

UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SOFTWARE

TRABAJO DE INTEGRACIÓN CURRICULAR
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN SOFTWARE

FORMA: PROYECTO DE INVESTIGACIÓN

TEMA:

VULNERABILIDADES EN REDES WI-FI DOMÉSTICAS Y PROPUESTA DE UNA GUÍA DE SEGURIDAD BASADO EN EL PROTOCOLO WPA-3

AUTOR:

MICHAEL JONATHAN MICHAY PINTA

DIRECTOR:

ING. DANILO GEOVANNY BARRENO NARANJO

GUARANDA – ECUADOR

2025

TEMA DEL PROYECTO DE INVESTIGACIÓN

"VULNERABILIDADES EN REDES WI-FI DOMÉSTICAS Y PROPUESTA DE UNA GUÍA DE SEGURIDAD BASADO EN EL PROTOCOLO WPA-3"

AGRADECIMIENTO

Agradezco profundamente a Dios, por ser mi guía espiritual y por darme la fortaleza necesaria para alcanzar esta meta. Su luz y compañía constante han sido fundamentales para superar cada desafío a lo largo de este camino.

Primeramente, expreso mi agradecimiento al Ing. Danilo Geovanny Barreno Naranjo, director de mi proyecto, por su valiosa orientación, paciencia y compromiso. Su guía ha sido esencial para dar forma, estructura y profundidad a este trabajo de tesis.

De manera especial, agradezco a la Universidad Estatal de Bolívar, y en particular a la Facultad de Ciencias Administrativas, Gestión Empresarial e Informática, así como a la Carrera de Ingeniería de Software, por brindarme una formación académica y de calidad. A todos los docentes, gracias por compartir sus conocimientos y experiencias, y por haber contribuido de manera significativa a mi desarrollo académico y profesional.

Extiendo también mi gratitud a mis amigos y compañeros, cuyo apoyo, compañía y amistad enriquecieron este proceso.

Este logro no es únicamente mío; es el reflejo del amor, la fe y el respaldo de todas las personas que me han acompañado. Cada palabra de aliento, cada gesto de apoyo y cada muestra de confianza fueron piezas clave en este camino. A todos ustedes, con el corazón, les doy mi más profundo y sincero agradecimiento.

DEDICATORIA

Con todo mi amor, dedico este logro a mis padres, Luis Michay y Carmen Pinta, quienes han sido el pilar fundamental de mi vida, brindándome siempre su apoyo y sus sabios consejos.

A mis hermanos Jenny, Miguel, Wilson y Marlon, así como a mi familia en general (abuelos, abuelas, tíos, tías, primos y primas) gracias por su cariño, por cada palabra de aliento y por estar presentes en los momentos importantes.

CERTIFICADO DE VALIDACIÓN

UEB
UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CERTIFICADO DE VALIDACIÓN

Ing. Danilo Geovanny Barreno, Ing. Rodrigo Del Pozo Durango e Ing. Juan Manuel Galarza, en su orden Director y Pares Académicos del Trabajo de Integración Curricular "VULNERABILIDADES EN REDES WI-FI DOMÉSTICAS Y PROPUESTA DE UNA GUÍA DE SEGURIDAD BASADO EN EL PROTOCOLO WPA-3" desarrollado por el señor **Michael Jonathan Michay Pinta.**

CERTIFICAN

Que, luego de revisado el Trabajo de Integración Curricular en su totalidad, cumple con las exigencias académicas de la carrera SOFTWARE, por lo tanto, autorizamos su presentación y defensa.

Guaranda, 25 de agosto del 2025



Danilo Geovanny Barreno
Director



Rodrigo H. Del Pozo
Par Académico



Juan Manuel Galarza
Par Académico

DERECHOS DE AUTOR

Yo Michael Jonathan Michay Pinta portador de la Cédula de Identidad No.1150867065 en calidad de autor y titular de los derechos morales y patrimoniales del Trabajo de Titulación: **VULNERABILIDADES EN REDES WI-FI DOMÉSTICAS Y PROPUESTA DE UNA GUÍA DE SEGURIDAD BASADO EN EL PROTOCOLO WPA-3**, modalidad Proyecto de Investigación, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservo a mi favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Estatal de Bolívar, para que realice la digitalización y publicación de este trabajo de titulación en el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Michael Jonathan Michay Pinta



C.I.: 1150867065

ÍNDICE DE CONTENIDO

TEMA DEL PROYECTO DE INVESTIGACIÓN..... i

AGRADECIMIENTO..... ii

DEDICATORIA..... iii

CERTIFICADO DE VALIDACIÓN..... iv

DERECHOS DE AUTOR..... v

INTRODUCCIÓN.....1

RESUMEN.....3

ABSTRACT.....4

KICHWA.....5

CAPÍTULO I.....**6**

FORMULACIÓN GENERAL DEL PROYECTO.....**6**

1.1. Descripción del Problema.....6

1.2. Formulación del Problema..... 7

1.3. Preguntas de Investigación.....7

1.4. Justificación.....7

1.5. Objetivos: General y Específicos.....9

1.6. Hipótesis.....9

1.7. Variables..... 10

CAPÍTULO II..... 11

MARCO TEÓRICO..... 11

2.1. Antecedentes..... 11

2.2. Científico..... 15

2.3. Conceptual.....16

2.4. Legal.....19

2.5. Georeferencial..... 24

CAPÍTULO III.....25

METODOLOGÍA.....25

3.1. Tipo de investigación.....25

3.2. Enfoque de la investigación.....25

3.3. Métodos de investigación.....25

3.4. Técnicas e instrumentos de recopilación de datos.....25

3.5. Universo, población y muestra.....26

3.6. Procesamiento de la información.....26

CAPÍTULO IV.....27

RESULTADOS Y DISCUSIÓN.....27

4.1. Análisis, interpretación y discusión de resultados.....27

4.1.1. *Revisión Bibliográfica*.....27

4.1.2. *Experimentación*.....33

a. *Sistema Operativo*.....33

b. *.Adaptadores Inalámbricos*.....37

c. *Router Inalámbrico*.....40

d. *Tipos de ataques en redes wifi*.....43

e. *Resultados de ataques*.....45

1. *Resultado de ataque de ingeniería social*.....45

Herramienta Utilizada.....46

Pasos a seguir.....46

2. *Resultado de ataque de diccionario*.....49

Herramienta Utilizada.....50

Pasos a seguir.....51

3. *Resultado de ataque de captura del handshake wpa/wpa2*.....54

Herramienta Utilizada.....55

Pasos a seguir.....56

4. *Resultado de ataque Evil Twin*.....61

Herramienta Utilizada.....61

Pasos a seguir.....62

5. *Resultado de ataque de desautenticación*.....65

Herramienta Utilizada.....66

Pasos a seguir.....67

6. *Resultado de ataque de punto de acceso falso*.....70

Herramienta Utilizada.....71

Pasos a seguir.....73

7. *Resultado de ataque de hombre en el medio*.....79

Herramienta Utilizada.....79

Pasos a seguir.....82

8. *Resultados de ataque de replay*.....85

Herramienta Utilizada.....85

Pasos a seguir.....87

9. *Resultados de ataque de filtrado Mac falso*.....90

Herramienta Utilizada.....90

Pasos a seguir.....91

f. *Interpretación*.....96

g. *Discusión*.....97

CAPÍTULO V.....98

PROPUESTA.....98

5.1. Guía de seguridad basada en el protocolo WPA3.....98

CONCLUSIONES.....99

RECOMENDACIONES.....100

BIBLIOGRFÍA.....101

ANEXOS.....103

INDICE DE TABLAS

Tabla 1. Variables independiente y dependiente del proyecto de investigación. 10
Tabla 2. Instrumentos de Investigación..... 28
Tabla 3. Requisitos del sistema operativo..... 33
Tabla 4. Características que se pueden conocer sobre Kali Linux..... 36
Tabla 5. Características de las tarjetas de red..... 38
Tabla 6. Comparativa de routers inalámbricos según requisitos técnicos..... 41
Tabla 7. Ataques y vulnerabilidades en redes wifi..... 43
Tabla 8. Estadística descriptiva de efectividad de ataques a redes wifi domesticas..... 95

INDICE DE FIGURAS

Figura 1. Variables independiente y dependiente.....10
Figura 2 Interfaz inicial de SET al ser ejecutado desde la terminal.....46
Figura 3 Ejecución de SET Desde la terminal.....47
Figura 4 Selección del tipo de ataque en SET.....47
Figura 5 Proceso de configuración del ataque en SET con las opciones seleccionadas y datos ingresados.....48
Figura 6 Visualización de la página clonada en el navegador, lista para capturar los datos de la víctima.....49
Figura 7 Visualización de los datos capturados de la víctima.....49
Figura 8 Interfaz inicial de CUPP al ser ejecutado desde la terminal.....51
Figura 9 Instalación de CUPP desde la terminal.....51
Figura 10 Ejecución de CUPP e Ingreso de Datos personales de la Víctima.....52
Figura 11 Visualización del Archivo Generado.....53
Figura 12 Comparación entre el contenido del diccionario generado por CUPP (izquierda) y la contraseña real registrada en la interfaz del router (derecha), donde se confirma la coincidencia.....53
Figura 13 Versión de IW al ser ejecutado desde la terminal.....55
Figura 14 Versión de AIRODUMP-NG al ser ejecutado desde la terminal.....55
Figura 15 Versión de AIREPLAY-NG al ser ejecutado desde la terminal.....56
Figura 16 Verificación del modo monitor en la tarjeta de red inalámbrica usando el comando iwconfig.....57
Figura 17 Escaneo de redes inalámbricas cercanas usando airodump-ng.....58
Figura 18 Captura del tráfico de la red objetivo mediante airodump-ng.....58
Figura 19 Ejecución del ataque de desautenticación para forzar la reconexión de un cliente.....59
Figura 20 Evidencia de la captura del handshake WPA/WPA2 en la parte superior derecha de la terminal de airodump-ng.....60
Figura 21 Visualización del archivo de captura .cap generado en el directorio de trabajo mediante el comando ls.....60
Figura 22 Versión de IW al ser ejecutado desde la terminal.....61
Figura 23 Versión de WIFIPHISHER al ser ejecutado desde la terminal.....62
Figura 24 Verificación del modo monitor en la tarjeta de red inalámbrica usando el comando iwconfig.....63
Figura 25 Ejecución de WIFIPHISHER desde la terminal de kali linux.....63
Figura 26 Lista de redes WIFI cercanas al ejecutar el ataque Wifiphisher.....64
Figura 27 Error generado por incompatibilidad del chipset RTL88x2BU.....64
Figura 28 Versión de AIRODUMP-NG al ser ejecutado desde la terminal.....66
Figura 29 Verificación del modo monitor en la tarjeta de red inalámbrica usando el comando iwconfig.....67
Figura 30 Captura del tráfico de la red objetivo mediante airodump-ng.....68
Figura 31 Captura del canal fijado con el comando sudo iwconfig wlan0.....68
Figura 32 Captura de salida en pantalla donde se muestra el envió de paquetes indicando que el ataque está activo.....69
Figura 33 Dispositivo víctima muestra desconexión repentina de la red Wi-Fi tras la ejecución del ataque.....70
Figura 34 Versión de Airbase-ng al ser ejecutado desde el terminal.....71
Figura 35 Versión de Dnsmasq al ser ejecutado desde el terminal.....72
Figura 36 Versión de Iptables al ser ejecutado desde el terminal.....72

Figura 37 Versión de Python(http.server) al ser ejecutado desde el terminal..... 72
Figura 38 Versión de IW al ser ejecutado desde la terminal..... 73
Figura 39 Verificación del modo monitor en la tarjeta de red inalámbrica usando el comando iwconfig..... 74
Figura 40 Ejecución del comando airbase-ng para crear un punto de acceso falso con el SSID En la terminal se muestra la creación de la interfaz virtual at0, indicando que la red Wi-Fi falsa ya está activa y lista para atraer víctimas.....74
Figura 41 Lista de redes wifi junto a red Falsa en la pc y teléfono..... 75
Figura 42 Configuración de IP en la interfaz at0.....75
Figura 43 Ejecución de dnsmasq para asignar IPs a dispositivos conectados..... 76
Figura 44 Ejecución de redirección con iptables.....76
Figura 45 Crear redirección del tráfico HTTP hacia tu servidor local..... 76
Figura 46 Visualización del Código del portal web falso creado en HTML..... 77
Figura 47 Visualización del servidor web activo mostrando el portal falso..... 77
Figura 48 Terminal mostrando la ejecución del servidor web en el puerto 80..... 78
Figura 49 Visualización de la página web falsa desde un navegador en un dispositivo conectado a la red falsa. El sitio se carga automáticamente al acceder a cualquier URL, redirigiendo a la IP 10.0.0.1 donde está alojado el portal HTML.....78
Figura 50 Versión de TEE al ser ejecutado desde el terminal.....79
Figura 51 Versión de CAT al ser ejecutado desde el terminal..... 80
Figura 52 Versión de NMAP al ser ejecutado desde el terminal.....80
Figura 53 Versión de arp-scan al ser ejecutado desde el terminal..... 81
Figura 54 Versión de wireshark al ser ejecutado desde el terminal..... 81
Figura 55 Ejecución de sudo desde el terminal.....82
Figura 56 Verificación del resultado en consola..... 82
Figura 57 Listado de redes escaneadas para realizar el ataque..... 83
Figura 58 Listado de redes escaneadas.....83
Figura 59 Engaño al router (10.0.2.2) haciéndole creer que es la víctima (10.0.2.3).....84
Figura 60 El atacante puede visualizar todos los paquetes intercambiados entre los dispositivos comprometidos, siempre que estos no estén cifrados adecuadamente..... 84
Figura 61 Versión de AIRODUMP-NG al ser ejecutado desde la terminal..... 86
Figura 62 Versión de AIREPLAY-NG al ser ejecutado desde la terminal.....86
Figura 63 Verificación del modo monitor en la tarjeta de red inalámbrica usando el comando iwconfig.....87
Figura 64 Captura del tráfico de la red objetivo mediante airodump-ng.....88
Figura 65 Escaneo específico sobre la red FORED-MICHAY mostrando el número de paquetes (#Data)..... 88
Figura 66 Ejecución del ataque de replay. Aireplay-ng inyectando tráfico ARP..... 89
Figura 67 Versión de AIRODUMP-NG al ser ejecutado desde la terminal..... 90
Figura 68 Versión de MACCHANGER al ser ejecutado desde la terminal.....91
Figura 69 Verificación del modo monitor en la tarjeta de red inalámbrica usando el comando iwconfig..... 92
Figura 70 Captura del tráfico de la red objetivo mediante airodump-ng..... 92
Figura 71 Falsificación exitosa de la dirección MAC..... 93
Figura 72 Conexión establecida a la red con la MAC falsificada, sin ser bloqueado por el router..... 93
Figura 73 Evidencia de conectividad a Internet después de realizar el ataque de filtrado MAC falso.....94
Figura 74 Interpretación Intelectual y Explicativa del Análisis Estadístico.....96

INTRODUCCIÓN

En la actualidad, el uso de redes Wi-Fi en entornos domésticos se ha vuelto una necesidad esencial para el acceso a internet. Sin embargo, muchas de estas redes presentan vulnerabilidades debido al uso de protocolos de seguridad obsoletos como WEP y WPA2, los cuales son susceptibles a ataques, dejando expuestos a los usuarios a tipos de ciberataques.

Frente a este panorama, surge la necesidad de adoptar nuevas tecnologías de protección, como el protocolo WPA-3, que ofrece mayores niveles de seguridad y resistencia ante ataques.

El interés por este tema surge de la creciente dependencia de las conexiones inalámbricas y la falta de adopción de medidas de protección adecuadas. Muchos usuarios desconocen que sus redes pueden ser vulnerables a ataques de fuerza bruta, interceptación de datos o suplantación, incluso cuando utilizan contraseñas aparentemente seguras.

Esta investigación busca concientizar a los propietarios de redes domésticas sobre los riesgos de seguridad asociados a protocolos obsoletos, ofreciendo una guía y aplicar configuraciones seguras. Al adoptar estas medidas, los usuarios podrán reducir significativamente la inseguridad en sus redes, protegiendo sus datos y dispositivos contra accesos no autorizados y ciberataques.

