UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

HACKING ÉTICO PARA LA DETECCIÓN DE VULNERABILIDADES MEDIANTE LA UTILIZACIÓN DE HERRAMIENTAS OPEN SOURCE EN LA RED INALÁMBRICA DE LA UNIDAD EDUCATIVA PELILEO

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniera en Tecnologías de la Información

ÁREA: Seguridad y Redes.

LÍNEA DE INVESTIGACIÓN: Tecnologías de la información y Sistemas de control.

AUTOR: Shirley de los Angeles Núñez López

TUTOR: Ing. Leonardo David Torres Valverde, Mg

Ambato - Ecuador

febrero – 2024

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: HACKING ÉTICO PARA LA DETECCIÓN DE VULNERABILIDADES MEDIANTE LA UTILIZACIÓN DE HERRAMIENTAS OPEN SOURCE EN LA RED INALÁMBRICA DE LA UNIDAD EDUCATIVA PELILEO, desarrollado bajo la modalidad Proyecto de Investigación por la señorita Shirley de los Angeles Núñez López estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, febrero 2024.

Firmado electrónicamente por:
LEONARDO DAVID
TORRES VALVERDE

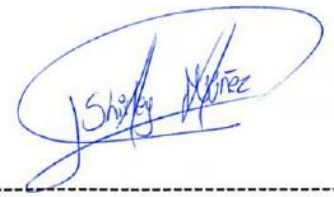
Ing. Leonardo David Torres Valverde, Mg

TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: HACKING ÉTICO PARA LA DETECCIÓN DE VULNERABILIDADES MEDIANTE LA UTILIZACIÓN DE HERRAMIENTAS OPEN SOURCE EN LA RED INALÁMBRICA DE LA UNIDAD EDUCATIVA PELILEO es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, febrero 2024.



Shirley de los Angeles Núñez López

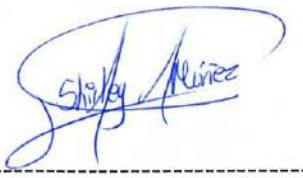
C.C. 1850461318

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, febrero 2024.



Shirley de los Angeles Núñez López

C.C. 1850461318

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por la señorita Shirley de los Angeles Núñez López estudiante de la Carrera de Tecnologías de la Información , de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado HACKING ÉTICO PARA LA DETECCIÓN DE VULNERABILIDADES MEDIANTE LA UTILIZACIÓN DE HERRAMIENTAS OPEN SOURCE EN LA RED INALÁMBRICA DE LA UNIDAD EDUCATIVA PELILEO, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, febrero 2024.

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

Ing. Elsa Pilar Urrutia Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
HERNAN FABRICIO NARANJO AVALOS

Ing. Hernán Fabricio Naranjo Ávalos, Mg
PROFESOR CALIFICADOR

Firmado electrónicamente por:
PAULO CESAR TORRES ABRIL

Ing. Paulo César Torres Abril, Mg
PROFESOR CALIFICADOR

DEDICATORIA

El presente proyecto de Investigación lo dedico primero a Dios, quién ha guiado cada paso que doy en mi vida.

A mis padres, Bolívar y Elva quienes son mis pilares fundamentales al brindarme su apoyo incondicional en todo el transcurso de mi vida, cuyo amor y sacrificio han sido mi mayor inspiración y fortaleza para cumplir está meta.

A mi hermana Gabriela y a mi sobrina Scarlett por estar conmigo brindándome su apoyo en todo momento.

AGRADECIMIENTO

Agradezco a Dios por darme salud y sabiduría para poder lograr mis metas y por tener a toda mi familia unida.

A mis padres, hermana y sobrina por nunca dejarme sola y apoyarme siempre.

A Jonathan mi novio por brindarme su amor y apoyo en cada momento de mi vida.

A mi amiga Jessica, quien me ha acompañado y apoyado a lo largo de la carrera. A David y Kevin por brindarme su amistad e impartirme sus conocimientos.

A los Ingenieros Andrea Sánchez y Leonardo Torres por su orientación y su disposición para compartir sus ideas y experiencia.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN EJECUTIVO

En la era digital actual, el uso de tecnologías inalámbricas ha transformado la forma en que nos conectamos. Diariamente, miles de personas acceden a la red a través de dispositivos como teléfonos inteligentes y computadoras portátiles. Sin embargo, al existir este aumento en la conectividad, los ciberdelincuentes buscan aprovechar las vulnerabilidades para acceder a datos confidenciales, comprometer la privacidad y, en casos extremos, llevar a cabo ataques más amplios, tanto a nivel comercial como doméstico.

Este proyecto de investigación tiene como objetivo encontrar vulnerabilidades mediante pruebas de penetración a la red Wi-Fi de la Unidad Educativa Pelileo para el análisis de amenazas, evaluando la fiabilidad, la integridad y la accesibilidad de la información y red.

Durante el desarrollo, en la fase de evaluación siguiendo la metodología ISSAF se realiza pruebas de intrusión controladas tales como el ataque de fuerza bruta, ataque Evil Twin, denegación de servicios y Man-in-the-Middle. Se aplican controles específicos de seguridad de OWISAM y se selecciona herramientas Open Source como Aircrack-ng y Ettercap, esenciales para la ejecución de estas pruebas. Los resultados obtenidos de estas evaluaciones proporcionan el estado de seguridad de la red.

En resumen, este trabajo destaca por su enfoque práctico, aplicando ataques de intrusión determinando debilidades que afecten la red Wi-Fi en un contexto educativo. La propuesta contribuye al campo de la ciberseguridad al proporcionar una metodología específica para analizar y reforzar redes inalámbricas en entornos similares.

Palabras clave: Hacking, ciberseguridad, vulnerabilidades, ataques.

ABSTRACT

In today's digital age, the use of wireless technologies has transformed the way we connect. Every day, thousands of people access the network through devices such as smartphones and laptops. However, with this increase in connectivity, cybercriminals are looking to exploit vulnerabilities to access sensitive data, compromise privacy and, in extreme cases, carry out broader attacks, both commercially and domestically.

This research project aims to find vulnerabilities by penetration testing the Wi Fi network of the Pelileo Educational Unit for threat analysis, assessing the reliability, integrity and accessibility of the information and network.

During the development, in the evaluation phase following the ISSAF methodology, controlled intrusion tests such as brute force attack, Evil Twin attack, denial of service and Man-in-the-Middle are performed. Specific OWISAM security controls are applied and Open Source tools such as Aircrack-ng and Ettercap, essential for the execution of these tests, are selected. The results obtained from these evaluations provide the network security status.

In summary, this work stands out for its practical approach, applying intrusion attacks by determining weaknesses affecting the Wi-Fi network in an educational context. The proposal contributes to the field of cybersecurity by providing a specific methodology to analyze and strengthen wireless networks in similar environments.

Keywords: Hacking, cybersecurity, vulnerabilities, attacks.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

HACKING ÉTICO PARA LA DETECCIÓN DE VULNERABILIDADES MEDIANTE LA UTILIZACIÓN DE HERRAMIENTAS OPEN SOURCE EN LA RED INALÁMBRICA DE LA UNIDAD EDUCATIVA PELILEO.

1.1.1 Planteamiento del problema

El crecimiento de las Tecnologías de la Información y Comunicación (TIC) no ha detenido su avance; por el contrario, ha experimentado transformaciones significativas en el último decenio. [1]. Las Redes Inalámbricas han adquirido un papel importante en la infraestructura de las TIC a nivel mundial. La capacidad de conectarse a internet de manera Inalámbrica ha permitido una mayor accesibilidad y portabilidad de los dispositivos tecnológicos.

La ciberdelincuencia ha surgido porque la tecnología ha pasado a ser un componente esencial en la ejecución de actividades delictivas. Los primeros ataques se identificaron desde los primeros días de Internet y han continuado ocurriendo desde entonces. En los últimos años, la digitalización empresarial como educativa ha aumentado rápidamente, lo que ha llevado a la actividad delictiva a trasladarse al ciberespacio, lo que ha aumentado la variedad de delitos cibernéticos.[1]. La mayoría de vulnerabilidades encontradas en las Redes Inalámbricas(Wi-Fi) no están vinculados a fallos en los dispositivos tecnológicos, sino a la incorrecta utilización. y configuración [2].

La mayoría de las empresas en Ecuador, son consideradas vulnerables a ciberataques porque no son conscientes del impacto de la inseguridad que pueden tener en sus negocios, porque no toman las medidas necesarias para proteger eficazmente sus datos para evitar grandes pérdidas de información, porque los ciberataques pueden causar daños irreversibles [3].

La Unidad Educativa Pelileo, al igual que muchas otras Instituciones Educativas, ha implementado una Red Inalámbrica para brindar acceso a Internet y recursos digitales a docentes, personal administrativo y directivos. Sin embargo, al no contar con la seguridad en la red, se pueden presentar algunos problemas que afectaría negativamente la operación de la Institución, la posible fuga de datos sensibles y la interrupción del servicio académico digital, identificando la importancia de la información y la necesidad de fortalecer un entorno digital seguro, que garantice que la información y la red sean confiables, mantengan su integridad y estén siempre disponibles.

1.2 Antecedentes investigativos

Después de haber realizado el análisis de fuentes de investigación dentro de los repositorios de algunas Universidades se han encontrado varios temas que servirán de apoyo para el trabajo propuesto.

Según B. Macías Pico [4], en su trabajo de investigación Hacking Ético, expresa que:

- Al analizar la red y sus aplicaciones en colaboración con los administradores, se utilizaron herramientas que ayuden a obtener parámetros relevantes y diseñar políticas de calidad de servicio.

- Mediante un entorno de prueba similar a uno real, se configuraron las políticas utilizando los recursos necesarios. El objetivo fue determinar amenazas y establecer precauciones óptimas para garantizar la seguridad de la red en la Universidad Estatal del Sur de Manabí.

Según L. Jaime Carrasco [5] concluye que:

- La implementación de soluciones informáticas permitió satisfacer las necesidades como la seguridad de la información y protección de datos sensibles del personal de administración, profesores y alumnos pertenecientes a la Escuela de Ingeniería en Sistemas de Uladech.

- Se mejoró la transferencia de información al bloquear usuarios los cuales utilizaban proxy para acceder a redes sociales y afectaban la red inalámbrica.

Esto mejoró la seguridad de la red y garantizó la integridad de la información académica, evitando pérdidas y problemas de rendimiento.

Según D. Castillo Tumbaco [6] en su trabajo de titulación, manifiesta que:

- La combinación de métodos y técnicas de hacking ético se considera una estrategia efectiva para llevar a cabo pruebas de intrusión.
- Las distribuciones informáticas ofrecen una variedad de herramientas diseñadas específicamente para evaluar y comprender la situación actual de la red, lo que permite proponer mecanismos de seguridad que ayuden a prevenir posibles ataques.

Según A. García Vega y D. Morales Baren [7] plantean que:

- La implementación de análisis de redes y el uso de herramientas para escaneos, junto con la virtualización de software libre, arrojaron resultados esperados en pruebas.
- La seguridad informática mediante pentesting permitió implementar mecanismos adecuados, como la configuración básica de Sistemas de Detección de Intrusiones (IDS), protegiendo esta red interna.

Según J. Benítez Guamán [8] comenta:

- La implementación de pentesting determinó vulnerabilidades que se pueden encontrar en las redes wifi dentro de la institución. Con la finalidad de brindar una mejor seguridad a los dispositivos tecnológicos.
- La documentación obtenida permitió que los administradores puedan ejecutar las medidas correspondientes con el afán de mitigar y reducir riesgos presentes.

1.3 Fundamentación teórica

1.3.1 Hacking Ético

También conocido como hacking de sombrero blanco, implica el uso de la experiencia de un experto en ciberseguridad para detectar vulnerabilidades. Los profesionales en este ámbito realizan "pruebas de penetración" para evaluar las barreras de seguridad en organizaciones, verificar la eficacia de los sistemas de seguridad y descubrir fallas y debilidades en la infraestructura de red. Este método se implementa de manera ética y controlada con el objetivo de proteger los sistemas antes de que puedan ser explotados por individuos malintencionados [9].

1.3.2 Herramientas básicas para ciberseguridad

Es responsabilidad del profesional de seguridad informática llevar a cabo el proceso de hackeo ético. Esto le permite prever posibles incidentes antes de que ocurran y mejorar o reparar el sistema para evitar que ocurran. Las herramientas básicas y viables se detallarán a continuación, adaptadas a las particularidades de las redes nacionales.[10].

a. Mapeador de red (NMAP)

Herramienta destinada a escanear redes. Utiliza paquetes IP sin procesar para encontrar servicios en ejecución en dispositivos remotos, así como equipos activos, sistemas operativos, filtros o firewalls, entre otras cosas. Aunque originalmente se desarrolló para el escaneo rápido de redes extensas, también se puede usar para sistemas individuales.[10].

b. Open Vulnerability Assessment Scanner (OpenVAS)

Este software puede funcionar dentro de una red como fuera de un servidor, representando a un ataque real. Al finalizar la ejecución, produce un informe detallado que detalla todas las vulnerabilidades potenciales que podrían poner en peligro la seguridad. Además, tiene la opción de configurarse en modo de monitorización

continua, lo que permite establecer alertas que se activarán cuando se detecte cualquier falla del sistema, incluso la más mínima.[10].

c. Bettercap

Esta herramienta, desarrollada en Go, es una solución integral que brinda a los investigadores de seguridad y equipos de red una interfaz única y fácil de ampliar. Su objetivo es facilitar todas las tareas necesarias para realizar reconocimientos y ataques en redes WiFi, dispositivos Bluetooth Low Energy, dispositivos HID inalámbricos y redes IPv4/IPv6. Lo convierte en una opción versátil y amigable para realizar una variedad de operaciones de seguridad informática debido a su diseño portátil y extensible. [10].

d. Metasploit

Posee una base de datos que alberga exploits, payloads y módulos, posibilitando la realización de una amplia variedad de pruebas de intrusión. Con su estructura modular y una interfaz de usuario intuitiva, agiliza el proceso de reconocimiento y aprovechamiento de vulnerabilidades en sistemas informáticos. Metasploit no solo ofrece un extenso conjunto de herramientas preexistentes, sino que también brinda un entorno de desarrollo que permite la creación de exploits personalizados y adaptados a necesidades específicas [10].

e. Aircrack-ng

Esta herramienta es una de las mejores opciones para evaluar la seguridad de cualquier red Wi-Fi en busca de vulnerabilidades potenciales que podrían permitir a un usuario no autorizado obtener la contraseña de la red. Este software es ampliamente utilizado a nivel mundial para violar la seguridad de las redes Wi-Fi, ya sea con cifrados WEP (Wired Equivalent Privacy), WPA (Wireless Protected Access) e incluso WPA2 (Wireless Protected Access v2). Sin embargo, es común que se utilice en conjunto con otros programas para mejorar el proceso de descifrado de múltiples contraseñas.[11].

f. Wireshark

Es programa analiza paquetes de red y registra una variedad de tipos de datos que pasan a través de una conexión. Herramienta versátil gratuita utilizada para diagnosticar problemas de red, realizar auditorías de seguridad. Permite examinar datos de un archivo de captura o de una red en tiempo real. Facilita el análisis de la información recopilada mediante el uso de detalles y resúmenes de cada paquete. Además, incluye un lenguaje completo para filtrar la información deseada y mostrar el flujo de sesión de TCP reconstruido [12].

g. Airgeddon

Utiliza cualquier tipo de cifrado para simplificar la auditoría de redes inalámbricas mediante un script en bash. Incluye la captura de handshake en redes WPA y WPA2, lo que permite obtener un proceso de descifrado fuera de línea e intentar recuperar la contraseña PSK de la red inalámbrica. El uso de un diccionario de claves o el uso de fuerza bruta son dos métodos posibles para llevar a cabo este ataque. Además, tiene una herramienta que facilita la selección del punto de acceso objetivo, lo que facilita la automatización del proceso.[13].

h. Wifite

Desarrollada para auditar la seguridad de las redes, generalmente en sistemas operativos Linux y Unix. Su objetivo principal es automatizar los procedimientos de evaluación de la seguridad de las redes inalámbricas. WiFite busca redes WiFi disponibles, intenta establecer conexiones utilizando diferentes técnicas de ataque y luego intenta descifrar las contraseñas de las redes que encuentra. Gracias a su facilidad de uso y capacidad de automatización, esta herramienta es popular entre los profesionales de seguridad informática y los pentesters.[14].

i. Fern Wifi Cracker

Herramienta para auditar la seguridad y ejecutar ataques, utiliza la biblioteca Qt-Gui y se basa en Python. El software puede realizar ataques basados en redes inalámbricas o Ethernet, así como recuperar y descifrar claves WEP/WPA/WPS.[15].

j. Ettercap

Es un interceptor/rastreador/registrador para conmutación de LAN. Se utiliza en LAN conmutadas, aunque se utiliza para auditoría en diferentes tipos de redes. Es una herramienta de olificación de red basada en la falsificación de la dirección ARP. Se utiliza principalmente para modificar configuraciones en redes locales. En este software con los medios para balanceo en ETTERCAP, los probadores de penetración pueden detectar la seguridad de la expresión de la comunicación de datos en la red, tome medidas oportunas, evitando datos, como el nombre de usuario / contraseñas sensibles de manera clara. [16].

k. Wifiphisher

Realiza ataques automatizados de suplantación de identidad dirigidos a redes WiFi para obtener contraseñas secretas u otras credenciales. Al no emplear fuerza bruta, este tipo de ataque de ingeniería social se distingue de otros métodos. Ayuda a obtener páginas de acceso a terceros, información de acceso para portales cautivo y contraseña secretas de seguridad WPA/WPA2.[17].

l. Acrylic WiFi Analyzer

Es una aplicación diseñada para supervisar las redes inalámbricas en las proximidades y evaluar su seguridad. Es capaz de escanear y analizar todos los puntos de acceso Wi-Fi disponibles, además, asiste en la optimización del canal de transmisión en el enrutador. Este proceso contribuye a mejorar tanto la cobertura como la velocidad de la conexión Wi-Fi. [18].

1.3.3 Seguridad en la Red

Se refiere a todas las acciones que se toman para proteger el acceso, el uso y la integridad de la red y los datos comerciales. Este enfoque hace uso de tecnologías de hardware y software con el propósito de prevenir la entrada o propagación de diversas amenazas en la red. [19]. En pocas palabras, se trata de un conjunto de acciones y procedimientos destinados a proteger los datos, las aplicaciones, los dispositivos y los sistemas conectados a la red. [20].

1.3.4 Seguridad Informática

También conocida como ciberseguridad, se enfoca en proteger la información y, particularmente, los procesos relacionados con el manejo de datos para evitar cambios por parte de personas no autorizadas. Su objetivo principal es garantizar que los usuarios, los equipos tecnológicos y los datos estén protegidos de daños y amenazas de terceros. [21].

La seguridad informática se fundamenta en cuatro pilares esenciales:

- **Disponibilidad:** Se debe admitir el acceso a la información en los sistemas, según las necesidades del usuario, manteniendo la privacidad.
- **Confidencialidad**: Solo las personas autorizadas deben tener acceso a la información.
- **Integridad**: Se debe asegurar la integridad de la información, sin errores ni modificaciones por parte de los sistemas.
- **Autenticación**: Verificar la información proveniente de un usuario para asegurar su identidad. [22].

1.3.5 Redes

En informática, se entiende por red (usualmente red informática o red de computadoras) a la interconexión de un número determinado de computadores (o de redes, a su vez) mediante dispositivos alámbricos o inalámbricos que, mediante impulsos eléctricos, ondas electromagnéticas u otros medios físicos, les permiten enviar y recibir información en paquetes de datos, compartir sus recursos y actuar como un conjunto organizado [23].

1.3.6 Red Inalámbrica

Un tipo de enlace entre sistemas informáticos, es decir, entre computadoras, que se establece mediante ondas del espectro electromagnético se conoce como red

inalámbrica. Se trata de una conexión de nodos que no requiere dispositivos alámbricos o cables. [24]. Aunque Wi-Fi Alliance posee una marca registrada específica, el término Wi-Fi se utiliza de manera genérica para referirse al acceso inalámbrico. Este grupo es responsable de verificar que los productos cumplen con los estándares inalámbricos 802.11 establecidos por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).[25]

1.3.7 Norma 802.11.

Incrementa el rendimiento y el alcance de las conexiones Wi-Fi, también amplia la disponibilidad en nuevas frecuencias. [25].

Las características que definen a 802.11Wi-Fi, según la IEEE son:

- El uso del medio (aire) no tiene un rango máximo de funcionamiento, sin embargo, se conoce que las STA fuera de su cobertura no pueden recibir tramas.
- Cada comunicación establecida está expuesta a otras comunicaciones que se produzcan en el medio.
- El medio empleado en IEEE 802.11 (aire) no es tan fiable como el medio de las redes cableadas.
- Tiene topologías cambiantes, debido a la movilidad que tienen los dispositivos.
- Las STAs no pasan conectadas todo el tiempo, por lo que se entiende que algunas STAs pueden estar ocultas.
- Las propiedades de propagación son variables y asimétricas.

1.3.8 Protocolo TCP/IP

El protocolo de control de transmisión o sus siglas en inglés TCP, es la forma predeterminada de transmitir datos entre varios dispositivos en una red. Durante todo el proceso de transferencia, este protocolo mantiene una conexión constante entre el

remitente y el destinatario. A través de sus mecanismos, TCP garantiza que todos los paquetes de datos lleguen correctamente, lo que permite una transmisión confiable y fluida entre varios dispositivos. El protocolo de transferencia de archivos (FTP) y Secure Shell (SSH) son ejemplos de protocolos de transferencia de archivos utilizados por TCP en servicios como el correo electrónico.[26].

1.3.9 Vulnerabilidades en redes inalámbricas

Se refiere a una amenaza en un sistema que posibilita que un atacante pueda comprometer la privacidad, integridad, control de acceso y consistencia del sistema o de sus datos y aplicaciones. Las redes inalámbricas presentan un riesgo mayor en comparación con las redes cableadas, ya que la señal se propaga en todas direcciones. [27].

1.4 Objetivos

1.4.1 Objetivo general

Aplicar Hacking Ético para la detección de vulnerabilidades mediante la utilización de herramientas Open Source en la Red Inalámbrica de la Unidad Educativa Pelileo.

1.4.2 Objetivos específicos

- Investigar las principales vulnerabilidades que se pueden presentar en las Redes Inalámbricas.
- Determinar la mejor herramienta Open Source para ejecutar pruebas de Hacking Ético en Redes Inalámbricas.
- Realizar pruebas de penetración controladas en la Red Inalámbrica de la Unidad Educativa Pelileo para identificar vulnerabilidades.
- Documentar los resultados obtenidos del análisis de vulnerabilidades en la Red Inalámbrica de la Unidad Educativa Pelileo.

CAPÍTULO II. METODOLOGÍA

2.1 Materiales

Para llevar a cabo esta investigación, los métodos de recopilación de datos empleados fueron una encuesta dirigida a docentes, administrativos y directivos, así como una entrevista al docente encargado de TI de la Unidad Educativa Pelileo. Estos recursos permitieron obtener una comprensión integral de la situación y las perspectivas en relación con el tema de tesis.

La encuesta incluye preguntas dicotómicas, escala de Likert, y selección múltiple, por lo que se consideró más factible tomar las preguntas de selección múltiple con el coeficiente de Alpa de Cronbach, el resultado que se obtuvo fue del 0.91 (Tabla 1) y las preguntas dicotómicas con el coeficiente de Kuder Richardson "KR-20" donde se obtuvo el 0.95 (Tabla 3) de confiabilidad.

Tabla 1**:** Coeficiente de alfa de Cronbach en la encuesta aplicado a los docentes.

Simbología	**Valor**
α (alfa)=	0,91
K(Número de ítems)=	4
∑Vi(Varianza cada ítem)=	0,94
Vt (Varianza total ítems) =	1,57

Tabla 2: Interpretación de la escala de consistencia del Alfa de Cronbash[28].

Alfa de Cronbash	**Interpretación**
0,9	Excelente
0,9-0,8	Buena
0,8-0,7	Aceptable
0,7-0,6	Débil
0,6-0,5	Pobre
0,5	Inaceptable

Tabla 3: Coeficiente de Kuder Richardson "KR-20" en la encuesta aplicada a los docentes.

Simbología	**Valor**
Kr-20=	0,95
K(Número de ítems)=	2
Σ(p*q)=	0,20
σ2(Varianza total del instrumento)=	0,13

Tabla 4: Interpretación de la escala de consistencia de Kuder Richardson [29].

Kuder Richardson	**Interpretación**
0,81 a 1	Muy Alta
0,61 a 0,80	Alta
0,41 a 0,60	Moderada
0,21 a 0,40	Baja
0,01 a 0, 20	Muy Baja

ENCUESTA A DOCENTES, ADMINISTRATIVOS Y DIRECTIVOS DE LA UNIDAD EDUCATIVA PELILEO

Objetivo: Recopilar información sobre el conocimiento de la seguridad de redes inalámbricas en la institución.

Seleccione la respuesta que crea conveniente

1. **¿Con qué frecuencia utiliza dispositivos como laptops o teléfonos móviles en su trabajo en la institución?**

   ◯ Diariamente

   ◯ Ocasionalmente

   ◯ Nunca

2. ¿Cuánto sabe sobre posibles debilidades o problemas de seguridad en la red inalámbrica de su institución?

- ◯ Muy informado
- ◯ Informado
- ◯ Poco
- ◯ No Informado

3. ¿Ha experimentado problemas de seguridad en la red inalámbrica de la institución en los últimos 12 meses?

- ◯ No he experimentado problemas de seguridad
- ◯ Pérdida de datos o información confidencial
- ◯ Acceso no autorizado a la red
- ◯ Interrupciones en el servicio

4. En su opinión, ¿Cuál considera que es la amenaza de seguridad más importante en las redes inalámbricas de las instituciones?

- ◯ Acceso no autorizado por parte de personas externas
- ◯ Pérdida de datos o información confidencial
- ◯ Malware o virus que afecten la red
- ◯ Falta de actualizaciones de seguridad regulares

5. ¿Considera usted que la seguridad en las redes inalámbricas es importante en un entorno educativo?

- ◯ Muy Importante

◯ Importante

◯ No es una prioridad

6. ¿Cuál de las siguientes medidas de seguridad inalámbrica se implementan en su institución?

