UNIVERSIDAD ESTATAL
PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA TECNOLOGÍAS DE LA INFORMACIÓN

TITULO DE TRABAJO DE TITULACIÓN

"Auditoría en Redes WIFI domésticas utilizando Herramientas Open Source de Computación Forense con Metodología PTES en tres puntos geolocalizados en la Península de Santa Elena"

AUTOR

FIGUEROA RODRÍGUEZ MARCOS COLANI

EXAMEN COMPLEXIVO

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

PROFESOR TUTOR :

ING. HAZ LÓPEZ LÍDICE MSI.

Santa Elena -ECUADOR

2024

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACÍON

Ing. José Sánchez A. Msc.
DIRECTOR DE LA CARRERA

Ing. Lídice Victoria Haz López, Msi
TUTOR

Lsi. Daniel Quirumbay, Msia.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel S. Mgti.
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 **FIGUEROA RODRÍGUEZ MARCOS COLANI** , como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 18 días del mes de junio del año 2024

TUTOR

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

ING. LIDICE VICTORIA HAZ LÓPEZ, Msi.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **FIGUEROA RODRÍGUEZ MARCOS COLANI**

DECLARO QUE:

El trabajo de Titulación, "**Auditoría en Redes WIFI domésticas utilizando Herramientas Open Source de Computación Forense con Metodología PTES en tres puntos geolocalizados en la Península de Santa Elena** " 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.

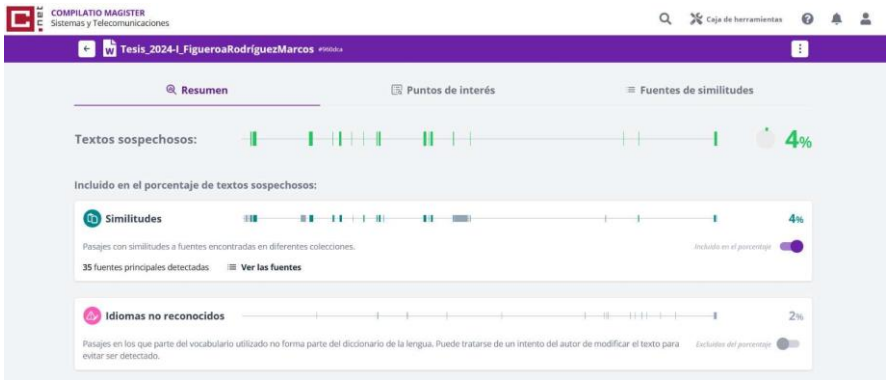
La Libertad, a los 18 días del mes de junio del año 2024

EL AUTOR

Marcos Colani Figueroa Rodríguez

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 "**Auditoría en Redes WIFI domésticas utilizando Herramientas Open Source de Computación Forense con Metodología PTES en tres puntos geolocalizados en la Península de Santa Elena",** presentado por el estudiante, **FIGUEROA RODRÍGUEZ MARCOS COLANI** fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 4%, por lo que se aprueba el trabajo para que continúe conel proceso de titulación.

TUTOR

Firmado electrónicamente por:
LIDICE VICTORIA HAZLOPEZ

ING. LIDICE VICTORIA HAZ LÓPEZ, Msi.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **FIGUEROA RODRÍGUEZ MARCOS COLANI**

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 18 días del mes de junio del año 2024

EL AUTOR

Marcos Colani Figueroa Rodríguez

AGRADECIMIENTO

En primer lugar , agradecer a Dios por darme la fortaleza y sabiduría necesarias para completar esta etapa de mi vida.

A mi familia , especialmente a mis padres ,por su amor incondicional , apoyo y sacrificio que ha sido constante a lo largo de mi formación la que ha sido fuente de motivación.

A la Facultad de Sistemas y Telecomunicación en especial a la carrera de Tecnologías de la Información por permitirme formar de manera profesional.

El respeto y agradecimiento a mi tutora Ing. Haz López Lídice. Msi, por haber compartido conmigo su conocimiento, consejos y experiencias para mi crecimiento personal y profesional, así como a todos mis profesores de la carrera de Ingeniería de Tecnologías de la Información.

Marcos Colani Figueroa Rodríguez.

DEDICATORIA

Dedico este trabajo a mis padres y hermanos , por su amor infinito e incondicional a lo largo de este camino arduo pero gratificante para alcanzar este logro , sus palabras y su fe en mí han impulsado a seguir a delante.

Me dedico a mí mismo , en reconocimiento al esfuerzo a pesar de los obstáculos, este trabajo es un reflejo de mi capacidad para enfrentar y superar dificultades.

“Jamás lo olvides que cualquier meta es alcanzable”.

Marcos Colani Figueroa Rodríguez

INDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la era digital actual, la seguridad de las redes inalámbricas es crucial para usuarios y organizaciones. Las redes WiFi domésticas son particularmente vulnerables a amenazas que comprometen la privacidad y seguridad de datos personales. Este proyecto audita redes WiFi domésticas usando herramientas de computación forense de código abierto y la metodología PTES. La investigación se centra en tres ubicaciones de la Península de Santa Elena: Salinas, La Libertad y Santa Elena.

El objetivo principal es identificar y evaluar vulnerabilidades en los protocolos de seguridad como WEP, WPA, WPA2 y WPA3. A través de hacking ético, se busca descubrir brechas de seguridad y probar herramientas forenses de código abierto para obtener y desencriptar claves de acceso. Esta investigación proporciona un análisis detallado de las debilidades en configuraciones de seguridad y recomendaciones prácticas para mejorar infraestructuras. Con el aumento de dispositivos conectados, proteger las redes WiFi es prioritario.

Este estudio contribuye al campo de la seguridad informática, mostrando cómo técnicas y herramientas pueden proteger redes inalámbricas domésticas. Además, guía a usuarios y profesionales para fortalecer la seguridad de sus redes con conocimientos prácticos basados en pruebas reales.

RESUMEN

El presente proyecto se llevó a cabo en entornos controlados y con la debida autorización. El estudio se centra en la detección de vulnerabilidades en los protocolos de seguridad WEP, WPA, WPA2 y WPA3 en redes inalámbricas. Las zonas de análisis fueron cuidadosamente seleccionadas y geolocalizadas en tres puntos específicos de la Península de Santa Elena: Salinas, La Libertad y Santa Elena. El objetivo principal es evaluar tanto las vulnerabilidades presentes en estos protocolos de seguridad como la eficacia de las herramientas empleadas para la obtención y desencriptación de claves de acceso a dichas conexiones.

En conformidad con lo expuesto previamente, el proyecto desarrollado implementó una auditoría en las redes inalámbricas mencionadas mediante la aplicación de una metodología adaptativa de hacking ético conocida como PTES y herramientas Open Source la cual también fueron seleccionas por su popularidad en este tipo de técnicas de instrucción.

El resultado esperado en este tipo de pruebas y el empleo de técnicas de hacking , es la obtención de informacion de claves wifi, por lo tanto, validaremos positivamente las pruebas, lo que permitirá proporcionar sugerencias y recomendaciones detalladas para mitigar las vulnerabilidades identificadas. Estas recomendaciones incluirán la implementación de medidas de seguridad avanzadas y prácticas óptimas para fortalecer la infraestructura de las redes auditadas.

Palabras claves: Redes Wifi , vulnerabilidad ,WEP,WPA ,WPA2, ciberseguridad, Wlan.

ABSTRACT

This project was conducted in controlled environments and with proper authorization. The study focuses on detecting vulnerabilities in WEP, WPA, WPA2, and WPA3 security protocols in wireless networks. The analysis areas were carefully selected and geolocated in three specific points of the Santa Elena Peninsula: Salinas, La Libertad, and Santa Elena. The primary objective is to evaluate both the vulnerabilities present in these security protocols and the effectiveness of the tools used for obtaining and decrypting access keys to these connections.

In accordance with the previously stated objectives, the project implemented an audit of the aforementioned wireless networks by applying an adaptive ethical hacking methodology known as PTES (Penetration Testing Execution Standard) and Open-Source tools, which were also selected for their popularity in such instructional techniques.

The expected outcome of these tests and the use of hacking techniques is the acquisition of WiFi key information, thereby positively validating the tests. This will allow for providing detailed suggestions and recommendations to mitigate the identified vulnerabilities. These recommendations will include the implementation of advanced security measures and best practices to strengthen the infrastructure of the audited networks.

Keywords: WiFi networks, vulnerability, WEP, WPA, WPA2, cybersecurity, Wlan.

1.FUNDAMENTACIÓN

1.1 ANTECEDENTES

Las redes inalámbricas aumentan la flexibilidad en el hogar, en el lugar de trabajo y en la comunidad al permitir la conexión a Internet sin estar atados a una ubicación específica. En los últimos años, las redes inalámbricas han experimentado un rápido aumento en popularidad. También ha habido un cambio en el uso de Internet por parte de los usuarios. Los usuarios domésticos han adoptado la tecnología inalámbrica y las empresas la ven como un factor que tiene un gran impacto en su eficiencia operativa. Tanto los usuarios domésticos como la industria están enviando información cada vez más sensible a través de estas redes inalámbricas, ya que la prestación en línea de servicios bancarios, comerciales y gubernamentales se vuelve más extendida.

Pese a los innegables beneficios de las redes inalámbricas, existen riesgos adicionales que no existen en las redes cableadas. Es imperativo que las empresas y los usuarios domésticos realicen una evaluación y gestión adecuada de los riesgos. Este artículo revisa los protocolos de redes inalámbricas, investiga cuestiones de confiabilidad, disponibilidad y seguridad al utilizar redes inalámbricas [1]. El enfoque de utilizar e implementar redes inalámbricas seguras es una práctica común y efectiva en el campo de la seguridad informática y las redes.

La aparición de la informática y el uso de comunicaciones digitales han ocasionado muchos problemas de seguridad contra los que se ha aprendido a lidiar con distintas técnicas e incluso buenas prácticas o políticas que se deben seguir. En el pasado existía un cifrado clásico con el que se cambiaban algunas letras de frases a cifrar por otras letras, números o combinaciones; al no ser suficientes, los criptógrafos investigaron y debido a los avances en la matemática y la tecnología se ha logrado obtener algoritmos mucho más seguros[1].

Aunque no lo parezca, la criptografía no es solo una cuestión de informáticos; por el contrario, suele formar cada vez más parte de nuestra vida cotidiana, ya que a diario usamos claves para producir la salida funcional de algoritmos criptográficos, que en palabras simples significa que usamos claves para verificar si estamos o no autorizados para acceder a algún servicio o sistema. Pero aun cuando este tema parezca tan sencillo, existe toda una psicología detrás, como también criterios que deben tomarse en cuenta para proteger nuestra información y más detalles que muchas veces pasamos por alto y

que de reparar en ello nos permitiría tener menos casos de robo y/o infiltración de información[1].

Una de las tecnologías más ampliamente utilizadas en la actualidad es el Wi-Fi, que permite la comunicación inalámbrica entre nuestros dispositivos. Su creciente popularidad se debe a su creciente disponibilidad y facilidad de uso. La mayoría de los pasos de conexión se realizan automáticamente en segundo plano en los dispositivos del usuario, lo que implica que estos almacenan de forma automática los datos necesarios, como el nombre de la red (SSID) y la contraseña, para una futura conexión. Esto significa que cuando se encuentran nuevamente con una red conocida, la reconexión puede llevarse a cabo sin intervención manual[2]. Conlleva riesgos muy altos ya que dispositivos muchas veces pueden conectarse de forma automática en redes pacificadas o creadas por personas malintencionadas o atacantes que utilicen SSID muy parecido al original o muchas veces falso[2].

La seguridad de las redes inalámbricas es un aspecto muy importante hoy en día, por ello se debe tener en cuenta que el avance de la tecnología y las amenazas informáticas se desarrollan simultáneamente para comprometer información confidencial de las empresas u organizaciones. Este proyecto tiene como objetivo sugerir una herramienta para realizar auditorías de seguridad inalámbrica.
Hay aspectos que no se toman en cuenta en una auditoria, y el esquema que se detalla en este documento deja claro que una red inalámbrica con encriptación WPA y WPA2, es vulnerable a una variedad de ataques. Esta investigación propone un ataque tipo phishing en donde se consigue engañar a los usuarios autorizados para que revelen información que compromete la integridad del sistema. La sugerencia de la herramienta Linset en este proyecto de titulación también busca recomendar a los usuarios sobre las medidas de seguridad que se deben tener en cuenta al configurar una red inalámbrica y el establecimiento de contraseñas seguras [3].

Las mayores amenazas a la seguridad de las empresas en 2013 dependerán de quién esté atacando el negocio: los delincuentes oportunistas seguirán buscando cuentas con contraseñas predeterminadas o débiles, mientras que los atacantes específicos perfeccionarán sus intentos de engañar a los empleados, a la empresa de servicios empresariales Verizon y a la empresa de software de seguridad McAfee. indicado en informes separados. El año pasado, alrededor del 90 por ciento de las infracciones exitosas analizadas por Verizon comenzaron con una contraseña débil o predeterminada,

o una credencial robada y reutilizada, lo cual es una tendencia que continuará, dijo Wade Baker, director gerente del equipo de RIESGO de la compañía. La empresa analizó los datos recopilados de los incidentes que investigó en 2012 para identificar las causas de las violaciones de datos [4].

En base a todo lo mencionado sobre los riesgos un entorno académico, empresarial y doméstico, donde la información y la comunicación son esenciales para el aprendizaje y la colaboración, la seguridad de las redes Wi-Fi adquiere un papel central en garantizar la privacidad y la integridad de los datos compartidos y transmitidos en la institución la información confidencial. Es necesario analizar las vulnerabilidades de la entidad la falta de seguridad a nivel de contraseñas mediante la aplicación de Computación Forense, técnicas de Hacking Ético y el uso de Software libres y gratuitas de ciberseguridad evitando posibles infiltraciones a la red.

1.2 DESCRIPCIÓN DEL PROYECTO

El proyecto consiste en realizar una auditoría de redes Wi-Fi para evaluar las amenazas y vulnerabilidades de la red. Para lo cual, se aplicó la metodología PTES Penetration Testing Execution Standard (Estándar de Ejecución de Pruebas de Penetración), desarrollada de forma sistemática para identificar y evaluar las vulnerabilidades de los sistemas informáticos. Se utilizan herramientas gratuitas como Wifi Slax O.S., Aircrack-Ng y Linset. Las pruebas de seguridad se realizan en entornos controlados, geolocalizados en tres puntos de la provincia de Santa Elena utilizando redes inalámbricas de tipo doméstica, con el objetivo de evaluar el nivel de riesgo mediante el análisis de vulnerabilidades de los protocolos de seguridad identificadas y el impacto que se genera sobre la confidencialidad, integridad y disponibilidad de la información.

Las técnicas de seguridad informática que se utilizaron fueron la captura de paquetes, ruptura de contraseñas, la inyección de tráfico, saturación de ancho de banda, y el análisis de la calidad de la señal. Los resultados fueron presentados mediante un informe detallado de las vulnerabilidades encontradas en cada red. Por último, se propone un conjunto de buenas prácticas y recomendaciones que permitan evaluar los riesgos encontrados según el análisis realizado. En base a lo mencionado durante el proyecto se tiene como referencia las siguientes fases: Recopilación de informacion, análisis de vulnerabilidades, explotación y el informe correspondiente.

- **Recopilación de informacion:** Una de las primeras fases para realizar pruebas donde se recopila toda la información necesaria del lugar y objetivo o del sistema de la auditoria
- **Análisis de vulnerabilidades:** Esta etapa se refiere a la búsqueda de vulnerabilidades basado en la información encontrada en la fase de reconocimiento
- **Explotación:** Lo cual en esta etapa donde la información es recopilada de las vulnerabilidades encontradas para hacer explotadas y tener acceso a la red o al sistema
- **Presentación de informe:** Consiste en documentar todos los resultados y las pruebas realizadas una vez concluida dichas prácticas para mostrar las mejores recomendaciones o resultados de la investigación

En el proyecto se utilizaron herramientas o recursos informáticos de tipo hardware y software tales como:

- **VirtualBox :** Oracle VM VirtualBox, el software de virtualización multiplataforma de código abierto más popular del mundo, permite a los desarrolladores entregar código más rápido, ya que pueden ejecutar múltiples sistemas operativos en un solo dispositivo[5].

- **Kali Linux :** Kali Linux es una distribución de Linux de código abierto basada en Debian orientada a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa[6].
- **Nmap**: Nmap ('Network Mapper') es una utilidad gratuita y de código abierto para el descubrimiento de redes y la auditoría de seguridad. Muchos administradores de redes y sistemas también lo encuentran útil para tareas como el inventario de la red, la gestión de cronogramas de actualización de servicios y el monitoreo del tiempo de actividad del host o del servicio [7].

- **Aircrack:** es una suite de software de seguridad inalámbrica. Consiste en un Analizador de paquetes de redes, recupera contraseñas WEP Y WAP/WPA2-PKS y otro conjunto de herramientas de auditoría inalámbrica [8].

- **Wifi Slax OS:** WiFi Slax es una distribución GNU/Linux en formato *.iso basada en Slackware con funcionalidades de LiveCD y LiveUSB pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general[9].
- **Wireshark:** Wireshark es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para análisis de datos y protocolos, y como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos de forma únicamente hueca[10].
- **Adaptador de Red:** Un adaptador de red es un hardware que te permite enlazar a varios ordenadores entre ellos con el fin de enviar y recibir documentos, fotos o archivos, discos duros, impresoras, entre otros [11].

1.3 OBJETIVOS DEL PROYECTO

Objetivos General

Evaluar las redes WIFI domesticas en entornos controlados mediante herramientas Open Source de computación forense para el análisis de los protocolos de seguridad.

Objetivos Específicos

- Describir el funcionamiento de los protocolos de comunicación de las redes wifi mediante un análisis bibliográfico.
- Identificar las vulnerabilidades en las redes wifi aplicando técnicas de Ethical hacking para evaluar el nivel de seguridad informática en dichas redes.
- Elaborar un reporte de las vulnerabilidades encontradas incluyendo recomendaciones basadas en normas internacionales de seguridad informática que permitan minimizar los riesgos identificados.

1.4 JUSTIFICACIÓN DEL PROYECTO

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas para tener calidad es imprescindible una conexión física al cable de la red acceso a una red, sin embargo, en una red inalámbrica cableada desde un hogar, un tercero puede acceder a la red sin ni siquiera estar ubicado dentro del hogar, bastaría con que estuviera en un lugar próximo donde le llegara la señal. Es más, en el caso de un

ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior[12].

Las redes domésticas son redes vulnerables debido a los ataques informáticos que no dejan de ser expuestas por simples configuraciones de fabrica como pueden ser una contraseña sólida, uso de un buen firewall, limitar el acceso a dispositivos desconocidos, una Whitelists (lista de direcciones IP designadas a los dispositivos), dados a estos posibles casos mencionados se aplica la seguridad de la informacion de los datos lo cual podría suponer una vulnerabilidad si no lo llegaran a tener.

Debido al aumento de las redes domésticas cada Router, cada configuración es diferente el estado actual de la seguridad de las redes Wi-Fi, que recientemente se han visto cuestionadas por el descubrimiento de nuevas vulnerabilidades, se expondrán conceptos básicos de este tipo de redes y analizarán los protocolos de seguridad actuales existentes para protegerlas. Posteriormente se estudiarán las principales vulnerabilidades existentes en los protocolos de seguridad, analizando en detalle los recientes ataques KRACK contra los protocolos WPA/WPA2 y los ataques del tipo EVIL TWIN que son muy difíciles de evitar [13]. Hoy en día el descubrimiento de vulnerabilidades en este tipo de redes es común encontrarlas debido a que, en su mayoría dichas redes tienen las configuraciones por defecto del fabricante o del ISP.

Por esta razón, es importante evaluar las vulnerabilidades inherentes a los protocolos de seguridad utilizados en las redes domésticas. Esta exploración es esencial para respaldar la ejecución del proyecto, ya que proporciona una comprensión más profunda y precisa de las debilidades en la seguridad de estas redes.

Además, al identificar las vulnerabilidades, estaremos abriendo la puerta a un examen más exhaustivo de una amplia gama de herramientas especializadas que pueden poner en riesgo estos protocolos de seguridad. Estas herramientas tienen la capacidad de llevar a cabo ataques de fuerza bruta y otros tipos de intrusión, en ocasiones sin que los usuarios sean conscientes de estas amenazas mientras están conectados a la misma red.

Por último, esta investigación no solo aumentará la comprensión de los protocolos de seguridad más conocidos WPE, WPA, WPA2 Personal y WPA3, sino que, también proporcionará soluciones y recomendaciones concretas para fortalecer la seguridad de

las redes domésticas y proteger a los usuarios de potenciales ataques cibernéticos inadvertidos.

Este tema esta alineado a los objetivos del Plan Nacional de Desarrollo al siguiente Eje:

Eje Social:

Objetivo 5: Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión social [14].

Pol. 5.4:

A4.: Fortalecer la conectividad y el acceso del TIC como una vía para mejorar el acceso a otros servicios [14].

Objetivo 7: Potenciar las capacidades de la ciudadanía y promover una educación innovadora inclusiva y de la calidad de todos los niveles [14].