Para llevar a cabo esta investigación, se empleó una metodología de tipo cuasi-experimental y aplicada, combinando revisión bibliográfica con pruebas controladas de seguridad en redes Wi-Fi domésticas. Se utilizó el enfoque inductivo, mediante el cual, a partir del análisis de casos particulares, se identificaron patrones comunes de vulnerabilidad.

Asimismo, se llevaron a cabo ataques controlados en entornos reales utilizando herramientas como Kali Linux, que permitieron analizar las debilidades de los protocolos antiguos.

El propósito principal del trabajo es diseñar una guía de seguridad basada en el protocolo WPA-3 para que los usuarios puedan mitigar los riesgos asociados al uso de redes Wi-Fi inseguras en el entorno doméstico. Para ello, se establecieron tres objetivos específicos: identificar las vulnerabilidades más comunes en redes domésticas, evaluar el impacto de los protocolos obsoletos frente a WPA-3, y proponer recomendaciones claras y prácticas para mejorar la protección de estas redes.

Este documento está estructurado en varios capítulos que abordan progresivamente el desarrollo del tema. En el primer capítulo se plantea el problema de seguridad en redes

Wi-Fi domésticas, evidenciando los riesgos que genera el uso de protocolos obsoletos.

El segundo capítulo describe los antecedentes investigativos y las bases científicas relacionadas.

En el tercer capítulo se detalla la metodología implementada. Finalmente, se expone una propuesta de guía práctica que incluye recomendaciones y pasos específicos para que los usuarios puedan implementar mejores prácticas de seguridad en sus redes Wi-Fi domésticas.

RESUMEN

El presente trabajo de investigación tuvo como objetivo general analizar las vulnerabilidades en redes Wi-Fi domésticas y diseñar una guía de seguridad basada en el protocolo WPA-3 para mitigarlas.

La metodología empleada fue cuasi-experimental y aplicada, con enfoque mixto, incluyendo revisión bibliográfica y experimentación mediante ataques controlados en redes propias utilizando herramientas de auditoría como Kali Linux, y observación directa de los efectos de cada prueba.

Los principales resultados demostraron que las redes que empleaban protocolos obsoletos, como WEP y WPA, eran altamente vulnerables a intrusiones no autorizadas, mientras que las redes con WPA-3 y configuraciones adecuadas mostraron una reducción significativa de los riesgos, Se validó la hipótesis de que la implementación de un modelo de seguridad basado en el protocolo WPA-3 en redes Wi-Fi domésticas en Ecuador reduce significativamente las vulnerabilidades existentes.

Se concluye que el protocolo WPA-3 representa una medida efectiva para la protección de redes domésticas; sin embargo, su eficacia depende de una correcta configuración del router, la actualización continua del firmware y la concienciación del usuario sobre buenas prácticas de seguridad. además, se evidencia la importancia de combinar tecnología avanzada con buenas prácticas de seguridad en entornos hogareños. Entre las recomendaciones se incluyen migrar a routers compatibles con WPA-3, desactivar funciones inseguras, utilizar contraseñas robustas y fomentar la educación básica en ciberseguridad.

Palabras clave: seguridad informática, redes Wi-Fi, WPA-3, ciberseguridad.

ABSTRACT

This research aimed to analyze vulnerabilities in domestic Wi-Fi networks and to design a security guide based on the WPA-3 protocol to mitigate them. The methodology employed was quasi-experimental and applied, with a mixed approach, including a literature review and experimentation through controlled attacks on proprietary networks using auditing tools such as Kali Linux, as well as direct observation of the effects of each test. The main results showed that networks using outdated protocols, such as WEP and WPA, were highly vulnerable to unauthorized intrusions, while networks with WPA-3 and proper configurations exhibited a significant reduction in risks. The hypothesis—that implementing a security model based on the WPA-3 protocol in domestic Wi-Fi networks in Ecuador significantly reduces existing vulnerabilities—was validated.

It is concluded that the WPA-3 protocol constitutes an effective measure for protecting domestic networks; however, its effectiveness depends on correct router configuration, continuous firmware updates, and user awareness of good security practices. Furthermore, the study highlights the importance of combining advanced technology with proper security habits in home environments. Recommendations include migrating to WPA-3 compatible routers, disabling insecure functions, using strong passwords, and promoting basic cybersecurity education.

Keywords: information security, Wi-Fi networks, WPA-3, cybersecurity.

KICHWA

Kay kunan yachay maskay llamkayqa huk objetivo general hina karqa, llaqta ukhupi Wi-Fi llikakunapi vulnerabilidades nisqakunata qawarinapaq, chaynallataqmi huk guía de seguridad nisqa ruwaypaq, chay protocolo WPA-3 nisqapi, chaykunata pisiyachinapaq. Kay metodología llamk'achisqa karqa cuasi-experimental chanta aplicasqa, kay mixto enfoque kaqwan, kay revisión bibliográfica kaqwan chanta experimentación kaqwan kay ataques controlados kaqwan kikin llikakunapi kay herramientas de auditoría kaqwan kay Kali Linux kaqwan, chanta kay directa observación kaqmanta kay efectos sapa prueba kaqmanta. Chay hatun ruwaykunan rikuchirqan chay llikakuna protocolos obsoletos nisqakunata utilizaq, ahinataq WEP hinallataq WPA nisqakuna, ancha vulnerables karqanku mana autorizasqa intrusiones nisqakunaman, hinallataq llikakuna WPA-3 nisqawan hinallataq allin churasqakuna rikuchirqanku huk hatun pisiyayta riesgokunapi, chay hipótesis nisqa, chay implementación nisqa huk modelo de seguridad nisqapi, protocolo WPA-3 nisqapi, Emcuador suyupi Wi-Fi nisqa llikakunapi, valido karqan kunan kaqkunapi.

Concluye que el protocolo WPA-3 representa una medida efectiva para la protección de las redes nacionales; Ichaqa, allin ruwayninqa huk allin router ruwanamanta, sapa kuti firmware musuqyachiymanta chaymanta llamk'aqpa riqsichiyninmanta allin waqaychasqa ruwaykunamanta. Hinallataq, ñawpaq tecnologiata allin waqaychasqa ruwaykunawan wasi pachakunapi allin waqaychasqa ruwaykunawan tupachiyqa ancha allinmi. Kay yuyaychakuykuna WPA-3 tupaq routerkunaman astakuy, mana seguro ruwanakunata mana llamk'achiy, sinchi contraseñakuna llamk'achiy chaymanta ciberseguridad básica yachachiyta kallpachay.

Sapaq simikuna: computadora seguridad, Wi-Fi llikakuna, WPA-3, ciberseguridad.

CAPÍTULO I

FORMULACIÓN GENERAL DEL PROYECTO

1.1. Descripción del Problema

En los últimos años, especialmente desde la pandemia de COVID-19, el uso del servicio de internet ha crecido significativamente en Ecuador debido a la necesidad de teletrabajo, educación en línea y entretenimiento digital. Según el INEC (2023), "el 60,5% de los hogares ecuatorianos tienen internet fijo, un aumento considerable en comparación con el 13% en 2010". La expansión ha sido posible gracias a la creciente oferta de dispositivos tecnológicos económicos, en su mayoría importados de China.

Sin embargo, este aumento en la conectividad ha traído consigo problemas de seguridad en redes Wi-Fi domésticas, ya que muchas personas no cuentan con conocimientos técnicos suficientes para configurar adecuadamente sus redes. Como resultado, muchas redes son vulnerables a ataques informáticos.

El problema radica en la falta de seguridad en redes Wi-Fi domésticas, lo que exponen a los usuarios a diversas amenazas cibernéticas. Las causas principales de esta vulnerabilidad incluyen:

Uso de protocolos de seguridad obsoletos como WEP y WPA, que pueden ser fácilmente comprometidos.

Configuraciones predeterminadas de los routers, como contraseñas débiles o nombres de redes que revelan información innecesaria;

Falta de concienciación y conocimientos técnicos por parte de los usuarios, quienes no implementan medidas de seguridad básicas.

Las consecuencias de esta inseguridad incluyen accesos no autorizados a las redes, robo de información sensible, ataques de malware y posibles afectaciones a la privacidad de los usuarios.

Si no se toman medidas correctivas, es probable que la inseguridad en las redes Wi-Fi domésticas continúe creciendo, lo que podría derivar en:

Un aumento en los ataques cibernéticos dirigidos a hogares, afectando la privacidad y los datos personales de los usuarios.

Para mitigar este problema, es fundamental promover la educación sobre seguridad en redes, actualizar los protocolos de seguridad utilizados en los routers y fomentar la implementación de buenas prácticas en la configuración de redes domésticas.

1.2. Formulación del Problema

¿Cómo las vulnerabilidades en redes Wi-Fi domésticas pueden ser mitigadas mediante la implementación de una guía de seguridad basada en el protocolo WPA-3?

1.3. Preguntas de Investigación

¿Cuáles son las vulnerabilidades más comunes en redes Wi-Fi domésticas?

¿Qué impacto tiene el uso de protocolos obsoletos como WEP, WPA y WPA-2 en la seguridad de las redes?

¿Cómo puede el protocolo WPA-3 mejorar la seguridad en redes domésticas?

¿Qué prácticas y pasos específicos pueden implementar los usuarios para proteger sus redes Wi-Fi?

1.4. Justificación

Actualmente, la seguridad en redes Wi-Fi se ha vuelto una preocupación, debido a su uso excesivo en la vida diaria. De acuerdo a Iturralde Piedra, Daniel Esteban Vázquez, Luis Miguel " Wi-Fi es una de las tecnologías más utilizadas en el mercado. Se implementa en hogares, universidades, negocios, empresas, entre otros. Al ser una tecnología de comunicación inalámbrica, brinda facilidad y comodidad a los usuarios, pero también expone la información que se está transmitiendo". A pesar de los avances tecnológicos, muchas personas no configuran adecuadamente sus routers debido a la falta de conocimiento, lo que las deja expuestas a ciberataques, accesos no autorizados y robo de información.

Además de proponer un modelo de seguridad basado en el protocolo WPA-3, el cual ofrece una protección superior en comparación con sus predecesores (WEP, WPA y WPA-2) y reduce significativamente el riesgo de ataques, es importante reconocer que ninguna red o sistema puede considerarse completamente seguro.

Según María Fernández y Olivia Madrigal (2020), en su tesis" VULNERABILIDADES EN REDES WIFI", trabajo realizado en la Universidad de Catalunya nos manifiestan que:

> Ninguna red o sistema es cien por ciento seguro, como lo demuestran los ataques zero-day ocurridos a lo largo de la historia. Un ataque zero-day explota vulnerabilidades desconocidas tanto para los usuarios como para los fabricantes del producto, lo que los convierte en una de las amenazas más peligrosas, aunque poco comunes. Un ejemplo de ello es el ataque de

Stuxnet en 2010, que logró infectar la central nuclear de Natanz en Irán.

En este contexto, la implementación de WPA-3 no solo refuerza la seguridad en entornos domésticos, sino que también contribuye a crear conciencia sobre las mejores prácticas en ciberseguridad, ayudando a minimizar vulnerabilidades y mitigar riesgos.

línea de investigación:

Dominio	Línea	
Tecnologías de la Información y Comunicación	Gestión De Tecnologías de la Información y Comunicación	
	Ingeniería De Software, Redes y Telecomunicaciones	**x**
	Educación Virtual, Teleeducación	
	Big Data, Cloud Computing, Gestión de Datos e Inteligencia Artificial	
	Geomática	

Sublínea	Pruebas y aseguramiento de la calidad del software, redes y telecomunicaciones.

1.5. Objetivos: General y Específicos

General

Diseñar una guía de seguridad basado en el protocolo WPA-3 para mitigar las vulnerabilidades en redes WI-FI domésticas

Específicos

- Identificar las vulnerabilidades y riesgos más comunes en redes Wi-Fi domésticas mediante análisis técnico y revisión bibliográfica.
- Evaluar el impacto de los protocolos de seguridad obsoletos y la efectividad del protocolo WPA-3 en la protección de redes Wi-Fi.
- Desarrollar una serie de recomendaciones y pasos específicos para que los usuarios puedan mejorar la seguridad de sus redes Wi-Fi domésticas.

1.6. Hipótesis

La implementación de un modelo de seguridad basado en el protocolo WPA-3 en redes Wi-Fi domésticas en Ecuador reduce las vulnerabilidades actuales, mitigando los riesgos de ataques cibernéticos, robo de información y violaciones de privacidad, especialmente en el contexto del aumento del uso de internet post-pandemia.

- La falta de conocimientos técnicos en los usuarios es un factor determinante en la configuración insegura de redes Wi-Fi domésticas, lo que incrementa su exposición a ataques cibernéticos.
- Las redes W-Fi domésticas que utilizan protocolos obsoletos (WEP, WPA, WPA-2) presentan un mayor número de vulnerabilidades en comparación con aquellas que implementan el protocolo WPA-3.
- La implementación de prácticas, como la actualización de contraseñas y la configuración adecuada de enrutadores, disminuye la vulnerabilidad de las redes Wi-Fi domésticas frente a ataques.

1.7. Variables

Tabla 1

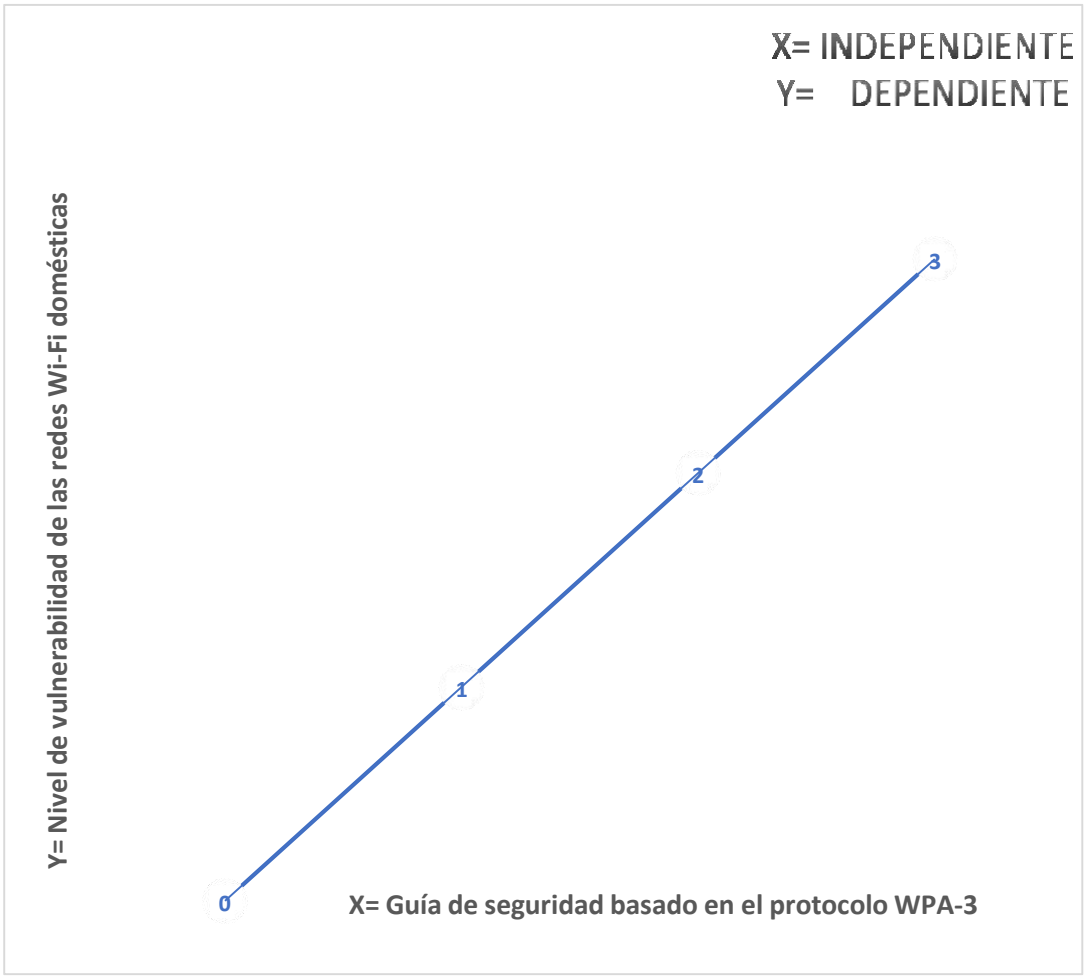
Variables independiente y dependiente del proyecto de investigación

Variable	Tipo	Descripción
Guía de seguridad basado en el protocolo WPA-3	Independiente	Uso del protocolo WPA-3 en redes Wi-Fi domésticas para mejorar la seguridad.
Nivel de vulnerabilidad de las redes Wi-Fi domésticas	Dependiente	Grado de exposición de las redes Wifi a ataques cibernéticos.

