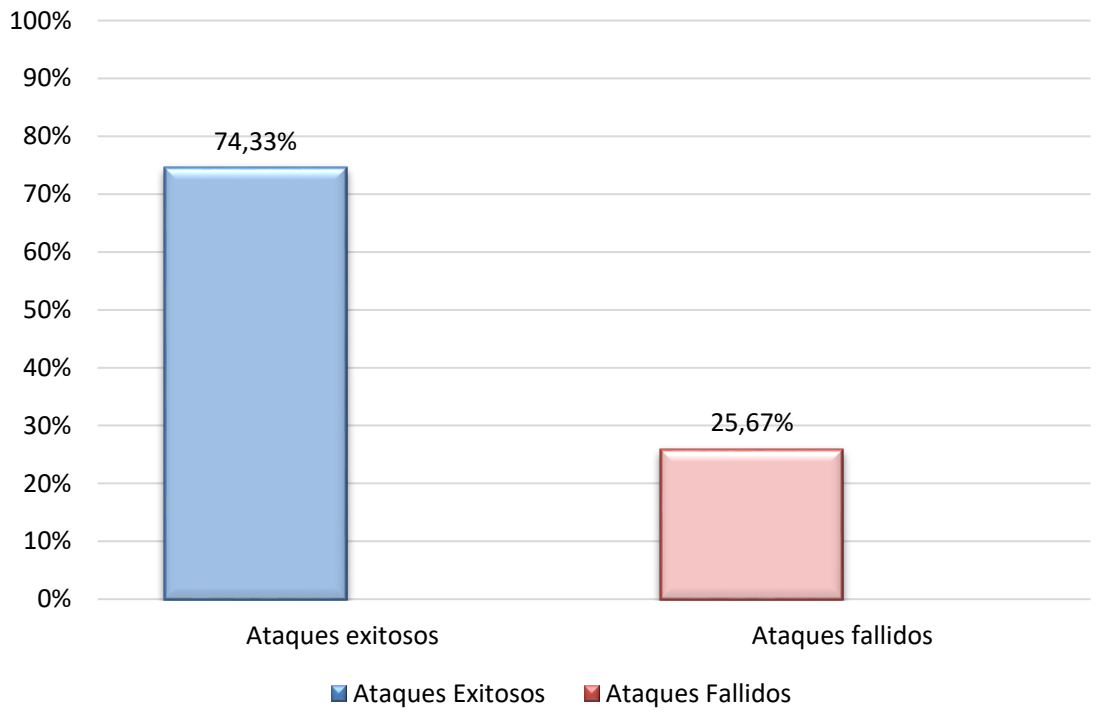


Fig. 30 Porcentaje de ataques en el Bloque B.

Se ejecutaron la cantidad de 300 ataques que representan el 100% obteniendo 74,33% ataques exitosos y 25,67% ataques fallidos en el Bloque B.

4.5.2.2 Análisis e interpretación de resultados de la variable Dependiente

Tabla 26. Ataques para medir los controles establecidos Bloque B

	Ataques ejecutados	Ataques exitosos	Ataques fallidos
Confidencialidad	100	75	25
Integridad	100	66	34
Disponibilidad	100	82	18

Fuente: Autor.

Para medir los controles en el bloque B se realiza la cantidad 100 ataques para cada uno de ellas, además, se describe el número de ataques exitosos y fallidos.