Pol. 7.1:

G.9.: Promover la investigación científica y de la transferencia del conocimiento que permite la generación de oportunidades de empleo y función de potenciales territorio[14].

1.5 ALCANCE

Para llevar a cabo este proyecto debe incluirse las siguientes fases:

Fase 1: Recopilación de Informacion:

- Se realiza un reconocimiento de toda la información de las redes en un punto específico geolocalizados con latitud y longitud de la Península de Santa Elena.
- La utilización de las herramientas en informáticas de computación forense para identificar las vulnerabilidades de los protocolos de seguridad.

Fase 2: Análisis de vulnerabilidades:

- La recolección de todos los resultados de la red.
- Identificación del tipo de vulnerabilidad del protocolo de seguridad que se encontró en la fase de recopilación de información.

Fase 3: Explotación:

- Eligiendo las herramientas para atacar las vulnerabilidades encontradas en los protocolos de las redes inalámbricas.

- Elegir el tipo de ataque en cada protocolo factible para vulnerarlo.
- Realizar ataques de fuerza bruta de acuerdo al protocolo correspondiente.

Fase 4: Presentación De Informe:

- Obtención de los resultados de las pruebas realizadas.
- Documentación referencial y sugerencias a seguir entorno a las mejoras de seguridad en base a los resultados obtenidos.

CAPÍTULO II. MARCO REFERENCIAL

2.1 MARCO CONTEXTUAL

Las pruebas se ejecutan en un ambiente virtual controlado dentro de 3 puntos específicos geolocalizados de la península de Santa Elena como Salinas, La Libertad, Santa Elena. El estudio de las vulnerabilidades de los protocolos de seguridad de una red doméstica se realizó dentro del alcance de la tarjeta de red. El primer punto de análisis se realizó en Salinas teniendo como latitud y longitud las coordenadas 2°12'21.5"S 80°58'13.6"W, la misma que hace referencia al “EL MERCADO ARTESANAL”.

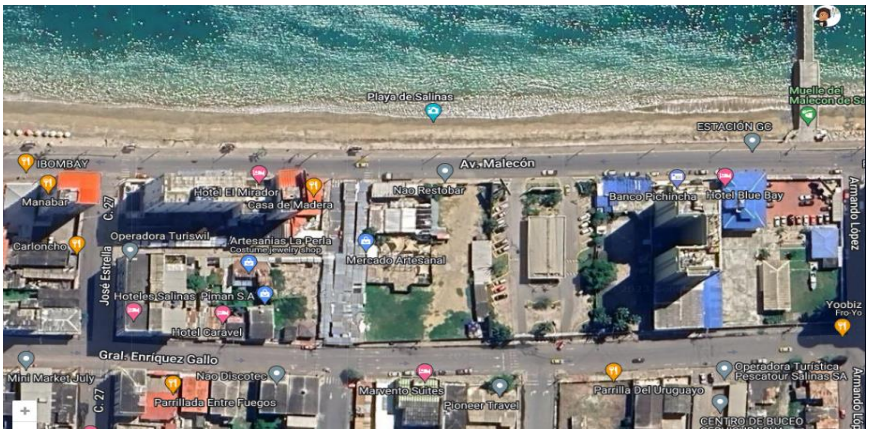


Fig. 1. Localización Sector Malecón de Salinas

La segunda ubicación se encuentra en La Libertad cuyas coordenadas son 2°13'14.3"S 80°54'31.2"W. Esta área se caracteriza por un perímetro de 15 metros que rodea al "CLUB DE LEONES". Dentro de este perímetro, se pueden observar diversas características y puntos de interés que forman parte del entorno inmediato del club.

Fig. 2. Localización Sector Malecón La Libertad

La tercera ubicación se encuentra en las coordenadas 2°13'56.6"S 80°52'01.2"W dando lugar a Santa Elena Av. Lounge 5, Santa Elena.

Fig. 3. Localización Sector Santa Elena

2.2 MARCO CONCEPTUAL

Cifrado: Es el método por el cual la información se convierte en un código secreto que oculta su verdadero significado. La ciencia de cifrar y descifrar información se llama criptografía [15]. La criptografía abarca tanto y el cifrado de datos la cual constituye una disciplina científica y técnica fundamental.

Handshake: La criptografía moderna se encarga, principalmente, de facilitar una comunicación confidencial, auténtica e íntegra entre usuarios a través de internet, ya que este es el medio más utilizado en la actualidad [16]. Este proceso asegura que ambas partes se autentiquen mutuamente a través de la red .

Psicología en claves : Radica como las personas eligen y gestionan sus propias contraseñas a la psicología decae individuo sea fácil es de recordar [17].

Desautentificación: Este ataque envía paquetes de des-asociación a uno o más clientes que actualmente están asociados con un punto de acceso en particular [18].

PSK: El Protocolo de Integridad de Clave Temporal ("TKIP", por su sigla en inglés) es un método de codificación. El "TKIP" proporciona una clave por paquete que mezcla la integridad de un mensaje con un mecanismo de re-escritura [19].

PMK: Es generada luego de toda la sesión, y debería ser expuesta lo menos posible al medio. No obstante, las claves para cifrar el tráfico sí deben ser enviadas. El handshake de 4-way es utilizado para establecer otra clave, llamada PTK [20].

802.11x: Protocolo de acceso a puertos para proteger redes mediante autenticación., este tipo de método de autenticación es extremadamente útil en el entorno Wi-Fi debido a la naturaleza del medio [21].

ISO 27002: Este estándar proporciona directrices detalladas para la implementación de controles de seguridad. Podría ser utilizado para seleccionar controles específicos que se apliquen a la gestión de la seguridad de la red inalámbrica doméstica [22].

CCMP: El CCMP es una credencial reconocida a nivel mundial establecida por ACMP para que los profesionales demuestren su compromiso de liderar la forma en que funciona el cambio. El CCMP fue desarrollado basado en el estándar líder de la industria de ACMP para la gestión del cambio ("el Estándar") que define las mejores prácticas en la gestión del cambio [23].

Fuerza bruta: Termino para referirse a todo tipo de combinaciones sea numérico o de caracteres en específico números letras y símbolos [24].

Ataques de diccionario: Este tipo de ataque es buscar la palabra en un diccionario compuesta de combinaciones prescritos en varios ficheros pero no siempre son efectivos eso depende mucho del idioma en cual se trabaja [24].

Pyrit: Es un programa que se ejecuta en lenguaje Python y en C la cual utiliza mediante varias librerías descifradas relacionadas con el cifrado, esto puede ser en bases de datos o OpenSSL la cual sirve para los protocolos WPA2 [24].

Cuadro comparativo de los Protocolos de Comunicación

PROTOCOLO	AÑO DE LANZAMIENTO	TAMAÑO	TIPO DE CIFRADO
WEP	1997	64/128 BITS	RC4
WAP	2003	256 bits	TKIP
WPA2	2004	256 bits	AES-CCMP
WPA3	2018	192/256 bits	Simultaneo: WPA3-Personal (SAE) y WPA3-Enterprise (192 bits)

Tabla 1:Cuadro comparativo Protocolo de comunicación

MECANISMOS DE SEGURIDAD DE UNA RED DOMÉSTICA.

SSID: Es el nombre público que identifica una red local inalámbrica, es decir, una WLAN son las siglas de Service Set Identifier. En español entenderíamos por esta expresión algo así como Identificador de Conjunto de Servicios [25].

Filtrado de Mac: una serie de caracteres alfanuméricos que sirven para identificar un dispositivo [26].

Estándares IEEE: una serie de caracteres alfanuméricos que sirven para identificar un dispositivo. Cada uno tiene un número propio, donde viene reflejado el modelo de dispositivo, la marca, etc. Es, por decirlo de alguna forma, como un DNI para ese equipo [27].

WEP (Wired Equivalet Piracy): Su objetivo principal consiste en proveer la confidencialidad de la transmisión de la información, tal como se ofrece en las LAN [28].

WPA (Wi-Fi Protected Access): Distribuye claves diferentes a cada usuario, mejora la integridad de la información, al igual que WEP, los usuarios malintencionados pueden obtener su clave, otra de sus desventajas es que, al tener una contraseña de al menos veinte caracteres, la cual es difícil que los usuarios la recuerden [28].

WPS: El sistema WPS (Wi-Fi Protected Setup) representa un enfoque de autenticación diseñado para simplificar la entrada a redes seguras de manera más práctica. Esta técnica de conexión se ha estado implementando desde aproximadamente 2007, coincidiendo con la introducción del estándar Wi-Fi 4 o Wi-Fi N. No obstante, la Wi-Fi Alliance ha retirado este método debido a consideraciones de seguridad, ya que se ha identificado como un punto de vulnerabilidad en la protección de redes inalámbricas [29].

Servicios Básicos de los Protocolos De Seguridad

Los protocolos de seguridad en redes inalámbricas se implementan para proteger la confidencialidad, integridad y autenticidad de los datos transmitidos. A continuación, se describen los servicios básicos que ofrecen estos protocolos.

SERVICIOS BÁSICOS DE SEGURIDAD	DESCRIPCIÓN
Integridad	Asegura que estos mensajes no serán modificados en el tráfico que sea de la red.
Confidencialidad	La privacidad es un compromiso y fundamental dentro de la seguridad de la información.
Autentificación	La verificación de un objeto es fundamental para garantizar el acceso de sistemas informáticos la cual se encuentra en la misma red.

Tabla 2: Servicios básicos en redes inalámbricas

HERRAMIENTAS Y SISTEMAS OPERATIVOS

Kali Linux: Kali Linux es una distribución de Linux diseñada específicamente para pruebas de penetración y evaluación de seguridad. Se basa en Debian y está destinada a ser una herramienta poderosa para profesionales de seguridad de la información y hackers éticos que desean identificar y corregir vulnerabilidades en sistemas informáticos y redes. Kali Linux viene preconfigurada con una amplia gama de herramientas de seguridad y pruebas de penetración, incluyendo herramientas de análisis de vulnerabilidades, herramientas de explotación y herramientas de auditoría de seguridad [30].

Kali Linux por su extensa colección de herramientas en pruebas de penetración y auditoria de seguridad la cual es una excelente plataforma educativa en técnicas de ciberseguridad , su actualización constante y su comunidad activa lo hace muy ideal para el entorno profesional en este campo de la informática.

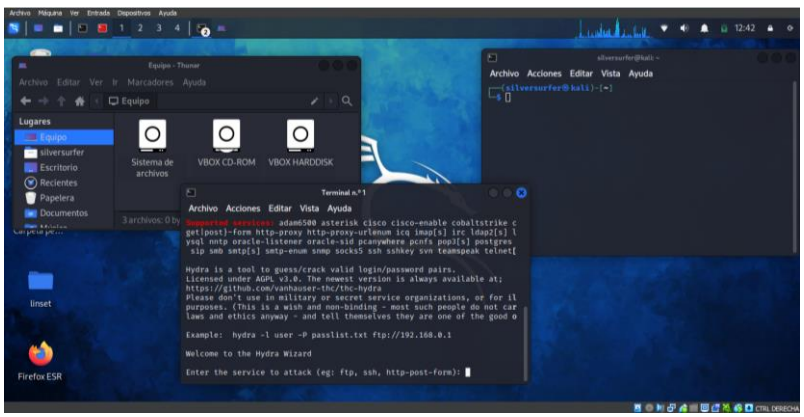


Fig. 4. Sistema operativo Kali Linux

WiFi Slax O.S: WiFi Slax es una distribución de Linux diseñada para pruebas de seguridad, auditoría de redes y evaluación de seguridad inalámbrica. Al igual que Kali Linux, WiFi Slax está orientado a profesionales de seguridad de la información y entusiastas de la seguridad que desean realizar pruebas éticas en redes y sistemas inalámbricos. Aunque comparten similitudes en sus objetivos, WiFi Slax y Kali Linux tienen algunas diferencias en términos de enfoque y conjunto de herramientas [31].

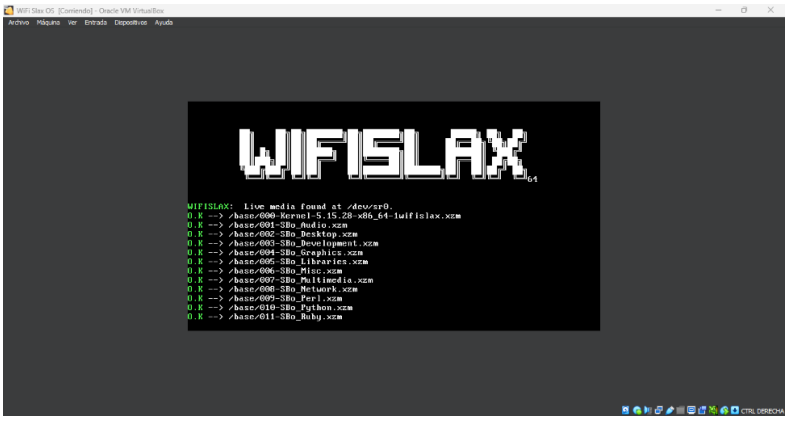


Fig. 5. Sistema operativo WiFi Slax

LINSET Abreviatura de "Linux Evil Twin," es una herramienta de software de código abierto que se utiliza para llevar a cabo ataques de suplantación de punto de acceso inalámbrico (AP) en redes Wi-Fi. Este tipo de ataque se conoce comúnmente como "ataque de Evil Twin." Linset se utiliza para crear un punto de acceso falso que se asemeja a un punto de acceso legítimo y engaña a los dispositivos cercanos para que se conecten a él en lugar del punto de acceso real [32].

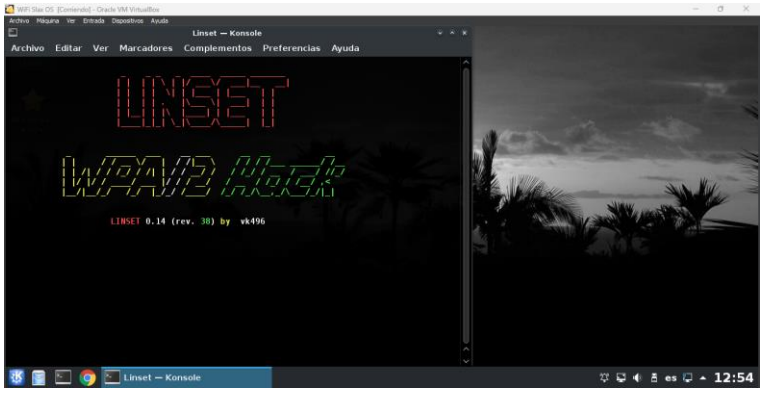


Fig. 6. La Herramienta Linset

WIFITE Es una herramienta de software de código abierto diseñada para automatizar y simplificar la auditoría de seguridad en redes inalámbricas, específicamente en redes Wi-Fi. Esta herramienta se utiliza comúnmente por profesionales de seguridad de la

información y hackers éticos para evaluar la seguridad de redes Wi-Fi y para identificar posibles vulnerabilidades en las mismas [33].

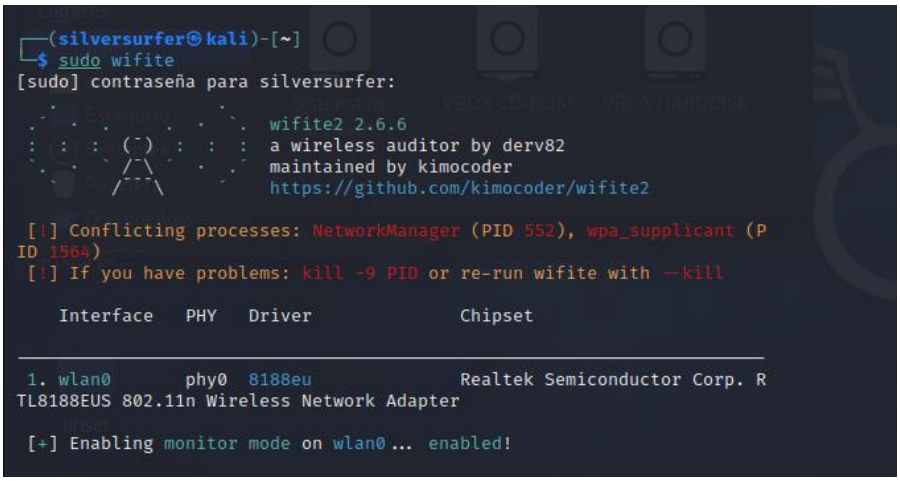


Fig. 7: Wifite 2.2.6v

TÉRMINOS DENTRO DE LAS CONSOLA DE ESCANEO

En la siguiente tabla se aprecia los ítems que tendremos en referencia más adelante en nuestra investigación

Ítem	Descripción
NUM	Número de la red en la lista de resultados. Esta etiqueta generalmente muestra el índice o la posición de la red en la lista.
CH	El número del canal de la red inalámbrica. Indica el canal en el que opera la red.
ENCR	Tipo de cifrado utilizado por la red (como WEP, WPA, WPA2, etc.).
WPS	Indica si la red tiene WPS (Wi-Fi Protected Setup) habilitado (Sí o No).
PWR	La potencia de la señal de la red, que muestra qué tan fuerte o débil es la señal.
CLIENT	Muestra si hay clientes (dispositivos conectados) en la red (Sí o No).
ESSID	El nombre de la red inalámbrica (SSID), que es el nombre que aparece en la lista de redes disponibles.

Tabla 3:Términos

2.2.1 Protocolo WEP

Fue uno de los primeros protocolos de seguridad para las redes Wifi diseñados para las redes cableadas y ofrecer un nivel de seguridad, pero esto demostró tener serias debilidades que comprometen su eficacia en la protección de datos y la seguridad de la red inalámbrica.

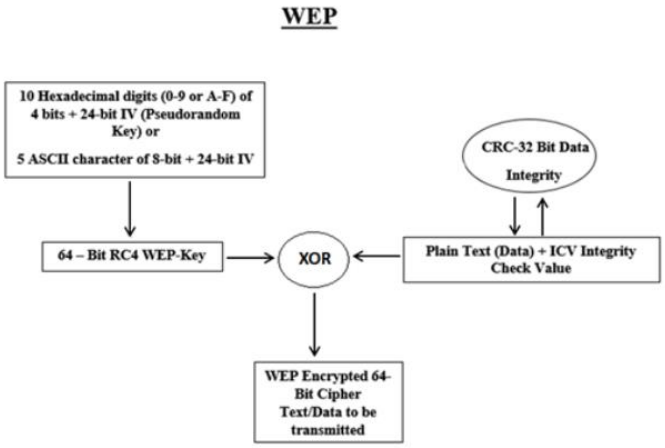


Fig. 8 Encriptación WEP según [34]

Vulnerabilidades del protocolo WEP

Inyección De Tramas: Un atacante que decida capturar una trama WEP a una determinada asociación y repetir tantas veces como quisiera el si la asociación continúa dándose, el receptor dará la trama por valida [34].

Falsificación De La Autentificación: Si un atacante decide capturar dichas tramas y en proceso intercambiarlas durante el autentificado de la clave compartida entre la estación y un Access Point o también conocido como AP podrá autentificarse con éxito sin necesidad de clave WEP [34].

El conjunto de ataques Korek: Se los conoce así por un atacante que tenía pseudónimo "Korek" el atacante conocía los dos primeros bytes de keystream la cual existe tres grupos:

- Ataques que permite averiguar k[n] a partir de K [0]……, K[n-1] y S [0]. El ataque FMS pertenece a este grupo.
- Ataques que permite averiguar k[n] a partir de K [0]……, K[n-1] y S [0] y S [1].
- Ataques "negativos" que si V cumplía ciertas condiciones y S [0] toma ciertos valores y así determina.

De hecho implementar algunos ataques en paralelo tiene una tasa de efectividad con el descubrimiento de la clave [35].

Herramientas Posibles: Aircrack-ng, Wireshark son comunes y utilizadas para analizar el tráfico WEP permitiendo la captura de ciertos paquetes y detectar esas vulnerabilidades claro existen otras herramientas como Kismet que se utiliza como Sniffer.

2.2.2 Protocolo WPA

Es diseñado para reemplazar a WEP brindando mejoras significativas en el cifrado y la autentificación.

Este cifrado ofrece dos tipos de autentificación WPA-Personal (Pre-Shared-key) y WPA-Enterprise (usando un servidor como RADIUS).
Normalmente existe una sola clave secreta compartida por el AP (Access point) y las estaciones (dispositivos).