Nota. Esta tabla presenta una descripción detallada de las variables que serán analizadas y aplicadas en el proceso de investigación.

Figura 1

Variables independiente y dependiente.



Nota. El gráfico muestra la relación entre la aplicación del protocolo WPA-3 y la disminución del nivel de vulnerabilidad de las redes Wi-Fi domésticas.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes

A través de la revisión bibliográfica de tesis, artículos científicos y otros trabajos académicos, se ha encontrado información relevante que contribuye significativamente al desarrollo y fundamentación de la presente investigación.

Según Hernández Ramírez Cristian Sebastián, en su tesis "DISEÑO E IMPLEMENTACIÓN DE UNA RED INALÁMBRICA WI-FI 5 CON EL PROTOCOLO DE AUTENTICACIÓN WPA3 PARA UN POSTERIOR ANÁLISIS DE VULNERABILIDADES EN EL CAMPUS UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA DEL NORTE", trabajo realizado en la Universidad Técnica del Norte concluyó:

En evidenciar la robustez que ofrece el protocolo WPA3 en términos de integridad y privacidad dentro de redes inalámbricas, en comparación con sus predecesores, al incorporar una capa adicional de seguridad que refuerza la protección frente a ataques cibernéticos.

Asimismo, dado que el protocolo RADIUS constituye una solución eficaz para el control de acceso en redes inalámbricas, ya que asegura la autenticación, autorización y el registro de usuarios, se considera relevante su análisis. En este contexto, Freeradius se presenta como una opción funcional para la realización de pruebas en investigaciones, ya que es un software de código abierto, ligero en cuanto a consumo de recursos, con amplias posibilidades de configuración y gran compatibilidad.

Por otro lado, la vulnerabilidad KRACK afecta la seguridad de las redes Wi-Fi al explotar fallas en la implementación del protocolo de cifrado, comprometiendo tanto el cliente como el punto de acceso. Aunque existen actualizaciones que corrigen esta falla, la responsabilidad recae en los usuarios, quienes deben aplicar dichos parches para prevenir riesgos.(2024, p. 167)

Según Vivar Franco Itaty Andreina, en su tesis "APLICACION DE HACKING ETICO PARA IDENTIFICAR AMENAZAS, RIESGOS Y VULNERABILIDADES EN LA RED WI-FI", trabajo realizado en la Universidad Técnica de Babahoyo concluyó que:

El uso de protocolos inseguros como SSL y TLS 1.1, junto con versiones desactualizadas de software como OpenSSL, expone a los sistemas a vulnerabilidades críticas debido a la falta de mecanismos criptográficos actualizados. En este contexto, el hacking ético se presenta como una herramienta fundamental para identificar estas debilidades antes de que puedan ser explotadas, permitiendo implementar medidas preventivas y fortalecer la seguridad de las redes.(2023, p. 36)

Según Olivia Madrigal y María Fernández, en su tesis "VULNERABILIDADES EN REDES WI-FI", trabajo realizado en la Universidad Oberta de Catalunya concluyó que:

Es fundamental implementar medidas de seguridad. a redes Wi-Fi como el uso de contraseñas seguras, que incluyan una combinación aleatoria de letras mayúsculas, minúsculas, números y caracteres especiales; y se recomienda evitar el uso del estándar WPS, debido a sus vulnerabilidades asociadas al acceso mediante PIN débiles o métodos alternativos como PBC, NFC o USB. Además, se enfatiza la necesidad de mantener siempre actualizados los dispositivos y de evitar compartir contraseñas a través de sitios web o aplicaciones no confiables. Como medidas complementarias, se sugiere implementar el filtrado por direcciones MAC y realizar un monitoreo constante de la red. Finalmente, se reconoce que el ámbito de la ciberseguridad, y en particular la seguridad en redes Wi-Fi, se encuentra en constante evolución. Las vulnerabilidades nuevas emergen a medida que las anteriores son corregidas, lo que exige un monitoreo y estudio permanente.(2020, p. 75)

Según Luis Miguel Serrano Vázquez, en su tesis "DEMOSTRACIÓN Y ANÁLISIS DE VULNERABILIDADES EXISTENTES EN REDES WI-FI Y RECOMENDACIONES DE SEGURIDAD", trabajo realizado en la Universidad del Azuay concluyó que:

Si bien la tecnología Wi-Fi ofrece facilidad y comodidad en su implementación en diversos entornos como hogares, universidades y empresas, también representa un riesgo para la seguridad de la información transmitida debido a su naturaleza inalámbrica. Por ello, es fundamental garantizar la confidencialidad, integridad y disponibilidad de las comunicaciones. A través del análisis de los protocolos de seguridad Wi-Fi, desde los más antiguos e inseguros como WEP y WPA, hasta los más modernos y confiables como WPA-2 y WPA-3.

Asimismo, mediante pruebas prácticas realizadas en una red de laboratorio, evidenció las debilidades presentes en cada protocolo. Finalmente, propuso una serie de medidas de

mitigación, recomendaciones de configuraciones seguras en los dispositivos, y resaltó la importancia de utilizar protocolos actualizados y reforzar la seguridad a través de técnicas complementarias y actualizaciones constantes de los equipos.(2022, p. 2)

De acuerdo con Jefferson Vite, Jhonatan Chema, Karen Vite y Freddy Núñez, en su artículo publicado en la revista científica "EVALUACIÓN DE VULNERABILIDADES Y MÉTODOS DE PROTECCIÓN", se manifiesta que la identificación de vulnerabilidades en los sistemas de comunicación inalámbrica es un proceso esencial para garantizar la seguridad de la información. Los autores destacan que, a medida que las tecnologías evolucionan, también lo hacen los métodos de ataque, lo que exige una actualización constante de las medidas de protección. Además, recalcan la importancia de aplicar protocolos de seguridad robustos, realizar auditorías periódicas y concienciar a los usuarios sobre las mejores prácticas para minimizar los riesgos.(2025a, p. 12)

Eugenio Rafael Mora Zambrano, en su artículo publicado en la revista *INSTA Magazine* titulado *"*ANÁLISIS DE VULNERABILIDADES EN REDES INALÁMBRICAS: MÉTODOS Y SOLUCIONES*"*, manifiesta que, además de las soluciones técnicas, la concienciación y capacitación del personal son fundamentales en la defensa contra ciberataques. Señala que educar a los usuarios sobre buenas prácticas, como el uso de contraseñas seguras y la identificación de amenazas potenciales, contribuye significativamente al fortalecimiento de la postura de seguridad de una organización. Se sugiere poner en marcha programas de formación en ciberseguridad dirigidos a usuarios, además de desarrollar campañas informativas que promuevan la conciencia sobre los peligros vinculados al uso de redes Wi-Fi..(2024, p. 4)

Según Javier Esteban Sánchez, en su tesis "SEGURIDAD ACTUAL EN REDES WI-FI", trabajo realizado en la Universidad Politécnica de Madrid concluyó que:
La evolución de los protocolos de seguridad, como el paso de WPA-2 a WPA-3, representa un avance significativo en la protección de las redes inalámbricas. No obstante, ningún sistema es completamente seguro. La seguridad efectiva no depende únicamente de los protocolos implementados, sino también de la correcta configuración de los dispositivos, la actualización continua de firmware, y, fundamentalmente, de la concienciación del usuario frente a las amenazas persistentes como los ataques de suplantación y la ingeniería social.(2021, p. 73)

Según Alexis Vicente Pardo Sánchez, en su tesis “ESTUDIO DE VULNERABILIDADES EN EL SISTEMA DE SEGURIDAD WPA-2 PERSONAL DEL ESTÁNDAR IEEE 802.11I Y PROPUESTAS DE MEJORAS A CONSIDERAR EN EL SISTEMA WPA”, trabajo realizado en la Universidad Nacional de Loja, se concluyó que:

El sistema de seguridad WPA-2 Personal, aunque representa una evolución significativa respecto a versiones anteriores de protección en redes inalámbricas, aún presenta vulnerabilidades importantes que pueden ser explotadas mediante ataques como fuerza bruta, diccionario, e interceptación del handshake de autenticación. Durante la investigación se evidenció que la dependencia de una clave precompartida (PSK) representa un riesgo considerable, ya que la seguridad depende directamente de la complejidad de la contraseña elegida por el usuario.

Asimismo, se constató que las fallas en el proceso de autenticación permiten que, mediante el análisis del tráfico capturado, un atacante pueda intentar adivinar la clave utilizando técnicas relativamente accesibles con herramientas públicas. El estudio resalta la necesidad de fortalecer las configuraciones de red, no solo mediante la elección de contraseñas más robustas, sino también implementando medidas adicionales como la desactivación del WPS, la actualización frecuente de firmware, y la segmentación de redes para mitigar posibles daños en caso de intrusión.

Finalmente, se propone considerar mejoras al sistema actual que incluyan métodos de autenticación más seguros y dinámicos, la adopción de protocolos más recientes como WPA-3, y la concienciación del usuario como un componente esencial para la protección efectiva de las redes inalámbricas.(2022, p. 130)

La revisión de antecedentes evidencia que, si bien el protocolo WPA-3 ofrece mejoras significativas en la seguridad de redes Wi-Fi, su eficacia depende de una implementación adecuada, configuraciones seguras, actualizaciones constantes y la capacitación de los usuarios. Los estudios destacan que las amenazas evolucionan continuamente, por lo que es esencial la actualización constante de dispositivos y la concienciación de los usuarios.

2.2. Científico

El desarrollo de las redes Wi-Fi ha transformado la conectividad en hogares, permitiendo el acceso a internet sin la necesidad de cables. Sin embargo, esta flexibilidad ha traído consigo vulnerabilidades en la seguridad de la información transmitida. La falta de configuraciones adecuadas y el uso de protocolos inseguros han sido factores determinantes en la creciente exposición a ataques cibernéticos.

Según LA VANGUARDIA, desde la pandemia de COVID-19, los ataques cibernéticos han aumentado en un 25%, afectando tanto a empresas como a usuarios domésticos. Estas amenazas provienen, en su mayoría, de actores estatales y grupos organizados ubicados en Rusia, China y, en menor medida, Vietnam. Esto demuestra que el crecimiento en los ataques evidencia la necesidad de implementar protocolos de seguridad más robustos y concienciar a los usuarios sobre la importancia de proteger sus redes Wi-Fi.

Por otro lado, la Wi-Fi Alliance, una organización sin fines de lucro, ha sido clave en la certificación y promoción de estándares de interoperabilidad para garantizar una conexión segura y eficiente. Compañías como Apple, Samsung, Sony, LG, Cisco, Broadcom, Intel, Qualcomm, Motorola y Microsoft han respaldado esta iniciativa, contribuyendo significativamente al avance y desarrollo de la tecnología Wi-Fi.

Gracias a este esfuerzo, en 1999, un grupo de investigación conformado por 3Com, Lucent y Nokia desarrolló el estándar IEEE 802.11, el cual permitió la transmisión inalámbrica de información en entornos domésticos y empresariales. Inicialmente, la velocidad de transmisión era de apenas 1 a 2 Mbps, en comparación con los 10 Mbps de la Ethernet clásica. No obstante, la posibilidad de conectividad sin cables propició su adopción masiva y el posterior desarrollo de versiones más avanzadas.

Además, en el año 2000, el grupo WECA certificó la interoperabilidad de la versión 802.11b, comercialmente conocida como Wi-Fi, permitiendo que dispositivos de diferentes fabricantes pudieran conectarse sin problemas. Desde ese momento, las redes inalámbricas han experimentado un notable desarrollo, llegando a ser una herramienta fundamental en las comunicaciones actuales.

En la actualidad, una red Wi-Fi básica, denominada Basic Service Set (BSS), se compone de tres elementos principales: los dispositivos finales (STA), el punto de acceso (AP) y la puerta de enlace (Gateway). Sin embargo, con los avances tecnológicos, el AP y el Gateway han sido integrados en un solo dispositivo, el router inalámbrico, facilitando así la configuración y gestión de la red (Rawat et al., 2014).

A medida que la adopción de redes inalámbricas ha crecido, también han surgido

preocupaciones sobre su seguridad. Para abordar estos riesgos, se han desarrollado diversos protocolos de seguridad diseñados para proteger la transmisión de datos.

El primero de estos fue el WEP, basado en cifrado RC4, que, aunque revolucionario en su momento, resultó ser altamente vulnerable a ataques criptográficos. Como medida de respuesta, se implementó el protocolo WPA, el cual integró un sistema de cifrado dinámico basado en TKIP (Protocolo de integridad de clave temporal).

Posteriormente, surgió el WPA-2, que implementó el cifrado, lo que mejoró significativamente la seguridad en redes inalámbricas.

Más recientemente, se desarrolló el WPA-3, el cual utiliza el protocolo SAE para prevenir ataques de diccionario y ofrecer mayor protección en redes públicas.

No obstante, a pesar de los avances en los protocolos de seguridad, muchas redes domésticas continúan operando con configuraciones predeterminadas inseguras, lo que las hace vulnerables a accesos no autorizados y ataques cibernéticos.

Entre las amenazas más comunes se encuentran la intercepción de datos sensibles debido a la falta de cifrado adecuado, accesos no autorizados que permiten el uso indebido de la red por parte de terceros y ataques de malware que comprometen la seguridad de los usuarios.

Por lo tanto, es fundamental adoptar medidas de seguridad como el uso de protocolos modernos, la actualización de credenciales predeterminadas del router, la desactivación de la difusión del SSID, la implementación de contraseñas robustas y la configuración de firewalls para restringir el acceso no autorizado.

2.3. Conceptual

Redes de Computadoras

Una red está compuesta por computadoras y dispositivos informáticos interconectados, permitiendo el intercambio de información. Se distinguen redes cableadas e inalámbricas, siendo estas últimas el foco de este estudio debido a su amplia adopción en entornos domésticos y la creciente demanda de medidas que garanticen su seguridad frente a posibles vulnerabilidades(IBM, 2021).

Tipos de Redes según su Cobertura Geográfica:

El tipo de red según su cobertura geográfica hace referencia a la clasificación de las redes

de comunicación en función del área o distancia que abarcan para conectar dispositivos. Esta clasificación permite identificar las características, el alcance y el propósito de cada tipo de red.

- **LAN** (Red de Áreas Locales): Red básica utilizada en espacios reducidos como una vivienda o una oficina, generalmente mediante cables(Cloudflare, s. f.-a)
- **WLAN** (Red de área local inalámbrica): Similar a la LAN, pero su transmisión se realiza a través de ondas de radio, mundialmente conocidas como Wi-Fi, eliminando la necesidad de cables físicos(Brañez Grau, 2024).
- **MAN** (Red del Área Metropolitana): Red que cubre áreas más amplias, como una ciudad completa(Cloudflare, s. f.-b)
- **WAN** (Red de área amplia): Red de gran alcance que conecta varias redes LAN o MAN a través de dispositivos llamados routers, que permiten el enrutamiento y direccionamiento de la información(AWS, s. f.).
- **VLAN** (Red de área local virtual): Red virtual que permite segmentar redes físicas en lógicas, optimizando la administración y seguridad de los dispositivos conectados(TechTarget, s. f.).

Tipos de protocolos de seguridad Wi-Fi

Según Villar Pineda (2024), los protocolos de seguridad Wi-Fi han evolucionado con el objetivo de proteger las redes inalámbricas mediante el cifrado de los datos transmitidos, incorporando mejoras progresivas en cada versión. El protocolo WEP, introducido en 1997, ofrecía un nivel de seguridad muy bajo debido a su cifrado estático fácilmente vulnerable, por lo que actualmente se considera obsoleto y no recomendable. En 2003 surgió WPA, que representó una mejora respecto a WEP, aunque también presentaba vulnerabilidades conocidas, lo que llevó a su desuso. Un año después apareció WPA2, que implementó cifrado AES y elevó la seguridad a un nivel medio, siendo aún ampliamente utilizado, aunque ya se han identificado fallas que lo vuelven vulnerable ante ataques avanzados. Finalmente, en 2018 se lanzó WPA3, considerado el estándar más seguro hasta la fecha, con cifrado reforzado, protección contra ataques por diccionario y forward secrecy, por lo que es el protocolo recomendado en la actualidad para redes domésticas y empresariales.