◯ Contraseñas seguras y cambiosregulares de contraseñas

◯ Encriptación de datos en la redinalámbrica

◯ Monitoreo continuo de la red paradetectar amenazas

◯ Políticas de acceso restringidobasadas en roles

7. ¿La falta de medidas de seguridad en las redes inalámbricas podría afectar su trabajo en la institución?

◯ Sí

◯ No

8. ¿Conoce las medidas de seguridad que debe aplicar para proteger su computadora o dispositivo al conectarse a la red de la institución?

◯ Sí

◯ No

9. ¿Qué tan satisfecho está con la seguridad de la red inalámbrica de la institución?

◯ Insatisfecho

◯ Neutral

◯ Satisfecho

10. ¿Para garantizar la seguridad de las redes inalámbricas utilizadas en su trabajo que le gustaría que haga la institución?

- ◯ Deseo que se tomen medidas adicionales para mejorar la seguridad
- ◯ Considero que la seguridad actual es suficiente y no requiere cambios
- ◯ No tengo una opinión definitiva alrespecto en este momento
- ◯ Prefiero no comentar al respecto.

La entrevista se realizó al docente encargado de los laboratorios de la Unidad Educativa y consta de 9 preguntas.

Guía de entrevista		
Nombre del entrevistado: Empresa: Cargo: Entrevistador:		
Objetivo: Recopilar información sobre el conocimiento de la seguridad de redes inalámbricas en la institución.		
Pregunta	Respuesta	Observación
¿Conoce el estado actual de la red inalámbrica y su funcionamiento?		
¿Existe algún departamento dedicado a la administración de redes, en el caso de no		

haber considera importante empezar a administrarla?		
¿Qué entiende por seguridad cibernética o seguridad en línea? ¿Existen políticas de conexión y de seguridad en la red inalámbrica?		
¿Ha experimentado su institución incidente de seguridad cibernética en el pasado? En caso afirmativo, ¿cómo los ha abordado y qué lecciones ha aprendido de ellos?		
¿Cómo cree que la seguridad en línea podría afectar al personal de la institución?		
¿Ha oído hablar de amenazas en línea como virus informáticos o hackers? ¿Qué sabe al respecto?		
¿Cree que es importante proteger la información en línea de la institución? ¿Por qué?		
Conclusión:		

2.2 Métodos

2.2.1 Modalidad de la investigación

a. Investigación de Campo

El presente trabajo investigativo es de campo, ya que la investigadora recopila datos mediante encuestas utilizando un cuestionario dirigido a los docentes de la Unidad Educativa Pelileo. El propósito es obtener información confiable que contribuyera a abordar el problema relacionado con amenazas que se generan en las redes inalámbricas en un contexto educativo, salvaguardando la comunicación.

b. Investigación Bibliográfica-documental

La investigación es bibliográfica-documental pues se fundamenta en la recopilación de datos a través de libros, artículos, revistas, tesis realizadas enfocadas al tema investigativo, los cuales se utilizaron para la construcción de la fundamentación teórica que estudia temas como Hacking Ético, herramientas Open Source para Hacking, Seguridad Informática, Redes Inalámbricas, entre otros.

2.2.2 Población y muestra

Para el presente proyecto se trabajó con administrativos, directivos y docentes de la Unidad Educativa Pelileo.

Tabla **5:** Población

Población	**Número**	**Porcentaje**
Directivos	3	12%
Administrativos	2	8%
Docentes	20	80%
Total	**25**	**100%**

Debido a que el número de población es menor a 100 no se procedió a sacar una muestra.

2.2.3 Recolección de información

La recopilación de los datos se efectuó mediante encuestas a docentes, administrativos y directivos, para el análisis e interpretación de resultados se los englobará y mencionará solo como docentes, al docente encargado de la administración TI en la Unidad Educativa se aplicó una entrevista y posteriormente para el análisis de los datos recolectados se utilizó el software Excel.

Análisis e interpretación de los resultados de la encuesta a docentes, administrativos y directivos de la Unidad Educativa Pelileo

Pregunta 1: ¿Con qué frecuencia utiliza dispositivos como laptops o teléfonos móviles en su trabajo en la institución?

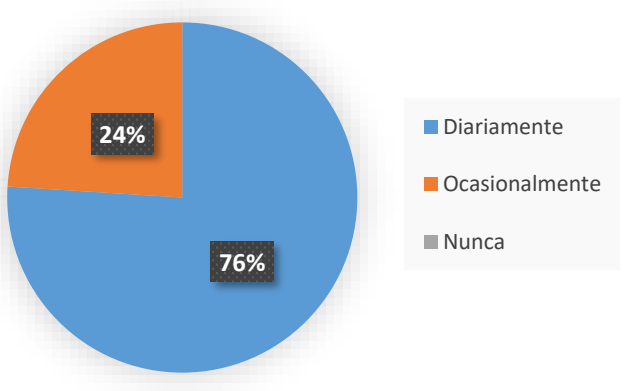


Figura 1**:** Datos de la pregunta 1

Análisis e interpretación de resultados

Conforme a los resultados de la encuesta, en la Figura 1, se puede observar que el 76% de los docentes indicaron utilizar dispositivos como laptops o teléfonos móviles diariamente en su trabajo en la institución. Un 24% mencionó utilizarlos ocasionalmente. En cuanto a la opción "Nunca", esta no fue seleccionada por ningún docente. Estos resultados sugieren que la mayoría de los docentes hacen un uso frecuente de dispositivos móviles en sus actividades laborales en la institución educativa.

Pregunta 2: ¿Cuánto sabe sobre posibles debilidades o problemas de seguridad en la red inalámbrica de su institución?

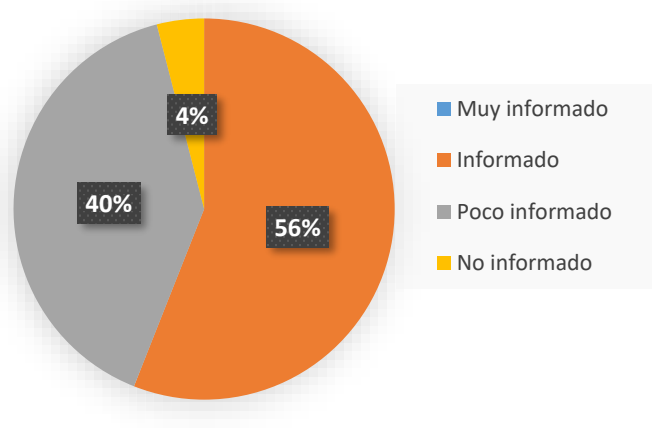


Figura 2: Datos de la pregunta 2

Análisis e interpretación de resultados

De acuerdo con la Figura 2, se evidencia que el 56% de los docentes se considera informado en cuanto a las debilidades o problemas de seguridad que se pueden presentar en la institución. El 40% se identifica con poca información al respecto, y solo un 4% menciona no contar con la información necesaria. Estos resultados reflejan una variabilidad en el grado de conocimiento de los docentes resaltando que la mayoría tiene una noción con respecto a las debilidades y problemas de seguridad en la red inalámbrica institucional.

Pregunta 3: ¿Ha experimentado problemas de seguridad en la red inalámbrica de la institución en los últimos 12 meses?

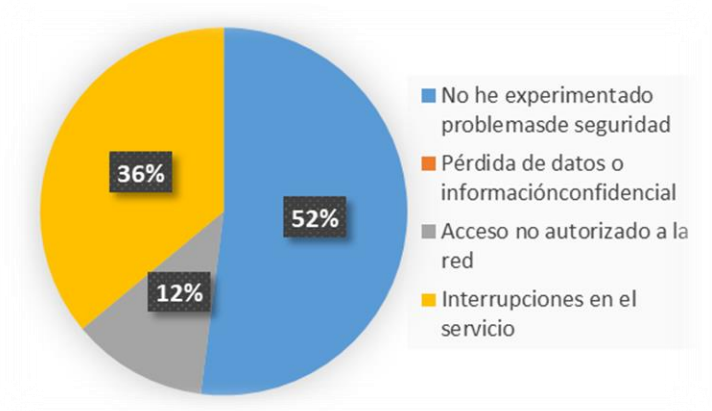


Figura 3: Datos de la pregunta 3

Análisis e interpretación de resultados

En la Figura 3, se puede observar que el 52% de los docentes indicó que no había experimentado problemas de seguridad. Sin embargo, el 36% reportó interrupciones en el servicio, lo que podría reflejar problemas técnicos o incidentes de seguridad. Además, un 12% mencionó haber experimentado acceso no autorizado a la red, lo que indica la presencia de posibles vulnerabilidades. Estos resultados sugieren que, si bien la mayoría de los docentes no ha experimentado problemas, existe una proporción notable que sí ha tenido experiencias negativas relacionadas con la seguridad y el servicio de la red inalámbrica. Estos datos podrían indicar la necesidad de medidas adicionales para fortalecer la seguridad de la red y garantizar un servicio más ininterrumpido.

Pregunta 4: En su opinión, ¿Cuál considera que es la amenaza de seguridad más importante en las redes inalámbricas de las instituciones?

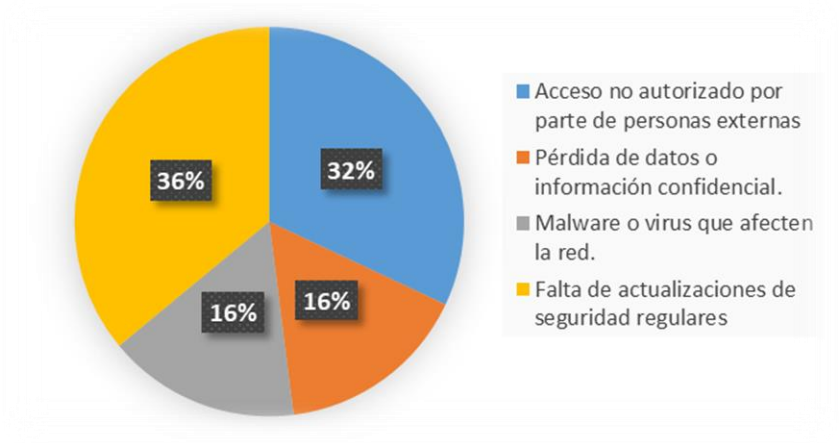


Figura 4: Datos de la pregunta 4

Análisis e interpretación de resultados

Con respecto a la Figura 4, el 36% de los encuestados mencionó la falta de actualizaciones de seguridad regulares como la principal preocupación, lo que sugiere la importancia de mantener las redes al día en términos de confidencialidad. Además, el acceso no autorizado por parte de personas externas fue destacado por un 32%, lo que indica la preocupación por posibles intrusiones en la red. El malware o virus que afecten la red y la pérdida de datos o información confidencial recibieron un 16% de las menciones. Estos resultados señalan que, según la percepción de los docentes, la falta de actualizaciones de seguridad y el acceso no autorizado son las amenazas más relevantes, lo que podría guiar a la institución en la implementación de medidas de seguridad y actualizaciones regulares para abordar estos desafíos.

Pregunta 5: ¿Considera usted que la seguridad en las redes inalámbricas es importante en un entorno educativo?

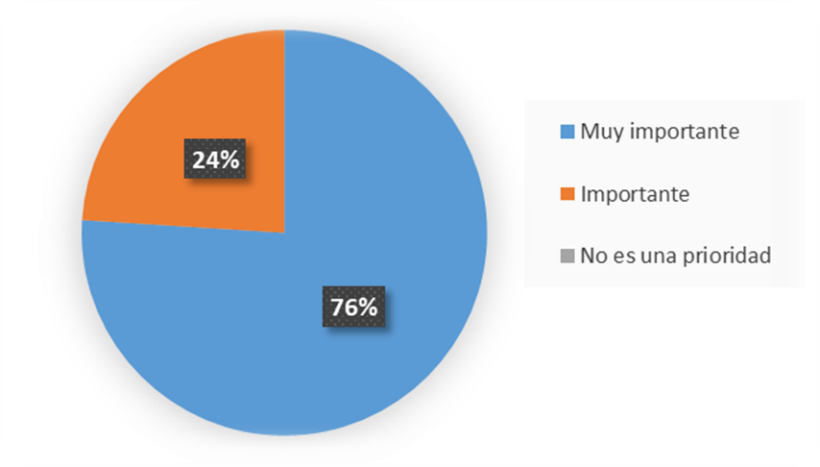


Figura 5: Datos de la pregunta 5

Análisis e interpretación de resultados

La Figura 5 revela que, el 76% de los docentes consideró que la seguridad en estas redes es muy importante. Un 24% adicional también la evaluó como importante. Estos resultados denotan una alta preocupación con respecto a la seguridad en las redes inalámbricas en el contexto educativo, para preservar la integridad de los datos y mantener un ambiente de aprendizaje seguro. Esta percepción reafirma la relevancia de implementar medidas de seguridad efectivas en la institución educativa para respaldar las actividades académicas.

Pregunta 6: ¿Cuál de las siguientes medidas de seguridad inalámbrica se implementan en su institución?

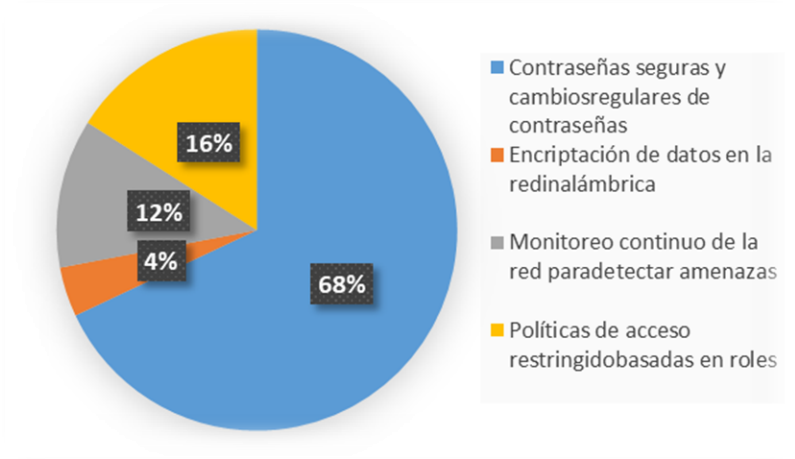


Figura 6: Datos de la pregunta 6

Análisis e interpretación de resultados

En la Figura 6, los resultados reflejan que el 68% de los docentes señalaron la aplicación de contraseñas seguras y cambios regulares de contraseñas como medida de seguridad, mientras que las políticas de acceso restringido basadas en roles fueron consideradas por un 16% de los encuestados. Además, el monitoreo continuo de la red para detectar amenazas fue citado por un 12%. En contraste, solo un 4% mencionó la encriptación de datos en la red inalámbrica, lo que podría indicar un área de mejora en la seguridad de la red. Estos resultados destacan la prevalencia de contraseñas seguras, aunque sugieren la necesidad de fortalecer la encriptación de datos en la red inalámbrica para garantizar una seguridad óptima. Además, la presencia de políticas de acceso restringido y el monitoreo de la red indican un enfoque en la seguridad, aunque con margen para mejoras.

Pregunta 7: ¿La falta de medidas de seguridad en las redes inalámbricas podría afectar su trabajo en la institución?

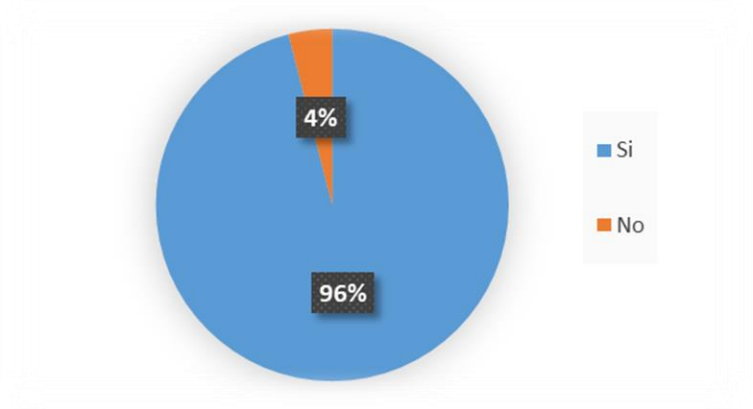


Figura 7: Datos de la pregunta

Análisis e interpretación de resultados

De acuerdo con la Figura 7, el 96% de los docentes expresó que ausencia de protocolos de seguridad en la red inalámbrica podría afectar su trabajo en la institución. El 4% restante no percibe que pueda afectar su trabajo. Este alto porcentaje subraya la clara preocupación de los docentes por la influencia negativa que la falta de seguridad en las redes inalámbricas podría tener en sus actividades laborales en la institución. Esta percepción destaca la importancia de implementar medidas efectivas para garantizar un entorno de trabajo más protegido y eficiente.

Pregunta 8: ¿Conoce las medidas de seguridad que debe aplicar para proteger su computadora o dispositivo al conectarse a la red de la institución?

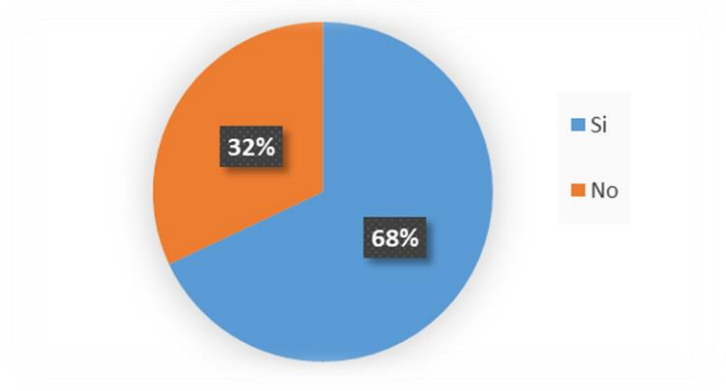


Figura 8: Datos de la pregunta 8

Análisis e interpretación de resultados

Según la Figura 8, el 68% de los docentes afirmó conocer estas medidas de seguridad, lo que indica una comprensión sólida de las prácticas de seguridad. No obstante, un 32% señaló no estar al tanto de las medidas de seguridad requeridas, lo que resalta una brecha en la comprensión de la seguridad en la red. Esto podría sugerir la necesidad de mejorar la concienciación y la educación sobre ciberseguridad entre los docentes para garantizar prácticas seguras y proteger sus dispositivos al conectarse a la red de la institución.

Pregunta 9: ¿Qué tan satisfecho está con la seguridad de la red inalámbrica de la institución?

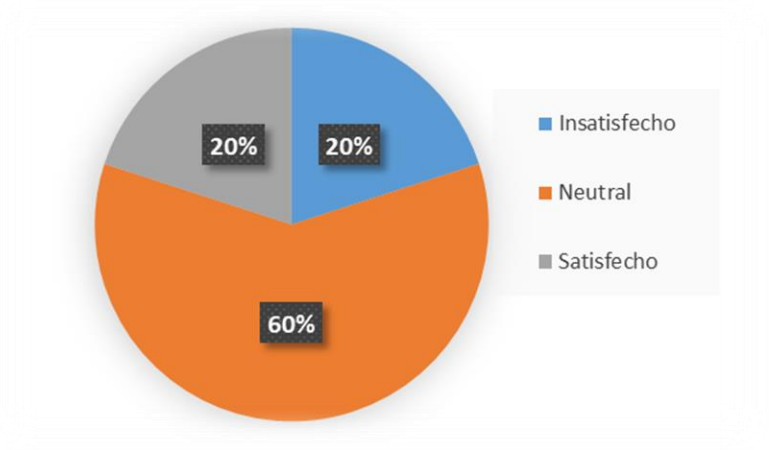


Figura 9: Datos de la pregunta 9

Análisis e interpretación de resultados

De acuerdo con la Figura 9, el 60% se encuentra en una posición neutral en cuanto a su satisfacción con la seguridad de la red WiFi de la institución. Un 20% expresó insatisfacción, mientras que otro 20% indicó estar satisfecho. Estos resultados revelan una percepción ambivalente en relación a la protección de la red inalámbrica, señalando una importancia para abordar las inquietudes sobre seguridad y posiblemente implementar mejoras en el entorno educativo.

Pregunta 10: ¿Que le gustaría que haga la institución para garantizar la seguridad de la red inalámbrica utilizada en su trabajo?

Figura 10: Datos de la pregunta 10

Análisis e interpretación de resultados

Según la Figura 10, el 68% desearía que la institución tome medidas adicionales para mejorar la seguridad de la red inalámbrica utilizada en su trabajo. El 16% se encuentra indeciso en este tema. Además, un 12% prefiere no emitir comentarios al respecto, mientras un reducido 4% considera que la seguridad actual es suficiente y no necesita cambios significativos. Estos resultados subrayan la voluntad de la comunidad docente de salvaguardar la información que se transmite por la red WiFi y resaltan la importancia de tomar medidas proactivas para satisfacer estas expectativas y garantizar un entorno seguro en la institución.

Al docente que se encarga de la administración TI de la Unidad Educativa Pelileo se aplica una entrevista y se obtuvieron las siguientes respuestas de las preguntas que se procedieron a realizar.

Tabla 6: Entrevista docente administración TI de la Institución

Nombre del entrevistado: Ing**.** Marco Chicaiza **Institución:** Unidad Educativa Pelileo **Entrevistador:** Shirley Núñez		
Preguntas	**Respuestas**	**Observación**
1. ¿Conoce el estado actual de la red inalámbrica y su funcionamiento?	La red se encuentra funcional, pero no cuenta con una estructura de seguridad adecuada.	La red funciona como una red local básica siendo vulnerable debido a la falta de medidas de seguridad.
2. ¿Existe algún departamento dedicado a la administración de redes, en el caso de no haber considera importante empezar a administrarla?	Actualmente no existe un departamento dedicado a la administración de redes. Sería muy conveniente e importante contar con uno.	La administración de la red recae en docentes.
3. ¿Existen políticas de conexión y de seguridad en la red inalámbrica?	No existen políticas de conexión ni medidas de seguridad en la red.	La conexión se encuentra en su configuración por defecto.
4. ¿Qué entiende por seguridad cibernética o seguridad en línea?	La seguridad cibernética involucra proteger la información y los sistemas de amenazas en línea.	Reconoce la importancia de proteger la información en línea.
5. ¿Ha experimentado su institución incidentes de seguridad cibernética?	No se ha experimentado incidentes de seguridad cibernética.	Considera que al no experimentar incidentes anteriores, no se puede asumir que la seguridad en línea esté suficientemente establecida

6. ¿Cómo cree que la seguridad en línea podría afectar al personal?	Mejoraría la transferencia y control de datos.	Identifica que la seguridad en línea es fundamental para la confidencialidad de la información.
7. ¿Ha oído hablar de amenazas en línea como virus informáticos o hackers?	Tiene conocimiento sobre virus informáticos y hackers, comprende que representan amenazas en línea.	Comprende la existencia de amenazas en línea. Así como también sus acciones y riesgos.
8. ¿Cree que es importante proteger la información en línea de la institución?	Considera fundamental proteger la información.	Reconoce la importancia de la protección de datos en línea y sus implicaciones.
Conclusión: En la institución, se identifica que la red inalámbrica se encuentra en un estado básico de configuración, sin políticas de seguridad. La falta de un departamento dedicado a la administración de redes y la escasa implementación de medidas de seguridad en la red son áreas de mejora identificadas. Además, reconoce la importancia de proteger la información en línea, especialmente en un entorno educativo, enfocándose en la confidencialidad y la necesidad de contar con un departamento de redes.		

2.2.4 Procesamiento y análisis de datos

- La mayoría de los docentes muestra una preocupación notable por la seguridad en las redes inalámbricas, lo que refleja un nivel de conciencia sobre esta cuestión.
- Algunos docentes destacaron la necesidad de medidas adicionales para reforzar la protección en la red inalámbrica, lo que sugiere mejorar la infraestructura de seguridad.

- En cuanto a la satisfacción general con la seguridad en la conexión inalámbrica, las opiniones son diversas. Mientras que algunos docentes están satisfechos, otros muestran inquietudes o mantienen una postura neutral.

- La red Wifi institucional, aunque es funcional, carece de medidas de seguridad, lo que la hace vulnerable.

- Actualmente, no existe un departamento dedicado a la administración de redes. La red se mantiene por docentes, lo que es una fuente de preocupación en términos de seguridad.

- También se enfatizó la importancia de proteger la información en línea, especialmente la confidencialidad de los datos de los usuarios de la red, para garantizar la continuidad de las operaciones.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1 Análisis y Discusión de los Resultados

3.1.1 Vulnerabilidades comunes en Redes Inalámbricas

Las vulnerabilidades más comunes que afectan a las redes inalámbricas se identifican y describen como puntos débiles que pueden ser explotados por atacantes, lo que incluye problemas relacionados con la autenticación, la configuración y otros aspectos de seguridad. Además, se realiza una clasificación de estas vulnerabilidades en función de su grado de riesgo [30], lo que ayudará en la posterior evaluación y mitigación. El análisis es fundamental para comprender el panorama de amenazas y prepararse adecuadamente para las pruebas de hacking ético en redes inalámbricas.

Tabla 7: Vulnerabilidades comunes en Redes Inalámbricas.

Vulnerabilidad	Definición	Consecuencias	Riesgo
Ataques de Fuerza Bruta	Intentos de adivinar contraseñas probando una amplia variedad de combinaciones, efectivos con contraseñas débiles. [31]	Riesgo de bloqueo de cuentas, posibles intrusiones. [31]	Medio[30]
Ataques de Diccionario	Uso de diccionarios de contraseñas para adivinar contraseñas mediante fuerza bruta.[31]	Posible acceso no autorizado, riesgo de compromiso de cuentas.[31]	Medio[30]
Falsificación de SSID (Evil Twin)	Creación de puntos de acceso falsos que parecen legítimos para engañar a los usuarios y robar datos.[32]	Suplantación de identidad, robo de información confidencial.[32]	Alto[30]

Ataques Man-in-the-Middle (MitM)	Interponerse en la comunicación entre dos partes para interceptar o modificar datos. [33]	Interceptación de datos, posible manipulación de comunicaciones. [33]	Alto[30]
Ataques DoS (Denegación de Servicio)	Forzar la desconexión de dispositivos legítimos de la red. [34]	Interrupción de la conectividad de dispositivos autorizados. [34]	Alto[30]

3.1.2 Tipos de Herramientas para Hacking Ético

Las herramientas de hacking ético son esenciales para la seguridad informática, ya que permiten identificar y corregir vulnerabilidades en sistemas y redes. Estas herramientas simulan ataques reales, proporcionando a las organizaciones una comprensión detallada de sus debilidades y mejorando su postura de seguridad. Además, son fundamentales para el entrenamiento y desarrollo profesional en el campo de la seguridad, contribuyen a la mejora continua de las medidas de seguridad, ayudan a cumplir con regulaciones y normativas, protegen la privacidad y los datos, sirven como herramientas educativas para crear conciencia sobre las amenazas cibernéticas.

