PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

TRABAJO DE TITULACIÓN

Tema: ANÁLISIS DE VULNERABILIDADES DE UNA RED INALÁMBRICA EN LA UNIDAD EDUCATIVA LICEO JOSÉ ORTEGA Y GASSET

AUTOR:

ENRIQUE AUGUSTO LUZURIAGA TEJADA

QUITO DM, 2024

DEDIDACTORIA

Este trabajo es dedicado a toda mi familia. En especial a mis padres que me fueron de apoyo para afrontar los momentos difíciles y a mi hermana que con sus ocurrencias me regalaba la energía y determinación para seguir adelante.

AGRADECIMIENTO

Agradezco en primer lugar a mis padres que con su apoyo y cariño incondicional me han enseñado a ser la persona quién soy hoy a afrontar cualquier adversidad con la frente en alto para poder alcanzar mis metas.

Agradezco también a la universidad y a sus docentes por brindarme todos los recursos necesarios para alcanzar mis metas tanto profesionales como personales.

Por último, agradecer a mis compañeros que me han acompañado por este largo camino, gracias por tantas horas compartidas y momentos inolvidables.

RESUMEN

El presente proyecto de titulación tiene como objetivo evaluar las vulnerabilidades de la red inalámbrica de la institución educativa Liceo José Ortega y Gasset mediante la implementación de ataques de penetración controlados. El trabajo tiene como foco principal el identificar y analizar las principales deficiencias de la infraestructura de la red inalámbrica con el fin del plantear medidas de mejora para garantizar la confidencialidad, integridad y disponibilidad de la información.

Se realizó un análisis detallado de la arquitectura de la red para planear de forma cuidadosa los ataques controlados que se ejecutarían mediante herramientas open source como Nmap, Bettercap y Wireshark en un entorno Kali Linux. El plan se basó en la metodología de pruebas de penetración PTES y se ejecutó cada fase rigurosamente, documentando cada aspecto importante para garantizar que el proceso de evaluación sea completo.

Por último, se plantearon recomendaciones específicas enfocadas en mejorar la seguridad de la red inalámbrica, mitigar los riesgos identificados y fortalecer las defensas cibernéticas contra amenazas futuras. El proyecto realizado además de enfatizar la importancia de la seguridad de la red en un entorno educativo también proporciona un modelo práctico y detallado para evaluar la seguridad de redes inalámbricas.

Tabla de contenidos

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1: INTRODUCCIÓN

1.1 Tema

Análisis de vulnerabilidades de una red inalámbrica en la Unidad Educativa Liceo José Ortega Y Gasset

1.2 Justificación

En la actual era digital, la seguridad cibernética es de vital importancia para cualquier organización, incluidas las instituciones educativas. Los ataques cibernéticos y las vulnerabilidades en las redes inalámbricas pueden tener consecuencias graves, como la filtración de datos confidenciales y la interrupción de las operaciones académicas.

Por esta razón, evaluar y mejorar la seguridad de la red inalámbrica es esencial para proteger la privacidad y los datos sensibles de todas las partes interesadas. La evaluación de seguridad y las recomendaciones de mejora son procesos continuos que junto con este trabajo establecerán una base para futuras mejoras en la seguridad de la red inalámbrica de la institución, lo que garantizará una protección continua contra amenazas cibernéticas.

1.3 Planteamiento del problema

La creciente dependencia de la conectividad inalámbrica para actividades académicas y administrativas expone a las instituciones educativas a una serie de amenazas y vulnerabilidades. A pesar de los esfuerzos por implementar medidas de seguridad, existe una falta de comprensión completa de la efectividad de las protecciones existentes y de la presencia de posibles vulnerabilidades en la red inalámbrica de estas instituciones.

En este sentido, la institución educativa Liceo José Ortega y Gasset no ha realizado ninguna evaluación de seguridad de su red inalámbrica. Por lo tanto, a menos que se evalúe la red inalámbrica, podrían existir vulnerabilidades no detectadas que los posibles atacantes podrían explotar. Dichas debilidades pueden permitir un acceso no autorizado a la red, lo que compromete los datos críticos del sistema y genera interrupciones en las operaciones académicas y administrativas. Por otra parte, la red inalámbrica no segura aumenta el riesgo de exposición no autorizada de información privada y sensible, incluida la información, los registros estudiantiles y los datos financieros. Al final, esto puede resultar en violaciones de la privacidad, robo de identidad y responsabilidad legal y financiera para la escuela.

1.4 Objetivos

1.4.1 Objetivo General

Evaluar la vulnerabilidad de la red inalámbrica de la institución educativa Liceo José Ortega y Gasset mediante la implementación de un ataque de Hombre en el Medio.

1.4.2 Objetivos Específicos

1.4.2.1 Fundamentar teóricamente los tipos de redes, protocolos, y estándares de seguridad en Redes Inalámbricas

1.4.2.3 Analizar la arquitectura de red, hardware y software asociado de la institución educativa Liceo José Ortega y Gasset.

1.4.2.3 Diseñar un ataque controlado a la Red Inalámbrica del Liceo José Ortega y Gasset.

1.4.2.4 Implementar un ataque de Hombre en el Medio (MITM) en la red inalámbrica utilizando herramientas open source.

1.4.2.5 Evaluar el tráfico de red comprometido durante el ataque de MITM utilizando la herramienta WireShark.

1.5 Alcance

Este proyecto se centrará en realizar un análisis detallado del entorno de red de la institución educativa Liceo José Ortega y Gasset, incluyendo la topología de la red, los dispositivos conectados y la infraestructura de red inalámbrica.

Con este enfoque, se investigará y diseñará un plan detallado para llevar a cabo un ataque de Hombre en el Medio controlado en la red inalámbrica de la institución. Esto incluirá una selección de herramientas de software open source y técnicas específicas para implementar el ataque.

Además, se llevará a cabo el ataque de Hombre en el Medio de acuerdo con el plan desarrollado, con el objetivo de interceptar y manipular el tráfico de red inalámbrica de manera controlada y ética. Con los datos obtenidos durante el ataque, se realizará un análisis de resultados para identificar vulnerabilidades, debilidades y áreas de mejora en la seguridad de la red inalámbrica de la institución. Esto puede incluir la identificación de dispositivos vulnerables, datos sensibles expuestos y posibles puntos de entrada para ataques maliciosos.

Finalmente, se preparará un informe detallado que documente el proceso de evaluación de vulnerabilidad, los resultados del ataque de MITM, las recomendaciones de seguridad y cualquier otra información relevante que será presentada de manera clara y comprensible a las partes interesadas relevantes de la institución, incluyendo al administrador de TI y la gerencia de la institución educativa.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2.1 Redes Inalámbricas

Las redes inalámbricas son redes que utilizan tecnologías de comunicación inalámbrica para conectar dispositivos y transmitir datos sin necesidad de conexiones físicas por cable. En lugar de utilizar cables, las redes inalámbricas se basan en las llamadas señales de radiofrecuencia (RF) o luz infrarroja para transmitir datos entre dispositivos.

Entre algunos de los beneficios que ofrecen las redes inalámbricas están:

- ✓ **Movilidad:** Las redes inalámbricas permiten a los usuarios conectarse a Internet y acceder a los recursos de la red desde cualquier lugar dentro del área de cobertura (Pérez 2022). Los usuarios pueden moverse de forma libre sin estar limitados por cables físicos, lo que permite una mayor flexibilidad y comodidad.
- ✓ **Rentabilidad:** Ikusi (2023) menciona que las redes inalámbricas pueden ser más rentables que redes cableadas especialmente en situaciones donde la aplicación de cables resulta impráctica. Además, los costos de mantenimiento e instalación suelen ser más bajos para infraestructuras inalámbricas comparadas con alternativas cableadas.
- ✓ **Facilidad de despliegue:** La instalación de redes inalámbricas suele ser más rápida y sencilla que la de redes cableadas. No es necesario pasar cables por paredes o techos, lo que simplifica el proceso de despliegue y reduce el tiempo de instalación.

2.2 LAN

Una LAN, o Red de Área Local, es una red que abarca un área geográfica pequeña, normalmente confinada a un único edificio, oficina, campus o grupo de edificios cercanos (Hwang, 2021). Las LAN están diseñadas para facilitar la comunicación y el intercambio de datos entre dispositivos y recursos dentro del área local, permitiendo a los usuarios colaborar, compartir archivos y acceder a servicios compartidos como impresoras y conexión a Internet.

Las redes de área local permiten la conexión, transmisión y entrega de información entre los dispositivos conectados, los beneficios que ofrecen las LAN incluyen:

- ✓ Escalabilidad
- ✓ Manejo centralizado
- ✓ Velocidad de transmisión de datos
- ✓ Compartición de recursos
- ✓ Eficiencia de costos

- ✓ Seguridad

En este sentido, las LAN desempeñan un papel crucial a la hora de facilitar la comunicación, la colaboración y el uso compartido de recursos en organizaciones y comunidades. Sirven de base para diversas aplicaciones y servicios en red, como el correo electrónico, el intercambio de archivos, las videoconferencias, la VoIP (Voz sobre Protocolo de Internet) y la computación en nube.

2.3 WLAN

IEEE 802.11, conocido comúnmente como Wi-Fi, es una familia de estándares de redes inalámbricas desarrollada por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). IONOS (2023) señala que las normas 802.11 definen las especificaciones de las redes de área local inalámbricas (WLAN) y proporcionan directrices para la comunicación inalámbrica entre dispositivos como ordenadores, smartphones, tabletas, impresoras y otros dispositivos conectados en red (p. 1). La evolución de los estándares WLAN 802.11 han llevado a mejoras en velocidad, rango, confiabilidad y seguridad, ampliando la adopción de Wi-Fi para distintas aplicaciones, incluyendo el acceso a internet, streaming, voz sobre IP (VoIP) y conectividad IoT.

Los puntos clave para entender los estándares WLAN 802.11 son:

- ✓ **Bandas de frecuencia:** WLAN 802.11 opera en las bandas de frecuencia de 2,4 GHz y 5 GHz, ofreciendo diferentes canales y opciones de ancho de banda para la comunicación inalámbrica. La banda de 2,4 GHz proporciona una cobertura más amplia, pero puede sufrir más interferencias, mientras que la banda de 5 GHz ofrece mayores velocidades y menos congestión.
- ✓ **Calidad de servicio (QoS):** Los mecanismos de QoS de los estándares 802.11 dan prioridad a determinados tipos de tráfico (por ejemplo, voz o vídeo) para garantizar una entrega fiable y puntual de los datos, especialmente en entornos con una elevada congestión de la red.

2.4 WAN

Trueba (2022) define a las WAN o redes de área extensa como una red que se extiende por una amplia zona geográfica y suele abarcar varias ciudades, regiones, países o incluso continentes (p. 3). A diferencia de las LAN (redes de área local), que están confinadas a una

única ubicación, las WAN conectan lugares geográficamente dispersos y proporcionan comunicación y conectividad a larga distancia entre usuarios, dispositivos y recursos.

Las WAN cubren una amplia zona geográfica, permitiendo la comunicación y la conectividad entre ubicaciones remotas separadas por grandes distancias. Pueden abarcar países enteros, continentes o regiones globales, proporcionando conectividad entre sucursales, centros de datos, sitios remotos y usuarios móviles (AWS, 2022). Además, interconectan LAN y otras redes a través de largas distancias, lo que permite una comunicación fluida y el intercambio de datos entre usuarios y dispositivos ubicados en diferentes lugares.

2.5 Protocolos de seguridad inalámbrica

Las redes inalámbricas son vulnerables a varias amenazas a la seguridad, como las escuchas, el acceso no autorizado y la interceptación de datos. Por esta razón, entender el funcionamiento de estos protocolos y conocer las alternativas más seguras es fundamental para erigir barreras sólidas de defensa y proteger la confidencialidad de nuestros datos.

2.5.1 Wi-Fi Protected Access (WPA/WPA2/WPA3)

No es posible hablar de protocolos de seguridad inalámbrica, sin antes mencionar a WPA y sus sucesores, WPA2 y WPA3 son protocolos de seguridad diseñados para proteger las redes inalámbricas. Estos, utilizan métodos de cifrado como el Protocolo de Integridad de Clave Temporal (TKIP) y el Estándar de Cifrado Avanzado (AES) para cifrar los datos transmitidos por la red (NordVPN, 2023). WPA3, la última versión y ofrece funciones de seguridad mejoradas, como un cifrado más potente y protección contra ataques de fuerza bruta.

2.5.2 Wi-Fi Protected Setup (WPS)

WPS es un protocolo que simplifica el proceso de conexión de dispositivos a una red WiFi segura. En forma general, consiste en pulsar un botón del router o introducir un código PIN para establecer una conexión segura. Sin embargo, WPS ha sido criticado por sus vulnerabilidades de seguridad y suele estar desactivado en los routers Wi-Fi modernos.

2.5.3 Wireless Intrusion Prevention Systems (WIPS)

Las soluciones WIPS están diseñadas de manera específica para detectar y prevenir las amenazas a la seguridad en las redes inalámbricas. Cisco (2015) añade que utilizan técnicas como la inspección de paquetes, el análisis del espectro y la detección de puntos de acceso no autorizados para identificar y mitigar posibles riesgos para la seguridad.

2.5.4 Virtual Private Networks (VPNs)

Las VPN crean túneles cifrados a través de redes públicas, como Internet, para transmitir datos de forma segura entre usuarios remotos y redes corporativas. Proporcionan una capa adicional de seguridad para las comunicaciones inalámbricas al cifrar el tráfico de datos y protegerlo de interceptaciones o escuchas (Ramírez, 2023).

2.6 Ciberseguridad

La Seguridad Informática o Ciberseguridad puede ser definida de varias formas, IBM (2022) define a la Ciberseguridad como el conjunto de prácticas dedicadas para proteger sistemas de computación, redes, programas y cualquier dato de ataques digitales (p 1). Estos ataques pueden venir de varias formas, incluyendo malware, phishing, ataques MITM, virus, etc. El objetivo de la ciberseguridad es asegurar la confidencialidad, integridad y disponibilidad de la información a través de la implementación de medidas de seguridad como firewalls, software antivirus, encriptación de datos, controles de acceso y evaluaciones periódicas de la seguridad. La ciberseguridad es esencial en el mundo interconectado de hoy para salvaguardar la información de información sensible y prevenir el acceso no autorizado o disrupción de los activos digitales.

2.6.1 Ciberataques

Fortinet (2021) define un ciberataque como una acción diseñada para apuntar a una computadora o a cualquier elemento de un sistema de información computarizado para cambiar, destruir o robar datos, así como explotar o dañar una red (p.1). En este sentido, La ciberseguridad abarca una amplia gama de ataques y amenazas dirigidos contra los sistemas informáticos, las redes y los datos.

2.6.1.1 Malware

El malware es software malicioso diseñado para interrumpir, dañar u obtener acceso no autorizado a sistemas o datos informáticos (Kaspersky, 2022). Los tipos de malware incluyen virus, gusanos, troyanos, ransomware, spyware y adware.

2.6.1.2 Phishing

Los ataques de phishing consisten en engañar a los usuarios para que revelen información confidencial, como nombres de usuario, contraseñas, números de tarjetas de crédito u otros datos personales, haciéndose pasar por una entidad de confianza a través del correo electrónico, mensajes de texto u otros canales de comunicación.

2.6.1.3 DoS y DDoS

Los ataques DoS y DDoS tienen como objetivo interrumpir el funcionamiento normal de un sistema informático, red o sitio web abrumándolo con una avalancha de tráfico o peticiones, dejándolo indisponible para los usuarios legítimos (Fortinet, 2021). En general, aunque tanto los ataques DoS como los DDoS tienen como objetivo interrumpir la disponibilidad de los sistemas o redes objetivo, los ataques DDoS son más sofisticados e impactantes debido a su naturaleza distribuida, coordinación a gran escala y uso de bots.

2.6.1.4 Inyección SQL

Los ataques de inyección SQL se dirigen a aplicaciones web explotando vulnerabilidades en la capa de base de datos de la aplicación. Yasar (2023) menciona que los atacantes inyectan consultas SQL maliciosas en los campos de entrada, aprovechando las consultas inseguras a la base de datos para obtener acceso no autorizado a los datos o ejecutar comandos arbitrarios (p.4).

2.6.1.5 Ransomware

El ransomware es un tipo de malware que cifra archivos o bloquea sistemas informáticos, exigiendo un pago (por lo general en criptomoneda) a la víctima a cambio de claves de descifrado o de restaurar el acceso a los datos o sistemas afectados.

2.6.1.6 Ingeniería social

Los ataques de ingeniería social manipulan a las personas para que realicen acciones o divulguen información confidencial a través de la manipulación psicológica, el engaño o la suplantación de identidad. Los atacantes explotan las vulnerabilidades humanas para obtener acceso no autorizado a sistemas o información sensible.

2.6.1.7 Ataques de Hombre en el Medio (MitM)

El presente proyecto de titulación se desarrollará en base a un ataque de Hombre en el Medio, por lo que es importante entender en qué consiste. Un ataque Man-in-the-Middle (MitM) es un tipo de ciberataque en el que un atacante intercepta altera las comunicaciones entre dos partes sin su conocimiento o consentimiento (Fernández, 2023). El atacante se sitúa entre las dos partes que se comunican, lo que le permite espiar la comunicación, robar información confidencial o manipular los datos que se transmiten.

En general, los ataques de MitM se dividen en las siguientes fases:

1. Interceptación: El atacante accede al canal de comunicación entre las dos partes. Esto podría implicar interceptar el tráfico de red a través de redes WiFi no seguras, comprometer routers o switches, o explotar vulnerabilidades en los protocolos de comunicación.

2. Suplantación: El atacante se hace pasar por una o ambas partes comunicantes, haciendo que parezca que se comunican directamente entre sí.

3. Espionaje: El atacante escucha la comunicación entre las partes, capturando información sensible como nombres de usuario, contraseñas, números de tarjetas de crédito u otros datos confidenciales.

4. Manipulación de datos: En algunos casos, el atacante puede alterar los datos que se transmiten entre las partes. Por ejemplo, podría modificar el contenido de un correo electrónico, inyectar código malicioso en una página web o redirigir a los usuarios a un sitio web falso diseñado para robar sus credenciales.