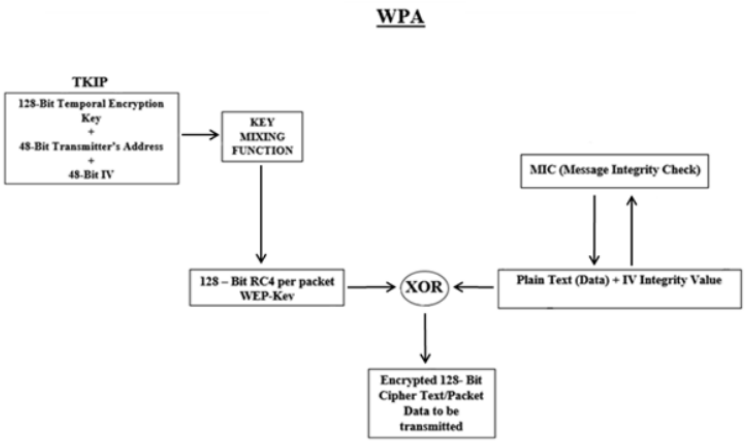


Fig. 9. Encriptación WPA según [34]

Vulnerabilidades Del Protocolo WPA

Una de las principales vulnerabilidades del sistema WPA es la autentificación de las claves compartidas WPA-PSK esto trabaja con 256 bits la cual es mínimo prácticamente esto lo contine una palabra y es viable a los ataques de fuerza bruta como de diccionario [35].

Entre más tramas tengas disponibles más factibles son de encontrar las claves con 4-way handshake en los paquetes de la asociación de los dispositivos.

Herramientas aplicables a WPA

Herramientas como Aircrack-ng, Wireshark pueden ser muy útil para este tipo de redes por las posibles vulnerabilidades.

Los métodos las herramientas ofrecen como ataques de diccionario y ataques reautenticación.

2.2.3 Protocolo WPA2

Es una evolución del protocolo anterior la cual se ha convertido un estándar de seguridad con mayor robustez y resistencia.

Utiliza métodos de autentificación más sólidos de clave maestras (PMK caching) esto agilita el reautenticación de los dispositivos.
Introduce también un nuevo algoritmo de cifrado CCMP esto no está basado en RC4 sino en AES-128 lo cual mejora el cifrado [35].

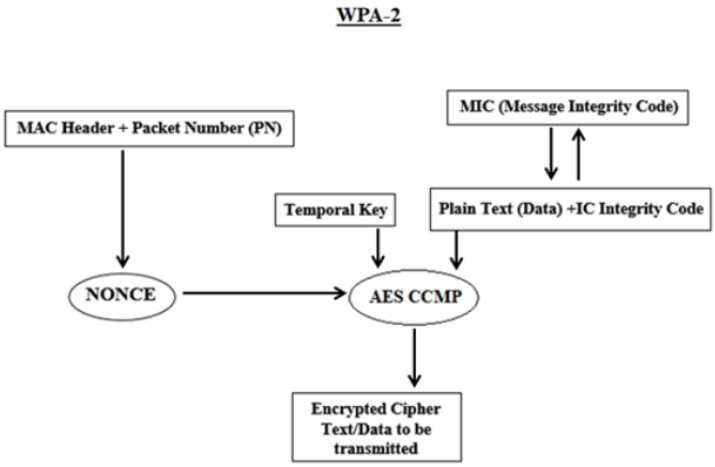


Fig. 10. Encriptación WPA2 según [34]

Herramientas aplicables a WPA2

Las mejores herramientas que podemos encontrar es Aircrack-ng, Wireshark la cual captura paquetes y para el análisis. Los métodos que se podrían emplear en este protocolo son ataques de fuerza bruta para las contraseñas débiles, análisis de tráfico para esos patrones susceptibles y ataques de reautenticación.

2.2.4 Protocolo WPA3

Al igual que los otros protocolos en estos entornos es implica evaluar su robustez y debilidades posibles. Las mejoras de este protocolo son significativas en autentificación y el cifrado en conexiones inalámbricas en las comunicaciones.

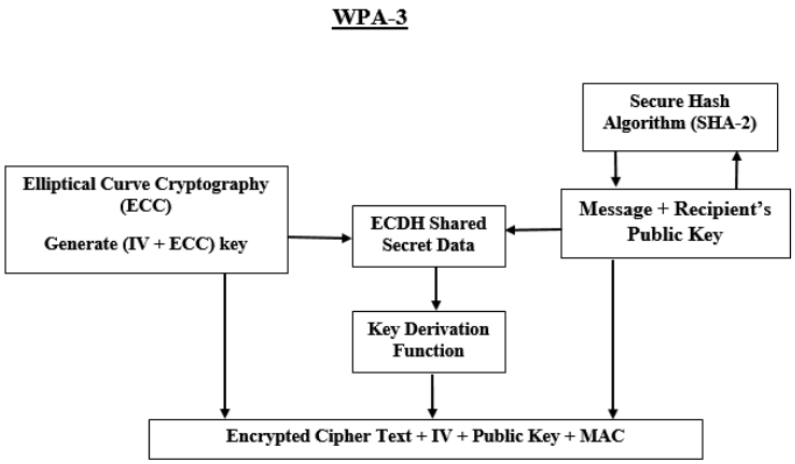


Fig. 11. Encriptación WPA3 según [34]

Este protocolo emplea Simultaneous Authentication of Equals (SAE) donde fortalece y dificulta los ataques de fuerza bruta a contraseñas.

Introduce cifrados individualizados, lo cual significa que cada dispositivo tiene una y propia clave de cifrado esto mejora la seguridad dentro de las comunicaciones.

WPA3 bloquea la autenticación después de un cierto número de intentos fallidos de inicio de sesión y, por lo tanto, también brinda protección contra ataques de fuerza bruta [36].

HERRAMIENTAS APLICABLES A WPA3:

Volvemos a escuchar a Aircrack-ng y Wireshark claro está que son herramientas especializadas para el análisis de tráfico para la seguridad de las redes WPA3.

Técnicas que se emplean es análisis de claves, monitoreo de tráfico y pruebas de penetración específicas.

TARJETA DE RED

Ambos dispositivos son utilizados comúnmente en auditorías de seguridad y pruebas de penetración debido a sus capacidades de frecuencia y certificaciones de compatibilidad. La comparación detallada incluye aspectos como marca, modelo, frecuencia de

operación, dimensiones físicas y certificaciones. Adicionalmente, se proporciona una ilustración visual de cada dispositivo para facilitar la identificación y comparación visual.

Especificación	Datos del dispositivo 1	Datos del dispositivo 2
Marca	TP-Link	TP-Link
Modelo	TL-WN722N	TL-WN725N
Frecuencia	2.400-2.4835GHz	2.400-2.4835GHz
Dimensiones	3,7 x 1,0 x 0,4 pulgadas (93,5 x 26 x 11 mm)	0.73x0.59x0.28 pulgadas(18.6x15x7.1mm)
Certificación	CE, FCC, RoHS	CE, FCC, IC, RoHS
Ilustración		

Tabla 4: Tarjetas de Red

TABLA SEGÚN SU NIVEL DE RIESGO

PROTOCOLO DE SEGURIDAD	RIESGO	COLOR
WEP	ALTO	ROJO
WPA	MODERADO	AMARILLO
WPA2	MODERADO	AMARILLO
WPA3	BAJO	VERDE

Tabla 5: Nivel de riesgo de los protocolos

- **ROJO:** Indica un alto nivel de riesgo, el protocolo tiene varias vulnerabilidades y se considera inseguro a ataques.
- **AMARILLO:** Indica un riesgo moderado, tanto WPA como WPA2 pueden ser explotadas bajo ciertas circunstancias.
- **VERDE:** Indica un riesgo bajo, WPA3 hasta la fecha es la opción más segura con mejoras y cifrados considerables.

2.3 MARCO TEÓRICO

Hacking Ético.

La expresión "hacker" es frecuentemente utilizada para hacer referencia a un individuo que intenta ingresar a un sistema de información o que de otro modo utiliza el conocimiento experto y la programación para actuar de manera maliciosa, este proceder es conocido como hacking y es importante tener claro que es posible que una prueba de hacking ético no identifique todas las vulnerabilidades, ni que ofrece garantía absoluta de que la información de la organización está segura [37].

Por lo tanto, el hacking ético son pruebas de penetración que la organización autoriza para simular las actividades de hackers que intentan acceder a sus activos de información y es por esta razón que se puede decir que es una herramienta para la seguridad informática [37].

Describiendo lo anterior, el Ethical Hacking o el hacking ético consiste en simular los posibles escenarios en la cual se incluyen ataques de una manera sumamente contralada así mismo las propias actividades del ciberdelincuente en ese entorno para proceder de manera inmediata.

Métodos de Pentesting

Una prueba de penetración implica diversas etapas o fases que conforman su proceso, si bien es necesario establecer un acuerdo con el cliente antes de su ejecución. Estas fases suelen seguir un esquema predefinido, que se describe a continuación.

Estos son algunos de los métodos de pentesting [38]:

- ISSAF (Information Systems Security Assessment Framework): Proporciona una estructura sistemática avanzadas y personalizadas para identificar, analizar y abordar las vulnerabilidades y riesgos de seguridad en los sistemas de información.
- OWASP (Open Web Application Security Project): Este estándar es utilizado en conocer vulnerabilidades de aplicaciones Web y móviles, con más de 66 controles con varias funcionabilidades para la evaluación.
- PTES (Penetration Testing Execution Standard): es puesto en práctica por muchos profesionales altamente reconocidos del sector, además de ser un modelo a seguir en libros de aprendizaje asociados al pentesting.

- OSSTMM (Manual de la Metodología Abierta de Testeo de Seguridad): sus pruebas no son especialmente innovadoras, pero es uno de los primeros acercamientos a una estructura global de concepto de seguridad. Este modelo es referente en instituciones que precisan de un pentesting de calidad, ordenado y eficiente.

Tener claro estos tipos de metodologías que son importante en pruebas de pentesting.

Tipos de ataques a conexiones wifi

Según el INCIBE en su "Guía de ciberataques" debes saber todo a nivel de usuario los ataques a estas conexiones. Los ataques a estas conexiones son muy comunes en delincuentes que sutilizan diversos software y herramientas con saltarse las medidas de seguridad [39].

Lo cual existen 8 subtipos de ataques en estas conexiones [39]:

- **Redes trampa:** Creación de redes falsas donde consiste en crear una red gemela a una legítima y segura dando nombres muy similares a la original
- **Spoofing o suplantaciones:** este empleo de manera maliciosa es las suplantaciones de alguna web, Email, IP, DNS donde la victima dispondrá de los datos que el atacante requiera para su ataque
- **Ataques de cookies:** El atacante puede insertar un script malicioso en un sitio web vulnerable que el usuario visita. Este script puede robar las cookies del usuario y enviarlas al atacante.
- **Ataques de DDoS:** Estos ataques se dirigen a la capa de autenticación de la conexión WiFi. Los atacantes envían paquetes de deautenticación a dispositivos conectados a una red WiFi
- **Inyección de paquetes:** El atacante puede crear paquetes maliciosos utilizando herramientas de generación de paquetes como Scapy, estos paquetes pueden contener comandos o instrucciones diseñadas para comprometer la seguridad de la red o realizar acciones no autorizadas.
- **Escaneo de puertos:** si un atacante se percata que un dispositivo tiene el puerto 22 (SSH) abierto, esto indica que el dispositivo podría estar ejecutando un servidor SSH y podría ser vulnerable a ataques de fuerza bruta o a exploits conocidos.

- **Man in the middle:** los ataques MITM pueden ser extremadamente peligrosos, ya que comprometen la confidencialidad, integridad y autenticidad de la comunicación en una red la cual los propietarios deben tener seguridades robustas.
- **Sniffing:** Un atacante puede utilizar un Sniffer para capturar paquetes de datos que contienen contraseñas y credenciales de inicio de sesión.

Ante lo mencionado estos ataques pueden tener graves implicaciones en términos de privacidad y seguridad.

Al poco conocimiento de aquello por lo que es importante estar al tanto de ellos y tomar medidas para protegerse contra ellos.

Tipos de Redes Inalámbricas

Una de las principales diferencias entre los tipos de redes inalámbricas se basa muchas veces en el alcance y la velocidad que ellos utilizan sea en una instalación de un hogar o dentro de una empresa esto dependerá mucho del uso y las necesidades de los propietarios para elegir [40].

Las redes inalámbricas de área personal (WPAN) tienen una longitud de alcance de hasta 10 metros y se utilizan comúnmente para conectar dispositivos de uso personal. Estas redes tienen una menor cobertura en comparación con otras redes inalámbricas, pero son más adecuadas para aplicaciones específicas y dispositivos portátiles [40].

Una red inalámbrica de área local (WLAN) es un tipo de red inalámbrica que puede cubrir distancias de hasta 100 metros y suele implementarse mediante protocolos Wi-Fi o Bluetooth. Estas redes se utilizan comúnmente para establecer conexiones de bajo costo y alta calidad en áreas de trabajo y con sistemas flexibles [40].

Un Wireless Metropolitan Area Network (WMAN) es un tipo de red inalámbrica que se extiende por áreas metropolitanas de tamaño mediano, cubriendo distancias de hasta 50 kilómetros y conectando varios puntos dentro de una zona geográfica [41].

La Red Inalámbrica de Área Amplia (WWAN) es la red inalámbrica que ofrece la mayor cobertura y es utilizada por las compañías telefónicas para establecer conexiones y servicios de largo alcance. La tecnología WWAN utiliza sistemas como GSM, GPRS y UMTS para proporcionar conexiones inalámbricas a áreas más amplias que las redes inalámbricas de área local (LAN) [42].

Pentesting

El pentesting, o test de penetración, es un método utilizado para evaluar la seguridad de una infraestructura informática mediante la simulación de un ataque real. Su objetivo es identificar y explotar vulnerabilidades en los sistemas de una organización con el fin de proporcionar un informe detallado que permita a la empresa mejorar su postura de seguridad. Este proceso implica la realización de pruebas exhaustivas que evalúan la resistencia de un sistema a diversos tipos de ataques, como intrusiones, exploits y fugas de información. Además, los pentesters analizan la capacidad de respuesta del equipo de seguridad de la empresa frente a estas amenazas [43].

En respuesta a lo mencionado, el pentesting, o prueba de penetración, se erige como una metodología fundamental en el ámbito de la ciberseguridad. Consiste en la simulación controlada de ataques cibernéticos con el fin de detectar y corregir vulnerabilidades en sistemas expuestos a niveles significativos de amenazas.
Este proceso implica una exhaustiva evaluación y análisis de la infraestructura digital, con el propósito de fortalecer sus defensas y mitigar posibles riesgos de seguridad para los gestores.

2.4 MARCO LEGAL

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 [44].

> **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[44].

> **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 [44].

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 [44].

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 [44].

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 [44].

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 [44].

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 [44].

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 [44].

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 [44].

2.5 METODOLOGÍA DE PROYECTO

2.5.1 METODOLOGÍA DE INVESTIGACIÓN

Se encontró proyectos de titulación similares realizados a nivel nacional e internacional, a nivel nacional está uno realizado en la Universidad Politécnica Nacional denominado "Utilización de Hacking Ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones"[45].
De esta manera a nivel internacional se halló un tema en el repositorio de la Universidad Privada del Norte en Perú, la cual tenía por título "aplicación de auditoría Penetration Testing, para contribuir con la seguridad de la información en los sistemas informáticos de la empresa data Business Sac, Trujillo" [46].

Investigación Descriptiva es aquella que puede desarrollarse con un enfoque de carácter cualitativo para poder llegar a conocer las diferentes situaciones, costumbres y actitudes que se consideran predominantes a través de la descripción detallada de actividades, procesos y personas [47].

La investigación adoptó un enfoque práctico experimental ya que se enfocó en la implementación y evaluación directa de teorías y métodos dentro de un entorno controlado para analizar sus efectos y resultados. Este método permitió la manipulación intencional de variables independientes con el fin de medir su impacto en las variables dependientes, asegurando un control riguroso de los factores externos y mejorando la validez interna del estudio. La metodología experimental es esencial para establecer relaciones causales precisas y ofrece una base empírica sólida que facilita la generalización de los resultados a contextos más amplios [48].

Cómo esta propuesta es tecnológica se analizará las redes de los puntos específicos para dar a conocer vulnerabilidades de los protocolos de seguridad e indirectamente reducir un riesgo, y así los propietarios de esos dispositivos o Routers pueden tener una correcta

gestión e incluso configuración como medidas correctivas, si es necesario para un nivel de seguridad y protección de sus redes domésticas.

Datos del Estudio

Se utilizaron 15 redes distribuidas en tres puntos geolocalizados en sectores como Salinas, La Libertad, Santa Elena. El muestro utilizado no es probabilístico, en otras palabras, la muestra se selecciona a conveniencia y disponibilidad del investigador.

Localización	Numero de redes
Salinas	5
La Libertad	5
Santa Elena	5
Total	**15**

Tabla 6:Tabla de población

2.5.2 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para recolectar información se aplicó la técnica de la observación , además de revisiones bibliográficas en investigaciones de propuestas tecnológicas similares disponibles en repositorios institucionales de las universidades y bases de datos indexadas; además dado que estas redes son de propiedad privada , se llevó a cabo el proceso ético legal que incluyó la obtención de permisos correspondientes de forma verbal de los propietarios de las redes que iban a ser auditados, dado una breve explicación de la misma ya que fue fundamental para garantizar la integridad e investigación ; respetar la privacidad de los datos obtenidos garantizando que no se realizará alguna modificación de los dispositivos pudimos obtener el consentimiento de los propietarios.

2.5.1 METODOLOGÍA DE DESARROLLO DEL PROYECTO

El desarrollo del proyecto se realiza mediante PENTESTING (Test de penetración). Para lo cual, se utiliza como referencia la metodología PTES que consiste en siete fases [49]; sin embargo en este proyecto se adapta a 4 fases, las cuales se describe a continuación.

Fase 1: Recolección de información: Proceso de recopilar información en los sistemas, redes y aplicaciones con el fin de identificar vulnerabilidades objetivamente los datos de los usuarios o dispositivos para planificar un ataque eficaz.

Fase 2: Análisis de Vulnerabilidades: Es una Evaluación sistemática de los sistemas explorados para la identificación de las debilidades y fallas de seguridad.

Fase 3: Explotación: Proceso de aprovechar las vulnerabilidades identificadas en sistemas informáticos, redes o aplicaciones con el fin de obtener acceso no autorizado, realizar acciones maliciosas o comprometer la seguridad de los mismos.

Fase 4: Presentación de Informe: Documento detallado que presenta los hallazgos, análisis y recomendaciones derivadas de actividades como la evaluación de vulnerabilidades o pruebas de penetración. Este documento suele incluir información sobre las vulnerabilidades encontradas, su impacto potencial en la seguridad de los sistemas, las técnicas utilizadas para identificarlas.

Dado a esta metodología podemos tener una estructura organizada en las fases de proceso para garantizar la validez, confiabilidad y relevancia.

CAPITULO III. PROPUESTA

REQUERIMIENTOS

En la tabla se especificó los requisitos de Hardware y Software, así como acuerdos por partes de los propietarios de dichas redes.

Requerimiento	**Software**
RQ1	Aircrack-ng
RQ2	WiFi Slax O.S
RQ3	Wifite 2.2.6 v
RQ4	Linset
RQ5	Kali Linux
RQ6	Drivers
Requerimiento	**Hardware**
RQ7	Tarjeta de red TL-WN722N
RQ8	Tarjeta de red TL-WN725N
RQ9	Laptop
RQ10	Routers
RQ11	Dispositivos móviles
Requerimientos	**Acuerdos**
RQ12	Evitar la saturación de la red durante la prueba de penetración.
RQ13	No realizar cambios en la configuración de los dispositivos auditados.
RQ14	Garantizar la confidencialidad de todo el tráfico capturado recolectada durante las pruebas con el único propósito de análisis técnico.
RQ15	Documentar meticulosamente los resultados para proporcionar recomendaciones en un informe detallado.

Fig. 12: Tabla de Requerimientos

DESARROLLO DE PROPUESTA

FASE 1.- RECOLECCIÓN DE INFORMACIÓN

El reconocimiento de información es de vital importancia ya que implica la identificación, captura y análisis de datos relevantes, con el objetivo de extraer conocimiento útil y significativo para las para iniciar el proceso de escaneo y explotación de vulnerabilidades; es necesario preparar el entorno virtual para ejecutar dichas pruebas como se muestra en la FASE DE ANALISIS O ESCANEO.

Tablas de Redes Obtenidos

A continuación, la tabla 7 , muestra la lista de las redes inalámbricas previo al reconocimiento del sector Salinas.

NUM	ESSID	CH	ENCR	PWR	WPS	CLIENTE
1	LENGT	3	WPA2-P	99db	No	1
2	TABARUHA_2G	4	WPA2-P	46db	No	
3	MARKITOS	1	WPA2-P	37db	No	3
4	CNT_FIBRA_OPTICA	8	WPA2-P	29db	No	
5	XTRIM_NANCY_PAEZ	11	WPA2-P	24db	Yes	
6	XTRIM_ABRIL_MUÑOZ	6	WPA2-P	23db	Yes	
7	SALINAS	2	WPA2-P	18db	Yes	
8	TERREROS 2	9	WPA2-P	18db	Yes	
9	XTRIM NIKA	4	WPA2-P	18db	Yes	1
10	XTRIM_ROGE_WI-FI5	6	WPA2-P	18db	Yes	
11	XTRIM_ROGE	6	WPA2-P	17db	Yes	
12	ALVAREZ2023	1	WPA2-P	15db	No	

Tabla 7: Escaneo Sector Salinas

En la tabla 8, se muestra la lista de las redes en la zona de La Libertad.