Importancia del protocolo WPA-3

WPA-3 es el protocolo de seguridad más reciente desarrollado por la Wi-Fi Alliance, y representa una mejora significativa frente a sus antecesores. Este protocolo ofrece:

Cifrado más fuerte para proteger los datos transmitidos, incluso si un atacante logra capturar el tráfico.

Protección contra ataques de diccionario, que intentan adivinar contraseñas débiles.

Mayor seguridad en redes abiertas (sin contraseña) mediante el cifrado individualizado de conexiones.

Forward secrecy, una técnica que garantiza que si una clave se ve comprometida, no se puedan descifrar sesiones anteriores.

Gracias a estas características, WPA-3 es la mejor opción para proteger redes Wi-Fi domésticas.(Celi et al., 2025b)

Seguridad Informática y Ciberseguridad

La seguridad informática comprende todas las medidas, políticas y tecnologías destinadas a proteger sistemas, redes, dispositivos y datos frente a accesos no autorizados, daños o robos según(Corvo & María, 2023) Dentro de este campo se encuentra la ciberseguridad, orientada a defenderse contra amenazas digitales como malware, phishing o ransomware. En redes Wi-Fi domésticas, la vulnerabilidad se refiere a debilidades en su configuración o en los protocolos de seguridad, que pueden ser explotadas por atacantes para interceptar o comprometer información.

Principales Amenazas a Redes Wi-Fi

Las redes Wi-Fi, al ser sistemas de comunicación inalámbrica, están expuestas a múltiples riesgos de seguridad que pueden comprometer la confidencialidad, integridad y disponibilidad de la información transmitida. Estas amenazas provienen tanto de atacantes externos como internos, y se aprovechan de vulnerabilidades en la configuración, protocolos, dispositivos o incluso del factor humano(Zambrano, 2024). Entre las amenazas más comunes se encuentran:

- **Malware**: Software malicioso que compromete equipos y sistemas.
- **Virus**: Se instala con la intervención del usuario, provocando daños en los dispositivos.
- **Gusanos**: Capaces de replicarse e infectar sistemas sin intervención del usuario.

- **Troyanos**: Se ocultan como aplicaciones legítimas para instalar otros programas maliciosos.
- **Ransomware**: Cifra la información de la víctima, exigiendo un rescate para liberarla.
- **Keyloggers**: Capturan todo lo que el usuario escribe en su teclado, incluyendo contraseñas.

Dispositivos de Red

Los enrutadores son dispositivos esenciales en una red doméstica, encargados de interconectar distintos equipos y dirigir el tráfico de datos. Su configuración adecuada es clave para garantizar la seguridad en redes inalámbricas(Oliveira Morilla, Synara, 2024).

Guías de seguridad informática

(Urbina, 2017)Señala que las guías ofrecen pautas claras para la configuración segura de dispositivos, el manejo responsable de la información y la prevención de incidentes de seguridad. En las redes Wi-Fi del hogar, las guías de seguridad son especialmente importantes, ya que muchas personas no tienen conocimientos técnicos y suelen dejar la configuración del router como viene de fábrica, lo que facilita que otras personas puedan conectarse sin permiso. Las buenas prácticas en redes Wi-Fi domésticas incluyen una serie de recomendaciones orientadas a minimizar las vulnerabilidades y garantizar la confidencialidad, integridad y disponibilidad de los datos transmitidos.

2.4. Legal

No existe ninguna restricción legal para llevar a cabo este proyecto de investigación, ya que se realizará exclusivamente en una red Wi-Fi doméstica de propiedad del investigador. Además, se conoce y respeta lo que indica el contrato con el proveedor de internet, por lo que el proyecto se realizará de forma legal y permitida.

CONSTITUCIÓN DE LA REPÚBLICA

Artículo 16.- Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos. 2. El acceso universal a las tecnologías de información y comunicación. 3. La creación de medios de comunicación social, y al acceso en igualdad

de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas. 4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad. 5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación;

Artículo 66.- Se reconoce y garantiza a las personas: (...) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (…) 21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación;

CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP)

Artículo 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley;

Artículo 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de

alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes;

Artículo 194.- Comercialización ilícita de terminales móviles. - La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años;

Artículo 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años;

Artículo 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad;

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro

del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años;

LEY ORGANICA DE GESTIÓN DE LA IDENTIDAD Y DATOS CIVILES

Artículo 3.- Objetivos. La presente Ley tiene como objetivos:

1. Asegurar el ejercicio del derecho a la identidad de las personas.
2. Precautelar la situación jurídica entre el Estado y las personas naturales dentro de sus relaciones de familia.
3. Proteger el registro de los hechos y actos relativos al estado civil de las personas.
4. Proteger la confidencialidad de la información personal.
5. Evitar el subregistro o carencia de datos en registro de una persona.
6. Proteger la información almacenada en archivos y bases de datos de los hechos y actos relativos al estado civil de las personas.
7. Propender a la simplificación, automatización e interoperabilidad de los procesos concernientes a los hechos y actos relativos al estado civil de las personas, de conformidad a la normativa legal vigente para el efecto;

LEY ORGÁNICA DE TELECOMUNICACIONES

Artículo 76.- Medidas técnicas de seguridad e invulnerabilidad. - Las y los prestadores de servicios ya sea que usen red propia o la de un tercero, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes. Dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente;

Artículo 77.- Interceptaciones. - únicamente se podrán realizar interceptaciones cuando exista orden expresa de la o el Juez competente, en el marco de una investigación de un delito o por razones de seguridad pública y del Estado, de conformidad con lo que

establece la ley y siguiendo el debido proceso;

Artículo 78.- Derecho a la intimidad. - para la plena vigencia del derecho a la intimidad, establecido en el artículo 66, numeral 20 de la Constitución de la República, las y los prestadores de servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal. Para tal efecto, las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos de carácter personal de conformidad con la ley;

Artículo 79.- Deber de información. - en caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de telecomunicaciones, el prestador de servicios de telecomunicaciones deberá informar a sus abonados, clientes y usuarios sobre dicho riesgo y sobre las medidas a adoptar;

Artículo 82.- Uso comercial de datos personales. - Las y los prestadores de servicios no podrán usar datos personales, información del uso del servicio, información de tráfico o el patrón de consumo de sus abonados, clientes o usuarios para la promoción comercial de servicios o productos, a menos que el abonado o usuario al que se refieran los datos o tal información, haya dado su consentimiento previo y expreso. Los usuarios o abonados dispondrán de la posibilidad clara y fácil de retirar su consentimiento para el uso de sus datos y de la información antes indicada. Tal consentimiento deberá especificar los datos personales o información cuyo uso se autorizan, el tiempo y su objetivo específico;

Artículo 84.- Entrega de información. - Las y los prestadores de servicios, entregarán a las autoridades competentes la información que les sea requerida dentro del debido proceso, con el fin de investigación de delitos. La Agencia de Regulación y Control de las Telecomunicaciones establecerá los mecanismos y procedimientos que sean necesarios;

Artículo 140.- Rectoría del sector. - El Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información es el órgano rector de las telecomunicaciones y de la sociedad de la información, informática, tecnologías de la información y las comunicaciones y de la seguridad de la información. A dicho órgano le corresponde el establecimiento de políticas, directrices y planes aplicables en tales áreas para el desarrollo de la sociedad de la información, de conformidad con lo dispuesto en la presente Ley, su Reglamento General y los planes de desarrollo que se establezcan a nivel nacional. Los planes y políticas que dicte dicho Ministerio deberán enmarcarse dentro de los objetivos del Plan Nacional de Desarrollo y serán de cumplimiento

obligatorio tanto para el sector público como privado.

2.5. Georeferencial

Debido a la naturaleza del problema, no se utilizó la georreferenciación, ya que el estudio abarcó redes WiFi ubicadas en distintos lugares y sin una ubicación específica.

CAPITULO III

METODOLOGÍA

3.1. Tipo de Investigación

La investigación será de tipo cuasi-experimental, aplicada.

- Cuasi-experimental debido a las pruebas de seguridad en redes Wi-Fi se realizan mediante ataques controlados a redes doméstica de propiedad del investigador.
- Aplicada porque busca ofrecer una solución al problema identificado, mediante la elaboración de una guía de seguridad que contribuya a mitigar las vulnerabilidades detectadas en redes domésticas.

3.2. Enfoque de la investigación

La investigación adopta un enfoque mixto, combinando elementos cuantitativos y cualitativos para obtener una comprensión integral del problema. Desde el enfoque cuantitativo, se realizan pruebas planificadas mediante ataques controlados, lo que permite recopilar datos sobre el comportamiento de las redes frente a diversas amenazas. En cuanto al enfoque cualitativo, se analiza e interpreta la información obtenida, lo que facilita la comprensión de las vulnerabilidades presentes y del nivel de seguridad en las redes Wi-Fi domésticas evaluadas.

3.3. Métodos de Investigación

Esta investigación utiliza el método inductivo, que, según Monroy Mejía y Nava Sanchezllanes (2018), ‘se basa en el razonamiento a partir de hechos específicos considerados válidos para llegar a conclusiones generales’. A través del análisis de vulnerabilidades en redes Wi-Fi domésticas, se identifican patrones comunes de seguridad deficiente, lo que permite generar una propuesta de guía basada en el protocolo WPA-3, con el fin de mejorar la protección de estas redes.

3.4. Técnicas e Instrumentos de Recopilación de Datos

Para la recopilación de datos, se emplearán tres métodos clave: la revisión bibliográfica, la experimentación y la observación directa.

La revisión bibliográfica permitirá recopilar información relevante proveniente de libros, artículos científicos, tesis y reportes especializados en seguridad informática, con énfasis en estudios relacionados con ataques a redes Wi-Fi.

En cuanto a la experimentación, se realizarán pruebas controladas de ataques simulados

a redes Wi-Fi con el fin de evaluar su nivel de seguridad. Para ello, se utilizarán herramientas especializadas como Kali Linux, entre otras, que permiten ejecutar ataques de penetración y evaluar vulnerabilidades específicas.

Por su parte, mediante la observación directa, se registrarán los efectos que generan estos ataques en la estabilidad y seguridad de las redes, permitiendo analizar cómo responden ante diferentes tipos de amenazas.

La integración de estos métodos, junto con un enfoque mixto, permitirá obtener datos claros y detallados sobre las vulnerabilidades que afectan a los usuarios en sus redes Wi-Fi domésticas, lo que contribuirá a respaldar la elaboración de una guía de seguridad con soluciones prácticas.

3.5. Universo, Población y Muestra

No es posible aplicar, universo población y muestra, ya que en Ecuador la mayoría de las personas utilizan redes Wi-Fi, y evaluar su seguridad implicaría acceder a ellas sin autorización, lo cual es ilegal.

3.6. Procesamiento de la Información

Una vez obtenida y recopilada la información, se procederá a su procesamiento, lo cual implica organizar y presentar de manera lógica y clara los resultados obtenidos mediante los instrumentos aplicados. Para ello, se utilizarán diferentes técnicas analíticas según el tipo de datos:

Datos Cuantitativos:

Los datos numéricos obtenidos a través de las pruebas de seguridad y análisis de redes Wi-Fi serán tabulados y procesados utilizando herramientas ofimáticas. Estos datos se presentarán mediante tablas, gráficos de barras y gráficos circulares, que permitirán visualizar de forma clara la incidencia y el impacto de las vulnerabilidades detectadas en las redes evaluadas.

Datos Cualitativos:

La información cualitativa no solo tomará en cuenta lo que piensan y saben los usuarios sobre la seguridad en redes Wi-Fi, sino también lo que se observe durante las pruebas realizadas con ataques simulados. Esta información se organizará en cuadros y tablas para analizarla con más facilidad, lo que permitirá descubrir patrones, comportamientos repetidos y aspectos comunes en la forma en que los usuarios protegen sus redes.

Este enfoque permitirá obtener una visión integral de la seguridad en redes Wi-Fi domésticas y validar la hipótesis de que WPA-3 mejora significativamente la protección contra ataques cibernéticos.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. Análisis, Interpretación y Discusión de Resultados

Con la finalidad de otorgar validez al presente trabajo de investigación, se desarrollaron diversas actividades metodológicas. En primer lugar, se efectuó una revisión bibliográfica exhaustiva para establecer los fundamentos teóricos necesarios.

A continuación, Se dio inicio a la etapa experimental, durante la cual se llevaron a cabo pruebas orientadas a analizar el nivel de seguridad de las redes Wi-Fi domésticas.

Finalmente, se interpretaron y discutieron los resultados obtenidos a partir de los ataques realizados, lo que permitió identificar y registrar de forma práctica las vulnerabilidades existentes.

4.1.1. Revisión Bibliográfica

La revisión bibliográfica realizada en el presente trabajo tuvo como finalidad recopilar y analizar información actualizada y relevante sobre la seguridad en redes Wi-Fi domésticas. Para ello, se consultaron diversas fuentes como libros, artículos científicos, tesis académicas y manuales técnicos, abarcando estudios recientes sobre protocolos de cifrado como WEP, WPA, WPA2 y WPA3. Esta búsqueda de información permitió identificar las principales vulnerabilidades, así como los métodos de ataque más utilizados y las herramientas de análisis que facilitan la evaluación de la seguridad en entornos inalámbricos.

La selección de fuentes se basó en su actualidad, relevancia y rigurosidad científica, priorizando investigaciones de los últimos cinco años. De esta manera, se garantizó que el marco teórico esté alineado con los avances tecnológicos más recientes y con las nuevas amenazas cibernéticas que afectan a los usuarios de redes domésticas.

Este análisis teórico no solo sirvió como base para diseñar la fase experimental del estudio, sino que también permitió establecer parámetros de comparación para los resultados obtenidos en las pruebas prácticas. Gracias a la revisión bibliográfica, fue posible contextualizar los hallazgos dentro de un marco más amplio de conocimiento, fortaleciendo la validez de la investigación y resaltando la urgencia de implementar protocolos más avanzados, como WPA-3, para mejorar la defensa ante amenazas informáticas.