Por otro lado, los ataques MITM pueden dirigirse a varios canales de comunicación, entre los que se incluyen:

- **Comunicación de red:** Interceptación de datos transmitidos a través de redes WiFi no seguras o infraestructuras de red comprometidas.
- **Comunicación segura:** Puede aprovechar las vulnerabilidades encontradas en protocolos de cifrado y certificados digitales para descifrar o falsificar conexiones seguras, como HTTPS.
- **Correo electrónico:** Al interceptar la comunicación por correo electrónico entre el remitente y el destinatario, el atacante logra acceder a información sensible o inyectar contenido malicioso.
- **VoIP (Voz sobre Protocolo de Internet):** Interceptar la comunicación de voz a través de Internet, pudiendo escuchar conversaciones o inyectar audio malicioso.

Los ataques MITM plantean graves amenazas a la confidencialidad, integridad y privacidad de las comunicaciones. Rudra (2022) expresa que “para mitigar el riesgo de ataques MITM, es esencial utilizar el cifrado, implementar protocolos de comunicación seguros, actualizar de forma regular el software y el firmware, y educar a los usuarios sobre los riesgos de las redes y canales de comunicación inseguros” (p.7). Además, el despliegue de sistemas de supervisión

de redes y detección de intrusos puede ayudar a detectar y prevenir los ataques MITM en tiempo real.

2.6.2 Tipos de atacantes

En el ámbito de la ciberseguridad, los atacantes pueden clasificarse en varios tipos en función de sus motivaciones, métodos y objetivos. Algunos tipos comunes de atacantes son:

- **Ciberdelincuentes:** Los ciberdelincuentes son individuos o grupos que se dedican a actividades de piratería informática con fines lucrativos.
- **Script Kiddies:** Sánchez (2018) define los "script kiddies" como individuos con conocimientos técnicos limitados que utilizan herramientas de hacking o scripts prefabricados para lanzar ataques sin tener una idea completa de cómo funcionan (p.3).
- **Hacktivistas:** Los hacktivistas son individuos o grupos que utilizan técnicas de pirateo para promover causas políticas o sociales.
- **Advanced Persistent Threats (APT):** Las APT son ciberamenazas sofisticadas y persistentes orquestadas por grupos bien financiados y organizados con la intención de infiltrarse y mantener el acceso a largo plazo a redes o sistemas objetivo.
- **Cracker:** Comúnmente confundidos con hackers, son los expertos en informática que tienen objetivos ilegales como dañar activos tecnológicos de empresas, robar credenciales, robar contraseñas, etc.
- **Hacker:** El término más común para referirse a un atacante informático, es un término que ha evolucionado con el tiempo y puede referirse a individuos con una amplia gama de habilidades, motivaciones y consideraciones éticas.

2.6.2.1 Hackers de sombrero blanco

También conocidos como hackers éticos, los hackers de sombrero blanco utilizan sus conocimientos técnicos para identificar y abordar vulnerabilidades de seguridad en sistemas informáticos, redes y software (Payo, 2023). Trabajan con organizaciones para realizar pruebas de penetración, auditorías de seguridad y evaluaciones de vulnerabilidades para mejorar las defensas de ciberseguridad y protegerse frente a ataques maliciosos.

2.6.2.2 Hackers de sombrero gris

Los hackers de sombrero gris actúan a medio camino entre los hackers de sombrero blanco y los de sombrero negro. Pueden descubrir vulnerabilidades de seguridad sin autorización, pero

por lo general no las explotan con fines maliciosos. Los hackers de sombrero gris pueden revelar vulnerabilidades a las partes afectadas, venderlas en el mercado negro o utilizarlas en beneficio propio sin causar daños significativos.

2.6.2.3 Hackers de sombrero negro

Los hackers de sombrero negro son individuos que se dedican a actividades de piratería informática con fines maliciosos, beneficio personal o actividades delictivas. Pueden explotar vulnerabilidades de seguridad para robar datos, cometer fraude, interrumpir servicios o causar daños a sistemas y redes informáticos.

2.7 Sistemas operativos utilizados en ciberseguridad

2.7.1 Parrot Security OS

Parrot Security OS es una distribución Linux basada en Debian adaptada a los profesionales de la ciberseguridad, que ofrece una amplia gama de herramientas y utilidades de seguridad para pruebas de penetración, evaluación de vulnerabilidades, análisis forense digital y protección de la privacidad (Altube, 2021). Es un sistema operativo que presenta un entorno de escritorio ligero y personalizable e incluye herramientas como Metasploit, Wireshark, Nmap y Burp Suite.

2.7.2 Ubuntu

Ubuntu es una popular distribución de Linux conocida por su interfaz fácil de usar, su estabilidad y sus amplios repositorios de software. Hixec (2023) señala que, aunque no está diseñado de manera específica para la ciberseguridad, los profesionales de la seguridad suelen utilizar Ubuntu como plataforma versátil para ejecutar herramientas de seguridad, realizar investigaciones de seguridad y desarrollar soluciones de seguridad personalizadas (p. 1).

2.7.3 Windows con PowerShell

Aunque las distribuciones Linux predominan en la ciberseguridad, Windows sigue siendo ampliamente utilizado en muchos entornos empresariales. Los sistemas operativos Windows, en particular las ediciones Windows Server, se utilizan a menudo para operaciones de seguridad, supervisión de redes y respuesta a incidentes. PowerShell, el lenguaje de scripting y la interfaz de línea de comandos de Microsoft, por otro lado, es muy utilizado por los profesionales de la ciberseguridad para automatizar tareas, gestionar sistemas y llevar a cabo operaciones de seguridad (GR, 2024).

2.7.4 Kali Linux

Kali Linux es una popular distribución de Linux ampliamente utilizada por profesionales de la ciberseguridad, hackers éticos, auditores informáticos y pentesters para diversas tareas relacionadas con la seguridad, incluida la evaluación de vulnerabilidades, pruebas de penetración, análisis forense digital e investigación de seguridad. Singh (2023) se refiere a Kali Linux como la distribución de Linux basada en Debian diseñada para análisis forenses digitales, pruebas de penetración y auditorías de seguridad (p. 3). Este viene preinstalado con una amplia gama de herramientas y utilidades diseñadas para el hacking ético y las pruebas de ciberseguridad, algunos de sus características clave son:

- ✓ **Open Source**: Kali Linux es un sistema operativo de código abierto, lo que significa que su código fuente está disponible de forma libre para que cualquiera pueda verlo, modificarlo y distribuirlo bajo los términos de las licencias open source.
- ✓ **Personalización:** Kali Linux permite a los usuarios personalizar su instalación seleccionando paquetes o herramientas específicas durante el proceso de instalación.
- ✓ **Herramientas de seguridad:** Kali Linux viene preinstalado con una amplia colección de herramientas de seguridad y utilidades para llevar a cabo pruebas de penetración, evaluación de vulnerabilidades, análisis de redes, análisis forense digital e investigación de seguridad.

2.8 Herramientas más usadas para ciberseguridad

Durante la realización de pruebas de penetración o hacking es importante la automatización de tareas, ya que podría haber miles de condiciones, que si se probaran de forma manual resultaría en un proceso largo y complicado, así que, para aumentar la eficiencia de tiempo, se hace uso de herramientas que vienen preinstaladas con Kali Linux. Estas herramientas no sólo ahorran tiempo, sino que también capturan datos precisos y obtienen resultados específicos (Lee, 2022). En este sentido, algunas de las más usadas o más populares son:

- ➢ **Wireshark:** popular analizador de protocolos de red que permite a los usuarios capturar y analizar el tráfico de red en tiempo real.
- ➢ **Nmap:** versátil herramienta de escaneo de red utilizada para descubrir hosts y servicios en una red, identificar puertos abiertos y realizar varias tareas de reconocimiento de red.

- **Hydra:** popular herramienta de descifrado de contraseñas utilizada para realizar ataques de fuerza bruta contra varios protocolos de red, incluidos SSH, FTP, Telnet, HTTP y otros.
- **Aircrack-ng:** conjunto de herramientas para evaluar y explotar la seguridad de las redes WiFi.
- **Metasploit:** Este es un potente marco para desarrollar, probar y ejecutar exploits contra sistemas vulnerables.
- **John the Ripper:** herramienta de descifrado de contraseñas rápida y versátil que se utiliza para recuperar contraseñas de varios tipos de archivos cifrados y hashes.
- **Bettercap:** potente y flexible framework de ataque y monitorización de redes diseñado para pruebas de penetración y evaluaciones de seguridad. Proporciona una amplia gama de características y capacidades para el reconocimiento de la red, ataques man-in-the-middle, manipulación de paquetes, sniffing de credenciales, y mucho más.
- **Nessus:** escáner de vulnerabilidades que se utiliza para identificar y gestionar vulnerabilidades de seguridad en diversos entornos informáticos, incluidos sistemas operativos, dispositivos de red e infraestructuras en la nube (Awati, 2023). Además, proporciona funciones de análisis completas para detectar fallos de software, parches faltantes y configuraciones incorrectas, garantizando una protección actualizada frente a las amenazas más recientes.

2.9 Pentesting

Las pruebas de penetración, a menudo abreviadas como "pentesting", son una práctica de ciberseguridad en la que profesionales de seguridad autorizados simulan ciberataques contra sistemas informáticos, redes o aplicaciones para identificar y explotar vulnerabilidades de seguridad (Hernández, 2022). El objetivo de las pruebas de penetración es evaluar la situación de seguridad de la infraestructura, las aplicaciones y las defensas de una organización y ofrecer recomendaciones para mejorar la seguridad y mitigar los riesgos.

2.9.1 Fases de un pentesting

Las pruebas de penetración suelen seguir un enfoque sistemático, que incluye los siguientes pasos:

- **Reconocimiento:** Durante el reconocimiento, el pentester recopila información sobre la organización objetivo, su infraestructura y los posibles vectores de ataque.

- **Análisis de vulnerabilidades:** En esta fase, el probador de penetración identifica y evalúa las vulnerabilidades de seguridad en los sistemas o aplicaciones objetivo.
- **Explotación:** La explotación implica intentar aprovechar las vulnerabilidades identificadas para obtener acceso no autorizado a los sistemas objetivo o a información sensible.
- **Post Explotación**: Después de obtener el acceso inicial a los sistemas objetivo, los expertos en pruebas de penetración realizan actividades de post-explotación para mantener el acceso, escalar privilegios y recopilar información o datos adicionales.

2.9.2 Modalidades de pentesting

Nowak (2022) menciona que las pruebas de penetración (pentesting) pueden realizarse utilizando diversas modalidades o enfoques, en función de los requisitos, objetivos y limitaciones específicos del encargo (p. 3). Algunas modalidades comunes de pruebas de penetración son:

- **Pruebas de caja negra:** En las pruebas de caja negra, también conocidas como pruebas externas, la persona que realiza las pruebas de penetración tiene un conocimiento limitado de los sistemas o aplicaciones objetivo y simula un ataque de un actor externo sin conocimiento interno.
- **Pruebas de caja blanca:** En las pruebas de caja blanca la persona que realiza las pruebas de penetración tiene un conocimiento completo de los sistemas objetivo, incluidos los diagramas de red, el código fuente y las configuraciones del sistema.
- **Pruebas de caja gris:** Las pruebas de caja gris combinan elementos de los enfoques de pruebas de caja negra y de caja blanca. En las pruebas de caja gris, el probador de penetración tiene un conocimiento parcial de los sistemas objetivo, como las direcciones de red, los privilegios de usuario o la arquitectura del sistema, pero carece de información detallada sobre el funcionamiento interno de los sistemas.

2.9.3 Metodologías más comunes para pentesting

Cuando se trata de hacking ético o pruebas de penetración, existen varias metodologías y marcos guían el proceso de identificar y explotar de forma sistemática las vulnerabilidades en sistemas informáticos, redes y aplicaciones.

2.9.3.1 OWASP

La Guía de Pruebas OWASP es un recurso muy utilizado para comprobar las vulnerabilidades de seguridad de las aplicaciones web. García (2022) señala que “proporciona

una metodología para identificar y probar fallos de seguridad comunes en aplicaciones web, incluidos ataques de inyección, autenticación rota, exposición de datos sensibles y más" (p. 2). Además, incluye instrucciones detalladas, listas de comprobación y técnicas de prueba para cada categoría de vulnerabilidad.

2.9.3.2 OSSTMM (Open Source Security Testing Methodology Manual)

OSSTMM es un marco completo para pruebas de seguridad desarrollado por el Instituto de Seguridad y Metodologías Abiertas (ISECOM). Ofrece un enfoque estructurado de las pruebas de seguridad, que abarca ámbitos como la gestión de la seguridad de la información, la seguridad operativa y las pruebas técnicas de seguridad (Guevara, 2020). OSSTMM hace hincapié en la importancia de probar los controles de seguridad, medir los riesgos de seguridad y evaluar la eficacia de las contramedidas de seguridad.

2.9.3.3 PTES (Penetration Testing Execution Standard)

PTES es un estándar completo para realizar pruebas de penetración y evaluaciones de seguridad. Desarrollado por el Grupo de Trabajo del Estándar de Ejecución de Pruebas de Penetración (PTES, por sus siglas en inglés), proporciona un enfoque estructurado y estandarizado para las pruebas de penetración, cubriendo áreas como las actividades previas, la recopilación de inteligencia, el análisis de vulnerabilidades, la explotación, la post-explotación y la elaboración de informes. Vienažindytė (2020) expresa que el objetivo de PTES es garantizar la coherencia, la calidad y la profesionalidad de las pruebas de penetración (p. 1).

CAPÍTULO III: METODOLOGÍA

3.1 Metodología de investigación

El presente proyecto de titulación utilizará un enfoque de investigación mixto, ya que integra elementos cualitativos y cuantitativos para obtener una comprensión más completa de la situación de la red inalámbrica de la institución. Este enfoque permitió explorar a través de una entrevista al encargado de Tecnologías, los conocimientos, percepciones y desafíos relacionados con la seguridad de la red inalámbrica, así como recopilar datos técnicos y prácticos sobre las vulnerabilidades de la red mediante pruebas de penetración.

Además, se revisó y analizó investigaciones previas, al igual que proyectos y tesis académicas relacionadas con el tema de seguridad de redes inalámbricas en instituciones educativas. La revisión de estos trabajos proporcionó un contexto teórico y práctico para la investigación realizada en este proyecto, así como un punto de referencia para comparar y contrastar los hallazgos de este estudio y establecer nuevas direcciones para investigaciones futuras.

Asimismo, se respetaron los principios éticos en todas las etapas de la investigación, garantizando el consentimiento informado de los participantes, la confidencialidad de los datos y el manejo responsable de la información sensible.

3.2 Instrumentos y Técnicas de Recolección de Datos

En esta sección, se consultaron diversas fuentes de información, incluyendo revistas especializadas, conferencias académicas, libros y repositorios de tesis electrónicas. Se prestó especial atención a los trabajos y tesis que abordaban temas relacionados con la evaluación de la seguridad de redes inalámbricas, pruebas de penetración, herramientas de seguridad de redes y prácticas de hacking ético en entornos educativos.

Por otro lado, se utilizaron herramientas especializadas de seguridad de redes dentro del sistema operativo Kali Linux como Wireshark, para analizar el tráfico de red comprometido durante el ataque de Hombre en el Medio. Los datos técnicos recolectados durante estas pruebas se registraron y analizaron para identificar vulnerabilidades y evaluar la seguridad de la red.

3.3 Metodología de desarrollo del proyecto

Para llevar a cabo la evaluación de la seguridad de la red inalámbrica en la institución educativa Liceo José Ortega y Gasset, se optó por utilizar la metodología PTES como marco de referencia. Esta metodología proporcionó una estructura clara y directrices sobre cómo planificar y llevar a cabo cada fase de la evaluación de la seguridad. Además, PTES es respaldado por la comunidad de seguridad cibernética y es un estándar de la industria en lo que respecta a la realización de pruebas de penetración.

Cómo ya se mencionó en el capítulo de marco teórico, la metodología PTES proporciona una guía detallada para la ejecución de pruebas de penetración, dividida en siete fases principales:

1. Interacción previa
2. Recopilación de información
3. Modelado de amenazas
4. Análisis de vulnerabilidades
5. Explotación
6. Post-Explotación
7. Reporte

En este sentido, en los próximos capítulos se detalló cómo se siguió de forma rigurosa la metodología PTES en todas las etapas del proyecto. Esto incluyó la identificación de objetivos de prueba, la recopilación de información sobre la red y sus sistemas, la evaluación de amenazas y riesgos potenciales, la ejecución de pruebas de penetración utilizando herramientas especializadas, el análisis de resultados y la elaboración de informes detallados que documentan los hallazgos y proporcionan recomendaciones para la mejora de la seguridad de la red.

CAPÍTULO IV: PROPUESTA

4.1 Requerimientos

Antes de comenzar con el desarrollo de la propuesta, se solicitó y se obtuvo el permiso necesario de las autoridades respectivas de la institución, mismo que se encuentra en el apartado de anexos (Véase anexo 1). Esto garantizó que todas las actividades del proyecto se realizaran conforme a las normativas y políticas internas de la institución, asegurando el apoyo y la colaboración necesarios para llevar a cabo el estudio de seguridad de la red inalámbrica.

4.1.1 Plataforma de Virtualización (VMware)

Se utilizó VMware Workstation por su robustez como plataforma de virtualización para proporcionar un entorno seguro, flexible y fácil de usar para alojar Kali Linux en el sistema operativo principal. Esto garantizó que todas las actividades del

4.1.2 Máquina virtual con Kali Linux

Se requirió de una máquina virtual que ejecute Kali Linux como sistema operativo, con al menos 20 GB de espacio libre en disco duro, mínimo 2 GB de RAM que sea alojada en una máquina host que posea un procesador de 64 bits con soporte de virtualización. Esto proporcionó el entorno de trabajo necesario para llevar a cabo las pruebas de penetración y análisis de seguridad en la red inalámbrica de la situación.

4.1.3 Herramientas de Seguridad

Se utilizaron varias herramientas de seguridad incluidas dentro de Kali Linux, como:

- **Nmap:** como herramienta para el escaneo de la red y descubrimiento de dispositivos, puertos abiertos y servicios.
- **Bettercap:** para realizar ataques de Hombre en el Medio e interceptar las comunicaciones.
- **Nessus:** como aplicación para realizar el escaneo de vulnerabilidades a la red u objetivos específicos.
- **Wireshark:** como herramienta para capturar y analizar el tráfico de red comprometido, además para identificar patrones anómalos y detectar posibles amenazas.