NUM	ESSID	CH	ENCR	PWR	WPS	CLIENTE	
1	FAMILIA_COBOS	3	WPA2-P	99db	YES	6	
2	NEO_FAMILIA_BUENO	4	WPA2-P	98db	YES	2	
3	XTRIM_DEL_PEZO	1	WPA2-P	96db	YES	5	
4	CNT_FIBRA_VELAZA	8	WPA2-P	88db	No		
5	XTRIM_SWORDGGD	11	WPA3	87db	Yes	3	
6	XTRIM_SEGURA_RED	6	WPA2-P	11db	Yes		
7	TECHHIVE	2	WPA2-P	18db	Yes	3	
8	DATAFOR	9	WPA2-P	18db	Yes		

Tabla 8:Escaneo Sector La Libertad

En la tabla 9, se muestra la lista de las redes en la zona de Santa Elena.

NUM	ESSID	CH	ENCR	PWR	WPS	CLIENTE
1	CASA_DIGITAL	3	WPA3	99db	NO	3
2	FERNANDEZ_WIFI	4	WPA2-P	63db	NO	
3	XTRIM_LOPEZ	1	WPA2-P	55db	YES	3
4	XTRIM_SOLIZ	8	WEP	51db	NO	
5	XTRIM_CASTRO_WIFI5G	11	WPA2-P	48db	NO	4
6	SANCHEZ_CRIOLLO	6	WPA2-P	10db	NO	

Tabla 9:Escaneo Sector Santa Elena

FASE 2.- ANÁLISIS DE VULNERABILIDADES

Esta fase implica la evaluación detallada del protocolo utilizada durante el proceso de escaneo para determinar dicha naturaleza y sus comportamientos.

Hay que tener claro el HDLC (High-Level Data Link Control) la cual es un tipo de trama que son utilizadas en comunicación de red.
HDLC es un protocolo de enlace de datos la cual define el formato en las tramas que intercambian entre los dispositivos dentro de la red.

- **Flag delimitador:** Marcadores especiales al inicio y final de cada trama para indicar el comienzo y el final de la trama.
- **Campo de dirección:** Identifica la estación de destino o el tipo de trama (unidireccional, multidifusión, etc.).
- **Campo de control:** Controla la secuencia y el flujo de datos entre las estaciones.
- **Campo de información:** Lleva los datos útiles que se están transmitiendo.
- **Campo de verificación de redundancia cíclica (CRC):** Utilizado para la detección de errores y asegurar la integridad de la trama.
- **Campo de flag de finalización:** Indica el final de la trama.

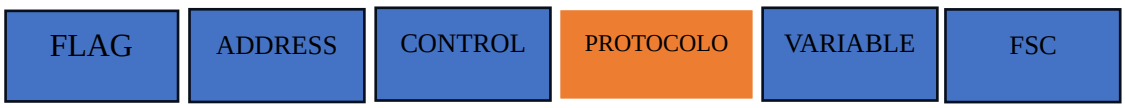


Figura 1: trama HDLC de Cisco

A diferencia del HDLC Estándar el de Cisco usa un campo de datos de protocolo para admitir entornos multiprotocolo.

HDLC se centra en la estructura de las tramas de datos y en cómo se comunican los dispositivos a nivel de enlace de datos. Por otro lado, los protocolos de seguridad como WEP, WPA, WPA2 y WPA3 están específicamente diseñados para asegurar la comunicación inalámbrica en las redes Wi-Fi.

Áreas críticas en redes domésticas.

En los ámbitos de la seguridad informática es importante tener el conocimiento y entender los diferentes tipos de ataques donde puedan comprometer la integridad.

A continuación, se presenta esta tabla detallada de algunos ataques comunes junto a una breve explicación de cada uno.

ATAQUE	DETALLE
Ataque de fuerza bruto	Por medio de este ataque se intenta adivinar la contraseña probando múltiples combinaciones hasta tener éxito
Ataque de diccionario	Esto se me hace en palabras y combinaciones en una lista extensa
Ataque phishing	Este ataque se envían mensajes falsos o correos para engañar a los usuarios y obtener información
Ataque de denegación de servicios	Es sobrecargar la red o los dispositivos con un tráfico de malicioso esto puede ser muchas solicitudes
Ataque de redes inalámbricas abiertas	Al tener una configuración incorrecta de la red cualquier dispositivo podría conectarse
Ataque de explotación de vulnerabilidades	Los atacantes aprovechan las debilidades sean configuraciones o dispositivos de esa red
Ataque de suplantación de identidad	Un atacante se hace pasar por un usuario legítimo para poder acceder a la red y servicios

Tabla 10:Cuadro áreas criticas

Vulnerabilidades de Los Protocolos de Seguridad

En esta tabla observamos las redes inalámbricas en un aspecto crucial en la protección de la informacion y como el acceso a los recursos de la red

Diferentes protocolos de seguridad Wifi a lo largo de tiempo han sido desarrollados cada uno con sus fortalezas y debilidades .Se presenta la siguiente informacion un resumen de las vulnerabilidades más significativas asociadas a cada uno de los principales protocolos de seguridad desde WEP hasta WPA3.

Dado que para la selección y configuración de estas medidas de seguridad en los entornos inalámbricos deben ser adecuados.

Protocolo	Vulnerabilidad
WEP (Wired Equivalent Privacy)	• Vulnerabilidad a ataques de diccionario • Vulnerabilidad a ataques de reinyección
WPA (Wi-Fi Protected Access)	• Vulnerabilidades de fuerza bruta • Vulnerabilidad a ataques de reinyección
WPA2 (Wi-Fi Protected Access 2)	• Vulnerabilidad a KRACK (Key Reinstallation Attacks) • Vulnerabilidades de fuerza bruta
WPA3 (Wi-Fi Protected Access 3)	Aunque WPA3 fue diseñado para abordar muchas de las vulnerabilidades presentes en sus predecesores, aún puede haber vulnerabilidades emergentes o desconocidas que puedan ser descubiertas con el tiempo.

Tabla 11:Vulnerabilidades Efectivas para cada Protocolo

WPS Activado

Es primordial percatarse al momento del escaneo si presenta la activación del protocolo WPS (Configuración de Wi-Fi Protegida) este método facilita la conexión de los dispositivos sin necesidad de introducir contraseña [50].

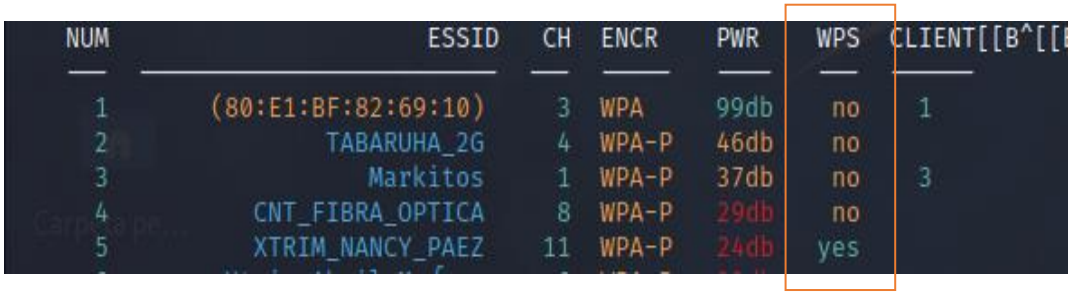


Fig. 13. Protocolo WPS activado

En la figura podemos se aprecia que 4 redes no tienen activado el protocolo WPS en su configuración por lo cual el “No “y en una red sí está activo. Podemos observar con más detalle(Wifite).

Wps Null Pin: este ataque WPS NULL PIN aprovecha de ciertas implementaciones defectuosas del WPS en aceptar el PIN de valor ´00000000´ o nulo como valido. Lo que hace efectivo este ataque cuando el punto de acceso tiene activado el WPS vulnerable permitiendo que el atacante conectarse a la red sin conocer el PIN correcto.

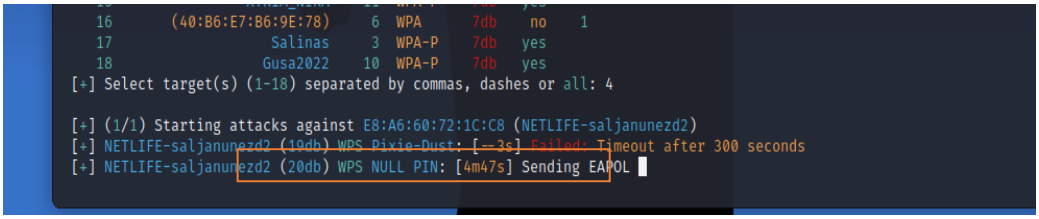


Fig. 14. ataque Wps Null Pin

Ataque Pixie-Dust

Este ataque explota una debilidad en el proceso de autentificación WPS para encontrar el PIN la cual busca capturar datos específicos durante el proceso [51]. La vulnerabilidad conocida como ataque Pixie-Dust afecta al Protocolo de Configuración Protegida de Wi-Fi (WPS). Esta vulnerabilidad se aprovecha de fallos en la forma en que se lleva a cabo el intercambio de claves E-S1 y E-S2 durante la configuración del WPS. En ciertas circunstancias, este fallo permite a un atacante calcular el PIN WPS en un corto periodo de tiempo, sin la necesidad de realizar un ataque de fuerza bruta prolongado.

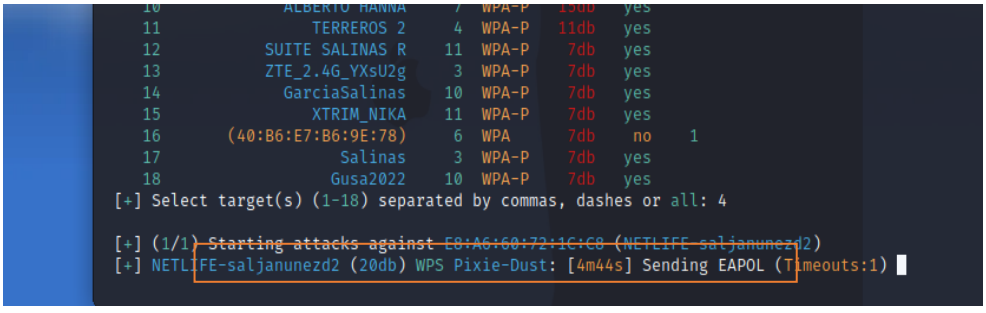


Fig. 15. Ataque Wps Pixie-Dust

El Ataque de PIN WPS

El uso de la técnica de fuerza bruta para descifrar el PIN del Protocolo de Configuración Protegida de Wi-Fi (WPS). Este protocolo segmenta el PIN en dos partes de cuatro dígitos cada una, lo que permite a un atacante disminuir considerablemente la cantidad de combinaciones que debe probar. Una vez que el atacante identifica el PIN correcto, puede acceder a la clave de seguridad WPA/WPA2 de la red.

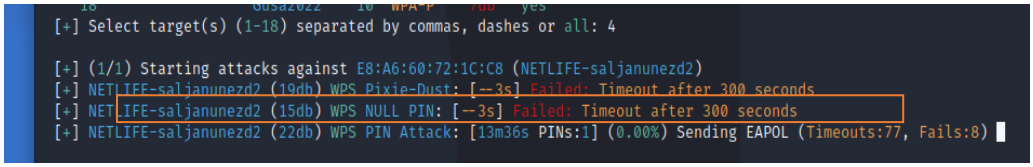


Fig. 16. Ataque Pin Attacks

Ataque PMKID (Pairwise Master Key Identifier)

La captura es una técnica para obtener el identificador de la clave maestra, utilizado en la fase de autenticación en redes WPA/WPA2. Este método no requiere que un cliente esté actualmente asociado con el punto de acceso, lo que facilita la captura del PMKID. Una vez capturado, un atacante puede intentar derivar la contraseña utilizando técnicas de fuerza bruta o diccionario.

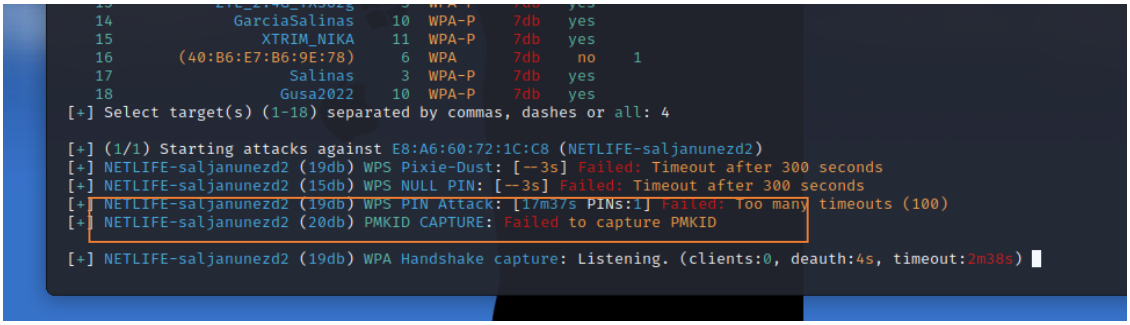


Fig. 17. Ataque PMKID capture

Ataque Pyrit Utiliza técnicas como generación de tablas de Hash Recalculadas también conocida como tablas Rainbow (contraseñas y hashes correspondientes en comparación de otros ataques de fuerza bruta) esto lo hace para la comprobación de contraseñas mediante la comparación de hash [52].

Ataque De Diccionario Es una técnica utilizada para descifrar contraseñas en Redes Wi-Fi la cual utiliza contraseñas o claves precompartida con múltiples combinaciones de caracteres y numéricas almacenadas en un archivo conocido como diccionario.

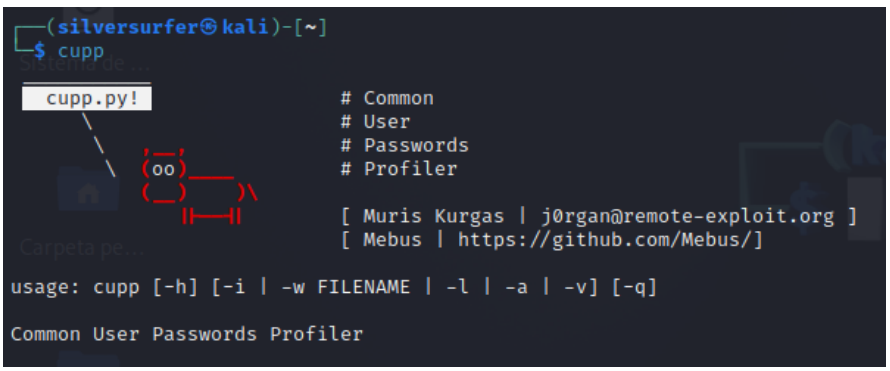


Fig. 18. Creación de Diccionario Cupp

Para este caso utilizaremos dos diccionarios la más conocida es Rockyou.txt que viene por defecto por la distribución de Kali Linux y Cupp esta herramienta te hará preguntas sobre el objeto para crear el diccionario tales como: Nombre ,Apellido, Nick-Name, Cedula de Identidad, Cumpleaños ,Mascotas

Vulnerabilidades Físicas De Redes Inalámbricas: Las vulnerabilidades físicas en este tipo de redes domésticas representan significativamente una amenaza para la seguridad la cual, permitir el acceso no autorizado a dispositivos desconocidos tiene como vulnerabilidades físicas más comunes.

Acceso Físico Al Enrutador: Dicho esto, el atacante tiene acceso físico a enrutador puede realizar cambios en su configuración y restablecer contraseñas e incluso podría instalar firmware muchas veces maliciosas.

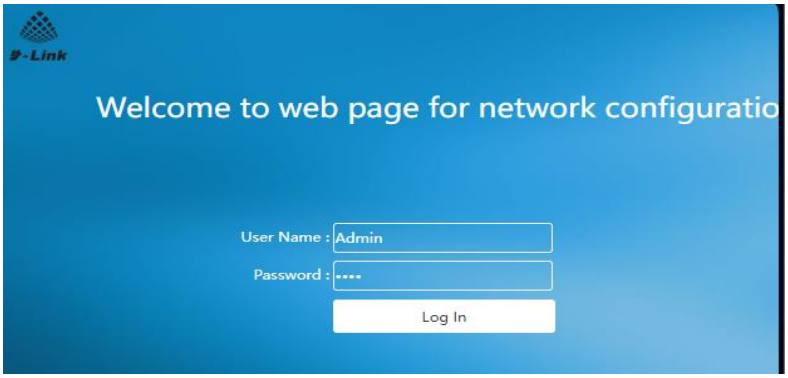


Fig. 19. Default Admin en Router

Muchos casos los Router viene por defecto la clave Usuario: Admin y Password: root desde ese punto ya estamos en una vulnerabilidad evidente cuyas claves se encuentran colgadas en sitios webs de los proveedores.

Herramientas De Aircrack-Ng

Herramientas	Descripción
Airodump-ng	Esta herramienta se utiliza para capturar paquetes de datos de redes Wi-Fi. Permite a los usuarios recopilar información sobre las redes inalámbricas cercanas, como SSID, direcciones MAC, canales y clientes conectados.
Aireplay-ng	Aireplay-ng se utiliza para inyectar tráfico en una red Wi-Fi, puede utilizarse para realizar ataques de desautenticación, de manera que los usuarios legítimos sean desconectados de la red.
Aircrack-ng	Aircrack-ng utiliza técnicas de fuerza bruta y diccionario para intentar descifrar las claves de cifrado.
Airmon-ng	Se utiliza para poner una interfaz de red inalámbrica en modo

Herramientas	Descripción
	monitor, lo que permite la captura de paquetes y la monitorización del tráfico de red.
Airbase-ng	Esta herramienta se utiliza para crear puntos de acceso falsos (AP) y realizar ataques de Rogue AP para probar la seguridad de las redes inalámbricas.
Airolib-ng	Se utiliza para manejar bases de datos de contraseñas y realizar ataques de recuperación de claves más eficientes, especialmente en el caso de contraseñas precompartidas (PSK).

Tabla 12. Herramientas de Aircrack-ng

FASE 3.- EXPLOTACIÓN

En esta etapa de explotación se ejecuta ataques de fuerza bruta a los protocolos de seguridad de tipo WPE, WPA, WPA2, WPA3 dentro de las redes inalámbricas seleccionadas (WLAN) mediante herramientas preseleccionadas como Aircrack-ng, Linset, Wifite este arsenal fue fundamental para el desarrollo de este proyecto.

AIRCRACK-NG: Ataque De Ingeniería Social

Aircrack-ng se despliega una evaluación en las llaves de encriptación esto conlleva a un ataque de diccionario de fuerza bruta meticuloso en las contraseñas permitiendo identificar patrones débiles. En el proceso de la auditoría de seguridad en la red wifi esta herramienta procura capturar paquetes de tráfico de la red específica utilizando "airodump-ng". Posteriormente realizar el diccionario con la herramienta Cupp (Fig. 18. Creación de Diccionario Cupp) y por default como rockyou.txt para el ataque. (vulnerabilidad con Aircrack-ng).

Fig. 20: Kali Linux y sus herramientas

WIFITE: Protocolo WPS : En esta herramienta sí incluyes el protocolo WPS puedes detectar y aprovechar la vulnerabilidad en que algunos Router específicos tienen activado este protocolo intentando descifrar con pin de acceso se lo se logró mediante la generación de pruebas de múltiples combinaciones de PIN lo que con ciertos casos permitió obtener el acceso no autorizado cómo podemos observar en la imagen (vulnerabilidad Wifite).

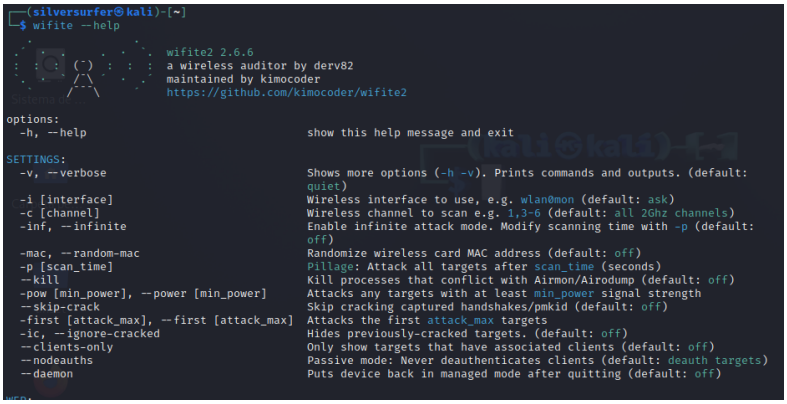


Fig. 21. WIFITE 2.6.6 y sus utilidades

LINSET: Evil Twin Attacks: El ataque que podríamos realizar con Linset son relacionados con creaciones de punto de acceso falsos que imitan las redes de wifi legitimas. Para llevar a cabo este tipo de ataque de suplantación de identidad de la red wifi se aprovecha posibles vulnerabilidades y desconocimientos que engañan a los dispositivos a conectarse a dicha red creando la famosa FakeAp. (FASE DE EXPLOTACION LINSET).

