

**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

**TÍTULO DEL TRABAJO DE TITULACIÓN**

Análisis de las vulnerabilidades del protocolo de seguridad WPA y WPA2  
en redes inalámbricas

**AUTOR**

**Salinas Vasquez, Robert Ivan**

Examen Complexivo

Previo a la obtención del grado académico en  
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

**TUTOR**

**Haz López, Lídice.**

**Santa Elena, Ecuador**

**Año 2023**



**UPSE**

**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

**TRIBUNAL DE SUSTENTACIÓN**

Ing. José Sánchez A. Mgt.  
**DIRECTOR DE LA CARRERA**

Ing. Lidice Haz L. Mgt.  
**TUTOR**

Lic. Daniel Quirumbay Y. Msi  
**DOCENTE ESPECIALISTA**

Ing. Marjorie Coronel S. 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 **Salinas Vasquez Robert Ivan**, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 02 días del mes de Agosto del año 2023

**TUTOR**

A handwritten signature in blue ink, which appears to read "Lidice Haz López", is written over a horizontal line.

**Lidice Haz López**



**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

**DECLARACIÓN DE RESPONSABILIDAD**

Yo, **Robert Ivan Salinas Vasquez**

**DECLARO QUE:**

El trabajo de Titulación, Análisis de las vulnerabilidades del protocolo de seguridad WPA y WPA2 en redes inalámbricas, 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 02 días del mes de Agosto del año 2023

**EL AUTOR**

A handwritten signature in black ink, appearing to read "Robert Salinas Vasquez", is written over a horizontal line.

**Robert Ivan Salinas Vasquez**



**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 las vulnerabilidades del protocolo de seguridad WPA y WPA2 en redes inalámbricas**, presentado por el estudiante, **Salinas Vasquez Robert Ivan** fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 7%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

COMPILATIO MAGISTER  
Sistemas y Telecomunicaciones

SalinasVasquez #f5b14e

7%

Ubicación de las similitudes en el documento:

Fuentes

CONFIGURACIÓN de las fuentes  
Agrupar las fuentes similares:

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	<a href="http://www.consejodecomunicacion.gob.ec">www.consejodecomunicacion.gob.ec</a> <a href="https://www.consejodecomunicacion.gob.ec/wp-content/uploads/downloads/2021/07/lotaip/ley...">https://www.consejodecomunicacion.gob.ec/wp-content/uploads/downloads/2021/07/lotaip/ley...</a>	3%		Palabras idénticas : 3% (432 palabras)
2	Documento de otro usuario #f6e28f El documento proviene de otro grupo	< 1%		Palabras idénticas : < 1% (81 palabras)

**TUTOR**



Firmado electrónicamente por:  
**LÍDICE VICTORIA HAZ  
LÓPEZ**

**Ing. Lídice Haz López**



**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

**AUTORIZACIÓN**

**Yo, Robert Ivan Salinas Vasquez**

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 02 días del mes de Agosto del año 2023

**EL AUTOR**

---

**Robert Ivan Salinas Vasquez**

## **AGRADECIMIENTO**

Es de mucha importancia agradecerle a mi madre por los esfuerzos y alientos necesarios para poder alcanzar esta etapa muy impórtate en mi vida, Gracias a todos mis familiares por el brindarme su apoyo, valores y conocimientos que me han servido para esta formación y crecer profesionalmente, gracias por el apoyo incondicional.

El respeto y agradecimiento a mi tutora Ing. Haz López Lídice. Msi, por todo el aprendizaje y conocimiento impartido y direccionarme para poder cumplir con todo lo necesario para este proceso.

*Robert Ivan Salinas Vasquez*

## **DEDICATORIA**

El presente proyecto de titulación esta dedico dedicación a nuestro creador, a mi madre y familiares que hicieron que esto sea posible, a las que en el momento siguen siendo una parte importante y siempre he recibido el apoyo emocional y elemental.

A mis compañeros y amigos que siempre estuvieron en constante motivación y me brindaron su apoyo.

*Robert Ivan Salinas Vasquez*

## ÍNDICE GENERAL

TÍTULO DEL TRABAJO DE TITULACIÓN	I
TRIBUNAL DE SUSTENTACIÓN	II
CERTIFICACIÓN	III
DECLARACIÓN DE RESPONSABILIDAD	IV
DECLARO QUE:	IV
CERTIFICACIÓN DE ANTIPLAGIO	V
AUTORIZACIÓN	VI
AGRADECIMIENTO	VII
DEDICATORIA	VIII
ÍNDICE GENERAL	IX
ÍNDICE DE TABLAS	XI
ÍNDICE DE FIGURAS	XII
RESUMEN	XIV
ABSTRACT	XV
INTRODUCCIÓN	1
CAPÍTULO 1	2
FUNDAMENTACIÓN	2
1.1 ANTECEDENTES	2
1.2 DESCRIPCIÓN DEL PROYECTO	4
1.3 OBJETIVOS	6
1.3.1 OBJETIVO GENERAL	6
1.3.2 OBJETIVOS ESPECÍFICO	6
1.4 JUSTIFICACIÓN	6
1.5 ALCANCE	8
CAPÍTULO 2	10
2.1 MARCO CONTEXTUAL	10
2.2 MARCO CONCEPTUAL	10
2.2.1 MÉTODOS O MECANISMOS DE SEGURIDAD	14
2.2.2 VENTAJAS DE LAS REDES INALÁMBRICAS	15
2.2.3 INCONVENIENTES DE LAS REDES INALÁMBRICAS	15
2.2.4 OBTENCIÓN DE CLAVES EN REDES WLAN CON WIFISLAX	16
2.2.5 SISTEMAS OPERATIVOS UTILIZADOS PARA AUDITORÍA DE REDES INALÁMBRICAS Y HERRAMIENTAS	17
2.2.6 COMPARACIÓN DE LOS PROTOCOLOS DE ENCRIPCIÓN	19
2.2.7 PUNTOS CRÍTICOS EN REDES INALAMBRICAS	20
2.2.8 BARRERAS DE PROTECCIÓN EN LAS REDES INALAMBRICAS	21
2.2.9 TERMINOS FRECUENTES EN EL ESCANEAMIENTO DE OBJETOS	21
2.3 MARCO LEGAL	22
2.3.1 LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES	22
2.4 MARCO TEÓRICO	24
2.4.1 ¿QUE ES EL HACKING ÉTICO Y PARA QUE SIRVE?	24
2.4.2 DETECCIÓN DE VULNERABILIDADES	24
2.4.3 ¿QUE ES LA CIBERSEGURIDAD?	24
2.4.4 TIPOS DE ESTANDARES PARA LAS REDES INALMBRICAS	25
2.4.5 ESTANDAR 802.11	26
	IX

2.4.6	TIPOS DE REDES INALAMBRICAS	27
2.4.7	ESQUEMAS DE LOS PROTOCOLOS WPA Y WPA2	28
2.4.8	ATAQUES DE CLAVES WPA Y WPA2	28
2.5	METODOLOGÍA	30
2.5.1	METODOLOGÍA DEL PROYECTO	30
2.5.2	METODOLOGÍA DE INVESTIGACIÓN	31
	INVESTIGACIÓN DESCRIPTIVA	31
	INVESTIGACIÓN EXPERIMENTAL	31
2.5.3	TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS	32
	CAPÍTULO 3	32
	PROPUESTA	32
3.1	FASE 1.- RECONOCIMIENTO	32
3.2	FASE 2.- ESCANEEO	34
3.3	FASE 3.- OBTENER ACCESO	35
3.4	FASE 4.- ELABORACIÓN DE REPORTE	36
	CONCLUSIONES	39
	RECOMENDACIONES	40
	BIBLIOGRAFIA	41
	ANEXO 1	46
	ANEXO 2	51

## ÍNDICE DE TABLAS

<b>Tabla 1</b>	Servicios Básicos de la seguridad en las redes inalámbricas	14
<b>Tabla 2</b>	Vista monitor de Aircrack.ng	17
<b>Tabla 3</b>	Protocolos WPA vs WPA2 diferencias	19
<b>Tabla 4</b>	Puntos Críticos y Detalles	20
<b>Tabla 5</b>	Barreras de protección en las redes inalámbricas	21
<b>Tabla 6</b>	Descripción de terminologías aplicadas en las herramientas	21
<b>Tabla 7</b>	Normas de tecnología	25
<b>Tabla 8</b>	Tabla de resultado fase 1 - Reconocimiento	33
<b>Tabla 9</b>	Tabla de resultado fase 2 - Escaneo	34
<b>Tabla 10</b>	Tabla de resultado fase 3 - Obtener Acceso	35
<b>Tabla 11</b>	Tabla detección de amenazas en la red	37
<b>Tabla 12</b>	Tabla de resultado Fase 4 - Elaboración de reporte	38

## ÍNDICE DE FIGURAS

<b>Figura 1.</b> Estadística de Security Report Latinoamérica.	7
<b>Figura 2.</b> Localidad donde se desarrollará el proyecto.	10
<b>Figura 3.</b> Aplicación del estándar 802.11.	27
<b>Figura 4.</b> Clasificación de las redes inalámbricas.	27
<b>Figura 5.</b> Cifrado del protocolo CCMP.	28
<b>Figura 6.</b> Esquema de las claves wpa y wpa2.	29
<b>Figura 7.</b> Esquema de las cabeceras wpa y wpa2.	29
<b>Figura 8.</b> Ventana principal para la creación de la maquina Kali Linux.	46
<b>Figura 9.</b> Ventana del apartado red para la conexión.	47
<b>Figura 10.</b> Arranque de la nueva máquina virtual.	47
<b>Figura 11.</b> Terminal de Kali Linux para el uso de Nmap.	48
<b>Figura 12.</b> Aplicación del comando ifconfig en la terminal de Kali.	49
<b>Figura 13.</b> Uso del comando nmap con la Ip para poder evaluar la red de manera global.	49
<b>Figura 14.</b> Mas información sobre la ip evaluada.	50
<b>Figura 15.</b> Resultado de toda la Ip evaluada.	50
<b>Figura 16.</b> Nmap uso de la ip de los dispositivos conectados.	50
<b>Figura 17.</b> verificación de los puertos abiertos de una Ip.	51
<b>Figura 18.</b> Descarga del Sistema Operativo Wifislax.	51
<b>Figura 19.</b> Interfaz de VirtualBox para la instalación del sistema operativo.	52
<b>Figura 20.</b> Creación y visualización de Wifislax.	52
<b>Figura 21.</b> Asignación del nombre de la máquina.	53
<b>Figura 22.</b> Selección de la memoria base.	53
<b>Figura 23.</b> Asignación de la memoria virtual de la máquina.	54
<b>Figura 24.</b> Características de la maquina levantada.	54
<b>Figura 25.</b> Desactivación de la opción disquete para que inicialicé desde la memoria virtual.	55
<b>Figura 26.</b> Borrar el disco .iso que se instaló al principio.	56
<b>Figura 27.</b> Interzas de la inicialización del s.o wifislax.	56
<b>Figura 28.</b> Selección del arrancador de Wifislax.	57
<b>Figura 29.</b> Instalación del sistema operativo.	57
<b>Figura 30.</b> Ambiente virtual de Wifislax, selección de HDD.	58
<b>Figura 31.</b> Despliegue de pantalla para crear una partición.	58
<b>Figura 32.</b> Destinar almacenamiento para la partición.	59
<b>Figura 33.</b> Aplicación de todos los cambios que se están realizando.	59
<b>Figura 34.</b> Aplicación de cambios para la aplicación de operaciones.	60
<b>Figura 35.</b> Descarga las operaciones que tiene el S.O.	60
<b>Figura 36.</b> Instalación de la partición ya creada.	61
<b>Figura 37.</b> Instalación de Wifislax.	61
<b>Figura 38.</b> culminación de la instalación.	62
<b>Figura 39.</b> Instalación de el cargador de arranque.	62
<b>Figura 40.</b> Interfaz de Wifislax, se hace uso de sus herramientas.	63
<b>Figura 41.</b> Inicialización de la herramienta Linset.	63
<b>Figura 42.</b> Selección del dispositivo USB inalámbrico.	64
<b>Figura 43.</b> Inicialización y carga de la herramienta.	64
<b>Figura 44.</b> Selección de la Interfaz que permitirá ver las redes.	65
<b>Figura 45.</b> Selección de los canales que se analizaran.	65

<b>Figura 46.</b> Escaneo de todos los probables objetivos.	66
<b>Figura 47.</b> Listado de los objetivos vulnerables.	67
<b>Figura 48.</b> Información del objetivo a posiblemente atacar.	67
<b>Figura 49.</b> Selección de la ruta de handshake.	68
<b>Figura 50.</b> Uso de la herramienta de comprobación aircrack-ng.	68
<b>Figura 51.</b> Captura del handshake del cliente.	69
<b>Figura 52.</b> Captura del handshake para establecer conexión.	69
<b>Figura 53.</b> Captura del canal de datos, handshake.	70
<b>Figura 54.</b> Selección de la interfaz al cliente.	70
<b>Figura 55.</b> Selección del idioma que tendrá la interfaz.	71
<b>Figura 56.</b> Se realiza el ataque y se desactivan los servicios.	72
<b>Figura 57.</b> Red que se creó para la obtención de acceso.	72
<b>Figura 58.</b> Visualización de todo el tráfico y dispositivos conectados a la red.	73
<b>Figura 59.</b> Verificación de la red creada por lisent.	74
<b>Figura 60.</b> Obtención del handshake de clientes activos.	74
<b>Figura 61.</b> Interfaz del punto falso creado.	75
<b>Figura 62.</b> Mensaje después de obtener las credenciales.	75
<b>Figura 63.</b> Resultado final de la obtención de las credenciales.	76

## RESUMEN

El proyecto consiste en la detección de vulnerabilidades del protocolo de seguridad WPA y WPA2 en las redes inalámbricas o también conocidas como redes wireless en la locación conocida como “sector 5 esquinas” que actualmente presenta problemas de seguridad en sus protocolos de encriptación. El objetivo de este análisis es evaluar que tan vulnerables son los protocolos de seguridad wifi de qué manera sus claves de seguridad pueden ser manipuladas por terceros para poder obtener acceso a conexiones inalámbricas como puntos de accesos, e identificar vulnerabilidades brindar un reporte de posibles soluciones a las amenazas detectadas.

En el presente proyecto se está utilizando una metodología de adaptación de hacking ético que consiste en 4 fases reconocimiento, escaneo, obtener acceso, elaboración de reportes. Se realizó en un ambiente virtualizado controlado haciendo uso de las herramientas especializadas para el descifrado de claves, se logró detectar 5 vulnerabilidades cada una con sus respectivas propuestas de solución para garantizar la seguridad de la red y dispositivos.

**Palabras claves:** Seguridad de la red, Vulnerabilidades, Claves de seguridad, Redes Wireless.

## **ABSTRACT**

The project consists of the detection of vulnerabilities of the WPA and WPA2 security protocols in wireless networks or also known as wireless networks in the location known as "sector 5 corners" that currently presents security problems in their encryption protocols. The objective of this analysis is to evaluate how vulnerable are the wifi security protocols and how their security keys can be manipulated by third parties to gain access to wireless connections as access points, and to identify vulnerabilities and provide a report of possible solutions to the detected threats.

In this project we are using an adaptive ethical hacking methodology that consists of 4 phases: reconnaissance, scanning, gaining access, reporting. It was performed in a controlled virtualized environment using specialized tools for decryption of keys, it was possible to detect 5 vulnerabilities each with their respective proposals for solutions to ensure the security of the network and devices.

**Keywords:** Network security, Vulnerabilities, Security key, Wireless Networks.

## INTRODUCCIÓN

Con la gran demanda dentro del campo de la ciberseguridad se están dando a conocer que grandes empresas y hogares afectados por la poca protección dentro de las redes inalámbricas estos tipos de redes son catalogadas las más inseguras, si bien es cierto dentro del área de redes se involucra demasiado las telecomunicaciones es importante saber el medio por el cual viajan nuestros datos ya sea de manera guiada, no guiada o de manera satelital es mediante estos tipos de redes donde se puede capturar datos cifrados que circulan por la red, esto se puede determinar cómo potencialmente información peligrosa o sensible ya sea de una organización o en redes domésticas.

Es por esta razón donde se involucra la identificación de vulnerabilidades en redes inalámbricas para poder llegar a identificar las amenazas, posteriormente llegar a evaluar el estado de la red y obtener un diagnóstico sobre las amenazas detectadas, logrando concluir cuales son los tipos de amenazas encontradas y cuál es el nivel de criticidad y determinar hacia donde está dirigida hardware o software, la finalización se realizara en un reporte detallado de las herramientas utilizadas y sus posibles soluciones que a manera de coincidencia ya pueden estar establecidas por la técnica de recopilación bibliográfica.

El uso de herramientas y sistemas operativos que se utilizan en el proyecto están destinados y utilizados de manera controlada sin la necesidad de ocasionar daños o perjudicar la integridad de dispositivos, con un conocimiento previo de todas las herramientas a utilizar para la detección de vulnerabilidades de los protocolos wpa y wpa2.

Dentro de una red es importante los protocolos al igual que el flujo de comunicación a través del modelo OSI que es el que se encarga de seguir de cerca el paquete de protocolos de internet, este tipo de modelo es muy elemental dentro las redes ya que es el que se encarga de poder administrar y resolver los problemas de la red de qué manera actúa puesto que son varias capas de este modelo se puede dar la aplicación de poder aislar el problema de la red en unas de las capas específicas y así solucionar los problemas de la red.

# CAPÍTULO 1

## FUNDAMENTACIÓN

### 1.1 ANTECEDENTES

Actualmente en la provincia de santa elena los proveedores del servicio de internet que suministran a sus usuarios lo realizan por el medio de routers el que posteriormente se maneja por una configuración básica donde se tiene riesgos de los ataques pueden ser con mayor frecuencia y más comunes es contra la clave PSK (Clave Pre Compartida), que en el acto de inmediato de tener contacto con el cliente y AP (Access Point) es decir que justo cuando el cliente se conecta a la red mediante la conexión que se establece tanto con el servidor de autenticación de 802.11x como el cliente genera dos claves aleatorias las que se denominan PMK(Clave Maestra Por Partes) [1].

El problema se manifiesta de manera en que las redes inalámbricas radican en la baja seguridad de sus protocolos mismos de encriptación de contraseñas, que son configuradas en los routers inalámbricos, dentro de estos protocolos se producen los ataques maliciosos para obtener una conexión no autorizada a la red con la finalidad de capturar el tráfico de todos los datos sensibles que viajan en el medio por las redes Wi - Fi es aquí en donde se ponen en riesgo la seguridad de la información, influye mucho las claves de WIFI que se demuestran grandes debilidades y ataques en donde aprovechan los ciberdelincuentes para la obtención de datos, donde pueden hacer usos de cualquier manera para beneficios propios y declive de las redes [2].

Puesto qué, los protocolos que manejan las redes de wifi de acceso protegido en la actualidad están siendo vulneradas se tratara de evaluar el estado de la red, por medio de las diversas herramientas de ciberseguridad que nos facilitaran la revisión de las redes Wireless sin tener que hacer procesos en los cuales se involucre los diferentes ataques de fuerzas brutas de tal manera que se pueda llegar a determinar qué tan seguro o inseguro son estos dos diferentes tipos de protocolos y de qué manera se los logra explotar y así de esta manera poder determinar cómo se pueden aplicar seguridades de mayor calidad dentro de las redes y sus protocolos de redes inalámbricas. [1], [2].

La cuestión de las redes Wireless consiste en la baja seguridad de sus protocolos y mecanismos de encriptación, por la implementación de protocolos de cifrado de datos basados en los estándares como IEEE 802.11i que son los más conocidos por que

originalmente se implementaron como (WI-Fi Protected Access) es una de las normas específicas para las redes inalámbricas estas se dan en los protocolos que son WPA y WPA2, son los que proveen el nivel de seguridad un poco más alto por su cifrado de datos mucho mayor y permite la veracidad y autenticación de usuarios [2].

El cifrado de estos protocolos se crea de tal manera que se calcula el SSID y la contraseña del punto de acceso inalámbrico es en este proceso en donde se intercambian las claves del cliente y el AP hacen uso del PSK para conseguir el PMK que es la meta de la mayoría de los ataques maliciosos en las redes que uno mayormente navega sin saber que puede ser vulneradas, acceder y hacer uso de la información propia desde donde conecten los dispositivos al AP. [2]

Existen mecanismos de protección de redes inalámbricas como configuración del protocolo de seguridad de WPA que es para las claves de navegación en donde las redes de Wi – Fi que no garantizan la máxima seguridad en los datos que son transmitidos por estas redes en donde se encuentran los famosos archivos de diccionario que son aplicados por los más comunes ataques de fuerza bruta que son estos métodos utilizados por piratas informáticos para búsqueda de las contraseñas dentro de los sistemas informáticos, en la actualidad ya se cuenta con múltiples técnicas y ataques de phishing han logrado que los ciberdelincuentes y crackers puedan acceder a las claves de encriptación del protocolo WPA2 sin otras herramientas de detentación de claves. [3]

Desde la invención del wifi se han venido presentando al público diferentes tipos de protocolos de seguridad para poder proteger las conexiones en general que rol cumplen los protocolos de seguridad en las redes inalámbricas pues son aquellos que se logran proteger, cifrar datos y el tráfico que viaja por la red mientras estamos conectado a una red inalámbrica, desde 1982 que apareció el primer protocolo de seguridad hasta la actualidad se han hecho públicos 4 diferentes tipos de protocolos en los que encontramos WEP, WPA, WPA2 Y WPA3 cada uno de estos cuenta con diversas características y cualidades, pero con una gran desventaja que cada uno no es lo suficientemente profundo como para garantizar que ningún ciberdelincuente pueda acceder a ella. [3]

Durante las últimas décadas se ha observado una muy buena creciente dependencia de las personas hacia los sistemas informáticos esta gran acogida a generado que una notable evolución en lo que viene siendo el concepto de seguridad y el cuidado de los sistemas

como así de los datos que estos mismos manejan, cada vez se plantean nuevas tecnologías y metodologías que deberían de brindar mayor seguridad y confianza a los sistemas informáticos y así en general poder tener mejores procesos y utilización de recursos para evitar las inseguridades y los diversos tipos de ciberataques que se pueden suscitar se debe hacer uso de tecnologías que cubran con mayor seguridad y robustez todo lo que se tenga relacionado con la penetración ilegal que pueda atentar con la integridad del sistema. [4]

Previo a las investigaciones realizadas se llega a determinar que las redes inalámbricas en general son muy vulnerables que no basta con sus diferentes tipos de protocolos para la seguridad de la información y la encriptación de las claves que se manejan dentro de estas, en su mayoría las señales de wifi están por protocolos de WPA y WPA2, por su supuesta seguridad de encriptación ya sea estas para las redes de área local o las más extensas como las redes de área metropolitana es importante empezar a tener en cuenta que se necesita una seguridad más robusta dentro de estos protocolos y redes Wireless ya que dentro del mundo de la tecnología y la ciberseguridad se busca tener una mayor exigencia en la seguridad de los datos, en la configuración de dispositivos un poco más avanzada, protección de información, etc.

## **1.2 DESCRIPCIÓN DEL PROYECTO**

En las redes inalámbricas del sector cinco esquinas de la provincia de Santa Elena, cuentan con protocolos de cifrado donde se hace presente el tráfico de datos por esta razón se evaluará el estado de la red con una herramienta que toma como nombre Linset, el que hace un examen hacia las redes Wireless que están con los protocolos WPA y WPA2 sin la necesidad de hacer uso de los métodos conocidos como ataque de fuerza bruta o ingeniería social las redes catalogadas como las más inseguras por esta razón, se pretende evaluar las redes en un rango determinado de medio kilómetro de la locación sector cinco esquinas para determinar que amenazas son las que encuentras en los protocolos de seguridad wpa y wpa2, puesto que es fundamental mantener la seguridad de la red por protocolos con pocas debilidades.

El no poder tener el control y conocimiento de quien o quienes están vulnerando nuestros datos de la red hace que seamos víctimas de robos de información, ciberataques e intrusos en el medio que no se puedan identificar por sus actos malintencionados, en consecuencia

de esto se hace un análisis técnico de la red en general, aplicando los conocimientos de protocolos, sistemas de cifrados y más herramientas que ayuden con la identificación de las debilidades de los protocolos estudiados, que posteriormente contribuyan de manera general y se puedan implementar en cualquier contexto.

Para el desarrollo de este proyecto se ha propuesto las siguientes fases [5]:

- **Fase 1: Reconocimiento.**
  - ✓ Investigación minuciosa de los diferentes métodos y herramientas para identificar las vulnerabilidades en las redes inalámbricas.
  - ✓ Se realiza el reconocimiento pasivo y activo, donde se tendrá que identificar la topología de la red que será el objetivo para vulnerar.
- **Fase 2: Escaneo.**
  - ✓ Identificación de los dispositivos conectados que presenta la red Wireless mediante la técnica ping sweep, para poder obtener los activos que se encuentran en la red mediante la herramienta Nmap.
- **Fase 3: Obtener el Acceso.**
  - ✓ Se hace uso de la herramienta Linset que nos permitirá el descifrado de credenciales de una red Wifi mediante el método evil twin attack y el estado de seguridad de los dispositivos.
  - ✓ Se levantarán máquinas virtuales para la recolección de datos y la determinación de veracidad de la información mediante sistemas operativos y sus respectivas configuraciones en algunas distribuciones de Linux como es Kali Linux, Wifislax ya que son S.O enfocados a la seguridad.
  - ✓ El uso de herramientas necesarias como Linset, Aircrack-ng, Nmap que ya se encuentran en los diferentes S.O: Kali Linux y Wifislax.
- **Fase 4: Elaboración de Reporte**
  - ✓ Elaboración de un informe de las herramientas utilizadas para la vulneración de los protocolos y el dispositivo AP.
  - ✓ Presentación de una tabla de las vulnerabilidades que se hayan localizado en el dispositivo por la accesibilidad de los protocolos de seguridad de la red.