4.1.4 Adaptador WiFi Compatible con Kali Linux

Se necesitó de un adaptador WiFi compatible con Kali Linux y con capacidad para operar en modo AP (punto de acceso), para lograr configurar y gestionar una red inalámbrica falsa con el objetivo de realizar pruebas de penetración y posteriores análisis de seguridad. Para la

ejecución de las pruebas de penetración, se utilizó un adaptador Atheros AR9271 (Véase Anexo 2)

4.2 Topología de la Red Inalámbrica

A través de la entrevista realizada al encargado de Tecnologías y Redes de la institución (Véase anexo 3), se logró identificar que la infraestructura de la red inalámbrica está conformada por 1 equipo Fortinet que cumple las funciones de modem (no firewall), que provee el servicio de internet, a este equipo se conectan por fibra óptica 5 switch Aruba administrables PoE, ubicados en cada uno de los bloques (primaria, secundaria y preescolar), estos a su vez en su totalidad conectan a 35 AP Aruba y Huawei Poe (Ver figura 1). El cableado estructurado es categoría 6a.

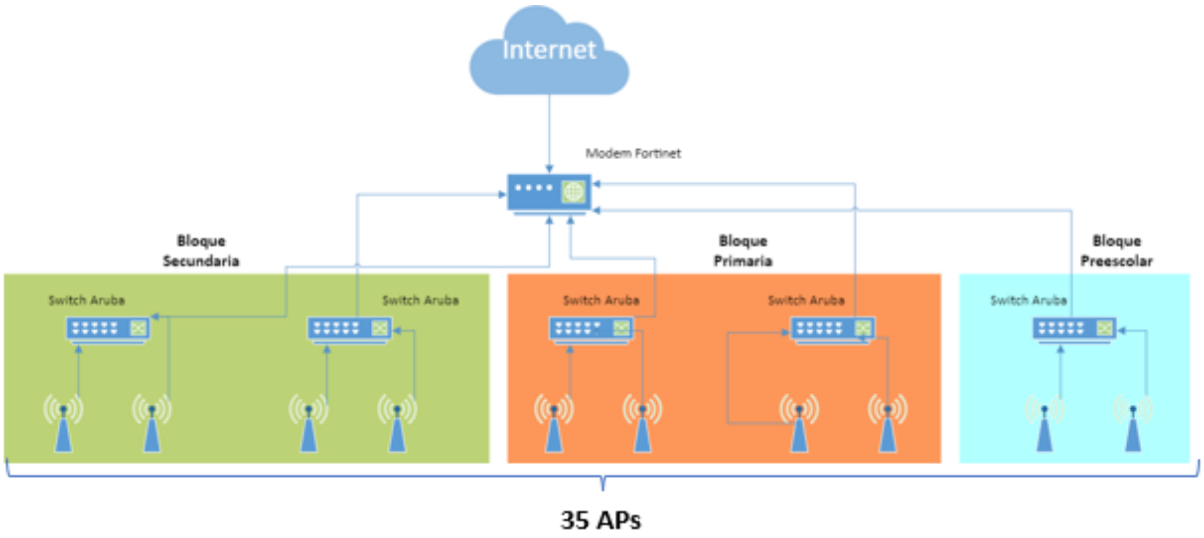


Figura 1 Topología de red inalámbrica de la institución

Cabe recalcar que, para llevar a cabo la propuesta del proyecto, se situó en la sala de profesores de secundaria conectado a un AP del Bloque Secundaria para escanear los dispositivos de los docentes y de varios estudiantes (Ver figura 2).

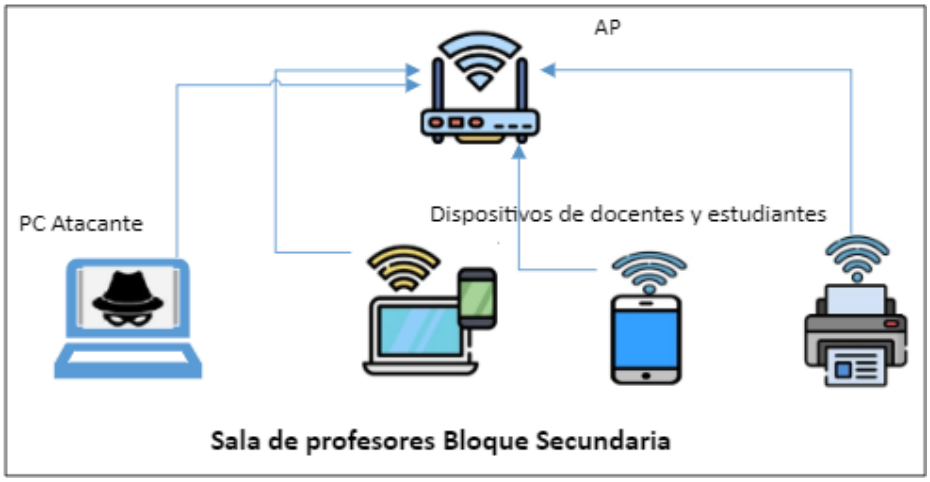


Figura 2 Diagrama de red de la propuesta a desarrollar

4.3 Desarrollo Fases de la Metodología de Pentesting

En esta sección, se demostró el proceso práctico realizado para ejecutar las pruebas de pentesting en conjunto con el ataque de Hombre en el Medio, basados sobre la metodología PTES y sus siete fases de ejecución.

4.3.1 Fase 1: Interacción Previa

Esta fase inicial del proyecto se basó en llevar a cabo una planificación detallada del alcance y los objetivos del proyecto, lo que permitió establecer una base sólida para la ejecución de las pruebas de penetración en la red inalámbrica de la institución educativa.

Si bien los objetivos y alcance del proyecto ya fueron detallados en el primer capítulo de introducción de este documento, fue crucial una revisión completa de estos aspectos para asegurar su validez y relevancia en el contexto actual. Por lo tanto, en esta fase se realizó una consulta y validación de los objetivos y alcance establecidos previamente para asegurarse de que estén definidos de manera clara y sean comprensibles para todas las partes interesadas, proporcionando una guía clara para la evaluación de la seguridad de la red inalámbrica en la

4.3.2 Fase 2: Recopilación de información

El objetivo de esta fase fue la de obtener una comprensión detallada de los equipos o dispositivos conectados a la red inalámbrica de la institución. Esta fase es fundamental para identificar los posibles puntos de entrada y vulnerabilidades que pueden ser explotadas en las fases posteriores del proyecto. Para esto, se utilizó la herramienta Nmap a través de su interfaz gráfica Zenmap para llevar a cabo un escaneo completo de la red y recolectar información como dispositivos conectados, direcciones IP, direcciones MAC, puertos abiertos, servicios activos, sistemas operativos, etc.

En primera instancia, se ejecutó un ping scan para determinar los hosts activos en la red en ese momento. Al haber estado conectado a la red 192.168.2.0/24 el comando a ejecutar fue el siguiente:

Figura 3 Escaneo tipo ping para descubrir dispositivos activos

Del escaneo realizado, se identificaron 81 hosts activos de 256 direcciones escaneadas, para observar a detalle los equipos escaneados revisar la sección de anexos (Véase anexo 4).

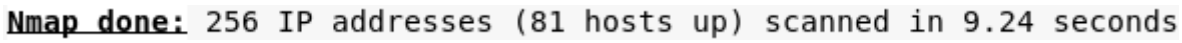


Figura 4 Resultado ping scan

A continuación, se ejecutó un escaneo de tipo **quick scan plus;** un tipo de escaneo rápido que permitió identificar los puertos abiertos, los servicios que se están ejecutando y si es posible, el tipo de sistema operativo de cada dispositivo conectado.

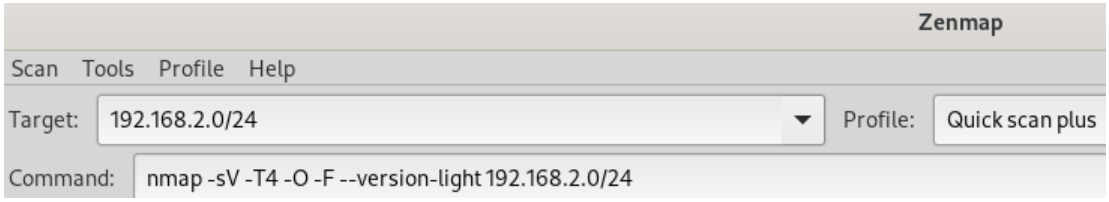


Figura 5 Escaneo de tipo quick scan plus

Del escaneo realizado, se logró obtener los siguientes resultados sobre los puertos abiertos y al servicio al que pertenece cada uno, para más detalles revisar apartado de anexos (Véase anexo 5).

Tabla 1 Resumen puertos abiertos encontrados

Puerto	Estado	Servicio
7070	abierto	ssl / realserver
8000	abierto	http-alt?
8008	abierto	http
8009	abierto	tcpwrapped
80	abierto	http
443	abierto	ssl/http
8080	abierto	http-proxy
49152	abierto	tcpwrapped

135	abierto	msrpc
139	abierto	Netbios-ssn
445	abierto	Microsoft-ds
5357	abierto	wsd
88	abierto	kerberos-sec
5000	abierto	rtsp
5432	abierto	postgresql

Además de los puertos encontrados y su estado, Nmap identificó el tipo de sistema operativo que poseía cada dirección encontrada, a continuación, se muestra una tabla con el resumen de hosts encontrados por sistema operativo.

Tabla 2 resumen dispositivos activos por sistema operativo

Dispositivo	Cantidad
Windows	20
Linux	17
Apple MacOS	4
Apple iOS	4
Android	5
Cisco Switch	1
Microsoft XBOX 360	1

De los resultados obtenidos se puede concluir que, en su mayoría, los dispositivos conectados a la red eran equipos Windows de los docentes que se encontraban en la sala de profesores. Cabe mencionar que los dispositivos Linux identificados, pertenecían a varios puntos de acceso de la marca Aruba, ya que, al momento de realizar el escaneo, se estaban realizando pruebas con nuevos equipos de red.

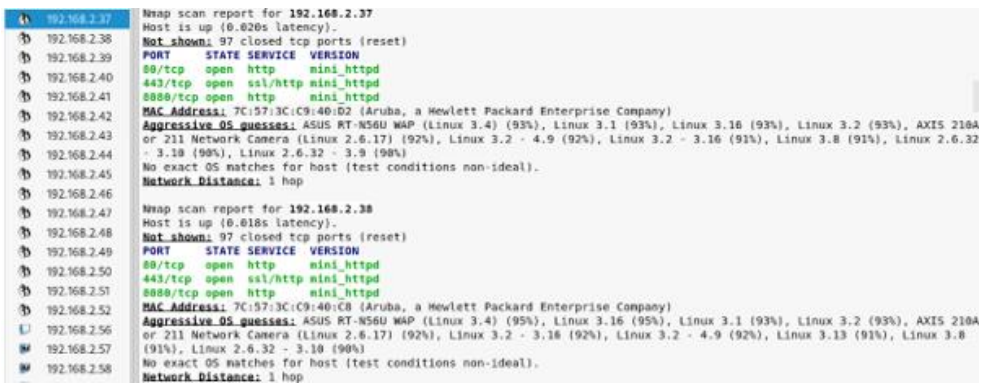


Figura 6 Puntos de acceso descubiertos

4.3.3 Fase 3: Modelado de amenazas

El objetivo de esta fase fue identificar, analizar y priorizar las posibles amenazas que pueda tener la red la red inalámbrica en la institución. Esta fase permitió comprender mejor los riesgos a los que a los que está expuesta la red y ayudó a planificar las pruebas de penetración de manera más efectiva.

4.3.3.1 Identificación de activos críticos

Basado en la información recopilada en las fases anteriores, se identificaron los activos críticos de la red, los cuáles se describen y clasifican a continuación en función de su importancia para la operación de la red y el impacto potencial de una amenaza sobre ellos:

Tabla 3 Identificación activos críticos de la red

Activo	Descripción	Función	Importancia	Impacto Potencial
Fortinet Modem	Dispositivo de red conectado directamente a internet	Proveer servicio de internet a los demás equipos	Alta	Una falla o ataque dirigido hacia este equipo podría desconectar a toda la institución de internet, afectando de forma directa las operaciones y aprendizaje.
Switch Aruba PoE	5 Switches administrables	Conectar y alimentar los APs	Alta	La falla de un switch podría dejar sin conectividad a un bloque entero ya sea preescolar, primaria o secundaria.
APs Aruba y Huawei	35 APs PoE	Proveer conectividad inalámbrica	Media	Sin acceso inalámbrico, los estudiantes, docentes y personal administrativo no podrían acceder a recursos en línea y sistemas.
Cableado estructurado	Cableado Cat 6a	Conectar dispositivos de red	Media/Baja	Interrupción parcial de la red; fácil reparación o reemplazo. Aunque es crucial, el cableado suele ser más fácil de reparar y reemplazar comparado con equipos de red.

4.3.3.2 Identificación y análisis de amenazas potenciales

En este apartado, se identificaron las amenazas más comunes que puede tener la red inalámbrica de la institución, incluyendo ataques de denegación de servicios (DoS), ataques de hombre en el medio (MITM) y ataques de fuerza bruta a contraseñas.

- **Ataques de Denegación de Servicios (DoS):** este tipo de ataque tiene como objetivo hacer que la red o ciertos servicios no estén disponibles para los usuarios legítimos, esto

a través de saturaciones de tráfico y solicitudes al servidor o dispositivos de red (Guaña-Moya et al., 2022, p.96).

Impacto potencial:

- Disminución en el rendimiento de la red, causando lentitud y desconexiones.
- Interrupción del acceso a internet y a servicios críticos, afectando la educación y operaciones administrativas.

Medidas de Mitigación:

- ✓ Configurar límites de conexión y aplicar controles de calidad de servicio (QoS)
- ✓ Implementar soluciones de monitoreo de tráfico y detección de anomalías.

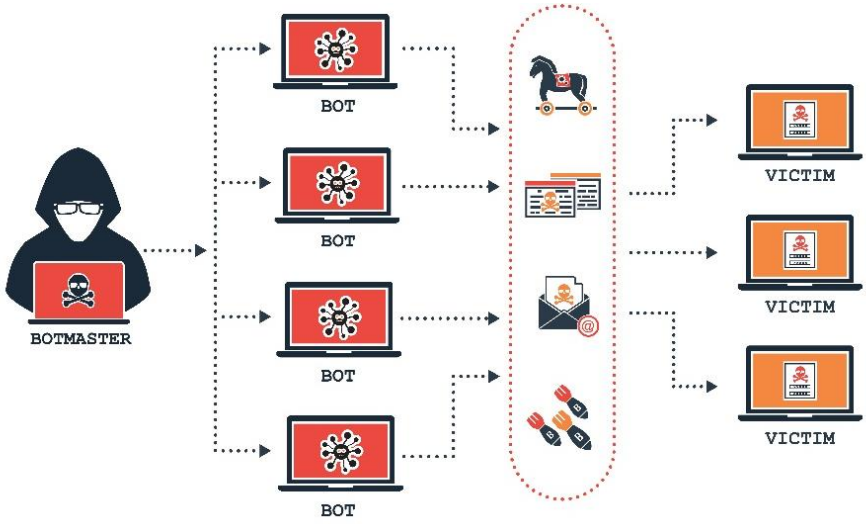


Figura 7 Modelo ataque de denegación de servicio

Tomado de Incibe (2018) https://www.incibe.es/ciudadania/blog/que-son-los-ataques-dos-y-ddos

- ❖ **Ataques de Hombre en el Medio (MITM):** en este tipo de ataque el atacante intercepta y altera la comunicación entre dos partes sin que estas se den cuenta, lo que puede permitir la captura de datos sensibles como credenciales de inicio de sesión y otra información confidencial.

Impacto potencial:

- Robo de información confidencial a docentes, estudiantes y personal administrativo, incluyendo credenciales de usuario y datos personales.
- Posible alteración de la comunicación, lo que puede llevar a manipulación de datos o desinformación.

Medidas de Mitigación:

- ✓ Implementar autenticación mutua y certificados SSL/TLS para asegurar la integridad y confidencialidad de los datos.
- ✓ Utilizar protocolos fuertes de seguridad más fuertes como WPA3 para la comunicación inalámbrica.

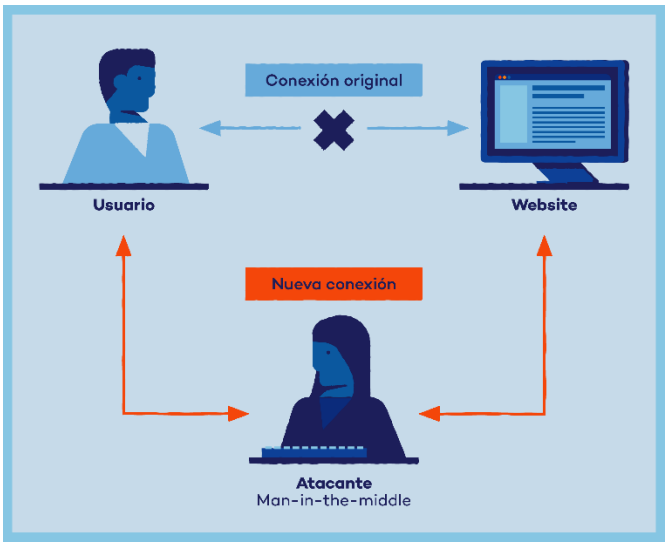


Figura 8 Modelo ataque de hombre en el medio

Tomado de PandaSecurity (2022) https://www.pandasecurity.com/es/mediacenter/ataque-man-in-the-middle/

Ataques de Fuerza Bruta – el atacante para este caso, a través de herramientas de software intenta adivinar una contraseña mediante diccionarios que poseen una serie de posibles contraseñas o combinaciones hasta encontrar la correcta.

Impacto potencial:

- ➢ Compromiso de cuentas de usuario, con la posibilidad de realizar acciones maliciosas.
- ➢ Acceso no autorizado a la red inalámbrica y a recursos internos.

Medidas de Mitigación:

- ✓ Configurar bloqueos de cuenta después de un cierto número de intentos fallidos.
- ✓ Implementar políticas de contraseñas fuertes y cambiar las credenciales predeterminadas.