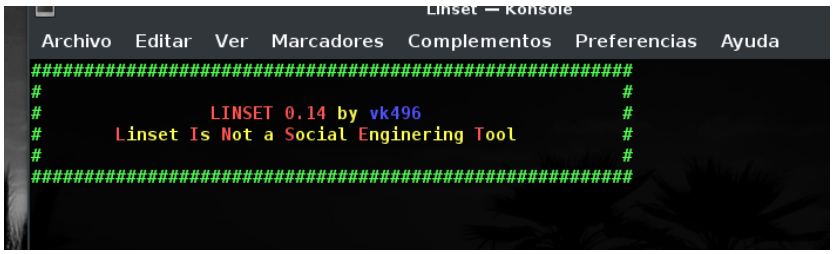


Fig. 22. LINSET Evil Twin Attacks

FASE 4.- ELABORACIÓN DE REPORTE

El reporte incluye tablas que contienen los resultados obtenidos durante la auditoría de seguridad, estas tablas ofrecen una visión detallada de los datos recolectados, las herramientas utilizadas, los procedimientos seguidos y los resultados obtenidos.

Tablas de reporte del sector Salinas

REPORTE DE EVALUACIÓN DE VULNERABILIDADES EN LA RED			
DATOS DE LUGAR			
Alcance Aprox.		150 metros Aprox con obstáculos	
Lugar		Salinas	
No. Prueba:		A-02	
DATOS DEL EXPERIMENTO			
ESSID	CH	ENCRIP	PWR
XTRIM_ROGE	4	WPA2-P	22 dBw
WPS		No	
FRECUENCIA		2,4GHz	
DETALLES DEL EXPERIMENTO			
Obj. del experimento:	Diccionario	Fase:	Adquisición de evidencia
Nivel Complejidad:	Medio	Tiempo ejecución:	1 hora 30 minutos
HERRAMIENTAS APLICADAS			
Hardware:	LAPTOP	Virtualización:	
	Antena TP-LINK WN722N		Kali Linux
Software:		Redes:	wifi domestica
	Aircrack-ng		Red móvil
HERRAMIENTAS			
HERRAMIENTA UTILIZADA:		Resultados obtenidos:	
Aircrack-ng	SI	clave :	@0914378880@
Wifite	NO		
Linset	NO		
TIPO DE ATAQUE			
Diccionario	PMKID	PIXIE DUST	NULL PIN
SI	NO	NO	NO
HANDSHAKE		SI	
DISEÑO DEL EXPERIMENTO			
Procedimientos:		Descripción del procedimiento:	
1. Escaneo de la red			
2.Seleccion		anexo 1	
3.Verificacion de protocolo			
5.Ataque			
Estado de la prueba		Validado	

Tabla 13: Reporte 1 WPA2 Salinas

Debido a la implementación de técnicas de ingeniería social para generar un diccionario específico para esa red, se ha identificado que los proveedores de servicios de Internet utilizan los números de identificación del propietario como clave principal.

REPORTE DE EVALUACIÓN DE VULNERABILIDADES EN LA RED			
DATOS DE LUGAR			
Alcance Aprox.		150 metros Aprox con obstáculos	
Lugar		Salinas	
No. Prueba:		A-01	
DATOS DEL EXPERIMENTO			
ESSID	CH	ENCRIP	PWR
MARKITOS	1	WPA2-P	61 dBw
WPS		No	
FRECUENCIA		2,4GHz	
DETALLES DEL EXPERIMENTO			
Obj. del experimento:	WPS ACTIVADO	Fase:	Adquisición de evidencia
Nivel Complejidad:	FACIL	Tiempo ejecución:	10 MINUTOS
HERRAMIENTAS APLICADAS			
Hardware:	LAPTOP	Virtualización:	
	Antena TP-LINK WN722N		Kali Linux
Software:		Redes:	wifi domestica
	Wifite 2.2.6 v		Red móvil
HERRAMIENTAS			
HERRAMIENTA UTILIZADA:		Resultados obtenidos:	
Aircrack-ng	NO	clave :	EspantaFoca123
Wifite	SI		
Linset	NO		
TIPO DE ATAQUE			
Diccionario	PMKID	PIXIE DUST	NULL PIN
No	Si	NO	NO
HANDSHAKE			No
DISEÑO DEL EXPERIMENTO			
Procedimientos:		Descripción del procedimiento:	
1. Escaneo de la red **2.Seleccion** **3.Verificacion de protocolo** **5.Ataque**			 Anexo 2
Estado de la prueba			Validado

Tabla 14: Reporte 2 WPA2 Salinas

Dado que la red tenía el protocolo WPS activado, es posible utilizar la herramienta Wifite, que realiza ataques aprovechando este protocolo. Incluso si la contraseña es robusta, puede ser descifrada mediante estos ataques.

REPORTE DE EVALUACIÓN DE VULNERABILIDADES EN LA RED			
DATOS DE LUGAR			
Alcance Aprox.		150 metros Aprox. con obstáculos	
Lugar		Salinas	
No. Prueba:		A-01	
DATOS DEL EXPERIMENTO			
ESSID	CH	ENCRIP	PWR
TABARUHA_2G	7	WPA2-P	38 dBw
WPS		No	
FRECUENCIA		2,4GHz	
DETALLES DEL EXPERIMENTO			
Obj. del experimento:	WPS ACTIVADO	Fase:	Adquisición de evidencia
Nivel Complejidad:	FACIL	Tiempo ejecución:	10 MINUTOS
HERRAMIENTAS APLICADAS			
Hardware:	LAPTOP	Virtualización:	
	Antena TP-LINK WN722N		Kali Linux
Software:		Redes:	wifi domestica
	Wifite 2.2.6 v		Red móvil
HERRAMIENTAS			
HERRAMIENTA UTILIZADA:		Resultados obtenidos:	
Aircrack-ng	NO	clave :	Tabaruasalinas2
Wifite	NO		
Linset	SI		
TIPO DE ATAQUE			
Diccionario	PMKID	PIXIE DUST	Fake Ap
No	No	No	Si
HANDSHAKE			Si
DISEÑO DEL EXPERIMENTO			
Procedimientos:		Descripción del procedimiento:	
1. Escaneo de la red **2.Seleccion** **3.Verificacion de protocolo** **5.Ataque**			 anexo 3
Estado de la prueba			Validado

Tabla 15:Reporte 3 WPA Salinas

Una de las funcionalidades de LINSET es la capacidad de ejecutar varios tipos de ataques para descifrar la contraseña de la red. En este caso particular, la herramienta no logró obtener la contraseña mediante la creación de una red falsa en la que el dispositivo objetivo ingresó la contraseña.

Tabla de la red sector La Libertad

REPORTE DE EVALUACIÓN DE VULNERABILIDADES EN LA RED			
DATOS DE LUGAR			
Alcance Aprox.		150 metros Aprox. con obstáculos	
Lugar		La Libertad	
No. Prueba:		B-01	
DATOS DEL EXPERIMENTO			
ESSID	CH	ENCRIP	PWR
FAMILIA_COBOS	6	WPA2-P	75 dBw
WPS		No	
FRECUENCIA		2,4GHz	
DETALLES DEL EXPERIMENTO			
Obj. del experimento:	WPS ACTIVADO	Fase:	Adquisición de evidencia
Nivel Complejidad:	FACIL	Tiempo ejecución:	41 MINUTOS
HERRAMIENTAS APLICADAS			
Hardware:	LAPTOP	Virtualización:	
	Antena TP-LINK WN722N		Kali Linux
Software:		Redes:	wifi domestica
	Aircrack-ng		Red móvil
HERRAMIENTAS			
HERRAMIENTA UTILIZADA:		Resultados obtenidos:	
Aircrack-ng	SI	clave :	2450395054COBOS
Wifite	NO		
Linset	NO		
TIPO DE ATAQUE			
Diccionario	PMKID	PIXIE DUST	NULL PIN
No	No	No	NO
HANDSHAKE		SI	
DISEÑO DEL EXPERIMENTO			
Procedimientos:		Descripción del procedimiento:	
1. Escaneo de la red **2.Seleccion** **3.Verificacion de protocolo** **5.Ataque**			 anexo 1
Estado de la prueba			Validado

Tabla 16: Reporte 4 WPA2 La Libertad

Identificando indicios en la red que sugerían la presencia de un nombre distintivo determino que el proveedor de servicios era Xtrim. Con esta información, generé un diccionario personalizado para utilizar con la suite de Aircrack-ng.

REPORTE DE EVALUACIÓN DE VULNERABILIDADES			
DATOS DE LUGAR			
Alcance Aprox.		150 metros Aprox. con obstáculos	
Lugar		La Libertad	
No. Prueba:		B-02	
DATOS DEL EXPERIMENTO			
ESSID	CH	ENCRIP	PWR
FAMILIA_COBOS	11	WPA3	99 dBw
WPS		No	
FRECUENCIA		2,4GHz	
DETALLES DEL EXPERIMENTO			
Obj. del experimento:	WPS OFF	Fase:	Adquisición de evidencia
Nivel Complejidad:	FACIL	Tiempo ejecución:	------
HERRAMIENTAS APLICADAS			
Hardware:	LAPTOP	Virtualización:	
	Antena TP-LINK WN722N		Kali Linux
Software:		Redes:	wifi domestica
	Aircrack-ng		Red móvil
HERRAMIENTAS			
HERRAMIENTA UTILIZADA:		Resultados obtenidos:	
Aircrack-ng	SI	clave :	
Wifite	NO		
Linset	NO		
TIPO DE ATAQUE			
Diccionario	PMKID	PIXIE DUST	NULL PIN
No	No	No	NO
HANDSHAKE		----	
DISEÑO DEL EXPERIMENTO			
Procedimientos:		Descripción del procedimiento:	
1. Escaneo de la red **2.Seleccion** **3.Verificacion de protocolo** **5.Ataque**			 anexo 1
Estado de la prueba			NO CONCLUYENTE

Tabla 17:Reporte 5 WPA3 La Libertad

Lamentablemente, no se pudo descifrar la contraseña debido a su protocolo de seguridad WPA3, que es robusto y resistente a este tipo de ataques.

Tabla de la red del sector Santa elena (Anexo 3)

REPORTE DE EVALUACIÓN DE VULNERABILIDADES EN LA RED			
DATOS DE LUGAR			
Alcance Aprox.		150 metros Aprox. con obstáculos	
Lugar		Santa Elena	
No. Prueba:		C-01	
DATOS DEL EXPERIMENTO			
ESSID	CH	ENCRIP	PWR
FAMILIA_SOLIZ	6	WEP	99 dBw
WPS		SI	
FRECUENCIA		2,4GHz	
DETALLES DEL EXPERIMENTO			
Obj. del experimento:	WPS OFF	Fase:	Adquisición de evidencia
Nivel Complejidad:	FACIL	Tiempo ejecución:	2 MINUTOS
HERRAMIENTAS APLICADAS			
Hardware:	LAPTOP	Virtualización:	
	Antena TP-LINK WN722N		Kali Linux
Software:		Redes:	wifi domestica
	Wifite 2.2.6v		Red móvil
HERRAMIENTAS			
HERRAMIENTA UTILIZADA:		Resultados obtenidos:	
Aircrack-ng	SI	clave :	Soliz123
Wifite	NO		
Linset	NO		
TIPO DE ATAQUE			
Diccionario	PMKID	PIXIE DUST	NULL PIN
No	No	No	NO
HANDSHAKE		----	
DISEÑO DEL EXPERIMENTO			
Procedimientos:		Descripción del procedimiento:	
1. Escaneo de la red			
2.Seleccion			anexo 2
3.Verificacion de protocolo			
5.Ataque			
Estado de la prueba			VALIDO

Tabla 18: Reporte 6 WEP Santa Elena

En este caso, la extracción de la clave se llevó a cabo utilizando la herramienta Wifite, ya que el protocolo WPS estaba activado y el protocolo de seguridad era WEP, que es muy vulnerable a este tipo de ataques.

Tabla de la red del sector Santa elena

REPORTE DE EVALUACIÓN DE VULNERABILIDADES EN LA RED			
DATOS DE LUGAR			
Alcance Aprox.		150 metros Aprox. con obstáculos	
Lugar		Santa Elena	
No. Prueba:		C-01	
DATOS DEL EXPERIMENTO			
ESSID	CH	ENCRIP	PWR
CASA_DIGITA	11	WPA	84 dBw
WPS		SI	
FRECUENCIA		2,4GHz	
DETALLES DEL EXPERIMENTO			
Obj. del experimento:	WPS OFF	Fase:	Adquisición de evidencia
Nivel Complejidad:	FACIL	Tiempo ejecución:	2 MINUTOS
HERRAMIENTAS APLICADAS			
Hardware:	LAPTOP	Virtualización:	
	Antena TP-LINK WN722N		Kali Linux
Software:		Redes:	wifi domestica
	Wifite 2.2.6v		Red móvil
HERRAMIENTAS			
HERRAMIENTA UTILIZADA:		Resultados obtenidos:	
Aircrack-ng	NO	clave :	12345678
Wifite	NO		
Linset	SI		
TIPO DE ATAQUE			
Diccionario	PMKID	PIXIE DUST	NULL PIN
No	No	NO	SI
HANDSHAKE		NO	
DISEÑO DEL EXPERIMENTO			
Procedimientos:		Descripción del procedimiento:	
1. Escaneo de la red **2.Seleccion** **3.Verificacion de protocolo** **5.Ataque**			 anexo 2
Estado de la prueba			VALIDADO

Tabla 19 Reporte 7 WPA Santa Elena

En este caso, la extracción de la clave se pudo llevar a cabo mediante la herramienta Wifite, a pesar de que el protocolo WPS estaba activado son demasiado vulnerables.

PROPUESTA DE BUENAS PRÁCTICAS

No existe una norma ISO específica aplicable exclusivamente al ámbito de las redes domésticas. No obstante, podemos considerar las siguientes normas ISO/IEC relevantes para este caso, ya que son aplicables tanto a entornos empresariales como a infraestructuras más pequeñas.

ISO/IEC 27001: De acuerdo a esta norma establece requisitos para un Sistema de Gestión de Seguridad de la Informacion también conocida (SGSI). Hay que tener claro que esta norma está muy orientada a empresas u organizaciones, pero los principios y controles podría bien adaptarse en un entorno domestico [53]. La aplicación de esta norma define políticas como gestión de activos , control de acceso y actualización de software.

ISO/IEC 27002: Proporciona un código de prácticas para las SGSI con un conjunto de implementos como el control de acceso , la criptografía y gestión de incidentes [53]. Esta norma específicamente es el uso de la criptografía (protocolo WPA3 y claves).

Además de adherirse a las normas ISO, es crucial otras prácticas recomendadas y estándares de seguridad esto firewalls para amenazas externas . La configuración de contraseñas robustas utilizando métodos de combinaciones seguras de letras números y caracteres especial.

Significativamente estas prácticas no solo cumplen con estándares sin que también fortalecen la seguridad de una red mitigando los riesgos potenciales y protegiendo a los usuarios

CONCLUSIONES

El uso de sistemas operativos virtualizados como Kali Linux y WiFi Slax, las cuales ambas están diseñadas para el pentesting para estos tipos de redes inalámbricas, dándoles un enfoque sobre las auditorias para la seguridad informática. Existen una variedad de herramientas que pueden ser utilizadas para este tipo de pruebas de descifrado de contraseñas, tanto como Linset que utiliza ataques de creación de una red falsa , Wifite que tiene búsquedas en tiempo real en puntos de acceso siempre y cuando el protocolo WPS esté activado sin necesidad de ataques de fuerza bruta o ataques diccionarios complejos , sin mencionar a Aircrack-ng con su amplia suite de herramientas aplicables en el contexto de auditorías de manera ética en estos tipos de protocolos de seguridad.

Se identifico 15 redes inalámbricas aproximadamente en tres zonas puntuales de la península de Santa Elena la cuales se detectaron protocolos WEP ,WPA,WPA2 en su mayoría y WPA3 en estas localidades Los protocolos WEP, WPA,WPA2 fueron vulnerados durante la investigación con técnicas de ataques de fuerza bruta ,ataques de diccionario , ataques de desautentificación , ataques WPS y Captura de handshakes

Para obtención de acceso a redes inalámbricas en esta investigación, se obtuvo un tiempo promedio de 2 minutos en Protocolos WEP y WPA , por otro lado, un tiempo un mínimo de 10 minutos hasta un estimado de una 1 hora en protocolos WPA2, como resultados se encontró una red WPA3 la cual no se concretó el ataque en ninguna de las herramientas ya antes mencionadas.

RECOMENDACIONES

Implementar buenas prácticas y el uso de estas herramientas, ya que la mayoría son Open Source y que siempre están en una actualización constante, los profesionales de la seguridad pueden identificar y explotar vulnerabilidades en redes Wi-Fi, permitiendo la implementación de medidas correctivas para fortalecer la seguridad.

Se plantea que las redes que fueron encontradas con protocolos WEP y WPA migren a protocolos como WPA2 e incluso WPA3 para fortalecer la seguridad de sus datos contra las amenazas, que empleen una buena configuración en gestión de contraseñas. Claro está que es muy difícil evitar ataques de este tipo de ingeniería social, ya sea en el ámbito doméstico o empresarial, es importante establecer políticas de seguridad claras y robustas, así como utilizar medidas de autenticación multifactor para añadir capas adicionales de protección a los sistemas.

Se recomienda llevar a cabo investigaciones adicionales sobre el descifrado de contraseñas utilizando unidades de procesamiento gráfico (GPU) y herramientas como HASHCAT , dado su potencial para acelerar significativamente el proceso de descifrado. Estas investigaciones podrían explorar en detalle los algoritmos y técnicas más eficientes para aprovechar al máximo el poder de cómputo de las GPU en este contexto. Asimismo, se sugiere investigar las implicaciones de seguridad y privacidad asociadas con el uso de esta tecnología, con el fin de desarrollar estrategias efectivas para mitigar posibles riesgos y vulnerabilidades.

BIBLIOGRAFIA

[1] M. I. Montero, «Criptografía y psicología de la contraseña: generando una contraseña fuerte para diferentes servicios», *Apuntes de Ciencia & Sociedad*, vol. 3, n.º 1, Art. n.º 1, jul. 2013, doi: 10.18259/acs.2013008.

[2] K. Juhász, V. Póser, M. Kozlovszky, y A. Bánáti, «WiFi vulnerability caused by SSID forgery in the IEEE 802.11 protocol», en *2019 IEEE 17th World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, ene. 2019, pp. 333-338. doi: 10.1109/SAMI.2019.8782775.

[3] I. A. Vivar Franco, «Aplicación de hacking ético para identificar amenazas, riesgos y vulnerabilidades en la red Wifi.», bachelorThesis, Babahoyo: UTB-FAFI. 2023, 2023. Accedido: 20 de septiembre de 2023. [En línea]. Disponible en: http://dspace.utb.edu.ec/handle/49000/14258

[4] J. L. Fernández-Alemán, A. Sánchez-Henarejos, V. M. García-Amicis, A. Toval, A. B. Sánchez-García, y I. Hernández-Hernández, «Estudio sobre la importancia y la seguridad de uso de las contraseñas en el ámbito laboral sanitario», *Gaceta Sanitaria*, vol. 29, n.º 1, pp. 74-76, feb. 2015, doi: 10.1016/j.gaceta.2014.07.003.

[5] «Oracle VM VirtualBox». Accedido: 27 de septiembre de 2023. [En línea]. Disponible en: https://www.oracle.com/es/virtualization/virtualbox/

[6] «Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution», Kali Linux. Accedido: 27 de septiembre de 2023. [En línea]. Disponible en: https://www.kali.org/

[7] «Nmap: the Network Mapper - Free Security Scanner». Accedido: 27 de septiembre de 2023. [En línea]. Disponible en: https://nmap.org/

[8] «Aircrack-ng». Accedido: 5 de julio de 2023. [En línea]. Disponible en: https://www.aircrack-ng.org/

[9] «Live Wifislax – GNU/Linux Wireless». Accedido: 5 de julio de 2023. [En línea]. Disponible en: https://www.wifislax.com/

[10] «Wireshark · Go Deep». Accedido: 27 de septiembre de 2023. [En línea]. Disponible en: https://www.wireshark.org/

[11] «¿Qué es un adaptador de red?» Accedido: 27 de septiembre de 2023. [En línea]. Disponible en: https://www.info-computer.com/blog/que-es-un-adaptador-de-red/

[12] G. A. Saavedra Rios, «Seguridad en redes inalámbricas domésticas», 2011, Accedido: 9 de octubre de 2023. [En línea]. Disponible en: http://repository.unilibre.edu.co/handle/10901/4612

[13] A. Paredes Risueño, «Redes Wi-Fi: ¿Realmente se pueden proteger?», jun. 2018, Accedido: 9 de octubre de 2023. [En línea]. Disponible en: https://openaccess.uoc.edu/handle/10609/81265

[14] «Plan-de-Creación-de-Oportunidades-2021-2025-Aprobado.pdf». Accedido: 18 de octubre de 2023. [En línea]. Disponible en: https://www.planificacion.gob.ec/wp-

content/uploads/2021/09/Plan-de-Creacio%CC%81n-de-Oportunidades-2021-2025-Aprobado.pdf

[15] J. T. P. García, «ANÁLISIS DE LOS PROTOCOLOS DE SEGURIDAD INALÁMBRICA IMPLEMENTADAS EN LAS REDES WIFI EN LA CIUDAD DE BOGOTÁ», 2022.