## **1.3 OBJETIVOS**

### **1.3.1 OBJETIVO GENERAL**

Elaborar un análisis de las vulnerabilidades de los protocolos de comunicación WPA y WPA2 en una red inalámbrica haciendo uso de técnicas de seguridad Wireless y algoritmos criptográficos.

### **1.3.2 OBJETIVOS ESPECÍFICO**

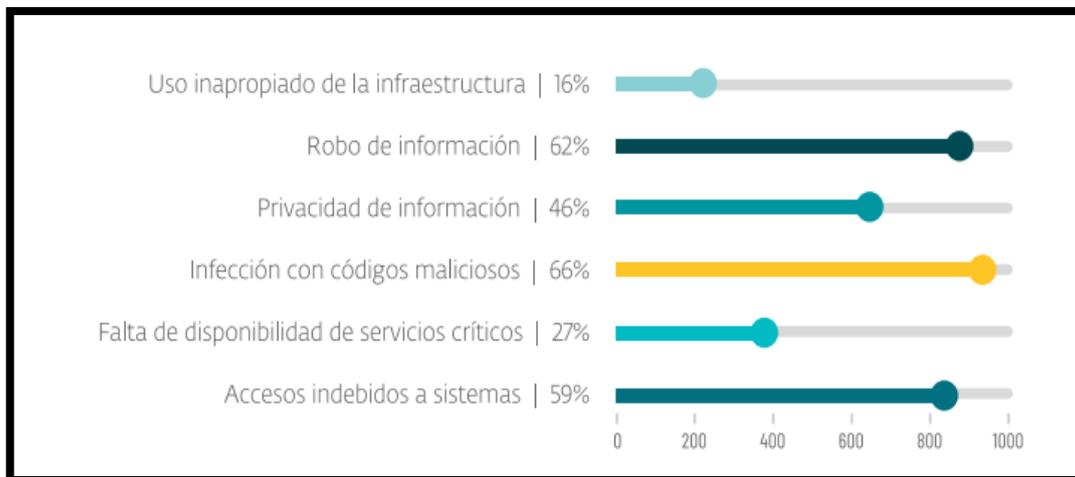
- Implementar un ambiente virtual para obtener los accesos en las redes inalámbricas mediante técnicas de ethical hacking.
- Determinar las vulnerabilidades que se encuentran en las redes Wi – Fi para identificar las amenazas y el nivel de riesgo de los equipos de comunicación.
- Realizar un informe de los resultados obtenidos en el análisis de vulnerabilidades.

## **1.4 JUSTIFICACIÓN**

La seguridad de las redes informáticas es uno de los aspectos más importantes para reducir los riesgos de exposición, datos y servicios que por ella circulan. Es necesario evitar que estos datos sean accedidos por individuos que no son los propietarios de la red o los verdaderos destinatarios. Sin embargo, la mayoría de las personas que utilizan este tipo de redes desconocen o no le dan la importancia que se debería para prevenir los riesgos [6]. La realización de buenas prácticas de análisis de vulnerabilidades en redes inalámbricas se puede llegar a determinar que los protocolos que actualmente se utilizan cuentan con diferentes métodos de ataques para poder obtener información del medio o establecer conexiones maliciosas, la investigación de estos protocolos se realiza con el propósito de establecer una solución para la protección de la información de los datos que se transmitan en las redes Wireless y el no descifrado de sus claves que se encuentran en el mismo medio [7].

El Security Report Latinoamérica (ESET), indica que el robo de información se posiciona como el segundo problema en compañías en toda Latinoamérica. Según estudios que realizó ESET en el año 2021 mediante ataques como el espionaje o robo de archivos confidenciales sus relevancias por amenazas como ransomware, intrusiones por vulnerabilidades, la gran capacidad de incidentes de manera interna que también forma parte a la percepción subjetiva de la ciberseguridad de las compañías en Latinoamérica.

Esto se da por malas configuraciones dentro de sus protocolos de seguridad y de los dispositivos, que causan principales preocupaciones hacia el robo de información [8].



**Figura 1.** Estadística de Security Report Latinoamérica [8].

Este proyecto esta direccionado al desarrollo académico y científico, el estudio ayudara a desarrollar la línea de investigación de seguridad de en redes inalámbricas, que aborda la capacidad de desarrollar soluciones a diferentes problemas de la seguridad de la información con los análisis aplicados a la ciberseguridad. Este proyecto se realizará para la obtención de un análisis detallado de las vulnerabilidades existentes en los protocolos de seguridad esto basado en políticas de seguridad y normativas [6].

En la actualidad los domicilios de la localidad del sector 5 esquinas, Cantón – Santa Elena no se mantiene una correcta verificación de los dispositivos tecnológicos con los que los diversos hogares no tienen un control adecuado ni por parte de la empresa prestadora de servicio ni por el usuario mismo, esto genera que dichos dispositivos estén totalmente expuestos a ataques no basta solo con los protocolos que estos dispositivos llegasen a tener porque las infiltraciones de seguridad a nivel global son muchas, y estas llegándose a atentar con la integridad de los paquetes que circulan por el medio.

La creación del ambiente virtual permitirá detectar las vulnerabilidades en la red y poder verificar con que protocolos cuenta la red ya sean estos los más conocidos como: WPA3, WPA2 Empresa, WPA2 Personal, WPA + TKIP, WEB, Red Abierta mediante esta detección de estos protocolos podemos brindar una mejor seguridad a las redes

inalámbricas de la localidad y de esta manera poder mantener seguro los datos de la red con protocolos de encriptación más seguros.

Lo que corresponde a reportes de acuerdo con el análisis realizado se determina que la información es válida y relevante para una correcta toma de decisiones que ya correspondería por parte de los destinatarios de los dispositivos de la red, en donde se tomen medidas correctivas con respecto a las amenazas detectadas que se pudieron encontrar aplicando los diferentes métodos de obtención de acceso.

El presente proyecto esta direccionado al Plan De Creación De Oportunidades, haciendo énfasis en los ejes que se redacta lo siguiente [9]:

### **Eje 2: Eje Social**

**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 7:** Potenciar las capacidades de la ciudadanía y promover una educación innovadora, inclusiva y de calidad en todos los niveles.

**Política 7.2:** Promover la modernización y eficiencia del modelo educativo por medio de la innovación y el uso de herramientas tecnológicas.

### **Eje 3: Eje Seguridad Integral**

**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**

La implementación del ambiente virtualizado permitirá analizar las redes inalámbricas que se encuentren en el rango de medio kilómetro de la localidad específica para el análisis la investigación toma como referencia el sector 5 esquinas del cantón santa elena

con la finalidad de identificar las amenazas que vulneren la seguridad de los protocolos WPA/WPA2 en las redes inalámbricas.

Mediante se vaya evaluando la red dentro de todo el proceso se hará uso del método de hacking de caja blanca (White box hacking), mediante este método podemos hacer uso de diversos escenarios donde se pueden hacer manipulación de los datos, obtener acceso a credenciales, IP's, servicios, etc. El proyecto está enfocado a un ambiente controlado por esta razón este tipo de método nos será factible.

Además, se hará uso de varias técnicas que nos permitirán vulnerar los protocolos para poder realizar el descifrado del password de la red, la técnica de observación nos permitirá recopilar información del diseño de la red y que sus componentes físicos del contexto que se está proponiendo al igual que los hechos o casos que sucedan, esto se realiza con la finalidad de llevarlo a un posterior análisis. Otras de las técnicas utilizadas es la recopilación documental o bibliográfica que nos permite obtener información mediante fuentes directas y veraces que son relacionado a los temas con hechos pasados y comprobados en ambientes de producción.

La técnica ping sweep nos permitirá realizar un barrido de los pings que se encuentren en nuestra red, específicamente nos permitirá evidenciar cuantos dispositivos son los que se encuentran en la red, esto se da en conjunto con herramientas que son destinadas para el escaneo de los pings que nos proporciona, la herramienta que permite trabajar en conjunto toma como nombre Nmap que ya viene incluida dentro del sistema operativo Kali Linux.

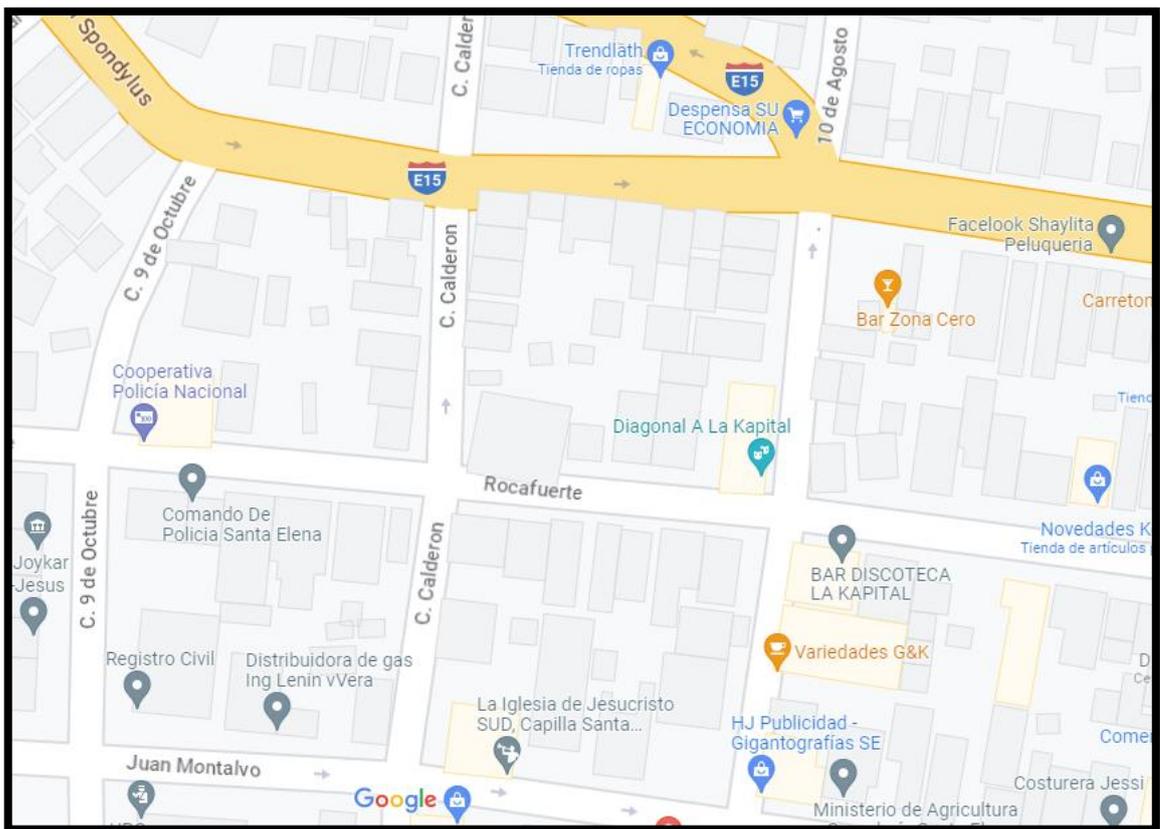
Otras de las técnicas que nos permitirá efectuar el ataque a los protocolos es Evil Twin Attack, el ataque de gemelo malvado este tipo de ataque es el que nos permitirá crear un punto de acceso falso, pero son las mismas similitudes de la red original para poder obtener acceso, esto se logra mediante el conjunto de dos herramientas que están destinadas para el mismo propósito estas son Linset y Wpa estas herramientas nos permitirán ejecutar este tipo de técnica.

Para la finalización del proceso, se presentará un informe a manera de tablas con todos los resultados obtenidos donde se podrán evidenciar las herramientas, tiempos de ejecución, software utilizado y equipos de hardware utilizados para este ambiente virtual creado y adaptado para el proyecto.

## CAPÍTULO 2

### 2.1 MARCO CONTEXTUAL

Las pruebas que se realizarán serán llevadas a cabo en un ambiente virtual controlado en la localidad del sector 5 esquinas, están ubicado específicamente en las calles calderón y Rocafuerte a una cuadra del comando policial de la provincia de Santa Elena - Cantón Santa Elena. Donde se realizarán el estudio y vulnerabilidades de los protocolos de seguridad.



**Figura 2.** Localidad donde se desarrollará el proyecto

### 2.2 MARCO CONCEPTUAL

**Handshake:** El handshake es un procedimiento de autenticación por medio del cual un cliente puede verificar que está recibiendo los datos del servidor web correcto se tiene algunas responsabilidades principales [10].

**Autenticar al servidor:** lo que se hace es que el navegador web de una cliente tiene mecanismos para verificar que los mensajes que se recibe llegan al servidor del sitio web o no de un hombre en el medio [10].

**Intercambio de claves:** después de autenticar la identidad del servidor web lo que procede a realizar el navegador establece una clave común con el servidor que se lo pide de manera secreta y no puede ser conocida por un tercero malicioso, ya que solo se encuentran en los extremos de la comunicación [10].

La manera de cómo se puede describir todo lo que sucede es mediante el cambio de las claves criptográficas, que se realiza para que se pueda asentar una comunicación de manera cifrada de forma simétrica entre el servidor y el navegador del usuario

**Desautenticación mdk3:** MDK3 es una herramienta usada para la seguridad Wireless que usualmente viene pre-empaquetada en distros como Kali\_Linux y la difunta Backtrack, no estoy seguro de si es posible instalarla vía repositorios, pero es posible descargar el tarball, este programa tiene una gran cantidad de opciones que permiten su uso de una forma flexible, esta aplicación saca ventaja de vulnerabilidades en el estándar 802.11 y debe ser usada solamente para pruebas de seguridad en un laboratorio propio con fines educativos [11].

**Firewall:** Es conocido de igual manera como cortafuegos es un dispositivo de seguridad de red que supervisa el tráfico de red entrante y saliente, decide si permite o bloquea tráfico específicos en función de un conjunto definido de reglas de seguridad [12].

Un firewall puede ser hardware, software, software como el servicio (SaaS), nube publica o nube privada (Virtual) [12].

**CCMP:** Es un protocolo de encriptación de IEEE Counter Mode With ipher block chaining Message Authentication Code Protocol (Modo de contador con protocolo de código de mensajes de encadenamiento de bloques cifrados), este fue creado para remplazar al TKIP que es uno de los protocolos infaltable en el WPA, tambien emplea algoritmos de seguridad como el AES [13].

**RogueAp:** Un rogue access point es cualquier punto de acceso inalámbrico que se encuentre dentro del alcance de la red y que no se reconoce como un punto de acceso autorizado, ni como una excepción configurada en la implementación inalámbrica un rogue access point puede ser un AP no autorizado conectado a su red por alguien dentro de su organización sin consentimiento [14].

Estos puntos de acceso son riesgos de seguridad para las redes inalámbricas y cableadas si no tienen las características de seguridad apropiadas habilitadas, además un rogue

access point puede ser un AP externo a su red inalámbrica que se encuentra dentro del rango de su red esto incluye los rogue access points Honeypot o Evil Twin que suplantan AP legítimos al difundir el mismo SSID de la red que sus AP autorizados [14].

**Hostapd:** Es un autenticador de IEEE 802.11 AP y IEEE 802.1X/WPA/WPA2/EAP/RADIUS lo que realiza es que el administra la tramas que requiere una interfaz en modo monitor, es aquí en donde se necesitaba de una interfaz corriendo en modo máster para el tráfico de datos, la autenticación, claves de administración, etc. [15].

**Aircrack-ng:** Es una suite de software de seguridad inalámbrica, que consiste en una seguridad inalámbrica para los paquetes de las redes, la función que cumple es recuperar contraseñas WEP y WPA/WPA2-PSK y diversos conjuntos de auditoria inalámbrica [16]. Su principal objetivo es la supervisión, ataque, prueba, craqueo de protocolos, en su mayoría de herramientas son de línea de comando, es lo que permite secuencias de comandos pesados, pero tambien vine me manera de interfaz dentro de otras herramientas que se dispone [16].

**DHCP:** El Protocolo de configuración dinámica de host (DHCP) es un protocolo cliente/servidor que proporciona automáticamente un host de Protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace predeterminada. Las RFC 2131 y 2132 definen DHCP como un estándar de Internet Engineering Task Force (IETF) basado en el Protocolo de arranque (BOOTP), un protocolo con el que DHCP comparte muchos detalles de implementación, DHCP permite a los hosts obtener la información de configuración de TCP/IP necesaria de un servidor DHCP [17].

**802.11x:** 802.11x es un término genérico para referirse al estándar IEEE 802.11 para definir la comunicación a través de una LAN inalámbrica (WLAN), 802.11 comúnmente conocido como Wi-Fi, especifica una interfaz inalámbrica entre un cliente inalámbrico y una estación base o entre dos clientes inalámbricos estos estándares se utilizan para implementar la comunicación WLAN en bandas de frecuencia de 2.4, 3.6 y 5 GHz [18].

**Redes Wireless:** Una red inalámbrica, por lo tanto, es aquella que permite conectar diversos nodos sin utilizar una conexión física, sino estableciendo la comunicación

mediante ondas electromagnéticas la transmisión y la recepción de los datos requieren de dispositivos que actúan como puertos [19].

Las redes inalámbricas permiten establecer vínculos entre computadoras y otros equipos informáticos sin necesidad de instalar un cableado, lo que supone una mayor comodidad y un ahorro de dinero en infraestructura [19].

Además de lo expuesto, tendríamos que señalar otra serie importante de ventajas que presenta cualquier red inalámbrica [19]:

- Es muy sencilla de instalar. Y es que, como hemos mencionado anteriormente, no lleva cableado por lo que se evita tener que ir realizando agujeros en las paredes para poder pasar aquel [19].
- Se convierte en una instalación más elegante precisamente porque no requiere tener cables por todas partes. De esta manera, se garantiza que en absoluto se perjudicará el estilo o la apariencia que tenga la estancia donde se ponga en funcionamiento [19].
- Permite que puedan estar interconectados un importante número de dispositivos, tanto ordenadores como tablets, teléfonos móviles, periféricos como impresoras [19].

Como punto negativo, este tipo de redes suele contar con una seguridad menor ya que, si no se cuenta con una protección eficiente, el ingreso de intrusos es muy probable [19].

**Protocolos:** La finalidad del protocolo informático es permitir que funcione lo que conocemos con la internet moderna es él encargado de permitir que diferentes computadoras sean capaces de comunicarse a través de las redes. Tiene el fin de evitar que los usuarios tengan que conocer las operaciones que ocurren en segundo plano a través del protocolo los dispositivos pueden comprender las señales electrónicas enviadas por medio de las conexiones de red [20].

**PSK:** Está diseñado para redes en hogares y oficinas pequeñas donde cada usuario tiene la misma frase contraseña. "WPA-PSK" también se conoce como "WPA-Personal" o "WPA-PSK" habilita la máquina inalámbrica hermana para asociarse con puntos de acceso utilizando el método de codificación "TKIP" o "AES", "WPA2-PSK" habilita la máquina inalámbrica hermana para asociarse con puntos de acceso utilizando el método de codificación "AES" [21].

**PMK:** Es una llave que se genera de forma secreta compartida que toma como nombre (PMK), se genera desde una contraseña que es establecida a través de una función Hash específicamente PBKDF-SHA1, que es un sistema de PSK y la PMK es realmente la misma PSK seteada por el usuario [22].

### 2.2.1 MÉTODOS O MECANISMOS DE SEGURIDAD

- SSID (Service Set Identifier): Consiste en que el cliente debe tener configurado el mismo SSID que el Access Point [23].
- WEP (Wired Equivalet Piracy): Tiene como objetivo principal proveer la confidencialidad de la transmisión de la información [23].
- Filtrado por dirección MAC: El Access Point está configurado para aceptar solo las peticiones de ciertos nodos de la red [23].
- WAP (Wi-Fi Protected Access): distribuye claves diferentes a cada usuario para mejorar la integridad de la información, al igual que WEP, los usuarios mal intencionados pueden obtener su clave, otras de las desventajas son que, al tener una contraseña de al menos veinte caracteres, la cual es muy complicada que los usuarios recuerden [23].

**Tabla 1**

Servicios Básicos de la seguridad en las redes inalámbricas

Servicios básicos de seguridad	Descripción
<b>Autenticación</b>	Provee servicios de seguridad para verificar la identidad entre las estaciones clientes que se comunican. Esto provee control de acceso a la red denegando acceso a las estaciones clientes que no pueden ser autenticadas propiamente.
<b>Confidencialidad</b>	Provee privacidad lograda por una red cableada. Lo que pretende es prevenir el compromiso de la información de un ataque pasivo.
<b>Integridad</b>	Este servicio asegura que los mensajes no son modificados en el tránsito entre los clientes

Nota: Información de la investigación realizada por Autor [23].

### 2.2.2 VENTAJAS DE LAS REDES INALÁMBRICAS

Los autores Carlos Varela y Luis Domínguez, establecen que estas son ventajas que contienen las redes inalámbricas para poder ser catalogadas como medianamente seguras, puesto que son redes que contiene baja fiabilidad de seguridad en este punto se darán a conocer sus mejores características. Las redes WLAN (red de área local inalámbrica) llegan a ser muy buenas y eficientes en diversas áreas donde estas sean configuradas y de qué manera vayan a hacer utilizadas para sacar le mejor rendimiento de este tipo de red [24].

- **Flexibilidad:** Dentro de una zona de cobertura de una red inalámbrica los nodos o puntos de acceso Ap se pueden comunicar y no es necesario de ningún tipo de cable para su comunicación [24].
- **Poca planificación:** En el caso de redes inalámbricas solo se enfocaría en que la cobertura de la red llegue a los espacios donde se requieren ya sean estas oficinas, residenciales, etc. De lo contrario para redes cableadas o guiadas se debe tener una planificación y ubicación de los dispositivos y máquinas para su comunicación [24].
- **Diseño:** La mayoría de los dispositivos conocidos como receptores son pequeños y son de fácil manipulación [24].
- **Robustez:** Una red inalámbrica puede llegar a soportar alcances inesperados sin la necesidad de llegar a ocurrir grandes daños todo lo contrario, a lo que es las redes guiadas que es donde sucesos inesperados empeoran toda la infraestructura de la red [24].

### 2.2.3 INCONVENIENTES DE LAS REDES INALÁMBRICAS

- **Calidad de Servicio:** se podría decir que las redes cableadas cuentan con mayor calidad de servicio a comparación con las inalámbricas que tiene un bajo potencial en los Mbps que se transmiten [24].
- **Coste:** En la actualidad se siguen tratando de bajar los costes de los materiales que se ocupan para red cableada, sigue siendo un desafío mientras que para redes

inalámbricas es mucho más económico y accesible y mucho más si es a manera de hogar que la estandarización y coste es menos [24].

- **Restricciones:** este tipo de redes inalámbricas operan actualmente en un trozo del espectro radioeléctrico, que hoy en día está muy quemado esto quiere decir que las redes deben amoldarse a las reglas de cada país [24].
- **Seguridad:** La seguridad e integridad de la mayor parte de información es muy crítica dentro de todos los estándares que se presentan hasta la actualidad para la protección de la información, la tentativa de robo puede ser algo muy delicado y peligroso, la interferencia con otro tipo de redes de comunicación es un problema grave si es que no se tiene con los mínimos protocolos de seguridad hay que tenerlo en cuenta a la hora del diseño [24].

#### 2.2.4 OBTENCIÓN DE CLAVES EN REDES WLAN CON WIFISLAX

- Este sistema operativo que cuenta con distribución Gnu/Linux está basada en Slackware y especializada en auditoria de redes inalámbricas y cuenta con diversas herramientas de gestión y uso cotidiano. En su mayoría las herramientas de auditorías de ataques a los protocolos de seguridad y encriptación de router se enfoca en unos de los alojamientos de Aircrack-ng que nos permite hacer uso de sus lanzadores gráficos que corresponden al modo monitor, sniffer de redes wireless y al correcto análisis de claves wireless [25].
- Aircrack-ng es uno de los programas crackeadores de las claves del estándar 802.11 WEP y WPA/WPA2, cumple con recuperar las claves una vez tenga los suficiente paquetes encriptados. Este programa del alojamiento de Aircrack-ng cuenta con varios tipos de ataques para descifrar claves con la cantidad mínima de paquetes que encuentre y capture, en ocasiones realiza combinaciones de ataques estadísticos con los conocidos ataque de fuerza bruta [26].
- En su vista de monitor cuenta con cuatro columnas muy importantes en las que tenemos Keybyte, Depth, Byte, Vote [26].

**Tabla 2**  
Vista monitor de Aircrack.ng

ENUNCIADO	DESCRIPCIÓN
<b>KB</b>	El número de cada uno de los bytes o caracteres calves.
<b>DEPTH</b>	Profundidad de la actual búsqueda de clave.
<b>BYTE</b>	Byte o carácter que está probando.
<b>VOTE</b>	votos o números que probabilidades de que sea correcto.