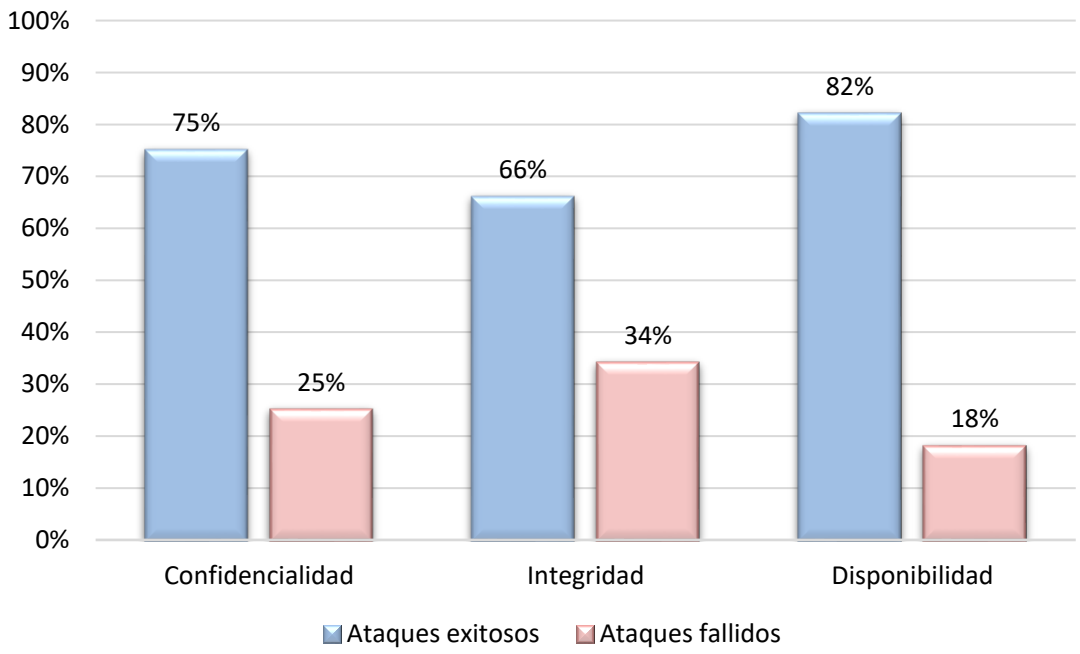


Fig. 31 Porcentaje de ataques de los controles Bloque B.

En la Fig.31 se observa el porcentaje de los ataques exitosos y fallidos para medir el nivel de seguridad mediante los controles establecidos, 75% de ataques exitosos y 25% de ataques fallidos en confidencialidad, 66% de ataques exitosos y 34% de ataques fallidos en integridad, y 82% de ataques exitosos y 18% de ataques fallidos en disponibilidad.
De acuerdo a los resultados que se obtiene en la tabla anterior se evalúa en una escala de 10 determinando la criticidad que corresponde.

Tabla 27. Evaluación de los controles de seguridad Bloque B

Controles	Ataques exitosos	Criticidad
Confidencialidad	7,5	Alto
Integridad	6,6	Medio
Disponibilidad	8,2	Alto

Fuente: Autor.

Tomando los resultados de la Tabla 24 se calcula la valoración de activos y posterior el nivel de riesgo.

$$\text{Valoración de Activos} = \frac{\text{Confidencialidad} + \text{Integridad} + \text{Disponibilidad}}{3}$$

$$\text{Valoración de Activos} = \frac{7{,}5 + 6{,}6 + 8{,}2}{3} = 7{,}43$$

$$\text{Nivel de Riesgo} = \text{VA(CID)} * \text{Nivel de amenaza} * \text{Nivel de Vulnerabilidad}$$

$$\text{Nivel de Riesgo} = 7{,}43 * 7 * 7 = 364{,}07$$

Durante las simulaciones de los bloques A y B, considerando los tres tipos de ataques (Diccionario y Fuerza Bruta, Denegación de Servicio y Fake/Rogue AP), y los parámetros de medición del nivel de riesgo, valor de activos obtenemos los siguientes resultados.

Tabla 28. Tabla de resumen

Parámetros	Valor de Activo	Nivel de Riesgo
Bloque A	6,7	328.3
Bloque B	7,43	364,07

Fuente: Autor.

El nivel de riesgo y el nivel de seguridad están inversamente relacionados: a medida que el nivel de seguridad aumenta, el nivel de riesgo disminuye, y viceversa. Con los resultados de la Tabla 28, el nivel de riesgo es 328,3 en el bloque A, y de acuerdo a la Tabla 21 equivale a un riesgo medio, por lo tanto, el nivel de seguridad es MEDIO (671.7) que equivale un porcentaje de 67,17%. Así mismo, si el nivel de riesgo es 364,07 en el Bloque B equivale a un riesgo medio y el nivel de seguridad es MEDIO (635.93) que equivale un porcentaje de 63.59%.