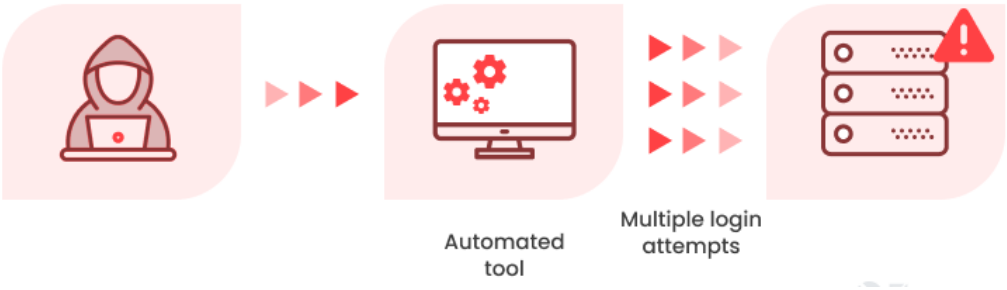


Figura 9 Modelo ataque de fuerza bruta

Tomado de Ekran (2023) https://www.ekransystem.com/en/blog/brute-force-attacks

4.3.4 Fase 4: Análisis de vulnerabilidades

El objetivo de esta fase fue identificar y evaluar las vulnerabilidades presentes en la red inalámbrica de la institución educativa, con el fin de comprender las debilidades de la infraestructura de red y proporcionar información crucial para planificar y ejecutar las pruebas de penetración dirigidas. Esto se lo logró utilizando la herramienta Nessus dentro de Kali Linux, la cual permitió identificar las vulnerabilidades conocidas en dispositivos y servicios.

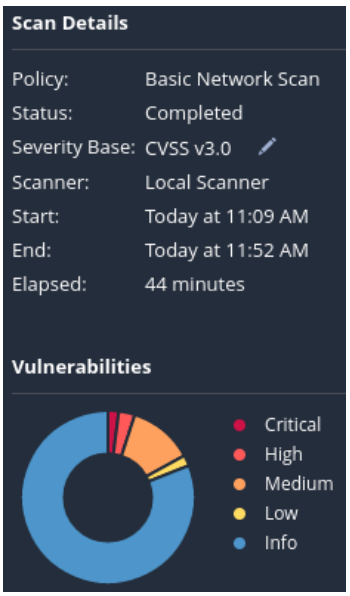


Figura 10 Resultado Escaneo Nessus

Según el nivel de las vulnerabilidades encontradas, Nessus las clasifica en cuatro niveles: crítico, alto, medio y bajo, cada una representada con un color específico.

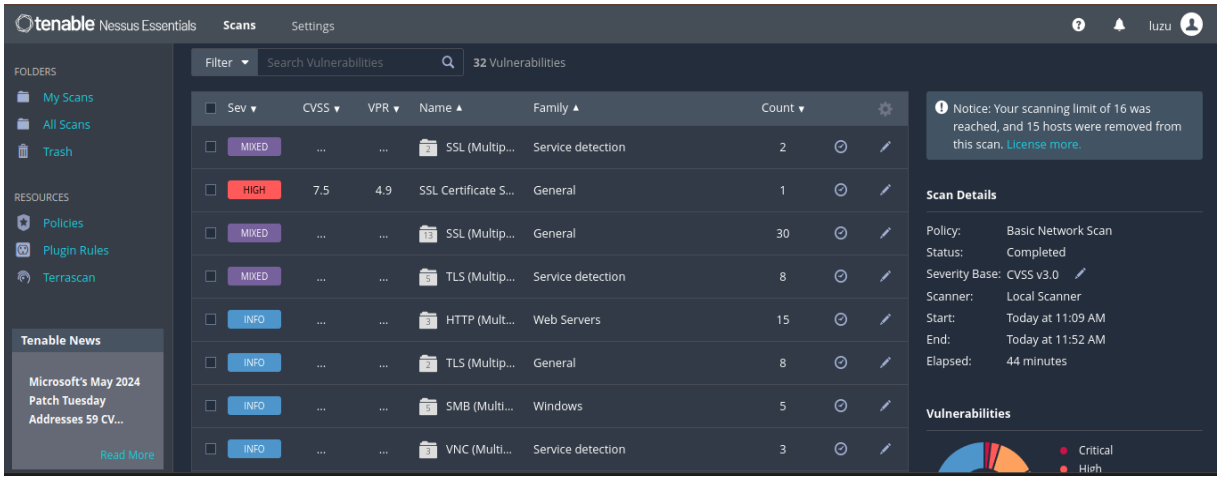


Figura 11 Vulnerabilidades encontradas

En total, se descubrieron 32 vulnerabilidades de las cuales se enfocó en las de nivel crítico, alto y medio, que se detallan a continuación en la siguiente tabla:

Tabla 4 Resumen vulnerabilidades encontradas de nivel crítico, alto y medio

Vulnerabilidad	Nivel	Descripción	Solución
Detección de protocolos SSL versiones 2 y 3	Crítico	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y/o SSL 3.0. Estas versiones de SSL están afectadas por varios fallos criptográficos, entre los que se incluyen: - Un esquema de relleno inseguro con cifrados CBC. - Esquemas inseguros de renegociación y reanudación de sesión. Un atacante puede aprovechar estos fallos para realizar ataques de intermediario o para descifrar las comunicaciones entre el servicio afectado y los clientes.	Consulte la documentación de la aplicación para desactivar SSL 2.0 y 3.0. Utilice en su lugar TLS 1.2 (con suites de cifrado aprobadas) o superior.
Certificado SSL firmado con un algoritmo hash débil	Alto	El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un algoritmo hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a ataques de colisión. Un atacante puede aprovecharse de ello para generar otro certificado con la misma firma digital, lo que le permitiría hacerse pasar por el servicio afectado.	Póngase en contacto con la autoridad de certificación para que vuelva a emitir el certificado SSL.
Suites de cifrado SSL de resistencia	Alto	El host remoto admite el uso de cifrados SSL que ofrecen un cifrado de fortaleza media. Nessus considera como cifrado de fortaleza media cualquier cifrado que utilice longitudes de	Reconfigure la aplicación afectada si es posible para

media compatibles (SWEET32)		clave de al menos 64 bits y menos de 112 bits, o bien que utilice el conjunto de cifrado 3DES.	evitar el uso de cifrados de fuerza media.
El certificado SSL no es de confianza	Medio	No se puede confiar en el certificado X.509 del servidor. Esta situación puede producirse de tres formas diferentes, en las que la cadena de confianza puede romperse. Si el host remoto es un host público en producción, cualquier ruptura en la cadena hace más difícil para los usuarios verificar la autenticidad e identidad del servidor web. Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.	Adquiera o genere un certificado SSL adecuado para este servicio.
Certificado SSL autofirmado	Medio	La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto. Tenga en cuenta que este complemento no comprueba las cadenas de certificados que terminan en un certificado que no está autofirmado, sino que está firmado por una autoridad de certificación no reconocida.	Adquiera o genere un certificado SSL adecuado para este servicio.
Suites de cifrado SSL RC4 compatibles (Bar Mitzvah)	Medio	El host remoto soporta el uso de RC4 en una o más suites de cifrado. El cifrado RC4 es defectuoso en su generación de un flujo pseudoaleatorio de bytes, de modo que se introduce una amplia variedad de pequeños sesgos en el flujo, disminuyendo su aleatoriedad. Si el texto plano se cifra repetidamente (por ejemplo, cookies HTTP) y un atacante es capaz de obtener muchos (es decir, decenas de millones) textos cifrados, el atacante puede ser capaz de obtener el texto plano.	Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere el uso de TLS 1.2 con suites AES-GCM sujetas a la compatibilidad del navegador y el servidor web.
Suites de cifrado débil SSL compatibles	Medio	El host remoto soporta el uso de cifrados SSL que ofrecen un cifrado débil. Nota: Esto es considerablemente más fácil de explotar si el atacante se encuentra en la misma red física.	Reconfigure la aplicación afectada, si es posible para evitar el uso de cifrados débiles.

Los resultados obtenidos evidencian que la mayoría de las vulnerabilidades encontradas en la red pueden ser explotadas a través de un ataque de hombre en el medio, como lo detalla la primera vulnerabilidad crítica. En este sentido, los resultados proporcionaron una base sólida para las siguientes fases del proyecto para planificar y ejecutar pruebas de penetración dirigidas hacia estas vulnerabilidades.

4.3.5 Fase 5: Explotación

El objetivo de esta quinta fase fue llevar a cabo ataques controlados para verificar la presencia y el impacto de las vulnerabilidades identificadas en las fases anteriores. De esta forma se logró demostrar cómo un atacante podría explotar estas vulnerabilidades para comprometer la seguridad de la red inalámbrica de la institución educativa. Cabe aclarar que los ataques fueron ejecutados de manera ética en un entorno controlado para minimizar el impacto en las operaciones normales de la institución.

4.3.5.1 Descifrando la contraseña WiFi mediante un ataque de diccionario

A través de la entrevista realizada al encargado de Tecnologías y Redes de la institución, se descubrió que la red inalámbrica utiliza el método WPA2/WPA-Personal como método de autenticación. Es necesario recalcar que al haber realizado un pentesting de caja gris, el encargado facilitó con la contraseña para acceder al Internet. Sin embargo, en este apartado se simuló la actividad de un atacante externo que no posee la clave de acceso e intenta obtenerla a través de un ataque de diccionario. Esto se realizó con la intención de medir que tan segura es la contraseña de la red inalámbrica y medir cuanto tiempo le tomaría a un atacante crackearla.

Para llevar a cabo el ataque de fuerza bruta se necesitó de dos elementos clave:

1. capturar el Handshake
2. contar con un diccionario robusto y completo que incluya una gran cantidad de palabras o posibles contraseñas.

4.3.5.2 Captura del handshake

Primero se debe entender qué es el handshake en las redes inalámbricas; este es el proceso que garantiza que tanto el cliente como el punto de acceso comparten la misma clave y pueden comunicarse de forma segura. (Pidis, 2023) lo define como el proceso de autenticación y establecimiento de claves de cifrado entre un cliente (como un dispositivo móvil o un ordenador) y un punto de acceso en el contexto de las redes Wi-Fi protegidas por WPA/WPA2 (p. 1).

Para capturar el handshake de la red inalámbrica de la institución se siguieron los siguientes pasos:

Primero se conectó la tarjeta de red inalámbrica compatible con Kali Linux y se la colocó como modo monitor, de este modo permitió capturar todos los paquetes de datos que se transmiten en el aire, sin necesidad de estar conectados a una red específica.

Utilizando el comando ifconfig o ip a se comprobó el nombre de la tarjeta de red inalámbrica.

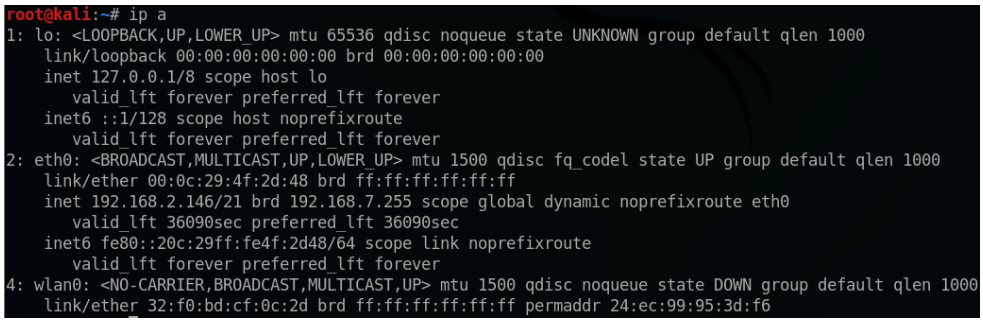


Figura 12 Resultado comando ip a

A continuación, con el comando “airmon-ng start” seguido del nombre de la tarjeta de red “wlan0” se cambió al modo monitor

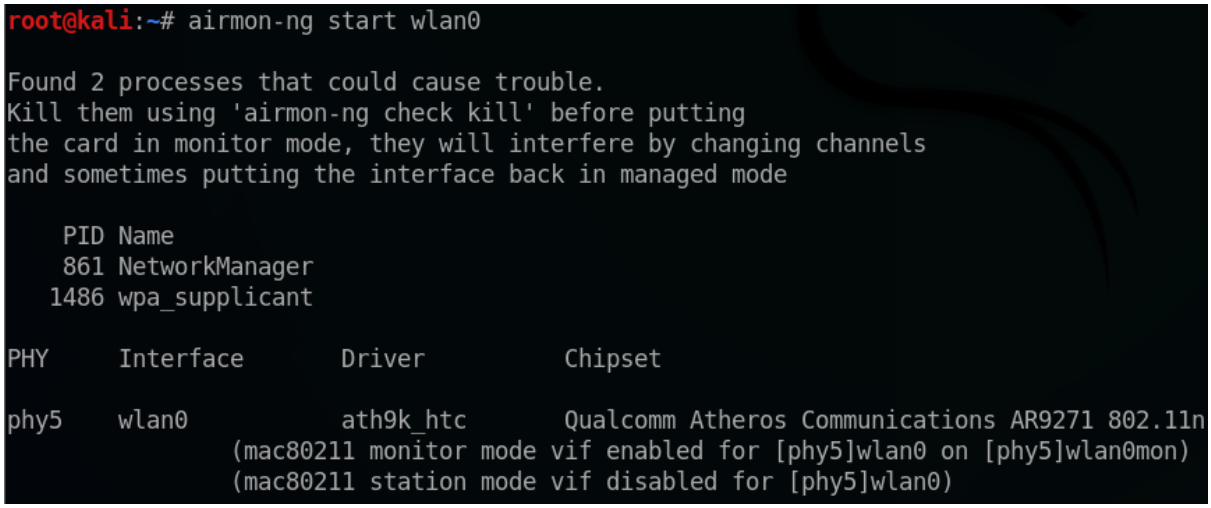


Figura 13 Cambio a modo monitor de la tarjeta de red

Con el comando “iwconfig” se comprobó el cambio realizado

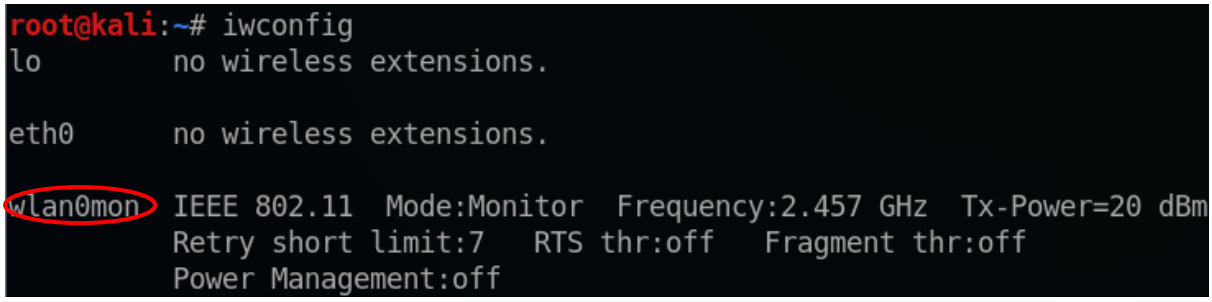


Figura 14 Comprobación cambio a modo monitor

Seguido de esto, se ejecutó el comando "airodump-ng wlan0mon" para descubrir todas las redes inalámbricas cercanas.

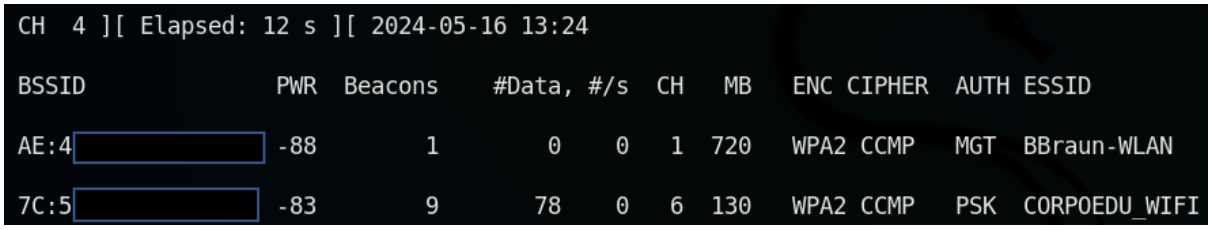


Figura 15 Descubrimiento de redes inalámbricas con el comando airodump

De esta forma, se identificó la red inalámbrica a ser atacada "CORPOEDU-WIFI" con esto se procedió a ejecutar el siguiente comando para almacenar el handshake capturado en un archivo:

airodump-ng –bssid **(bssid del objetivo)** –channel **(canal de la red objetivo)** –write **(nombre del archivo donde se va a almacenar el handshake) (nombre del adaptador inalámbrico en modo monitor)**

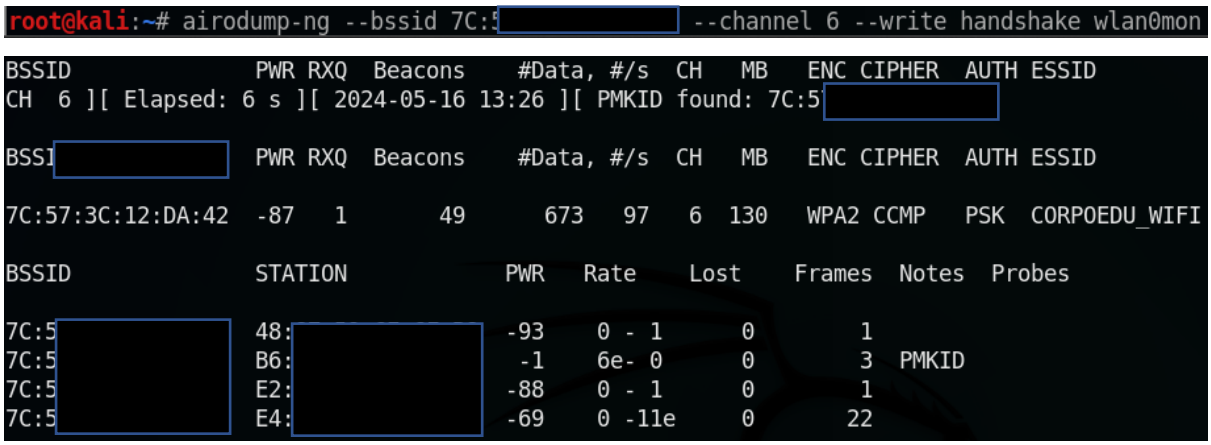


Figura 16 Captura del handshake

Cabe mencionar que el handshake es capturado cuando un nuevo dispositivo se conecta a la red, por lo que no tardó mucho en capturarlo. Además, el handshake capturado no contiene

la información para recuperar la clave solo contiene la información que es usada para verificar si una clave es válida o no. Por esta razón, el otro elemento clave necesario es una "wordlist" o diccionario con las posibles opciones y variantes de posibles contraseñas.