[16] R. KeepCoding, «¿Qué es handshake en informática? | KeepCoding Bootcamps». Accedido: 6 de noviembre de 2023. [En línea]. Disponible en: https://keepcoding.io/blog/que-es-handshake-en-informatica/

[17] L. A. Gil Lluís, «Estudio de los ataques y su defensa en la Ingeniería Social», mar. 2022, Accedido: 6 de noviembre de 2023. [En línea]. Disponible en: http://e-spacio.uned.es/fez/view/bibliuned:master-ETSInformatica-II-Lagil

[18] «deauthentication [Aircrack-ng]». Accedido: 6 de noviembre de 2023. [En línea]. Disponible en: https://www.aircrack-ng.org/doku.php?id=deauthentication

[19] «¿Qué son "WPA-PSK", "WPA2-PSK", "TKIP" y “AES”? | Brother». Accedido: 6 de noviembre de 2023. [En línea]. Disponible en: https://support.brother.com/g/b/faqend.aspx?c=mx&lang=es&prod=p900weus&faqid=faqp00100020_000

[20] D. Córdoba, «WPA2: ¿Cómo funciona este algoritmo? Seguridad Wi-Fi», Junco TIC. Accedido: 6 de noviembre de 2023. [En línea]. Disponible en: https://juncotic.com/wpa2-como-funciona-algoritmo-wifi/

[21] «Descripción general de 802.1X y tipos de EAP», Intel. Accedido: 6 de noviembre de 2023. [En línea]. Disponible en: https://www.intel.com/content/www/xl/es/support/articles/000006999/wireless/legacy-intel-wireless-products.html

[22] «Serie 27k». Accedido: 6 de noviembre de 2023. [En línea]. Disponible en: https://www.iso27000.es/iso27000.html

[23] «CCMP™ - The Association of Change Management Professionals». Accedido: 13 de noviembre de 2023. [En línea]. Disponible en: https://www.acmpglobal.org/page/ccmp

[24] «WEP, WPA, WPA2 y WPA3: diferencias y explicación», latam.kaspersky.com. Accedido: 31 de octubre de 2023. [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/wep-vs-wpa

[25] «¿Qué es el SSID y para qué sirve? - Definición», GEEKNETIC. Accedido: 6 de noviembre de 2023. [En línea]. Disponible en: https://www.geeknetic.es/SSID/que-es-y-para-que-sirve

[26] «Qué es el filtrado MAC y para qué sirve esta opción». Accedido: 6 de noviembre de 2023. [En línea]. Disponible en: https://www.testdevelocidad.es/2020/01/02/que-es-filtrado-mac-router/

[27] M. F. Miranda, «¿Qué es el IEEE y los estándares de Seguridad de la Información?» Accedido: 6 de noviembre de 2023. [En línea]. Disponible en:

https://www.deletetechnology.com/blog/qué-es-el-ieee-y-los-estándares-de-seguridad-de-la-información

[28] M. S. Gutiérrez, «MECANISMOS DE SEGURIDAD EN REDES INALÁMBRICAS».

[29] «WPS Wi-Fi Protected Setup: Qué es y cómo funciona este protocolo WiFi», RedesZone. Accedido: 15 de noviembre de 2023. [En línea]. Disponible en: https://www.redeszone.net/tutoriales/redes-wifi/wps-que-es-como-funciona/

[30] «Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution», Kali Linux. Accedido: 6 de noviembre de 2023. [En línea]. Disponible en: https://www.kali.org/

[31] «Sociedad – Live Wifislax». Accedido: 6 de noviembre de 2023. [En línea]. Disponible en: https://www.wifislax.com/category/wifislax-red-sociedad/

[32] «Manual Linset para crackear claves WPA y WPA2 de redes Wi-Fi», RedesZone. Accedido: 6 de noviembre de 2023. [En línea]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/crackear-redes-wi-fi-wpa-wpa2-linset/

[33] «wifite | Kali Linux Tools», Kali Linux. Accedido: 11 de junio de 2024. [En línea]. Disponible en: https://www.kali.org/tools/wifite/

[34] «Tornil - Seguridad en redes WLAN.pdf». Accedido: 25 de diciembre de 2023. [En línea]. Disponible en: https://openaccess.uoc.edu/bitstream/10609/142846/29/PLA7_Seguridad%20en%20redes%20WLAN.pdf

[35] X. P. Tornil, «Seguridad en redes WLAN».

[36] G. Singh, «WPA3: Next-Gen Security for Next-Gen Internet of Things», Copperpod IP. Accedido: 26 de diciembre de 2023. [En línea]. Disponible en: https://www.copperpodip.com/post/2018/04/11/wpa3-next-gen-security-for-next-gen-internet-of-things

[37] E. F. Medina Rojas, «Hacking ético: una herramienta para la seguridad informática», *instname:Universidad Piloto de Colombia*, feb. 2015, Accedido: 28 de mayo de 2024. [En línea]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2932

[38] J. Prenafeta, «Qué es pentesting y cómo detectar y prevenir ciberataques», Blog de hiberus. Accedido: 28 de mayo de 2024. [En línea]. Disponible en: https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/

[39] Ciberpyme, «Tipos de ciberataques: ataques a las conexiones inalámbricas.», Revista de Ciberseguridad y Seguridad de la Información para Empresas y Organismos Públicos. Accedido: 29 de mayo de 2024. [En línea]. Disponible en: https://www.ciberseguridadpyme.es/actualidad/ataques-a-las-conexiones/

[40] M. SL, «Tipos de redes inalámbricas | Blog MODI», modisl. Accedido: 13 de noviembre de 2023. [En línea]. Disponible en: https://www.modisl.com/post/tipos-redes-inalambricas

[41] «Overview of Wireless Metropolitan Area Network (WMAN)», GeeksforGeeks. Accedido: 13 de noviembre de 2023. [En línea]. Disponible en: https://www.geeksforgeeks.org/overview-of-wireless-metropolitan-area-network-wman/

[42] P. Gannon, «WW1: First World War communications and the "Tele-net of Things"». Accedido: 13 de noviembre de 2023. [En línea]. Disponible en: https://eandt.theiet.org/content/articles/2014/06/ww1-first-world-war-communications-and-the-tele-net-of-things/

[43] E. Bello, «¿Qué es pentesting? Cómo detectar tus debilidades ante un ciberataque», *Thinking for Innovation*, jun. 2022, Accedido: 14 de mayo de 2024. [En línea]. Disponible en: https://www.iebschool.com/blog/que-es-pentesting-tecnologia/

[44] «Asamblea Nacional del Ecuador», Asamblea Nacional del Ecuador. Accedido: 7 de noviembre de 2023. [En línea]. Disponible en: https://www.asambleanacional.gob.ec/es/leyes-aprobadas

[45] «Gaibor - UTILIZACIÓN DE HACKING ÉTICO PARA DIAGNOSTICAR, AN.pdf». Accedido: 24 de octubre de 2023. [En línea]. Disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf

[46] «Cruz Saavedra, Walter Gonzalo.pdf». Accedido: 24 de octubre de 2023. [En línea]. Disponible en: https://repositorio.upn.edu.pe/bitstream/handle/11537/10239/Cruz%20Saavedra%2c%20Walter%20Gonzalo.pdf?sequence=7&isAllowed=y

[47] A. Valle, L. Manrique, y D. Revilla, *La Investigación descriptiva con enfoque cualitativo en educación*. Pontificia Universidad Católica del Perú. Facultad de Educación, 2022. Accedido: 3 de noviembre de 2023. [En línea]. Disponible en: https://repositorio.pucp.edu.pe/index/handle/123456789/184559

[48] K. Srinagesh, *The Principles of Experimental Research*. 2006. doi: 10.1016/B978-0-7506-7926-8.X5000-6.

[49] «The Penetration Testing Execution Standard — pentest-standard 1.1 documentation». Accedido: 25 de octubre de 2023. [En línea]. Disponible en: https://pentest-standard.readthedocs.io/en/latest/index.html

[50] D. Zisiadis, S. Kopsidas, A. Varalis, y L. Tassiulas, «Enhancing WPS security», en *2012 IFIP Wireless Days*, nov. 2012, pp. 1-3. doi: 10.1109/WD.2012.6402836.

[51] «WPS Pixie Dust Attack (Offline WPS Attack)». Accedido: 23 de noviembre de 2023. [En línea]. Disponible en: https://forums.kali.org/showthread.php?24286-WPS-Pixie-Dust-Attack-(Offline-WPS-Attack)

[52] «Luengo - Ataques a WPA2 con Pyrit.pdf». Accedido: 23 de noviembre de 2023. [En línea]. Disponible en: https://openaccess.uoc.edu/bitstream/10609/73067/7/danielmartTFG0118memoria.pdf

[53] «Serie 27k». Accedido: 14 de junio de 2024. [En línea]. Disponible en: https://www.iso27000.es/iso27000.html

Link de Google :

https://www.copperpodip.com/post/2018/04/11/wpa3-next-gen-security-for-next-gen-internet-of-things

ANEXOS

ANEXOS 1

FASE DE ANALISIS O ESCANEO

En esta fase es muy importante la cual se tiene que tener en cuenta las herramientas que se utilizaran para este proyecto Kali Linux que contendrá las herramientas como Aircrack-ng y Wifite. Y WiFi Slax Os que almacena Linset.

Lamentablemente no trata de una guía de instalación ya que tendrías varias alternativas de previas a estos sistemas operativos sea por Images, Live Boot, Cloud y otras incluso los programas de virtualización tales como VirtualBox y VMware.

Una vez teniendo las herramientas seleccionadas e instaladas nos dirigimos a la ISO correspondiente en este caso Kali Linux como paso número la inicialización.

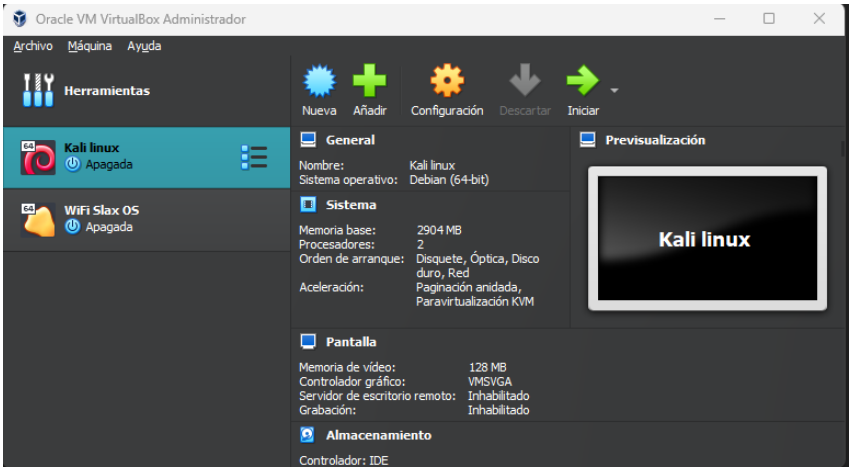


Fig. 23. Entorno VirtualBox

Iniciaras en el proceso mediante con un inicio de sesión, la cual deberás ingresar tanto el nombre de usuario y el clave correspondiente a dicha preinstalación para poder acceder al sistema.

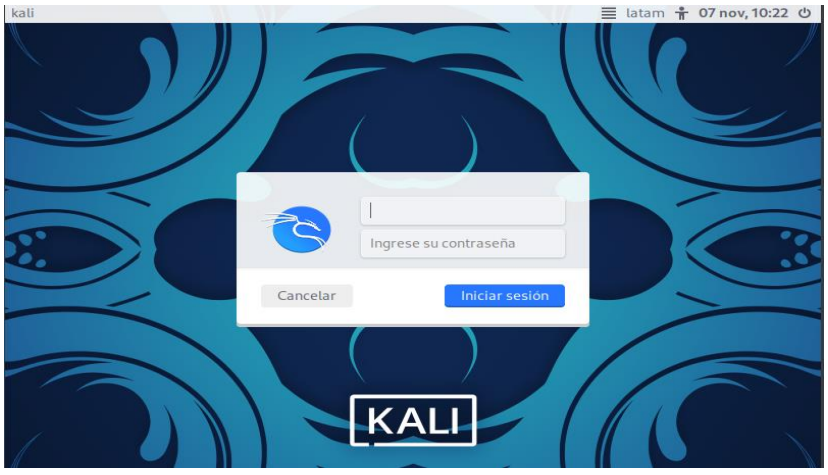


Fig. 24. Login Kali Linux

Encontraras un ambiente agradable para el usuario fácil de administrar a diferencia de otras distribuciones como Arch Linux y Parrot OS.

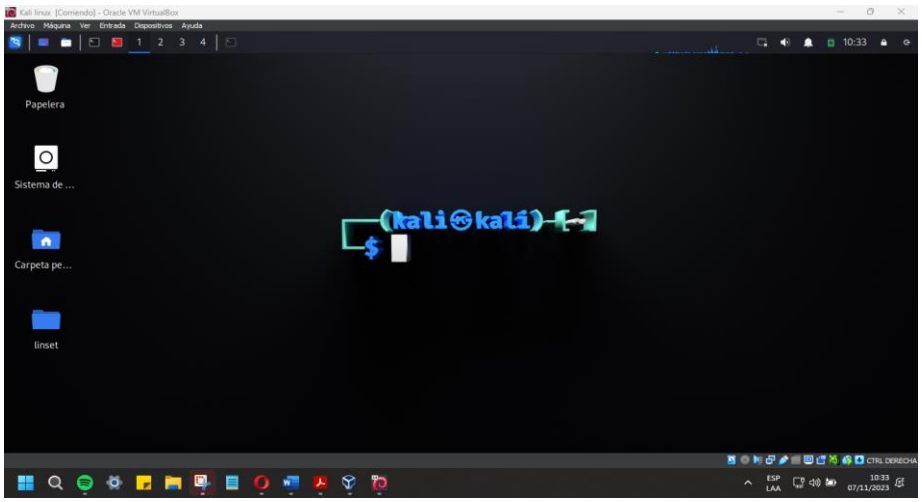


Fig. 25. Escritorio Kali

Algo importante en esta fase es tener identificado que tarjeta de red utilizaremos existe varios modelos y marcas la cual se utilizó de la marca TP-LINK los modelos TL-722N y TL-WN725N.

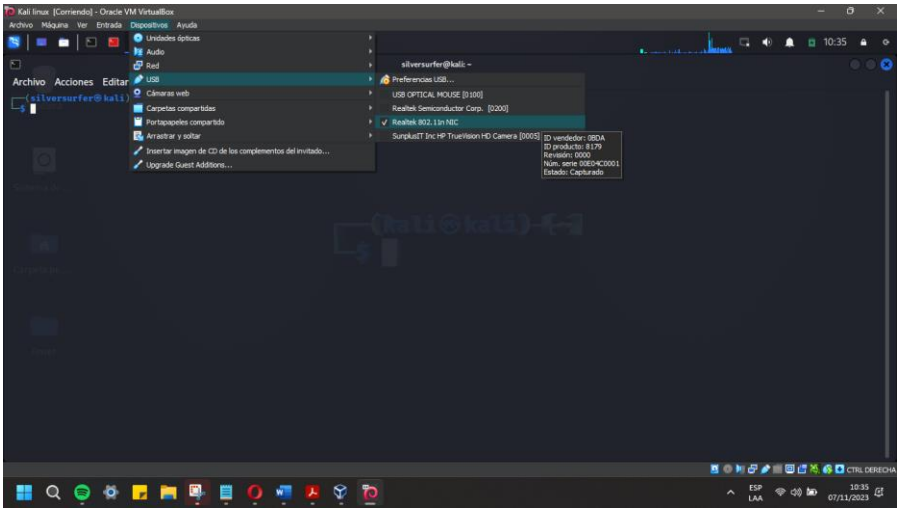


Fig. 26. Verificar el adaptador

El comando lsus se utiliza para enumerar todos los dispositivos USB conectados al sistema. Al ejecutar este comando, el sistema escanea los buses USB y presenta una lista detallada de los dispositivos detectados, mostrando información relevante como el

ID del fabricante y del producto, el número de bus y el dispositivo

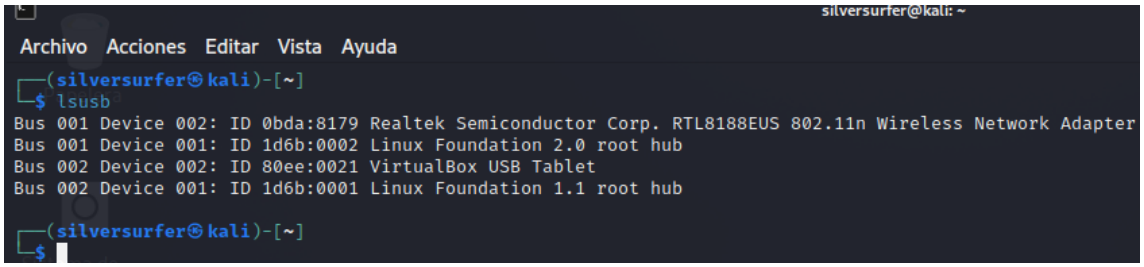


Fig. 27. Lista de Adaptador

Si queremos que nuestra tarjeta de red no registre la MAC por temas de seguridad para eludir restricciones basadas en direcciones MAC podemos utilizar el comando MACCHANGER -m (nos da la opción de cambiar la Mac manualmente)

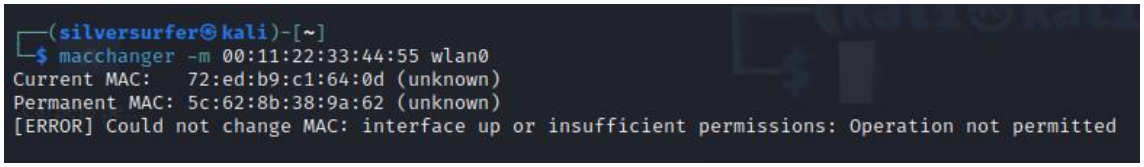


Fig. 28. Cambio de Mac de la tarjeta de red

Para inicializar la tarjeta de red y que este pase a modo monitor colocamos el siguiente comando:
sudo airmong-ng start wlan0

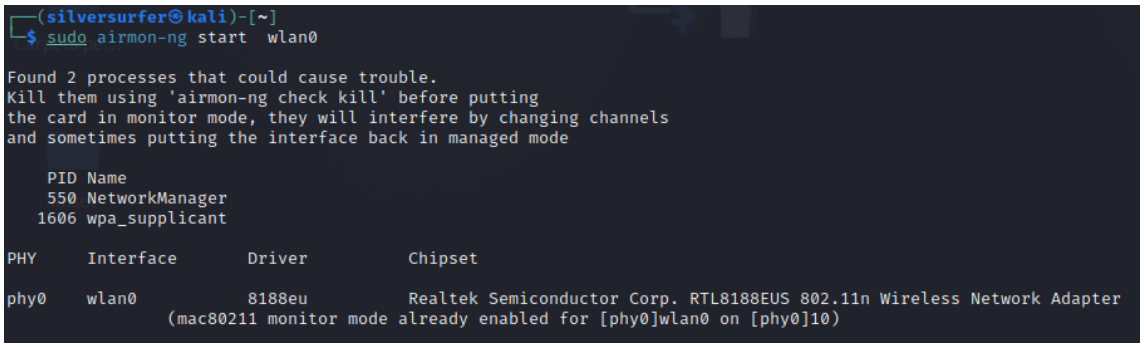


Fig. 29. Activar la tarjeta de red modo manager

Se utiliza para habilitar el modo monitor en la interfaz de red inalámbrica especificada, en este caso, wlan0. Ejecutar este comando con privilegios de superusuario (sudo) es necesario para obtener los permisos adecuados para modificar el estado de la interfaz de red.