5. CAPÍTULO V

5.1 Conclusiones y Recomendaciones

5.1.1 Conclusiones

- Luego de estudiar la topología, información de DTIC y fuentes bibliográficas, se ha identificado amenazas, vulnerabilidades como la autenticación mediante contraseñas es simple, el atacante puede interceptar datos comprometiendo la seguridad de la conexión. Además, el tipo de encriptación WPA2 Enterprise es propenso a ataques de diccionario y fuerza bruta.
- Para evaluar la seguridad se estableció los controles de manera que garantiza el principio fundamental de confidencialidad, integridad y disponibilidad de la red inalámbrica de la Facultad de Ingeniería UNACH.
- La implementación de un escenario de pruebas fue de gran utilidad, en el cual se simuló condiciones reales de la infraestructura de red donde se realizó varios tipos de ataques utilizando las herramientas de software libre, tales como: Sistema Operativo Linux, Kali Linux y aircrack.
- Una vez explotado las vulnerabilidades detectadas, se procedió a realizar un análisis de los controles de seguridad mediante criterios e indicadores, y se determinó que el nivel de seguridad en el Bloque A es medio (671.7) con un porcentaje de 67,17% y para el Bloque B es medio (635.93) con un porcentaje de 63.59%.

5.1.2 Recomendaciones

- Se recomienda a los administradores de red aplicar medidas de seguridad con respecto a las contraseñas de los usuarios tales como: contraseñas robustas y actualización de forma periódica que ayudara aprevenir y reducir la probabilidad de posibles ataques de acceso no autorizado.
- Monitorear constantemente el tráfico de la red inalámbrica para detectar actividades maliciosas identificando dispositivos intrusos, posteriormente aplicar controles de seguridad que ayudan a proteger información sensible de los usuarios.
- Capacitar a los usuarios en las buenas prácticas de seguridad con la finalidad de concientizar sobre los riesgos proporcionando conocimientos necesarios para proteger los datos personales y sus dispositivos a fin de evitar que sean víctimas de ataques.
- Investigar nuevas formas de implementar el servicio de red inalámbrica como: cifrado WPA3, Autenticación Multifactor, Portal Cautivo integrando con el Sistema de Prevención de Intrusiones que detecta y previene intrusos de manera automática bloqueando las amenazas.

BIBLIOGRAFÍA

[1] A. F. Salazar Herrera, D. A. Barahona Cuji, J. V. Delgado Delgado, y J. C. Suárez León, «Seguridad en Redes WIFI», *UIDE*, 2023.

[2] Rom-Mayer, «Ventajas y desventajas de implementar redes inalámbricas», Rom Mayer. Accedido: 7 de abril de 2024. [En línea]. Disponible en: https://rom-mayer.cl/redes-inalambricas-2/

[3] «Red Inalámbrica - Qué es, tipos, ventajas, desventajas y ejemplos». Accedido: 7 de abril de 2024. [En línea]. Disponible en: https://concepto.de/red-inalambrica/

[4] J. M. Basurto Delgado, «ANÁLISIS DE SEGURIDAD MEDIANTE METODOLOGÍA OWASP A REDES INALÁMBRICAS EN "UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EN EL CARMEN"», UNIVERSIDAD LAICA «ELOY ALFARO» DE MANABÍ EXTENSIÓN EN EL CARMEN, EL CARMEN, 2020.

[5] R. I. Salinas Vasquez, «Análisis de las vulnerabilidades del protocolo de seguridad WPA y WPA2 en redes inalámbricas», UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA, Santa Elena, 2023.

[6] S. M. Barahona Uriña y J. R. Gonzalez Crespo, «AUDITORIA INFORMÁTICA DE LAS VULNERABILIDADES DE SEGURIDAD EN LA RED INALÁMBRICA DE LA EMPRESA PUNTO DE VISTA CON LAS HERRAMIENTAS ACRYLIC WI-FI Y OPENVAS UTILIZANDO LA METODOLOGÍA DE EVALUACIÓN DE SEGURIDAD WIRELESS ABIERTA (OWISAM)», *Univ. GUAYAQUIL*, 2022.