Para este caso se descargó una gran cantidad de diccionarios predefinidos desde internet con contraseñas comunes, menos seguras, más usadas, etc. Además, se utilizaron scripts en Python que permitieron crear contraseñas más personalizadas y sofisticadas.

Uno de los scripts utilizados fue el siguiente:

```python
import itertools

patron = "corpoedu"
anios = ["2021", "2022", "2023", "2024"]

# genera todas las combinaciones de mayúsculas y minúsculas para el patrón
variaciones = list(itertools.product(*((c.lower(), c.upper()) for c in patron)))

# abre el archivo para escribir los resultados
with open("passwords.txt", "w") as f:
    for variacion in variaciones:
        clave_base = "".join(variacion)
        for anio in anios:
            f.write(clave_base + anio + "\n")
```

Figura 17 Script de python utilizado

Explicación del script:

- ✓ **"itertools.product"** se utiliza para generar el producto cartesiano de las opciones de mayúsculas y minúsculas para cada carácter en el patrón.
- ✓ La variable **"patron"** contiene la cadena base corpoedu y "anios" contiene los años que se agregarán al final.
- ✓ La función **"itertools.product"** genera todas las combinaciones posibles de mayúsculas y minúsculas para cada carácter en corpoedu.
- ✓ **"open"** abre o crea el archivo passwords.txt en modo escritura.
- ✓ Para cada combinación generada, se une en una cadena usando **"".join(variation)** y se asigna a **"clave_base".**
- ✓ Para cada año en **"anios",** se concatena con **"clave_base"** y se escribe en el archivo, agregando un salto de línea al final de cada una.

En resumen, este script generó todas las combinaciones del patrón "corpoedu" con letras en mayúsculas y minúsculas, y les añadirá los años 2021, 2022, 2023 y 2024, guardándolas en el archivo passwords.txt.

Por último, se ejecutó el script en una terminal con el comando **python3 generar_claves.py** que es el nombre con el cual se guardó el script.

Con el handshake capturado y el diccionario de contraseñas, se procedió a ejecutar el siguiente comando utilizando "aircrack-ng" el cuál descomprime el handshake y extrae la información útil, haciendo uso del llamado MIC (Message integrity code) para verificar si una contraseña es correcta o no, recorriendo todo el diccionario, probando cada posible contraseña una por una. La herramienta tardó 2 horas y 10 minutos en descifrar la contraseña dentro del diccionario que poseía aproximadamente 14 millones de posibles claves.

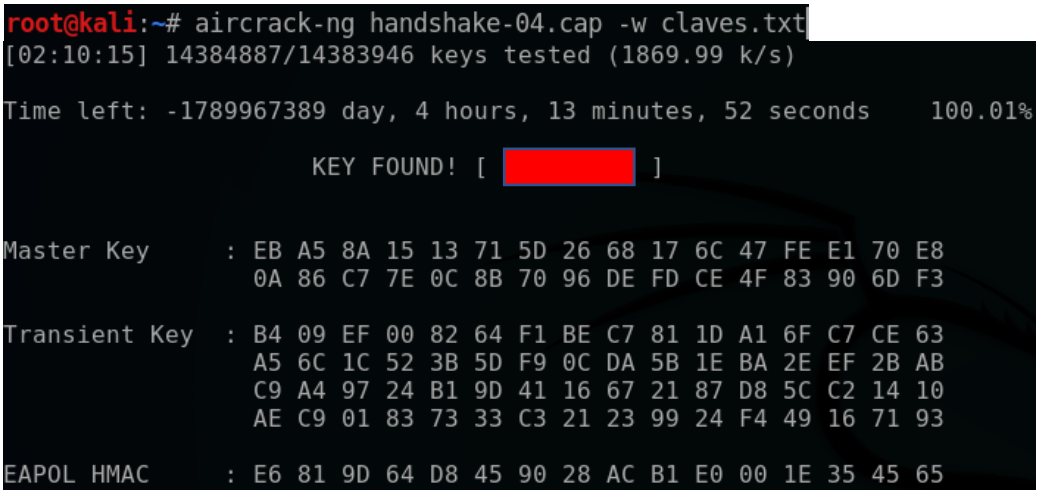


Figura 18 Ejecución ataque de fuerza bruta

Es importante aclarar que el ataque fue realizado con herramientas básicas de hackeo para descifrar la contraseña. Esto quiere decir que, si un atacante experimentado o con los suficientes recursos intentara realizar el mismo ataque, este podría ejecutarlo de forma más efectiva y descifrar la contraseña mucho más rápido debido a lo débil que es esta.

4.3.5.2 Ataque Hombre en el Medio mediante Arp-Spoofing

El ataque de Hombre en el Medio consiste en que un atacante intercepta la comunicación entre dos partes que creen estar comunicándose entre sí. De esta forma, el atacante logra escuchar y modificar la información transmitida, lo que puede resultar en el robo de datos sensibles, la manipulación de mensajes y otros tipos de compromisos de seguridad. Para llevar a cabo este ataque, se utilizó una de las técnicas más comunes en ataques de Hombre en el Medio; el ARP-Spoofing o también conocido como ARP-Poisoning. Esta técnica explota la falta de autenticación en el protocolo ARP (Address Resolution Protocol), que es el protocolo utilizado para resolver direcciones IP a direcciones MAC en una red local.

El ARP-Spoofing se divide en las siguientes etapas:

1. Primero el atacante envía mensajes ARP maliciosos a los dispositivos objetivo en la red, de esta forma las tablas ARP de estos dispositivos asocian la dirección IP de la víctima con la dirección MAC del atacante.
2. Una vez que las tablas ARP han sido envenenadas, el tráfico destinado a la dirección IP de la víctima se envía al atacante en lugar de al destino legítimo.
3. El atacante ahora puede interceptar, analizar o modificar el tráfico antes de enviarlo a su destino original. Esto permite al atacante robar credenciales, datos sensibles o incluso insertar malware en la comunicación.

Las figuras 19 y 20 muestran un diagrama de red antes y después de un ARP-Spoofing

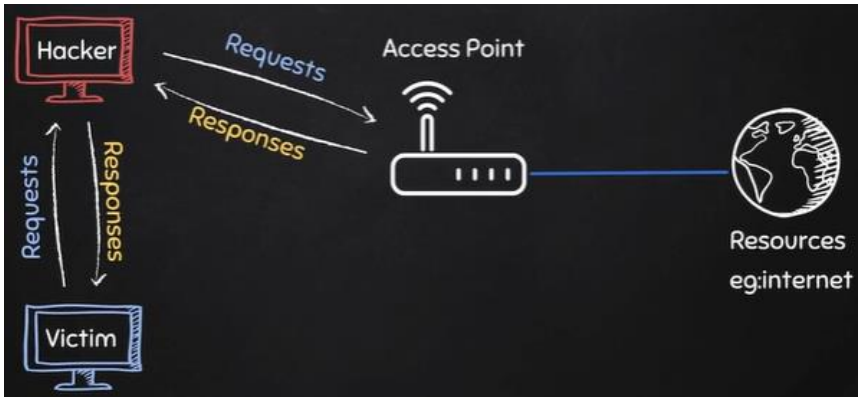


Figura 19 Diagrama del funcionamiento normal de una red WiFi (antes ARP-Spoofing)

Tomado de GoLinuxCloud (2023) https://www.golinuxcloud.com/man-in-the-middle-attack-arp-spoofing/

En la siguiente figura se observa cómo funciona un ataque de ARP-Spoofing a nivel lógico, donde todo el tráfico que genere la máquina víctima también pasará por la máquina atacante.

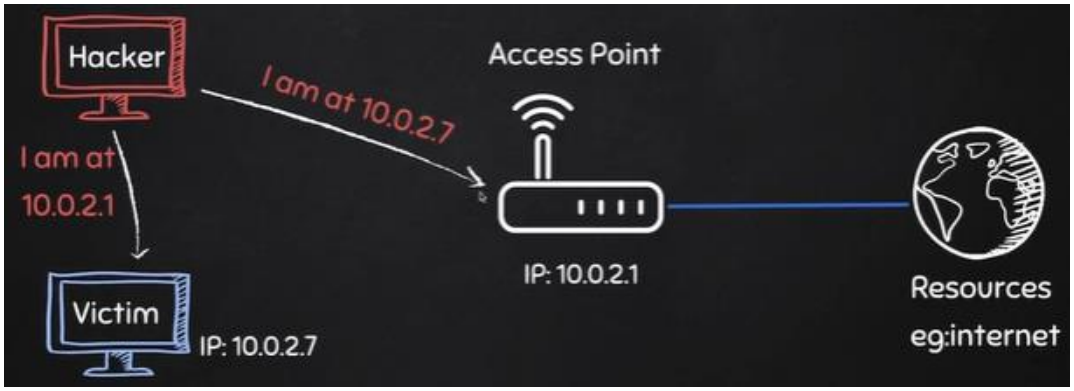


Figura 20 Diagrama funcionamiento ARP-Spoofing

Tomado de AntonyViet (2023) https://en.anonyviet.com/pyhack-lesson-3-network-scanner-scan-network-information/

Para llevar a cabo la ejecución del ataque de Hombre en el Medio, se necesitó de las siguientes herramientas:

- ✓ Máquina virtual Kali Linux en VMware
- ✓ Bettercap
- ✓ Adaptador inalámbrico WiFi con soporte para modo AP
- ✓ Wi Hotspot para la creación del falso AP

4.3.5.3 Ejecución ataque MITM

Es necesario recalcar que el ataque fue realizado hacia una máquina con Windows 10 que no poseía ningún tipo de protección, solo se activó la protección de Windows Defender con el objetivo de verificar también su eficacia frente a este tipo de ataques.

La siguiente figura muestra el diagrama del ataque en cuestión:

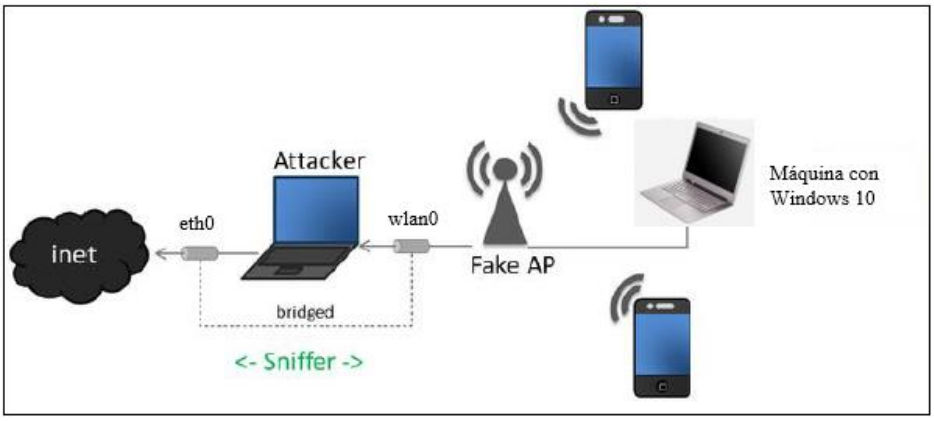


Figura 21 Diagrama de ataque MITM con falso AP

En primer lugar, se procedió a crear un falso Access Point utilizando el adaptador de red inalámbrico. Para esto se utilizó la herramienta Wi Hotspot que permite convertir adaptadores inalámbricos en puntos de acceso a través de la conexión a la red del adaptador de red principal. Dentro de la interfaz de Wi Hotspot, en el apartado de **SSID** de colocó el nombre de la red para reconocer a nuestro adaptador de red en modo AP (CORPOEDU_WIFI FREE). En **WiFi interface** se seleccionó el nombre de el adaptador de red WiFi que pasará a modo Access Point (wlan0) y en el apartado de **Internet Interface** se colocó la interfaz de red por donde nuestra máquina está obteniendo su conexión a internet (eth0).

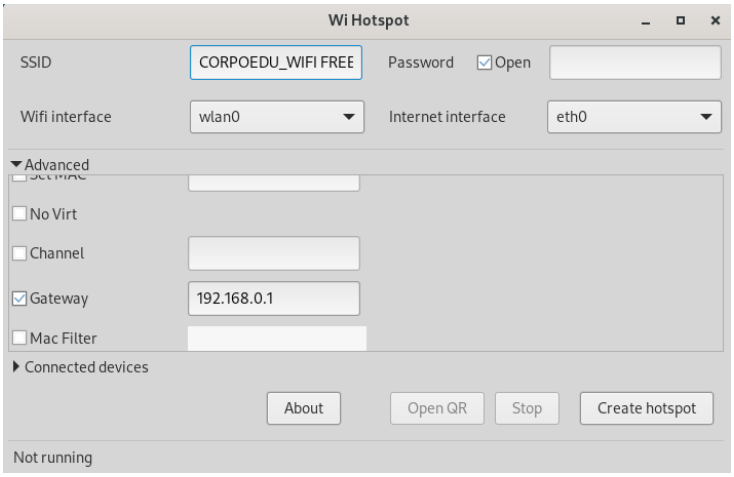


Figura 22 Configuración herramienta Wi Hotspot para crear falso AP

A continuación, para ejecutar la herramienta de bettercap, se inició una nueva terminal en modo super usuario y se colocó el siguiente comando: **bettercap iface** (seguido de la interfaz conectada a la red con la que se desea realizar el ataque)

```
root@kali:~# bettercap iface wlan0
bettercap v2.32.0 (built for linux amd64 with go1.22.1) [type 'help' for a list of commands]

192.168.0.0/24 > 192.168.0.102 » [14:33:06] [sys.log] [war] Could not find mac for 192.168.0.1
192.168.0.0/24 > 192.168.0.102 »
```

Figura 23 Ejecución herramienta bettercap

Al colocar el comando help, nos despliega todos los módulos que ofrece bettercap, ya que esta es una herramienta que no solo permite realizar ataques de Hombre en el Medio con Arp-Spoofing, también funciona como sniffer básico, para realizar inyecciones SQL, redirecciones DNS y más.

```
192.168.0.0/21 > 192.168.2.146 » help

          help MODULE : List available commands or show module specific help if no module name is provided.
               active : Show information about active modules.
                 quit : Close the session and exit.
        sleep SECONDS : Sleep for the given amount of seconds.
             get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
       set NAME VALUE : Set the VALUE of variable NAME.
  read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
                clear : Clear the screen.
       include CAPLET : Load and run this caplet in the current session.
            ! COMMAND : Execute a shell command and print its output.
       alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

     any.proxy > not running
      api.rest > not running
     arp.spoof > not running
     ble.recon > not running
            c2 > not running
       caplets > not running
   dhcp6.spoof > not running
     dns.spoof > not running
  events.stream > running
           gps > not running
           hid > not running
```

Figura 24 Módulos disponibles en bettercap

Luego, se colocó el comando **net.probe on** para activar el módulo que permite el descubrimiento de hosts que están conectados a la misma red.

Figura 25 Decubrimiento de hosts conectados a la misma red

Seguido de esto, con el comando **net.show** se desplegó la lista de hosts que fueron descubiertos en la misma red, es decir, conectados al falso AP. El host objetivo para este caso es el que posee la dirección 192.168.0.101 que pertenece a la máquina Windows.

Figura 26 Despliegue hosts encontrados en la misma red

A continuación, se procedió a activar los módulos de arp.spoof para que se empiece a ejecutar el ataque. Para esto, se ingresó el comando **arp.spoof.fullduplex true** que configura el módulo arp.spoof para el objetivo seleccionado al igual que el Gateway de la red sean atacados, de otra forma solo el dispositivo objetivo sería atacado. Seguido de esto, se colocó el comando **arp.spoof.targets 192.168.0.101** para que bettercap identifique quién va a ser el objetivo a atacar. Por último se ingresó el comando **arp.spoof on** para activar el módulo de arp.spoof y empezar con el ataque.

Figura 27 Activación módulos arp.spoof

Para comprobar si el ataque se está ejecutando correctamente, se procedió a ejecutar el comando **arp-a** en la máquina objetivo con Windows 10 para verificar si la tabla ARP en efecto ha sido modificada.

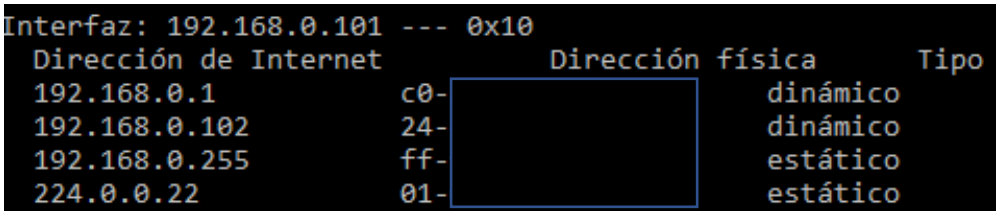


Figura 28 Tabla ARP del objetivo antes de realizar el ataque

A continuación, se puede observar como la tabla ARP de la víctima ha sido modificada, por lo que ahora todo el tráfico que genere pasará primero por la máquina atacante y luego hacia el Gateway.

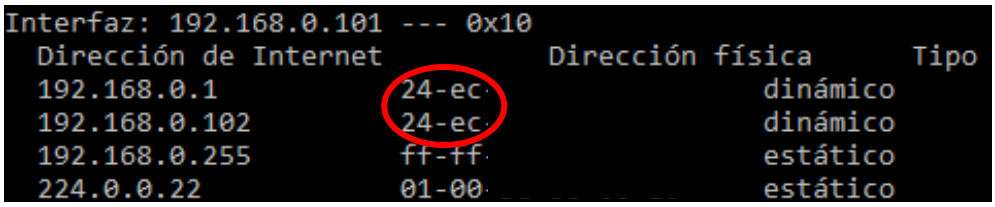


Figura 29 Tabla ARP del objetivo después de realizar el ataque

Con esto, se verificó el envenenamiento de la tabla ARP del objetivo por lo que ahora todo el tráfico que pase por el Gateway también pasará por nuestra máquina y podremos escucharlo. Para comenzar con la "escucha" del tráfico se utilizó el comando **net.sniff on** que permite capturar todo el tráfico que está enviando el objetivo atacado.

Figura 30 Activación módulo para captura de tráfico

De esta forma, se procedió a ingresar a páginas web e ingresar credenciales para que bettercap pueda capturalas y efectivamente al revisar bettercap se logró visualizar las credenciales que se ingresaron en la máquina atacada y a qué página se ingresó.