Nota: Información de la investigación realizada por Autor [26].

### 2.2.5 SISTEMAS OPERATIVOS UTILIZADOS PARA AUDITORÍA DE REDES INALÁMBRICAS Y HERRAMIENTAS

#### **Wifislax**

Es una distribución GNU/Linux en formato .iso basada en Slackware con funcionalidades de LiveCD y LiveUSB pensada y diseñada para la auditoria de seguridad y relacionada con la seguridad informática. Este Sistema Operativo incluye con una larga lista de herramientas de seguridad y auditorias listas para ser utilizadas, entre las que destacan numerosos escáneres de puertos y vulnerabilidades, herramientas para la creación y diseño de exploits, sniffers, herramientas de análisis forense y herramienta para auditoria inalámbrica [27].

#### **Kali Linux**

Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoria y seguridad informática en general, fundada y mantenida por Offensive Security Ltd, Mati Aharoni y Devon Keams, ambos pertenecientes al equipo de Offensive Security.

Hoy en día la cantidad de herramientas o scripts existentes, que realizan tareas similares, el universo de herramientas es enorme por lo tanto es bueno mantener un repositorio, de

herramientas para pruebas de penetración actualizado. Kali Linux, mantiene una relación estrecha con los repositorios de Debian GNU/Linux por lo que reciben actualizaciones de seguridad tan frecuentemente [28].

### **Forensics Mode en Kali Linux**

Se introdujo la opción Forensics Boot al sistema operativo y se vio continuada en **Back Track5** que en la actualidad ya es conocida como Kali Linux, que sirve para poder trabajar las herramientas de software libre populares en materia forense de forma rápida y sencilla. Kali cuenta con el software libre forense más popular instalado por que es rápido y sencillo de bootear [28].

El conocido antes como **Back Track5** que es uno de los Sistemas Operativos con versiones anteriores cuenta con una variedad de herramientas que favorecen a las buenas prácticas forenses, Herramientas como: Aircrack-ng (herramienta para auditoria inalámbrica), Kismet (Sniffer inalámbrico), Wireshark (analizador de protocolos), Medusa (ataque de fuerza bruta) [29].

### **Que es linset**

Linset es una utilidad de origen español que sirve para auditar y acceder a las claves de redes inalámbricas utilizando la técnica como Evil Twin Attack en la que es la propia víctima la que nos proporciona la contraseña de acceso, cabe mencionar que hay muchas maneras de poder conseguir las claves de las redes inalámbricas o Wireless que se encuentras en nuestro alrededor, pero el método usado por linset es uno de los más efectivos a la hora de su ejecución ya que supera ampliamente a las demás herramientas similares sin tener que ocurrir a diccionario de fuerza bruta o demás métodos [30].

La funcionalidad de linset es prácticamente sencilla lo que hace es crear un clon de la página de acceso al router (Interfaz), donde el propio usuario es que nos proporcionara la clave de acceso tras haber lanzado un ataque DoS, que prácticamente es el que lo obliga a ingresar nuevamente las credenciales para conectarse de nuevo en tiempo muy corto [30].

### **Funcionamiento de linset**

- ✓ Escanea la red
- ✓ Selecciona la red

- ✓ Busca handshake – se puede usar sin un handshake
- ✓ Se elige una de las varias interfaces web, son adaptaciones para el usuario de red.
- ✓ Se monta un FakeAP imitando la original
- ✓ Se crea un servidor DHCP sobre el FakeAP
- ✓ Se crea un servidor DNS para redirigir las peticiones al host
- ✓ Se lanza el mecanismo para comprobar la validez de las contraseñas que se van a introducir
- ✓ Se desautentifica a todos los usuarios de la red, esperando que se conecten al FakeAP (Fake Access Point) y que introduzcan la contraseña posteriormente
- ✓ Se detiene el ataque tras la comprobación correcta de la contraseña.

### Evil twin attack

El ataque de gemelo malvado es un ciber ataque de suplantación de identidad que funciona engañando a los usuarios para que se conecten a un punto de acceso rápido WIFI (Falso), que imita o simula una red legítima, una vez que un usuario está conectado a una red de Gemelos Malvados, se puede acceder a todo desde el tráfico de la red las credenciales de inicio de sesión privadas. Estos tipos de ataques tienen la capacidad de imitar redes WIFI. Al punto que son indistinguibles entre sí, este tipo de ataque es casi imposible de identificar y el ataque suele ser lo más creíble posible. Este tipo de ataque si representa un riesgo significativo para la seguridad cibernética y para los usuarios finales, empresas [31].

### 2.2.6 COMPARACIÓN DE LOS PROTOCOLOS DE ENCRIPCIÓN

**Tabla 3**  
Protocolos WPA vs WPA2 diferencias

	WPA	WPA2
<b>Año de publicación</b>	2003	2004
<b>Método de encriptación</b>	Temporal key integrity protocol (TKIP).	Advanced encryption standard (AES).
<b>Seguridad</b>	Más fuerte que una WEP, seguridad básica.	Más fuerte que una WPA, seguridad avanzada.
<b>Soporte de dispositivo</b>	Funciona en software antiguo	Funciona con software nuevo

<b>Longitud de la contraseña</b>	Contraseña corta	Contraseña larga
<b>Uso en las empresas</b>	Si solución profesional	Incluye solución profesional
<b>Procesamiento</b>	Mínima	Gran parte

Nota: Tabla de comparación entre protocolos, según diseño de investigación [32].

## 2.2.7 PUNTOS CRÍTICOS EN REDES INALAMBRICAS

**Tabla 4**  
Puntos Críticos y Detalles

Puntos Críticos	Detalles
<b>Denegación de Servicio (DoS)</b>	Se trata de incapacitar la red inalámbrica a través de peticiones de servicios masivas a los puntos de accesos, busca sobrecargar el punto de acceso o router para no hacer uso de los servicios que este presta.
<b>Hombre en el medio (Man in the middle)</b>	Es donde el atacante puede situarse entre el emisor y el receptor, suplantando el destinatario de la comunicación.
<b>Ataques de Fuerza Bruta</b>	Este es uno de los métodos que consiste en hacer uso de todas las contraseñas posibles, con la finalidad de conseguir las claves criptográficas.
<b>Escuchar a Escondidas (Eavesdropping)</b>	Es donde se captura el tráfico de red que no es autorizada y se da mediante antenas de gran alcance o dispositivos con estándares.
<b>Suplantación de Mac (MAC Spoofing)</b>	Se trata de suplantar la dirección MAC de un dispositivo.

Nota: Puntos críticos en redes inalámbricas, según diseño de investigación [33].

## 2.2.8 BARRERAS DE PROTECCIÓN EN LAS REDES INALAMBRICAS

**Tabla 5**

Barreras de protección en las redes inalámbricas

<b>SSID identificador de servicio – una contraseña</b>
<b>Filtrado de direcciones MAC</b>
<b>WEP (Privacidad Equivalente por cable)</b>
<b>Estándares IEEE</b>
<b>Protocolo WPA</b>
<b>Configuración del router</b>
<b>Cambios de las claves por defecto del dispositivo</b>
<b>Antivirus, Firewall, Antispyware</b>
<b>Puntos de Acceso</b>

Nota: Barrera de protección en redes inalámbricas de área local Wlan [34].

## 2.2.9 TERMINOS FRECUENTES EN EL ESCANEEO DE OBJETOS

**Tabla 6**

Descripción de terminologías aplicadas en las herramientas

<b>Opción</b>	<b>Descripción</b>
<b>BSSID</b>	Dirección MAC del punto de acceso
<b>PWR</b>	Nivel de señal que es detectado por la tarjeta USB, funciona de tal forma que cuanto más cerca este del punto de acceso la señal aumentara.
<b>Beacons</b>	Es el número de paquetes -anuncios que se envían por el AP, siempre se envían unos 10 beacons por cada minuto, por lo general es recogido desde lejos.
<b>#Data</b>	Es el número de paquetes capturados.
<b>CH</b>	Es el número de canal por el cual viajan los paquetes, se suele chocar con los paquetes de datos que se suelen alternar debido a la interferencia de la radiofrecuencia.
<b>ENC</b>	Algoritmo de encriptación en uso pueden ser WEP, WPA, WPA2, cuando no se muestra nada suele ser que es WEP estática o dinamina
<b>CIPHER</b>	Es un cifrado o conocido como protocolo de código de autenticación de mensaje

<b>AUTH</b>	Muestra de igual manera que en el ENC, protocolos en esta parte pueden aparecer los protocolos PSK o TKIP son los que están.
<b>ESSID</b>	Se la conoce también como SSID, suele no aparecer en la interfaz por si la red esta es modo oculta.
<b>STATION</b>	Es la dirección MAC de cada estación asociada.
<b>Rate</b>	Es solo como un índice.
<b>Lost</b>	Se los puede tomar como paquetes perdidos dentro de la red.
<b>Frames</b>	Son marcos que sirven para dividir páginas web en ventanas más chicas.
<b>Probe</b>	Es donde se detecta el nombre de la red, para poder tener acceso a la misma.

Nota: Términos que aparecen en las herramientas, según diseño de investigación [35].

## 2.3 MARCO LEGAL

### 2.3.1 LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

La ley orgánica de protección de datos personales en Ecuador establece los siguientes artículos con relación al tema de investigación propuesto [36].

**Art. 3.-** Ámbito de aplicación territorial. – sin perjuicio de la normativa establecida en los instrumentos internacionales ratificados por el estado ecuatoriano que verse sobre esta metería, se aplicara la presente ley cuando:

1. El tratamiento de datos personales se realice en cualquier parte del territorio ecuatoriano.
2. El responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional.

**Art. 4.-** Términos y definiciones. – Para los afectados de la aplicación de la presente Ley se establecen las siguientes definiciones:

**Autoridad de Protección De Datos Personales:** Autoridad pública independiente encargada de supervisar la aplicación de la presente ley, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, cuando al tratamiento de sus datos personales.

**Consentimiento:** Manifestación de la voluntad libre, especificada, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos.

**Delegado de protección de datos:** Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la autoridad de protección de datos personales.

**Art. 10.- Principios.** – Sin perjuicio de otros principios establecidos en la constitución de la república, los instrumentos internacionales ratificados por el estado u otras normas jurídicas, la presente Ley se regirá por los principios de:

- a) **Juridicidad.** – los datos personales deben tratarse con estricto apego al cumplimiento a los principios, derechos y obligaciones establecidas en la constitución, los instrumentos internacionales, la presente ley, su reglamento y las demás normativas y jurisprudencia aplicable.
- b) **Lealtad.** – El tratamiento de datos personales deberá ser leal, por los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernan, así como las formas en que dichos datos son o serán tratados.
- e) **Pertinencia y minimización de datos personales.** – Los datos personales deben ser pertinentes y estar a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento.
- j) **Seguridad de datos personales.** – los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas 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.

**Art. 17.- Derecho a la portabilidad.** – El titular tiene el derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características; o a

transmitirlos a otros responsables. La autoridad de protección de datos personales deberá dictar la normativa para el ejercicio del derecho a la portabilidad.

## **2.4 MARCO TEÓRICO**

### **2.4.1 ¿QUE ES EL HACKING ÉTICO Y PARA QUE SIRVE?**

El hacking ético se realiza para poder atrapar a un intruso como uno de sus principales puntos, bajo esta premisa se puede decir que el hacking ético a medida que pasa el tiempo se vuelve mucho más demandado por razones de protección de infraestructura de la red, sistemas de información y aplicaciones que se vuelven susceptibles de ser atacadas es por esto que la protección de estos activos se puede volver crítico [37].

El hacking ético o ethical hacking es unos de los grandes métodos probados por diversos profesionales para el aseguramiento de los sistemas de información o protección de redes donde se ve involucrado las telecomunicaciones todo esto se converge en la protección contra ataques, donde se pueden detectar vulnerabilidades que tan solo con poco tiempos estas pueden ser explotadas el labor fundamental del hacking es poder disminuir el riesgo de perdidas en infraestructuras y sistemas de información [37].

### **2.4.2 DETECCIÓN DE VULNERABILIDADES**

Puesto que la mayoría de las empresas, hogares y personas no comprende y desconoces las medidas de seguridad que son necesarias y que se deben utilizar en cada uno de los contextos, es por esta razón que recurren a personas con el conocimiento dentro de este campo para poder tener mejores servicios de escogimiento a las mejores soluciones que se puedan presentar o detectar dentro del campo [38].

Para poder comprender de mejor manera de cómo es que funciona y que es lo que permite una red inalámbrica es importante saber para qué sirve, las redes inalámbricas o también conocidas como redes wireless son las que nos permiten compartir recursos o servicios a través de la red que estemos enganchados, de la misma manera nos permite conectar computadoras para poder enviar y transmitir datos entre sí, esta cuenta con características de poder conectarse a redes existentes inalámbricas mismas [38].

### **2.4.3 ¿QUE ES LA CIBERSEGURIDAD?**

La ciberseguridad definida así por ISACA asociación de auditoría y control de sistemas de información, estipula que la ciberseguridad tiene du implementación para la protección

de acticos de información, a través de control de amenazas que pone en riesgo la información procesada, almacenada y transportada por sistemas de información que están interconectados para la comunicación [39]. La ciberseguridad es el conjunto de herramientas, métodos, medidas de seguridad, políticas, enfoques de gestión de riesgos, mejores prácticas, protección y garantías tecnológicas para la protección de ambientes cibernéticos. Sirve para la protección y control interno del ciberespacio en un ámbito global [40].

#### 2.4.4 TIPOS DE ESTANDARES PARA LAS REDES INALMBRICAS

La normalización IEEE para las WLAN, especializada en la norma 802 fue desarrollada por el instituto de ingenieros eléctricos IEEE, y está basada en la arquitectura de redes de datos LAN (Local Área Network). Esta norma establece que un estándar de tecnología en el mercado mundial garantizando que los productos compatibles con la norma 802 sean también compatibles entre sí. La norma contiene varios apartados que se los describirá más adelante, cada una de estas normas de comunicación de datos cumple con una función en específico [41].

**Tabla 7**  
Normas de tecnología

Normas	Descripción
802.1	Define las primitivas de interfaz, para la interconexión de redes.
802.2	Describe la parte superior de la capa de enlace que utiliza el protocolo LLC.
802.3	Describe normas CSMA/CD.
802.4	Describe las normas token bus.
802.5	Describen las normas token ring.
802.6	Red de área metropolitana.
802.7	Grupo asesor para técnicas de banda ancha.
802.8	Grupo asesor para técnicas de fibra óptica.
802.9	Redes integradas para voz y datos.

<b>802.10</b>	Seguridad de red en la comunicación de datos.
<b>802.11</b>	Redes inalámbricas, especifica una interface inalámbrica para comunicaciones de datos compatibles con la norma IEEE 802.

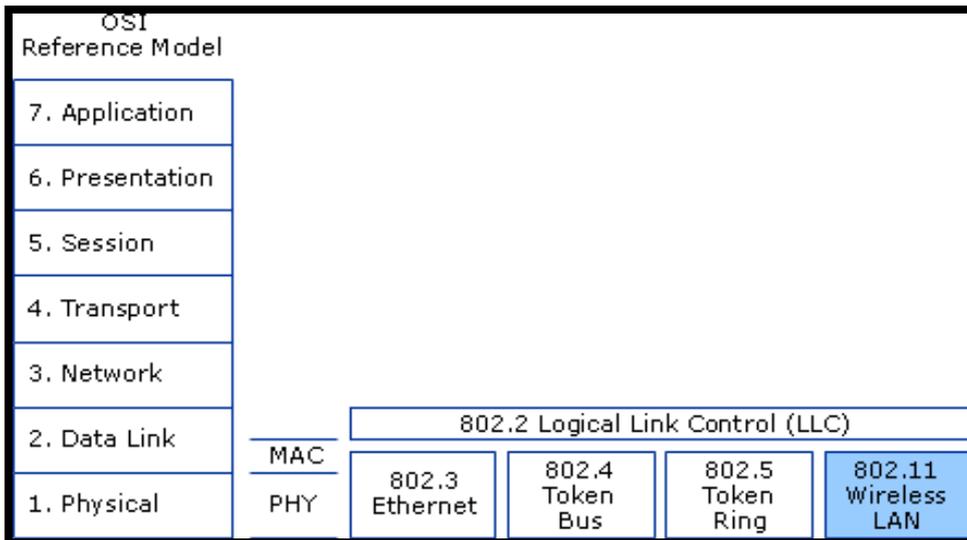
Nota: Tabla general de las normas estandarizadas, según diseño de investigación [41].

#### 2.4.5 ESTANDAR 802.11

Los estándares WLAN 802.11 especifican y están más dirigidas a las dos capas más bajas del modelo de red OSI que son las capas físicas y enlace de datos, cumplen con los principales objetivos de IEEE para crear estos estándares se realizó un acercamiento a la capa física donde se alojan las diferentes frecuencias, diferentes métodos de codificación y comparten sus mismas capas superiores [42].

Las capas de control de acceso al medio (MAC) de los protocolos 802.11 a, b, g son considerablemente idénticas, en la capa inmediatamente superior todos los protocolos WLAN 802.11 especifican el protocolo 802.2 (LLC) de la capa de enlace de datos. En las WLAN la privacidad se logra mediante el contenido de datos en manera de protección de encriptación. En el estándar 802.11 la encriptación es opcional, pero lo importante esta que sin este estándar cualquier otro dispositivo inalámbrico puede leer todo el tráfico de la red, los mayores enfoques en las generaciones de seguridad son [42]:

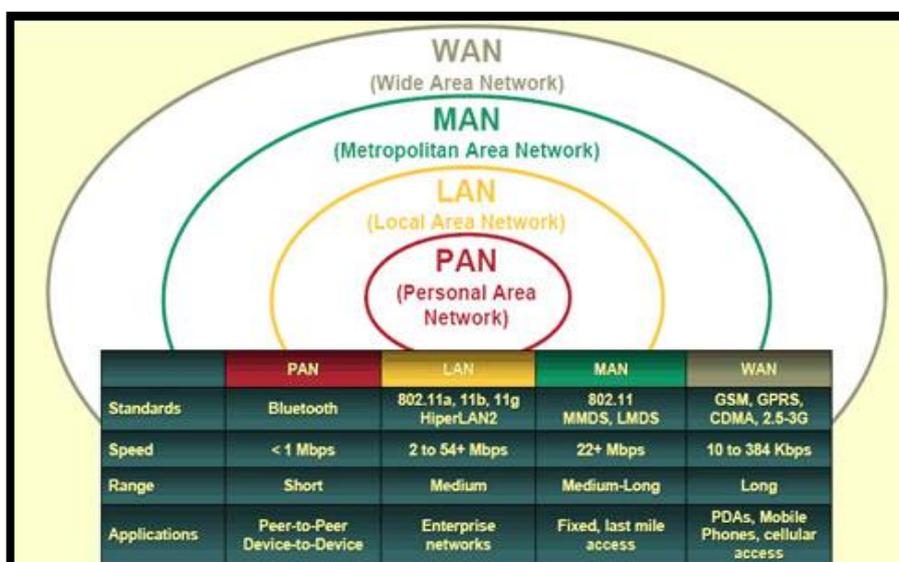
- **WEP** (Privacidad equivalente por cable) [42].
- **WAP** (Acceso protegido WIFI) [42].
- **WPA2/802.11i** (Acceso protegido WIFI, versión 2) [42].



**Figura 3.** Aplicación del estándar 802.11 [42].

#### 2.4.6 TIPOS DE REDES INALAMBRICAS

Las redes inalámbricas comparten diversas ventajas que son importantes esto es indistinto de cómo se diseñen los diversos protocolos o del tipo de dato que transporten, lo más importante de las redes inalámbricas es la movilidad que esta nos proporciona los usuarios de este tipo de redes pueden conectarse a redes existentes y posteriormente trabajar libremente. Las redes inalámbricas liberan a los desarrolladores de software con la otra manera de poner tener conectividad mediante cable ethernet, los usuarios que hacen uso de redes inalámbrica tendrán acceso siempre y cuando se encuentre dentro del rango permitido por la red [43].

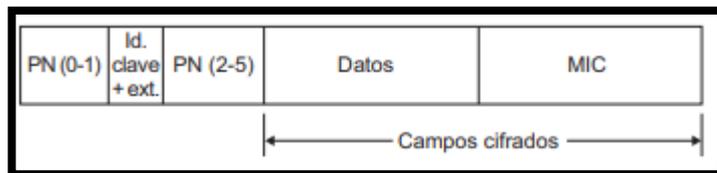


**Figura 4.** Clasificación de las redes inalámbricas [43].

### 2.4.7 ESQUEMAS DE LOS PROTOCOLOS WPA Y WPA2

Este tipo de estándar se ha mantenido en cambio constante esto se da mediante el método de autenticación de la estación así mismo como el algoritmo de cifrado de las tramas. Este protocolo hace uso de una clave única compartida entre el AP y las demás estaciones tiene similitud con otro tipo de protocolos esta clave única se apropia de la red inalámbrica doméstica, es importante conocer si el atacante llega a tener acceso con alguna estación puede ser un riesgo grande [44].

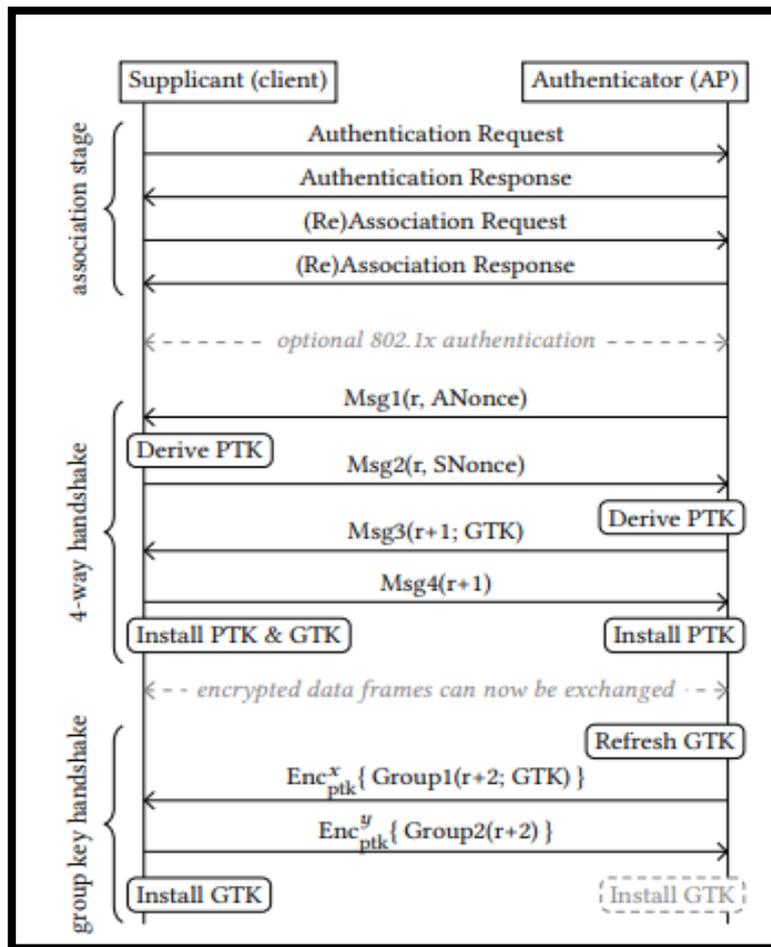
El estándar IEEE 802.1x es el que permite el intercambio seguro de claves entre dos nodos de la red, la autenticación tiene que ser mutua entre los dispositivos para que el AP sea autenticado mediante la estación principal y de esta manera se asegura que no se esté hablando con un AP ficticio. Dentro del protocolo WPA2 se ve involucrado el estándar IEEE 802.11i, ya que tiene mecanismos de preautenticación y el almacenamiento de llaves maestras PMK lo que hace que la reautenticación se realice de manera más rápida estos protocolos tienen que soportar el cifrado CCMP [44].



**Figura 5.** Cifrado del protocolo CCMP [44]

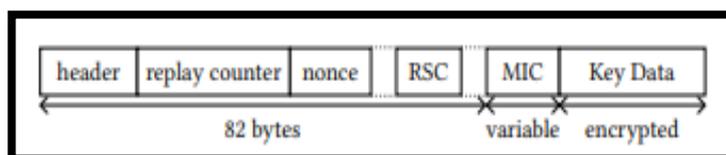
### 2.4.8 ATAQUES DE CLAVES WPA Y WPA2

A continuación, se mostrará el gráfico de los intercambios cuando un cliente se enlaza con un AP, en este proceso se realiza la captura de un handshake y esto se ejecuta periódicamente para obtener acceso.



**Figura 6.** Esquema de las claves wpa y wpa2 [44].

Para los protocolos WPA y WPA2 la manera de poder acceder según Mathy Vanhoef, es mediante una conexión de 4 vías que proporcionan autenticación mutua basado en el secreto compartido conocido también clave maestra paritaria PMK, que busca establecer una clave nueva se denomina clave transitoria por partes PTK. El handshake que es unas de las comunicaciones que también se establecen y se denomina suplicante y AP autenticador la clave maestra se deriva de un password precompartido en una red personal y trata de convencer con el otro tipo de protocolo WPA para que le proporcione una autenticación a la red, lo que se busca es negociar una comunicación de PTK derivada de la PMK [44].