[7] C. P. Miranda Silva, «AUDITORÍA DE REDES, APLICANDO LA METODOLOGÍA OSSTMM V3, PARA EL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL.», *Univ. Téc. AMBATO*, 2019.

[8] G. Bustelo, «Sniffing: ¿qué es y cómo podemos evitarlo?», Red Seguridad. Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://www.redseguridad.com/actualidad/sniffing-que-es-como-evitar_20230713.html

[9] G. RGPD, «Los principales riesgos y amenazas en las redes inalámbricas (II)», Adaptación RGPD. Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://www.adaptacion-rgpd.eu/los-principales-riesgos-y-amenazas-en-las-redes-inalambricas-ii/

[10] INCIBE, «Seguridad en redes wifi: una guia de aproximación para el empresario». Instituto Nacional de ciberseguridad, 2019.

[11] D. Cunha Barbosa, «Qué es un ataque de Man-in-the-Middle y cómo funciona». Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2021/12/28/que-es-ataque-man-in-the-middle-como-funciona/

[12] «OpenVAS - Open Vulnerability Assessment Scanner». Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://www.openvas.org/

[13] «Kismet: Wi-Fi, Bluetooth, RF, and more», Kismet. Accedido: 19 de marzo de 2024. [En línea]. Disponible en: https://www.kismetwireless.net/

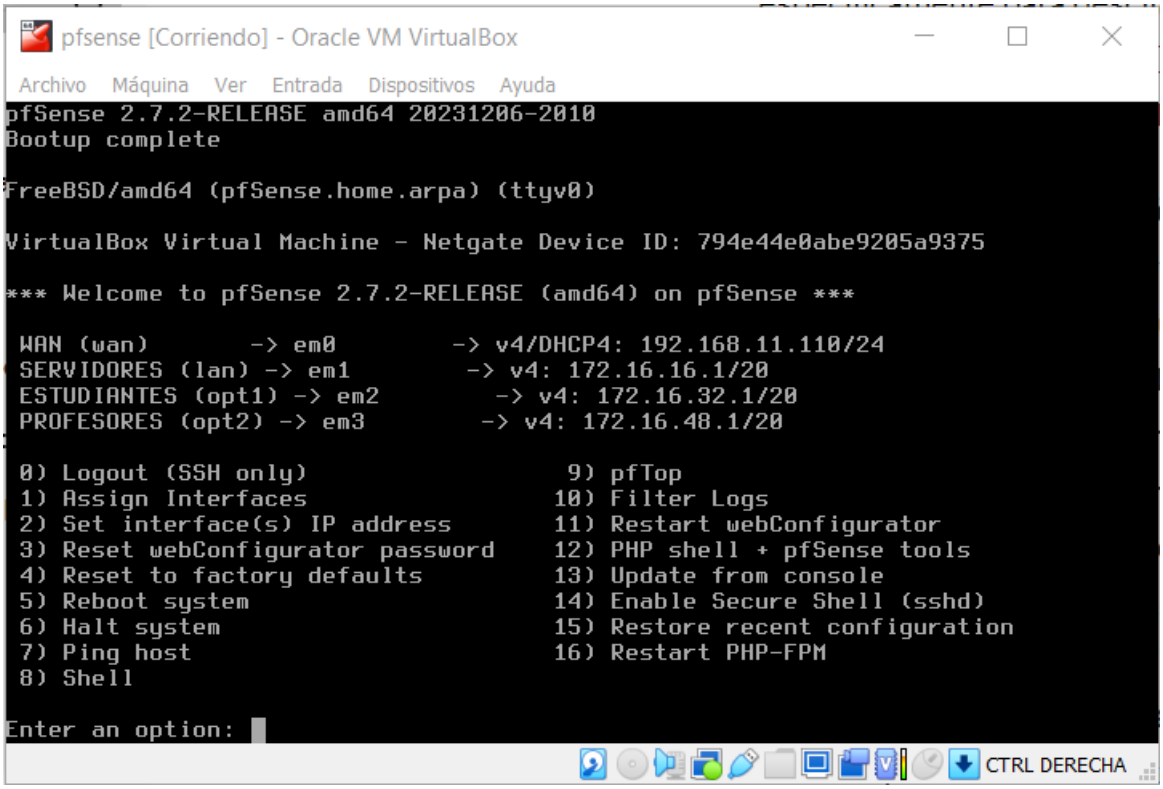
[14] «Nmap: the Network Mapper - Free Security Scanner». Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://nmap.org/