Artículos elegidos para la investigación

Tabla 2

Instrumento de Investigación

N°	Titulo	Autor(es)	Tipo de Fuente	Año de edición	Objetivo Principal	Aporte al trabajo de investigación
1	Análisis de vulnerabilidades en redes inalámbricas: métodos y soluciones	Mora Zambrano Eugenio Rafael	Articulo científico	2024	Identificar y evaluar las vulnerabilidades presentes en redes inalámbricas, mediante métodos como pruebas de penetración, auditorías de seguridad y monitoreo continuo	Proporciona el fundamento práctico y teórico necesario para entender las amenazas reales a las redes Wi-Fi domésticas, guía la elección de técnicas de prueba aplicadas en la experimentación y respalda la formulación de recomendaciones basadas en protocolos de seguridad actualizados
2	Aplicación de hacking ético para identificar amenazas, riesgos y vulnerabilidades en la red Wifi.	Vivar Franco Itaty Andreina	Tesis de grado	2023	Analizar con la aplicación de hacking ético para identificar amenazas, riesgos y vulnerabilidades en la red wifi.	La aplicación de técnicas de hacking ético permite obtener una evaluación realista y controlada del nivel de seguridad de la red Wi-Fi, identificando vulnerabilidades que

						podrían ser explotadas por atacantes malintencionados.
3	Auditoría de seguridad en redes wifi: evaluación de vulnerabilidades y métodos de protección: Wi-Fi security audit: vulnerability assessment and protection methods	Jefferson Vite Jhonatan Cheme Karen Vite Freddy Nuñez	Artículo científico	2025	Implementar mejoras en la seguridad y el rendimiento de la red inalámbrica de la carrera de Electrónica del Instituto Superior Tecnológico Tsáchila, migrando del protocolo WPA2 a WPA3, mediante auditorías de seguridad y optimización de infraestructura tecnológica.	Proporciona evidencia práctica y concreta de cómo la migración a WPA3 incrementa la protección contra ataques comunes (como ataques de diccionario y des autenticación) y mejora el desempeño de la red, sirviendo como modelo de referencia para la aplicación de soluciones similares en redes Wi-Fi domésticas o institucionales.
4	Demostración y Análisis de Vulnerabilidades Existentes en Redes Wi-Fi y Recomendaciones de Seguridad	Luis Miguel Serrano Vázquez	Tesis de posgrado	2022	Describir, analizar y demostrar de manera práctica las vulnerabilidades presentes en los protocolos de seguridad Wi-Fi para finalmente proponer medidas de seguridad en redes inalámbricas.	Proporciona una comprensión profunda de la evolución de los protocolos de seguridad Wi-Fi, evidenciando sus fortalezas y debilidades mediante pruebas prácticas en un entorno controlado.
5	Diseño e implementación de una red inalámbrica WiFi 5 con el	Cristian Sebastián Hernández Ramírez	Tisis de grado	2024	Diseñar e implementar una red inalámbrica	Proporciona evidencia comparativa sobre las

	protocolo de autenticación WPA3 para un posterior análisis de vulnerabilidades en el Campus Universitario de la Universidad Técnica del Norte				Wi-Fi 5 con el protocolo de autenticación WPA3 en un entorno universitario y realizar un estudio acerca de las diferentes vulnerabilidades existentes en dicho protocolo de autenticación con respecto a su antecesor.	mejoras y limitaciones de WPA3, contribuyendo a la comprensión de su eficacia ante amenazas modernas y sirviendo como base para futuras recomendaciones de actualización tecnológica en redes
6	Estudio de vulnerabilidades en el sistema de seguridad WPA-2 Personal del estándar IEEE 802.11i y propuestas de mejoras a considerar en el sistema WPA-3	Alexis Vicente Pardo Sánchez.	Tesis de grado	2022	Analizar las vulnerabilidades del sistema de seguridad WPA2 en redes Wi-Fi y proponer mejoras que puedan ser implementadas en el protocolo WPA3, mediante el estudio teórico y pruebas experimentales	Contribuye al conocimiento sobre la protección de redes domésticas, ofreciendo estrategias preventivas para minimizar riesgos en la transmisión de datos inalámbricos.
7	Seguridad Actual en redes Wifi	Javier Esteban Sánchez	Tesis de grado	2021	Analizar y comparar las vulnerabilidades de los protocolos de seguridad WPA2 y WPA3 en redes Wi-Fi, mediante la aplicación	Proporciona una visión integral de la evolución de los protocolos de seguridad en redes Wi-Fi, evidenciando las debilidades de WPA2 y

					de técnicas de hacking ético, pruebas de penetración y el estudio de ataques históricos relevantes, con el fin de demostrar las mejoras de seguridad que ofrece WPA3 frente a sus antecesores.	validando la superioridad de WPA3 a través de pruebas prácticas.
8	Vulnerabilidades en redes Wifi	Olivia Madrigal María Fernández	Tesis de posgrado	2020	Concienciar sobre las vulnerabilidades de las redes Wi-Fi, proporcionando al lector los conocimientos teóricos y prácticos necesarios para identificar riesgos, proteger sus redes mediante buenas prácticas de seguridad y utilizar herramientas de auditoría para fortalecer la protección inalámbrica.	Ofrece una guía completa y prácticas de auditoría de seguridad, facilitando la identificación de vulnerabilidades comunes y promoviendo la aplicación de medidas efectivas como el uso de WPA2, contraseñas robustas, actualizaciones constantes y filtrado de direcciones MAC, fortaleciendo así la seguridad en redes domésticas.
9	Análisis de vulnerabilidades de redes inalámbricas domesticas	María Fabiola Curay Colucho	Tesis de grado	2023	Diagnosticar vulnerabilidades de redes inalámbricas	Esta investigación contribuye de manera significativa al estudio

	utilizando pentesting en Tungurahua				domésticas de diferentes proveedores utilizando una herramienta adecuada para Pentesting.	de las vulnerabilidades en redes Wi-Fi domésticas al ofrecer un enfoque práctico y controlado para la identificación y evaluación de riesgos de seguridad. A través del uso de máquinas virtuales, adaptadores de red Wi-Fi externos compatibles con modo monitor, y herramientas especializadas como Airgeddon, Aircrack-ng, Wifite y Nessus

Elaborado por: Michael Michay, 2025.

La revisión bibliográfica realizada aporta de manera significativa al desarrollo del proyecto de investigación, ya que proporciona tanto fundamentos teóricos como metodologías prácticas clave para el análisis de vulnerabilidades en redes Wi-Fi domésticas. Los estudios consultados permiten comprender las amenazas más comunes, los protocolos de seguridad existentes y las debilidades.

Además, se destacan enfoques prácticos como el uso de técnicas de hacking ético, pruebas de penetración, auditorías de seguridad y herramientas especializadas, que han sido adaptadas al diseño experimental de esta investigación.

4.1.2. Experimentación

Sistema Operativo

La elección del software y sistema operativo es fundamental para el análisis de vulnerabilidades en redes Wi-Fi, ya que influye directamente en la precisión de los resultados obtenidos. Los sistemas operativos permiten integrar diversas herramientas de evaluación de seguridad, por lo que su selección debe considerar la compatibilidad y el propósito de su diseño. En el ámbito de la ciberseguridad, existen sistemas operativos especializados, generalmente basados en Linux, que son gratuitos y optimizados para realizar auditorías de seguridad. Por ello, resulta esencial identificar la opción más adecuada que facilite una evaluación efectiva y confiable, como se detalla en la Tabla 3.

Tabla 3

Requisitos del Sistema Operativo

Requisitos	Descripción	Windows	MacOs	Kali linux	Black Arch Linux	Parrot OS
Software dedicado para ataques informáticos	Enfoque del sistema operativo al campo del hacking ético y la ciberseguridad.	No	No	Si	Si	Si
Soporte para programas de ataques informáticos	Compatibilidad del Sistema operativo con programas diseñados para	Si	Si	Si	Si	Si

	ataques informáticos.					
Servicios de red deshabilitados	Capacidad para desactivar los servicios de red para evitar ataques hacia el usuario.	No	No	Si	No	No
Modo Forense	Modo de ejecución del Sistema operativo utilizado para buscar información del sistema sin alterar su funcionamiento.	No	No	Si	Si	Si
Compatibilidad con la mayoría de tarjetas de red para monitoreo	Capacidad del Sistema operativo para emplear diferentes tipos de tarjetas de red (externas) para monitorear paquetes.	Si	Si	Si	Si	Si
Robustez del Sistema	Resistencia ante amenazas externas existentes que podrían comprometer el Sistema operativo	Si	Si	Si	Si	Si
Soporte para Sniffers (Al menos uno)	Capacidad de ejecutar al menos un programa tipo Sniffer.	Si	Si	Si	Si	Si
Posibilidad de Configurar	Soporte para la configuración de servidores de	Si	Si	Si	Si	Si

Servidores de Autenticación	autenticación como RADIUS.					
Capacidad de ejecutarse en dispositivos móviles	Capacidad de ejecutarse en dispositivos coprocesadores ARM, generalmente dispositivos móviles.	No	No	Si	Si	Si
Entorno amigable para usuarios de todos los niveles.	Facilidad de navegación sobre su entorno gráfico para todos los niveles (Inicial, Intermedio y Experto).	Si	Si	Si	No	No
Estabilidad	Pocos errores en el sistema.	No	Si	Si	Si	Si
Fácilmente configurable	Herramientas intuitivas que no son muy complejas de utilizar y configurar.	Si	Si	Si	No	Si
Compatibilidad con los sistemas de seguridad WPA-2 y WPA-3	Soporte para los sistemas de seguridad de las redes Wi-Fi	Si	Si	Si	Si	Si

Elaborado por: Michael Michay, 2025.

Al analizar los diferentes sistemas operativos se optó por utilizar el sistema operativo Kali Linux para realizar las pruebas debido a su robustez y especialización en la seguridad informática. Kali Linux es ampliamente reconocido y utilizado en el ámbito del hacking ético y auditoría de redes, lo que garantiza una gran compatibilidad en las herramientas diseñadas para el análisis de vulnerabilidades y ataques informáticos. Aunque existen otras alternativas, estas no ofrecen la misma estabilidad y soporte.

Tabla 4

Características Que se Pueden Conocer Sobre Kali Linux

Característica	**Descripción**
Captura de Paquetes y Agrietamiento de Contraseñas	Permite capturar paquetes, desautenticar usuarios, inyectar tráfico y descifrar claves. Compatible con WEP, WPA y WPA-2.
Suplantación de Identidad	Herramienta Wifite para falsificar direcciones MAC y suplantar la identidad de usuarios. Compatible con WEP, WPA y WPA-2.
Monitoreo de Paquetes	Utiliza Wireshark para analizar el tráfico y monitorear los paquetes transmitidos en la red.
Vulneración de IEEE 802.1X	Hostapd-WPE permite ataques de suplantación de servidores, vulnerando redes WPA Enterprise basadas en IEEE 802.1X.
Creación de Puntos de Acceso Falsos	Airmon-ng crea puntos de acceso falsos para engañar a los usuarios y obtener su información personal.
Ataques Man-in-the-Middle (MITM)	Ettercap permite realizar ataques MITM para interceptar y modificar comunicaciones entre dos partes sin su conocimiento.
Denegación de Servicio (DoS)	HPing3 permite realizar ataques DoS mediante el envío de paquetes TCP/IP maliciosos para saturar la red o el sistema objetivo.
Seguridad y Robustez	Kali Linux es un sistema operativo confiable y robusto, diseñado para auditorías de seguridad con pruebas exhaustivas en cada versión.

Soporte para Configuración de Servidores	FreeRadius permite configurar servidores RADIUS, proporcionando autenticación segura sin necesidad de servidores dedicados.
Portabilidad	Kali Linux Live permite ejecutar Kali Linux desde unidades portátiles (USB), pudiendo usarse en cualquier computador sin instalación previa.

Elaborado por: Michael Michay, 2025.

Adaptadores Inalámbricos

El monitoreo de redes Wi-Fi es una actividad fundamental en la evaluación de la seguridad de las redes inalámbricas. A diferencia de las redes cableadas, las redes Wi-Fi transmiten datos a través del aire, lo que las hace susceptibles a ser interceptadas por cualquier persona dentro del alcance de la señal. Para realizar una auditoría o un análisis de seguridad en estas redes, es crucial contar con herramientas que permitan capturar y analizar los paquetes de datos transmitidos.

Una de las principales herramientas necesarias para realizar este tipo de monitoreo son los adaptadores inalámbricos, que son dispositivos capaces de conectar un equipo a una red Wi-Fi, pero con una capacidad adicional: la posibilidad de entrar en modo monitor. En este modo, los adaptadores inalámbricos pueden interceptar todos los paquetes de datos que pasan por el aire, incluso aquellos que no están destinados al equipo, lo que permite realizar un análisis detallado del tráfico y detectar vulnerabilidades en la red.

El uso de adaptadores inalámbricos para el monitoreo de paquetes es indispensable, ya que las computadoras de uso general no están equipadas con antenas ni chipsets que permitan esta función de forma nativa. Estos dispositivos son esenciales en el hacking ético y en las auditorías de seguridad, ya que permiten la captura de información relevante para la identificación de vulnerabilidades en la red.

Sin embargo, no todos los adaptadores inalámbricos son compatibles con las herramientas de auditoría de Kali Linux, un sistema operativo ampliamente utilizado para hacking ético y pruebas de penetración. La compatibilidad con Kali Linux es un requisito esencial, ya que la elección de un adaptador que no sea compatible podría limitar la efectividad del análisis y la capacidad para realizar ataques controlados en la red.

A lo largo de este estudio, se enfatiza la importancia de seleccionar un adaptador inalámbrico adecuado, no solo por su capacidad para realizar el monitoreo de paquetes, sino también por su compatibilidad con Kali Linux. Esta compatibilidad es crucial para

asegurar el correcto funcionamiento de las herramientas de monitoreo y la recopilación precisa de datos durante el análisis de la seguridad de las redes Wi-Fi. Por lo tanto, es fundamental identificar el adaptador más adecuado que cumpla con estos requisitos, lo cual se detalla en la Tabla 5.

Tabla 5

Características de las Tarjetas de Red

Características Técnicas	**Alfa AWUS036 NH**	**TP-LINK TL-WN722N**	**TP-Link Archer T4U**	**TP-Link Archer T4U Plus**	**TP-Link TL-WN823N**
Compatibilidad con Kali Linux	Sí	Sí	Sí	Sí	Parcial (requiere configuración)
Ganancia	5 dBi	4 dBi	4 dBi	5 dBi (x2 antenas)	Interna (sin especificar)
Chipset	Realtek RTL8188RU	Atheros AR9271	Realtek RTL8812AU	Realtek RTL8812AU	Realtek RTL8192EU
Tipo de Antena	1 antena RP-SMA desmontable	Desmontable RP-SMA	2 antenas desmontables	2 antenas externas de alta ganancia	Antena interna
Software disponible (Drivers)	Sí	Sí	Sí	Sí	Sí (instalación manual en Kali)
Información disponible	Sí	Sí	Sí	Sí	Sí
Versión de Wi-Fi soportada	IEEE 802.11b/g/n	IEEE 802.11b/g/n	IEEE 802.11a/b/g/n/ac	IEEE 802.11a/b/g/n/ac	IEEE 802.11b/g/n

Seguridad Wi-Fi soportada	WEP 64/128 bits, WPA/WPA 2	WEP 64/128 bits, WPA-PSK/WPA 2-PSK	WPA/WPA2 -PSK, WPA3	WPA/WPA2 -PSK, WPA3	WEP, WPA/WP A2-PSK
Modulación	BPSK, QPSK, CCK, OFDM	DBPSK, DQPSK, CCK, OFDM, 16/64-QAM	QPSK, QAM, OFDM, 16/64-QAM	QPSK, QAM, OFDM, 16/64-QAM	CCK, OFDM, QAM
Bandas de frecuencia	2.4 GHz	2.4 GHz	2.4 GHz / 5 GHz	2.4 GHz / 5 GHz	2.4 GHz
Modos inalámbrico s	Ad-Hoc / Infraestruct ura	Ad-Hoc / Infraestruct ura	Ad-Hoc, Infraestructu ra, AP	Ad-Hoc, Infraestructu ra, AP	Infraestruct ura
Interfaz de salida	Mini USB 2.0	USB 2.0	USB 3.0	USB 3.0	USB 2.0
Disponibilid ad en el país	Sí	Sí	Sí	Sí	Sí
Precio (referencial)	$80	$20	$25	$30	$15

Elaborado por: Michael Michay, 2025.

El adaptador USB Wi-Fi TP-Link Archer T4U fue elegido debido a su excelente compatibilidad con Kali Linux, lo que permite ejecutar herramientas de auditoría y monitoreo de seguridad de redes de manera efectiva. Su soporte para los estándares IEEE 802.11a/b/g/n/ac y su capacidad de operar en doble banda (2.4 GHz y 5 GHz) le permiten trabajar en una amplia variedad de redes, ofreciendo velocidades de hasta 1300 Mbps en la banda de 5 GHz y 400 Mbps en la banda de 2.4 GHz. Además, su diseño compacto y su interfaz USB 3.0 mejoran la eficiencia en la transferencia de datos, mientras que es compatible con WPA/WPA2/WPA3, lo que facilita la evaluación de la seguridad en

diferentes niveles de encriptación. Su precio accesible de $25 y su facilidad de disponibilidad en el mercado lo convierten en una opción económica y práctica para realizar auditorías de seguridad sin comprometer el rendimiento ni la calidad.

Router Inalámbrico

Es un dispositivo esencial en las redes modernas, ya que permite gestionar y distribuir la conexión a Internet de manera inalámbrica a múltiples dispositivos dentro de su rango de cobertura.

Esto posibilita que los usuarios se conecten desde cualquier punto que se encuentre dentro del área de alcance de la señal, brindando flexibilidad y movilidad en el acceso a la red. El rango de cobertura es un parámetro muy importante, especialmente en evaluaciones de seguridad, donde se requiere comprobar que un ataque a la red Wi-Fi puede ser realizado desde una distancia considerable.