Figura 31 Captura de credenciales en bettercap

Sin embargo, es importante mencionar que con este método solo es posible capturar las credenciales y el tráfico proveniente de páginas HTTP. Por lo que la solución para poder capturar el tráfico y credenciales de páginas HTTPS, es conseguir degradar las conexiones HHTPS a HTTP. Para lograr esto, se ejecutó uno de los muchos "caplets" que incluye bettercap; los caplets son archivos de texto que contienen comandos y scripts escritos en el lenguaje de Bettercap y permiten realizar diversas tareas como intercepción de tráfico, manipulación de sesiones y otras actividades relacionadas con el análisis y la explotación de redes.

Para este caso específicamente se ejecutó el caplet que permite la degradación de conexiones HTTPS a HTTP que lleva por nombre **hstshijack/hsthijack.**

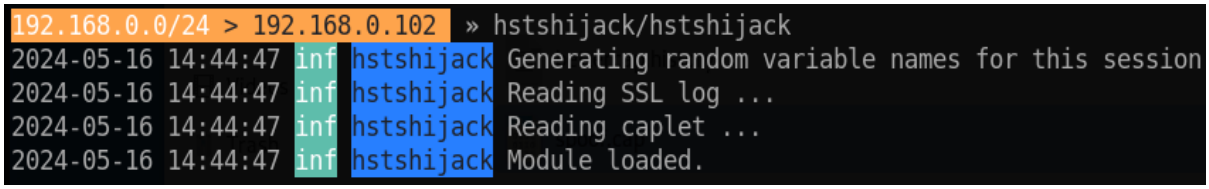


Figura 32 Ejecución caplet para degradar conexiones HTTPS

Luego de haber ejecutado el caplet, se realizó la captura de tráfico y credenciales ahora de páginas web bajo el protocolo HTTPS. En las siguientes figuras se demuestra que en efecto se logró capturar las credenciales ingresadas a páginas que funcionan con el protocolo HTTPS, como lo fueron Stackoverflow y Linkedin que son sitios web muy populares.

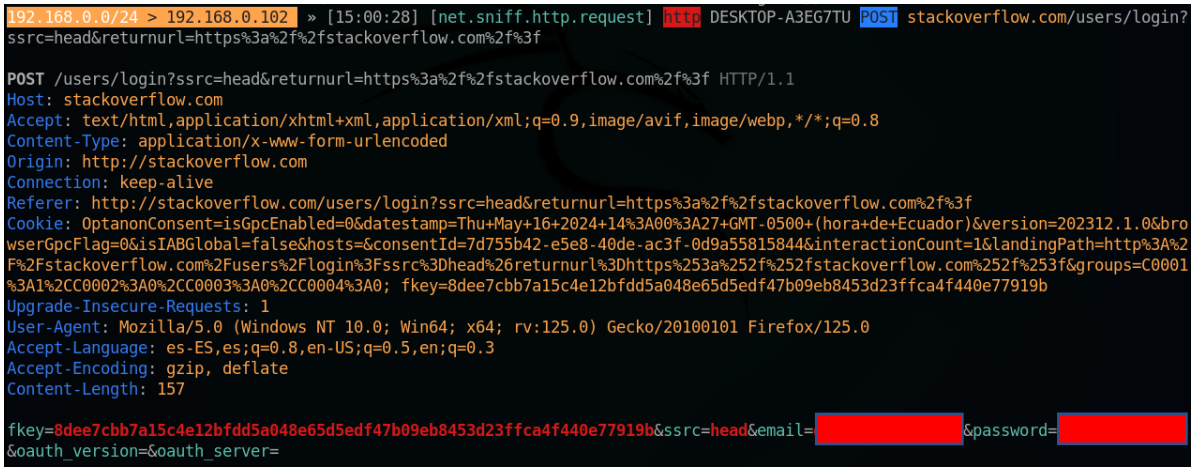


Figura 33 Captura de credenciales ingresadas al sitio web de stackoverflow

La siguiente figura muestra la captura de las credenciales de usuario, definido por "**sesion_key**" y su respectiva contraseña definida por el parámetro "**sesión_password**" referentes al sitio web de Linkedin.com

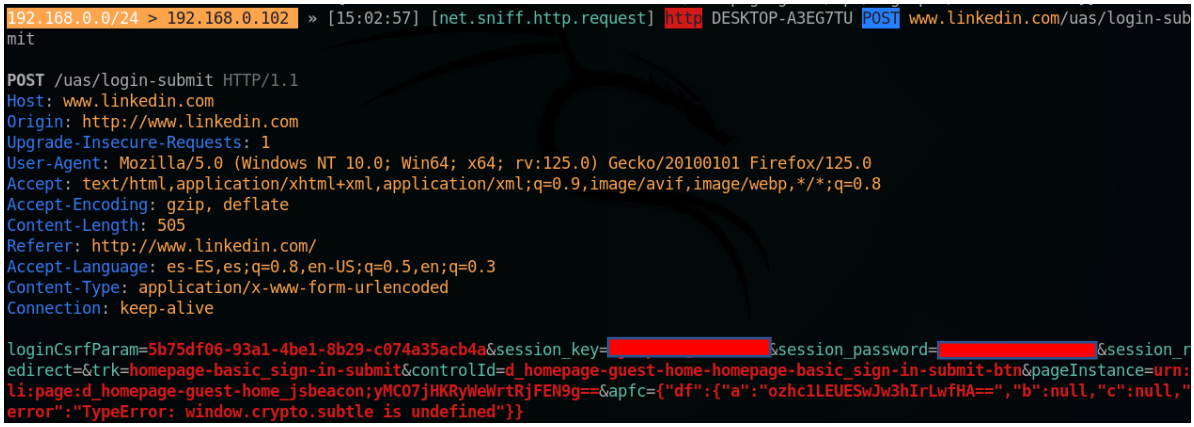


Figura 34 Captura de credenciales ingresadas al sitio web de Linkedin

Por otro lado, cuando se intentó realizar el mismo ataque en una máquina con protección de un antivirus, el antivirus detectó la amenaza y bloqueó el acceso a las páginas inseguras, cuyo protocolo HTTPS fue degradado a HTTP. Esto demuestra que, con las medidas de seguridad adecuadas, se pueden evitar fácilmente este tipo de ataques.

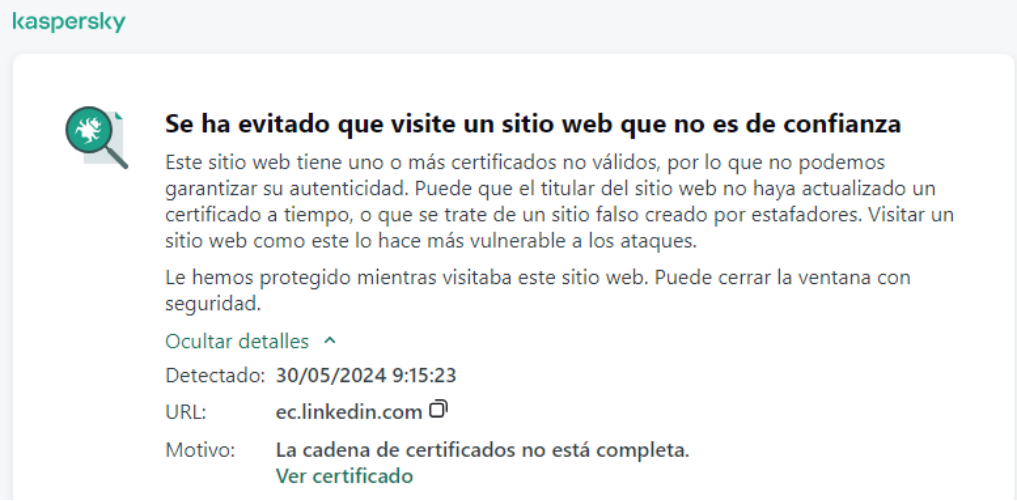


Figura 35 Detección del antivirus ante sitio peligroso

4.3.6 Fase 6: Post-Explotación

Después de haber obtenido acceso al sistema objetivo, se realizaron acciones adicionales para mantener el acceso y recopilar más información sensible. En esta fase se realizó un análisis más profundo del sistema comprometido para identificar movimientos laterales o cualquier otra actividad maliciosa que pueda llevarse a cabo.

4.3.6.1 Análisis del tráfico capturado con Wireshark

Para llevar a cabo esta fase se utilizó la herramienta Wireshark, que a diferencia de Bettercap, no es una herramienta de hacking, pero es más adecuada cuando se requiere realizar un examen detallado del tráfico capturado. Además, su capacidad para desglosar y analizar en profundidad los datos de red fue invaluable para entender el comportamiento de la red e identificar los datos sensibles.

Lo primero que se realizó fue ejecutar Wireshark que por defecto ya se encuentra instalado en Kali Linux y seleccionar la interfaz de red que se utilizó para realizar el ataque de Hombre en el Medio **wlan0**.

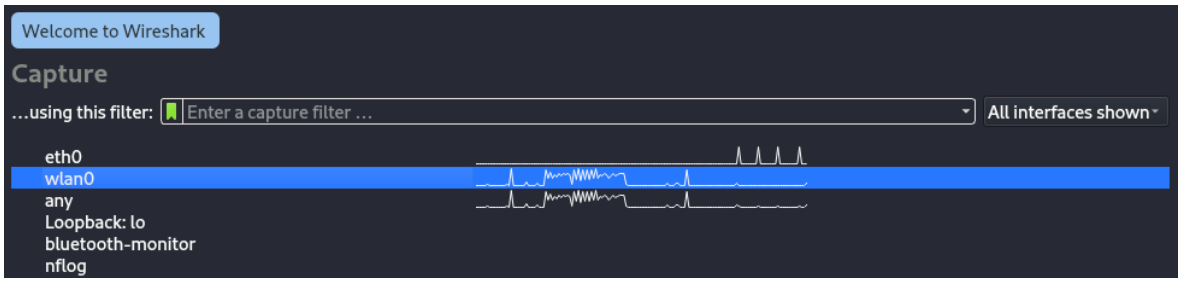


Figura 36 Interfaz Wireshark

A continuación, Wireshark comenzará a desplegar todos los paquetes que capture, por lo que, cualquier tipo de tráfico que fluya a través de la interfaz wlan0 ya sea páginas web, imágenes, mensajes, cookies, etc. Todo lo que la máquina atacada realice en internet pasará a través de la wlan0 y será capturado por Wireshark.

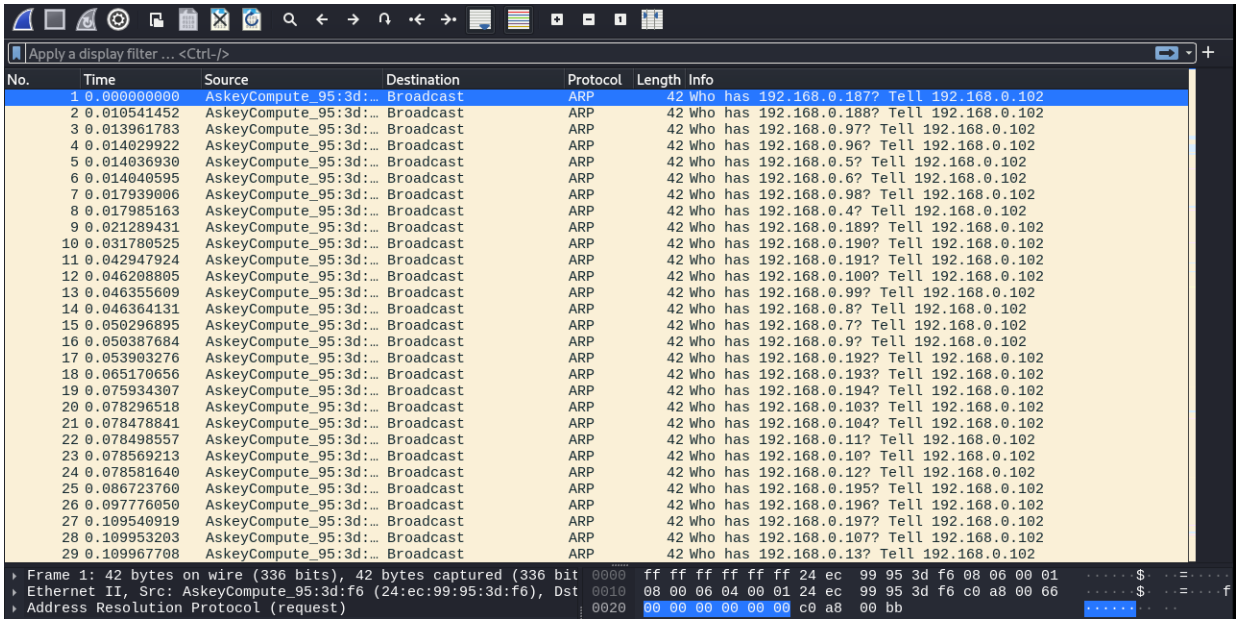


Figura 37 Tráfico capturado por Wireshark

En la figura anterior se puede observar una serie de paquetes ARP, estos son los paquetes enviados por Bettercap para que el ataque de Hombre en el Medio se siga ejecutando, de esta forma se puede mantener el acceso con el objetivo atacado. Al dar doble click en el primer paquete se logró desplegar toda la información de el mismo, en el apartado de origen se reconoció la dirección MAC de la máquina atacante y en el apartado de solicitud de paquete se identificó la dirección IP de la máquina objetivo.

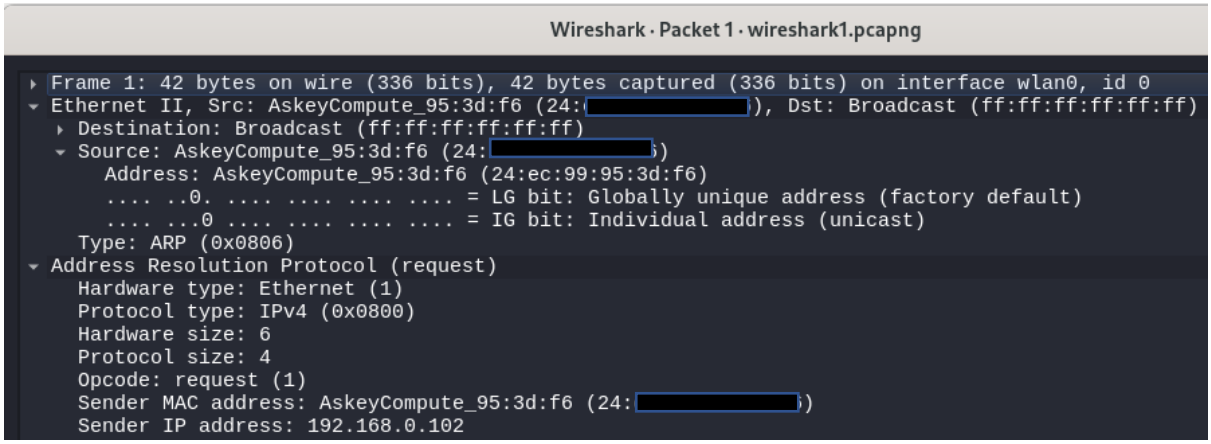


Figura 38 Desglose paquete ARP

Wireshark despliega todos los paquetes que son capturados incluyendo información como el origen, destino, protocolo, longitud de la información, etc. Sin embargo, para identificar la información que fue más relevante para el estudio, se aplicó un filtro para mostrar los paquetes HTTP que incluyen todos los datos sobre la navegación realizada en la máquina víctima.

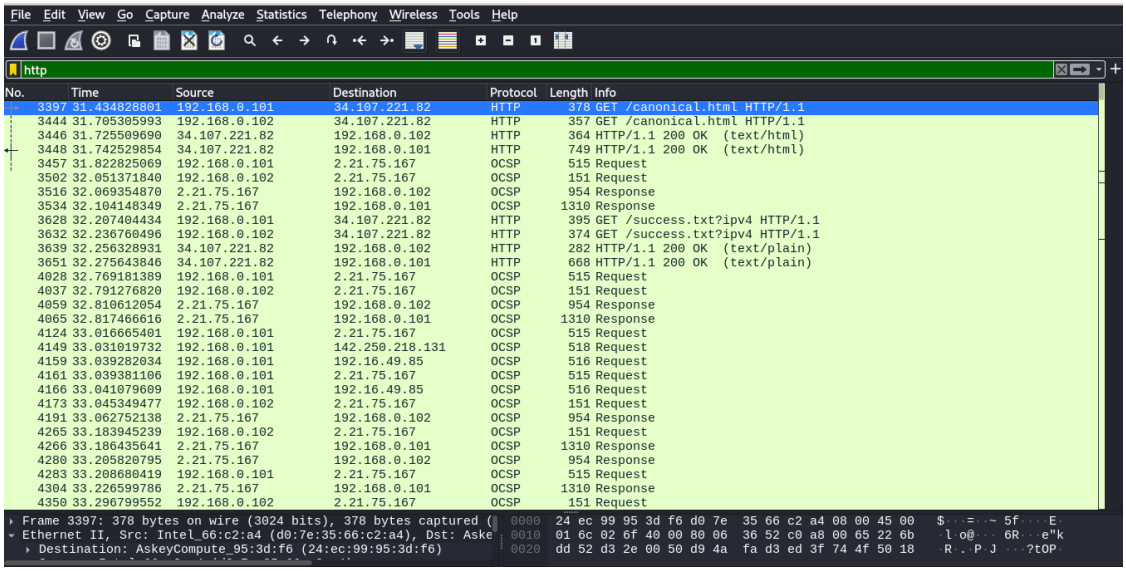


Figura 39 Filtrado paquetes HTTP

Navegando sobre estos paquetes, se logró identificar las solicitudes GET y POST sobre el tráfico de la navegación web realizada desde la máquina atacada.