[15] «Aircrack-ng». Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://www.aircrack-ng.org/doku.php?id=es:aircrack-ng
[16] «Auditorías de Seguridad Informática», Wardsec. Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://wardsec.com/en/wireless-audit/
[17] ISECOM, «RESEARCH». Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://www.isecom.org/research.html
[18] «¿Qué es la tríada CIA y por qué es importante? | Fortinet». Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/cia-triad
[19] «Principios Fundamentales», Ciberseguridad. Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://ciberseguridad.comillas.edu/principios-fundamentales/
[20] J. M. Sánchez Alès, «Servidor RADIUS». Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://sio2sio2.github.io/doc-linux/98.apendice/99.radius/index.html
[21] «IBM Documentation». Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://www.ibm.com/docs/es/i/7.1?topic=authentication-remote-dial-in-user-service-overview
[22] «¿Qué es un firewall? Definición y explicación», latam.kaspersky.com. Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/firewall
[23] «¿Qué es un firewall?», Cisco. Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html
[24] «Conceptos básicos sobre bases de datos - Soporte técnico de Microsoft». Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://support.microsoft.com/es-es/topic/conceptos-b%C3%A1sicos-sobre-bases-de-datos-a849ac16-07c7-4a31-9948-3c8c94a7c204
[25] «¿Qué es una base de datos?» Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://www.oracle.com/mx/database/what-is-database/
[26] «¿Qué es un punto de acceso en redes?», Juniper Networks. Accedido: 21 de marzo de 2024. [En línea]. Disponible en: https://www.juniper.net/mx/es/research-topics/what-is-an-access-point-in-networking.html
[27] «Guía para la gestión de riesgos de seguridad de información». Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020.