Tabla 8: Cuadro comparativo de herramientas para Hacking

Herramientas	Características	Ventajas	Desventajas
Aircrack-ng	-Utilizado para auditorías de seguridad en redes inalámbricas. - Realiza ataques de fuerza bruta y diccionario. [35]	-Efectivo para recuperar contraseñas Wi-Fi. [35]	- Requiere conocimiento técnico. - Ataques pueden ser ilegales sin permiso. [35]

Wireshark	- Analiza el tráfico de red en tiempo real. - Puede descifrar contraseñas Wi-Fi capturadas. [36]	-Muestra detalles precisos del tráfico. - Fácil de usar. [36]	- No se especializa en pruebas de penetración Wi-Fi. - Requiere capturar tráfico previamente. [36]
Bettercap	- Especializada en pruebas de penetración de Wi-Fi. - Captura información sobre SSID. - Realiza ataques MITM[37].	- Ideal para auditorías de redes inalámbricas. - Automatiza tareas[37].	- Requiere comandos. - Debe utilizarse con autorización[37].
Ettercap	- Realiza ataques MITM - Específicamente para atacar redes LAN o WLAN [38].	- Efectivo en redes con WPS habilitado. - Automatiza el proceso [38].	- Utiliza interfaz gráfica. - Puede requerir tiempo para encontrar claves [38].
Fern Wi-Fi Cracker	- Realiza ataques de fuerza bruta y diccionario. - Crea informes detallados.[39]	- Interfaz gráfica fácil de usar. - Genera estadísticas.[39]	- Limitado a contraseñas débiles. - Requiere buen conocimiento de redes.[39]
Wifiphisher	- Utilizado para atacar ingeniería social. - Realiza ataques de Evil Twin[40].	- Especializado en ataques pishing[40].	- No es efectivo en redes donde se ha habilitado el WPS3. - Inmediato en generar la red falsa [40].
Airgeddon	- Realiza múltiples ataques Wi-Fi, incluyendo WPS, WEP y WPA. - Automatiza el proceso de obtención de claves. [41]	- Amplia gama de ataques disponibles. - Interfaz intuitiva.[41]	- Requiere un buen conocimiento de las redes. - Debe utilizarse con autorización. [41]

Wifite2	- Automatiza la auditoría de redes Wi-Fi. - Realiza ataques WEP, WPA y WPS. [42]	- Fácil de usar y automatiza muchos ataques. [42]	- Requiere conocimiento técnico para su configuración. - Debe utilizarse con autorización. [42]
Nmap	Escaneo rápido de dispositivos. Identificación servicios de un sistema [43].	Detecta dispositivos, servidores, enrutadores, servidores web, los servidores DNS [43].	Los firewalls del equipo escaneado, pueden bloquear las comunicaciones[43].
Metasploit	Escaneo de Vulnerabilidades Ataques [44].	Explotación manual Ingeniería social [44].	Módulos posteriores para explotación [44].
Acrylic Wifi Analyzer.	Escanea los APs que transmiten en la zona[45].	Muestra SSID, MAC, RSSI, canales de la red[45].	Para escaneo más completo se necesita versión paga [45].

Después de realizar una comparativa de las herramientas en la Tabla 6, se seleccionó Acrylic WiFi para obtener información relevante de la red. Nmap por su versatilidad en el escaneo. Mientras que las herramientas Wifiphisher, Ettercap y Aircrack-ng ofrecen capacidades específicas para detectar vulnerabilidades en cuanto a los ataques evaluando la seguridad de la red, gracias a la funcionalidad técnica y la presencia de interfaces gráficas de usuario que facilitan su ejecución.

3.1.3 Metodologías de Hacking Ético

La realización de pruebas de seguridad incluye el uso de una metodología específica en hacking ético. Proporciona un marco estructurado que dirige todo el proceso de evaluación, desde la planificación hasta la implementación de pruebas y la presentación de informes. La estructura asegura que se cubran todas las áreas pertinentes del sistema bajo evaluación, lo que maximiza la ejecución de las pruebas. Además, facilita la replicabilidad al permitir que otros profesionales verifiquen y validen los resultados. Al implementar una metodología, se garantiza la coherencia en

la ejecución de pruebas, se pueden identificar de manera más efectiva las vulnerabilidades y se proporciona una base sólida para la determinación de medidas de protección.

Tabla 9: Metodologías de seguridad informática.

Aspectos	OSSTMM	OWISAM	ISSAF
Enfoque Principal	Pruebas de seguridad en general, incluyendo redes, sistemas y aplicaciones. [46]	Pruebas de seguridad enfocadas en aplicaciones web [47].	Enfoque integral para la evaluación de seguridad de sistemas de información [48].
Estructura	Amplia cobertura de temas con enfoque en seguridad en redes. [46]	Metodología con énfasis en la documentación y procesos de aplicación [47].	Incluye fases como recopilación de información, análisis de vulnerabilidades y explotación [48].
Uso de Herramientas	Ofrece orientación sobre el uso de herramientas y técnicas, pero no está tan orientado a herramientas específicas. [46]	Se centra en técnicas y herramientas para pruebas de seguridad de aplicaciones web [47].	Enfatiza el uso de herramientas respaldadas por el marco ISSAF, además de técnicas específicas [48].
Tiempo de Ejecución	Puede requerir varias semanas a meses, dependiendo del alcance del proyecto. [46]	Generalmente más rápido que OSSTMM debido a un enfoque más específico; semanas a pocos meses [47].	Depende de la profundidad de las pruebas; podría variar desde semanas hasta meses, según el alcance del proyecto.
Número de Personas en el Equipo	Puede funcionar con equipos de diferentes tamaños, dependiendo de la complejidad del proyecto. [46]	Puede funcionar bien con equipos más pequeños, especialmente en pruebas de aplicaciones web [47].	Puede requerir un equipo más grande debido a la variedad de pruebas de seguridad que cubre.

Documentación y Reportes	Se enfoca en la documentación de procedimientos de prueba. [46]	Pone un énfasis especial en la documentación y generación de reportes detallados [47].	Proporciona pautas para la documentación, pero con un enfoque en las pruebas en sí [48].
Enfoque Ético	Enfatiza la ética y la responsabilidad en las pruebas de seguridad en redes. [46]	Promueve pruebas de aplicaciones web y sistemas con ética [47].	Los criterios se alinean con la satisfacción de estándares de seguridad y regulaciones [48].
Cobertura de Temas	Amplia cobertura de seguridad en redes, sistemas y aplicaciones. [46]	Enfocado principalmente en pruebas de seguridad en aplicaciones web [47].	Enfocado en pruebas de seguridad en varios dominios en general [48].
Popularidad	Enfocada en seguridad en redes, utilizada en proyectos que involucran redes inalámbricas. [46]	Menos común que OSSTMM, pero utilizado en pruebas de aplicaciones web [47].	Reconocida en la comunidad de seguridad y utilizada en pruebas variadas [48].

La elección de la metodología ISSAF se fundamenta en su enfoque integral y detallado para realizar pruebas éticas de hacking. Proporciona una estructura organizada que abarca desde la planificación hasta la ejecución y la presentación de informes. Sin embargo, para una evaluación más específica, se ha decidido complementar esta metodología con OWISAN para abordar los controles de seguridad. Esta combinación de metodologías se selecciona para garantizar una evaluación profunda y bien equilibrada de la seguridad en redes inalámbricas, así como para fortalecer los controles de seguridad en general.

3.2 Desarrollo de la Propuesta

La propuesta incorpora un enfoque integral para abordar la evaluación y el fortalecimiento de la seguridad en la conexión Institucional. El esquema de esta fase de este proyecto se basa en los principios y directrices de la metodología ISSAF. La planificación y la preparación son esenciales para determinar el alcance del trabajo, establecer modalidades de ejecución y crear un plan que oriente las actividades a lo largo de las diferentes fases. En esta etapa, la evaluación implica la realización de pruebas tanto activas como pasivas para descubrir y abordar posibles vulnerabilidades. Este método resulta en un análisis de la seguridad que no solo proporciona una visión crítica de las áreas de riesgo, sino que también establece las bases para futuras implementaciones y mejoras en el marco de la ciberseguridad de la institución.

3.2.1 Fases de aplicación de Pruebas de la metodología IssaF

La ejecución de las pruebas de vulnerabilidad en las redes inalámbricas, se llevará a cabo conforme a las directrices establecidas por la metodología ISSAF específicamente en la sección M que aborda la Evaluación de Seguridad WLAN [48]. Este enfoque metódico proporcionará un marco estructurado para la identificación y evaluación de posibles amenazas en la infraestructura de red.

Figura 11: Fases de metodología ISSAF

Se seguirá los pasos delineados por esta metodología estructurada en tres fases que constituye el marco principal para garantizar la integridad de las pruebas y la ética en cada fase del proceso de hacking ético. Este enfoque organizado facilitará la identificación de vulnerabilidades en la red inalámbrica, permitiendo así una comprensión detallada de los riesgos potenciales.

Las fases y tareas a realizar son:

- **Fase 1 (Planeación y Preparación):** Se crea el marco de trabajo, se establecen y delimitan los propósitos de análisis de esta fase inicial. Para el éxito de las siguientes fases, es necesaria una planificación detallada y la identificación de los recursos necesarios.
- **Fase 2 (Evaluación):** El núcleo de la metodología es la etapa de evaluación. Las pruebas de penetración se realizan en esta fase. Se realiza una exploración de la red con el fin de identificar posibles brechas de seguridad. Los hallazgos se registran de manera meticulosa, lo que da una imagen clara de los puntos débiles.
- **Fase 3 (Reportes, Limpieza y Destrucción de Artefactos):** La fase final implica la presentación de informes que documentan los resultados de la evaluación, destacando las vulnerabilidades identificadas y proponiendo soluciones para su mitigación. Además, se aborda la limpieza de cualquier rastro dejado durante las pruebas y la destrucción de artefactos utilizados, garantizando la integridad y confidencialidad de la información.

a. Fase 1: Planificación y Preparación.

- ***Alcance del Trabajo:***

  - El proyecto se lleva a cabo en la Institución Educativa.
  - Los tipos de pruebas de penetración son intrusivo y no intrusivo.
  - La modalidad del desempeño de caja negra se aplica en el servicio de hacking.
  - Las pruebas de seguridad se llevan a cabo durante las horas laborales.

- ***Planificación de Actividades***

La planificación de actividades se rige por las etapas esenciales de la metodología ISSAF. Con atención particular a la Fase 2: Evaluación, en la cual se lleva a cabo las pruebas de penetración.

b. Fase 2: Evaluación

Mediante la ejecución de pruebas según la metodología ISSAF, se pueden identificar dos modalidades de ataques:

- ***Ataques Activos***

Es una acción deliberada y directa realizada por un agente malintencionado con el objetivo de comprometer, alterar o dañar sistemas, redes o datos. En este tipo de ataque, el atacante interviene directamente, ejecutando acciones intrusivas como la manipulación de datos, la inyección de código malicioso o la interrupción del funcionamiento normal de un sistema.

- ***Ataques Pasivos***

Es sutil y se centra en la observación y recopilación de información sin alterar activamente los sistemas. Durante un ataque pasivo, un atacante intercepta y monitoriza comunicaciones, tráfico de red o datos, con el propósito de obtener información confidencial sin dejar rastros evidentes de su presencia.

- ***Identificación de Pruebas de Seguridad:***

Basándose en las secciones de los controles OWISAM, se determinaron las pruebas de seguridad a llevar a cabo, siguiendo las subfases específicas de la metodología ISSAF para redes WLAN. Además, es importante vincular las herramientas de hacking ético y sus modos de ataque a las pruebas.

Aunque existen 64 controles de la metodología OWISAM, más detalles en Anexo A, en esta evaluación se selecciona nueve de las diez secciones. Esto se basa en la importancia de concentrarse en los elementos significativos para la seguridad de la red, lo que permite una evaluación de infraestructura completa.

Tabla 10: Identificación de Pruebas de Seguridad Inalámbrica

SubFase ISSAF	Pruebas OWISAM	Controles OWISAM	Herramientas	Modo Ataque
Recopilación de Información	Descubrimiento activo de dispositivos y redes.	**(OWISAM-DI-005)**	Acrylic Wifi Analyzer.	Pasivo
Escaneo	Identificación de funcionalidades soportadas por el dispositivo.	**(OWISAM-FP-002)**	Acrylic Wifi Analyzer.	Pasivo
Auditoría	Pruebas sobre WPS.	**(OWISAM-AU-002)**	Acrylic Wifi Analyzer.	Pasivo
	Interfaces accesibles desde la red.	**(OWISAM-IF-002)**	Navegador	Pasivo
	Prueba de AP/Router	**N/A**	Nmap.	Activo
Análisis y Búsqueda	Verificación del grado de amplitud de señal o área de alcance.	**(OWISAM-CF-003)**	Acrylic Wifi Analyzer.	Pasivo
	Análisis protocolos de cifrado WEP, TKIP	**(OWISAM-CP-004)**	Aircrack-ng	Activo
Explotación y Ataques	Captura y cracking de claves en el proceso de autenticación.	**(OWISAM-AU-004)**	Wifiphisher	Activo

	Pruebas de desautenticación.	**(OWISAM-DS-001)**	Aircrack-ng	Activo

3.2.2 Ejecución de pruebas

La ejecución de las pruebas de seguridad se registra mediante el empleo de una plantilla recomendada por la norma ISSAF. Este enfoque estructurado facilita la documentación detallada de los procedimientos, resultados y hallazgos, contribuyendo a una evaluación de protección en conexiones inalámbricas.

En la Tabla 8 se indica las pruebas que se ejecutaron en cada ítem de las subfases y fases proporcionadas por la metodología ISSAF y los controles OWISAM.

Las pruebas pasivas, como la recopilación de información, el escaneo y el análisis, se incluye en el Anexo B del para proporcionar un panorama general del entorno sin interferir en el desarrollo de los ataques activos.

Por otro lado, durante el desarrollo de la propuesta, se detalla y complementa las pruebas activas que implica el ataque directo a la red inalámbrica. Las especificadas en los controles de la metodología como la captura y el cracking de claves transmitidas, las pruebas de de autenticación y se adiciona la implementación de ataques como Man-in-the-middle y Evil Twin.

Esta estrategia tiene como objetivo no solo proporcionar un análisis ambiental completo, sino también evaluar activamente la resistencia y la seguridad de los sistemas involucrados.

Se ejecuta 4 de los ataques más comunes en redes inalámbricas, estos ataques activos se ejecutan mediante una secuencia.

Para evaluar la fortaleza de contraseñas se decidió iniciar con el ataque de fuerza bruta ya que pueden representar la mayor vulnerabilidad. En el caso de no obtener resultados

o para verificación de la contraseña capturada en el ataque anteriormente mencionado, se llevó a cabo un ataque de Evil Twin que se centra en crear puntos de acceso falsos para engañar a los usuarios. Este método sirve para buscar posibles debilidades en la percepción de los usuarios sobre las conexiones de red legítimas. Después, se implementó un ataque de denegación de servicio para evaluar la capacidad de la red soportando situaciones de saturación y agotamiento. Luego, se llevó a cabo un ataque Man-in-the-Middle con el objetivo de interceptar y analizar la comunicación entre los dispositivos conectados. La lógica de explorar desde las vulnerabilidades más básicas hasta los escenarios más complejos permitió una evaluación completa de la seguridad de la red en estudio.

Se optó por ocultar la información confidencial obtenida durante los procesos de penetración debido a la sensibilidad de los datos y la necesidad de cumplir con normas éticas y legales. Este proceso se implementó para proteger la privacidad de los usuarios y cualquier información sensible que se descubriera durante las pruebas de seguridad.

Instalación Máquina Virtual

Kali Linux, un sistema operativo conocido por su amplia gama de herramientas de seguridad, se utilizó para crear una máquina virtual en VMware como entorno de prueba para detectar vulnerabilidades potenciales en redes inalámbricas. Esta configuración proporciona un entorno controlado para explorar y utilizar una variedad de herramientas especializadas para encontrar fallas en redes Wi-Fi.

Asegurarse de que la máquina virtual pueda detectar conexiones Wi-Fi es esencial para realizar pruebas de penetración de manera efectiva. Al instalar Kali Linux, la conexión a Internet se establece por defecto a través de cable. No puede asignar la tarjeta de red del equipo a la máquina virtual porque ya está en uso en la máquina principal. Como resultado, para permitir que la máquina virtual se conecte inalámbricamente, se requiere una tarjeta de red Wi-Fi externa. Este paso garantiza que las pruebas abarquen redes inalámbricas, lo que proporciona una evaluación completa.

Configuración del adaptador o tarjeta de red

Esta tarjeta está configurada por defecto en modo Managed es decir "gestionado" o "administrado, debido a que está conectada a una red específica, lo que limita la capacidad de observación, no puede capturar todos los paquetes de datos que circulan por el aire.

Es necesario ajustar la configuración de la tarjeta de red al modo monitor en lugar de mantener la forma predeterminada.

En el modo "Monitor", la tarjeta de red puede capturar tráfico sin estar conectada a una red específica, lo que permite un análisis completo de las comunicaciones entre dispositivos. Esta modificación es importante en escenarios de investigación y evaluación de seguridad, donde se busca comprender y abordar los riesgos potenciales de las interacciones inalámbricas.

a. Ataque de Fuerza Bruta y Diccionario

Es una técnica de intrusión cibernética que se basa en la tenacidad y persistencia del atacante para descifrar contraseñas Wi-Fi y obtener acceso no autorizado a sistemas protegidos. En este tipo de ataque, el atacante intenta sistemáticamente varias combinaciones de contraseñas hasta obtener la adecuada. Es una estrategia que explora la debilidad de las contraseñas al probar todas las opciones, desde combinaciones simples hasta complejas, con el objetivo de encontrar la clave correcta que permita el acceso no autorizado. Esta prueba se realiza con la ayuda de un diccionario para evaluar todas las combinaciones posibles.

Se ha elegido Aircrack-ng como herramienta para llevar a cabo el primer ataque durante la realización de este proyecto de investigación, la misma se destaca por su capacidad para analizar vulnerabilidades en redes Wi-Fi.

La selección de estas herramientas se basa en que la metodología lo establece usar, además en su capacidad para detectar y explotar fallas en redes inalámbricas. Usar esta combinación estratégica para llevar a cabo un ataque de fuerza bruta controlado, utilizando metodologías y principios éticos estrictos.

Para llevar a cabo el ataque se aplica los siguientes pasos:

1. Abrir la máquina virtual VMWare e iniciar sesión en Kali Linux una vez dentro abrir una terminal y en modo root instalar aircrack-ng.

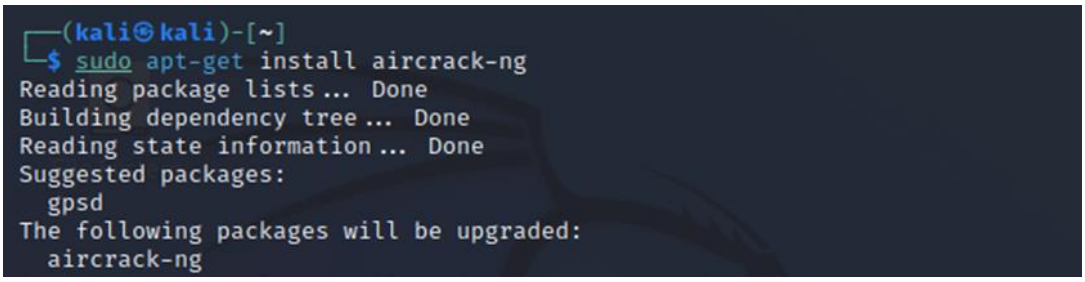


Figura 12: Instalación de aircrack-ng.

2. Con el comando iwconfig, se verifica la tarjeta de red, en esta práctica se denomina wlan0

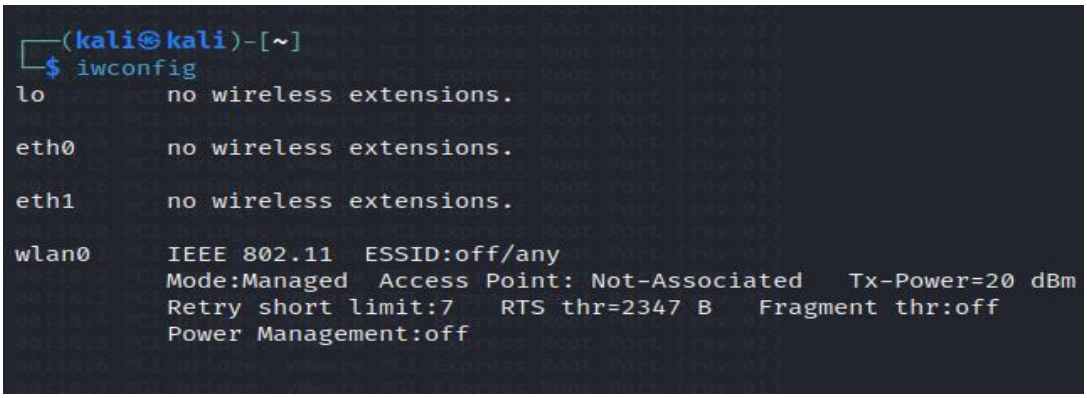


Figura 13: Visualización interfaz de red

3. Activar el modo escucha o monitor del adaptador de red con el comando **airmon-ng start wlan0** que se visualiza en la Figura 14.

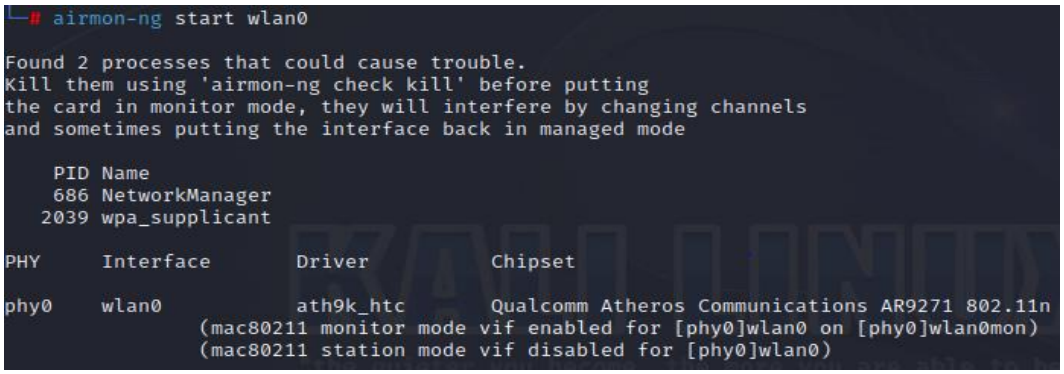


Figura 14: Comando habilitar modo monitor tarjeta de red

4. Verificar con el comando iwconfig, la tarjeta de red ahora aparece con el nombre wlan0mon

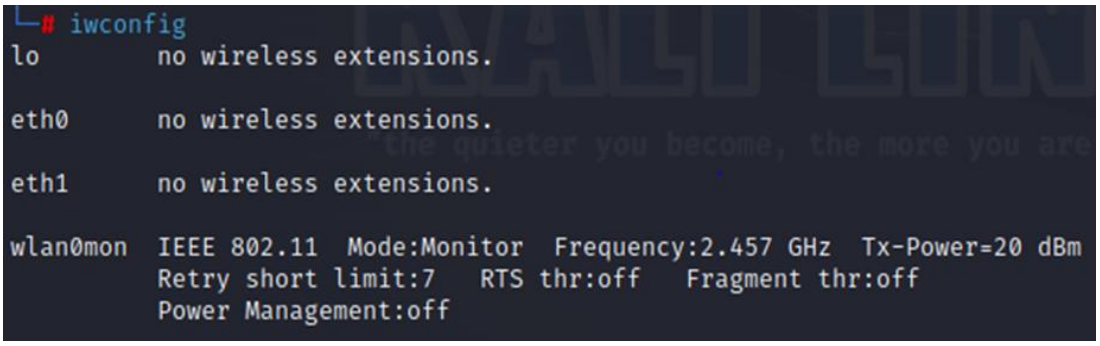


Figura 15: Tarjeta de red modo monitor

5. Monitorear las redes disponibles o redes en el área de cobertura con el comando airdump-ng y la interfaz de red wlan0mon.