**Figura 7.** Esquema de las cabeceras wpa y wpa2 [44].

## **2.5 METODOLOGÍA**

### **2.5.1 METODOLOGÍA DEL PROYECTO**

Los estudios exploratorios se emplean cuando el objetivo es examinar un tema o problema de investigación poco estudiado o novedoso, del cual se tienen muchas dudas o no se ha abordado antes, se tienen ideas vagas relacionadas con el problema de estudio y si deseamos indagar desde nuevas perspectivas [45].

El presente trabajo consiste en la implementación de la metodología del hacking ético el cual consiste en 5 fases, en el presente proyecto se ha adaptado a 4 fases que consisten en:

**Reconocimiento:** Consiste en realizar el reconocimiento pasivo y activo en donde se tiene como objetivo poder identificar y obtener información del lugar, topología donde se realizará la identificación de las vulnerabilidades de las redes que serán posteriormente evaluadas.

**Escaneo:** Se realiza un escaneo activo, una vez ya teniendo la información de la fase anterior que nos servirá para examinar la red, obtener las direcciones IP, MAC, redes abiertas posiblemente vulnerables.

**Obtener Acceso:** El objetivo consiste en explotar las vulnerabilidades que se lograron identificar en la fase de escaneo, de esta manera se podrá verificar si la red es susceptible a no ser atacada o de lo contrario es de manera mucho más fácil de atacar esto consiste en verificar la factibilidad de los protocolos de seguridad que se encuentran en la red, capturar información que está pasando en la red al igual que capturar datos o paquetes en la red.

**Elaboración de Reporte:** Se presentará un informe detallado de cada uno de los procesos que se logren realizar dentro de este proyecto, evidenciando con capturas de pantalla cada uno de los procesos que realizarán así mismo los mecanismos aplicados, métodos y técnicas que se aplicarán, las amenazas que se encontraron en cada red que logre llegar a evaluar en todo el proceso.

El presente proyecto abarca las siguientes fases:



## **2.5.2 METODOLOGÍA DE INVESTIGACIÓN**

### **INVESTIGACIÓN DESCRIPTIVA**

Este tipo de investigación se los considera como investigación de segundo nivel, su objetivo principal es recopilar datos e informaciones, sobre las características propiedades, aspectos o dimensiones de las personas de los procesos sociales. Tiene objetivo principal comprender la recolección de datos para probar las hipótesis, preguntas o dudas sobre el tema o situación en la que se está evaluando [46].

### **INVESTIGACIÓN EXPERIMENTAL**

En la investigación experimental lo que quiere llegar a manipular son una o varias variables de estudio, para de esta manera poder llegar a evaluar los aumentos o disminución de estas variables se puede llegar a dar a manera de observación. El experimento consiste en hacer el cambio en el valor de una variable independiente y observar que ocasiona con la variable independiente, estos tipos de métodos experimentales son muy factibles en la prueba de hipótesis de relaciones casuales [47].

### **2.5.3 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS**

Se detallará 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 de manera natural, puesto que son influencias producidas por el observador este tipo de técnicas son más difícil de adecuarse a un estudio experimental, esta técnica tiene un tope que es lo que imposibilita resaltar todo ya depende del observador tomar una elección de lo observado según lo requiera el proyecto de trabajo [48].

- La observación se inclina también para propósitos exploratorios esto es adaptable de acuerdo con el investigador en el estudio de la situación donde se puede realizar el análisis de datos simultaneo y la recolección. El observador se limita a las normas de la comunidad de lo que equivale a poder reconocer y aceptar lo que es ajeno [48].

- **Instrumentos**

- Ficha de observación

## **CAPÍTULO 3**

### **PROPUESTA**

#### **3.1 FASE 1.- RECONOCIMIENTO**

Para obtener información del proyecto que se llevara a cabo y lograr los objetivos plantados, se emplearan varios instrumentos y técnicas para la recolección de datos. Posteriormente en función de los datos e información que se requiere usar técnicas documentales y de observación.

**Tabla 8**  
Tabla de resultado fase 1 - Reconocimiento

<b>Responsable:</b> Robert Salinas Vasquez	<b>Nombre de la Fase:</b> Reconocimiento						
<p><b>Objetivo de esta fase:</b> Recopilar información de la topología de la red.</p> <p><b>Tiempo de ejecución:</b> 1 hora <span style="float: right;"><b>Nivel de complejidad:</b> bajo</span></p> <p><b>Herramientas tecnológicas empleadas:</b> Para la resolución de esta fase se hace uso de herramientas que permiten identificar y mostrar los dispositivos que están activos dentro de la red, tanto activos como inactivos, aplicando técnicas de observación.</p> <table border="1" style="width: 100%; text-align: center;"> <thead> <tr> <th style="width: 50%;">HARDWARE</th> <th style="width: 50%;">SOFTWARE</th> </tr> </thead> <tbody> <tr> <td>Computador</td> <td>Sistema operativo Kali Linux</td> </tr> <tr> <td colspan="2">Lucidchart</td> </tr> </tbody> </table> <p><b>Técnicas</b> El resultado se obtiene mediante la técnica de observación.</p> <p><b>Resultados Obtenidos</b> El resultado de esta fase es obtener la topología de la red que está configurada por:</p> <ul style="list-style-type: none"> <li>▪ 1 Router principal GPON ONU, modelo AN5506-04-FAT.</li> <li>▪ 1 AP marca Huawei.</li> <li>▪ 1 Computadora</li> <li>▪ 2 dispositivos móviles</li> <li>▪ 1 D-Link</li> </ul> <div style="border: 2px solid black; padding: 10px; margin: 10px 0;"> </div>		HARDWARE	SOFTWARE	Computador	Sistema operativo Kali Linux	Lucidchart	
HARDWARE	SOFTWARE						
Computador	Sistema operativo Kali Linux						
Lucidchart							

Nota: Tabla de resultados de la fase 1.

### 3.2 FASE 2.- ESCANEO

Para el desarrollo de esta fase se hace uso de la herramienta Nmap que permite visualizar direcciones IP, puertos de la red.

**Tabla 9**  
Tabla de resultado fase 2 - Escaneo

<b>Responsable:</b> Robert Salinas Vasquez	<b>Nombre de la Fase:</b> Escaneo										
<b>Objetivo de esta fase:</b>											
<p>Descubrir los hosts activos que se encuentran dentro de la red que se va a evaluar, toma como nombre de la red TOPOIDE CNT.</p> <p>Con su dirección 192.168.1.10 mask 255.255.255.0 mediante el uso de Nmap de Kali Linux.</p>											
<b>Tiempo de ejecución:</b> 2 horas	<b>Nivel de complejidad:</b> Medio										
<b>Herramientas tecnológicas empleadas:</b>											
<b>HARDWARE</b>	<b>SOFTWARE</b>										
Computador	Sistema operativo Kali Linux										
D-Link	Nmap										
<b>Técnicas</b>											
<p>Se hace uso de la técnica de ping sweep, es la manera mediante podemos recopilar la información de los dispositivos conectados a la red.</p>											
<b>Resultados Obtenidos</b>											
<p>El resultado de esta fase se muestra en el anexo 1, el cual contiene el detalle técnico de las configuraciones realizadas en los dispositivos activos de la red (<b>Ver Anexo 1</b>).</p> <p>A continuación, se describen los dispositivos conectados en la red.</p>											
<b>DISPOSTIVOS</b>	<b>DIRECCIONES</b>										
	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%; border-bottom: 1px solid black;">IP</th> <th style="width: 70%; border-bottom: 1px solid black;">MAC</th> </tr> </thead> <tbody> <tr> <td style="text-align: center; border-bottom: 1px solid black;"><b>1</b></td> <td style="text-align: center; border-bottom: 1px solid black;">192.168.1.2 54:B8:0A:46:30:B6</td> </tr> <tr> <td style="text-align: center; border-bottom: 1px solid black;"><b>2</b></td> <td style="text-align: center; border-bottom: 1px solid black;">192.168.1.8 F8:3F:51:D7:0F:17</td> </tr> <tr> <td style="text-align: center; border-bottom: 1px solid black;"><b>3</b></td> <td style="text-align: center; border-bottom: 1px solid black;">192.168.1.13 18:D6:1C:12:90:DB</td> </tr> <tr> <td style="text-align: center; border-bottom: 1px solid black;"><b>4</b></td> <td style="text-align: center; border-bottom: 1px solid black;">192.168.1.14 54:B8:0A:46:30:B6</td> </tr> </tbody> </table>	IP	MAC	<b>1</b>	192.168.1.2 54:B8:0A:46:30:B6	<b>2</b>	192.168.1.8 F8:3F:51:D7:0F:17	<b>3</b>	192.168.1.13 18:D6:1C:12:90:DB	<b>4</b>	192.168.1.14 54:B8:0A:46:30:B6
IP	MAC										
<b>1</b>	192.168.1.2 54:B8:0A:46:30:B6										
<b>2</b>	192.168.1.8 F8:3F:51:D7:0F:17										
<b>3</b>	192.168.1.13 18:D6:1C:12:90:DB										
<b>4</b>	192.168.1.14 54:B8:0A:46:30:B6										

5	192.168.1.10	54:B8:0A:46:30:B6
---	--------------	-------------------

Nota: Tabla de resultados de la fase 2.

### 3.3 FASE 3.- OBTENER ACCESO

Se quiere llegar a vulnerar la seguridad de los protocolos wpa y wpa2 entonces hacemos uso de otro sistema operativo que es Wifislax que está diseñado para auditorias de seguridad, detección de vulnerabilidades y relacionada con seguridad informática. Al igual en la fase dos pudimos hacer uso de la herramienta Nmap en este proceso se hace uso de linset que nos permitirá el descifrado de las redes que están vulnerables en conjunto con wpa que nos proporciona una variedad de herramientas para distintos tipos de pruebas.

**Tabla 10**  
Tabla de resultado fase 3 - Obtener Acceso

<b>Responsable:</b> Robert Salinas Vasquez	<b>Nombre de la Fase:</b> Obtener acceso
<b>Objetivo de esta fase:</b>	
Obtener las características que la red dispone.	
Identificar si los puertos de la red llegasen a tener vulnerabilidades.	
<b>Tiempo de ejecución:</b> 3 horas	<b>Nivel de complejidad:</b> Medio
<b>Herramientas tecnológicas empleadas:</b>	
<b>HARDWARE</b>	<b>SOFTWARE</b>
Computador	Sistema operativo Kali Linux
D-Link	Linset
	WPA
	Aircrack-ng
	Ataque DoS
<b>Técnicas</b>	
El resultado se obtiene mediante la técnica de Evil Twin Attack.	
<b>Resultados Obtenidos</b>	
El resultado de esta fase es obtener el descifrado del password de la red que se está vulnerando, mediante la técnica evil twin Attack, lograremos el descifrado mediante	

unos de los dispositivos que se encuentran conectados a la red, los dispositivos son el medio importante para la obtención (**Ver Anexo 2**).



```
Esperando la pass
Aircrack-ng 1.2 r
c2 r2701
[00:00:00] 1 keys tested (915.7
5 k/s)
KEY FOUND! [ topoideDH
]H
Master Key      : AB FD F4 89 44 66 4B 0C C2
B2 50 A5 3E FB 35 C7      30 5D 3D 1A 7B 69 2F DE 05
46 25 Transient Key : 26 9B CA 60 63 6B 9F EF B8
E8 48 F8 0A B9 E6 86      73 43 FA BC F0 BD 86 FB A9
F4 F8 25 7A 73 17 89      51 53 62 3C C5 A8 9F 30 6B
C3 09 EAPOL HMAC   : 94 C5 4C 16 00 58 F2 8C 7B
DC EC 15 03 AA 7F 4E      52 44 B3 3E 43 5E C5 55 7D
83 E1 02 E4 4F 90 B0
Se ha guardado en /root/TOPOIDE CNT-password.txt
```

Nota: Tabla de resultados de la fase 3.

### 3.4 FASE 4.- ELABORACIÓN DE REPORTE

En esta siguiente tabla se mostrará las vulnerabilidades que se llegaron a encontrar dentro de la red evaluada, con su nivel de criticidad los resultados obtenidos se dan mediante el conjunto de todas las técnicas utilizadas en el proceso, de la misma manera la técnica de observación y bibliográfica que nos han hecho un gran aporte dentro de este proyecto.

**Tabla 11**  
Tabla detección de amenazas en la red

NOMBRE DEL LUGAR: Sector Cinco Esquinas			CIUDAD: Santa Elena		
ENCARGADO DEL SECTOR: Robert Ivan Salinas Vasquez					
AMENAZA	VULNERABILIDADES ENCONTRADAS	NIVEL DE CRITICIDAD	DISPOSITIVOS AFECTADOS	TIPO DE VULNERABILIDADES	POSIBLES SOLUCIONES
Falta de las listas de control de acceso	Identificación de dispositivos clientes por la MAC de la tarjeta de red.	MEDIA	<ul style="list-style-type: none"> <li>- PC escritorio</li> <li>- Portátiles</li> <li>- Dispositivos móviles</li> </ul>	Hardware	Programar los puntos de acceso con una lista de direcciones MAC asociadas a los dispositivos clientes para permitir el acceso a los AP.
Mantener el nombre de la red oculta	Fácil detección del nombre de la red, mediante la antena USB D-Link	MEDIA	<ul style="list-style-type: none"> <li>- PC escritorio</li> <li>- Portátiles</li> <li>- Dispositivos móviles</li> <li>- Routers</li> <li>- Modem</li> </ul>	Hardware	Entrar a las configuraciones del dispositivo (MODEN), AP, para poder ocultar el nombre de la red y así que sea menos detectable por las tarjetas de red o antenas USB detectora de señales inalámbricas.
Password y ESSID	Password de fabrica o designado por los dispositivos, muy pocos caracteres o comunes.	ALTA	<ul style="list-style-type: none"> <li>- AP</li> </ul>	Configuraciones	Cambiar las credenciales de manera general cuando ya tiene instalado los dispositivos en su localidad para mayor.
Tamaño de la clave de encriptación poco segura	La clave del dispositivo es muy débil que permite poder observar el tráfico de la red auditada.	ALTA	<ul style="list-style-type: none"> <li>- AP</li> </ul>	Configuraciones	Seguridad lograr ingresar caracteres alfanuméricos mayor a 12 caracteres para mayor seguridad y descifrado.
Actualizaciones de hardware y software	Dispositivos y software poco sofisticados.	BAJO	<ul style="list-style-type: none"> <li>- PC Escritorio</li> <li>- Portátil</li> </ul>	Software	En lo más seguro posible siempre mantener actualizados dispositivos y software ya que muchos de estos ayudan a la protección del tráfico generado en la WLAN.

Nota: Resultado de las amenazas detectadas.

La siguiente tabla muestra el resumen de las vulnerabilidades encontradas describiendo las amenazas, dispositivos afectados, tipo de vulnerabilidad, lugar, banda de frecuencia en la siguiente tabla se detalla.

**Tabla 12**

Tabla de resultado Fase 4 - Elaboración de reporte

<b>Localidad</b>	Santa Elena			
<b>Tipo de prueba</b>	Red Cerrada - Red Doméstica			
<b>Alcance aproximado</b>	100 metros			
<b>Nivel de señal</b>	- 68 dBm			
<b>Banda de frecuencia</b>	2.4Ghz			
<b>Canal</b>	11			
<b>Número de ataques</b>	2			
<b>Tiempo total de duración del (los) ataques(s)</b>	2 horas 45 minutos			
<b>ROUTER ATACADO – ACCESS POINT</b>				
<b>MAC address</b>	<b>Marca</b>	<b>Modelo</b>	<b>Configuración por defecto</b>	
20:08:ED:E4:6C:5C	Huawei		Configuración vía navegador web 192.168.10.1 Username: instalador Password: robert2001	
<b>WIRELESS NIC 802.11b/g PARTICIPANTES</b>				
<b>Marca</b>	<b>Tipo</b>	<b>Mac</b>	<b>Address</b>	
D-LINK	USB		54:B8:0A:46:30:B6	
<b>ENCRIPCIÓN WPA / WPA2</b>				
<b>BSSID</b>	<b>ESSID</b>	<b>Datos</b>	<b>Canal</b>	<b>SEC</b>
20:08:ED:E4:6C:64	TOPOIDE CNT	29	11 (2.42 MHz)	WPA2
<b>HERRAMIENTAS UTILIZADAS</b>				
<b>Nombre</b>	<b>Uso</b>	<b>Minutos estimados</b>		
Aircrack-ng handshake	Si	30 minutos		
Airmon-ng	No	-		
Airodump-ng	No	-		
Aireplay-ng	No	-		
Linset	Si	1 hora 20 minutos		
Pyrit	Si	30 minutos		
<b>DISTRIBUCIÓN DE SOFTWARE LIBRE</b>				
<b>WifiSalx</b>	Versión 4.11.1 script Linset			
<b>Clave de acceso localizada: topoideDH</b>				
<b>Diagnóstico:</b> Dado el cuadro de resultados de la parte superior se puede tomar la decisión que la red que está siendo evaluada con los protocolos de encriptación WPA/WPA2 cuenta con cuadros críticos al nivel intermedio y alto, esto quiere decir que la red con estos protocolos son vulnerables tanto en el tráfico de sus datos que viajan por el medio, el descifrado de sus credenciales y cierta parte de la manipulación de su servicio de internet, al ser un AP el que está siendo vulnerado PSI, hace que su configuración interna sea muy débil en ocasiones suele ser también por modelo del hardware del que se esté utilizando. El dispositivo evaluado cuenta con vulnerabilidades mientras que el dispositivo de donde sale la extensión no tiene ningún tipo de vulnerabilidad ya que también pasó por el mismo proceso para sus detecciones de vulnerabilidades, pero las opciones salían denegadas por la robustez del dispositivo.				

Nota: Reporte general de todo el proceso realizado.

## CONCLUSIONES

El ambiente virtualizado con el sistema operativo Wifislax cuenta con variedad de herramientas y técnicas que permiten vulnerar los protocolos de seguridad, obtención de acceso de las redes inalámbricas que están diseñadas para este tipo de redes, mientras que el sistema operativo Kali Linux tiene un enfoque sobre las auditoria de seguridad y seguridad informática en general.

Entre la variedad de herramientas que se pueden utilizar para el descifrado de claves, linset es una herramienta que nos permite comprobar con facilidad la seguridad de las redes, haciendo uso de su técnica de descifrado Evil Twin Attack que realiza la búsqueda en tiempo real en los routers y puntos de acceso sin la necesidad de otras técnicas como ataque de fuerza bruta o diccionarios.

Se pudo identificar 5 amenazas que están expuestas en la red inalámbrica, se determinar el nivel de criticidad de cada amenaza detectada que están divididas en: alto, medio, bajo estas amenazas son las que ponen en riesgos los equipos de la localidad se pueden presentar en empresas o compañías.

Los protocolos de seguridad WPA y WPA2 son vulnerados mediante la técnica que contiene linset y su ataque DoS, lo que se realiza es una solicitud de autenticación entre el solicitante (cliente) y el autenticador (AP) lo que espera es la respuesta de la autenticación esto en su etapa de asociación, en la etapa de obtener acceso lo que se derivan son comunicación entre PTK de cada extremo cliente y punto de acceso.

El tiempo promedio para vulnerar estos protocolos de seguridad tuvo un tiempo como promedio de 2 horas, haciendo uso del sistema operativo Wifislax en conjunto con tu herramienta integrada linset.

## **RECOMENDACIONES**

Realizar buenas prácticas en ambientes controlados donde se mantenga la integridad de los dispositivos, de la misma manera poder estar en el constante aprendizaje de los diversos sistemas operativos y herramientas que permiten la seguridad de nuestra información con la finalidad de realizar buenas prácticas con resultados positivos.

El uso de herramientas que actualmente se utilizan están en constante evolución por esta razón los usuarios de los diferentes tipos de redes siempre sean conscientes de evaluaciones periódicas en la infraestructura de la red mediante un hacker de sombrero blanco, hacker de sombrero gris o personal que cuente con los conocimientos necesarios para poder evaluar la red y les proporcione soluciones a los problemas que se llagasen a encontrar.

Se plantea que los dispositivos detectados con amenazas estén en proceso de revisión continuo donde se empleen políticas de seguridad, esto mejorara el cuidado de los dispositivos y la seguridad de los datos tanto en redes inalámbricas empresariales y domésticas.

Evitar las vulnerabilidades de los protocolos de manera definitiva es muy complicado, pero reducir el riesgo de evitar que se conviertan en amenazas si es posible, haciendo los correctos cambios en los dispositivos correspondientes ya que las redes por medios no guiados son más propensas a ataques.

## BIBLIOGRAFIA

- [1] E. K. B. C. Luca, «Análisi de uso y ventajas de linset para auditorías de redes inalámbricas con encriptación wpa y wpa2,» Guayaquil, 2016.
- [2] E. K. Bermudez Castro, « Análisis de Uso y Ventajas de Linset para Auditorias de Redes Inalámbricas con Encriptación WPA y WPA2,» 2016. [En línea]. Available: <http://repositorio.ug.edu.ec/handle/redug/17104>.
- [3] J. T. P. García, «Análisis de los protocolos de seguridad inalámbrica implementadas en red wifi en la ciudad de bogotá,» 2022. [En línea]. Available: <https://repository.unad.edu.co/bitstream/handle/10596/51604/1019116994.pdf?sequence=1&isAllowed=y>.
- [4] S. F. & P. A. Lena, «Protección de Redes con Infraestructura de Procesamiento ante Ciberataques,» Buenos Aires - Argentina .
- [5] A. A. Jorge Veloz, «Ethical hacking, una metodología para descubrir fallas de seguridad en sistemas de informacion mediante la herramienta Kali Linux,» Manabi, 2017.
- [6] H. R. T. Acevedo, «Tecnica basadas en explotación de vulnerabilidades.,» Colombia - Bogotá, 2015.
- [7] J. A. Q. S. I. A. P. Crespo, «Auditoria de seguridad en redes inalámbricas con encriptación wep, wpa y wpa2 utilizando la placa arduino wifi-jammer y la metodología owisan para la empresa importecell ubicado en el cantón el triunfoperteneciente a la provincia del guayas.,» Ecuador - Guayaquil, 2018.
- [8] S. R. L. ESET, «Security Report Latinoamérica 2022».
- [9] S. N. D. Planificacion, «Plan de Creacion de Oportunidades,» Quito - Ecuador, 2021-2025.

- [10] R. KeepCoding, «KEEPCOSING Tech School,» 27 07 2022. [En línea]. Available: ransomware. [Último acceso: 21 02 2023].
- [11] W. S. Seguridad informaticac, «Ciberseguridad Compresible,» 2 03 2015. [En línea]. Available: <https://cloudswxsecure.wordpress.com/2015/03/02/que-es-mdk3-y-para-que-sirve/>. [Último acceso: 21 02 2023].
- [12] Cisco. [En línea]. Available: <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>. [Último acceso: 21 02 2023].
- [13] d. d. y. tecnologia, «ALEGSA,» 14 11 2010. [En línea]. Available: <https://www.alegsa.com.ar/Dic/ccmp.php>. [Último acceso: 21 02 2023].
- [14] R. A. P. Detection, «Fireware WatchGuard,» [En línea]. Available: [https://www.watchguard.com/help/docs/help-center/es-419/Content/es-419/Fireware/wireless/wireless\\_rogue\\_ap\\_detection\\_c.html](https://www.watchguard.com/help/docs/help-center/es-419/Content/es-419/Fireware/wireless/wireless_rogue_ap_detection_c.html). [Último acceso: 21 02 2023].
- [15] J. C. J. Pitriqueo. [En línea]. Available: <https://es.scribd.com/document/335873583/Hostapd-Es-Un-Autenticador-IEEE-802#>. [Último acceso: 21 02 2023].
- [16] Aircrack-NG. [En línea]. Available: <https://www.aircrack-ng.org/>. [Último acceso: 21 02 2023].
- [17] Microsoft. [En línea]. Available: <https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top>. [Último acceso: 21 02 2023].
- [18] I. 802.11. [En línea]. Available: <https://es.theastrologypage.com/ieee-802-11x>. [Último acceso: 21 02 2023].
- [19] R. Inalambrica. [En línea]. Available: <https://definicion.de/red-inalambrica/>. [Último acceso: 21 02 2023].

- [20] E. E. SEGURIDAD, «cyberwade,» [En línea]. Available: <https://cyberwade.com/que-es-un-protocolo-en-informatica/>. [Último acceso: 21 02 2023].
- [21] Educalingo, 20 02 2020. [En línea]. Available: <https://educalingo.com/es/dic-en/psk>. [Último acceso: 21 02 2023].
- [22] D. Còrdoba, «Junco TIC,» [En línea]. Available: <https://juncotic.com/wpa2-como-funciona-algoritmo-wifi/#:~:text=Despu%C3%A9s%20de%20la%20autenticaci%C3%B3n%20de,PSK%20seteada%20por%20el%20usuario..> [Último acceso: 21 02 2023].
- [23] M. G. & R. Hytten, «An analysis of wireless security, Journal of Computing Sciences in Colleges,» 2006.
- [24] C. & D. L. Varela, «Redes inalámbricas,» España, 2002.
- [25] G. G. T. M. C. & Q. G. N. Vargas, «Obtención de claves en redes WLAN/WPS usando Wifislax y Denegación de Servicios con Kali Linux.,» (E18), (2019).
- [26] Aircrack-ng, «es/aircrack-ng,» 05 09 2009. [En línea]. Available: <https://www.aircrack-ng.org/doku.php?id=es:aircrack-ng>. [Último acceso: 17 05 2023].
- [27] SeguridadWireless.net, «wifislax.com,» 19 10 2021. [En línea]. Available: <https://www.wifislax.com/>. [Último acceso: 4 1 2023].
- [28] O. Security, «kali.org,» Debian, 2007 - 2013. [En línea]. Available: <https://www.kali.org/about-us/>. [Último acceso: 4 1 2023].
- [29] R. Exploit, «web.archive.org,» 17 3 2011. [En línea]. Available: <https://web.archive.org/web/20110317183307/http://www.backtrack-linux.org/backtrack/backtrack-5-release-tool-suggestions/>. [Último acceso: 4 1 2023].