Por lo tanto, es indispensable seleccionar un dispositivo que cuente con un amplio alcance de señal para asegurar que los resultados de las pruebas sean lo más precisos y realistas posibles.

Además del rango, el router debe cumplir con otros requisitos técnicos fundamentales, como compatibilidad con los protocolos de seguridad actuales y estabilidad en la transmisión de datos. Para determinar el equipo más adecuado, en la Tabla 6 se presenta una comparativa de diferentes dispositivos evaluados.

Tabla 6

Comparativa de Routers Inalámbricos según Requisitos Técnicos

Requisitos Técnicos	Descripción	TP-Link AX1800	Asus RT-AX82U	D-Link AC2100	Netgear Nighthawk RAX40	Linksys MR7350	Xiaomi Wi-Fi AX3
Soporte IEEE 802.11ax (Wi-Fi 6)	Soporte de la última versión de Wi-Fi	Sí	Sí	No	Sí	Sí	Sí
Soporte para WPA3	Incorporación del último sistema de seguridad certificado	Sí	Sí	No	Sí	Sí	Sí
Soporte para WPA2 Personal y Enterprise	Compatibilidad con versiones anteriores de seguridad WPA-2	Sí	Sí	Sí	Sí	Sí	Sí
Rango de cobertura mayor	Capacidad de cubrir una oficina o un hogar	Sí	Sí	Medio	Sí	Sí	Sí
Tecnología MIMO o MU-MIMO	Comunicación simultánea con varios dispositivos	Sí	Sí	Sí	Sí	Sí	Sí
Rompemuros	Capacidad de atravesar obstáculos físicos como paredes	Sí	Sí	Medio	Sí	Sí	Sí
Soporte para múltiples dispositivos	Manejo de gran cantidad de conexiones simultáneas	Sí	Sí	Sí	Sí	Sí	Sí
Compatibilidad con estándares anteriores	Soporte para IEEE 802.11ac/n/b/g	Sí	Sí	Sí	Sí	Sí	Sí
Mecanismos de filtrado de MACs	Control de acceso mediante filtrado de direcciones MAC	Sí	Sí	Sí	Sí	Sí	Sí
Soporte de Seguridad Firewall	Incorporación de cortafuegos para impedir ataques DoS	Sí	Sí	Medio	Sí	Sí	Sí

Procesador Eficiente	Procesamiento rápido de múltiples flujos de datos	Sí	Sí	Medio	Sí	Sí	Sí
Beamforming	Optimización de la señal dirigida hacia cada dispositivo	Sí	Sí	No	Sí	Sí	Sí

Elaborado por: Michael Michay, 2025.

La elección del router TP-Link AX1800 se fundamentó principalmente en su soporte al protocolo de seguridad WPA3, el estándar más reciente para redes Wi-Fi, que aporta un cifrado más robusto de las contraseñas y mayor resistencia frente a ataques de fuerza bruta, garantizando así una elevada protección de la red doméstica ante amenazas modernas.

Tipos de ataques en redes wifi

En el ámbito de la seguridad de redes inalámbricas domésticas, las redes que utilizan los protocolos WPA y WPA2 no están exentas de vulnerabilidades.

Aunque estos protocolos representan una mejora significativa respecto a estándares anteriores como WEP, siguen siendo susceptibles a diferentes tipos de ataques que comprometen la confidencialidad, integridad y disponibilidad de la red.

Entre las amenazas más comunes se encuentran los ataques de diccionario, fuerza bruta, de desautenticación y los ataques basados en la creación de puntos de acceso falsos.

Cada uno de estos métodos explota debilidades específicas en la autenticación, el cifrado o el comportamiento de los usuarios para acceder sin autorización a los datos transmitidos. A continuación, en la Tabla 7, se detallan los principales tipos de ataques y sus respectivas definiciones, como parte del análisis de riesgos en redes Wi-Fi domésticas.

Tabla 7

Ataques y Vulnerabilidades en Redes Wi-Fi

Ataque	**Definición**
Ataques de ingeniería social	No son ataques técnicos directamente al protocolo, pero buscan engañar a los usuarios para que revelen su contraseña o información de acceso (por ejemplo, mediante phishing o sitios falsos).
Ataque de diccionario	Consiste en capturar el handshake de autenticación y luego probar una lista predefinida de contraseñas comunes hasta encontrar la correcta.
Ataque de fuerza bruta	Similar al ataque de diccionario, pero prueba todas las combinaciones posibles de caracteres hasta encontrar la contraseña correcta.

Ataque Evil Twin (Gemelo Malvado)	El atacante crea un punto de acceso falso (con el mismo nombre que la red real) para engañar a los usuarios y capturar su tráfico o credenciales.
Ataque de desautenticación (Deauth Attack)	Se envían paquetes de desautenticación para forzar a los dispositivos a desconectarse, capturar handshakes o hacer que se conecten a redes falsas.
Rogue AP (Punto de Acceso Falso)	El atacante configura un punto de acceso no autorizado para interceptar el tráfico de usuarios desprevenidos.
Ataque de Hombre en el Medio (MITM)	El atacante intercepta la comunicación entre el usuario y el router para leer, modificar o robar datos sin que las partes lo sepan.
MAC Spoofing (Suplantación de MAC)	El atacante suplanta la dirección MAC de un dispositivo autorizado para conectarse a la red evitando controles de acceso.
Ataque de WPS (Wi-Fi Protected Setup)	Aprovecha vulnerabilidades en el protocolo WPS, como la debilidad del PIN de autenticación, para acceder a la red sin conocer la clave principal.
Captura de Handshake WPA/WPA2	Técnica que permite interceptar el proceso de autenticación entre un cliente y el router para luego intentar descifrar la contraseña.
Ataque de Reinstalación de Claves (KRACK)	Explota fallos en el protocolo WPA2 para reinstalar claves de cifrado y descifrar paquetes transmitidos, incluso sin conocer la contraseña.
Ataque de Reinyección de paquetes ARP	Técnica utilizada para generar tráfico en una red inalámbrica con el fin de facilitar la obtención de handshakes o claves.
Ataque por desbordamiento de búfer en routers	El atacante aprovecha errores de programación en el firmware del router para ejecutar código malicioso.
Ataque a través de dispositivos IoT vulnerables	Se comprometen dispositivos inteligentes conectados a la red (como cámaras o asistentes virtuales) para acceder a la red interna.

Ataque por canal lateral (Side-Channel)	Se basa en la observación del comportamiento del sistema (tiempos de respuesta, consumo eléctrico, etc.) para inferir claves criptográficas.
Ataque mediante jamming (interferencia)	El atacante bloquea la señal Wi-Fi enviando ruido o interferencia para negar el servicio (Denegación de Servicio - DoS).
Ataques a routers con firmware desactualizado	Se explotan vulnerabilidades conocidas en routers que no han sido actualizados con parches de seguridad.
Ataques por DNS Spoofing/DNS Hijacking	El atacante redirige el tráfico de los usuarios hacia sitios maliciosos haciéndose pasar por el DNS legítimo.
Ataque mediante portales cautivos falsos	Se crea una red Wi-Fi gratuita falsa que redirige a un portal de inicio de sesión falso para robar credenciales.
Ataque a través de redes abiertas (sin cifrado)	Permite al atacante interceptar libremente todo el tráfico sin ninguna barrera de seguridad.

Elaborado por: Michael Michay, 2025.

Resultados de ataques

1. **Resultado de ataque de ingeniería social**

El ataque de ingeniería social es una técnica que se basa en la manipulación psicológica de las personas para obtener información confidencial. A diferencia de otros métodos de hacking más técnicos, esta estrategia explota la confianza, desconocimiento o distracción del usuario.

Uno de los métodos más representativos de este tipo de ataque es el phishing, que consiste en engañar a la víctima para que acceda a un sitio web falso, el cual simula visualmente ser un sitio legítimo, como Facebook, Gmail, Outlook, entre otros. Al ingresar sus credenciales creyendo que están en el sitio real, la víctima entrega su información confidencial directamente al atacante.

Esta técnica, aunque ampliamente conocida, sigue siendo efectiva. Se tiene constancia de ataques de phishing desde la década de los años 90, pero uno de los casos más difundidos ocurrió en 2003, cuando millones de usuarios de fueron víctimas de sitios clonados. Desde

entonces, ha evolucionado y se ha integrado incluso en campañas de espionaje, estafas bancarias y robos de identidad.

Herramienta Utilizada

SET

Para este ataque se utilizó el Social-Engineer Toolkit (SET), una herramienta desarrollada en Python por David Kennedy, fundador de TrustedSec, con el propósito de automatizar ataques de ingeniería social en entornos de auditoría ética y pruebas de penetración.

SET es una de las herramientas más utilizadas en el ámbito de la ciberseguridad ofensiva, y viene preinstalada en Kali Linux, una distribución especializada en pruebas de seguridad informática.

Figura 2

Interfaz inicial de SET al ser ejecutado desde la terminal.



Elaborado por: Michael Michay, 2025.

Pasos a seguir:

1. Para comenzar, se debe Iniciar SET desde la terminal de Kali Linux con privilegios de superusuario usando el siguiente comando:

sudo setoolkit

Figura 3

Ejecución de SET Desde la terminal.



Elaborado por: Michael Michay, 2025.

2. Una vez iniciado SET, se accede al menú principal, donde se seleccionan las

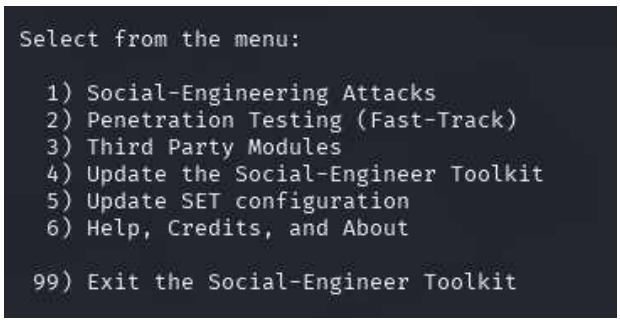
siguientes opciones para configurar el ataque:

[1] Social-Engineering Attacks

Se elige esta opción para iniciar un ataque basado en ingeniería social.

Figura 4

Selección del tipo de ataque en SET.



Elaborado por: Michael Michay, 2025.

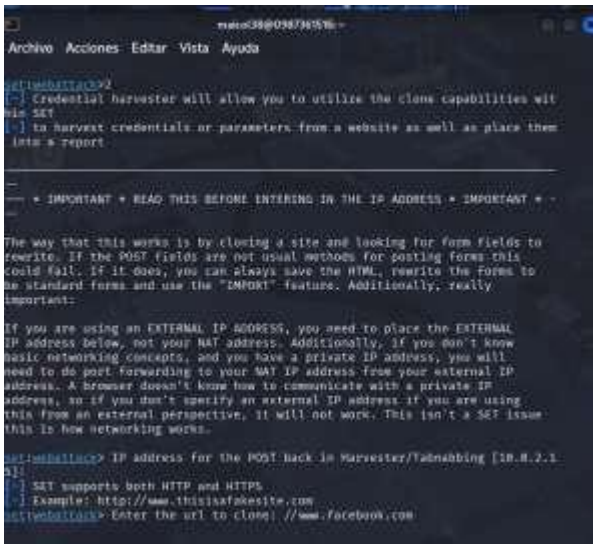
3. Dentro del submenú de ataques sociales de SET, se continúa con la opción [2] Website Attack Vectors, la cual permite realizar ataques basados en sitios web. Posteriormente, se selecciona [3] Credential Harvester Attack Method, una técnica orientada a capturar credenciales ingresadas por las víctimas en formularios falsos. Finalmente, se elige [2] Site Cloner, que permite clonar una página web legítima para que funcione como señuelo.

Al seleccionar esta opción, el sistema solicita primero ingresar la dirección IP del atacante, que será el destino donde se almacenarán las credenciales capturadas. Luego, se debe introducir la URL del sitio web a clonar, como por ejemplo https://www.facebook.com, la cual se muestra en la Figura 4, donde se evidencia este paso.

Una vez proporcionados estos datos, SET procede a clonar automáticamente la página seleccionada y deja el entorno configurado, listo para que una víctima acceda al enlace malicioso e introduzca su información personal, la cual será capturada en tiempo real por el atacante.

Figura 5

Proceso de configuración del ataque en SET con las opciones seleccionadas y datos ingresados



Elaborado por: Michael Michay, 2025.

4. Ejecución del ataque y captura de credenciales

Cuando la víctima accede al sitio clonado, generalmente a través de un engaño como un correo electrónico, mensaje en redes sociales, anuncio falso o código QR, se le muestra una página visualmente idéntica a la original. Al ingresar sus credenciales de acceso, estos datos se registran en tiempo real en la terminal del atacante.

Figura 6

Visualización de la página clonada en el navegador, lista para capturar los datos de la víctima.

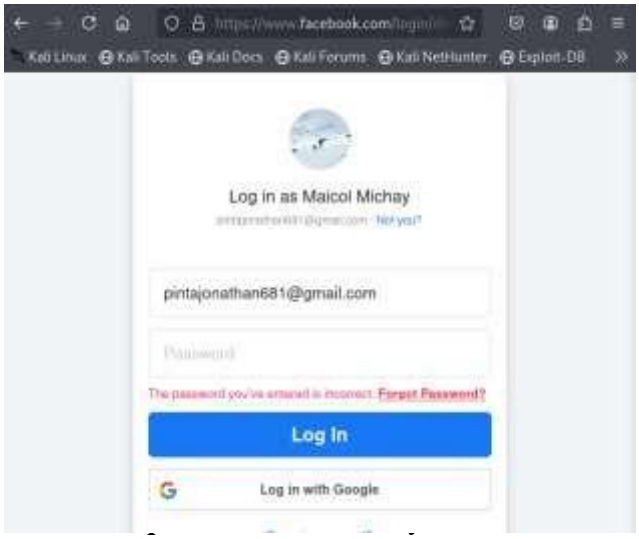


Figura 7

Visualización de los datos capturados de la víctima.



Elaborado por: Michael Michay, 2025.

Este proceso permite evidenciar cómo un atacante puede, sin necesidad de vulnerabilidades técnicas, robar credenciales mediante la simple imitación visual y el aprovechamiento de la confianza del usuario.

2. Resultado de ataque de diccionario

El ataque de diccionario es una técnica ampliamente utilizada en el ámbito de la ciberseguridad ofensiva, cuyo objetivo es descifrar contraseñas mediante la prueba

sistemática de palabras contenidas en un archivo de texto conocido como diccionario. La cuál se basa en una lista previamente definida de contraseñas potenciales, compuesta generalmente por palabras y combinaciones que los usuarios suelen emplear con frecuencia.

Este método tiene sus orígenes en los primeros sistemas UNIX, donde los atacantes empleaban listas simples de contraseñas comunes, como 123456, password o admin, para obtener acceso no autorizado. Con el tiempo, estas listas se han vuelto más sofisticadas, incluyendo patrones de escritura, combinaciones personales y palabras clave generadas a partir de técnicas de ingeniería social.

El principio del ataque es sencillo: se toma cada palabra del diccionario y se prueba como posible contraseña hasta encontrar una coincidencia. La efectividad del ataque se incrementa significativamente cuando se utilizan diccionarios personalizados, creados a partir de información específica de la víctima como su nombre, fecha de nacimiento, nombres de familiares, mascotas o lugares frecuentes lo que aumenta las probabilidades de éxito al aprovechar el uso de contraseñas débiles o predecibles.