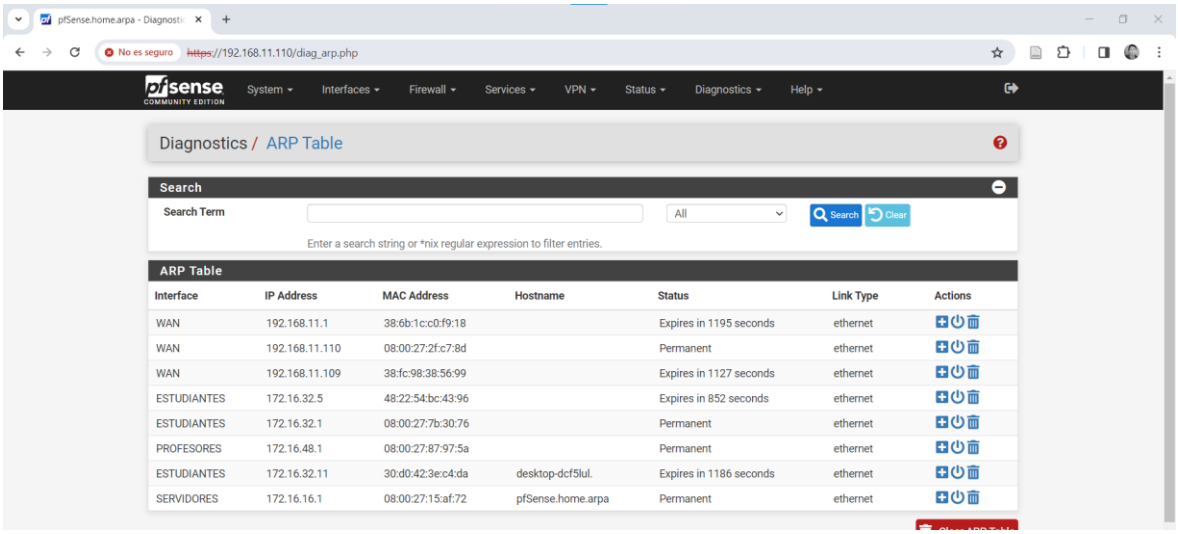
ANEXOS

ANEXO 1: Captura de pantalla de los servidores levantados

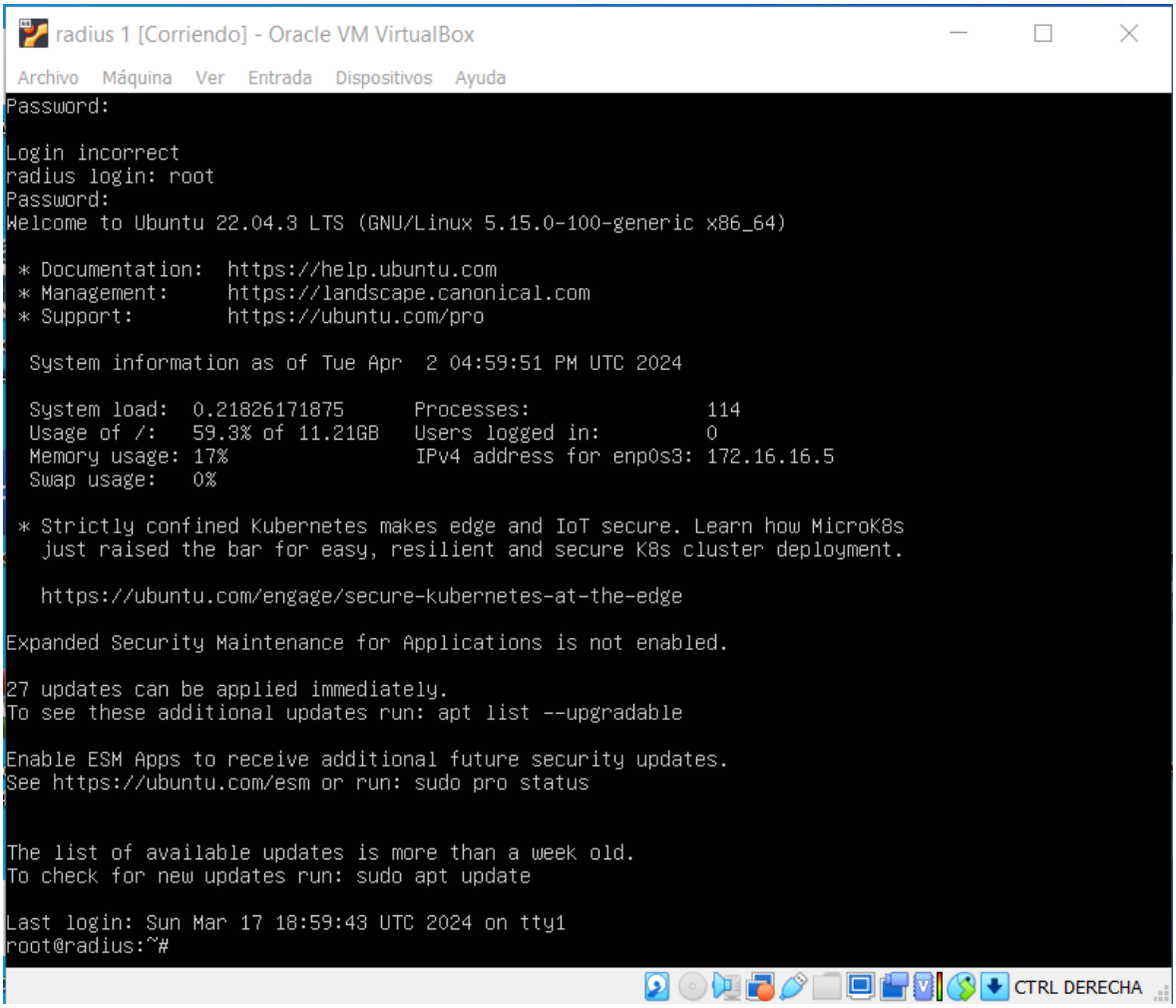
Iniciamos la máquina virtual de pfSense, en el cual se simula router y firewall del escenario.