- [30] MundoHackers. [En línea]. Available: <https://mundo-hackers.weebly.com/linset.html>. [Último acceso: 2023 02/ 01/].
- [31] P. Mediacyber. [En línea]. Available: <https://www.pandasecurity.com/en/mediacyber/security/what-is-an-evil-twin-attack/>. [Último acceso: 2023 02 01].
- [32] J. R. & E. Pazmiño, «Análisis de WPA/WPA2 vs WEP,» ECUADOR, 2008.
- [33] I. d. s. Ciberseguridad, «Seguridad en redes wifi».
- [34] J. A. N. Espinoza, «Análisis de los mecanismos de seguridad en redes inalámbricas de área local (WLAN),» Guayaquil , 2016.
- [35] H. R. T. Acevedo, «Técnica básica de explotación de vulnerabilidades en los sistemas de protección de redes wifi,» 2015.
- [36] L. o. d. p. d. d. p. -. Ecuador, «Asamblea Nacional,» 2021.
- [37] E. F. Medina Rojas, «Hacking Ético: una herramienta para la seguridad informática,» Colombia, 2015.
- [38] A. López Sempere, «Identificación y detección de vulnerabilidades (Universitat Politècnica de València),» Valencia, (2022)..
- [39] L. r. h. Carlos Arturo Tataes Almedida, «La Ciberseguridad en el Ecuador, una propuesta de organización,» Ecuador, 2018.
- [40] C. A. O. Bonilla, «Estrategias algorítmicas orientadas a la ciberseguridad: un mapeo sistemático,» Guayaquil, 2021.
- [41] S. M. B. & F. Jhonathan, «Buenas prácticas para auditar redes inalámbricas aplicadas a las empresas del rubro hotelero de la ciudad de Chiclayo,» 2012.

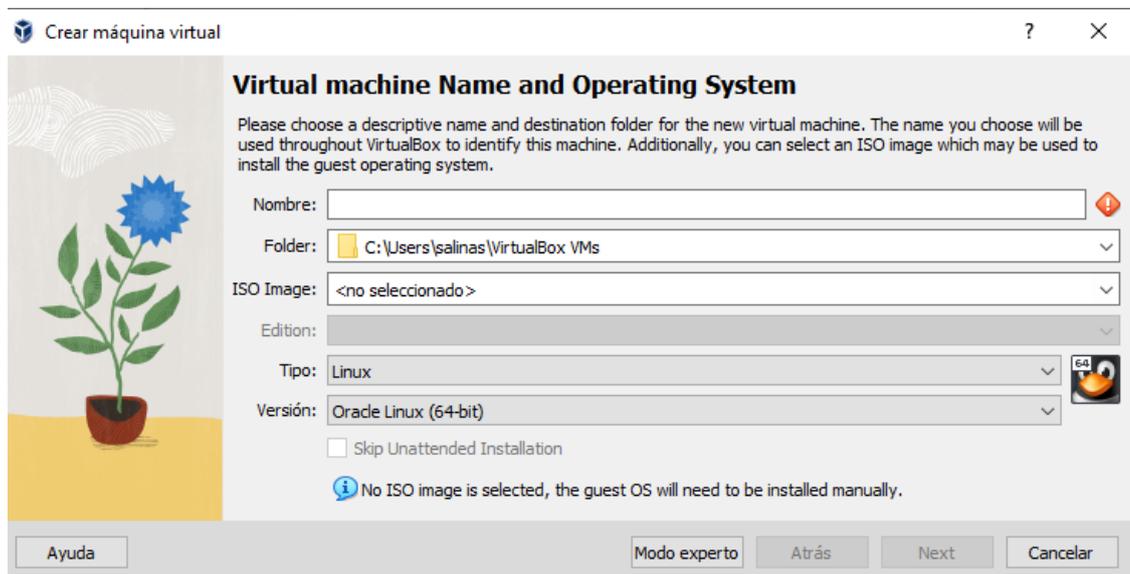
- [42] B. S. J. S. V. Arash Hbibi Lashksri, «Encuesta sobre protocolos de seguridad inalámbrica,» 2009.
- [43] K. d. Carlos verela, «Redes Inalambricas,» 2016.
- [44] X. P. Tornil, «seguridad en redes wlan,» España.
- [45] R. H. & P. Bapista, Metodologia de la Investigacion, Sexta edicion, Mexico: 978-1-4562-2396-0, 2014.
- [46] N. T. E. NIeto, «Tipos de Investogacion,» Santo Domingo, 2018.
- [47] J. m. Atenea Alonso Serrano, «Metodos de investigacion de enfoque experiemntal,» 2011.
- [48] M. S. Fabbri, «Las tecnicas de investiagacion: la observacion».

## ANEXO 1

### DESARROLLO DE LA FASE DE ESCANEO

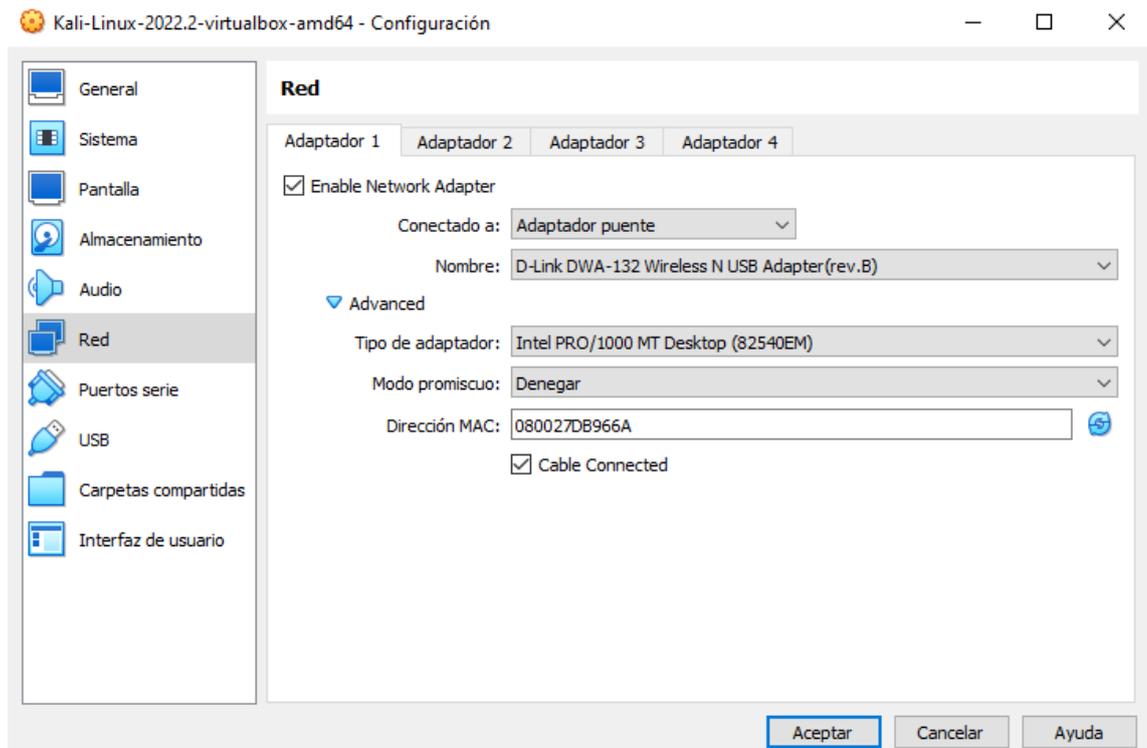
Para la ejecución de esta fase aremos uso del sistema operativo Kali Linux y unas de sus herramientas que este S.O contiene que toma como nombre Nmap, para poder llevar a cabo la herramienta se debe realizar una serie de paso.

1. Se debe ya tener instalado un software de virtualización que nos permitirá poder tener el S.O Kali Linux en uso en esta ocasión haremos uno de virtual box.
2. Se debe tener descargado el S.O que se va a utilizar ya puede ser este la imagen .iso o .ova que son el tipo de formato que se puede obtener.
3. Al tener los dos pasos anteriores se puede hacer uso de la correcta virtualización de Kali Linux, al abrir virtual box en su interfaz encontraremos un icono que toma como nombre nuevo es ahí donde se empezará a crear el S.O en donde se le tendrá que dar el nombre de la maquina a crear, seleccionar el tipo de imagen permitido, tipo y versión.



**Figura 8.** Ventana principal para la creación de la maquina Kali Linux.

4. Una vez teniendo ya todo lo anterior creado nos dirigimos al apartado de configuración donde se podrá ver unas varias opciones no dirigiremos al apartado donde dice red y es importante tener seleccionado donde dice conectado a como adaptador puente para que la máquina que se está creando sea tomada como parte de la red.



**Figura 9.** Ventana del apartado red para la conexión.

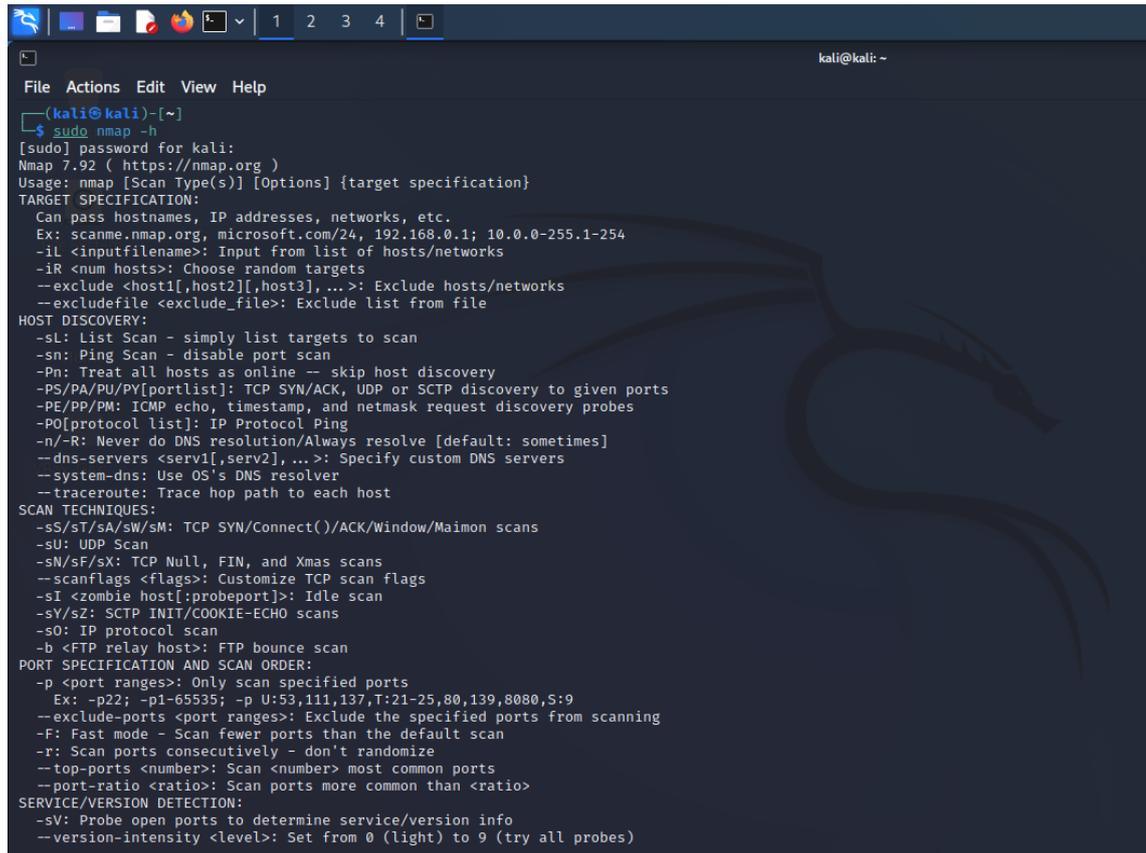
5. Ya habiendo realizado la configuración se procede a correr la máquina, en la interfaz de virtual box encontraremos un icono que dice iniciar de color verde.



**Figura 10.** Arranque de la nueva máquina virtual.

6. Al ya tener corriendo el S.O de Kali Linux, al ingresar te pide que te registres usualmente el usuario y la contraseña suelen ser las mismas “Kali”, ya estando dentro aremos uno de la terminal de Kali Linux para el cual como primera opción siempre debemos de ingresar como super usuario.
7. Como en esta fase se hará uso de la herramienta Nmap es importante verificar si ya contamos con la herramienta, la verificamos de la siguiente manera escribiendo

en la terminal Nmap – h se tiene que desplegar la variedad de opciones de esta herramienta si no es así debes de instalar las librerías para poder hacer uso.



```
(kali@kali)~$ sudo nmap -h
[sudo] password for kali:
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] [target specification]
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludedefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
```

**Figura 11.** Terminal de Kali Linux para el uso de Nmap.

8. Ya al tener verificado que todo funcione se procede a identificar la ip de la red que vamos a evaluar con el comando ifconfig.

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fedb:966a prefixlen 64 scopeid 0<link>
    ether 08:00:27:db:96:6a txqueuelen 1000 (Ethernet)
    RX packets 280 bytes 26792 (26.1 KiB)
    RX errors 0 dropped 44 overruns 0 frame 0
    TX packets 30 bytes 3576 (3.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figura 12. Aplicación del comando ifconfig en la terminal de Kali.

- Ya teniendo identificado la IP de la red procedemos a verificar que dispositivos están conectados en el tiempo de ejecución dentro de la red, con el comando `sudo nmap -o 192.168.1.0/24` la IP proporcionada es la de la red anterior la diferencia es que al poner el último dígito 0 me permitirá evaluar de manera general toda la red.

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo nmap -o 192.168.1.0/24
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-05 14:50 EDT
Nmap scan report for 192.168.1.4
Host is up (0.012s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
8008/tcp  open  http
8009/tcp  open  ajp13
8443/tcp  open  https-alt
9000/tcp  open  cslistener
MAC Address: 0E:42:69:96:02:AD (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=7/5%OT=8008%CT=1%CU=44224%PV=Y%DS=1%DC=D%G=Y%M=0E4269
OS:TM=64A5BC04P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10E%TI=Z%CI=Z%TS=
OS:A)SEQ(SP=101%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M5B4ST11NW6%O2=M5B
OS:4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST11NW6%O6=M5B4ST11)WIN(W
OS:1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%
OS:0=M5B4NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=
OS:N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A
OS:=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%D
OS:F=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL
OS:=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

Nmap scan report for 192.168.1.8
Host is up (0.019s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
7676/tcp  open  imqbrokerd
8080/tcp  open  http-proxy
MAC Address: F8:3F:51:D7:0F:17 (Samsung Electronics)
Device type: general purpose
Running: Linux 2.6.X13.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop

```

Figura 13. Uso del comando nmap con la IP para poder evaluar la red de manera global.

```
Nmap scan report for 192.168.1.9
Host is up (0.0097s latency).
All 1000 scanned ports on 192.168.1.9 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: B6:F4:E7:D4:5A:AA (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.1.13
Host is up (0.087s latency).
All 1000 scanned ports on 192.168.1.13 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 18:D6:1C:12:90:DB (Shenzhen Tinno Mobile Technology)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Figura 15. Resultado de toda la Ip evaluada.

```
Nmap scan report for 192.168.1.14
Host is up (0.00072s latency).
All 1000 scanned ports on 192.168.1.14 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 54:B8:0A:46:30:B6 (D-Link International)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.1.15
Host is up (0.0053s latency).
All 1000 scanned ports on 192.168.1.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 3E:42:02:9A:A7:3F (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.1.10
Host is up (0.000046s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 139.45 seconds
```

Figura 14. Mas información sobre la ip evaluada.

10. Al ya tener el escaneo realizado procedemos a evaluar varios de los dispositivos que se encuentran dentro de la red con el siguiente comando `sudo Nmap -p- -sVC -sC -open -sS -vvv -n -Pn 192.168.1.8 -oN` escaneo, lo que me permite el comando es poder identificar servicio, puertos, versiones y cosas que no quiero se me tomen demasiado tiempo al realizar el escaneo y la IP proporciona es de unos de los dispositivos encontrados en la red.

```
Nmap scan report for 192.168.1.9
Host is up (0.0097s latency).
All 1000 scanned ports on 192.168.1.9 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: B6:F4:E7:D4:5A:AA (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.1.13
Host is up (0.087s latency).
All 1000 scanned ports on 192.168.1.13 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 18:D6:1C:12:90:DB (Shenzhen Tinno Mobile Technology)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.1.14
Host is up (0.00072s latency).
All 1000 scanned ports on 192.168.1.14 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 54:B8:0A:46:30:B6 (D-Link International)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.1.15
Host is up (0.0053s latency).
All 1000 scanned ports on 192.168.1.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 3E:42:02:9A:A7:3F (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.1.10
Host is up (0.000046s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

Figura 16. Nmap uso de la ip de los dispositivos conectados.

```
PORT      STATE SERVICE REASON      VERSION
7011/tcp  open  tcpwrapped syn-ack ttl 64
7676/tcp  open  upnp        syn-ack ttl 64 AllShare UPnP
8080/tcp  open  http        syn-ack ttl 64 lighttpd
|_ http-methods:
|_ Supported Methods: OPTIONS GET HEAD POST
|_ http-title: 404 - Not Found
MAC Address: F8:3F:51:D7:0F:17 (Samsung Electronics)
Service Info: OS: Bada; CPE: cpe:/o:samsung:bada:1.2