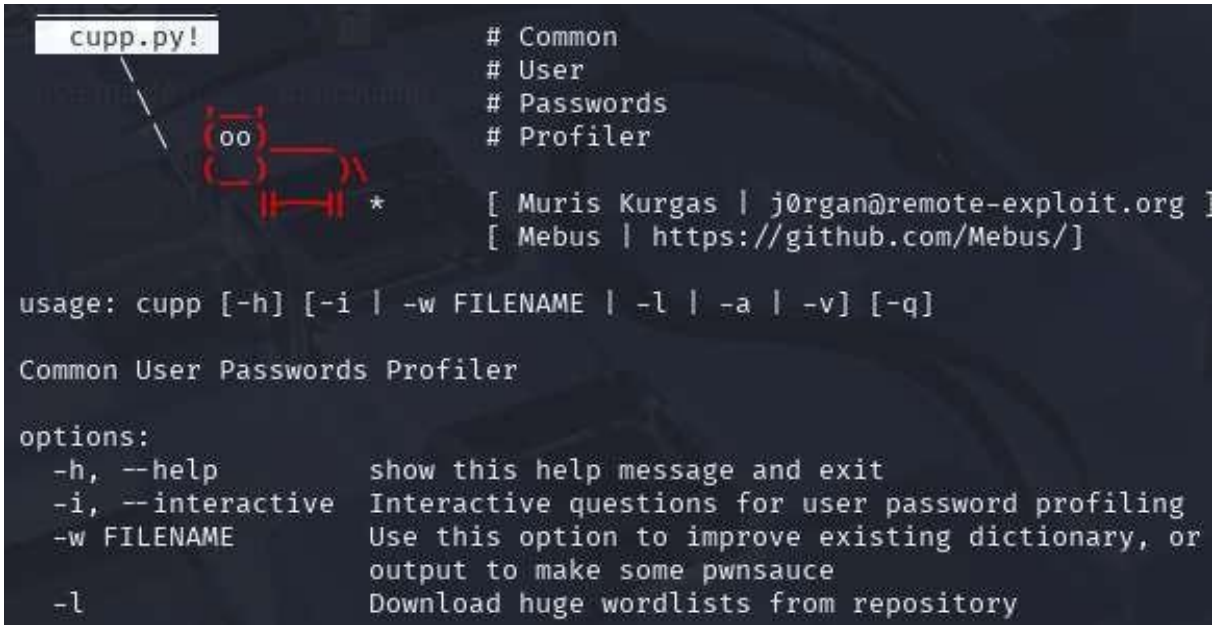
Herramienta utilizada

CUPP

Para la ejecución de este ataque se utilizó la herramienta Common User Passwords Profiler (CUPP), ya que es ideal para generar diccionarios personalizados basados en información específica de la víctima. Desarrollada por Murilo Polese y escrita en Python, CUPP permite automatizar la creación de listas de contraseñas utilizando datos personales como nombres, fechas de nacimiento, apodos, mascotas, entre otros. Esta herramienta es especialmente útil en ataques de diccionario, ya que aplica reglas y patrones comunes del comportamiento humano en la creación de contraseñas, aumentando significativamente las probabilidades de éxito frente a contraseñas débiles o predecibles.

Figura 8

Interfaz inicial de CUPP al ser ejecutado desde la terminal.



Elaborado por: Michael Michay, 2025.

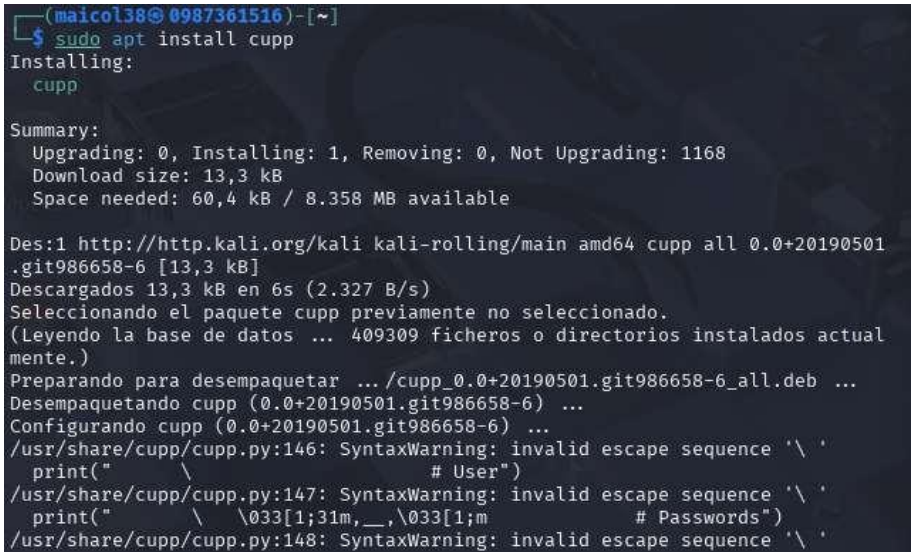
Pasos a seguir:

1. Para comenzar, se debe instalar CUPP desde la terminal de Kali Linux con el siguiente comando:

sudo apt install cupp

Figura 9

Instalación de CUPP desde la terminal.



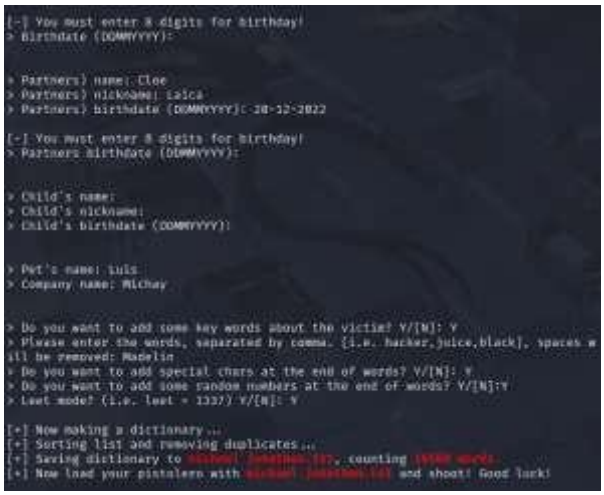
Elaborado por: Michael Michay, 2025.

2. Una vez instalado, se puede ejecutar CUPP en modo interactivo utilizando el comando:

cupp –i

Figura 10

Ejecución de CUPP e Ingreso de Datos personales de la Víctima



Elaborado por: Michael Michay, 2025.

Al ejecutarlo, el sistema solicita una serie de datos personales del objetivo, como el nombre completo, apodo, fecha de nacimiento, nombres de la pareja o hijos, mascota, empresa en la que trabaja y otras palabras clave adicionales (como colores favoritos, gustos, ciudades, etc.). Esta información, que muchas veces las personas comparten abiertamente en redes sociales o con amigos de confianza, puede ser aprovechada por un atacante para generar combinaciones lógicas de posibles contraseñas. CUPP utiliza estos datos para construir un diccionario personalizado, aplicando patrones comunes de comportamiento humano en la creación de claves, lo que incrementa la probabilidad de éxito del ataque al enfocarse en contraseñas predecibles y relacionadas con el entorno personal de la víctima.

1. Una vez completado el ingreso de datos, CUPP crea un archivo .txt que contiene todas las combinaciones posibles de contraseñas. Este archivo se guarda automáticamente en el mismo directorio lo cual se puede acceder a él con utilizando el comando:

Cat ‘nombre del archivo.txt’

Figura 11

Visualización del Archivo Generado.



Elaborado por: Michael Michay, 2025.

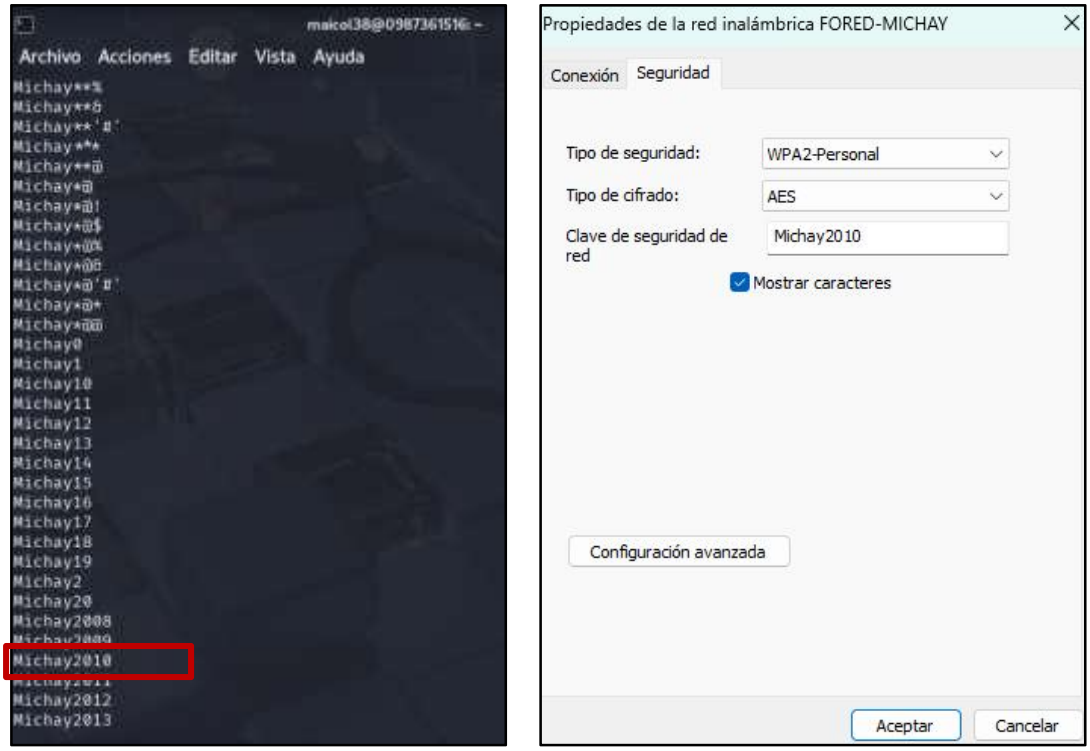
El ataque de diccionario, aunque simple en su ejecución, demostró ser altamente efectivo en este experimento. Tras generar un diccionario personalizado con CUPP utilizando información real de la víctima, se procedió a revisar manualmente el contenido del archivo generado. Al hacerlo, se identificó que una de las entradas coincidía exactamente con la contraseña actual de la red Wi-Fi.

Esta coincidencia confirmó que la clave utilizada era débil y predecible, construida a partir de datos personales fácilmente accesibles.

Este hallazgo subraya la importancia de evitar el uso de información personal al momento de crear contraseñas, y la necesidad urgente de promover prácticas de seguridad más robustas entre los usuarios.

Figura 12

Comparación entre el contenido del diccionario generado por CUPP (izquierda) y la contraseña real registrada en la interfaz del router (derecha), donde se confirma la coincidencia.



Elaborado por: Michael Michay, 2025.

3. Resultado de ataque de captura del handshake wpa/wpa2

El ataque de captura del handshake WPA/WPA2 es una técnica ampliamente utilizada en auditorías de seguridad para redes Wi-Fi. Este ataque consiste en interceptar el proceso de autenticación de 4 vías que se da cuando un cliente (dispositivo) se conecta a un punto de acceso (router).

Este intercambio, conocido como "handshake", contiene datos cifrados que pueden ser utilizados posteriormente en un ataque de diccionario o fuerza bruta para intentar descubrir la contraseña de la red, sin necesidad de estar conectado a ella.

El objetivo no es romper el cifrado directamente (ya que WPA/WPA2 son seguros en ese aspecto), sino aprovechar contraseñas débiles o predecibles usadas por los usuarios.

La técnica de captura del handshake comenzó a ganar popularidad a partir del año 2008, cuando herramientas como aircrack-ng se volvieron accesibles para la comunidad de seguridad. Desde entonces, ha sido una técnica básica de prueba en pentesting (pruebas de penetración) sobre redes inalámbricas.

Con el surgimiento de distribuciones como BackTrack (antecesor de Kali Linux) y luego Kali Linux, esta técnica se estandarizó y se simplificó para pruebas de seguridad en

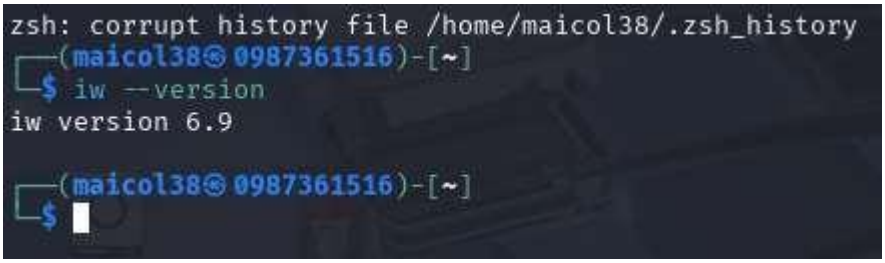
entornos controlados. Hoy en día, sigue siendo uno de los ataques más comunes y efectivos en redes Wi-Fi mal protegidas.

Herramienta utilizada

IW

Figura 13

Versión de IW al ser ejecutado desde la terminal



Elaborado por: Michael Michay, 2025.

Es una herramienta de línea de comandos utilizada para configurar dispositivos inalámbricos en sistemas Linux. Permite cambiar modos de operación (como de managed a monitor), ver información del adaptador, cambiar el canal, entre otras funciones.

Fue desarrollada como reemplazo moderno de la herramienta iwconfig, con soporte completo para nl80211, el nuevo estándar de comunicación con el kernel de Linux para interfaces inalámbricas. Se usa ampliamente desde 2010 en distribuciones como Ubuntu, Debian y Kali.

AIRODUMP-NG

Figura 14

Versión de AIRODUMP-NG al ser ejecutado desde la terminal



Elaborado por: Michael Michay, 2025.

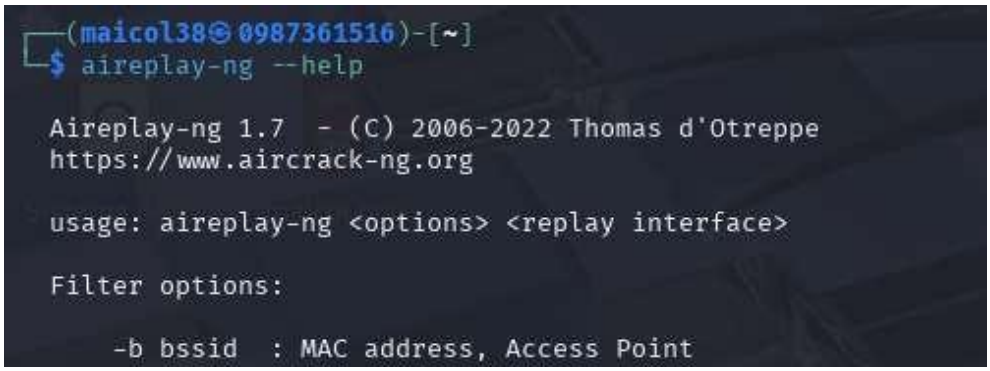
Es una herramienta del paquete Aircrack-ng que permite escanear redes Wi-Fi cercanas, mostrar información de puntos de acceso y clientes conectados, y capturar paquetes, incluyendo el handshake WPA/WPA2.

Lanzado como parte del proyecto Aircrack-ng en los años 2006–2007, airodump-ng se convirtió en una herramienta estándar en auditoría Wi-Fi. Fue diseñado para funcionar específicamente con el modo monitor, facilitando el análisis del tráfico inalámbrico.

AIREPLAY-NG

Figura 15

Versión de AIREPLAY-NG al ser ejecutado desde la terminal



Elaborado por: Michael Michay, 2025.

Es otra herramienta del paquete Aircrack-ng, utilizada para realizar inyecciones de paquetes en redes Wi-Fi. Entre sus usos más comunes están los ataques de desautenticación (deauth) y reinyección de ARP para generar tráfico útil. Como parte de Aircrack-ng, aireplay-ng ha sido una herramienta clave en auditorías Wi-Fi desde la era de WEP cracking hasta pruebas modernas de WPA/WPA2. Se popularizó en BackTrack y ha sido mantenida activamente desde entonces.