Figura 16: Comando buscar redes disponibles

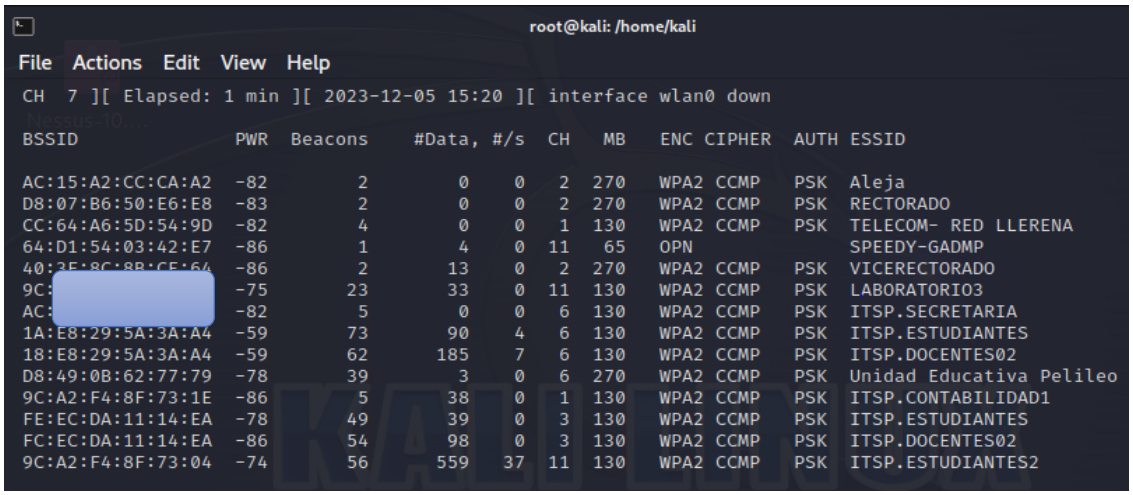


Figura 17: Redes encontradas al auditar

6. Seleccionar la red de la Institución para monitoriar y capturar su tráfico con el comando airodump-ng -w “Nombre del archivo .cap” -bssid “Dirección MAC del router de red” -c “Numero canal de la red” “Interfaz de la tarjeta de red”

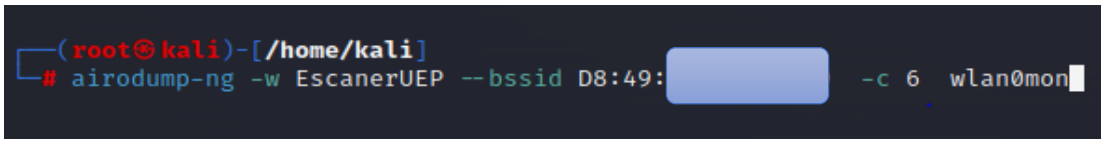


Figura 18: Comando para crear archivo cap

7. Captura de handshake para determinar que el cliente como el punto de acceso tienen las credenciales correctas

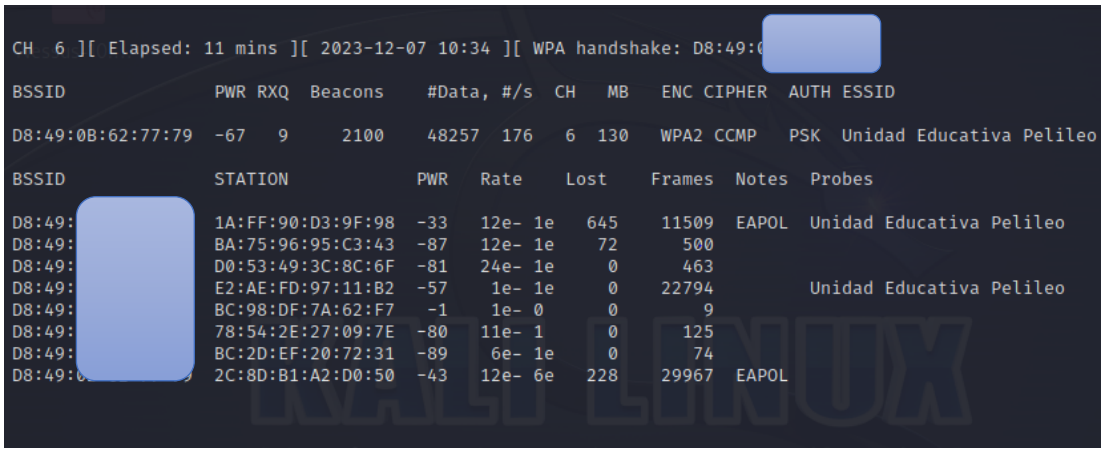


Figura 19: Captura Handshake

8. Emplear un diccionario (Creado o Preestablecido) para intentar “adivinar” la contraseña de la red, con el comando aircrack-ng “Dirección de la ubicación del archivo .cap” -w “Dirección de la ubicación del diccionario”

Figura 20: Comparación archivo cap y diccionario preestablecido

9. Luego que ha realizado una comparación el archivo .cap creado con el tráfico de la red y el diccionario no se ha podido obtener la contraseña de la red.

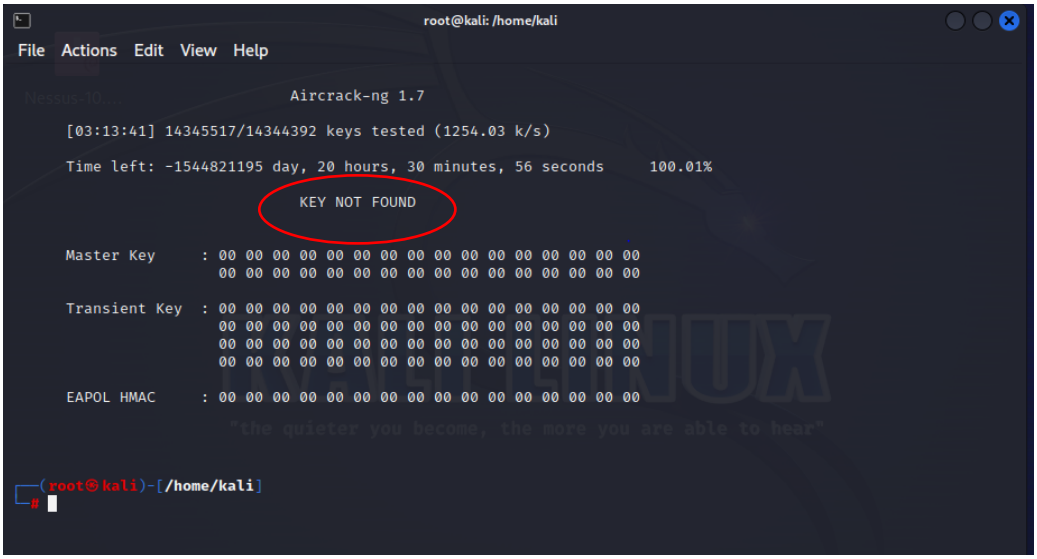


Figura 21: Captura de contraseña

El proceso de conseguir la combinación correcta de passwords puede resultar complicado, porque depende de la dificultad de determinar las claves. Las contraseñas suelen ser sencillas en la mayoría de los hogares porque son muy fácil de recordar. En este caso, se puede realizar un ataque de fuerza bruta y diccionario, pero no obtener la clave de red, el resultado depende si la clave no es muy compleja.

b. Ataque Evil Twin o Gemelo Malvado

Este ataque es considerado como una parte de ingeniería social para engañar a los internautas y obtener credenciales de usuario que, sin darse cuenta, proporcionan datos que permiten violaciones de seguridad.

También llamados ataque del "gemelo malvado", donde el atacante imita un punto de acceso similar al que el cliente se conecta habitualmente y, tras desencadenar diversas situaciones, permite al usuario obtenga más información sobre las contraseñas.

Para efectuar el ataque de Evil Twin, se hace uso de Wifiphisher en el entorno de pruebas. Es una herramienta diseñada para realizar ataques de suplantación de identidad en redes inalámbricas. Su habilidad para crear copias maliciosas de puntos

de acceso legítimos le permite desempeñar un papel importante en la ejecución de este ataque.

El uso de Wifiphisher conlleva a la utilización de dos antenas que funcionan como:

Un punto de acceso falso antena: (TP-LINK).

Para des autenticar a los usuarios que se encuentren en el punto de acceso real se utiliza la antena: (Alfa Network).

1. Instalar wifiphisher y abrir con el siguiente comando visualizado en la **Figura 22.**

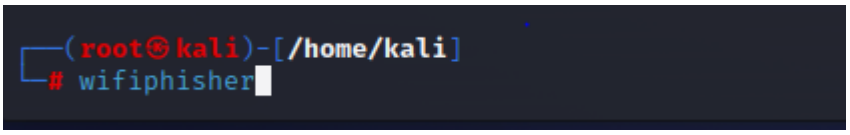


Figura 22: Comando wifiphisher

2. Se despliega una ventana con las redes cercanas. Para esta práctica se selecciona la red con el nombre de la Institución Unidad Educativa Pelileo.

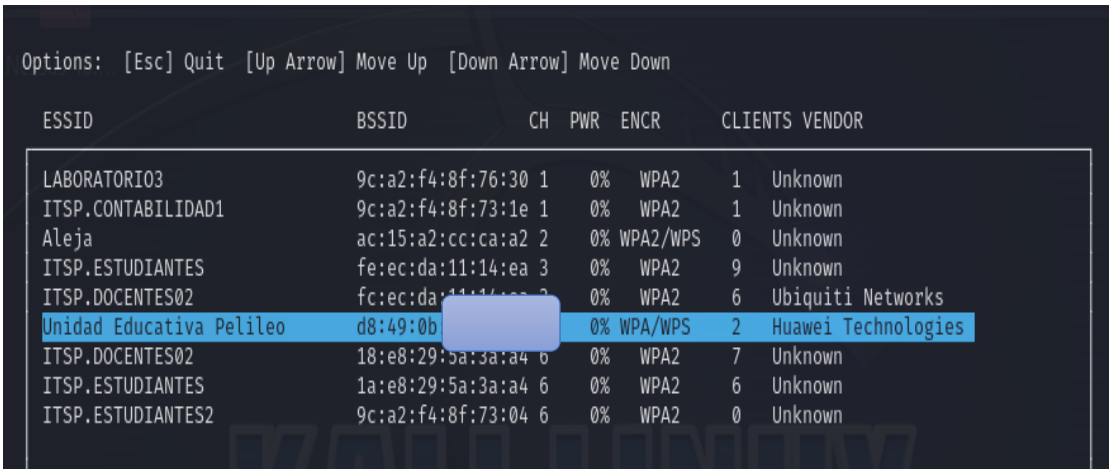


Figura 23: Selección de la red a atacar

3. En la siguiente interfaz se selecciona DAuth Login Page, este simula un portal de login de Facebook para intentar capturar credenciales importantes.

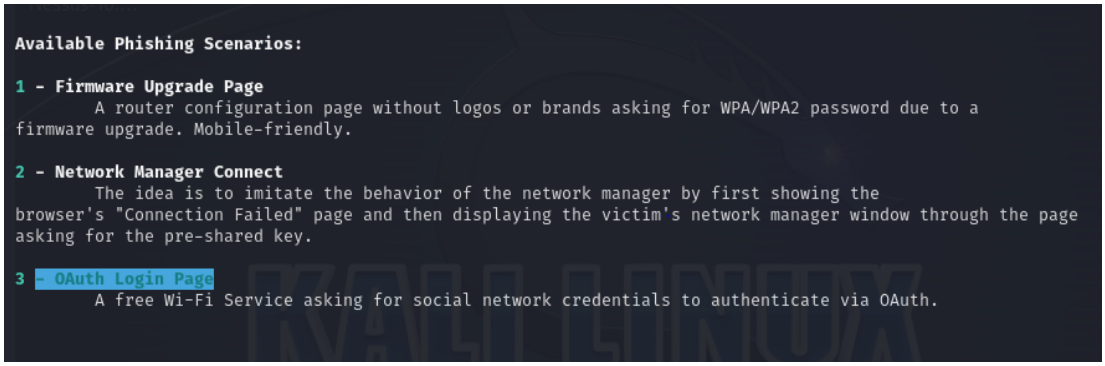


Figura 24: Selección del portal cautivo

4. Visualizar en el apartado de las redes WiFi que se ha creado una red con el nombre igual a la que vamos a obtener la contraseña, pero su estado es abierto.

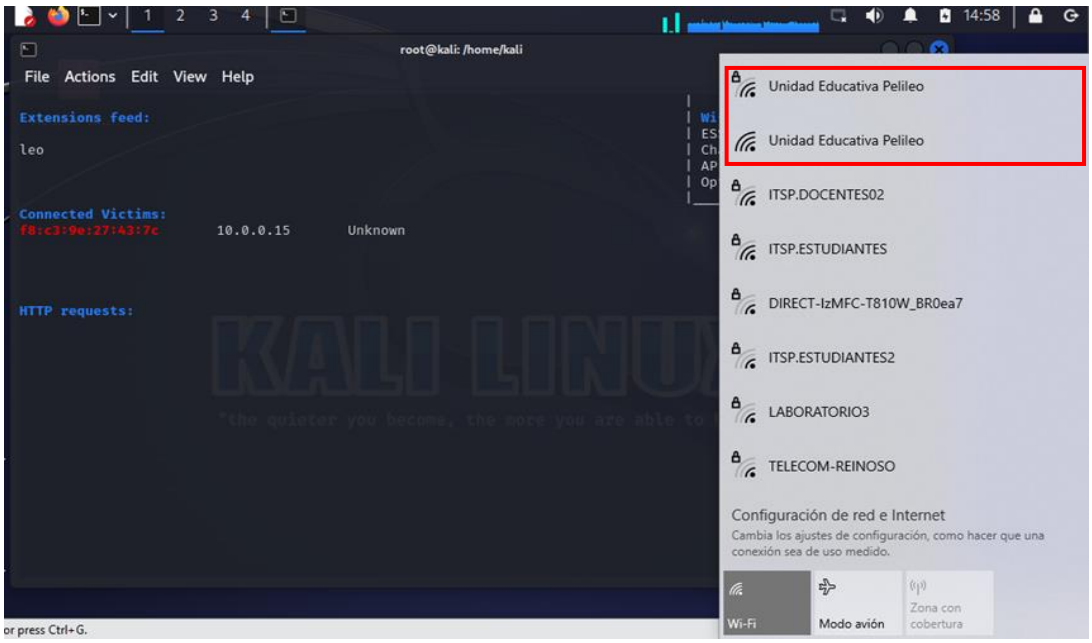


Figura 25: Red atacada duplicada

5. Los usuarios serán desconectados de la red y no se le permitirá conectarse otra vez por lo que tendrán que acceder a la red abierta con el mismo nombre, al intentar conectarse de nuevo se re direcciona a un portal cautivo para intentar obtener credenciales.

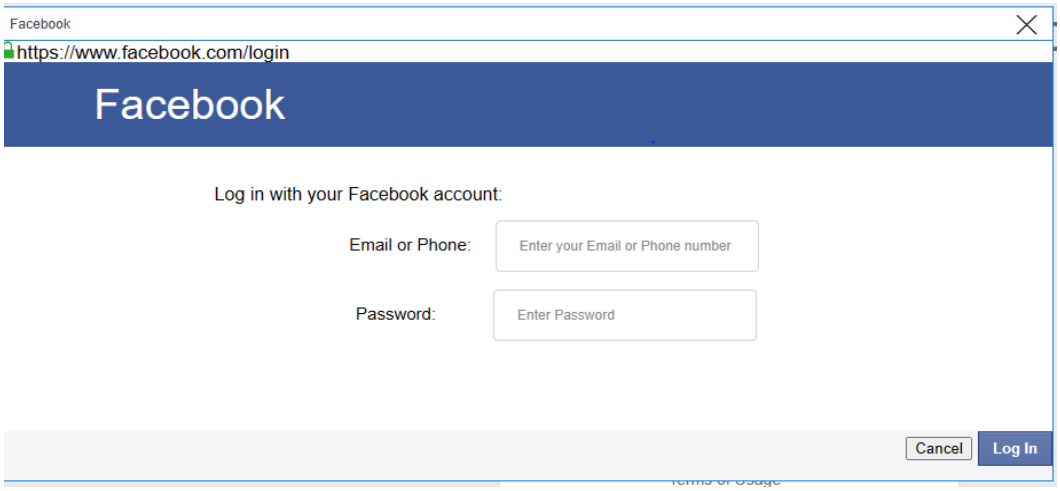


Figura 26: Portal cautivo simulando login de Facebook

6. En la interfaz de wifiphisher se muestra las víctimas posibles, se logró obtener las credenciales que un usuario ingreso mediante el login de Facebook para poder obtener acceso a la red.

Figura 27: Interfaz wifiphisher capturando credenciales

7. Presionar ESC y se termina la ejecución de ese portal. Al salir también se muestra las credenciales capturadas.

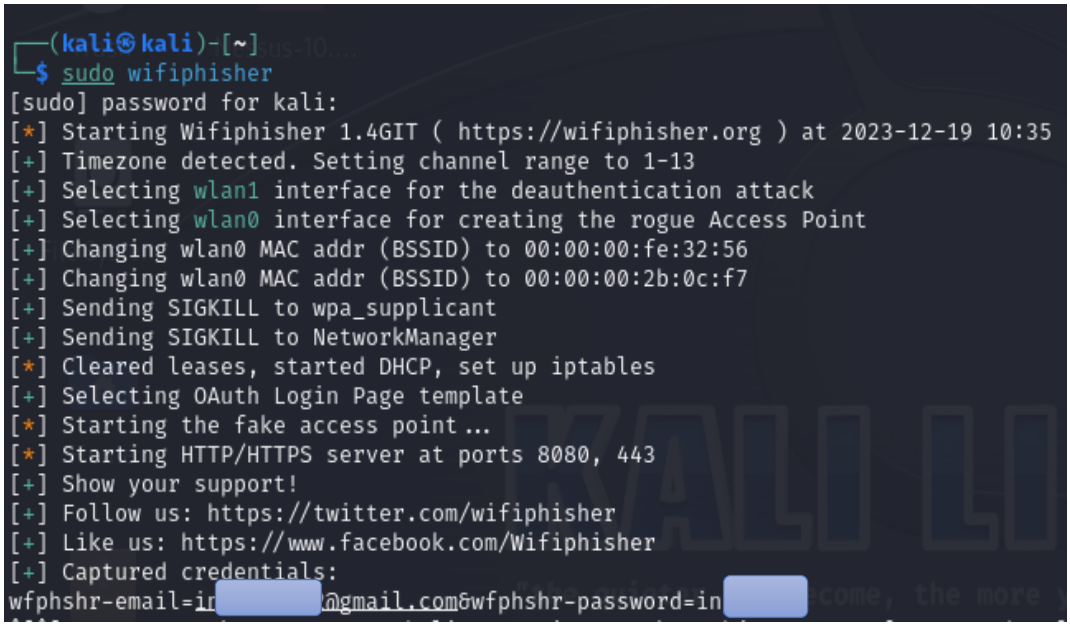


Figura 28: Captura de credenciales login Facebook

8. Ingresar nuevamente el comando wifiphisher y seleccionar Network Manager Connect, este portal interrumpe la conexión y solicita que se ingrese la contraseña otra vez.

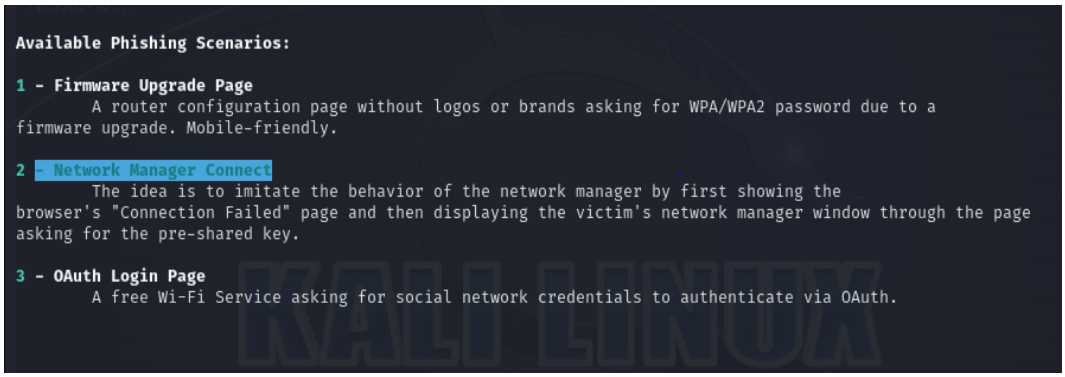


Figura 29: Portal Network Manager Connect

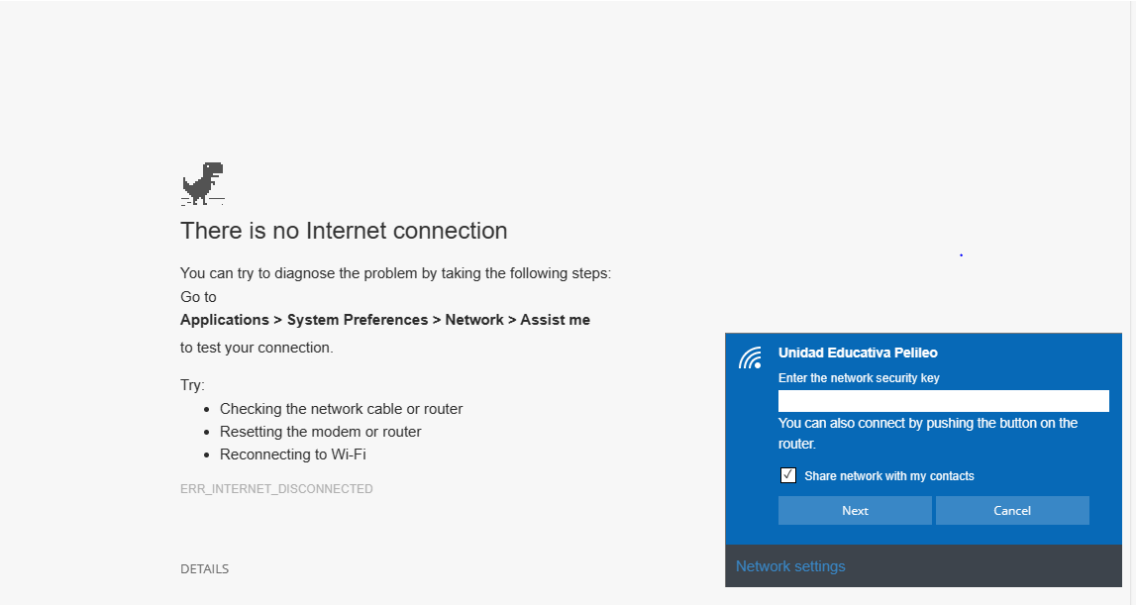


Figura 30: Portal cautivo obligando a ingresar nuevamente credenciales de red

9. Terminar la ejecución de wifiphisher con ESC, visualizar que se ha capturado la contraseña de la red. En este caso varios usuarios ingresaron nuevamente la clave de red.

Figura 31: Wifiphisher capturando credenciales de red

c. Ataque de Denegación de Servicios (DoS)

Son estrategias cibernéticas maliciosas destinadas a paralizar o disminuir la disponibilidad de un servicio, recurso o red, haciéndolos inaccesibles para los usuarios legítimos.

Estos ataques tienen como objetivo abrumar los sistemas objetivo con una carga tan fuerte que impidan su funcionamiento adecuado.

En esencia, un atacante satura la capacidad de procesamiento, el ancho de banda o los recursos del sistema, lo que hace que los usuarios legítimos no puedan acceder al servicio. Esto puede lograrse de una variedad de maneras, como saturar una red con tráfico, explotar fallas en el software o agotar los recursos del sistema.

Para el ataque DoS se utilizó la herramienta Aircrack-ng esta aplicación, proporciona las capacidades necesarias para generar tráfico malicioso y saturar deliberadamente los recursos de la red. Aircrack-ng se utiliza para evaluar la capacidad de la infraestructura de red de la institución educativa para resistir interrupciones. Para fortalecer la seguridad de la red, este enfoque táctico permite identificar posibles debilidades y sugerir métodos de mitigación específicos.

Los pasos para este ataque son los siguientes:

1. Habilitar el modo monitor de la tarjeta de red con el comando que se visualiza en la Figura 32.

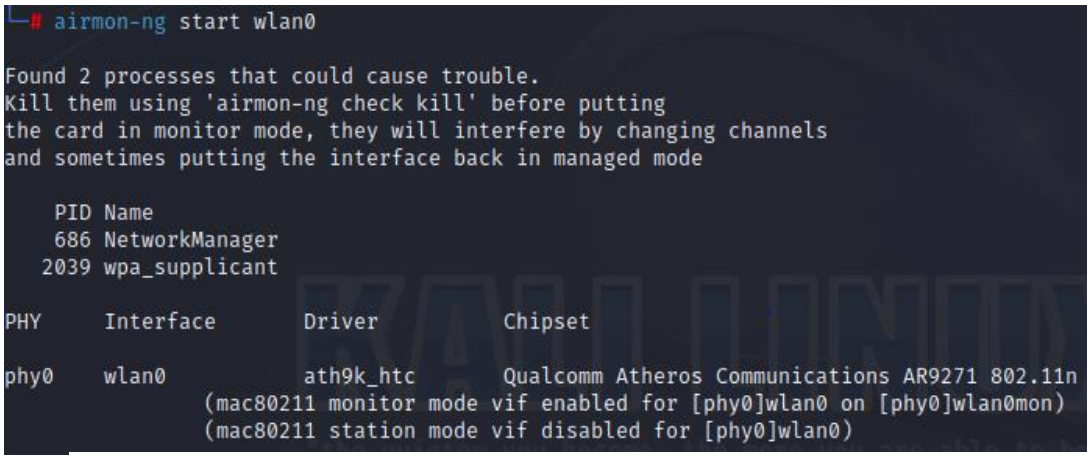


Figura 32: Habilitar tarjeta de red modo monitor

2. Verificar con el comando iwconfig, la tarjeta de red ahora aparece con el nombre wlan0mon

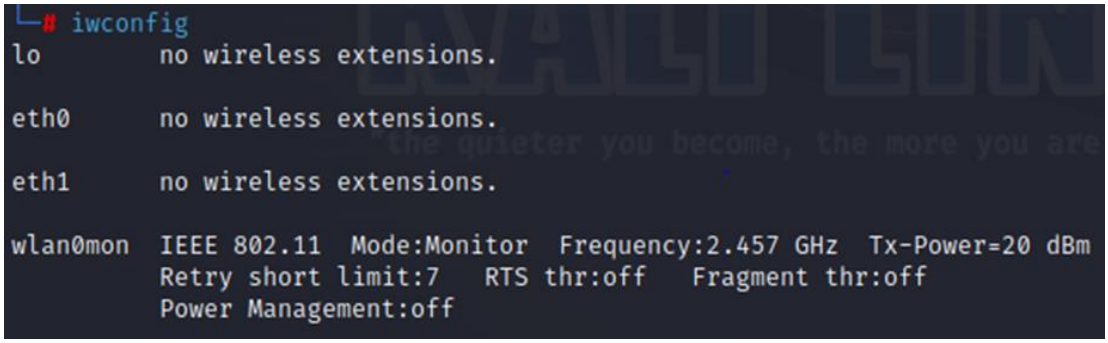


Figura 33: Interfaz de red en modo monitor

3. Monitorear las redes disponibles o redes en el área de cobertura con el comando airdump-ng y la interfaz de red wlan0mon.