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:01
Completed NSE at 15:01, 0.01s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:01
Completed NSE at 15:01, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:01
Completed NSE at 15:01, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.07 seconds
Raw packets sent: 67521 (2.971MB) | Rcvd: 67517 (2.701MB)
```

**Figura 17.** verificación de los puertos abiertos de una Ip.

## ANEXO 2

### DESARROLLO DE LA FASE OBTENER ACCESO

Con el seguimiento de este ambiente personalizado tenemos que poder descargarnos la iso del sistema operativo WIFISLAX, que es un sistema que nos ayudara a la identificación de las vulnerabilidades de las redes Wireless. La descargamos de la siguiente dirección <https://mrroox.blogspot.com/2015/10/wifislax-4111-descarga-directa-desde.html> & <https://www.wifislax.com/category/download/nuevas-versiones/>



**Figura 18.** Descarga del Sistema Operativo Wifislax.

Para su proceso de instalación de hace uso del ambiente grafico que toma como nombre Oracle VM VirtualBox, que es el que nos ayudara para la instalación del archivo .iso, en la siguiente imagen se muestra la interfaz del software.

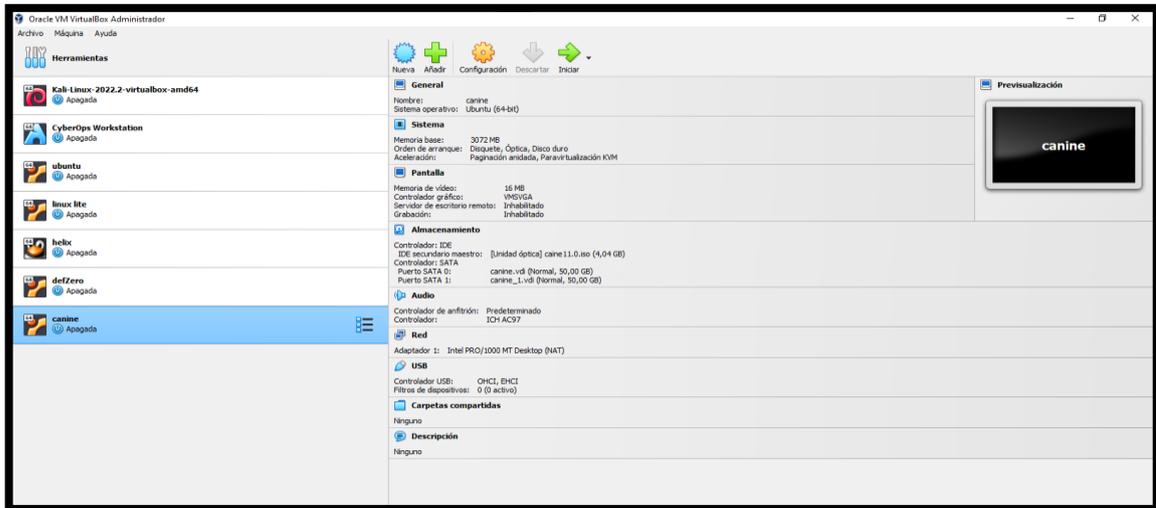


Figura 19. Interfaz de VirtualBox para la instalación del sistema operativo.

Para la creación y visualización de la iso dentro de VirtualBox, seleccionamos en la interfaz la opción que dice nuevo, se abrirá una pantalla con los siguientes datos a llenar en cada uno de sus apartados.

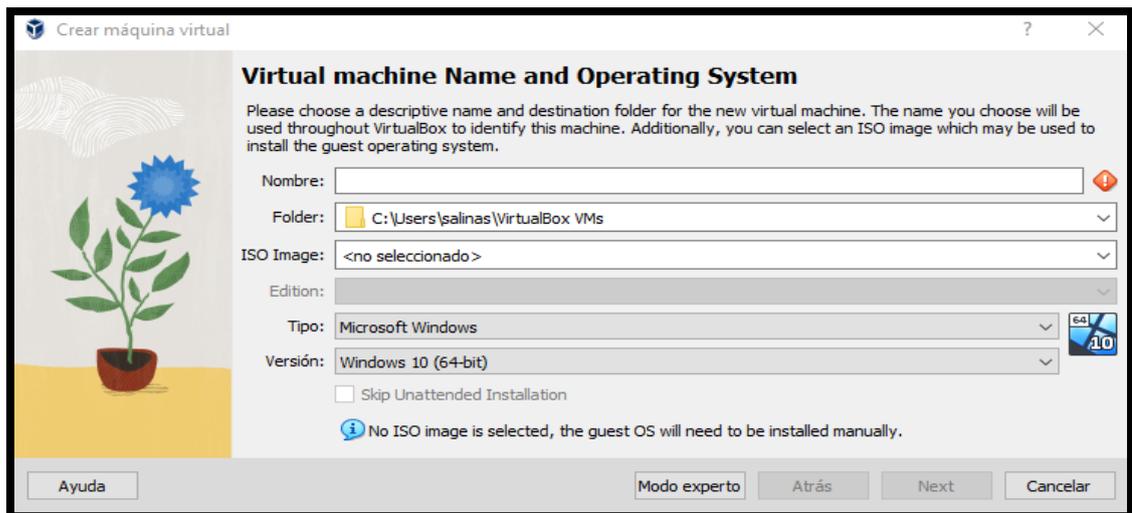


Figura 20. Creación y visualización de Wifislax.

En el grafico anterior se evidencio los campos a llenar dentro de la nueva máquina virtual que se está creando, para esta máquina se llenan los campos como nombre para el proyecto le colocamos el nombre de iso descargada, folder es donde se alojara la maquina creada se deja de manera predeterminada, en el campo tipo se selecciona la distribución que es Linux, versión other Linux.

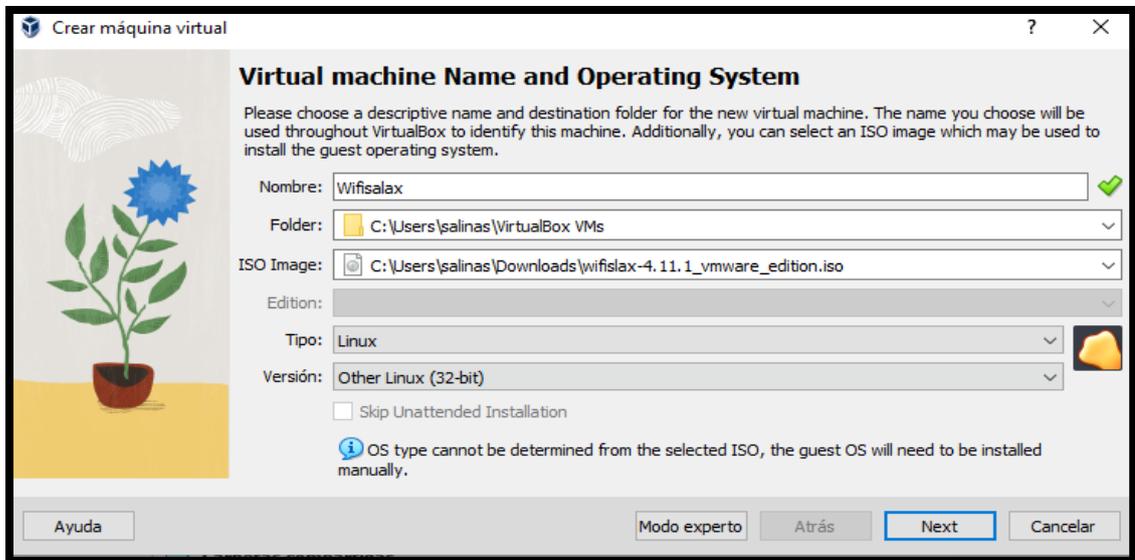


Figura 21. Asignación del nombre de la máquina.

De la misma manera al darle siguiente, seleccionamos la memoria base con la que se mandara a correr nuestro sistema operativo, que es 5197MB.

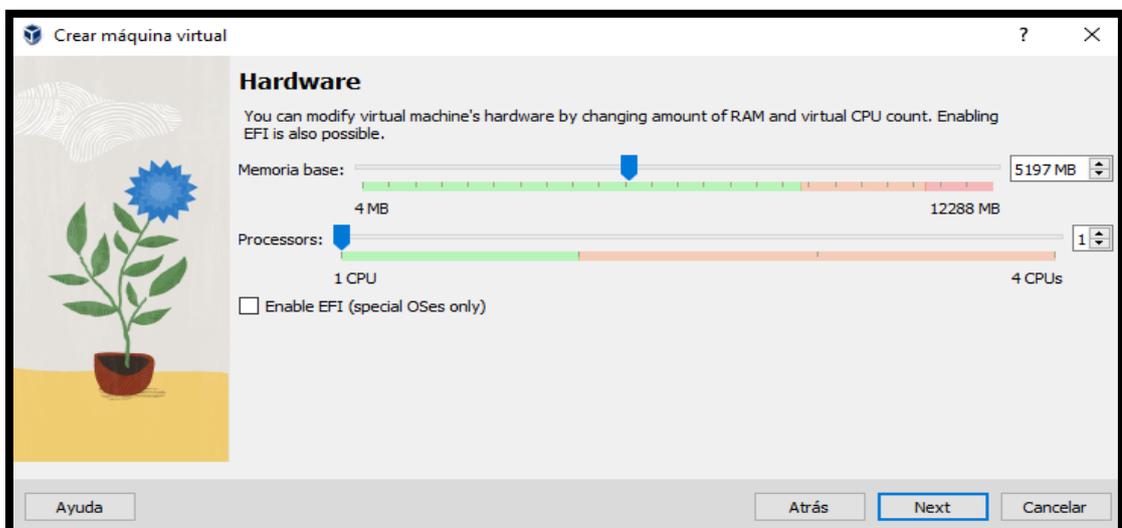


Figura 22. Selección de la memoria base.

Siguiendo la secuencia de pasos nuestro sistema operativo tendrá un disco virtual de 40,00 GB, porque este tamaño por la razón que lo instalaremos de manera permanente y no solo como un lector de disco de .iso.

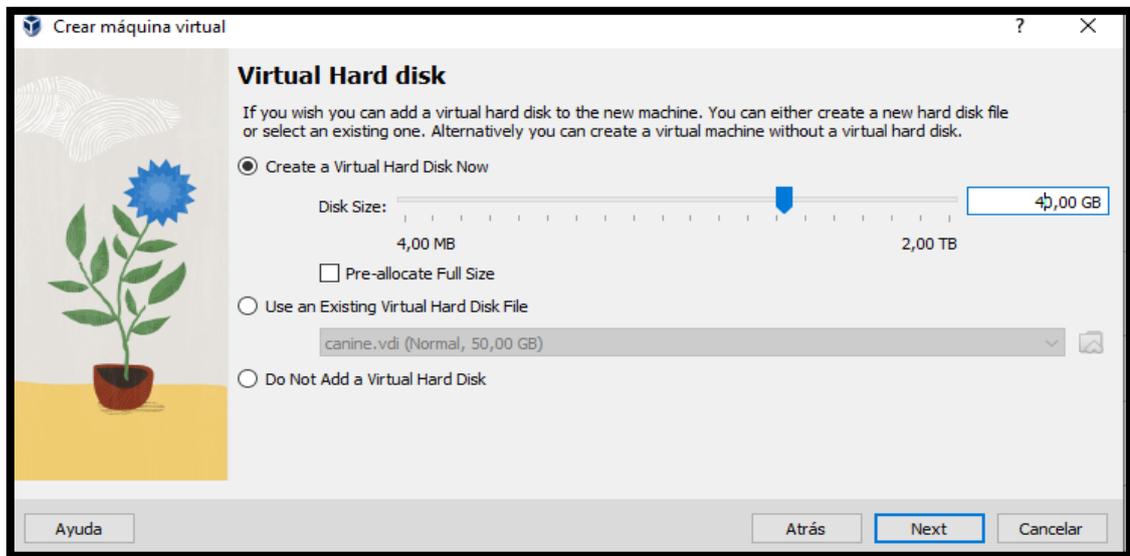


Figura 23. Asignación de la memoria virtual de la máquina.

Al darle siguiente se nos mostrara una tabla con el resumen que contendrá nuestro sistema operativo que posteriormente será iniciado para su correcto levantamiento, pero antes de eso se realizaran varias configuraciones adicionales.

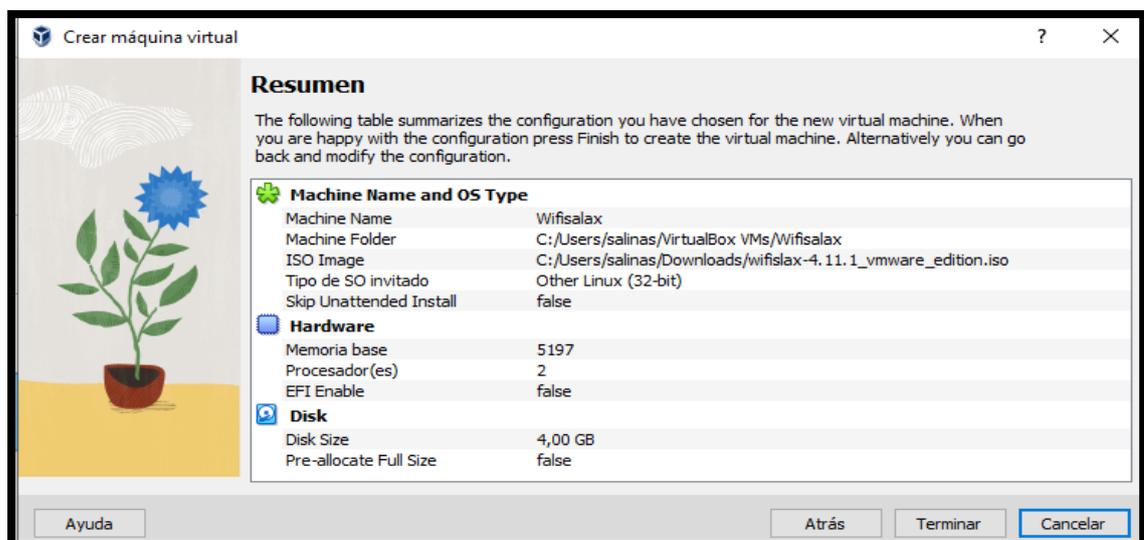
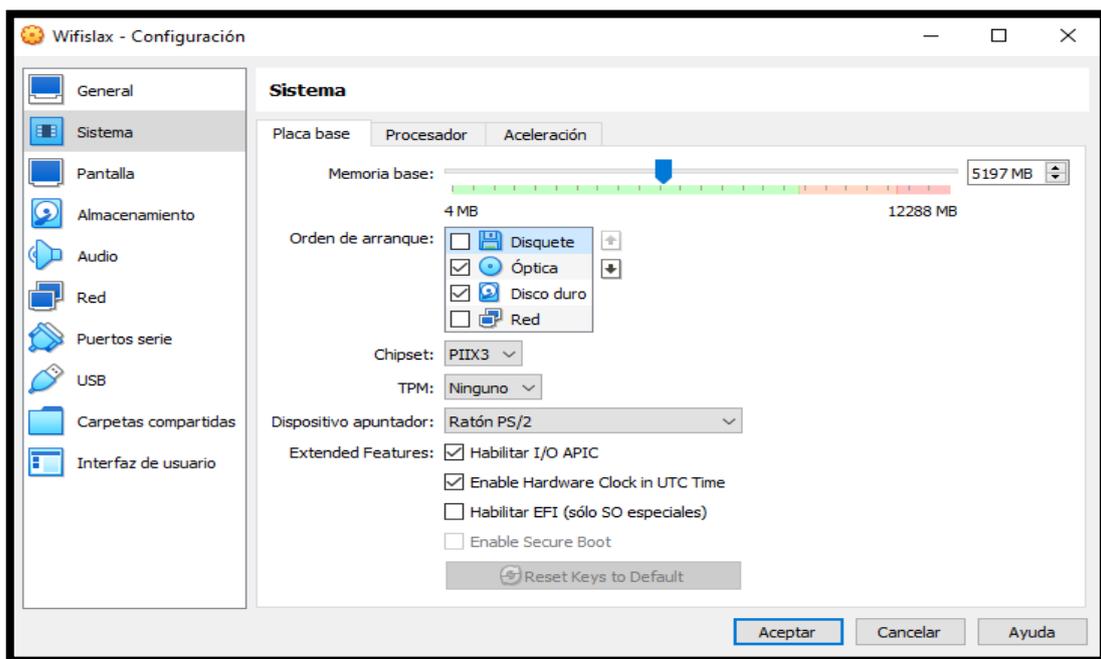


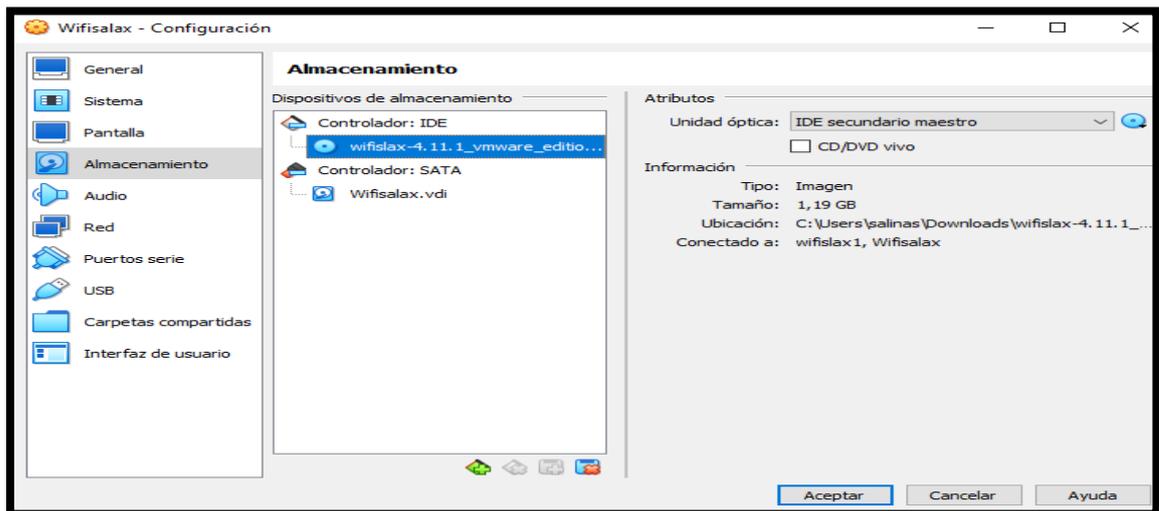
Figura 24. Características de la maquina levantada.

Nos dirigimos al icono de configuración que se muestra en la interfaz de VirtualBox se nos desplegara una ventana como la de la imagen, nos dirigimos al apartado que dice sistema que es en donde desactivaremos el visto de donde dice disquete para, que no corra desde el cd que se seleccionará primeramente para proceder con su instalación ya dentro del S.O en el disco duro virtual creado anteriormente, se procede a darle clic en el apartado de procesador y para que se dé con mejor rendimiento se seleccionan dos procesadores y se procede a aceptar los cambios.



**Figura 25.** Desactivación de la opción disquete para que inicialicé desde la memoria virtual.

Dentro de configuración en el apartado de almacenamiento se selecciona el disco .iso que realizara la visualización del S.O, se procede a seleccionar la memoria óptica y se aceptan los cambios.



**Figura 26.** Borrar el disco .iso que se instaló al principio.

En la interfaz se muestra opciones que están de color naranja que dice iniciar se le hace clic, para que posteriormente con todas las configuraciones ya realizadas proceda a levantarse el sistema operativo, de tal manera que la iniciarse se muestra como en el grafico a continuación.



**Figura 27.** Interfaz de la inicialización del s.o wifislax.

Al haber seleccionado la primera opción del paso anterior se debe esperar unos segundos en donde aparecerá más opciones de seleccionar para ello debemos de seleccionar la primera o la que sale por defecto y que se espera unos segundos para poder seleccionar de manera automática.



Figura 28. Selección del arrancador de Wifislax.

Una vez pasen los minutos que se muestra en la anterior captura de pantalla se muestran líneas de comando que es donde se indica que todos los paquetes se están cargando para posteriormente, se inicialice la interfaz gráfica de Wifislax.

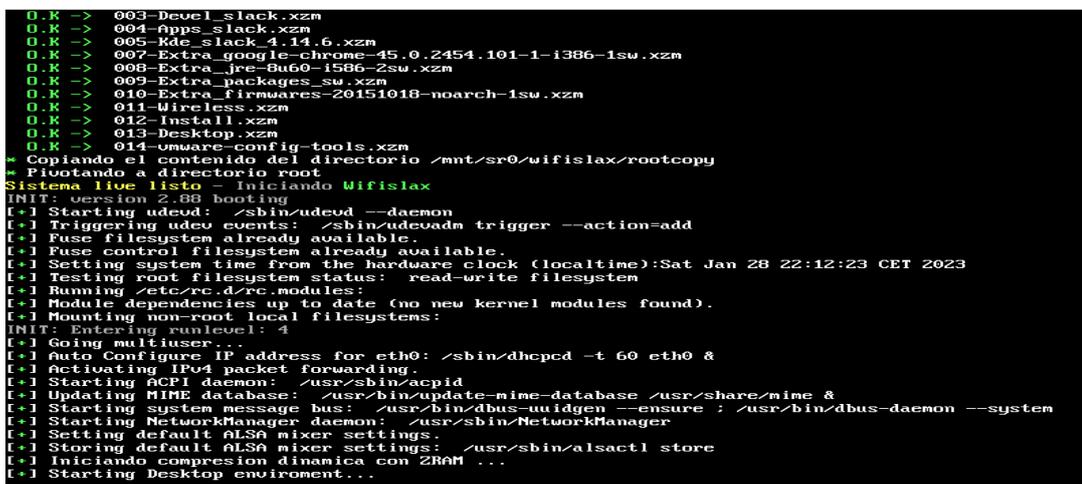


Figura 29. Instalación del sistema operativo.

Una vez ya teniendo la interfaz gráfica ya visualizada se procede a realizar la instalación de manera estática por llamarlo así dentro del disco virtual que se dejó creado en los anteriores pasos que son parte del proceso, nos dirigimos al icono que está en la parte inferior izquierda, nos dirigimos hacia sistemas y siguiente a Wifislax que está con un icono color rojo aparecen dos opciones y seleccionamos el que tiene terminología HDD.

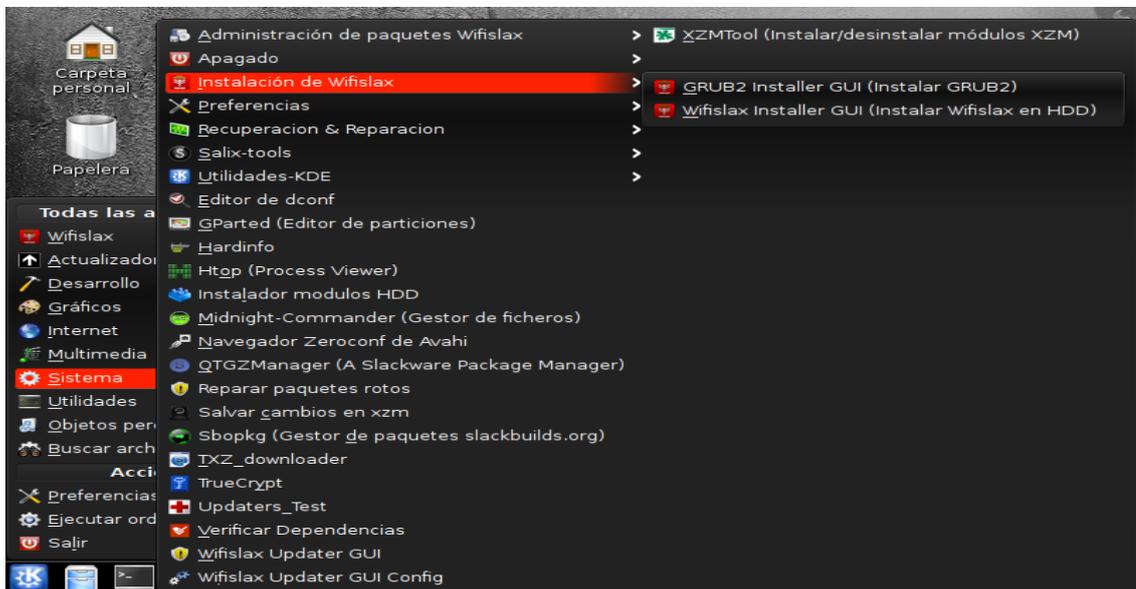


Figura 30. Ambiente virtual de Wifislax, selección de HDD.

A continuación de seleccionar en HDD, aparece una nueva ventana que dice que primero se debe crear la partición dentro del iso que está corriendo (disco), y siguiente se selecciona Abrir Gparted para confirmar.

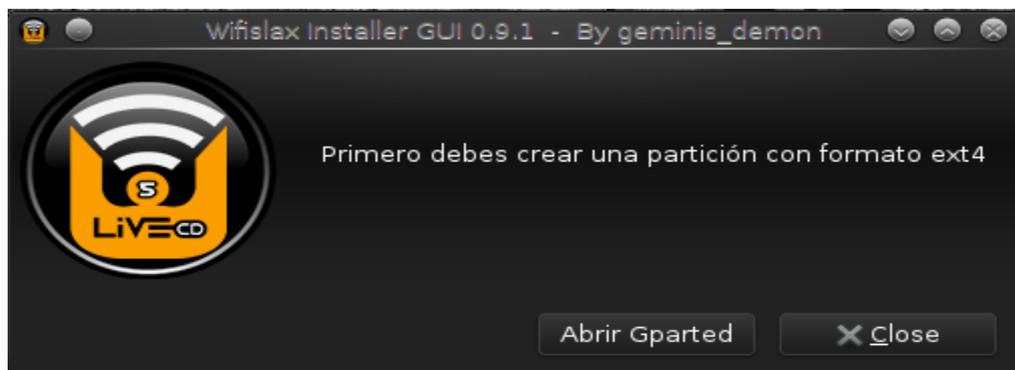


Figura 31. Despliegue de pantalla para crear una partición.

A continuación, se abre una nueva ventana en donde sale cuanto es la cantidad de disco que se tiene configurada antes, se procede a crear la tabla de particiones en la opción dispositivo y a asignar la partición se eliminan los datos existentes en el disco, se abre una ventana y se procede a aplicarla.

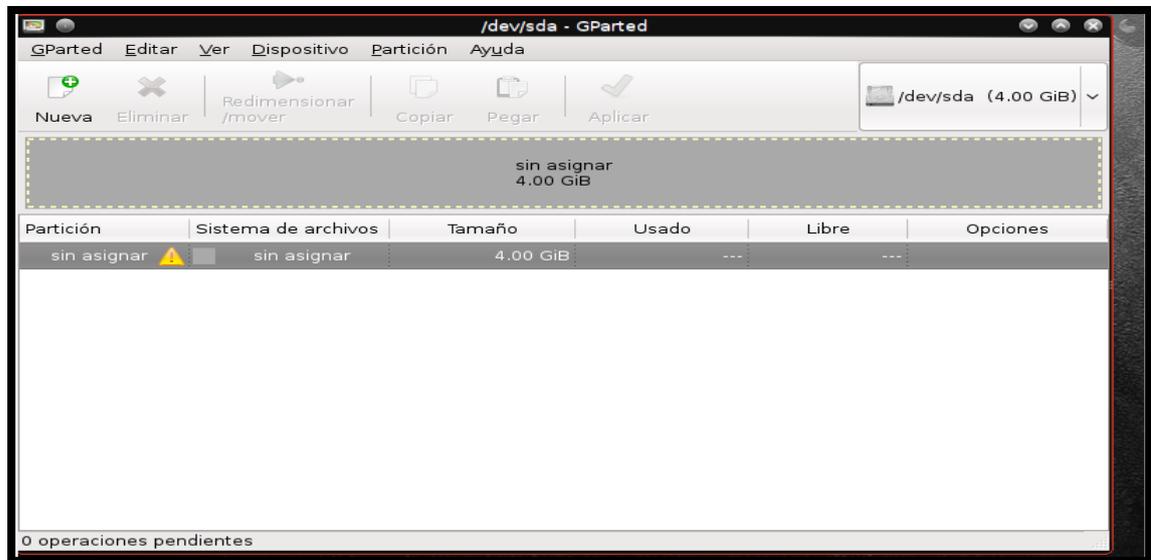


Figura 32. Destinar almacenamiento para la partición.



Figura 33. Aplicación de todos los cambios que se están realizando.

Una vez ya teniendo la partición se procede a aplicar las operaciones sobre el dispositivo para que se hagan los cambios, se hace clic en el visto de la interfaz, aparece la barra que realiza la aplicación.

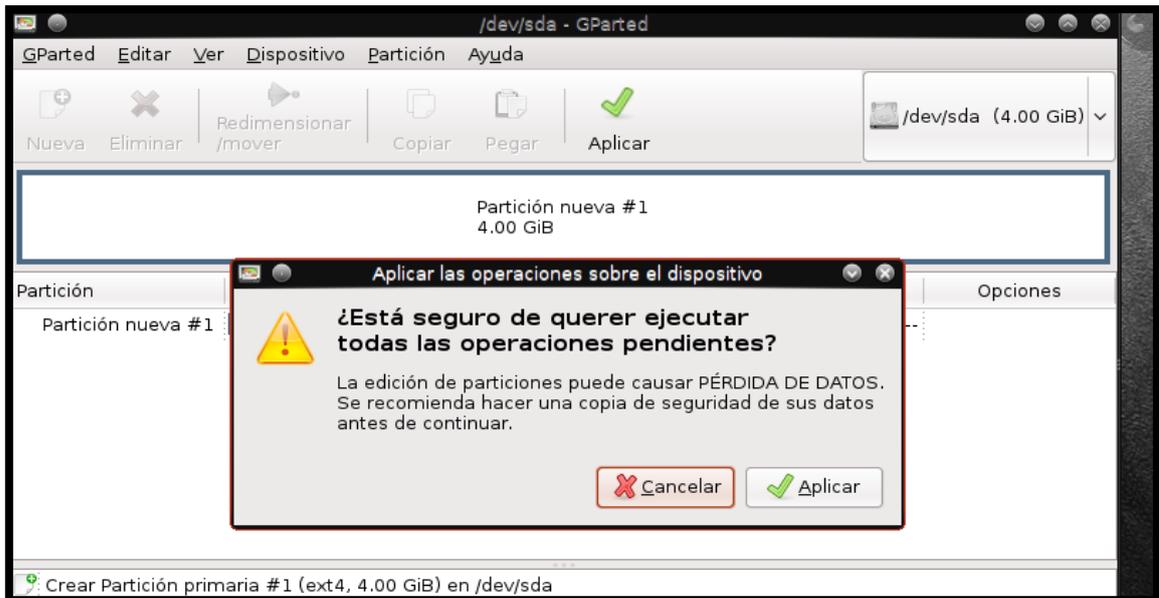


Figura 34. Aplicación de cambios para la aplicación de operaciones.

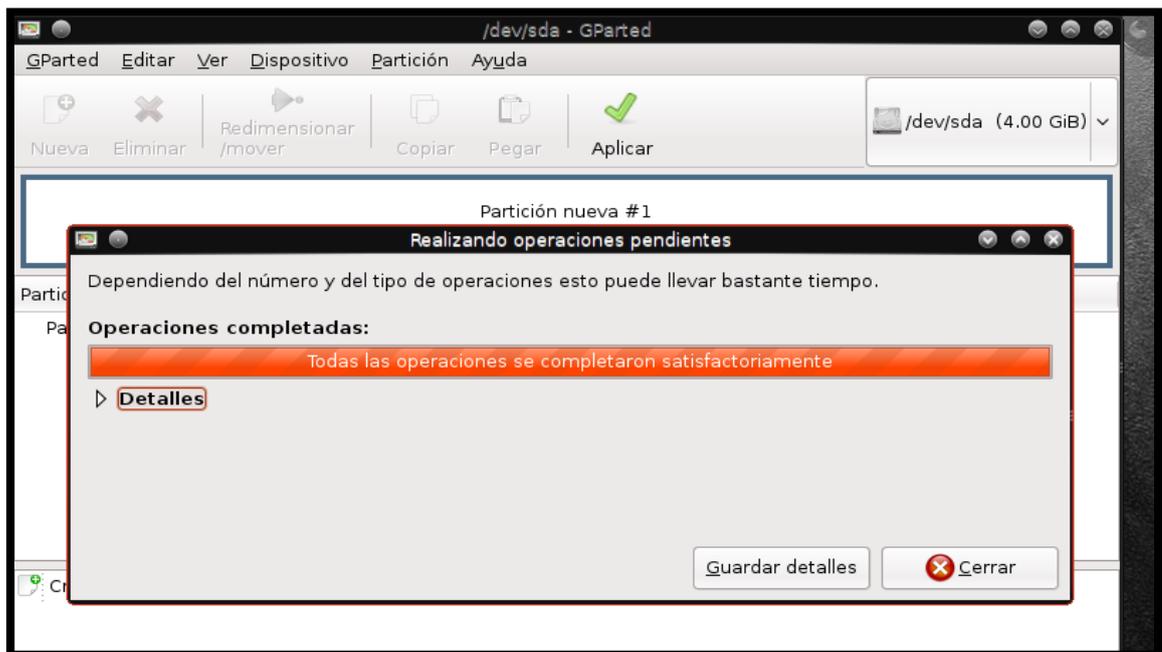
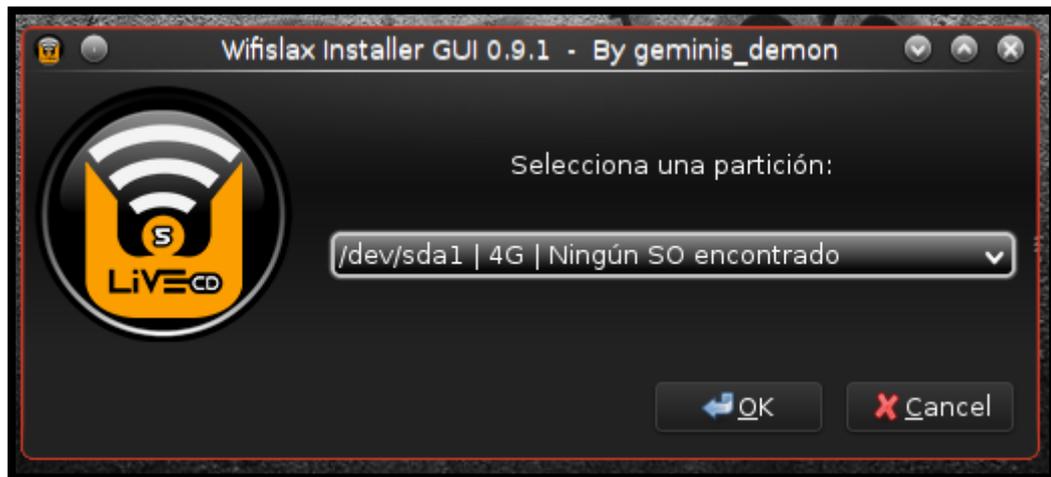
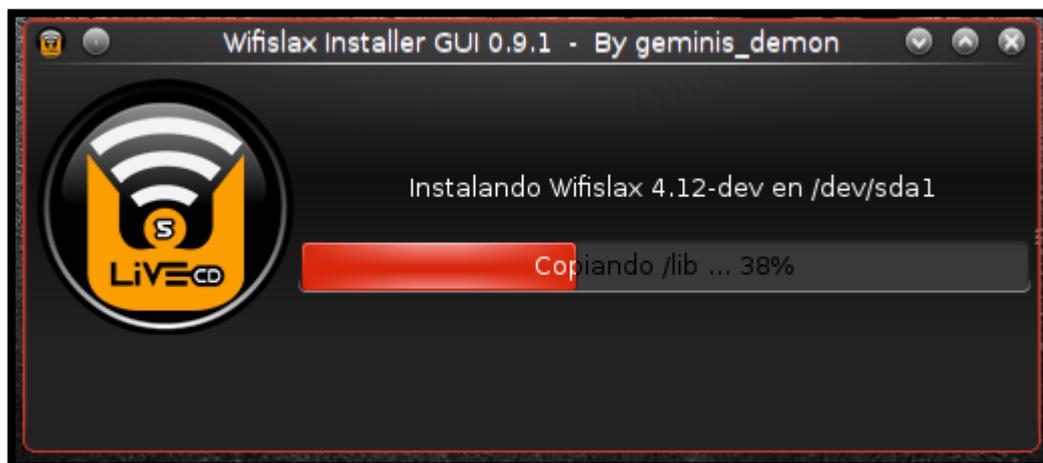


Figura 35. Descarga las operaciones que tiene el S.O.

Cerramos la ventana anterior y en el escritorio de Wifislax nos aparecerá la ventana que se muestra a continuación, donde muestra que se ha seleccionado la partición que es en donde se procederá a la instalación una vez haciendo, clic en la opción OK.



**Figura 36.** Instalación de la partición ya creada.



**Figura 37.** Instalación de Wifislax.

Una vez se culmina la instalación aparece un mensaje de confirmación que ya está completado la instalación y a continuación se instalara GRUB, que es lo que selecciona anteriormente, con este paso aparece una nueva ventana en donde se procede a seleccionar el recomendado para que se instale.

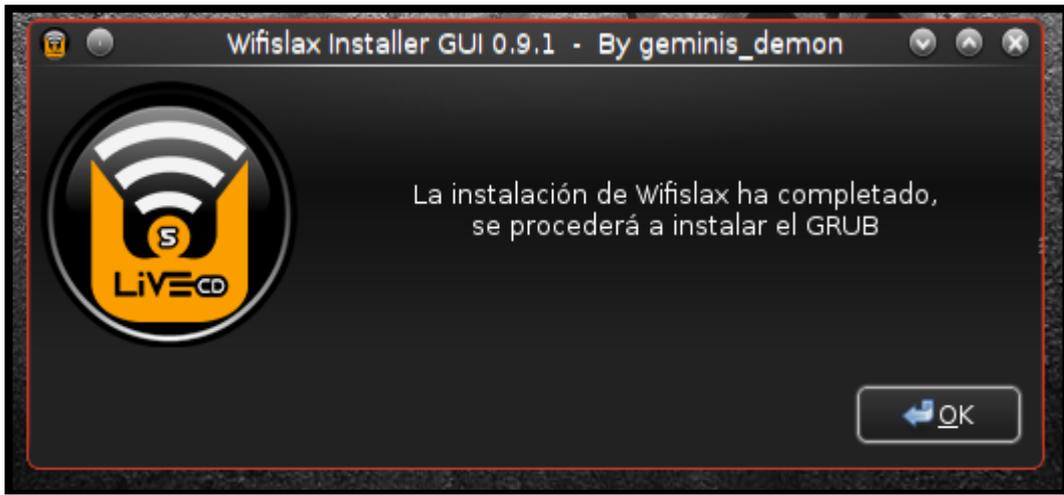


Figura 39. Instalación de el cargador de arranque.

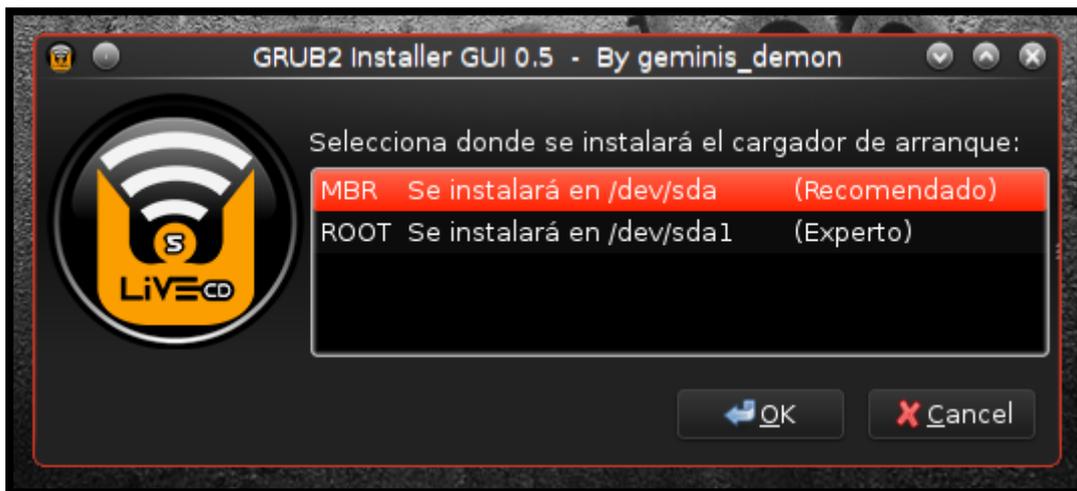
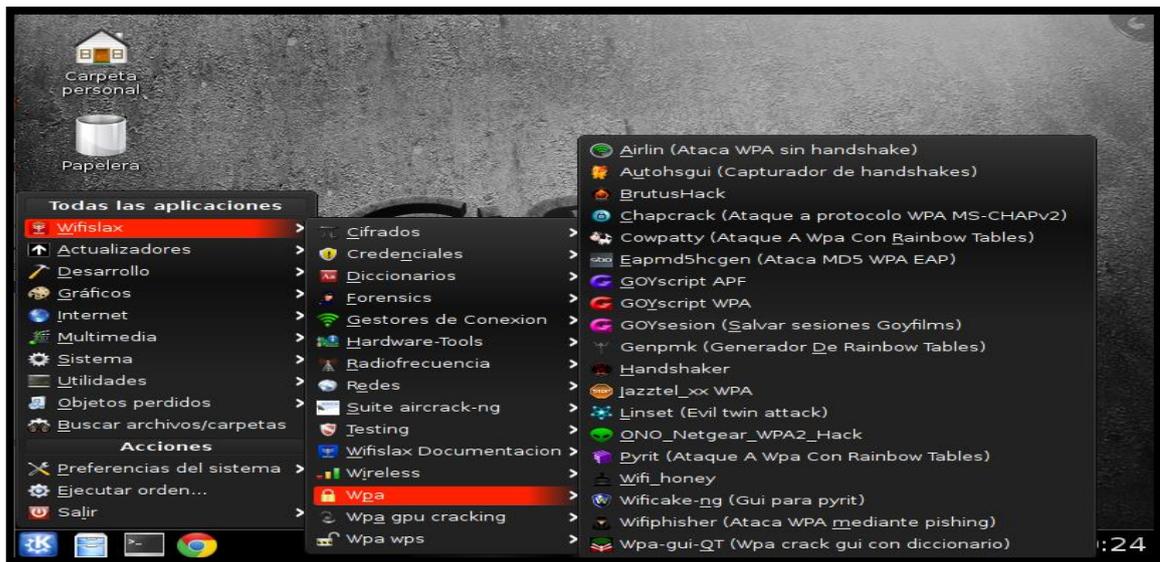


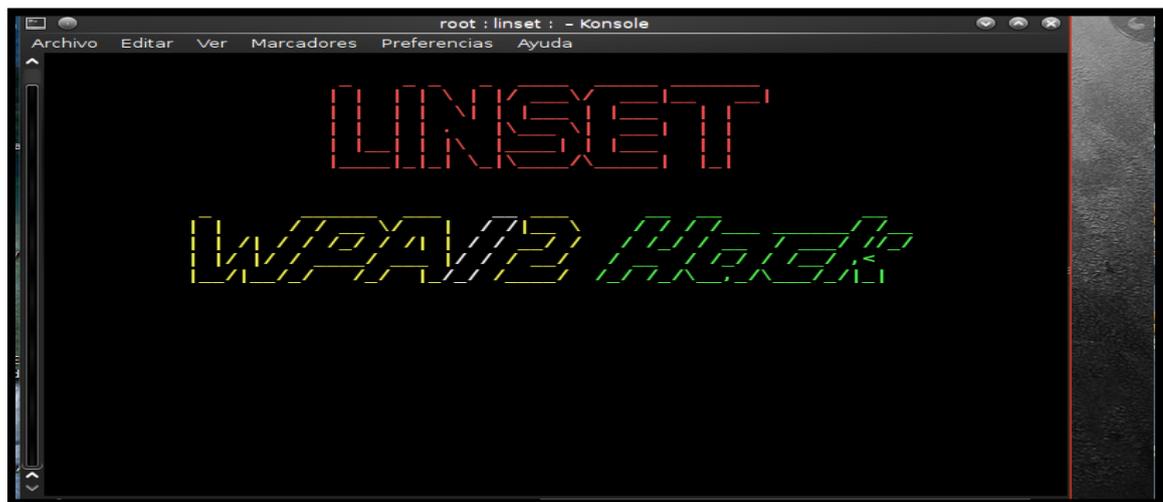
Figura 38. culminación de la instalación.

Una vez ya tenemos instalado, procedemos a hacer uso de linset que lo encontramos en el icono de inicio del sistema operativo que estamos haciendo uso en este caso Wifislax, lo encontramos en la parte inferior izquierda, damos clic y nos dirigimos hacia el icono de Wifislax → Wpa → Linset (Evil twin attack), esta herramienta es de mucha ayuda para crackear redes WPA y WPA2



**Figura 40.** Interfaz de Wifislax, se hace uso de sus herramientas.

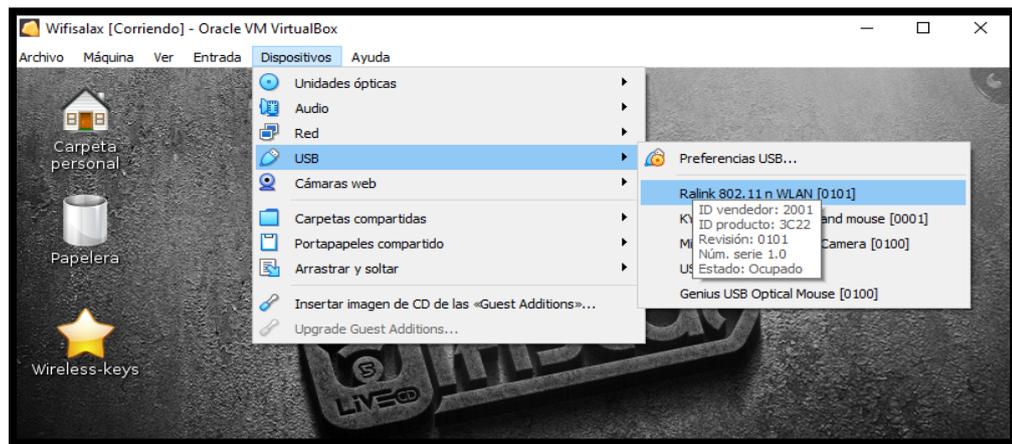
Una vez ya entrando al apartado de linset, podemos hacer el uso de sus herramientas que nos ofrece.



**Figura 41.** Inicialización de la herramienta Linset.

Antes de poder escanear las redes con la herramienta, tenemos que hacer uso de una interfaz que es la que acogerá todas las redes Wireless de la localidad, para esto los dirigiremos a la opción de dispositivos que nos da VirtualBox, para hacer uso de nuestra antena receptora de señal en esta auditoria se está haciendo uso de adaptador USB inalámbrico que está bajo los estándares 802.11 n que es con los que trabaja las redes

inalámbricas y es así como captará las señales de la localidad y en específico la red que será vulnerada.



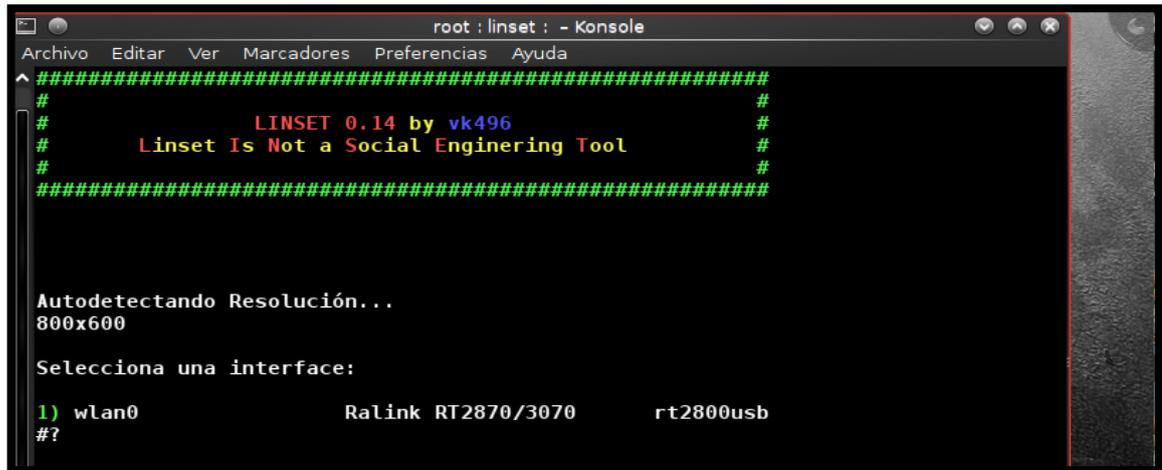
**Figura 42.** Selección del dispositivo USB inalámbrico.

Al abrir linset nuevamente ya aparece una barra que es la que indica, cierta cantidad de tiempo de espera que es lo que indica que se están cargando los paquetes y a su vez detectando la interfaz con la que se va a trabajar para la recolección de las diferentes redes con sus SSID.



**Figura 43.** Inicialización y carga de la herramienta.

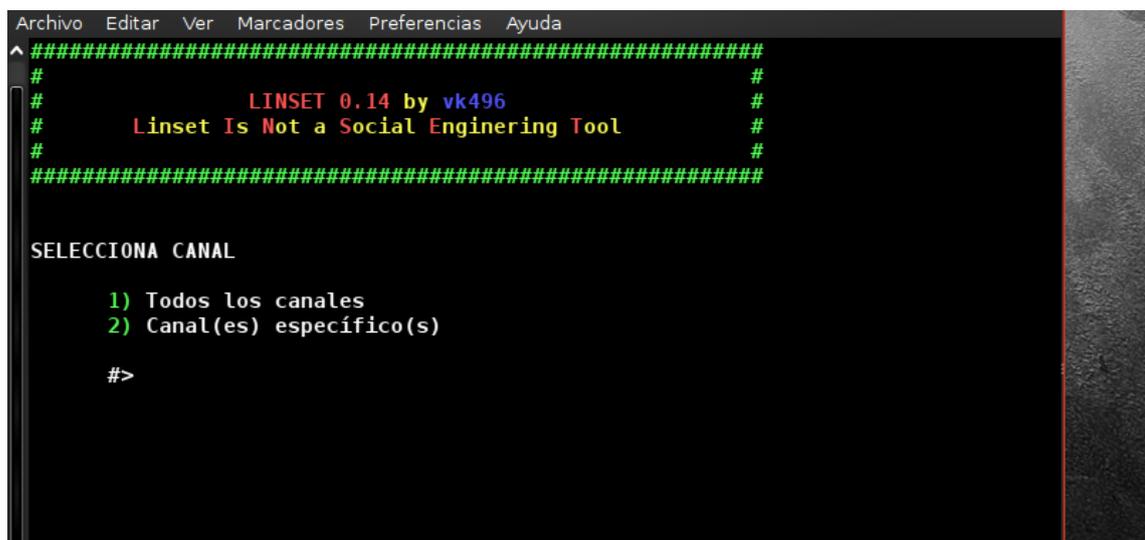
Se elige la interfaz de red que se va a utilizar para realizar es escaneo de las redes para su posterior auditoria, en este caso en excepción solo nos aparecerá una interfaz asi como se observa en el gráfico, y se escoge la opción 1.