ESCANEO DE AIRCRARCK-NG

Con "sudo airodump-ng wlan0 "este comando damos la inicialización en modo monitor previamente para escanear las redes cercanas la cual desplegará toda la información relevante que necesitaremos más adelante en la fase de explotación

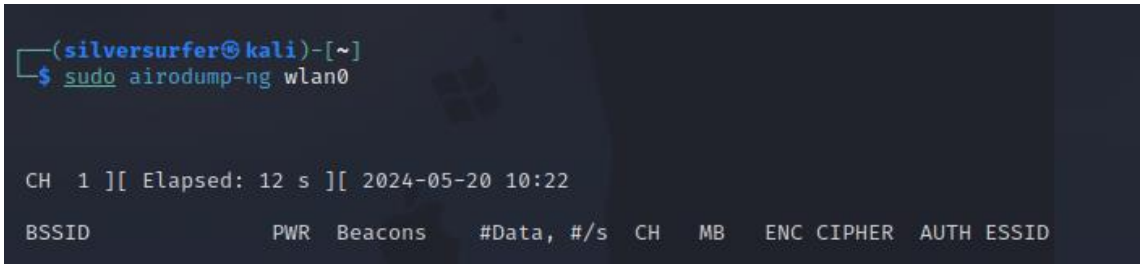


Fig. 30. Inicialización del escaneo

En la ventana de captura de redes cercanas, se presentarán diversos ítems que proporcionan información detallada sobre cada red detectada. Estos ítems incluyen:

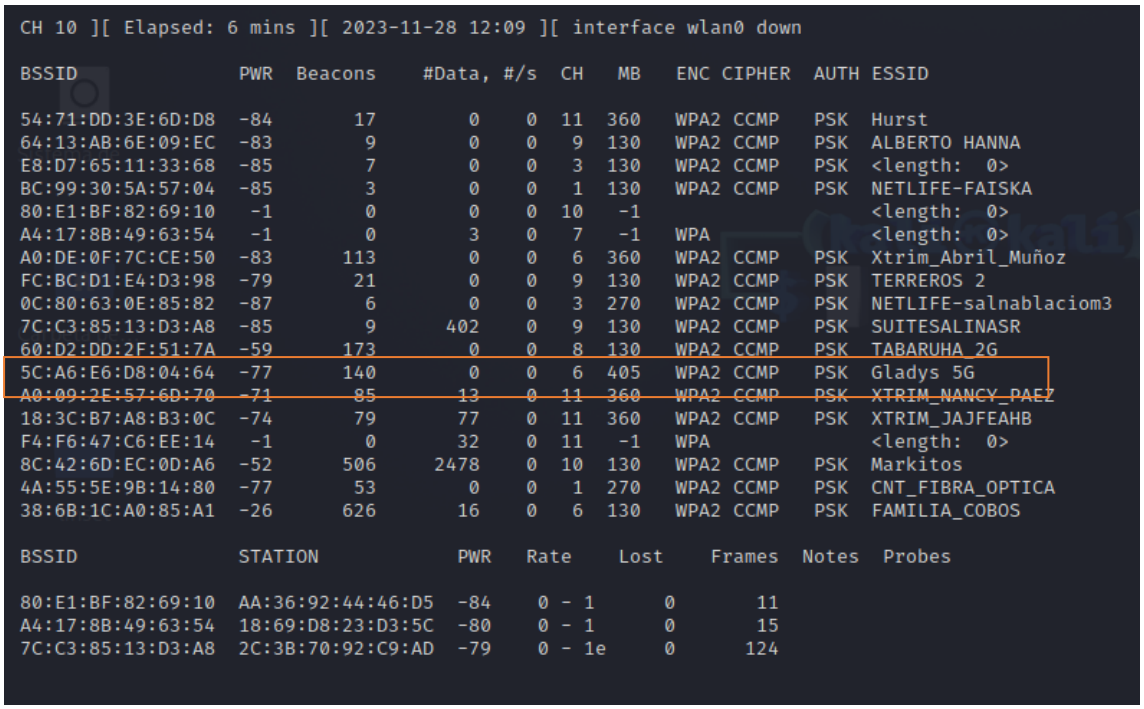


Fig. 31. Escaneo de Aircrack-ng

- **BSSID:** Dirección MAC del punto de acceso (Router) Wi-Fi.
- **PWR**: Potencia de la señal recibida del punto de acceso, en dBm.
- **Beacons:** Número de paquetes de Beacons enviados por el punto de acceso.
- **#Data:** Número de paquetes de datos capturados.
- **#/s:** Tasa de paquetes de datos por segundo.
- **CH:** Canal en el que está operando el punto de acceso.

- **MB:** Velocidad máxima de transmisión en Mbps.
- **ENC:** Tipo de cifrado utilizado (WPA, WPA2).
- **CIPHER**: Algoritmo de cifrado utilizado (CCMP).
- **AUTH:** Método de autenticación (PSK - Pre-Shared Key).
- **ESSID:** Nombre de la red inalámbrica (SSID).

Es crucial que identifiquemos y comprendamos exhaustivamente estos elementos durante el proceso de análisis de redes, ya que serán fundamentales para la ejecución efectiva de las etapas posteriores.

FASE DE EXPLOTACION DE AIRCRACK-NG

La terminal se ingresa el siguiente comando para dar al escaneo de esa red seleccionada: silversurfer (*) ~ sudo airodump-ng -c 6 -w cobos0 –bssid 38:6B:1C:A0:85:A1 wlan0

- El airodump-ng permite capturar y analizar la red seleccionada,
- -c: se utiliza para especificar el canal de radiofrecuencia en el que deseas que la herramienta escuche o monitoree en este caso es el 6.
- -w: se utiliza para especificar el archivo de salida donde se guardarán los datos capturados, la cual creará un archivo .cap que almacenará todo el tráfico de la red.
- --bssid: Esto es especialmente útil cuando se quiere enfocar en una única red inalámbrica en entornos con muchas redes disponibles.

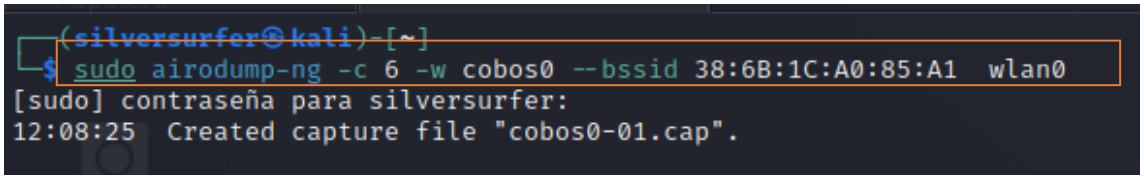


Fig. 32. Creación del archivo .cap

A continuación, se enumerarán varios ítems junto con otros términos previamente mencionados en la Tabla 3:Términos. Por ejemplo, el término "STATION" se refiere a los dispositivos que están conectados a la red. Además, se recopilará todo el tráfico generado por estos dispositivos, etiquetado como #data, lo que permitirá proceder al siguiente paso en el proceso de análisis. Esta recopilación exhaustiva de datos es fundamental para entender el comportamiento de la red y los patrones de tráfico, proporcionando una base sólida para futuras evaluaciones y medidas de seguridad.

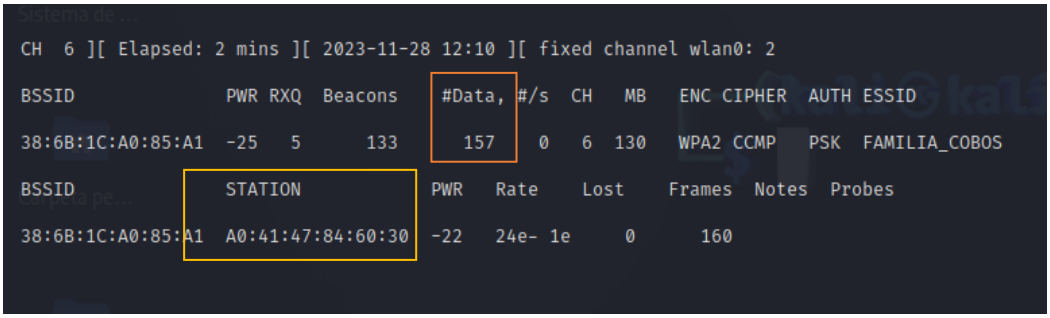


Fig. 33. Recolectando tráfico de la red seleccionada

A continuación , se describen varios modos de ataque comúnmente utilizados, cada uno con sus respectivas funcionalidades:

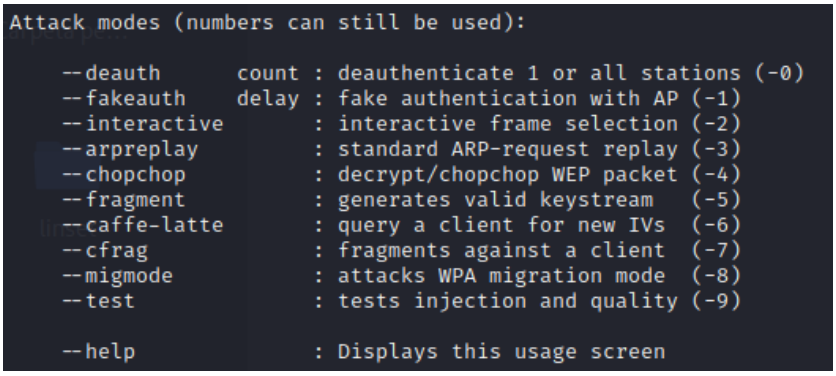


Fig. 34. Suite de herramientas de Aircrack-ng

Modos de Ataque y Descripción

- **deauth count:** Realiza un ataque de desautenticación, desconectando a uno o todos los dispositivos de una red. El parámetro count especifica la cantidad de intentos.
- **fakeauth delay:** Ejecuta una autenticación falsa con el punto de acceso (AP). El parámetro delay define el intervalo de tiempo entre intentos de autenticación.
- interactive: Permite la selección interactiva de tramas para inyección o análisis.
- **arpreplay:** Realiza una retransmisión estándar de solicitudes ARP para generar tráfico en una red, útil para ataques de recolección de IVs en WEP.
- **chopchop:** Desencripta paquetes WEP utilizando el ataque chopchop, que permite obtener la clave WEP sin necesidad de capturar un gran número de IVs.
- **fragment:** Genera un flujo de claves válido (keystream) mediante la fragmentación de paquetes, útil en ataques WEP.

- **caffe-latte:** Realiza un ataque para obtener nuevos vectores de inicialización (IVs) desde un cliente, útil en redes WEP.
- **cfrag:** Fragmenta paquetes contra un cliente específico, utilizado para obtener información necesaria en ataques de inyección.
- **mimode:** Ataca el modo de migración WPA (WPA Migration Mode), que puede estar presente en redes híbridas WPA/WEP.
- **test:** Prueba la capacidad de inyección y calidad de la señal para determinar la eficacia del ataque.
- **help**: Muestra la pantalla de ayuda con información sobre el uso de los modos de ataque.

Estos distintos métodos o modos de ataques que pueden ser utilizados por esta herramienta de auditoría de seguridad para penetrar duchas redes inalámbricas

Utilizando el comando "sudo aireplay-ng -0 5 -a (bssid) -c (station) wlan0", donde se sustituye el BSSID por la dirección MAC del enrutador objetivo y el STATION es la MAC del dispositivo conectado a esa red.

- **-0 5:** Indica que se enviarán 5 paquetes de desautenticación.
- **-a 38:6B:1C:A0:85:A1**: Especifica el BSSID del punto de acceso objetivo.
- **-c A0:41:47:84:60:30:** Especifica la dirección MAC del cliente que se desea desautenticar.
- **wlan0:** Es la interfaz de red en modo monitor.

El parámetro "-0" indica el ataque de desautenticación, mientras que el número "5" determina la cantidad de repeticiones del ataque, una opción que el atacante puede ajustar según su preferencia, como se ilustra en la imagen adjunta:

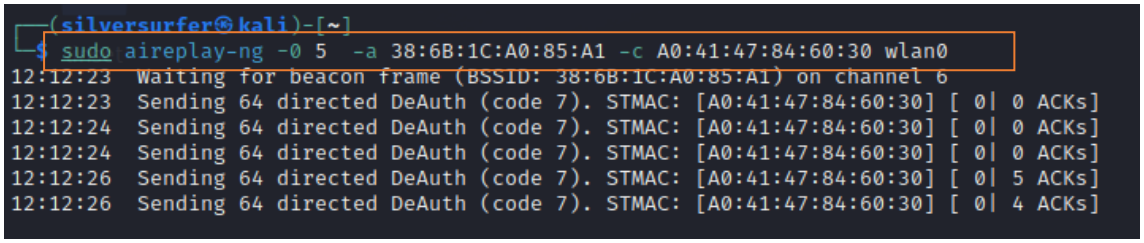


Fig. 35. Desautentificación

El siguiente paso es seleccionar el diccionario con el comando: sudo Aircrack-ng -w /usr/share/wordlists/rockyou.txt/ -b (bssid de la Mac) cobos-01.cap (archivo del tráfico)

```
┌──(silversurfer㉿kali)-[~]
└─$ aircrack-ng -w /usr/share/wordlists/rockyou.txt/ -b 38:6B:1C:A0:85:A1 cobos0-01.cap
```

Fig. 36. Aircrack-ng y el diccionario

- **Aircrack-ng:** Es el programa utilizado para descifrar claves WEP y WPA/WPA2 mediante ataques de fuerza bruta y diccionario.
- **-w /usr/share/wordlists/rockyou.txt/:** Especifica la ruta del archivo de diccionario. En este caso, se está utilizando el archivo rockyou.txt, que es un diccionario muy conocido y utilizado en pruebas de seguridad.
- **-b 38:6B:1C:A0:85:A1:** Especifica el BSSID del punto de acceso objetivo. Esto es opcional, pero puede ayudar a focalizar el ataque si hay múltiples handshakes en el archivo de captura.
- **cobos0-01.cap:** Es el archivo de captura que contiene el handshake necesario para intentar descifrar la clave de la red.

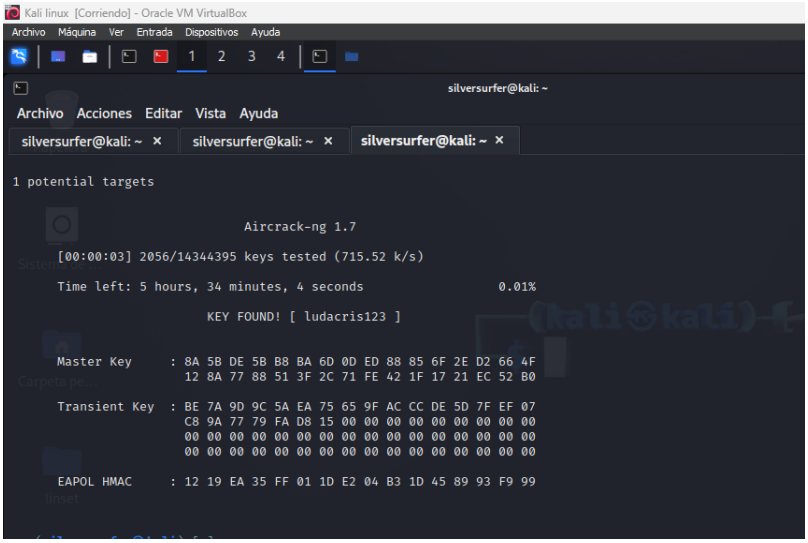


Fig. 37. Descifrar la contraseña

Una vez que Aircrack-ng encuentra la contraseña correcta en el archivo .cap donde contiene el tráfico de paquetes capturados mostrará un mensaje donde indicará la contraseña correspondiente.

Este proceso es fundamental en auditorías de seguridad para evaluar la robustez de las contraseñas utilizadas en redes inalámbricas y para identificar posibles vulnerabilidades en la configuración de la seguridad de la red.

ANEXO 2

ESCANEO DE WIFITE

En este caso la herramienta WIFITE la interfaz cambia rotundamente, pero con la misma informacion de los ítems.

Observación: esta herramienta es útil siempre y cuando la red tenga activado el protocolo WPS

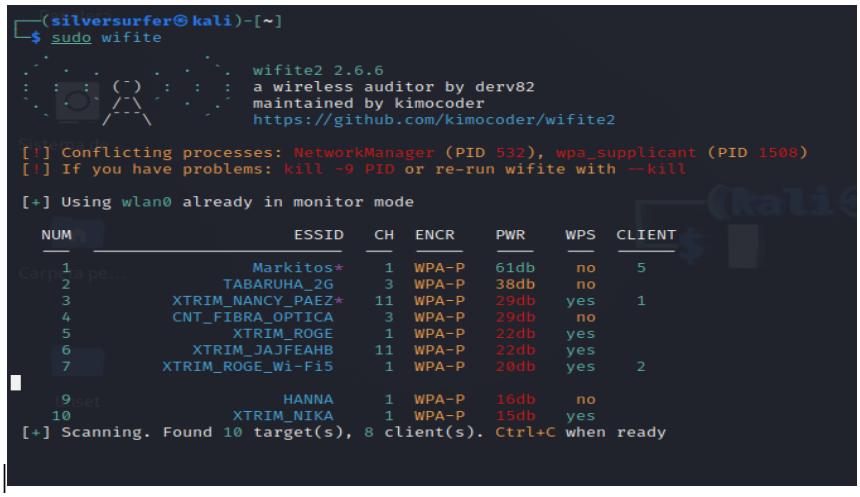


Fig. 38. Escaneo de Wifite

Una vez tenemos el objetivo dando pausa el escaneo CTRL+C procedemos a seleccionar la red del ítem NUM, nos indicará que número corresponde a cada red.

FASE DE EXPLOTACIÓN DE WIFITE

Para esta herramienta debes darte cuenta de la etiqueta WPS si esta activado “yes” por ende el protocoló esta activado lo cual facilita el ataque.

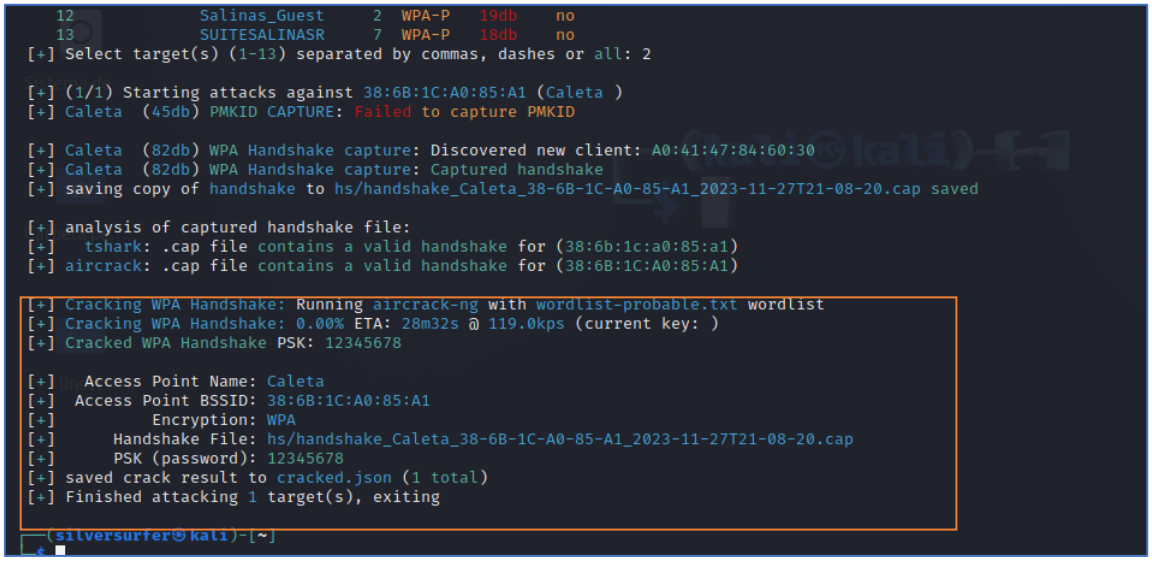


Fig. 39. ataque de Wifite con protocolo WPS activado

El ataque es automático como en la figura muestra falla el ataque PMKID y continua al ataque HANDSHARE y muestra todos los datos.

ANEXO 3

ESCANEO DE LINSET

En el caso de utilizar Linset, es imperativo seleccionar la tarjeta de red adecuada para que la herramienta pueda identificar las redes inalámbricas circundantes. Posteriormente, Linset configurará automáticamente la tarjeta en modo monitor.

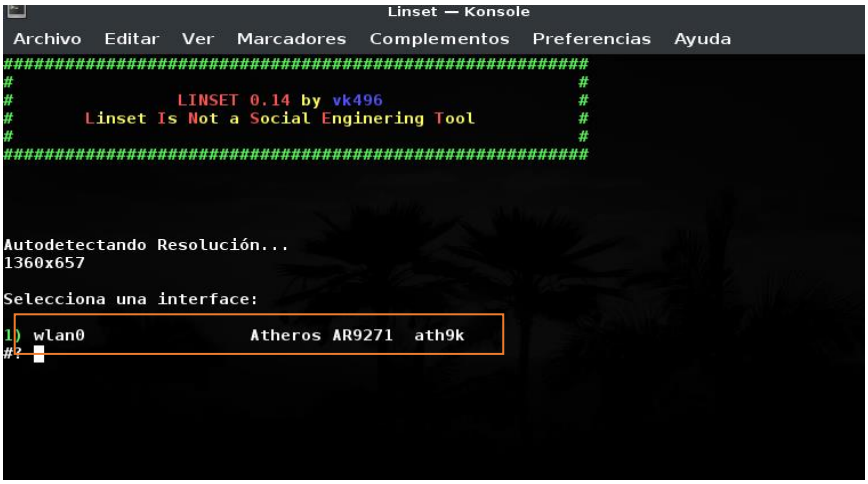


Fig. 40. Tarjeta de red reconocida por Linset

Como se muestra en la figura, es posible visualizar todas las redes disponibles junto con su respectivo protocolo y su ESSID (Nombre de la red). Por lo tanto, aquellas redes que no muestran un ESSID están ocultas.