Figura 34: Comando buscar redes disponibles

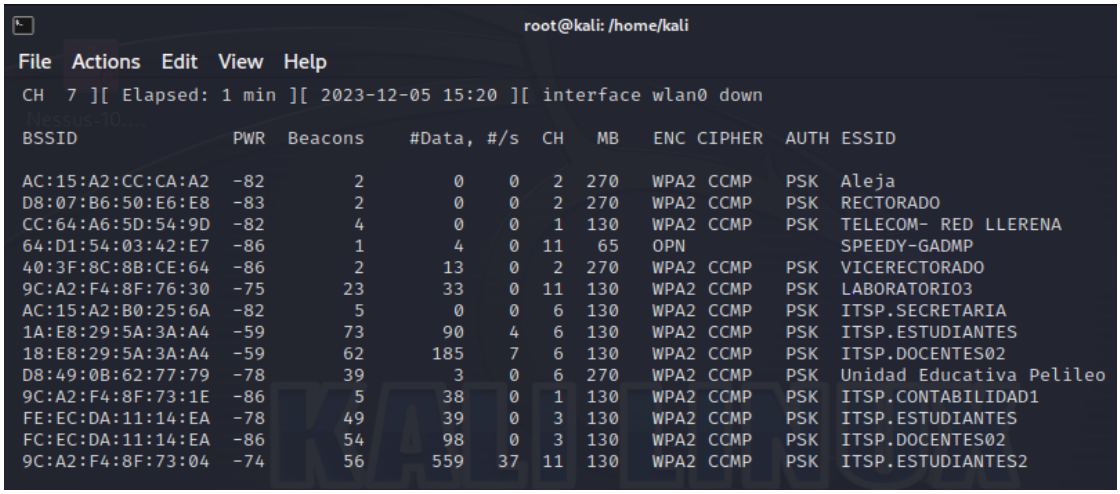


Figura 35: Redes disponibles encontradas

4. Seleccionar un dispositivo que se encuentre conectado a la red víctima para realizar la denegación de servicios.

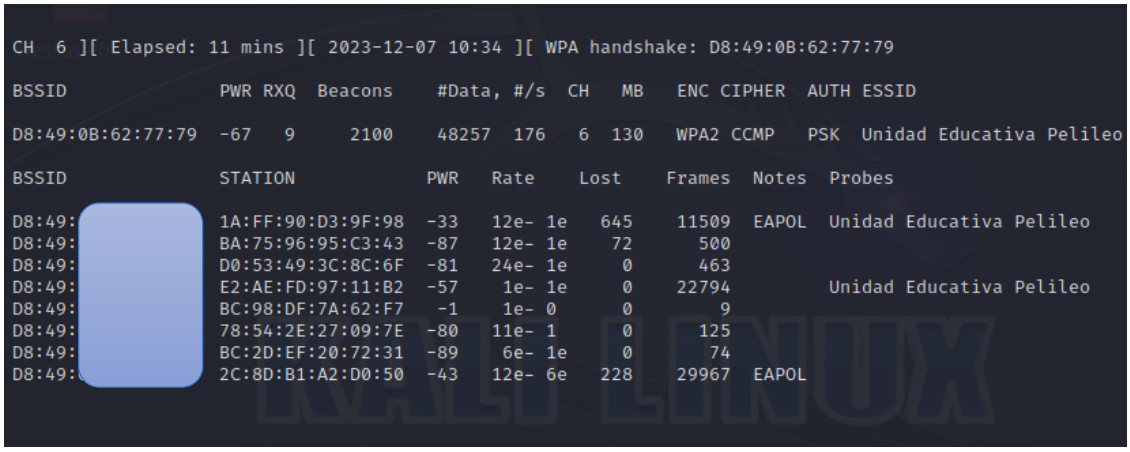


Figura 36: Dispositivos conectados

5. Antes de ejecutar el ataque es importante capturar el handshake, la primera prueba se realiza al router y se envían 300 mensajes, se utiliza la MAC de la puerta de enlace.

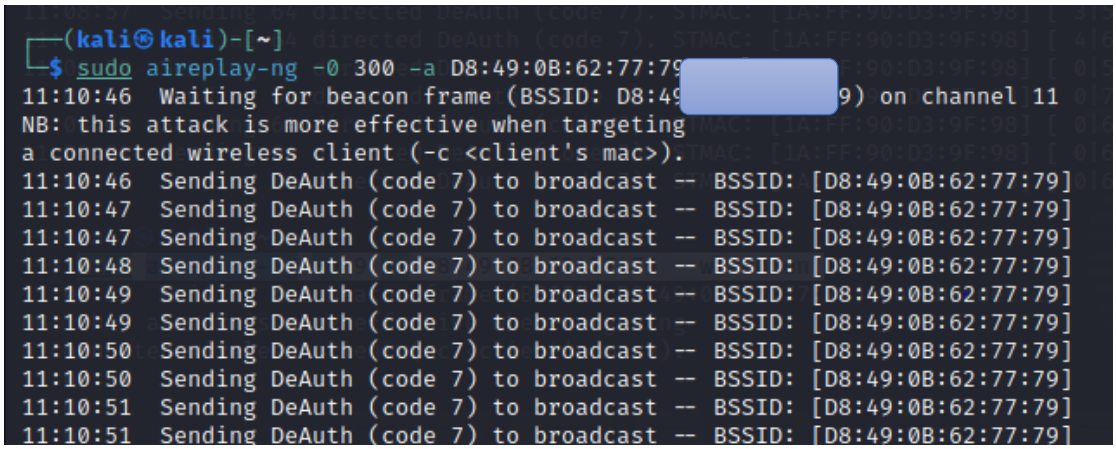


Figura 37: Comando de DoS a todos los dispositivos conectados al router

6. Con el comando de la figura se envía 200 mensajes de des-autenticación al dispositivo con dirección MAC 2C:8D: B1:A2: D0:50

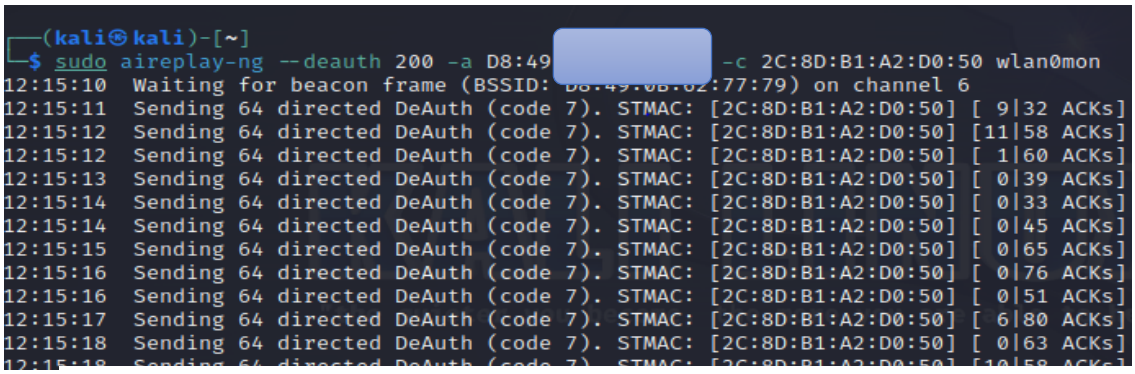


Figura 38: Comando de des-autenticación a un dispositivo

Al enviar 200 mensajes de des-autenticación dirigidos a un dispositivo específico, se logró evitar que dicho dispositivo se conectara a la red. Este ataque tuvo un resultado exitoso, mientras que los demás dispositivos continuaron manteniendo su conexión sin interrupciones.

d. Ataque Man-in-the-Middle

Es una táctica compleja que pone en peligro la seguridad de las comunicaciones digitales. Este tipo de ataque está en el centro de la vulnerabilidad porque actúa como un intruso invisible que interfiere con la comunicación entre dos partes.

Infiere entre dispositivos, usuarios o sistemas. El atacante man-in-the-middle intercepta, altera e incluso genera datos en tiempo real, creando una ilusión de comunicación legítima en lugar de ser detectado directamente. Este fenómeno pone en peligro la confidencialidad y la privacidad de la información transmitida.

Para realizar este ataque se ejecuta a través de la herramienta Ettercap en Kali Linux. Este método estratégico simula una situación en la que un atacante puede interrumpir la comunicación entre dos partes. Para evaluar la vulnerabilidad de la red ante estas amenazas, se emplea una variedad de técnicas MitM, como el envenenamiento de ARP. Este análisis detallado ayudará a desarrollar estrategias específicas para mejorar la seguridad de la red al identificar posibles puntos de debilidad.

Los pasos para la ejecución de este ataque son:

1. En la parte superior izquierda seleccionar el icono de Kali y buscar ettercap grafical. Abrir y seleccionar como primary interface **wlan0**, en los tres puntos escoger promisc mode, finalmente presionar en el símbolo de visto.

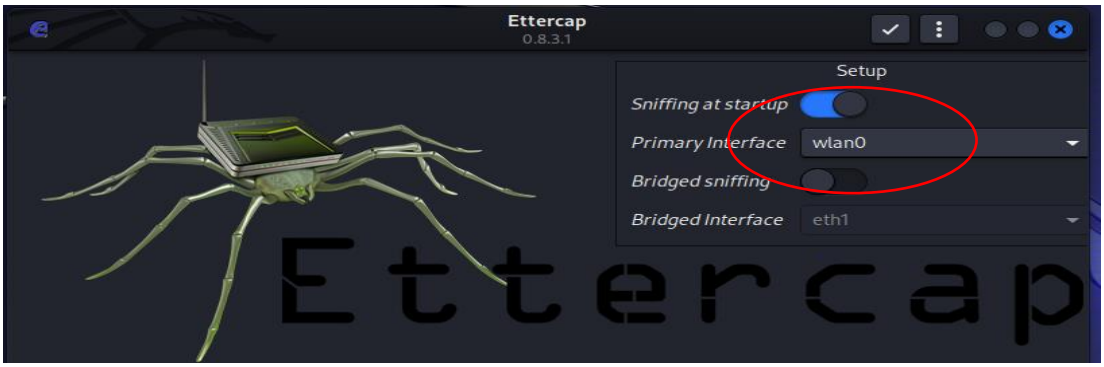


Figura 39: Ettercap, interfaz gráfica

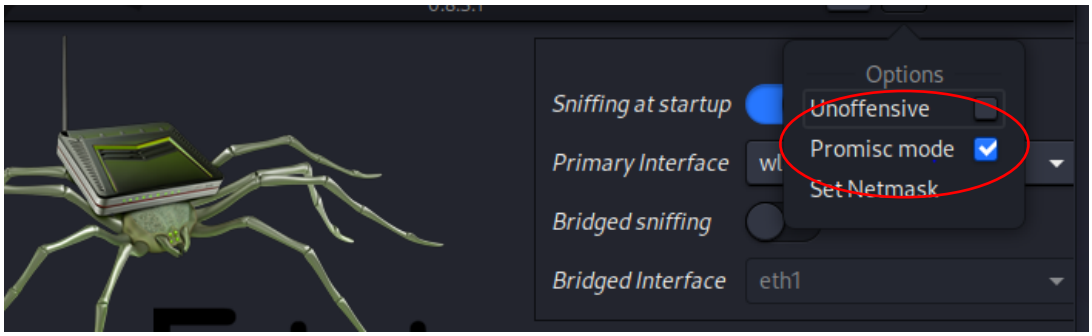


Figura 40: Activar modo promiscuo

2. En la parte superior presionar en el icono de lupa para la búsqueda de host de la red.

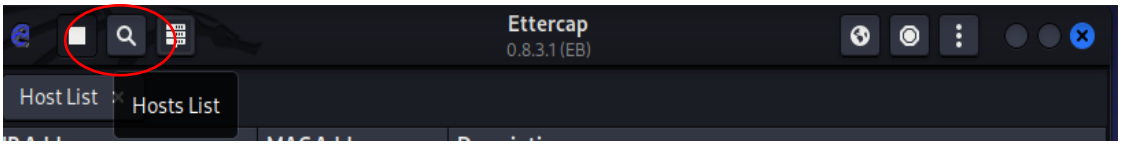


Figura 41: Búsqueda de hosts

3. Con la opción List Host, se listan los Host activos.

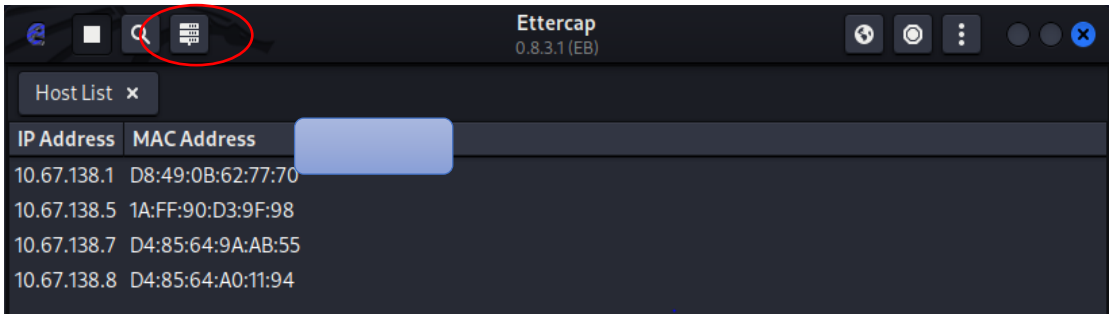


Figura 42: Host encontrados

4. Seleccionar los targets, la IP de la víctima como TARGET1 y la IP de la puerta de enlace como TARGET2 como se visualiza en la Figura 43.

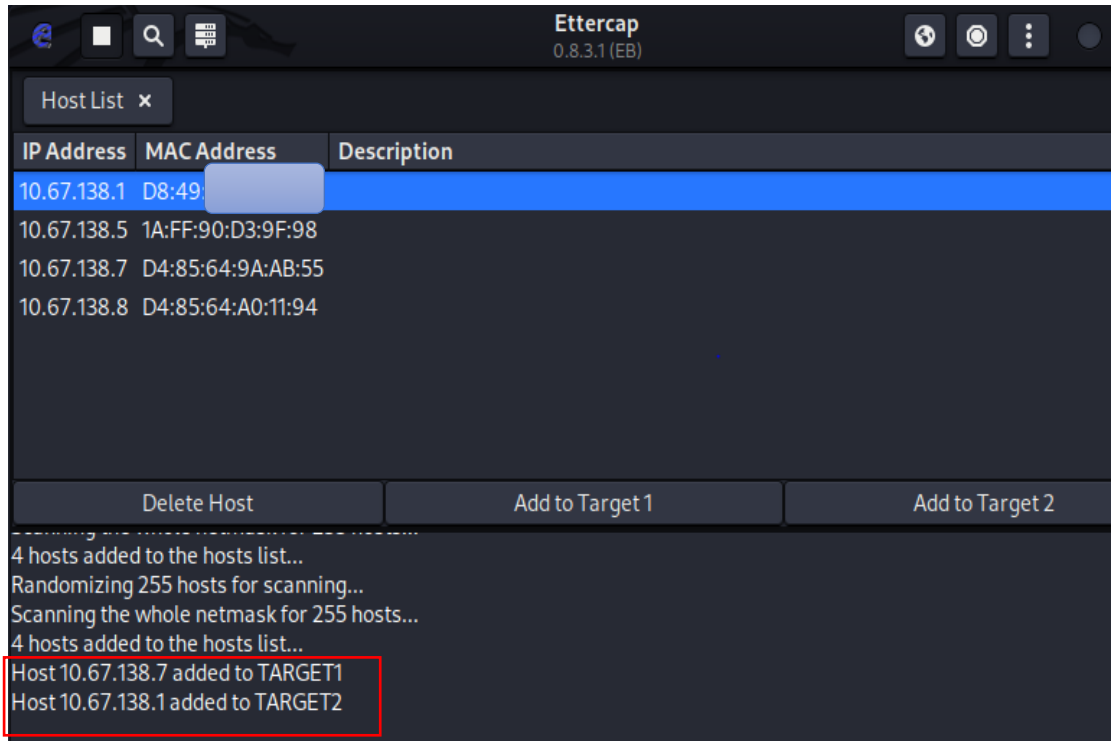


Figura 43: Selección de targets, IP de victima e IP del atacante

5. En la parte superior derecha escoger el icono de mundo y seleccionar ARP Poisoning para envenenar las tablas ARP.

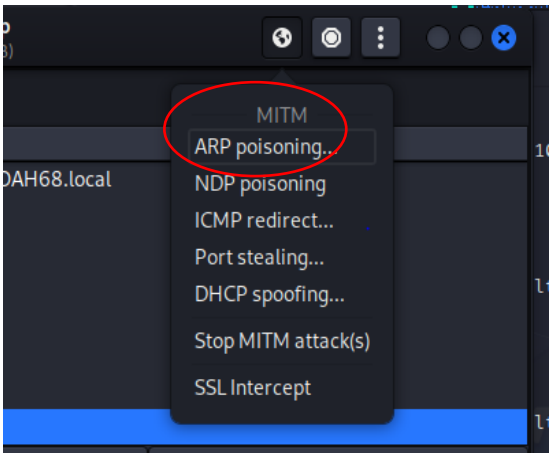


Figura 44: ARP poisoning

6. Seleccionar Sniff remote connections.

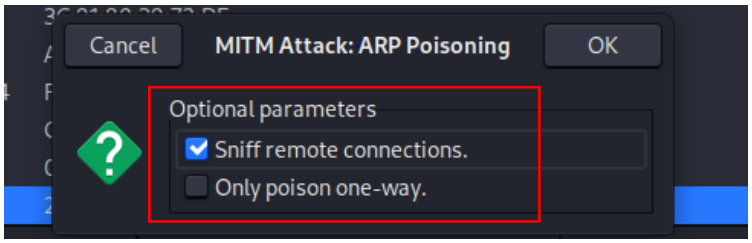


Figura 45: Sniff remote connections

7. Para observar el tráfico de la red que existe ingresar a Wireshark. Elegir el tipo de tarjeta de red que está utilizando, en este caso wlan0, de esta manera se visualiza el tráfico de los dispositivos inalámbricos conectados en la red.

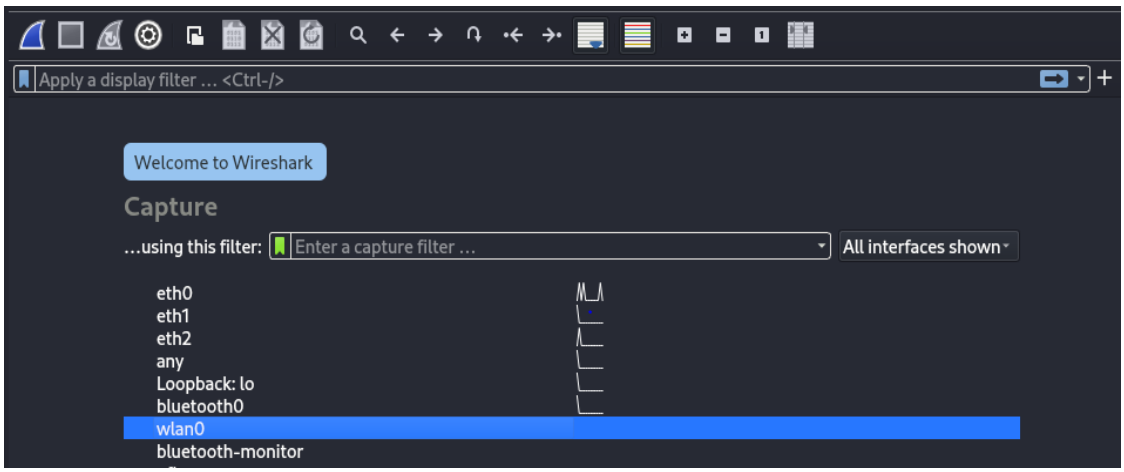


Figura 46: Elección de tarjeta de red en la Interfaz de Wireshark

8. Wireshark muestra todo el tráfico, los protocolos de red, los paquetes de datos, IP emitidas y receptadas en consultas, entre otras cosas.

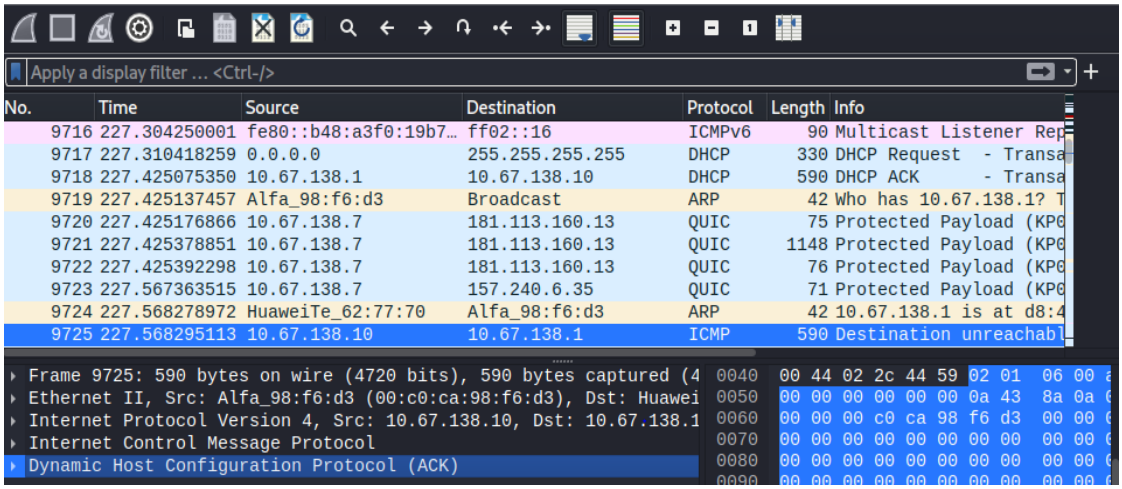


Figura 47: Tráfico de red en Wireshark

9. Ingresar http como filtro para observar los paquetes que se envían por este protocolo de internet, el cual refleja la navegación.

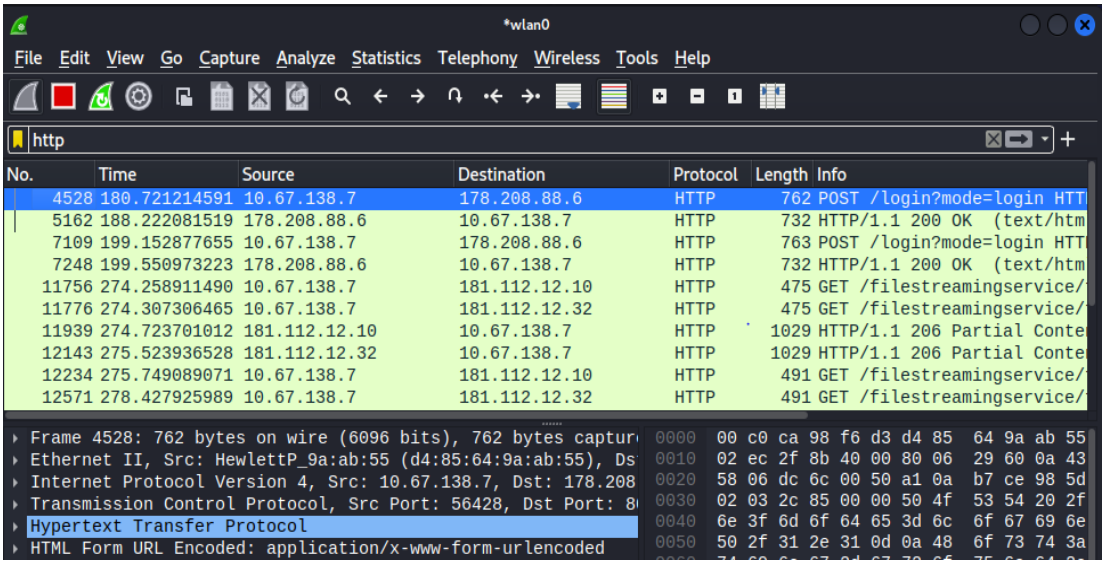


Figura 48: Filtrado de Http en Wireshark

10. Ettercap captura credenciales las cuales provienen de un Http seguido de una dirección url de un sitio web.

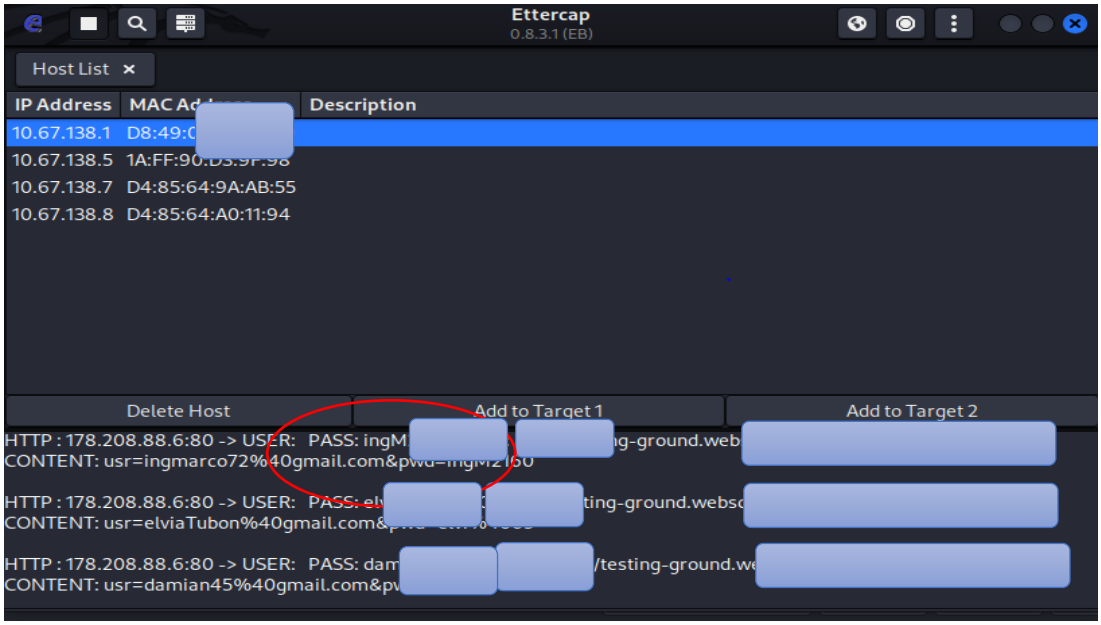


Figura 49: Captura de credenciales

Durante el análisis de Wireshark se observan dos métodos: GET y POST. Ambos métodos analizan el tráfico de datos de la navegación web, especialmente cuando un usuario completa un formulario de registro en un sitio web. Se puede verificar información importante sobre las actividades de inicio de sesión al concentrarnos en el método POST.

La función Follow se utilizó para explorar estos datos de manera más profunda, y luego se realizó el análisis del flujo TCP correspondiente. Este método permitió acceder y examinar de manera precisa los paquetes de datos relacionados con las interacciones de inicio de sesión, lo que mejoró la comprensión de la seguridad y los detalles del proceso.