```
root : linset : - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
^#####
#
#           LINSET 0.14 by vk496           #
#           Linset Is Not a Social Engineering Tool           #
######
Autodetectando Resolución...
800x600
Selecciona una interfaz:
1) wlan0           Ralink RT2870/3070           rt2800usb
#?
```

Figura 44. Selección de la Interfaz que permitirá ver las redes.

En este paso se elige el canal en donde se realizará el análisis para la posterior búsqueda de las redes vulnerables, hay dos opciones la de un canal en específico o uno donde analizas de manera general que se obtiene todo lo que está en el medio, seleccionamos todos los canales opción 1.



```
Archivo Editar Ver Marcadores Preferencias Ayuda
^#####
#
#           LINSET 0.14 by vk496           #
#           Linset Is Not a Social Engineering Tool           #
######
SELECCIONA CANAL
1) Todos los canales
2) Canal(es) específico(s)
#>
```

Figura 45. Selección de los canales que se analizaran.

Al haber ya escaneado en todos los canales, los aparecerá todas las redes detectadas en la tabla se muestra detalles como el BSSID, PWR que es el nivel de señal reportado por la tarjeta inalámbrica, BEACONS es el número de paquetes enviados por el AP, DATA número de datos capturados, CH número del canal que se obtiene los paquetes de beacons, HB la velocidad máxima soportada por el AP, ENC protocolos de encriptación con el que cuenta la red, se muestra también el ESSID que también se conoce como SSID, es donde se muestra la el nombre de la red, en la parte inferior se muestra las MAC de cada una de las redes asociadas.

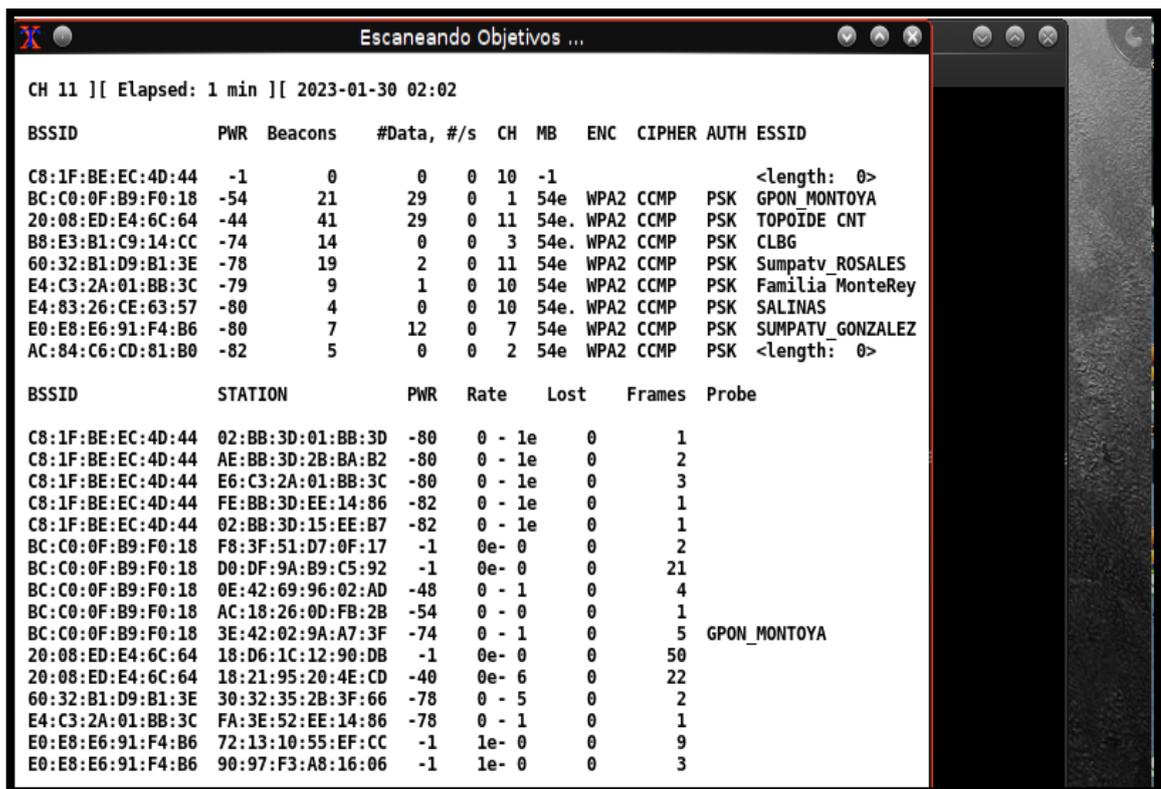


Figura 46. Escaneo de todos los probables objetivos.

Al salir de la tabla de las redes detectadas, se procede a visualizar en la ventana de linset los puntos de acceso que se encuentran disponibles y se marca con un asterisco las redes que cuentan con clientes en su red conectados, para hacer uso de esta herramienta se tiene que tomar muy en cuenta que la red a auditar debe tener al menos un cliente conectado a la red y eso debe ser hasta mucho antes desde cuando se eligen los canales.

Al ya tener la red con clientes conectados, recordar que aparecen con un asterisco las que tienen clientes, las redes salen con un identificador en este caso es un número y se procede a elegir como opción el numero de la red, seleccionamos el número 6 que es nuestra red.