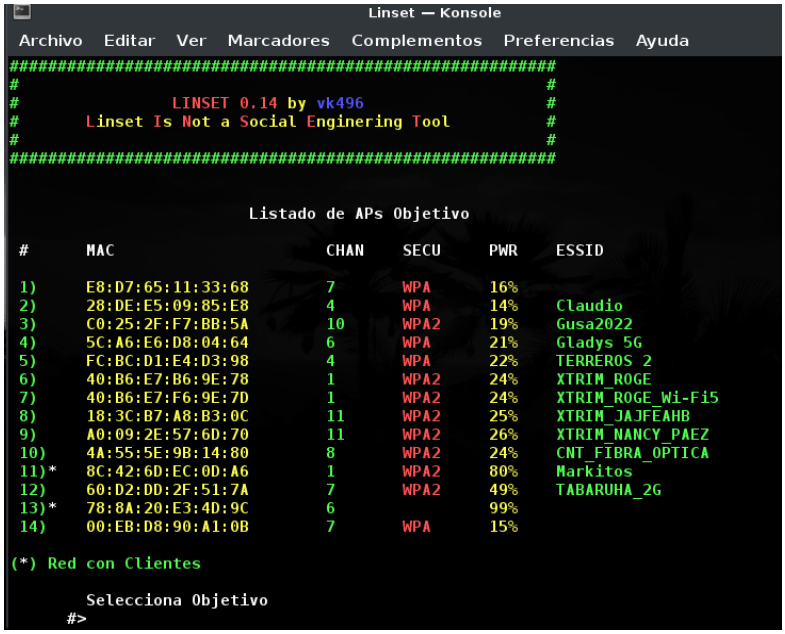


Fig. 41. Redes cercanas por Linset

FASE DE EXPLOTACION LINSET

Una vez seleccionada la red podemos observar la información de la misma como SSID Velocidad, canal y la Mac. En este paso dos opciones la cual nos permite utilizar dos tipos de script en acceso de punto fantasma de manera FakeAp.

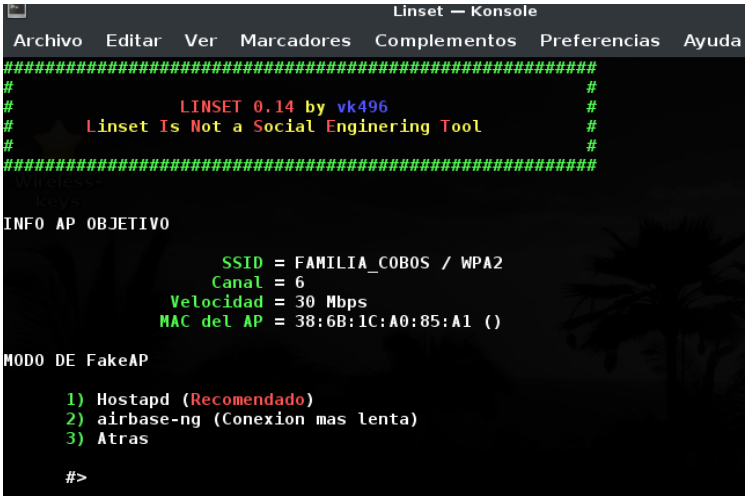


Fig. 42. Datos de la red y 2 ataques diferentes

Hostapd (Host Access Point Daemon) una selección de preferencia debido a su fiabilidad y eficiencia, representa un demonio que facilita la conversión de cualquier interfaz de red en un punto de acceso inalámbrico.

Por otro lado, Airbase-ng, integrante de la suite Aircrack-ng, se emplea para generar puntos de acceso falsos; sin embargo, su utilización se desaconseja en vista de su menor rendimiento y potenciales inconvenientes de estabilidad. Una herramienta utilizada en auditorias de seguridad para realizar ataques Evil Twin.

Fig. 43. Ruta del archivo .cap

Para capturar el handshake se elegirá el tipo de examinación dónde tenemos como ataque de Aircrack-ng y Pyrit se opta por la primera opción la cual Aircrack-ng (posibles fallos) pero es muy funcional en el ataque.

Pyrit es una utilidad que se enfoca en realizar ataques de fuerza bruta contra redes Wi-Fi haciendo uso de la potencia de procesamiento de unidades de procesamiento gráfico (GPU).

Figura 2:Aircrack posibles de fallo

En esta etapa se procede a seleccionar una desconexión con el fin de capturar el handshake, la cual, al emplearse como primera alternativa, tiene como propósito autenticar todos los clientes o dispositivos vinculados a la red.

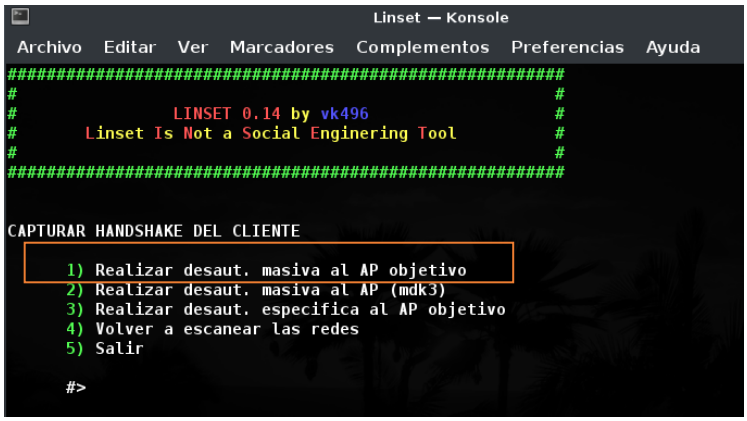


Fig. 44. Desaut. masiva al AP objetivo

Este procedimiento es de suma importancia, considerando todos los puntos donde la herramienta haya detectado el handshake, y verificando que el estado del handshake sea corrupto", lo cual indica que ha sido capturado exitosamente.

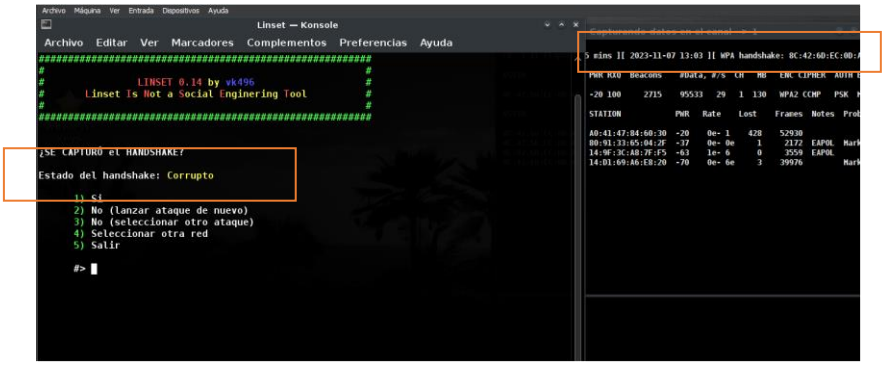


Fig. 45. Captura de Handshake Corrupto

Una vez capturado el handshake, se nos brinda la opción de seleccionar la interfaz de web Neuta como la primera alternativa. Esta acción resultará en la creación de una réplica exacta de la red.

A continuación, para configurar la interfaz como una interfaz web, es necesario seleccionar tanto la interfaz de red como el idioma deseado. Esta configuración se reflejará en la interfaz web que aparecerá al establecer la conexión con cualquier dispositivo vinculado a esa red. Posteriormente, se procede eligiendo la opción 2 para continuar con el proceso.

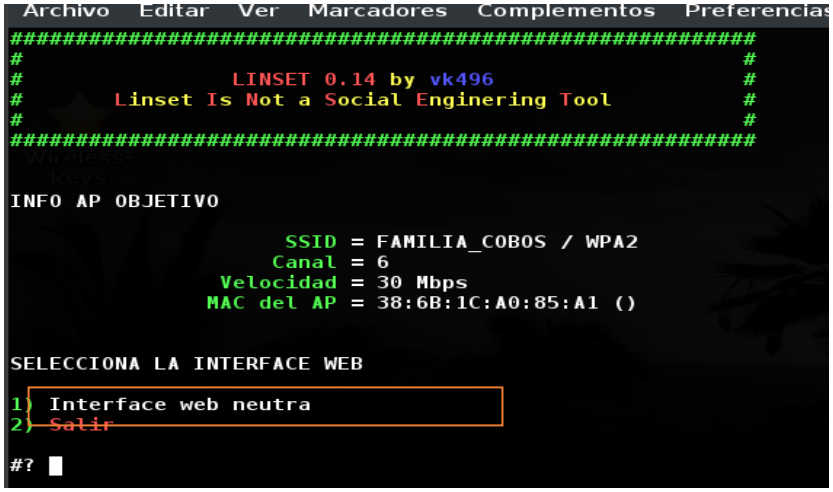


Fig. 46. Interface web neutra

Esta configuración garantiza una interacción coherente y comprensible para los usuarios de la red, facilitando un manejo adecuado de las funciones y opciones disponibles a través de la interfaz web seleccionada. El diseño de la interfaz web se ha optimizado para asegurar que los elementos de navegación sean intuitivos y accesibles, proporcionando una experiencia de usuario fluida y eficiente

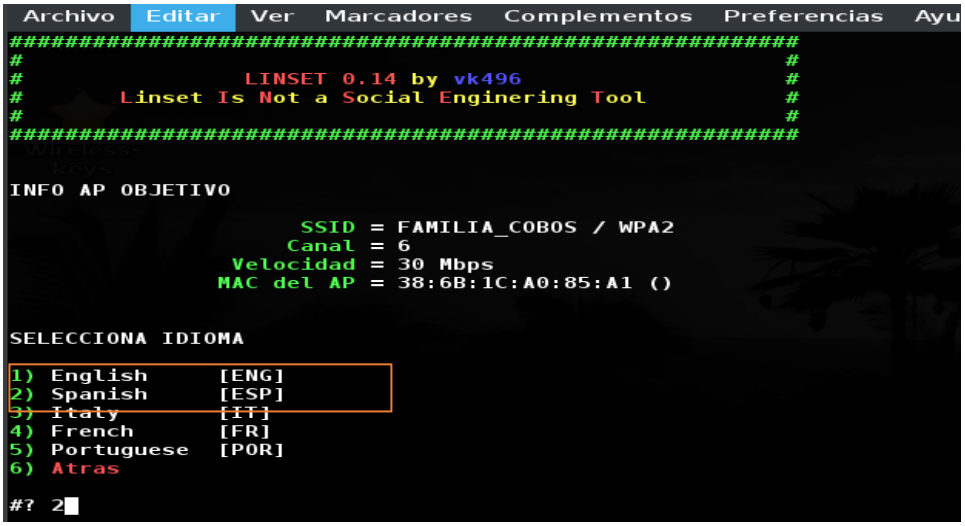


Fig. 47. Selección del idioma

A continuación, Demuestra una interfaz de usuario de usuario donde podemos seleccionar el idioma que se presenta como un menú para seleccionar , sin dejar a un lado que proporciona información detallada sobre el punto AP del objetivo:

- SSID: FAMILIA_COBOS / WPA2
- Canal: 6
- Velocidad: 30 Mbps
- MAC del AP: 38:6B:1C:A0:85

Los pasos anteriores nos llevan a este tipo de información donde se muestra un cuadro de un servidor de DHCP DNS la desautentificación mediante MDK 3 y una breve visualización del tráfico del punto falso.

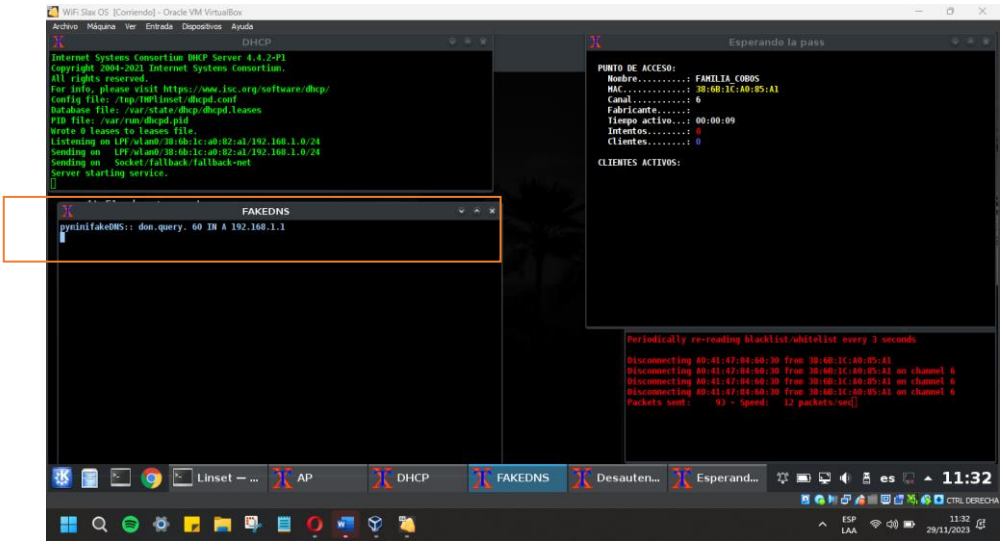


Fig. 48. Creación de la red falsa y el monitoreo

Como podemos observar en dicha ilustración está pasando algunos procesos en este caso tenemos 4 ventanas activas.

Por lo tanto:

DHCP (Dynamic Host Configuration Protocol)

La ventana superior izquierda muestra la configuración y el arranque del servicio DHCP. El servicio DHCP asigna direcciones IP dinámicas a los dispositivos que se conectan a la red.

El servicio está escuchando en la interfaz de red con la dirección MAC 0a:1b:2c:0a:82:a4 y la dirección IP 192.168.1.0/24.

FAKEDNS

La ventana inferior izquierda muestra el servicio FakeDNS, que es probablemente parte del ataque Linset. Este servicio responde a las consultas DNS de los clientes, redirigiéndolas a una dirección IP específica (192.168.1.1), que es la dirección IP del atacante.

El comando en la ventana pymkfakdeDNS: dom.query. indica que está configurando una respuesta DNS falsa.

PUNTO DE ACCESO

La ventana superior derecha muestra los detalles del punto de acceso falso creado por la herramienta. Este punto de acceso tiene el nombre FAMILIA COBOS, y está operando en el canal 6.

La dirección MAC del punto de acceso es 38:8C:1C:A0:85:A1. En esta ventana también se muestra que actualmente no hay clientes activos conectados al punto de acceso.

LOGS DE ACTIVIDAD

La ventana inferior derecha muestra los registros de actividad. Se observan mensajes indicando que se está releyendo la lista de bloqueo/permitidos cada 3 segundos y mensajes de desconexión de varias direcciones MAC desde el punto de acceso falso en el canal 6.

Los paquetes enviados y la velocidad de transmisión también se registran en esta ventana.

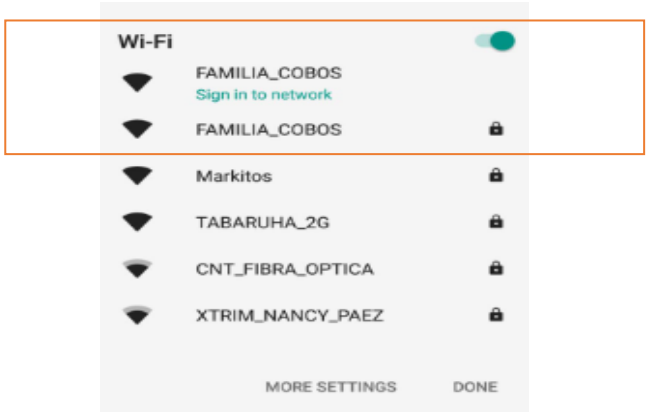


Figura 3:Duplicado de la red

Podemos analizar que se ha creado una red falsa totalmente libre para poder ser punto de acceso directamente como muestra la imagen está libre de contraseña.

En los pasos previos, se ha desarrollado un script de herramientas que genera una interfaz. En esta interfaz, la víctima introducirá la clave necesaria para acceder al sitio web y utilizar la red.

Figura 4:ataque

Este paso está diseñado para inducir a la víctima que ingrese su clave, bajo la falsa premisa de que se ha producido un error en el proceso de autenticación al intentar acceder a su red. Mediante la simulación de un fallo en la autenticación el usuario reintroduzca sus credenciales de acceso, creyendo que se trata de un procedimiento legítimo para resolver el supuesto problema técnico. Este mecanismo de ingeniería social explota la confianza del usuario en los sistemas de seguridad de la red, manipulándolo para que revele información sensible.

Esta versión incluye terminología más específica y detalla el proceso y los mecanismos involucrados en el ataque.

El tráfico será capturado automáticamente por la herramienta Linset, permitiéndonos así monitorear el progreso del ataque.

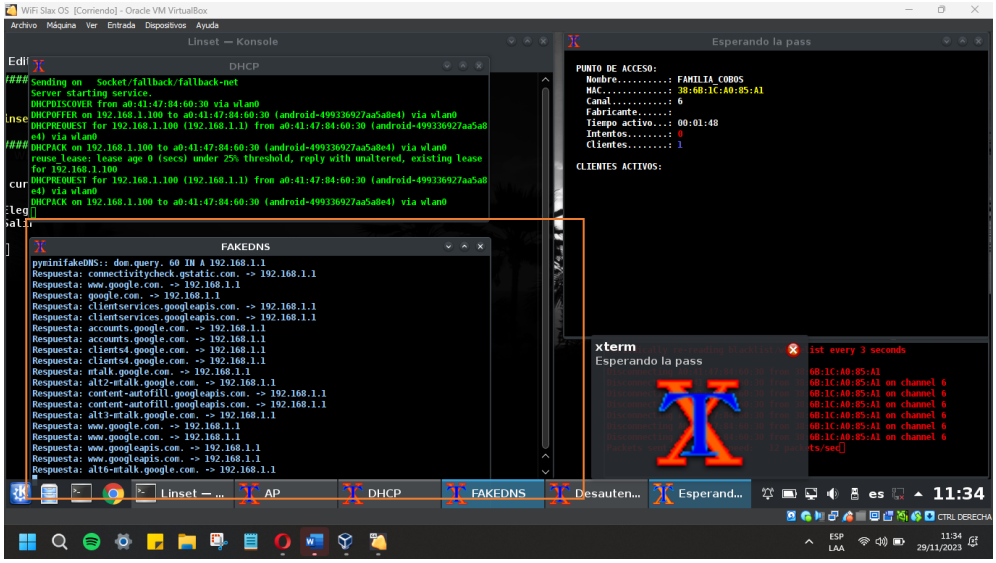


Fig. 49. Ataque Exitoso

La herramienta Linset ha logrado que un cliente se conecte al punto de acceso falso, interceptando su tráfico DNS y esperando que el usuario ingrese sus credenciales de red. El servidor DHCP está funcionando correctamente, asignando direcciones IP a los dispositivos que intentan conectarse.

Una vez ingresada dicha contraseña la herramienta proporcionará un mensaje que la conexión se restablecerá.

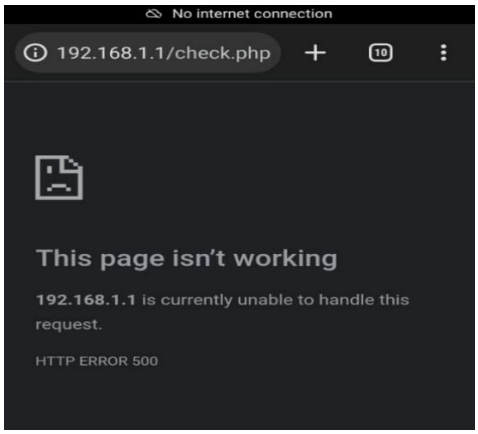


Fig. 50.Mensaje de espera

Automáticamente mostrará la contraseña de la red interfaz como muestra la imagen acabada el ataque las conexiones se restablecen con normalidad sin que los propietarios se percaten del ataque .

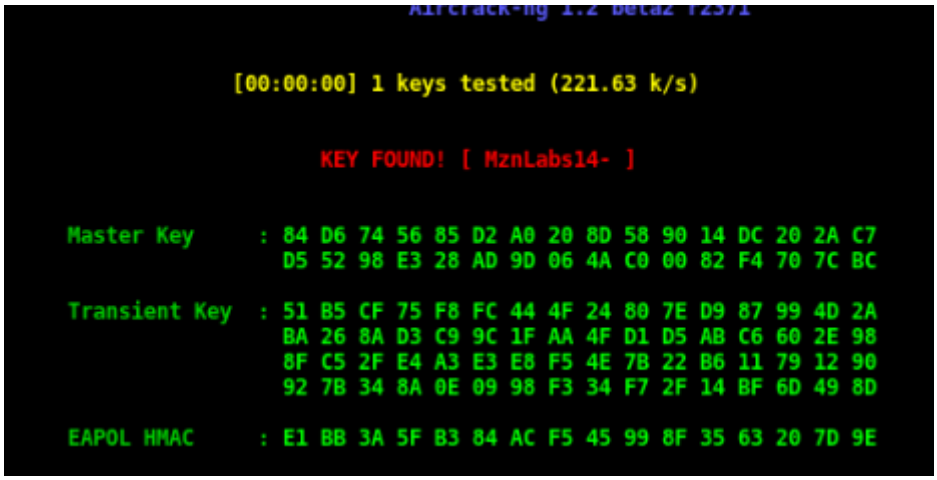


Fig. 51. Captura de la contraseña