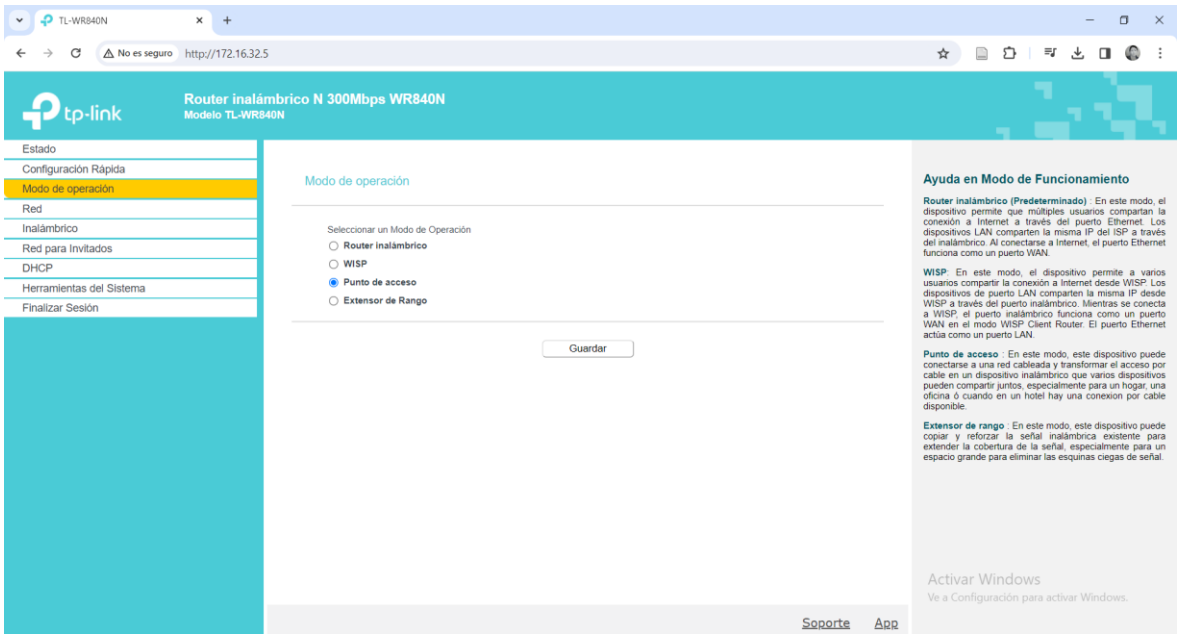
Con la dirección IP WAN ingresamos a un navegador y podemos visualizar de manera gráfica para realizar cualquier tipo de configuración de acuerdo a los requerimientos del administrador.



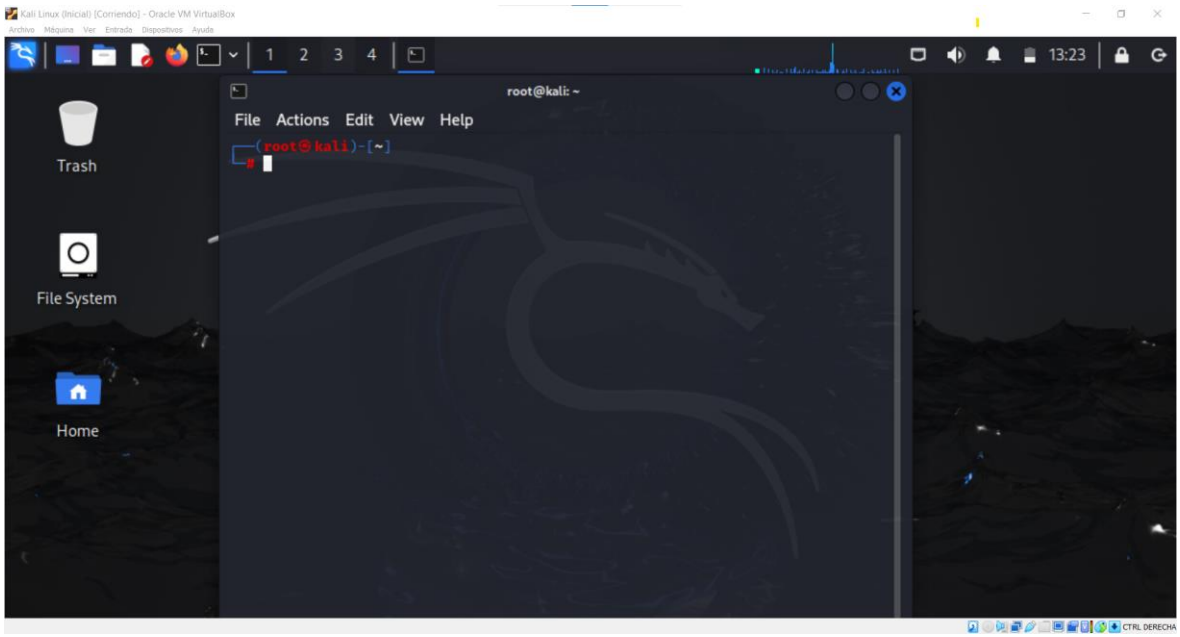
Se inicia el servidor radius donde se aloja la base de datos de los usuarios y realiza el proceso de autenticación.