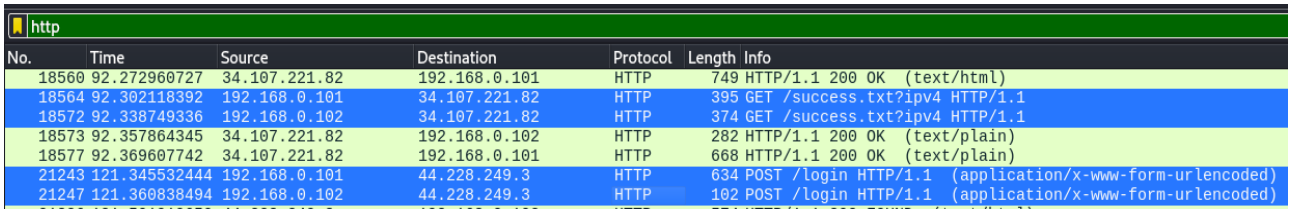


Figura 40 Métodos GET y POST identificados

Al ingresar a los paquetes con los métodos POST, se descubrió la información de inicio de sesión que se realizaron en la máquina atacada. Logrando identificar información sensible como la página visitada, los nombres de usuario y sus respectivas contraseñas. En la figura se observa las credenciales capturadas del sitio web de Stackoverflow.

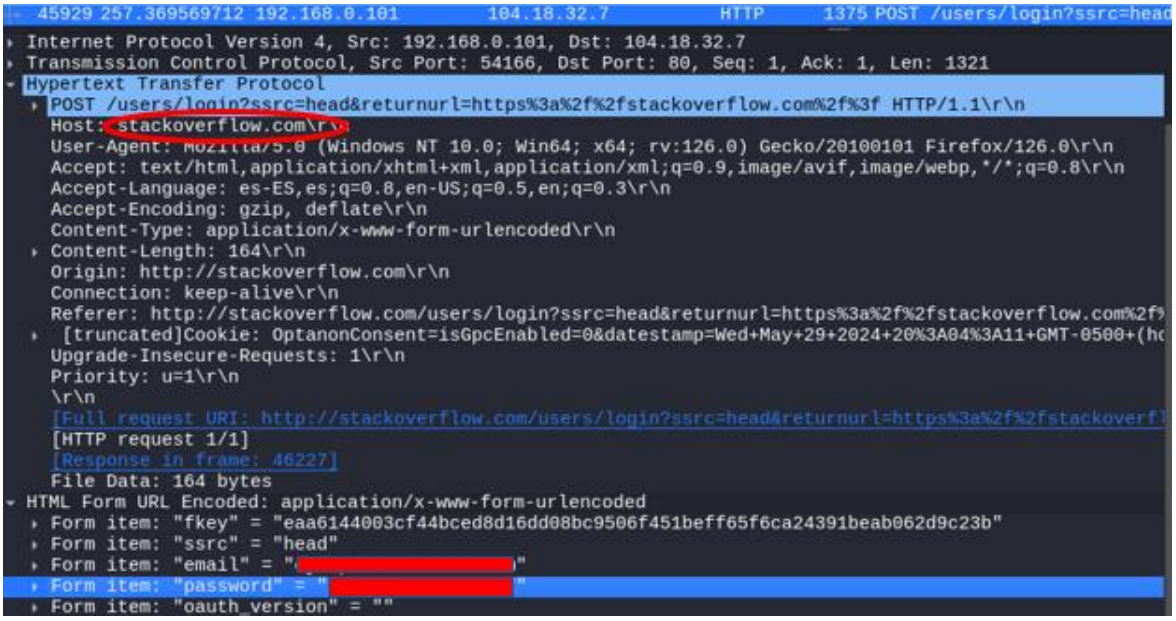


Figura 41 Credenciales capturadas sitio web Stackoverflow

La siguiente figura muestra las credenciales capturadas del sitio web de Linkedin, el campo de **sesión_key** contiene el usuario y el campo **sesión_password** la contraseña.

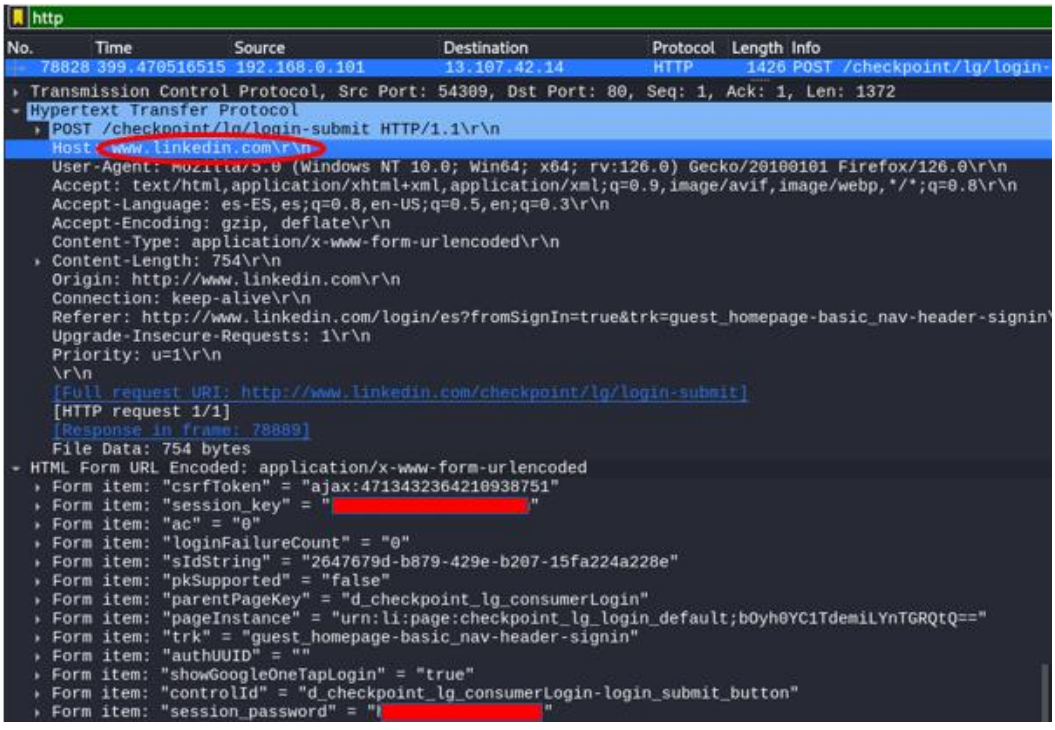


Figura 42 Credenciales capturadas sitio web Linkedin

En resumen, esta fase fue crucial para obtener una visión detallada del impacto real y potencial de la vulnerabilidad explotada, en este caso con el ataque de Hombre en el Medio, lo que fue fundamental para fortalecer la postura de seguridad de la institución.

4.3.7 Fase 7: Reporte

Esta fase tiene como objetivo compilar y presentar de manera comprensible los hallazgos y resultados obtenidos durante la ejecución de las pruebas de penetración.

4.3.7.1 Resultados pruebas de pentesting

En las fases de explotación y post-explotación del proyecto, se llevaron a cabo dos ataques específicos para evaluar la seguridad de la red inalámbrica de la institución educativa Liceo José Ortega y Gasset, los cuáles fueron un ataque de fuerza bruta utilizando un diccionario de palabras para descifrar la contraseña de la red y un ataque de Hombre en el Medio mediante ARP-Spoofing. Los resultados de estos ataques se describen a continuación:

1. **Ataque de Fuerza bruta mediante un diccionario de palabras**

Objetivo: Comprometer la contraseña del WiFi de la institución a través de un ataque de fuerza bruta con un diccionario de palabras.

Metodología:

- **Herramienta utilizada:** Se utilizó la herramienta "aircrack-ng" dentro de Kali Linux para realizar el ataque de fuerza bruta.
- **Diccionario de Palabras:** Se creó un diccionario de palabras con contraseñas comúnmente utilizadas, descargadas de internet y posibles contraseñas creadas a partir de scripts en Python
- **Proceso:**
    - Primero se capturó el handshake de la red inalámbrica y se lo almacenó en un archivo.
    - Con la herramienta "aitcrack-ng" y el diccionario de palabras se ejecutó el ataque para descifrar la contraseña del handshake capturado.
- **Resultados:**
    - El ataque de fuerza bruta fue exitoso y la contraseña de la red inalámbrica fue descifrada.
    - El tiempo total necesario para comprometer la contraseña dependió del tamaño del diccionario y la complejidad de la contraseña. En este caso, la contraseña fue descifrada en 2 horas aproximadamente.
    - Descifrar la contraseña de la red en tan poco tiempo demostró una vulnerabilidad significativa, ya que cualquier atacante con acceso a un diccionario robusto podría comprometer la red.

- **Conclusión:**

El resultado de este ataque destacó la importancia de utilizar contraseñas complejas y únicas para la red inalámbrica y considerar el uso de una autenticación más fuerte.

2. **Ataque de Hombre en el Medio utilizando ARP-Spoofing**

Objetivo: Interceptar y analizar el tráfico de red entre dispositivos conectados a la red mediante un ataque de Hombre en el Medio a través de la técnica de ARP-Spoofing.

- **Metodología:**
  - **Herramientas utilizadas:** Se utilizó "bettercap" como herramienta de hacking para ejecutar el ARP-Spoofing y "Wireshark" como herramienta de escaneo para capturar y analizar el tráfico de red.
- **Proceso:**
  - Se inició y configuró "bettercap" para enviar paquetes ARP falsos a un dispositivo víctima en la red provocando que sus tablas ARP se asocien con la dirección MAC de la máquina atacante.
  - Una vez ejecutado el ataque de Hombre en el Medio, se utilizó la herramienta Wireshark para capturar y analizar el tráfico de red que se transmitía a través del atacante.
- **Resultados:**
  - Se logró interceptar y capturar una cantidad significativa de tráfico de red, incluyendo credenciales de inicio de sesión y otros datos sensibles.
  - Se capturaron varias contraseñas de usuario que accedían a diferentes sitios web.
  - El análisis de tráfico capturado reveló datos sensibles transmitidos sin cifrar lo que destacó la falta de medidas de seguridad adecuadas en la red.
- **Conclusión:** El éxito del ataque de Man in the Middle con ARP-Spoofing demostró la vulnerabilidad a la red a interceptaciones de tráfico no autorizadas; así como la importancia de implementar medidas de seguridad como el cifrado de tráfico, al igual que una autenticación mutua para proteger la comunicación en la red entre dispositivos.

La siguiente tabla expresa el resumen de resultados demostrando las vulnerabilidades críticas en la red inalámbrica de la institución educativa.

Tabla 5 Resumen de resultados pruebas de penetración

Ataque de Fuerza Bruta	Ataque de Hombre en el Medio
La contraseña de la red fue comprometida en aproximadamente 2 horas.	El tráfico de red fue interceptado con éxito, incluyendo credenciales y sitios web visitados.
Resaltó la necesidad de contraseñas más fuertes y métodos de autenticación robustos.	Evidenció la falta de cifrado y medidas de seguridad adecuadas en la comunicación de la red

4.3.7.2 Sugerencias

A continuación, se detallan una serie de medidas tanto a nivel lógico como a nivel de formación de los usuarios para mejorar la seguridad de la red inalámbrica de la institución y proteger a los usuarios (alumnos, docentes y personal administrativo).

Tabla 6 Sugerencias técnicas para los dispositivos de red

Medida técnica para los dispositivos de red	Descripción	Sugerencias
Mejoras en la configuración del Hardware de red	Equipo Fortinet	• Habilitar y configurar reglas de firewall para filtrar el tráfico entrante y saliente.
	Switches Aruba	• Implementar VLANs para segmentar la red y limitar el acceso entre diferentes grupos de usuarios como alumnos, docentes, administración. • Activar funciones de seguridad avanzadas como DHCP snooping, Dynamic ARP Inspection y Port Security.
	Puntos de Acceso	• Configurar los AP con cifrados de seguridad más fuertes como WPA3
Políticas de seguridad de red	Cifrado y autenticación	• Implementar autenticación 802.1x con un servidor RADIUS para controlar el acceso a la red inalámbrica. • Utilizar certificados digitales para autenticar dispositivos y usuarios.
	Actualización y parches	• Mantener todos los dispositivos de red actualizados con los últimos parches de seguridad y firmware.

	Monitoreo y detección	• Implementar un sistema de detección de intrusos (IDS) y un sistema de prevención de intrusos (IPS) para detectar y responder a actividades sospechosas en la red.

La siguiente tabla detalla las sugerencias de seguridad para proteger a los usuarios de la red, incluyendo los alumnos, docentes y personal administrativo.

Tabla 7 Sugerencias de concienciación y formación para usuarios

Medida de concienciación y formación para los usuarios	**Sugerencias**
Capacitación en seguridad	• Chancusig Ruiz (2023) señala que una buena práctica es realizar talleres y clases educativas regulares para informar a los alumnos, docentes y personal administrativo sobre buenas prácticas de seguridad en la red (p.3). • Incluir temas como la importancia de contraseñas fuertes o cómo reconocer correos electrónicos fraudulentos.
Concienciación sobre phishing y ataques de ingeniería social	• Implementar programas de concienciación sobre phishing y otras técnicas de ingeniería social para enseñar a los usuarios a identificar y evitar ataques (Guaña-Moya et al., 2022, p. 4). • Realizar simulaciones de ataques de phishing para evaluar la eficacia de las capacitaciones y ajustar las estrategias en base a los resultados obtenidos.
Gestión de contraseñas	• Promover el uso de gestores de contraseñas para ayudar a los usuarios a crear y almacenar contraseñas fuertes y únicas. • Formular políticas relacionadas con cambios periódicos de contraseñas y que prohíban el uso de contraseñas simples o que sean fáciles de adivinar.

A través de este reporte, se aseguró de que los hallazgos y sugerencias planteadas puedan ser comunicadas de manera efectiva a todas las partes interesadas, lo que facilitará la implementación de mejores medidas de seguridad que ayudarán a fortalecer la red contra futuras amenazas y a mantener a los usuarios protegidos.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

El proyecto realizado demostró que la red inalámbrica de la unidad educativa Liceo José Ortega y Gasset presenta vulnerabilidades significativas que pueden ser explotadas a través de ataques de Hombre en el Medio, por lo que la adopción de prácticas de seguridad más fuertes y la educación continua en seguridad cibernética son pasos cruciales para mantener la red segura y resiliente.

La elección de Kali Linux como sistema operativo para la ejecución de las pruebas de penetración fue decisiva, puesto que su extensa colección de herramientas de seguridad, como Nmap, Bettercap, Wireshark, entre otras; permitieron realizar las tareas de escaneo de red, análisis de tráfico y explotación de vulnerabilidades de manera eficiente y efectiva; facilitando además el seguimiento de la metodología PTES utilizada en este estudio.

El análisis de la arquitectura de red de la institución reveló una infraestructura de red simple, de la cuál, se identificaron los activos críticos clasificándolos según su importancia y el impacto potencial de una amenaza; lo que permitió reconocer los puntos más vulnerables y cruciales de la red.

El diseño del ataque controlado de Hombre en el Medio involucró una planificación meticulosa para garantizar que la evaluación de la red se realizara de manera ética y segura; su ejecución exitosa por otro lado demostró la vulnerabilidad de la red a intercepciones no autorizadas.

El éxito del ataque de fuerza bruta utilizando un diccionario de palabras para descifrar la contraseña de la red inalámbrica evidenció una vulnerabilidad de la red inalámbrica de la institución al utilizar una contraseña débil o predecible, destacando un área crítica de mejora en sus prácticas de seguridad cibernética.

La evaluación del tráfico comprometido llevada a cabo con la herramienta Wireshark, permitió capturar y analizar paquetes de datos sensibles en detalle, evidenciando la exposición de información crítica, lo cual podría tener graves repercusiones para la institución si fuera explotada por actores malintencionados.

5.2 Recomendaciones

Para mejorar significativamente la seguridad de la red inalámbrica de la institución educativa Liceo José Ortega y Gasset, se recomienda la adquisición e implementación de un firewall robusto y de última generación, para proporcionar una capa de protección crítica, mejorando la seguridad crítica y la resiliencia de la infraestructura de TI de la institución.

Seleccionar herramientas de hacking y ciberseguridad adecuadas permitirá a la institución llevar a cabo sus propias pruebas de penetración de manera segura, mejorando de esta forma la seguridad de su red inalámbrica y mitigando posibles riesgos que se presenten a futuro.

Es indispensable contar con actualizaciones y mantenimientos continuos de los equipos de red, ya que mantener todos los dispositivos de red actualizados con los últimos parches de seguridad y firmware proporcionan la protección necesaria contra vulnerabilidades conocidas.

Se debe asegurar que tanto las comunicaciones internas como externas utilicen un cifrado seguro como HSTS o VPNs, lo que reducirá de forma significativa las vulnerabilidades de la red a intercepciones no autorizadas como ataques de Hombre en el Medio.

Se recomienda adoptar políticas de seguridad que involucren el uso obligatorio de contraseñas complejas y únicas para accesos a la red e inicios de sesión a las cuentas de los usuarios, incluyendo combinaciones de letras mayúsculas y minúsculas, números, caracteres especiales y que estas sean cambiadas cada cierto tiempo.

Para proteger de forma adecuada la red inalámbrica y los dispositivos para uso de los estudiantes o docentes de la institución educativa Liceo José Ortega y Gasset, es crucial contar con un antivirus robusto o un sistema de detección de malware que proporcionen una capa de protección adicional para mantener un ambiente de aprendizaje seguro y confiable.