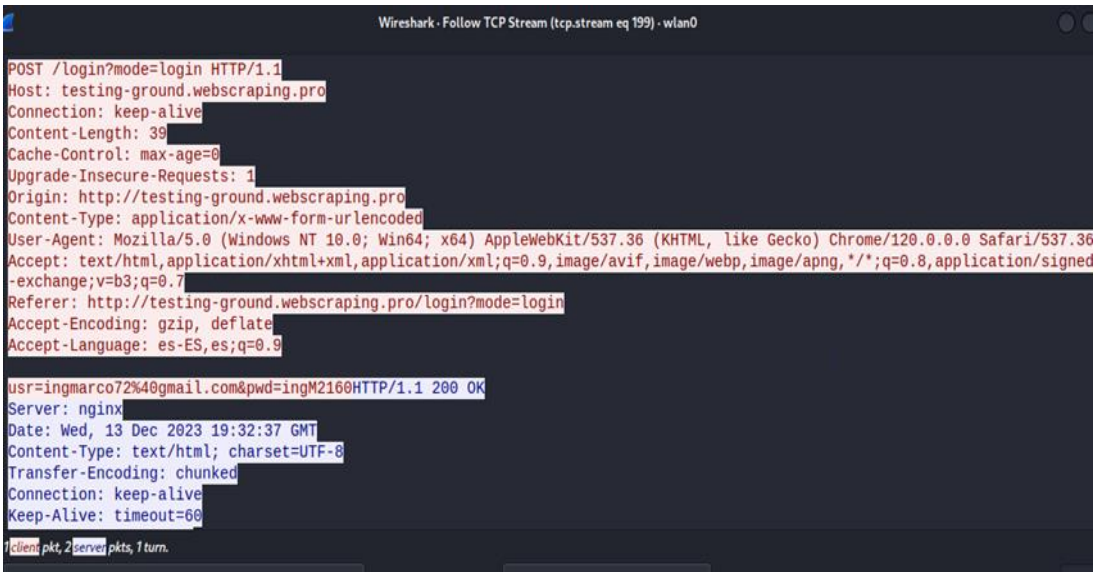


Figura 50: Información y credenciales de usuario mediante el método Post.

Para verificar que el ataque se ha dado con éxito, podemos observar la MAC del equipo que realiza el ataque, en este escenario es Kali Linux.

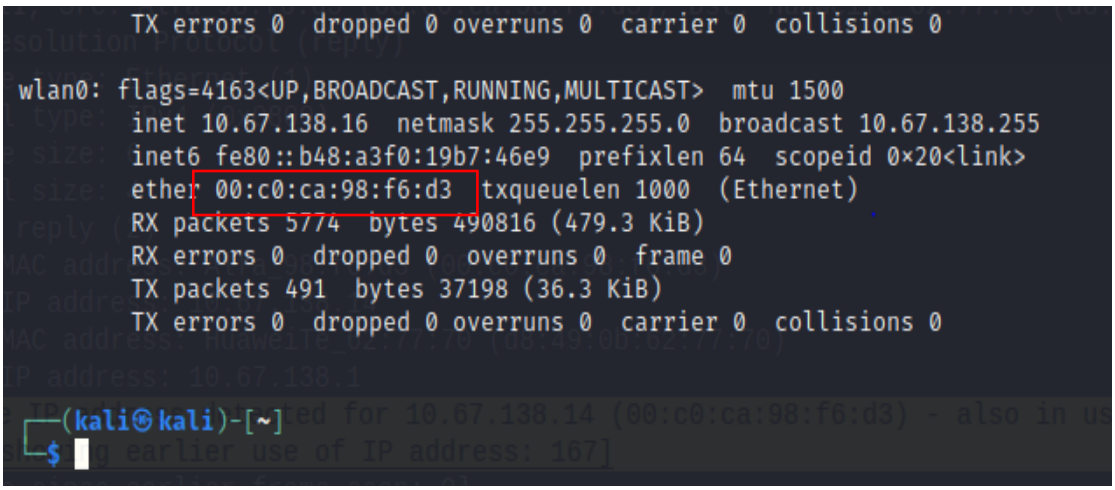


Figura 51: Dirección MAC máquina atacante

En Wireshark se puede observar que la puerta de enlace adquiere la Mac del equipo intruso y de la misma forma el dispositivo atacado. Así todo el tráfico que envían al realizar solicitudes pasa por la máquina que realiza el ataque como se puede visualizar en la Figura 52 y en la Figura 53.

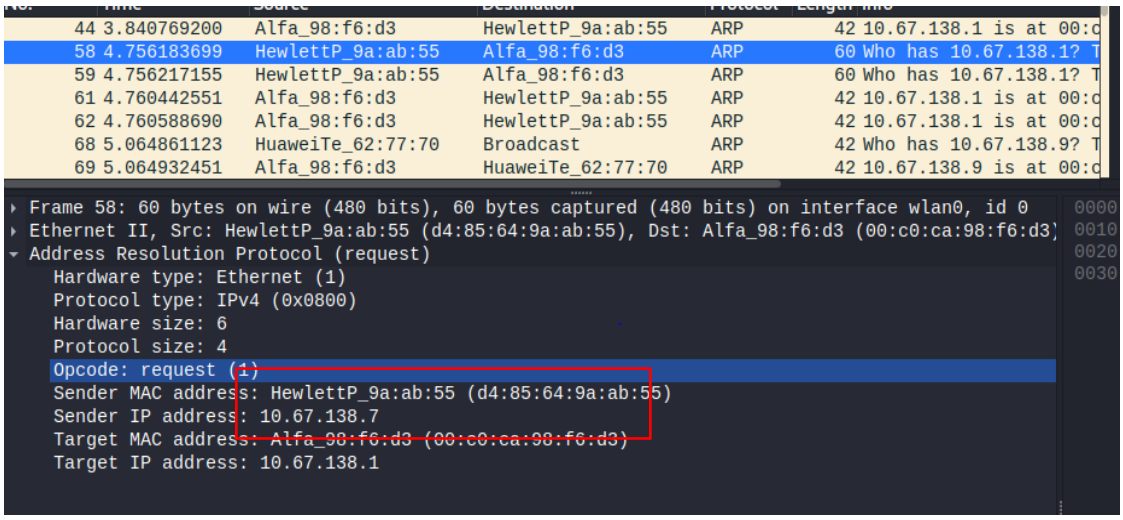


Figura 52: Dirección MAC atacante, adquirida por la puerta de enlace

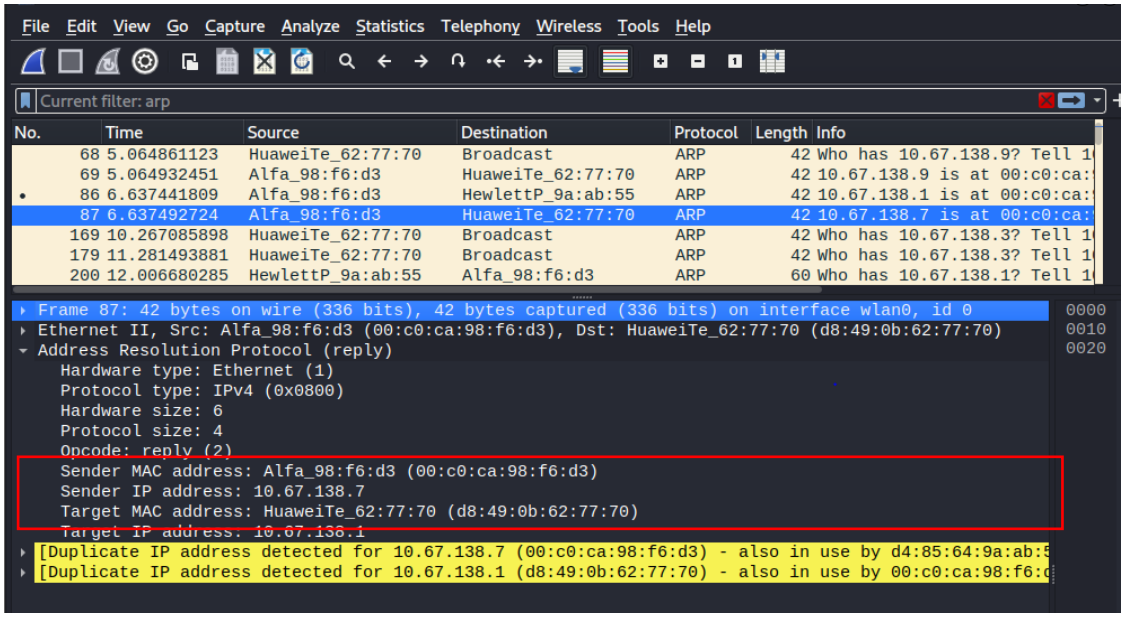


Figura 53: Dirección MAC atacante, adquirida por la victima

3.2.3 Resultado de los ataques

Para presentar los resultados de los ataques se optó en formato de tabla, para proporcionar una visión general completa y organizada de las pruebas realizadas. Este enfoque tabular permite una rápida asimilación de mensajes clave, destacando claramente el estado y los resultados de cada tipo de ataque. Además, ayuda a comparar diferentes ataques, proporcionando una vista estructurada para ayudar a identificar patrones y tendencias de seguridad en la red evaluada. Este formato proporciona una herramienta de visualización eficaz que simplifica la interpretación de los resultados y le ayuda a tomar decisiones informadas sobre las medidas de seguridad necesarias.

Tabla 11: Resultados de los ataques

Ataque	**Estado**	**Resultado**
Fuerza Bruta y diccionario	**No Exitoso**	• Se seleccionaron diccionarios preestablecidos y reconocidos, así como uno creado con palabras clave. • Se basó en la prueba de múltiples comparaciones con diccionarios con combinaciones de contraseñas hasta encontrar la de la institución. • Fue un proceso intensivo y requirió tiempo. • Su efectividad dependió en gran medida de la debilidad de la contraseña.
Evil Twin	**Exitoso**	• Implicó la creación de un AP falso para engañar a los usuarios. • Aprovecha la falta de autenticación adecuada y la divulgación de SSID. • Fue efectivo cuando los usuarios se conectaron automáticamente a redes conocidas.

Denegación de Servicios	**Exitoso**	• Se abrumo el sistema o red con tráfico, incapacitando sus servicios. • Se pudo ejecutar por una sola entidad con recursos limitados. • Destaca vulnerabilidades en la disponibilidad de servicios.
Man in the Middle	**Exitoso**	• Se logró la intercepción de la comunicación entre dos partes. • Fue utilizado para espionaje y robo de datos. • Se explotó vulnerabilidades en la autenticación y cifrado de la comunicación.

3.2.4 Identificación de Vulnerabilidades

Mediante la utilización de la metodología ISSAF con controles OWISAM durante el proceso de identificación de vulnerabilidades en la red inalámbrica, permitió explorar y evaluar la infraestructura de la red en busca de debilidades potenciales que podrían ser explotadas por personas malintencionadas. La Tabla 10 proporciona un resumen de las vulnerabilidades identificadas tanto de los ataques activos como los pasivos y una descripción detallada de cada elemento evaluado. Este proceso de identificación es esencial para fortalecer la red y garantizar la privacidad de los recursos conectados.

Tabla 12: Identificación de Vulnerabilidades

SubFase ISSAF	**Pruebas/ Controles OWISAM**	**Vulnerabilidades**
Recopilación de Información	Descubrimiento activo de dispositivos y redes.	Divulgación de información de la red wifi.
Escaneo	Identificación de funcionalidades soportadas por el dispositivo.	Obtención de datos de dispositivos de comunicación inalámbrica (hardware y software).

Auditoría	Pruebas sobre WPS.	Ingreso no autorizado a la red Wi-Fi. Funcionalidad activada de autenticación mediante el protocolo WPS.
	Interfaces administrativas expuestas a la red.	Entrada a la gestión de dispositivos mediante la puerta de enlace predeterminada.
	Prueba de AP/Router	Recopilación de información sobre los puertos, servicios y protocolos activos.
Análisis y Búsqueda	Verificación del grado de amplitud de señal o área de alcance.	Rango de cobertura limitado. Transmisión de señales de clientes no autorizados.
	Análisis protocolos de cifrado WEP, TKIP	Intervención en la comunicación. Adquisición de datos confidenciales.
Explotación y Ataques	Captura y cracking de claves transmitidas en el proceso de autenticación. Evil Twin	Autenticación de redes inalámbricas.
	Pruebas de desautenticación -DoS	Interrupción de servicios. Red inaccesible para un solo usuario o para todos los usuarios legítimos.
	Ataque Man in the middle	Intercepción y manipulación de la comunicación entre dispositivos.
	Fuerza Bruta	No implementación de medidas de seguridad, especialmente robustez en contraseñas.

c. Fase 3: Reportes, Limpieza y Destrucción de Artefactos

Esta etapa implica mostrar los resultados de las pruebas de penetración y las pruebas de seguridad basados en los controles OWISAN cabe recalcar que estas pruebas se encuentran detallados en el Anexo B. El informe resultante es significativo porque documenta las debilidades descubiertas, los métodos utilizados y las sugerencias para mejorar la seguridad de la red. Este informe no solo brinda información a los responsables del área TI, también proporciona sugerencias sobre cómo mitigar las debilidades identificadas en la infraestructura de red Institucional, ver Anexo C.

La limpieza y destrucción de artefactos se enfoca en garantizar que cualquier cambio o inserción realizada durante las pruebas sea revertida. Es fundamental para mantener la integridad del sistema y eliminar cualquier huella de las actividades de evaluación.

Las pruebas se realizan creando un entorno virtual que se eliminara después de enviar los archivos correctos sin guardar una copia en el disco. Si el docente encargado de TI de la Institución lo desea, el autor permite que la revisión se realice en su ordenador, con el objetivo de indicar que no existe información sobre la organización del mencionado entorno virtual.

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Se investigó las vulnerabilidades presentes en las redes inalámbricas, brindando una perspectiva sobre cómo ejecutar las pruebas éticas y seguras durante el desarrollo de esta investigación, reduciendo los posibles daños y maximizando la efectividad de los ataques.

- Se determinó que Aircrack-ng posee suites que lograron desautenticar usuarios y obtener el handshake de la red en poco tiempo, Ettercap intercepto credenciales como usuario y contraseña. Además, se duplico la red para capturar la clave de acceso utilizando Wifiphisher.

- Durante la realización de las pruebas de intrusión controladas en la infraestructura de red WiFi de la Unidad Educativa Pelileo, se proporcionaron resultados relevantes, evidenciando vulnerabilidades como ataques Evil Twin, DoS y Man in the middle.

- Al documentar las pruebas de intrusión realizadas, se logró verificar el éxito de los diferentes ataques con la información obtenida en cada uno de estos, como el cracking de contraseñas logrando el ingreso no permitido a la red e intercepción del tráfico http.

4.2 Recomendaciones

- Antes de ejecutar cualquier prueba de intrusión en las redes inalámbricas, se recomienda realizar una investigación de vulnerabilidades más recientes y prácticas de pentesting. La probabilidad de fallar o cometer errores durante el desarrollo de estas, puede reducirse en gran medida.

- Se recomienda utilizar herramientas como Ettercap, Wifiphisher o Wireshark que pueda realizar los diferentes tipos de ataques para obtener una evaluación más detallada de la red, garantizando la ejecución de pruebas de seguridad.

- Se recomienda tener una tarjeta de red con chipset compatible para realizar pruebas de penetración, de lo contrario no se podrá realizar ningún tipo de ataque y evaluar la seguridad o vulnerabilidades presentes en la red.

- Es importante proporcionar una documentación detallada de los resultados obtenidos durante la identificación de vulnerabilidades en la conexión inalámbrica, para registrar los hallazgos y también de manera efectiva las recomendaciones con el fin de mejorar la seguridad de la infraestructura Institucional.

REFERENCIAS BIBLIOGRÁFICAS

[1] I. González Pulido, «DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICAS PARA LA LUCHA CONTRA LA CIBERDELINCUENCIA GRAVE. ESPECIAL REFERENCIA A LA UTILIZACIÓN DEL REGISTRO REMOTO PARA LA INVESTIGACIÓN DE CIBERATAQUES CONTRA INFRAESTRUCTURAS CRÍTICAS Y ESTRATÉGICAS.», http://purl.org/dc/dcmitype/Text, Universidad de Salamanca, 2022. Accedido: 2 de junio de 2023. [En línea]. Disponible en: https://dialnet.unirioja.es/servlet/tesis?codigo=308643

[2] I. E. Briones Castro, «APLICACIÓN DE HACKING ÉTICO PARA LA DETERMINACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES EN LA RED DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ», bachelorThesis, Jipijapa.UNESUM, 2020. Accedido: 2 de junio de 2023. [En línea]. Disponible en: http://repositorio.unesum.edu.ec/handle/53000/2588

[3] W. S. Rodriguez Delgado, «ANÁLISIS DE VULNERABILIDADES DE LA RED INALÁMBRICA PARA MITIGAR LA INSEGURIDAD DE ATAQUE INFORMÁTICOS», bachelorThesis, Jipijapa-Unesum, 2023. Accedido: 2 de junio de 2023. [En línea]. Disponible en: http://repositorio.unesum.edu.ec/handle/53000/4798

[4] B. M. Macías Pico, «APLICACIÓN DE HACKING ÉTICO PARA LA DETERMINACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES EN LA RED WIFI DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ», bachelorThesis, Jipijapa.UNESUM, 2021. Accedido: 2 de junio de 2023. [En línea]. Disponible en: http://repositorio.unesum.edu.ec/handle/53000/3062

[5] L. Jaime Carrasco, «SOFTWARE LIBRE PARA MEJORAR LAS VULNERABILIDADES DE REDES INALÁMBRICAS EN LA SEGURIDAD DE INFORMACIÓN ULADECH», *Universidad Católica Los Ángeles de Chimbote*, ago. 2019, Accedido: 6 de junio de 2023. [En línea]. Disponible en: https://repositorio.uladech.edu.pe/handle/20.500.13032/13418

[6] D. A. Castillo Tumbaco, «IMPLEMENTACIÓN DE HACKING ÉTICO PARA LA EVALUACIÓN DE VULNERABILIDADES EN LA RED DE DATOS DE

UNA INSTITUCIÓN EDUCATIVA DE NIVEL PRIMARIO.», bachelorThesis, La Libertad: Universidad Estatal Península de Santa Elena, 2021, 2021. Accedido: 6 de junio de 2023. [En línea]. Disponible en: https://repositorio.upse.edu.ec/handle/46000/6486

[7] A. R. Garcia Vega y D. J. Morales Baren, «SEGURIDAD INFORMÁTICA MEDIANTE HACKING ÉTICO EN LA APLICACIÓN DE PENTESTING PARA EL ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE DATOS DE LA COOPERATIVA SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI.» Accedido: 6 de junio de 2023. [En línea]. Disponible en: http://repositorio.utc.edu.ec/handle/27000/8458

[8] J. A. Benítez Guamán, «Análisis de riesgo en redes wifi aplicando técnicas de hacking ético», bachelorThesis, Quito: Universidad de las Américas, 2019, 2019. Accedido: 28 de diciembre de 2023. [En línea]. Disponible en: http://dspace.udla.edu.ec/handle/33000/10769

[9] Tecnología para los negocios, «Hacking ético: qué es y para que sirve | TICNegocios». Accedido: 16 de mayo de 2023. [En línea]. Disponible en: https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-el-hacking-etico/

[10] A. E. R. Llerena, «Herramientas fundamentales para el hacking ético», [En línea]. Disponible en: https://www.medigraphic.com/cgi-bin/new/resumen.cgi?IDARTICULO=94154

[11] RedesZone, «Mejores escáner de vulnerabilidades gratis para hacker ético». Accedido: 20 de junio de 2023. [En línea]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/mejores-escaner-vulnerabilidades-gratis-hacker/

[12] J. Vasquez Perez, «UCM-Proyecto de Innovación Software libre para ciencias e ingenierías». Accedido: 31 de diciembre de 2023. [En línea]. Disponible en: https://www.ucm.es/pimcd2014-free-software/wireshark

[13] Estación Informática, «Estación Informática: airgeddon: Wireless Security». Accedido: 31 de diciembre de 2023. [En línea]. Disponible en: https://estacioninformatica.blogspot.com/2017/06/airgeddon-wireless-security.html

[14] J. JHL73, «Wifite2 Auditando Redes Inalámbricas», Medium. Accedido: 31 de diciembre de 2023. [En línea]. Disponible en: https://medium.com/@javierjhl73/wifite2-auditando-redes-inal%C3%A1mbricas-96e287aa8dc1

[15] ANTRAX, «Fern Wifi Cracker - Suite completa de auditoria Wireless», Underc0de. Accedido: 31 de diciembre de 2023. [En línea]. Disponible en: https://underc0de.org/foro/index.php?topic=40943.0

[16] Programador clic, «Uso de la herramienta ETTERCAP». Accedido: 31 de diciembre de 2023. [En línea]. Disponible en: https://programmerclick.com/article/90672272302/

[17] C. HN, «Herramienta genera ataque de phishing | Hostname.cl», Hosting Rápido con cPanel y certificado SSL en Chile | HN Datacenter. Accedido: 31 de diciembre de 2023. [En línea]. Disponible en: https://www.hn.cl/blog/herramienta-genera-ataques-de-phishing-para-obtener-claves-wifi/

[18] RedesZone, «Acrylic WiFi : Análisis de este monitor de redes inalámbricas Wi-Fi», RedesZone. Accedido: 12 de enero de 2024. [En línea]. Disponible en: https://www.redeszone.net/tutoriales/redes-wifi/acrylic-wifi/

[19] Cisco, «¿Qué es la seguridad de red?» Accedido: 16 de mayo de 2023. [En línea]. Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

[20] IBM, «¿Qué es la seguridad de red? | IBM». Accedido: 16 de mayo de 2023. [En línea]. Disponible en: https://www.ibm.com/es-es/topics/network-security

[21] UNIR Ecuador, «¿Qué es la Seguridad Informática?» Accedido: 16 de mayo de 2023. [En línea]. Disponible en: https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/

[22] Cibernos, «¿Qué es la seguridad informática y cómo implementarla?» Accedido: 16 de mayo de 2023. [En línea]. Disponible en: https://www.grupocibernos.com/blog/que-es-la-seguridad-informatica-y-como-implementarla

[23] Concepto, «Red - Concepto, tipos de red, topología y elementos», Concepto. Accedido: 20 de junio de 2023. [En línea]. Disponible en: https://concepto.de/red-2/

[24] Concepto, «Red Inalámbrica - Qué es, tipos, ventajas, desventajas y ejemplos». Accedido: 16 de mayo de 2023. [En línea]. Disponible en: https://concepto.de/red-inalambrica/

[25] ComputerWorld, «802.11: estándares de Wi-Fi y velocidades». Accedido: 20 de junio de 2023. [En línea]. Disponible en: https://www.computerworld.es/wifi/80211-estandares-de-wifi-y-velocidades

[26] D. Vargas, «Protocolo TCP: definición y funcionamiento», Tutoriales Hostinger. Accedido: 16 de mayo de 2023. [En línea]. Disponible en: https://www.hostinger.es/tutoriales/protocolo-tcp

[27] Google Docs, «Vulnerabilidades en las Redes Inalámbricas», Google Docs. Accedido: 16 de mayo de 2023. [En línea]. Disponible en: https://docs.google.com/document/u/0/d/1clGBBXA9Ygoj3uFF-0HeqnN4Vz-qqVnoA0FewAEMVM8/edit?hl=es&usp=embed_facebook

[28] T. Caycho Rodríguez, «Intervalos de Confianza para el coeficiente alfa de Cronbach: aportes a la investigación pediátrica». Accedido: 7 de febrero de 2024. [En línea]. Disponible en: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0186-23912017000400291

[29] G. F. Kuder y M. W. Richardson, «The theory of the estimation of test reliability», *Psychometrika*, vol. 2, n.º 3, pp. 151-160, sep. 1937, doi: 10.1007/BF02288391.