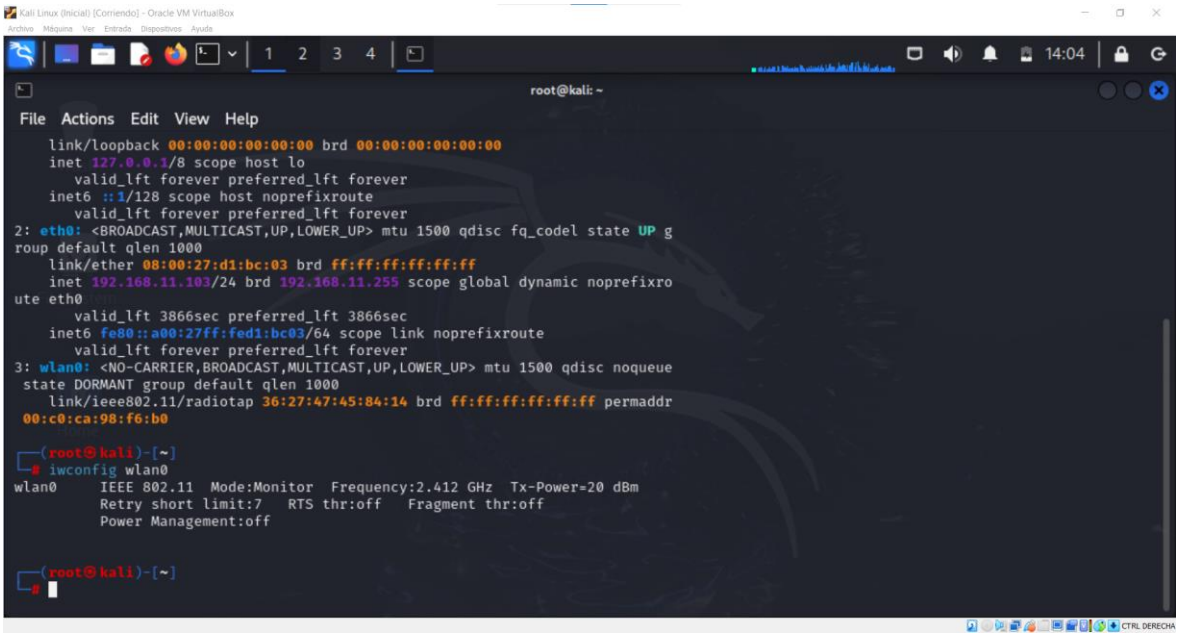
Configuramos el Dispositivo tp-link en modo punto de acceso



Iniciamos Kali Linux en modo root para realizar las pruebas de seguridad a la infraestructura inalámbrica. Una vez iniciado se puede instalar o hacer uso de las herramientas que ya vienen de manera predeterminada para realizar escaneos y ataques.



Para realizar el escaneo de red y hacer uso de las herramientas de kali Linux la tarjeta inalámbrica debe estar en modo monitor



Registro de los ataques