BIBLIOGRAFÍA

Altube, R. (12 de noviembre de 2021). *Parrot OS: Qué es y características principales*. OpenWebinars.net. https://openwebinars.net/blog/parrot-os-que-es-y-caracteristicas-principales/

Awati, R. (2023). *Nessus*. Networking; TechTarget. https://www.techtarget.com/searchnetworking/definition/Nessus

de Zúñiga, G. (8 de junio de 2022). *¿Qué es OWASP? ¿Qué es OWASP TOP 10? | Arsys*. Blog de Arsys.es. https://www.arsys.es/blog/owasp

Fortinet. (2022). *DoS vs. DDoS: ¿Cuál es la diferencia? | Fortinet*. Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/dos-vs-ddos

GeeksforGeeks. (6 de septiembre de 2022). *Top 10 Kali Linux Tools For Hacking*. GeeksforGeeks; GeeksforGeeks. https://www.geeksforgeeks.org/top-10-kali-linux-tools-for-hacking/

GR, R. (10 de junio de 2022). *Qué es Windows Powershell y cómo puedes sacarle partido*. ADSLZone; ADSLZone. https://www.adslzone.net/esenciales/preguntas/que-es-powershell/

Hixec. (8 de abril de 2023). *BlackBuntu el Ubuntu para Hackers*. Hixec. https://archive.hixec.com/blackbuntu-el-ubuntu-para-hackers/

Hwang, D. (2021). *Red de área local o LAN*. ComputerWeekly.es; TechTarget. https://www.computerweekly.com/es/definicion/Red-de-area-local-o-LAN

Julián Pérez Porto, & Merino, M. (19 de agosto de 2011). *Red inalámbrica - Qué es, ventajas, desventajas, elementos y clasificación*. Definición.de; Definicion.de. https://definicion.de/red-inalambrica/

Kaspersky. (20 de mayo de 2024). *Más información sobre el malware y cómo proteger todos tus dispositivos*. Latam.kaspersky.com. https://latam.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

Molenaar, R. (12 de diciembre de 2023). *WPA and WPA2 4-Way Handshake*. NetworkLessons.com. https://networklessons.com/cisco/ccnp-encor-350-401/wpa-and-wpa2-4-way-handshake

Nowak, S. (28 de noviembre de 2022). *¿Qué es el Pentesting? Tipos, fases y herramientas*. Nuclio Digital School. https://nuclio.school/blog/que-es-el-pentesting/

Payo, A. (5 de agosto de 2022). *Los distintos tipos de hackers: por el color de su sombrero los conocerás*. Escudo Digital; Escudo Digital. https://www.escudodigital.com/ciberseguridad/distintos-tipos-hackers-por-color-su-sombrero-conoceras_52573_102.html

Ramiréz, I. (17 de mayo de 2024). *¿Qué es una conexión VPN, para qué sirve y qué ventajas tiene?* Xataka.com; Xataka Basics. https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

Singh, T. (30 de agosto de 2023). *What is Kali Linux? Everything to know about the popular Linux distro*. XDA Developers; XDA. https://www.xda-developers.com/kali-linux/

Trueba, J. (18 de febrero de 2022). *Guía de redes WAN: configuración y características - Tokio School*. Tokio School. https://www.tokioschool.com/noticias/guia-de-redes-wan-configuracion-y-caracteristicas/

Vienažindytė, I. (6 de febrero de 2020). *¿Qué es un pentesting, o prueba de penetración?* NordVPN; https://nordvpn.com/es/blog/que-es-el-pentesting/

Castillo, D. (2021). *Implementación de hacking ético para la evaluación de vulnerabilidades en la red de datos de una institución educativa de nivel primario.* [Tesis previo a la obtención del título de Ingeniero en Tecnologías de la Información, Universidad Estatal Provincia de Santa Elena]. Repositorio Universidad Estatal Península de Santa Elena. https://repositorio.upse.edu.ec/handle/46000/6486

Chancusig Ruiz, F. (2023). Herramientas digitales para fomentar la alfabetización mediática en la era digital. Revista Ingenio Global, 2(1), 35–45. https://doi.org/10.62943/rig.v2n1.2023.60

Cisco. (14 de enero de 2015). Guía de configuración e implementación de wIPS ELM adaptable. Cisco. https://www.cisco.com/c/es_mx/support/docs/wireless/5500-series-wireless-controllers/113027-wips-00.html

Cisco. (2022). ¿Qué es una red inalámbrica? - Cableada frente vs. inalámbrica. Cisco. https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/wireless-network.html

Fernández, Y. (20 de diciembre de 2023). Ataque Man-in-the-Middle: qué es, cómo funciona y cómo protegerte de él. Xataka.com; Xataka Basics. https://www.xataka.com/basics/ataque-man-in-the-middle-que-como-funciona-como-protegerte

Fortinet. (2022). ¿Qué es un ciberataque y los tipos de ataques en la red? | Fortinet. Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks

García, K. (2021). Aplicación de hacking ético mediante test de intrusión "pentesting" para la detección y análisis de vulnerabilidades en la red inalámbrica de una institución educativa de la provincia de Santa Elena [Tesis previo a la obtención del título de Ingeniero en Tecnologías de la Información, Universidad Estatal Provincia de Santa Elena]. Repositorio Universidad Estatal Península de Santa Elena. https://repositorio.upse.edu.ec/handle/46000/5855

Guaña-Moya, J., Chiluisa-Chiluisa, M. A., Jaramillo-Flores, P. D. C., Naranjo-Villota, D., Mora-Zambrano, E. R., & Larrea-Torres, L. G. (2022). Ataques de phishing y cómo prevenirlos. En A. Rocha, B. Bordel, F. G. Penalvo, & R. Goncalves (Eds.), *Proceedings of 2022 17th Iberian Conference on Information Systems and Technologies, CISTI 2022* (Iberian Conference on Information Systems and Technologies, CISTI; Vol. 2022-June). IEEE Computer Society. https://doi.org/10.23919/CISTI54924.2022.9820161

Guaña-Moya, J., Sánchez-Zumba, A., Chérrez-Vintimilla, P., Chulde-Obando, L., Jaramillo-Flores, P., & Pillajo-Rea, C. (2022). Ataques informáticos más comunes en el mundo digitalizado. Revista Ibérica de Sistemas e Tecnologias de Informação, 87-100. https://www.proquest.com/docview/2812112763?pq-origsite=gscholar&fromopenview=true&sourcetype=Scholarly%20Journals#

Hernandez, M. (26 de enero de 2022). Pentesting con OWASP: fases y metodología - Blog de hiberus. Blog de Hiberus. https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

IBM. (24 de abril de 2024). *¿Qué es la ciberseguridad? | IBM*. Ibm.com. https://www.ibm.com/es-es/topics/cybersecurity

incibe. (21 de agosto de 2018). *¿Qué son los ataques DoS y DDoS? | Ciudadanía | INCIBE*. Incibe.es. https://www.incibe.es/ciudadania/blog/que-son-los-ataques-dos-y-ddos

IONOS. (31 de agosto de 2023). *¿Cuáles son las distintas normas WLAN 802.11?* IONOS Digital Guide; IONOS. https://www.ionos.mx/digitalguide/servidores/know-how/ieee-80211/

Panda Security. (13 de abril de 2022). *¿Qué es un ataque Man-in-the-Middle (MITM)? Definición y prevención*. Panda Security Mediacenter. https://www.pandasecurity.com/es/mediacenter/ataque-man-in-the-middle/

Powernet. (26 de julio de 2023). *Protocolos de seguridad en las redes inalámbricas: ¿cuáles existen y en qué se diferencian?* Powernet; Powernet. https://www.powernet.es/blog/protocolos-de-seguridad-en-las-redes-inalambricas-cuales-existen-y-en-que-se-diferencian

Rudra, A. (25 de noviembre de 2022). *PowerDMARC*. PowerDMARC. https://powerdmarc.com/es/what-is-a-mitm-attack/

Sánchez, M. (7 de marzo de 2018). *Tipos de atacantes, amenazas y técnicas de ataque*. Blogspot.com. https://tichoradadams.blogspot.com/2018/12/atacantes.html

Šlekytė, I. (5 de junio de 2013). *WEP, WPA, WPA2, and WPA3: Main differences*. NordVPN; https://nordvpn.com/es/blog/wep-vs-wpa-vs-wpa2-vs-

wpa3/#:~:text=WEP%2C%20WPA%2C%20WPA2%2C%20and%20WPA3%20are%20Wi%2DFi,intruders%20can't%20read%20it.

Stechynskyi, I. (21 de diciembre de 2021). *Brute Force Attacks: Top 8 Ways to Detect & Prevent Them | Ekran System*. Ekran System. https://www.ekransystem.com/en/blog/brute-force-attacks

ANEXOS

Anexo 1: Aprobación por parte de la institución educativa

ORTEGA Y GASSET

Quito, 26 de septiembre de 2023

Señore
ENRIQUE AUGUSTO LUZURIAGA TEJADA
Presente

De mi consideración:

De acuerdo a la carta recibida el día 26 de septiembre de 2023, misma que fue emitida por el señor Enrique Augusto Luzuriaga Tejada – ex alumno de nuestra institución, en la que solicita llevar a cabo su proyecto de titulación el cual involucra la evaluación de seguridad de la red inalámbrica del Liceo, me es grato indicar que dicha solicitud ha sido aprobada; esta aprobación permite tu ingreso a las instalaciones y a la red del Liceo.

Sabemos que este proyecto será beneficioso para las dos partes y sabemos también que sabrás cumplir con todas las políticas, regulaciones y protocolos de seguridad en cualquier información sensible que este proyecto arroje.

Quedamos pendientes de los pasos a seguir para iniciar con el desarrollo del proyecto indicado.

Atentamente,
U. E. Liceo José Ortega y Gasset

Sr. Ignacio Merino
SUBDIRECTOR GENERAL

Calle E4 - De Los Cipreses N64 - 552 Teléfonos: 2 801 825 / 2 482 976 / 2 484 154 www.gasset.edu.ec
Quito-Ecuador

Anexo 2: Adaptador de red inalámbrico utilizado

La siguiente imagen muestra el adaptador de red inalámbrico que fue empleado para ejecutar las pruebas de penetración, el modelo usado fue el Atheros AR9271 que poseía un chipset compatible con Kali Linux.

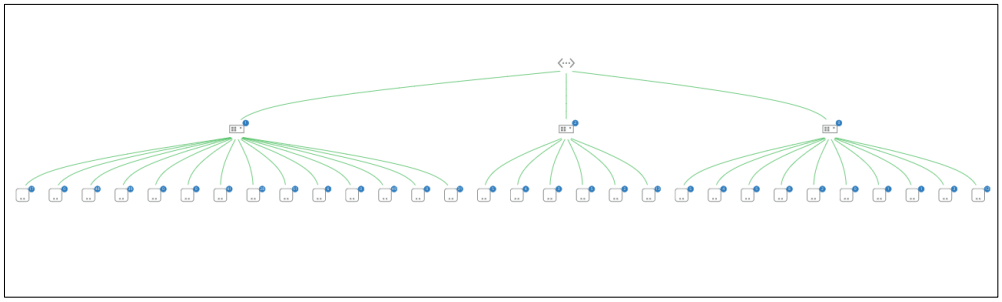
Figura 43 Adaptador de red inalámbrico usado

Anexo 3: Entrevista realizada al encargado de tecnologías de la institución

1. **¿Podría proporcionar una descripción general de la infraestructura de red de la institución, incluyendo el tipo de tecnologías utilizadas, la topología de la red y la distribución de los dispositivos?**

La infraestructura de la red inalámbrica está conformada por 1 equipo Fortinet que cumple las funciones de modem (no firewall), que provee el servicio de internet, a este equipo se conectan por fibra óptica 5 switch Aruba administrables PoE, ubicados en cada uno de los bloques (primaria, secundaria y preescolar), estos a su vez en su totalidad conectan a 35 AP Aruba y Huawei Poe. El cableado estructurado es categoría 6a.

La topología de la red es la siguiente:



2. **¿Tiene la institución políticas y procedimientos para garantizar la seguridad de la red y cuáles son?**

No.

3. **¿Qué medidas se han implementado para controlar el acceso a la red inalámbrica?**

La red inalámbrica es de uso libre, la contraseña de acceso a la red inalámbrica se entrega estudiantes, profesores y personal administrativo.

4. **¿Se utiliza algún método de autenticación, como WEP, WPA, WPA2 Enterprise, para asegurar el acceso autorizado?**

Se utiliza el método WPA/WPA2-personal.

5. **¿Se utiliza algún sistema de monitoreo de tráfico de red o de detección de intrusiones para identificar actividades maliciosas en la red?**

La red cuenta con un filtro web a través de DNS configurados en el equipo de enlace del proveedor de internet.

6. **¿Cuál es el procedimiento para responder a posibles amenazas detectadas?**

No se dispone de un procedimiento.

7. **¿Se han realizado pruebas de seguridad o evaluaciones de vulnerabilidades en la red de la institución en el pasado?**

No.

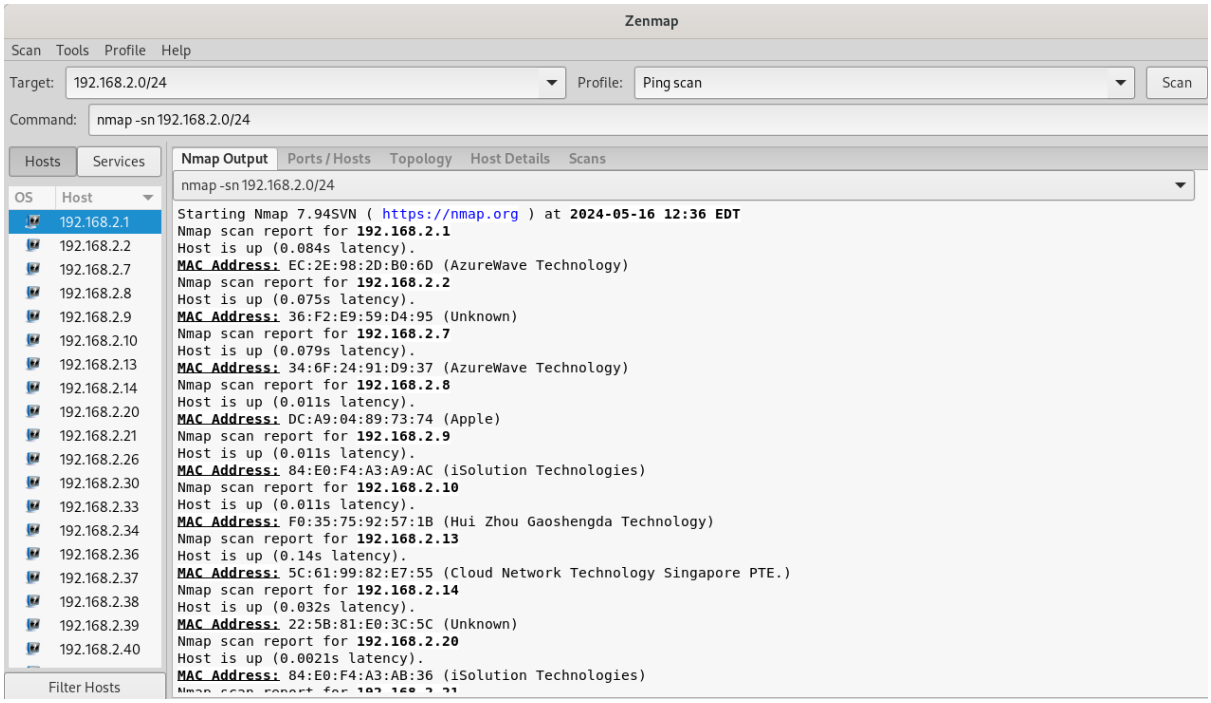
8. **¿Se proporciona capacitación y concientización sobre seguridad cibernética al personal y a los usuarios de la red?**

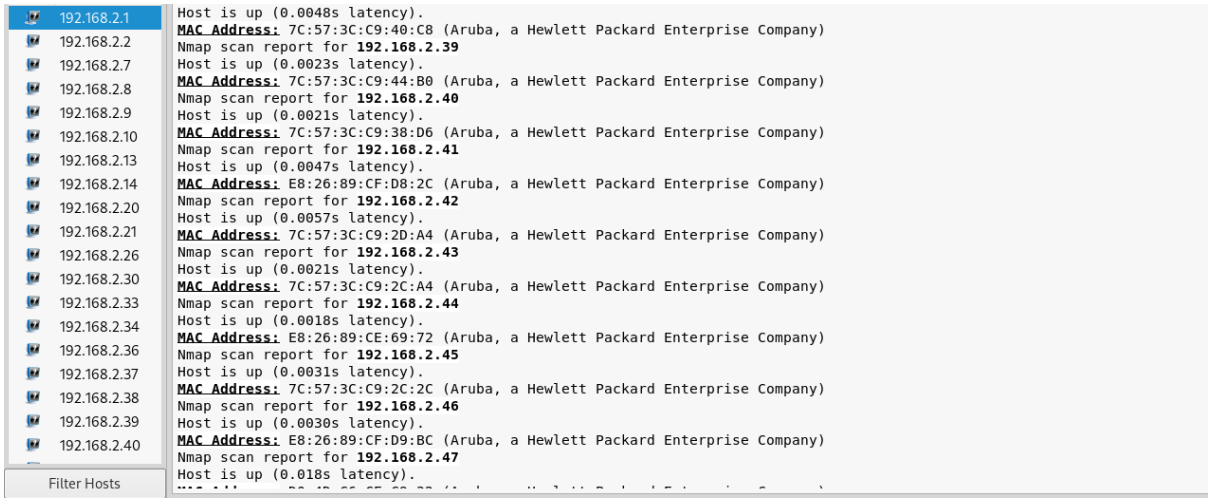
Si.

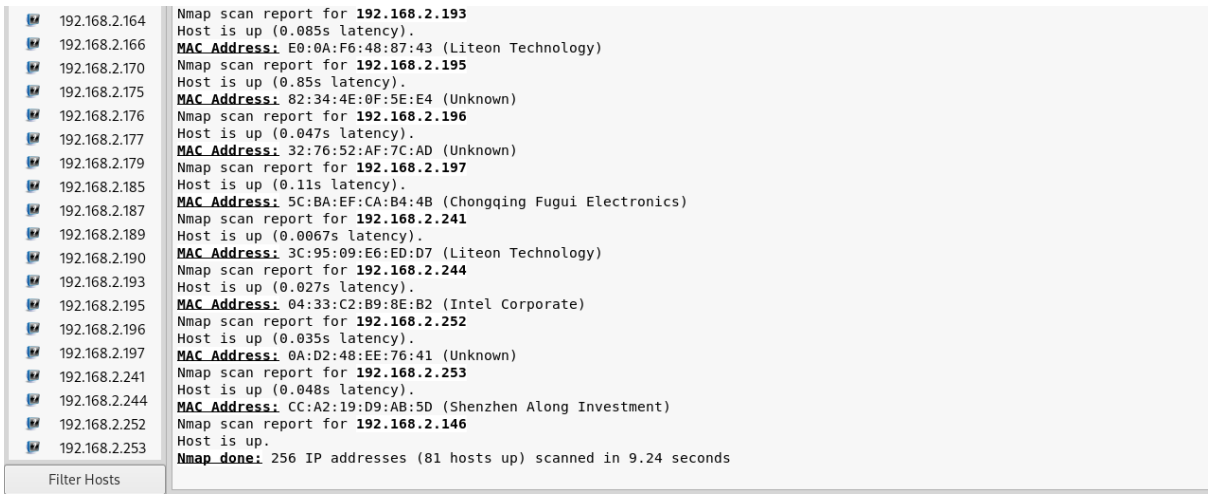
9. **¿Qué iniciativas se han implementado para promover una cultura de seguridad en la institución?**

Ninguna.

Anexo 4: Resultados Ping Scan







Anexo 5: Resultados Quick Scan Plus