[30] C. Ortega Diaz, «Vulnerabilidades de las redes WiFi by Carlos Ortega Diaz - Issuu». Accedido: 3 de enero de 2024. [En línea]. Disponible en: https://issuu.com/losisams/docs/articulo-carlos_ortega-1993-14-2297

[31] I. D. M. Group, «Los ataques de fuerza bruta y de diccionario ponen las contraseñas en peligro | Seguridad», IT Reseller. Accedido: 7 de noviembre de 2023. [En línea]. Disponible en: https://www.itreseller.es/seguridad/2019/05/los-ataques-de-fuerza-bruta-y-de-diccionario-ponen-las-contrasenas-en-peligro

[32] Ciberseguridad.net, «Gemelo malvado (Evil Twin Hotspot)(Ataques Informáticos XI) - Ciberseguridad,seguridad informática,redes y programación.» Accedido: 7 de noviembre de 2023. [En línea]. Disponible en:

https://cyberseguridad.net/gemelo-malvado-evil-twin-hotspot-ataques-informaticos-xi

[33] IONOS Digital Guide, «Ataque man-in-the-middle (mitm attack)». Accedido: 7 de noviembre de 2023. [En línea]. Disponible en: https://www.ionos.es/digitalguide/servidores/seguridad/ataques-man-in-the-middle-un-vistazo-general/

[34] Cloudflare, «¿Qué es un ataque de denegación de servicio (DoS)?» Accedido: 7 de noviembre de 2023. [En línea]. Disponible en: https://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/

[35] RedesZone, «Cómo usar Aircrack-ng para hackear redes Wi-Fi WEP, WPA y WPA2». Accedido: 4 de noviembre de 2023. [En línea]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/aircrack-ng-hackear-redes-wifi/

[36] OpenWebinars.net, «Wireshark: Qué es y ejemplos de uso». Accedido: 4 de noviembre de 2023. [En línea]. Disponible en: https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/

[37] elhacker.NET, «bettercap: la navaja suiza del tráfico de red», Blog. Accedido: 27 de diciembre de 2023. [En línea]. Disponible en: https://blog.elhacker.net/2021/05/bettercap-la-navaja-suiza-del-trafico-analizar-red.html

[38] A. SANDOVAL, «Rastreando nuestra red con ettercap», MicroTeknologias. Accedido: 1 de febrero de 2024. [En línea]. Disponible en: https://microteknologias.wordpress.com/2009/01/22/rastreando-nuestra-red-con-ettercap/

[39] Zerolynx Cybersecurity, «Fern Wifi Cracker», Flu Project | Blog. Accedido: 7 de noviembre de 2023. [En línea]. Disponible en: https://www.flu-project.com/2015/06/fern-wifi-cracker.html

[40] S. D. Luz, «Wifiphisher v1.3 ya disponible: Conoce una de las mejores herramientas de auditorías Wi-Fi», RedesZone. Accedido: 31 de diciembre de 2023. [En línea]. Disponible en: https://www.redeszone.net/2017/05/24/wifiphisher-v1-3-ya-disponible-conoce-una-las-mejores-herramientas-auditorias-wi-fi/

[41] S. D. Luz, «Conoce Airgeddon, un programa para realizar auditorías Wi-Fi en Linux», RedesZone. Accedido: 6 de noviembre de 2023. [En línea]. Disponible

en: https://www.redeszone.net/2016/06/19/conoce-airgeddon-un-programa-para-realizar-auditorias-wi-fi-en-linux/

[42] J. C. Baudi, «WIFITE 2.1.0 – LA HERRAMIENTA PARA AUDITAR EL WIFI»: Accedido: 7 de noviembre de 2023. [En línea]. Disponible en: https://es.linkedin.com/pulse/wifite-210-la-herramienta-para-auditar-el-wifi-julio-c-baudi

[43] M. Beucher, «Nmap: Guía básica para escanear puertos + Listado de comandos», Ciberseguridad. Accedido: 8 de enero de 2024. [En línea]. Disponible en: https://ciberseguridadtips.com/nmap/

[44] Ciberseguridad, «¿Qué es Metasploit Framework y cómo funciona?» Accedido: 8 de enero de 2024. [En línea]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

[45] T. Research, «Acrylic wifi Analyzer - Analizador, Solución de problemas Windows», Acrylic WiFi. Accedido: 12 de enero de 2024. [En línea]. Disponible en: https://www.acrylicwifi.com/blog/analizador-wifi-windows-solucion-problemas/

[46] DragoN, «OSSTMM, Manual de la Metodología Abierta de Testeo de Seguridad - DragonJAR», DragonJAR - Servicios de Seguridad Informática. Accedido: 1 de febrero de 2024. [En línea]. Disponible en: https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

[47] Ctxdetectives, «Qué es el OWISAM | Seguridad en redes inalámbricas». Accedido: 7 de noviembre de 2023. [En línea]. Disponible en: https://www.ctxdetectives.com/que-es-el-owisam/

[48] FutureLearn, «Information System Security Assessment Framework (ISSAF)». Accedido: 7 de noviembre de 2023. [En línea]. Disponible en: https://www.futurelearn.com/info/blog

ANEXOS

Anexo A. Lista controles OWISAM

Controles OWISAM			
Sección	**Referencia**	**Control**	**Vulnerabilidad**
OWISAM Discovery (OWISAM-DI)	OWISAM-DI-001	Descubrimiento de puntos de acceso.	Existencia de rogue Aps.
	OWISAM-DI-002	Descubrimiento de redes ocultas.	debilidades en el firmware y seguridad por oscuridad.
	OWISAM-DI-003	Identificación pasiva de direcciones MAC de dispositivos.	Dispositivos no autorizados.
	OWISAM-DI-004	Descubrimiento de preferencias de redes conocidas de clientes.	Conexión automática a redes inseguras.
	OWISAM-DI-005	Descubrimiento activo de dispositivos y redes.	Descubrimiento de información.
	OWISAM-DI-006	Identificación de relaciones entre dispositivos.	Descubrimiento de información.
OWISAM Fingerprinting (OWISAM-FP)	OWISAM-FP-001	Identificación del dispositivo.	Obtención de información sobre el hardware y software.
	OWISAM-FP-002	Identificación de funcionalidades soportadas por el dispositivo.	Obtención de información sobre el hardware y software.

	OWISAM-FP-003	Enumeración de mecanismos de autenticación radius (802.1x)	Mecanismos de autenticación inseguros
	OWISAM-FP-004	Detección de Rogue APs	Intrusos en redes Wi-Fi.
	OWISAM-FP-005	Pruebas de client isolation	Ataques a clientes.
	OWISAM-FP-006	Detección de ataques por parte de dispositivos Wi-Fi.	Intrusos en redes Wi-Fi.
Pruebas sobre la autenticación (OWISAM-AU)	OWISAM-AU-001	Detección de protección de acceso basado en MAC.	Autenticación contra redes Wi-Fi.
	OWISAM-AU-002	Pruebas sobre WPS	Acceso no autorizado a redes Wi-Fi.
	OWISAM-AU-003	Pruebas de downgrade del método de autenticación	Inseguridad en mecanismos de autenticación.
	OWISAM-AU-004	Captura y cracking de claves transmitidas en el proceso de autenticación.	Credenciales débiles.
	OWISAM-AU-005	Uso de protocolos de autenticación inseguros (FAST-EAP,LEAP,EAP-MD5,...)	Interceptación y descifrado de credenciales.
	OWISAM-AU-006	Pruebas de fuerza bruta de usuarios contraseñas de radius (802.1x)	Credenciales débiles.
	OWISAM-AU-007	Pruebas de fuerza bruta de contraseñas contra el	Posibilidad de descifrar

		proceso de autenticación (PSK)	contraseñas débiles offline.
	OWISAM-AU-008	Debilidades en repositorio de credenciales	Acceso no autorizado y robo de credenciales.
Pruebas de cifrado de comunicaciones (OWISAM-CP)	OWISAM-CP-001	Captura y análisis de tráfico en red abierta.	Transmisión de información sensible.
	OWISAM-CP-002	Descifrado de trafico cifrado	Transmisión de información insegura.
	OWISAM-CP-003	Pruebas de análisis de información transmitida a través de Wireless	Obtención de información sensible.
	OWISAM-CP-004	Análisis de protocolos de cifrado inseguro (WEP, TKIP,...)	Debilidad de seguridad en la red.
	OWISAM-CP-005	Pruebas de renovación de claves de cifrado	Tiempo de vida de claves criptográficas elevado.
	OWISAM-CP-006	Pruebas de re-inyección de tráfico (replay attack, Mic,..)	Suplantación de identidad.
Pruebas de configuración de la plataforma (OWISAM-CF)	OWISAM-CF-001	Identificación de redes wireless con ESSID genérico.	Suplantación de identidad y ataques basados en memory trading.
	OWISAM-CF-002	Contraseñas genéricas en interfaz administrativa del	Credenciales débiles y acceso no

		punto de acceso	autorizado.
	OWISAM-CF-003	Verificación del nivel de intensidad de señal o área de cobertura.	área de cobertura excesiva.
	OWISAM-CF-004	Análisis del solapamiento de redes en el mismo canal de comunicaciones	Degradación de la calidad del servicio.
	OWISAM-CF-005	Generación de claves en base a algoritmos conocidos	Algoritmos de claves PSK o WPS débiles.
	OWISAM-CF-006	Pruebas sobre Upnp	Redirección de puertos.
Análisis de Infraestructura (OWISAM-IF)	OWISAM-IF-001	Debilidades en el firmware del AP.	Robo de credenciales y acceso no autorizado.
	OWISAM-IF-002	Interfaces administrativas expuestas a la red	Acceso no autorizado e interceptación de tráfico.
	OWISAM-IF-003	Política de firewall incorrecta	Acceso a segmentos de red restringidos.
	OWISAM-IF-004	Controles sobre mecanismos de detección de intrusos.	Ausencia de sistemas de monitorización.
	OWISAM-IF-005	Pruebas de verificación de túneles VPN (sobre redes abiertas...)	Interceptación de comunicaciones
	OWISAM-	Debilidades en servidor	Ejecución remota

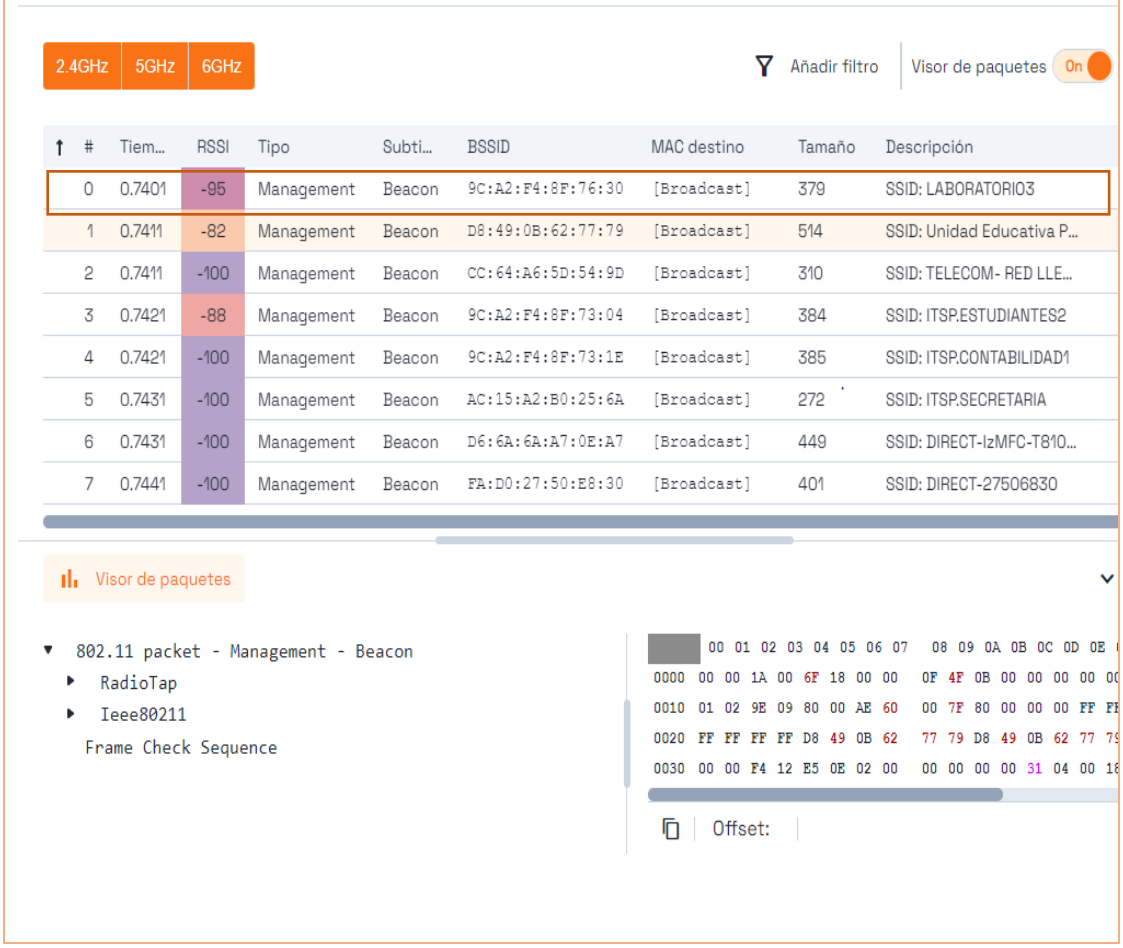
	IF-006	radius	de código o denegación de servicio.
	OWISAM-IF-007	Vulnerabilidades incubadas	Debilidades en elementos de arquitectura o software.
	OWISAM-IF-008	Gestión (Alta/baja/modificación) de claves y certificados.	Gestión incorrecta de claves de acceso.
	OWISAM-IF-009	Dispositivos de comunicaciones accesible/expuestos físicamente	Acceso no autorizado y modificación de firmware.
	OWISAM-IF-010	Detección y análisis de sistemas Scada.	Acceso a sistemas de control industrial.
Denegación de servicio (OWISAM-DS)	OWISAM-DS-001	Pruebas de deautenticación	Interceptación de credenciales de autenticación.
	OWISAM-DS-002	Saturación del canal de comunicaciones (CTS/RTS,ruido, jammering, ...)	Ataques a la disponibilidad del servicio.
	OWISAM-DS-003	Bloqueo de cuentas de usuario	Bloqueo de cuentas.
	OWISAM-DS-004	Bloqueo de dispositivo de comunicaciones	Suplantación de punto de acceso y DOS.
	OWISAM-DS-005	Pruebas de degradación del canal de comunicaciones	Degradación del servicio.

Pruebas sobre directivas y normativa (OWISAM-GD)	OWISAM-GD-001	Identificación de dispositivos que no cumplen el estándar / propietarios	n/a
	OWISAM-GD-002	Detección de dispositivos emitiendo en frecuencias restringidas.	Emisión de señal no autorizada.
	OWISAM-GD-003	Análisis de la política de uso/restricción de uso de redes inalámbricas	Accesos indebidos.
	OWISAM-GD-004	Análisis de la configuración de dispositivos.	Configuración incorrecta.
	OWISAM-GD-005	Análisis de la política de gestión y cambio de claves	Tiempo de vida de contraseñas elevado.
	OWISAM-GD-006	Verificación de inventario de dispositivos autorizados	Inventario no actualizado.
Pruebas sobre clientes inalámbricos (OWISAM-CT)	OWISAM-CT-001	Pruebas de Rogue Ap y asociación automática	Suplantación de identidad y robo de credenciales.
	OWISAM-CT-002	Analisis de APTs (Advanced Persistent Threats) sobre Wireless.	Existencia de ataques persistentes.
	OWISAM-CT-003	Desbordamiento de buffer en cliente.	Ausencia de parches de seguridad y ejecución remota de código.
	OWISAM-CT-004	Extracción de identificadores de usuarios	Recopilación de información y

		(802.1x)	configuración insegura.
	OWISAM-CT-005	Pruebas sobre suplicant débil o inseguro.	Ausencia de validación de certificados.
	OWISAM-CT-006	Ataques contra clientes	Modificación de respuestas DNS,..
	OWISAM-CT-007	Extracción de credenciales de los clientes	Suplantación de identidad.
Pruebas sobre Hotspots / portales cautivos (OWISAM-HS)	OWISAM-HS-001	Acceso a otros segmentos de red sin autenticación	Segmentación o política de cortafuegos incorrecta
	OWISAM-HS-002	Debilidades en el mecanismo de autenticación.	Acceso no autorizado.
	OWISAM-HS-003	Pruebas de encapsulación de tráfico con el exterior	Evasión del mecanismo de autenticación.
	OWISAM-HS-004	Debilidades en portal captivo	Acceso no autorizado.

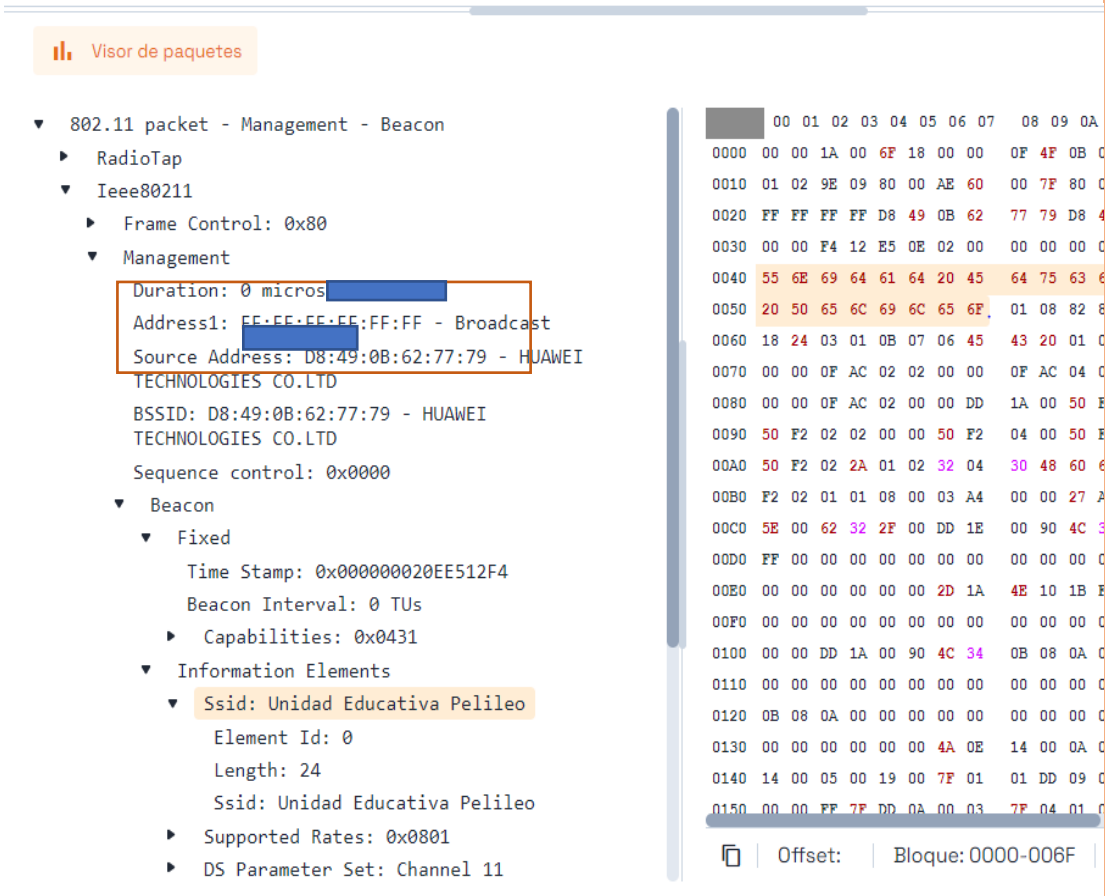
Anexo B. Subfase de la metodología ISSAF con pruebas de controles OWISAM

Prueba 1. Descubrimiento activo de dispositivos y redes
Proceso
Descubrir información de la red inalámbrica de la Institución.
Pre- requisitos
Instalar Acrylic Wifi Analyzer
Ejemplos/Resultados



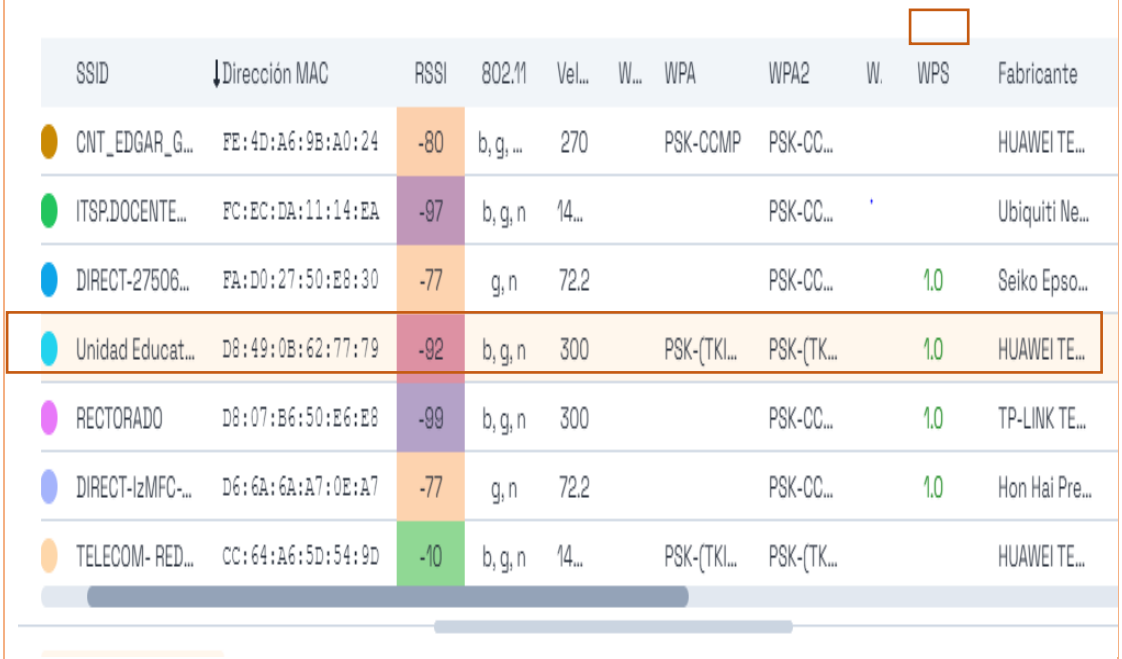
Análisis/ Conclusión/ Observación
Se encuentra habilitados los beacons frames para acceder a la red inalámbrica, lo que posibilita la obtención de información del software y hardware del dispositivo.
Contramedidas
Desactivar la transmisión de los "beacon frames" implica que la red inalámbrica no se anunciará automáticamente, lo que significa que los usuarios interesados deberán ingresar manualmente la información, como el nombre de la red (SSID), para encontrarla y conectarse.
Lecturas Adicionales
https://www.owisam.org/es/Descubrimiento_de_dispositivos_OWISAM-DI https://www.owisam.org/es/OWISAM-DI-005 https://www.owisam.org/es/OWISAM-DI-003
Observaciones
Subfase de Metodología ISSAF: Recolección de información. **Control OWISAM:** OWISAM Discovery. **Subcontrol OWISAM:** Descubrimiento activo de dispositivos y redes (OWISAM-DI-005).
Modo de ataque:
Pasivo

Prueba 2. Identificación de funcionalidades soportadas por el dispositivo.
Proceso
Conseguir detalles del dispositivo, tales como la información del fabricante, el controlador utilizado, la velocidad de transmisión, el tiempo de respuesta, entre otros, mediante Acrylic Wifi Analyzer en la sección de Paquetes
Pre- requisitos
Instalar Acrylic Wifi Analyzer
Ejemplos/Resultados



Análisis/ Conclusión/ Observación
Se logró adquirir datos tales como el fabricante, , el SSID, la dirección MAC, la encriptación, la autenticación entre otros.
Contramedidas
Es recomendable que las redes de comunicación inalámbrica utilicen nombres no indicativos de la organización y, en su lugar, opten por denominaciones genéricas con el fin de mitigar riesgos asociados a posibles ataques de suplantación de puntos de acceso.
Lecturas Adicionales
OWISAM: https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi/owisam/ https://auditoriawifi.es/controles-owisam/
Observaciones
Subfase de Metodología ISSAF: Escaneo. **Control OWISAM:** OWISAM Fingerprinting. **Subcontrol OWISAM:** Identificación de funcionalidades soportadas por el dispositivo (OWISAM-FP-002).
Modo de Ataque:
Pasivo.

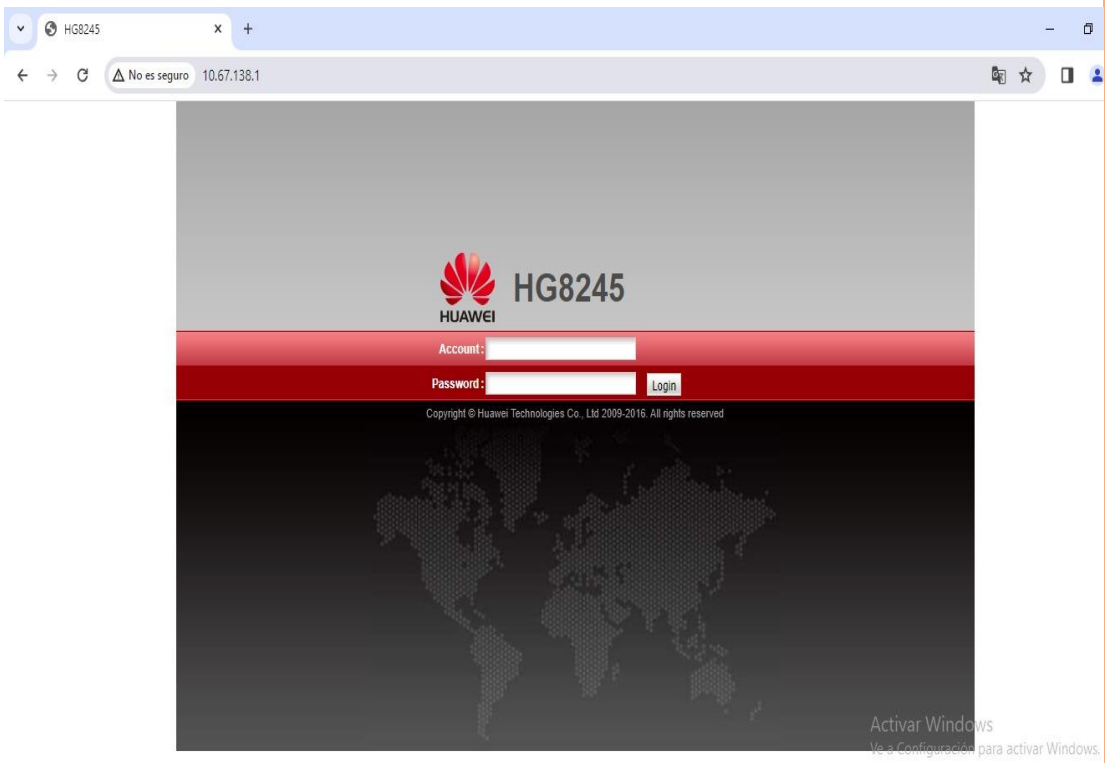
Prueba 3. Pruebas sobre WPS.
Proceso
Comprobar si los dispositivos cuentan con la función WPS habilitada.
Pre- requisitos
Instalar Acrylic Wifi Analyzer
Ejemplos/Resultados



SSID	Dirección MAC	RSSI	802.11	Vel...	W...	WPA	WPA2	W.	WPS	Fabricante
CNT_EDGAR_G...	FE:4D:A6:9B:A0:24	-80	b, g, ...	270		PSK-CCMP	PSK-CC...			HUAWEI TE...
ITSP.DOCENTE...	FC:EC:DA:11:14:EA	-97	b, g, n	14...			PSK-CC...			Ubiquiti Ne...
DIRECT-27506...	FA:D0:27:50:E8:30	-77	g, n	72.2			PSK-CC...		1.0	Seiko Epso...
Unidad Educat...	D8:49:0B:62:77:79	-92	b, g, n	300		PSK-(TKI...	PSK-(TK...		1.0	HUAWEI TE...
RECTORADO	D8:07:B6:50:E6:E8	-99	b, g, n	300			PSK-CC...		1.0	TP-LINK TE...
DIRECT-IzMFC-...	D6:6A:6A:A7:0E:A7	-77	g, n	72.2			PSK-CC...		1.0	Hon Hai Pre...
TELECOM- RED...	CC:64:A6:5D:54:9D	-10	b, g, n	14...		PSK-(TKI...	PSK-(TK...			HUAWEI TE...