```

root : linset : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^#
#          LINSET 0.14 by vk496          #
#          Linset Is Not a Social Engineering Tool          #
#          #####          #
#
#          Listado de APs Objetivo          #
#
#          #          MAC          CHAN          SECU          PWR          ESSID          #
#          1)*          C8:1F:BE:EC:4D:44          10          #          99%          #
#          2)          AC:84:C6:CD:81:B0          2          WPA2          18%          #
#          3)          E4:83:26:CE:63:57          10          WPA2          19%          SALINAS          #
#          4)*          E4:C3:2A:01:BB:3C          10          WPA2          19%          Familia MonteRey_EXT          #
#          5)*          E0:E8:E6:91:F4:B6          7          WPA2          20%          SUMPATV_GONZALEZ          #
#          6)*          60:32:B1:D9:B1:3E          11          WPA2          22%          Sumpatv_ROSALES          #
#          7)          B8:E3:B1:C9:14:CC          3          WPA2          27%          CLBG          #
#          8)*          BC:C0:0F:B9:F0:18          1          WPA2          48%          GPON_MONTOYA          #
#          9)*          20:08:ED:E4:6C:64          11          WPA2          48%          TOPOIDE CNT          #
#          10)*          80:69:33:56:2D:D0          2          #          99%          #
#
#          (*) Red con Clientes          #
#
#          Selecciona Objetivo          #
#>

```

Figura 47. Listado de los objetivos vulnerables.

En este paso ya linset lo que hace es pedir que se elija un script en donde se montara el punto de acceso fantasma o falso, el acceso falso se creara con los mismos datos de la red seleccionada tenemos varias opciones y hacemos uso de la recomendada, porque es la que nos proporciona eficacia, de esta manera de nacerá el FakeAp, que es donde los usuarios se conectarán al punto de acceso falso.

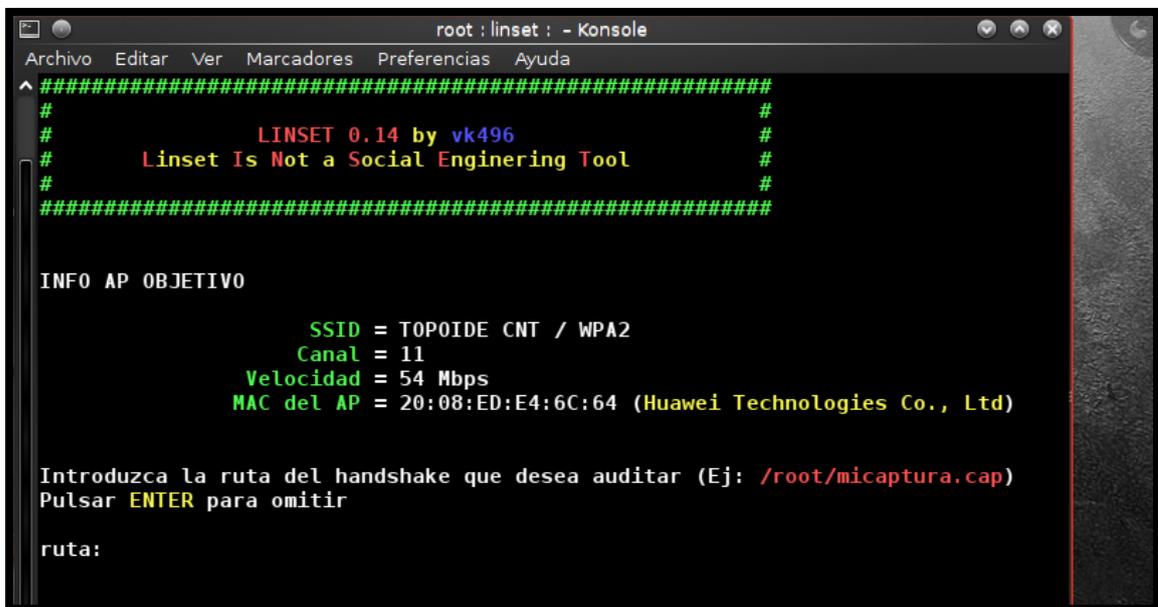
```

root : linset : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^#####
#
#          LINSET 0.14 by vk496          #
#          Linset Is Not a Social Engineering Tool          #
#          #####          #
#
#          INFO AP OBJETIVO          #
#
#          SSID = TOPOIDE CNT / WPA2          #
#          Canal = 11          #
#          Velocidad = 54 Mbps          #
#          MAC del AP = 20:08:ED:E4:6C:64 (Huawei Technologies Co., Ltd)          #
#
#          MODO DE FakeAP          #
#          1) Hostapd (Recomendado)          #
#          2) airbase-ng (Conexion mas Lenta)          #
#          3) Atras          #
#
#>

```

Figura 48. Información del objetivo a posiblemente atacar.

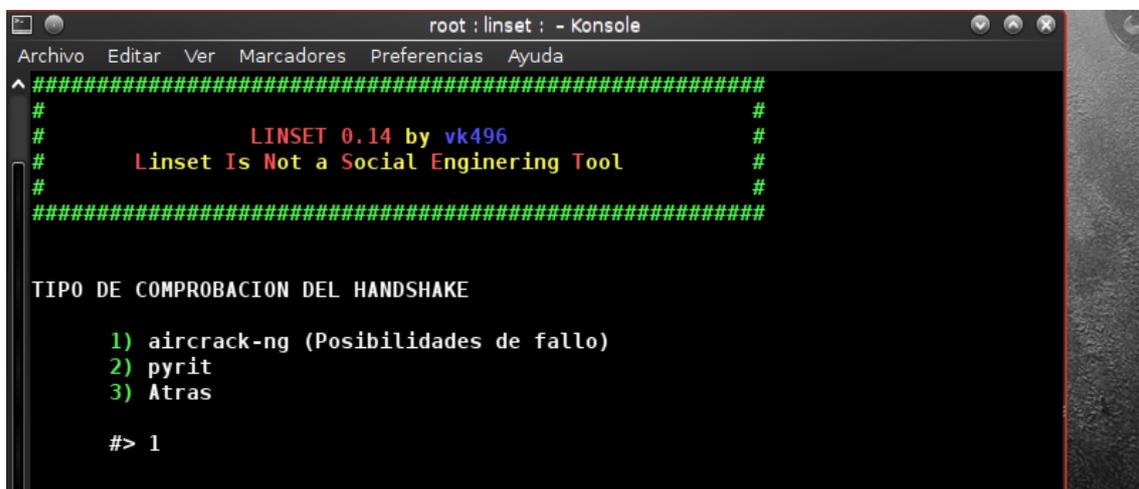
En esta parte ya linset lo que hace es solicitar una handshake en otras palabras, pide un apretón de manos o un anclaje con la red que estamos auditando usualmente no se lo tiene identificado, pero en el caso de tenerlo se lo coloca de manera directa, para este proceso solo se presiona enter y lo que hará es capturar el handshake posteriormente.



```
root : linset : - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
^#####
#
#          LINSET 0.14 by vk496          #
#    Linset Is Not a Social Engineering Tool    #
######
INFO AP OBJETIVO
          SSID = TOPOIDE CNT / WPA2
          Canal = 11
          Velocidad = 54 Mbps
          MAC del AP = 20:08:ED:E4:6C:64 (Huawei Technologies Co., Ltd)
Introduzca la ruta del handshake que desea auditar (Ej: /root/micaptura.cap)
Pulsar ENTER para omitir
ruta:
```

Figura 49. Selección de la ruta de handshake.

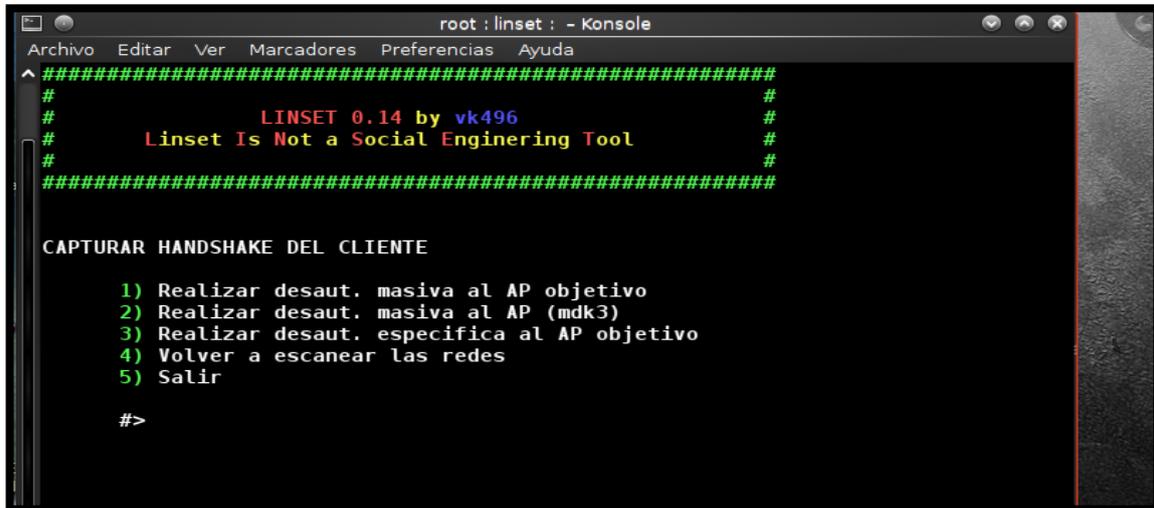
Para capturar el handshake se elegirá el tipo de examinación, que es el que lograra capturarlo siempre y cuando sigan estando clientes conectados a la red, para la captura se procede a hacer uso de la primera opción que es aircrack-ng dice que es posible a fallos, pero es muy funcional.



```
root : linset : - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
^#####
#
#          LINSET 0.14 by vk496          #
#    Linset Is Not a Social Engineering Tool    #
######
TIPO DE COMPROBACION DEL HANDSHAKE
    1) aircrack-ng (Posibilidades de fallo)
    2) pyrit
    3) Atras
#> 1
```

Figura 50. Uso de la herramienta de comprobación aircrack-ng.

Es esta parte lo que hacemos es decirle a linset, que al momento de capturar el handshake me proporcione la desconexión hacia todos los clientes que estén en la red, para poder hacer eso hacemos uso de la primera opción que logre desautenticar a todos los clientes que están conectados en la red.



```
root : linset : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^#####
#
#          LINSET 0.14 by vk496          #
#    Linset Is Not a Social Engineering Tool    #
######
#
CAPTURAR HANDSHAKE DEL CLIENTE

1) Realizar desaut. masiva al AP objetivo
2) Realizar desaut. masiva al AP (mdk3)
3) Realizar desaut. especifica al AP objetivo
4) Volver a escanear las redes
5) Salir

#>
```

Figura 51. Captura del handshake del cliente.

Linset procede a capturar el handshake, con la manera de desautenticar todos los dispositivos conectados, y el que se detecta en el ataque es el que toma el handshake al ya tenerlo escogemos la opción 1 de linset para confirmar y proseguir.



```
#
#          LINSET 0.14 by vk496          #
#    Linset Is Not a Social Engineering Tool    #
######
#
¿SE CAPTURÓ el HANDSHAKE?
Estado del handshake: Sin handshake

1) Si
2) No (lanzar ataque de nuevo)
3) No (seleccionar otro ataque)
4) Seleccionar otra red
5) Salir

#> □
```

```
Desautenticando a todos de TOPOIDE CNT
02:08:03 Waiting for beacon frame (BSSID: 20:08:ED:E4:6C:64) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
02:08:03 Sending DeAuth to broadcast -- BSSID: [20:08:ED:E4:6C:64]
02:08:03 Sending DeAuth to broadcast -- BSSID: [20:08:ED:E4:6C:64]
02:08:04 Sending DeAuth to broadcast -- BSSID: [20:08:ED:E4:6C:64]
02:08:05 Sending DeAuth to broadcast -- BSSID: [20:08:ED:E4:6C:64]
```

Figura 52. Captura del handshake para establecer conexión.

```

root : linset : - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
^#####
#
#                               Linset Is Not a Social Engineering Tool
#
#####
¿SE CAPTURÓ el HANDSHAKE?
Estado del handshake:
1) Si
2) No (lanzar ataque)
3) No (seleccionar canal)
4) Seleccionar interfaz
5) Salir
#>

```

```

Capturando datos en el canal --> 11
CH 11 ][ Elapsed: 1 min ][ 2023-01-30 02:08 ][ WPA handshake: 20:08:ED:E4:6C:64
BSSID          PWR RXQ Beacons  #Data, #/s  CH MB  ENC  CIPHER AUTH ESSI
20:08:ED:E4:6C:64 -52 100    731    12056   4 11  54e. WPA2 CCMP  PSK  TOPO
BSSID          STATION            PWR  Rate  Lost  Frames  Probe
20:08:ED:E4:6C:64 18:21:95:20:4E:CD -38  0e- 0e   4    11856 TOPOIDE CNT
20:08:ED:E4:6C:64 18:D6:1C:12:90:DB -60  1e- 1   0     281

```

Figura 53. Captura del canal de datos, handshake.

Ya capturado el handshake, se tiene que escoger el tipo de interfaz que será mostrada posteriormente al usuario para que mediante este método proceda introducir la contraseña, seleccionamos la interfaz neutra.

```

root : linset : - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
^#####
#
#                               LINSET 0.14 by vk496
#                               Linset Is Not a Social Engineering Tool
#
#####
INFO AP OBJETIVO
      SSID = TOPOIDE CNT / WPA2
      Canal = 11
      Velocidad = 54 Mbps
      MAC del AP = 20:08:ED:E4:6C:64 (Huawei Technologies Co., Ltd)
SELECCIONA LA INTERFACE WEB
1) Interface web neutra
2) Salir
#?

```

Figura 54. Selección de la interfaz al cliente.

Al seleccionar la interfaz se muestra seguidamente varias opciones de idioma en que se podrá mostrar la interfaz web anteriormente seleccionada, esta interfaz es la que se mostrará al momento de que se trate de establecer la conexión, la misma se mostrará en dispositivos móviles o computadoras, esto servirá para capturar el password de la red, seleccionamos la opción 2.

```
root : linset : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^#####
#
#          LINSET 0.14 by vk496          #
#          Linset Is Not a Social Engineering Tool          #
#
######

INFO AP OBJETIVO

          SSID = TOPOIDE CNT / WPA2
          Canal = 11
          Velocidad = 54 Mbps
          MAC del AP = 20:08:ED:E4:6C:64 (Huawei Technologies Co., Ltd)

SELECCIONA IDIOMA

1) English      [ENG]
2) Spanish      [ESP]
3) Italy         [IT]
4) French       [FR]
5) Portuguese   [POR]
6) Atras

^#?
```

Figura 55. Selección del idioma que tendrá la interfaz.

Con todos los pasos y opciones que llevamos ya seleccionando desde antes, tenemos ya toda la información de la red recopilada ya se puede lanzar ataque de manera que se pueda lograr capturar la contraseña de su red, al momento de iniciar el ataque se despliegan varias ventanas en donde aparecen servidores alzados como DHCP, DNS, la desautenticación que se realiza mediante mdk3, el estado del punto de acceso que se a montado con los mismos detalles de la red idéntica, en una de las ventanas podemos

observar el tráfico del dispositivo que se está anclando a la red falsa o fantasma que se crea.

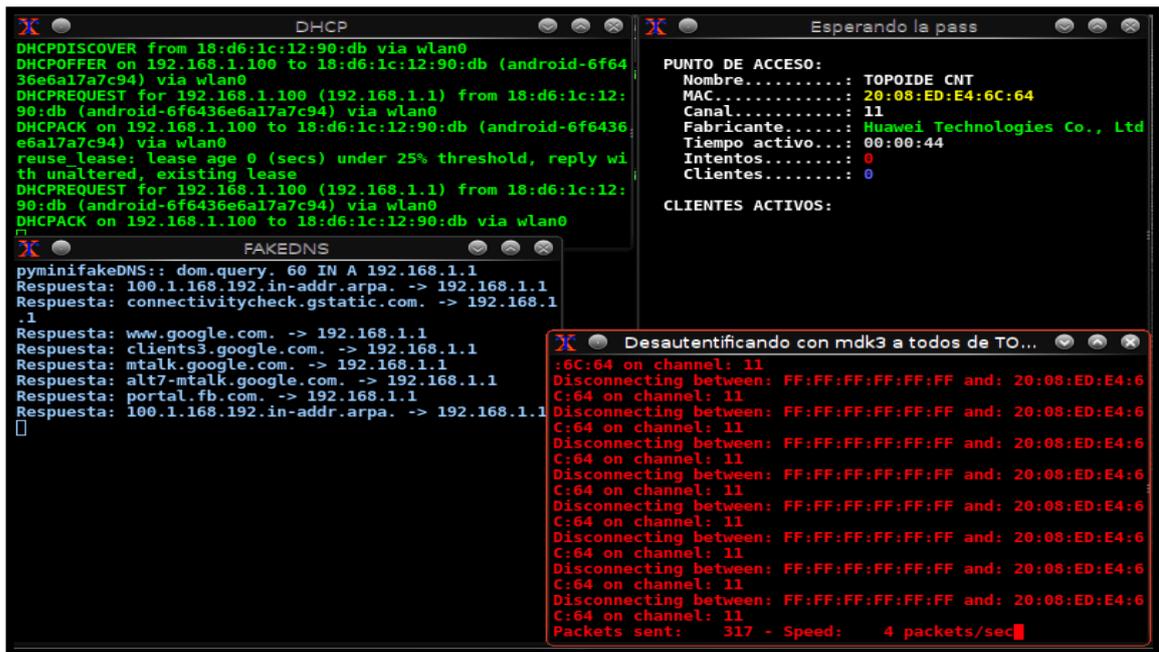


Figura 56. Se realiza el ataque y se desactivan los servicios.

Una vez lanzamos el ataque, se nos corta la conectividad de la red segura, y aparece una red de wifi con el mismo nombre, pero de manera abierta que es donde ya linset ha cometido tu ataque que es de poder crear la red para mediante esto poder sacar la contraseña.



Figura 57. Red que se creó para la obtención de acceso.

Identificando el móvil con el que se captó la red en el paso anterior, cuenta como uno de los clientes conectados dentro de esta red en la captura se evidencia en el aparatado de esperando la pass, es donde te arroja la cantidad de clientes conectados.

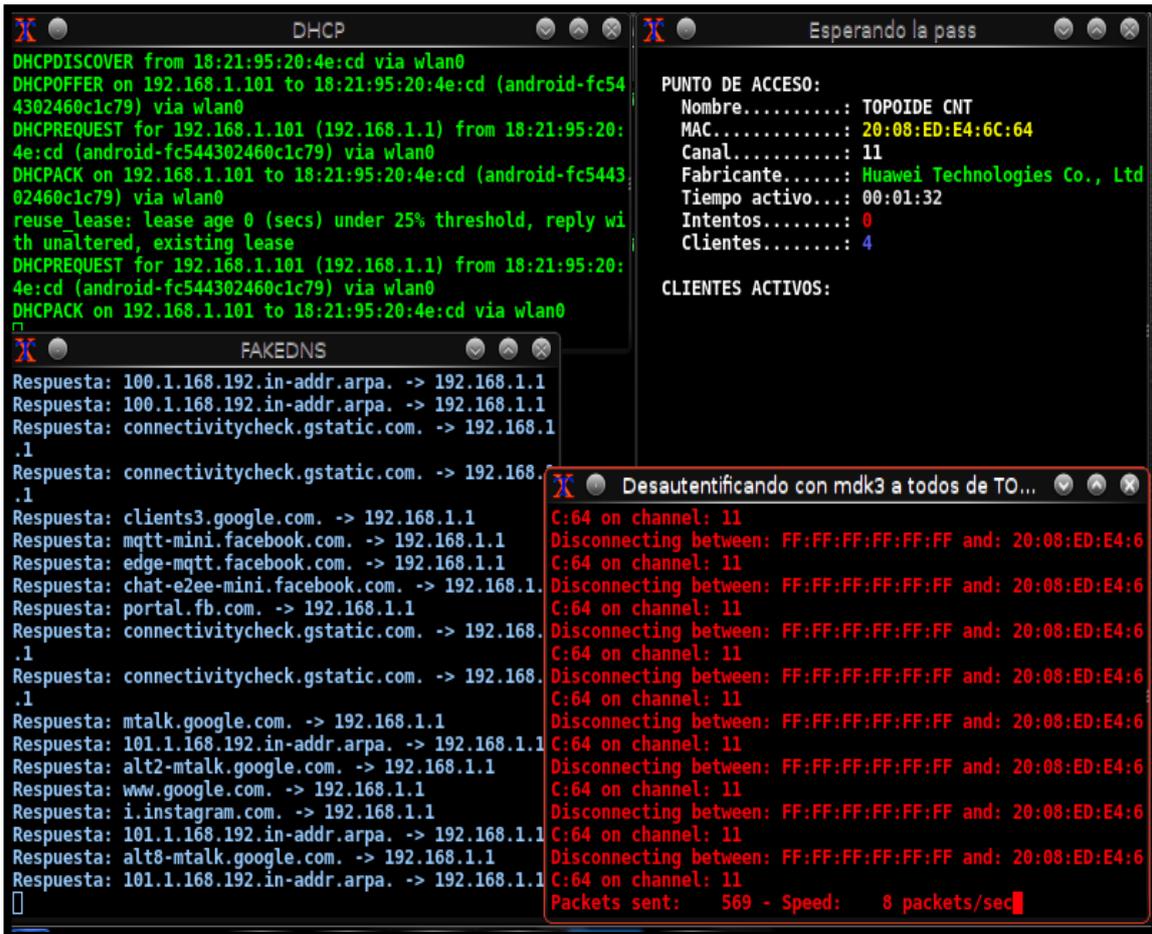
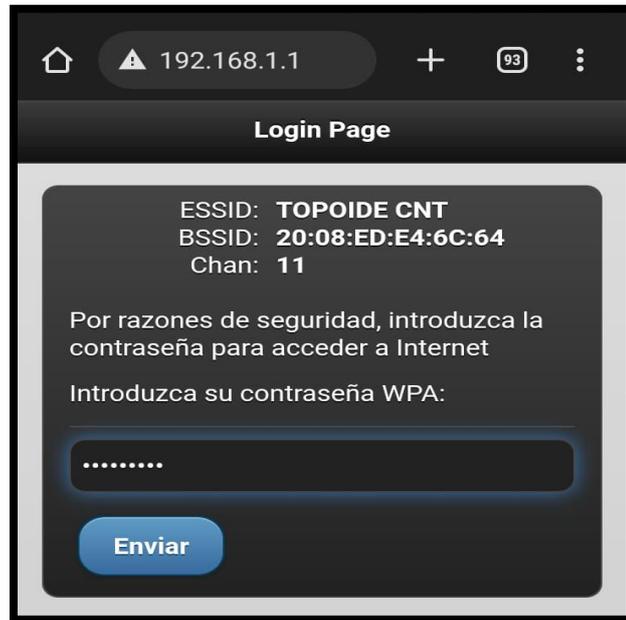


Figura 58. Visualización de todo el tráfico y dispositivos conectados a la red.

Nos dirigimos hacia opciones avanzadas de la red, para que permita desplegar los datos de la red así como se muestra en la imagen, nos dirigimos hacia una página web para que se pueda hacer uso de la aparentemente red que nos estamos conectando, de esta manera la ventana de donde se muestra los clientes conectados se ha capturado la dirección IP del dispositivo el cual será la víctima para que coloque la contraseña posteriormente.

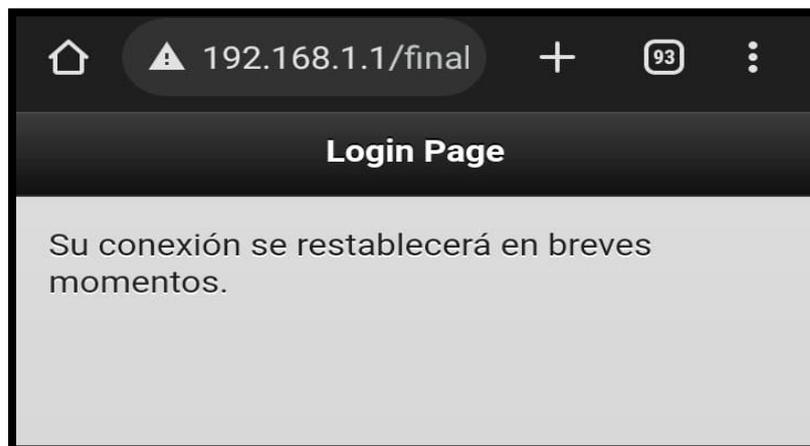


Al entrar a la opción del sitio web para hacer uso de la red, se nos abrirá en el navegador la interfaz que hemos creado en los pasos anteriores en donde pide que se introduzca la contraseña para que se pueda tener conectividad con el internet.



**Figura 61.** Interfaz del punto falso creado.

Una vez ingresada la contraseña y enviada sale una opción que se muestra un mensaje así como se metra a continuación en la imagen.



**Figura 62.** Mensaje después de obtener las credenciales.

Al ya mostrar el mensaje anteriormente, en la interfaz donde se esperaba que se conecte los clientes ya cambia totalmente y se muestra así como en la imagen, en donde saca la contraseña de la red y el master key, una vez acabado el ataque automáticamente se restablece la conexión con norma



```
Esperando la pass
Aircrack-ng 1.2 r
c2 r2701
[00:00:00] 1 keys tested (915.7
5 k/s)
KEY FOUND! [ topoideDH
]H
Master Key      : AB FD F4 89 44 66 4B 0C C2
B2 50 A5 3E FB 35 C7      30 5D 3D 1A 7B 69 2F DE 05
46 25 Transient Key : 26 9B CA 60 63 6B 9F EF B8
E8 48 F8 0A B9 E6 86      73 43 FA BC F0 BD 86 FB A9
F4 F8 25 7A 73 17 89      51 53 62 3C C5 A8 9F 30 6B
C3 09 EAPOL HMAC    : 94 C5 4C 16 00 58 F2 8C 7B
DC EC 15 03 AA 7F 4E      52 44 B3 3E 43 5E C5 55 7D
83 E1 02 E4 4F 90 B0
Se ha guardado en /root/TOPOIDE CNT-password.txt
```

Figura 63. Resultado final de la obtención de las credenciales.