Análisis/ Conclusión/ Observación
La red de la institución tiene habilitado el protocolo WPS

Contramedidas
Desactivar la funcionalidad de WPS en los dispositivos y enrutadores inalámbricos. Configurar WPA2 estableciendo un intervalo prudente para la renovación de claves.
Lecturas Adicionales
ISSAF: http://www.oissg.org/issaf.html **OWISAM:** https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi/owisam/ https://auditoriawifi.es/controles-owisam/
Observaciones
Subfase de Metodología ISSAF: Auditoria. **Control OWISAM:** Pruebas sobre la autenticación. **Subcontrol OWISAM:** Pruebas sobre WPS (OWISAM-AU-002).
Modo de Ataque:
Pasivo.

Prueba 4. Interfaces accesibles desde la red.
Proceso
Determinar el procedimiento de acceso a la administración del dispositivo inalámbrico en la Institución. Esta Prueba se realizó después de ejecutar los ataques activos para conocer el Gateway de la red.
Pre- requisitos
Navegador Web
Ejemplos/Resultados


Análisis/ Conclusión/ Observación
Se verificó que el acceso a la administración del dispositivo inalámbrico está habilitado, lo que lo vuelve vulnerable a posibles accesos no autorizados por parte de un atacante.
Contramedidas
Desactivar el acceso a la administración del dispositivo inalámbrico cuando no sea esencial, o implementar medidas de seguridad adicionales, como autenticación multifactor y restricciones de direcciones IP autorizadas, para mitigar el riesgo de accesos no autorizados.
Lecturas Adicionales
ISSAF: http://www.oissg.org/issaf.html **OWISAM:** https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi/owisam/ https://auditoriawifi.es/controles-owisam/
Observaciones
Subfase de Metodología ISSAF: Auditoria Control OWISAM: Análisis de Infraestructura. Subcontrol OWISAM: Interfaces administrativas expuestas a la red (OWISAM-IF-002).
Modo Ataque
Pasivo

Prueba 5. Prueba de APs/Router

Proceso

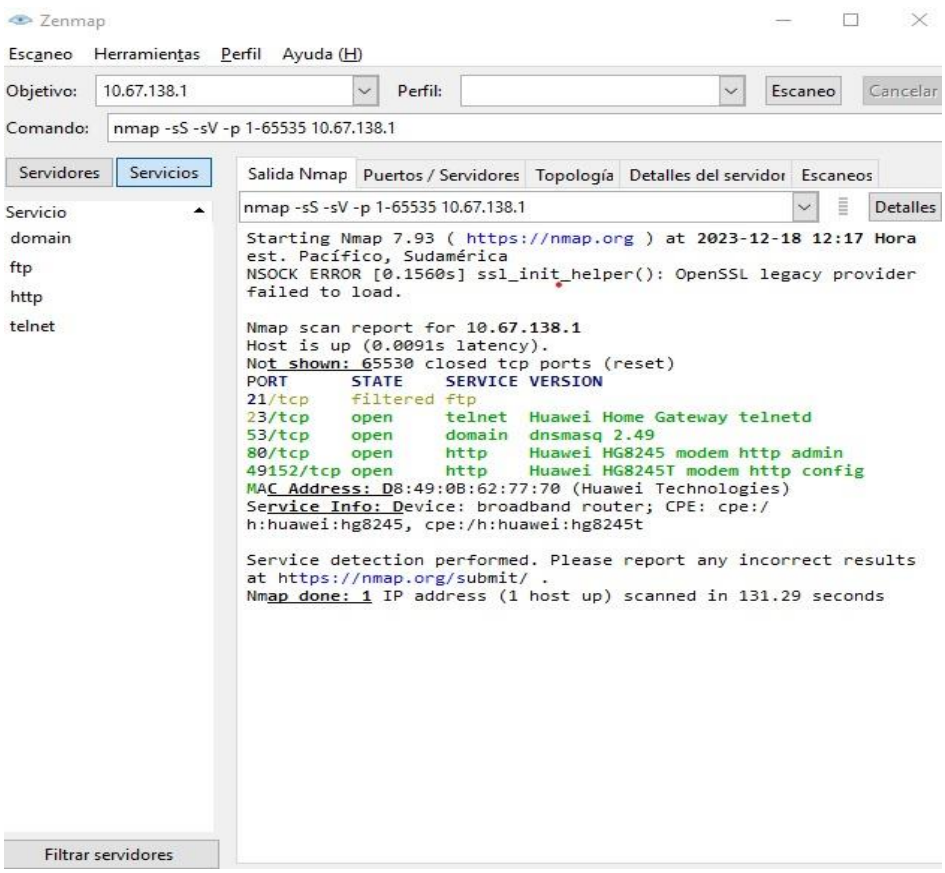
Identificar los puertos, protocolos y servicios de enrutamiento que estén abiertos.

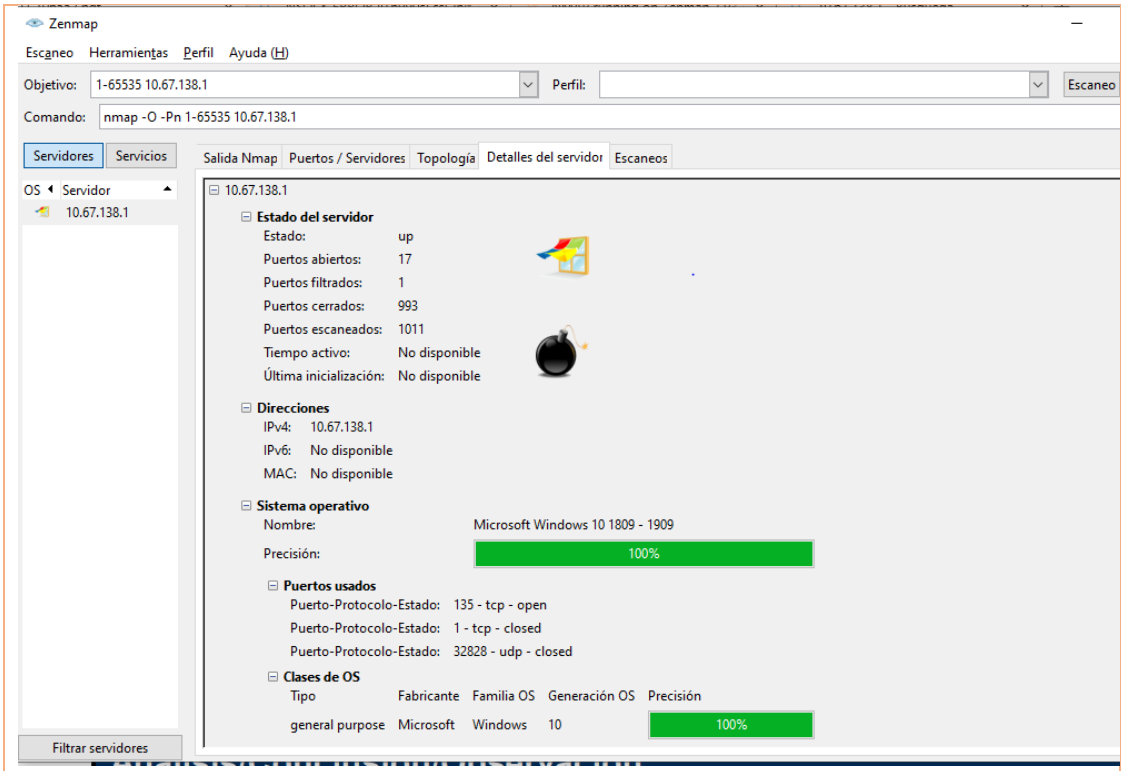
Esta Prueba se realizó después de ejecutar los ataques activos para conocer el Gateway de la red.

Pre- requisitos

Instalar Zenmap.

Ejemplos/Resultados





Análisis/ Conclusión/ Observación

"Not shown: 65530 closed protocols" señala que 65530 puertos están cerrados, reflejando una práctica cautelosa en este aspecto.

El puerto 23 está abierto, pero se especifica que la administración del dispositivo inalámbrico se realiza a través de la web y no a través de este puerto.

Contramedidas

Modificar los valores predeterminados de configuración en los dispositivos inalámbricos.

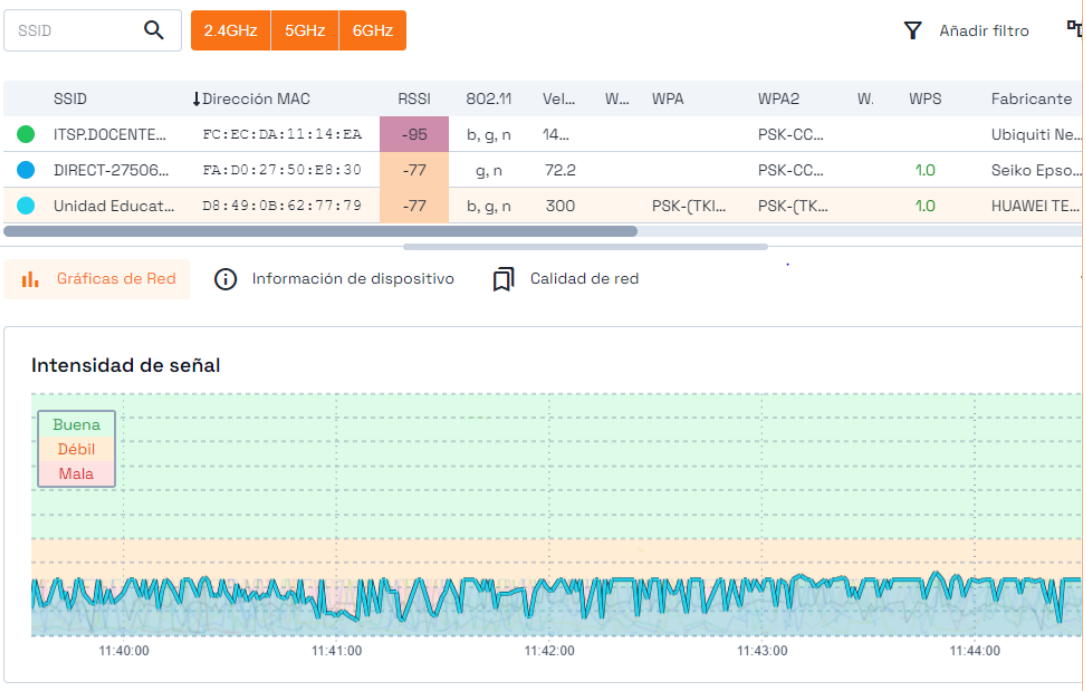
Lecturas Adicionales

ISSAF:

http://www.oissg.org/issaf.html

Observaciones
Subfase de Metodología ISSAF: Auditoria.
Modo de Ataque:
Pasivo

Prueba 6. Verificación del grado de amplitud de señal o área de alcance.
Proceso
Determinar si la cobertura de la red se extiende o no dentro de los límites de la institución según los niveles de potencia.
Pre- requisitos
Revisar Controles OWISAM
Ejemplos/Resultados



Análisis/ Conclusión/ Observación

Se pudo verificar el nivel de la señal; existen redes inalámbricas vecinas configuradas y que trabajan en el mismo área de cobertura de señal.

Contramedidas

Ajustar y optimizar la configuración de la potencia de la red inalámbrica para que se alinee de manera precisa con los límites físicos de la institución. Además, se podría considerar la implementación de tecnologías como VLANs y firewalls para reforzar la segmentación de la red.

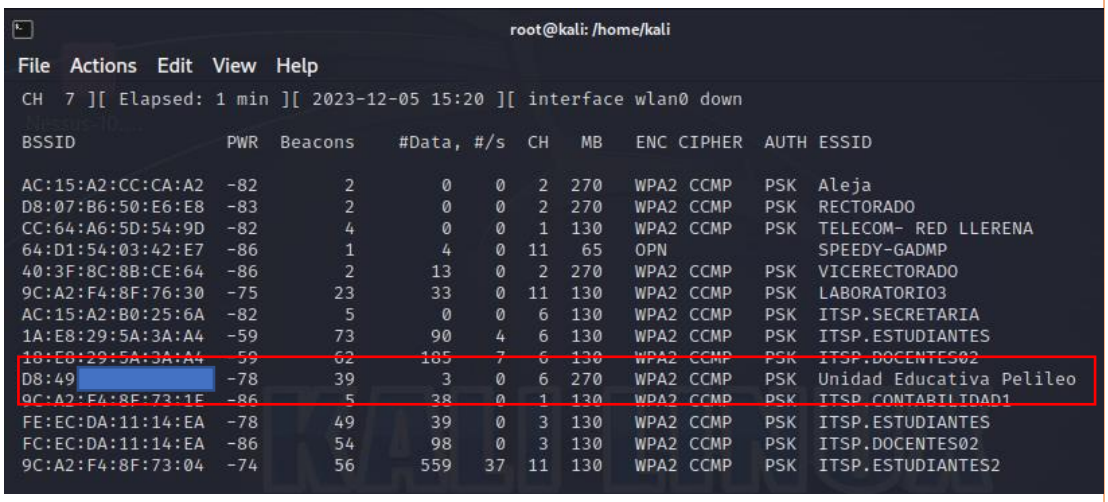
Lecturas Adicionales

OWISAM:

https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx
https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifiowisam/
https://auditoriawifi.es/controles-owisam/

Observaciones
Subfase de Metodología ISSAF: Análisis y Búsqueda. **Control OWISAM:** Pruebas de configuración de la plataforma. **Subcontrol OWISAM:** Verificación del nivel de intensidad de señal o área de cobertura (OWISAM-CF-003).
Modo de Ataque:
Pasivo

Prueba 7. Análisis protocolos de cifrado WEP, TKIP
Proceso
Evaluar los protocolos de cifrado (WEP, TKIP) y comprobar las posibles vulnerabilidades de seguridad en la red.
Pre- requisitos
Instalar el Sistema Operativo Kali Linux, utilizar la suite Aircrack.
Ejemplos/Resultados



Análisis/ Conclusión/ Observación

Se observó que los dispositivos inalámbricos están establecidos con la configuración de WPA PSK-TKIP.

Lecturas Adicionales

OWISAM:https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx
https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifiowisam/
https://auditoriawifi.es/controles-owisam/

Observaciones

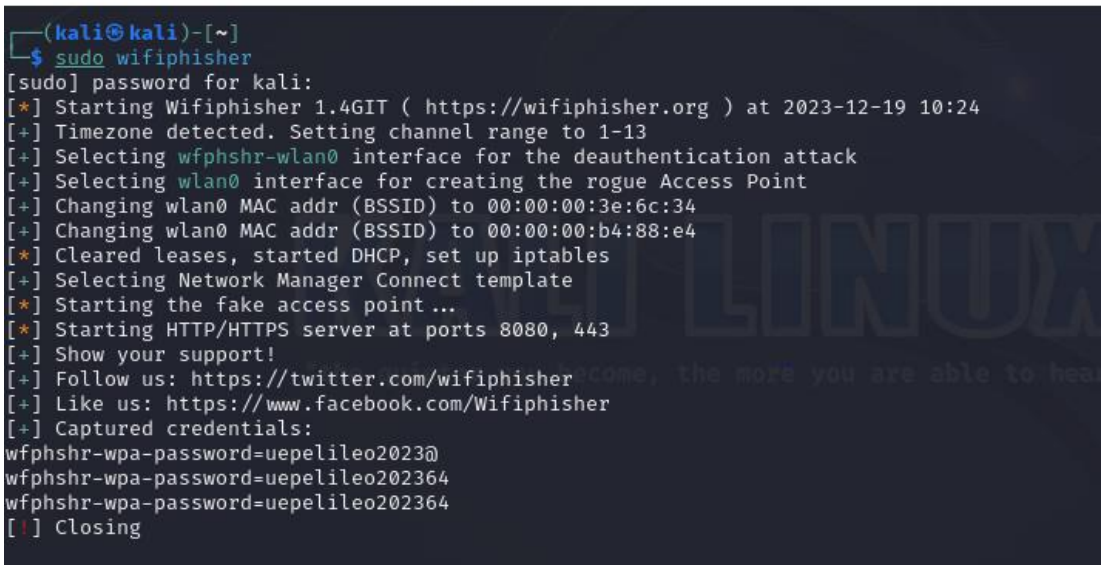
Subfase de Metodología ISSAF: Auditoria.

Control OWISAM: Pruebas sobre directivas y normativa.

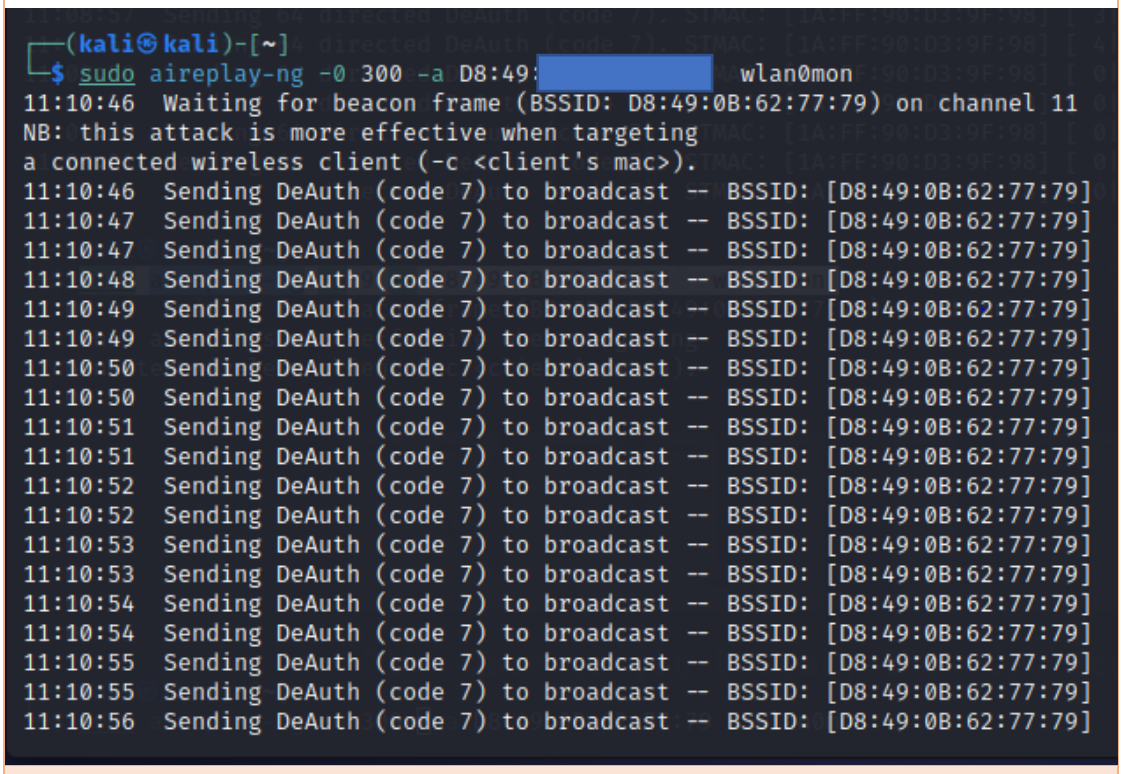
Subcontrol OWISAM: Análisis de la configuración de dispositivos (OWISAM-GD-004).

Modo de Ataque:

Pasivo

Prueba 8. Captura y cracking de claves transmitidas en el proceso de autenticación
Proceso
Comprobar la captura de contraseñas transmitidas durante el proceso de autenticación en la red Wi-Fi.
Pre- requisitos
Instalar el SO Kali Linux, wifiphisher
Ejemplos/Resultados

Análisis/ Conclusión/ Observación
Se logró obtener credenciales en el proceso de autenticación de la red inalámbrica

Contramedidas
Adoptar protocolos de cifrado fuertes como WPA3, implementar autenticación de dos factores y mantener una vigilancia constante mediante monitoreo de red
Lecturas Adicionales
OWISAM: https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifiowisam/ https://auditoriawifi.es/controles-owisam/
Observaciones
Subfase de Metodología ISSAF: Explotación y Ataque. **Control OWISAM:** Pruebas sobre la autenticación. **Subcontrol OWISAM:** Captura y cracking de claves transmitidas en el proceso de autenticación (OWISAM-AU-004). **Modo de Ataque:** Activo.
Modo de Ataque:
Activo

Prueba 9. Pruebas de deautenticación
Proceso
Cortar la conexión de los usuarios, impidiendo el acceso a los servicios en la red inalámbrica.
Pre- requisitos
Instalar el SO Kali Linux, Aircrack.-ng suite
Ejemplos/Resultados

Análisis/ Conclusión/ Observación
Se llevó a cabo la des autenticación del servicio de Internet para un único usuario, requiriéndole así que se vuelva a conectar a la red.

Contramedidas
Se recomienda implementar sistemas de detección de intrusos, filtrar tráfico anómalo y fortalecer métodos de autenticación
Lecturas Adicionales
OWISAM: https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifiowisam/ https://auditoriawifi.es/controles-owisam/
Observaciones
Subfase de Metodología ISSAF: Explotación y Ataque. **Control OWISAM:** Denegación de servicio. **Subcontrol OWISAM:** Pruebas de deautenticación (OWISAM-DS-001).
Modo de Ataque:
Activo

Anexo C. Informe de Vulnerabilidades identificadas con pruebas de intrusión en la red de la Institución

UNIVERSIDAD TECNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS, ELECTRONICA E INDUSTRIAL

CARRERA DE TECNOLOGIAS DE LA INFORMACION

HACKING ÉTICO PARA LA DETECCIÓN DE VULNERABILIDADES MEDIANTE LA UTILIZACIÓN DE HERRAMIENTAS OPEN SOURCE EN LA RED INALÁMBRICA DE LA UNIDAD EDUCATIVA PELILEO

Realizado por:	Shirley Núñez	**Nombre del Documento :**	Obtención de contraseñas

Objetivo:

Determinar si la red es vulnerable para el cracking de contraseñas para la evaluación de seguridad de la red

Técnica:

La técnica fue el ataque de fuerza bruta y diccionario

Herramientas tecnológicas aplicadas:

Kali Linux, Aircrack-ng.

Tiempo de ejecución:

Se empleó tres horas y 23 minutos para este ataque, ya que se hizo una comparación con el diccionario rockyou con más de 14 millones de las contraseñas que se puede encontrar.

Resultados Obtenidos:

La red posee una contraseña basada en los estándares propuestos por lo que no se pudo obtener la clave.

Recomendaciones:

- Imponer políticas de contraseñas robustas.
- Implementar autenticación de dos factores para aumentar la seguridad.

UNIVERSIDAD TECNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS, ELECTRONICA E INDUSTRIAL

CARRERA DE TECNOLOGIAS DE LA INFORMACION

HACKING ÉTICO PARA LA DETECCIÓN DE VULNERABILIDADES MEDIANTE LA UTILIZACIÓN DE HERRAMIENTAS OPEN SOURCE EN LA RED INALÁMBRICA DE LA UNIDAD EDUCATIVA PELILEO

Realizado por:	Shirley Núñez	**Nombre del Documento:**	Autenticación de la red Inalámbrica

Objetivo:

Determinar si la red es vulnerable ante Ingeniería Social para evaluar la seguridad de red

Técnica:

La técnica fue el ataque de Evil Twin o portal cautivo

Herramientas tecnológicas aplicadas:

Kali Linux, wifiphisher.

Tiempo de ejecución:

Se empleó 1 hora para este ataque, debido a la intermitencia de la red y el tiempo en que los usuarios se conectaban para poder capturar información.

Resultados Obtenidos:

Se logró obtener las credenciales de la red, al engañar a los usuarios con un portal cautivo similar al de la red.

Recomendaciones:

- Implementar estándares de seguridad robustos como WPA3 en lugar de WPA o WEP.
- Utilizar autenticación de dos factores para el acceso a la red.

UNIVERSIDAD TECNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS, ELECTRONICA E INDUSTRIAL

CARRERA DE TECNOLOGIAS DE LA INFORMACION

HACKING ÉTICO PARA LA DETECCIÓN DE VULNERABILIDADES MEDIANTE LA UTILIZACIÓN DE HERRAMIENTAS OPEN SOURCE EN LA RED INALÁMBRICA DE LA UNIDAD EDUCATIVA PELILEO

Realizado por:	Shirley Núñez	**Nombre del Documento:**	Interrupción de servicio

Objetivo:

Evaluar la vulnerabilidad de la red frente a interrupciones de servicios y sobrecarga, con el propósito de analizar la capacidad de la red para resistir ataques que busquen interrumpir su funcionamiento normal

Técnica:

La técnica fue el ataque de DoS

Herramientas tecnológicas aplicadas:

Kali Linux, Aircrack-ng

Tiempo de ejecución:

Se empleó 20 minutos para este ataque, al enviar 200 mensajes se esperó que se procese los mismo para seguir enviando más tráfico de red.

Resultados Obtenidos:

Se logró des autenticar a toda la red, así como a un solo usuario de la misma.

Recomendaciones:

- Implementar firewalls y sistemas de detección de intrusiones para filtrar el tráfico malicioso.
- Utilizar servicios de mitigación de DDoS para manejar grandes volúmenes de tráfico.
- Configurar reglas y límites de conexión para prevenir conexiones excesivas desde una única fuente.

UNIVERSIDAD TECNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS, ELECTRONICA E INDUSTRIAL

CARRERA DE TECNOLOGIAS DE LA INFORMACION

HACKING ÉTICO PARA LA DETECCIÓN DE VULNERABILIDADES MEDIANTE LA UTILIZACIÓN DE HERRAMIENTAS OPEN SOURCE EN LA RED INALÁMBRICA DE LA UNIDAD EDUCATIVA PELILEO

Realizado por:	Shirley Núñez	**Nombre del Documento:**	Captura de tráfico de datos

Objetivo:

Evaluar la vulnerabilidad de la red mediante un análisis de sniffing para la evaluación de susceptibilidad de la información transmitida.

Técnica:

La técnica fue el ataque Man-in-the-Middle

Herramientas tecnológicas aplicadas:

Kali Linux, Aircrack-ng, Ettercap

Tiempo de ejecución:

Se empleó dos horas para este ataque, debido a la intermitencia de la red.

Resultados Obtenidos:

Se logró obtener credenciales de un login que se generó con el trafico http

Recomendaciones:

- Utilizar conexiones seguras mediante el cifrado de datos. HTTPS para sitios web y VPNs para conexiones de red.
- Establecer protocolos seguros como WPA3 para redes Wi-Fi.