Pasos a seguir:

1. Para iniciar el proceso de auditoría, es necesario colocar la tarjeta de red inalámbrica en modo monitor, lo cual permite capturar paquetes que circulan por el aire sin necesidad de estar conectado a una red. Este procedimiento se realiza utilizando los siguientes comandos en la terminal:

sudo ip link set wlan0 down

sudo iw dev wlan0 set type monitor

sudo ip link set wlan0 up

Este método es directo y eficiente, ya que no crea interfaces adicionales, a diferencia de otras herramientas como airmon-ng

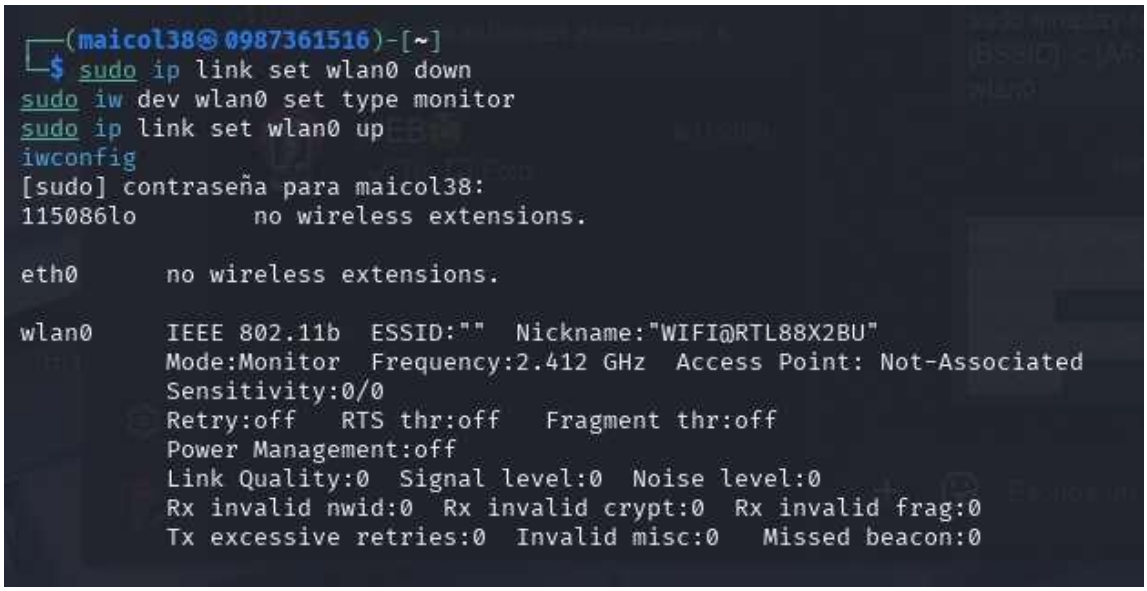
2. Una vez cambiada la interfaz a modo monitor, verifica su estado con:

iwconfig

Esto confirma que la tarjeta está operando en el modo adecuado para capturar paquetes inalámbricos

Figura 16

Verificación del modo monitor en la tarjeta de red inalámbrica usando el comando iwconfig



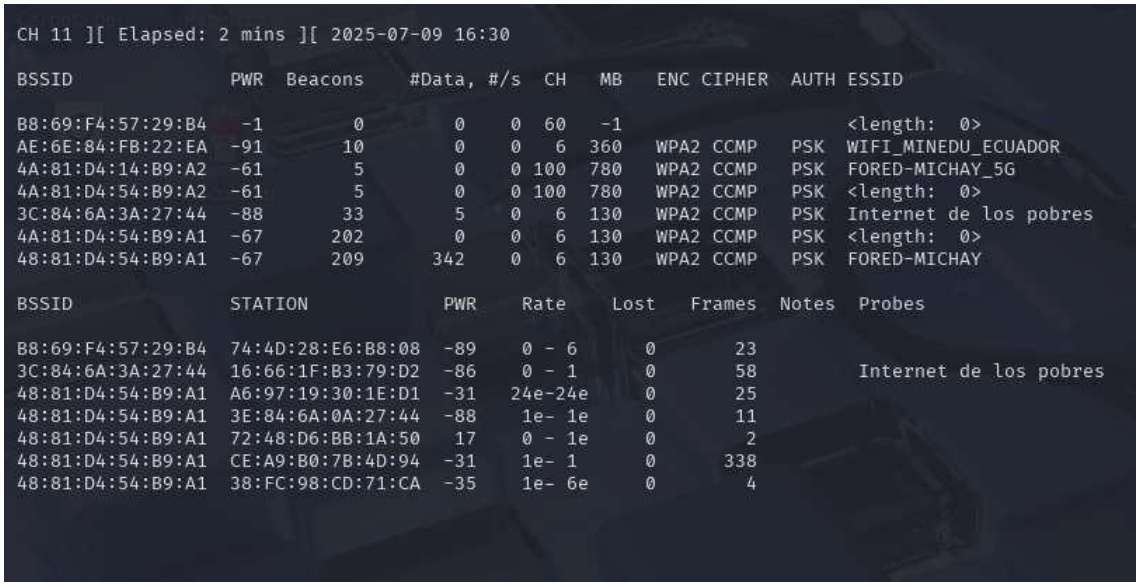
Elaborado por: Michael Michay, 2025.

3. Una Una vez que la tarjeta está en modo monitor, se utiliza airodump-ng para escanear todas las redes inalámbricas disponibles dentro del alcance. Esta herramienta permite identificar el nombre de la red (ESSID), su dirección MAC (BSSID), el canal (CH) en el que transmite, el tipo de cifrado, y los dispositivos conectados usando el siguiente comando:

sudo airodump-ng wlan0

Figura 17

Escaneo de redes inalámbricas cercanas usando airodump-ng



Elaborado por: Michael Michay, 2025.

Este escaneo es fundamental para seleccionar la red objetivo que se desea auditar.

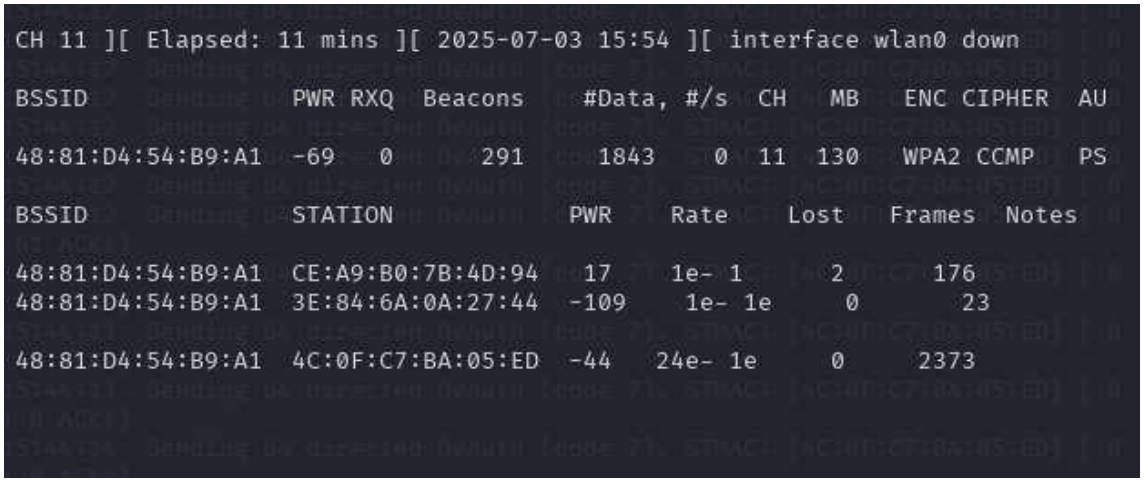
4. Con los datos obtenidos del escaneo anterior (ESSID, BSSID y canal), se inicia la captura del tráfico exclusivamente de la red objetivo. Esto permite almacenar todos los paquetes transmitidos entre el router y los clientes en un archivo con extensión.cap, usando el siguiente comando:

sudo airodump-ng --bssid 48:81:D4:54:B9:A1 -w captura wlan0

Se debe de Mantener esta terminal abierta mientras se realiza el ataque. Aquí es donde se capturará el handshake.

Figura 18

Captura del tráfico de la red objetivo mediante airodump-ng.



Elaborado por: Michael Michay, 2025.

5. Una vez iniciada la captura de paquetes con airodump-ng, es necesario que un cliente (dispositivo conectado) se reconecte al punto de acceso para generar un nuevo handshake WPA/WPA2. Si ningún cliente se reconecta por sí solo, se puede forzar este proceso mediante un ataque de desautenticación (deauth) usando la herramienta aireplay-ng.

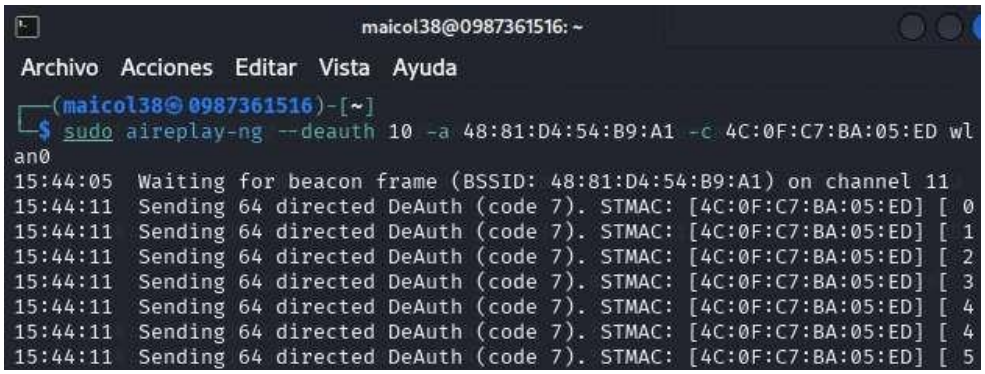
Este ataque envía paquetes especiales que hacen que el router desconecte temporalmente a los clientes. Cuando estos intentan reconectarse, se lleva a cabo nuevamente el proceso de autenticación, permitiendo capturar el handshake.

Comando utilizado:

sudo aireplay-ng --deauth 10 -a 48:81:D4:54:B9:A1 -c 4C:0F:C7:BA:05:ED wlan0

Figura 19

Ejecución del ataque de desautenticación para forzar la reconexión de un cliente.

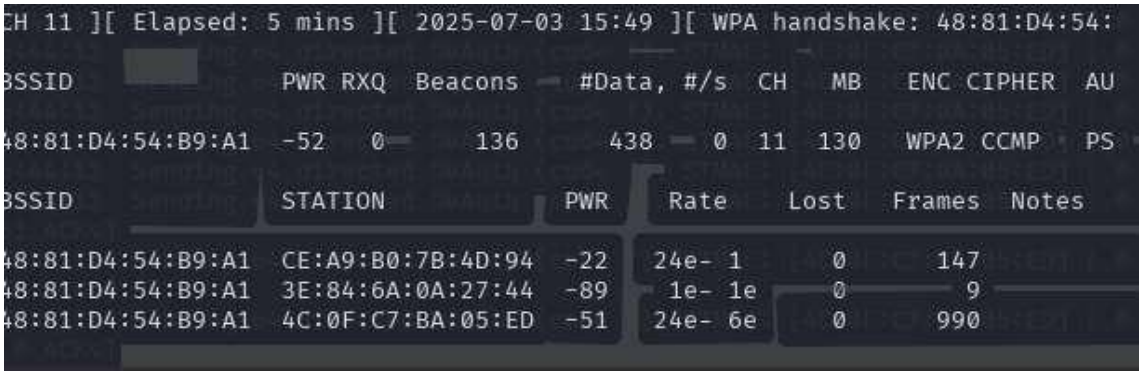


Elaborado por: Michael Michay, 2025.

6. Después de realizar el ataque de desautenticación y mantener activo el proceso de captura, se debe comprobar que el handshake fue efectivamente interceptado.En la parte superior derecha de la terminal, aparecerá el mensaje: WPA handshake: [BSSID]. Esto indica que el proceso de autenticación entre el cliente y el punto de acceso fue registrado correctamente en el archivo .cap.

Figura 20

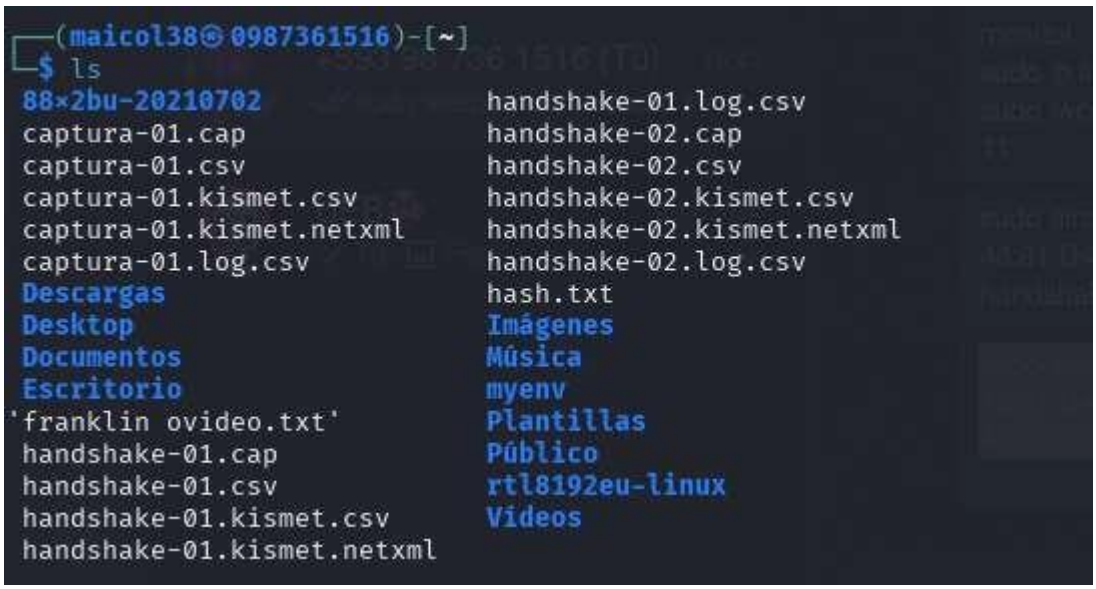
Evidencia de la captura del handshake WPA/WPA2 en la parte superior derecha de la terminal de airodump-ng.



Elaborado por: Michael Michay, 2025.

Figura 21

Visualización del archivo de captura .cap generado en el directorio de trabajo mediante el comando ls.



Elaborado por: Michael Michay, 2025.

Este ataque permitió capturar exitosamente el proceso de autenticación handshake de cuatro vías, que ocurre entre un cliente y un punto de acceso inalámbrico. Esta operación se realizó sin necesidad de conectarse a la red, lo que evidencia una debilidad inherente al diseño del protocolo: el handshake puede ser interceptado pasivamente por cualquier atacante en las cercanías.

El archivo generado (.cap) contiene información crítica de ese proceso de autenticación, la cual puede ser utilizada posteriormente en un ataque de diccionario o fuerza bruta para intentar descifrar la contraseña de la red Wi-Fi. Esto representa una vulnerabilidad significativa, especialmente en redes que utilizan contraseñas débiles, predecibles o reutilizadas.

4. **Resultado del ataque evil twin**

El ataque Evil Twin, también conocido como Gemelo Malvado, es una técnica de suplantación de redes Wi-Fi que consiste en crear un punto de acceso (Access Point) falso que simula ser una red legítima al replicar su SSID (nombre de red) y configuración. Su propósito es engañar a los usuarios para que se conecten al AP malicioso, creyendo que están accediendo a su red habitual.

Una vez conectados, el atacante puede interceptar datos sensibles como nombres de usuario, contraseñas, tokens de sesión, cookies o incluso realizar ataques.

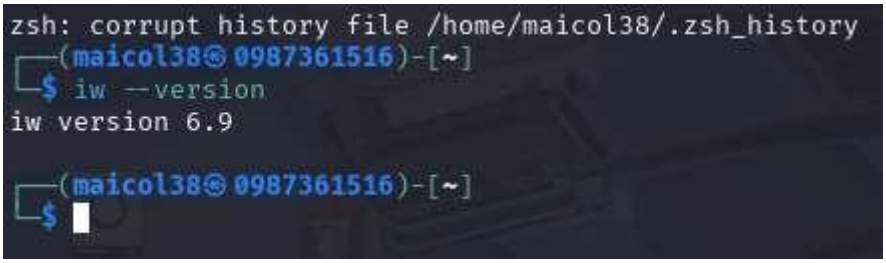
Este tipo de ataque se popularizó en los años 2000, cuando los ciberatacantes comenzaron a aprovechar la falta de autenticación mutua en redes Wi-Fi abiertas. A lo largo de los años, ha evolucionado y es empleado en campañas de espionaje, robo de identidad y pruebas de penetración, siendo una amenaza real en entornos públicos como cafeterías, aeropuertos o bibliotecas.

Herramienta utilizada

IW

Figura 22

Versión de IW al ser ejecutado desde la terminal



Elaborado por: Michael Michay, 2025.

Es una herramienta de línea de comandos utilizada para configurar dispositivos inalámbricos en sistemas Linux. Permite cambiar modos de operación (como de managed a monitor), ver información del adaptador, cambiar el canal, entre otras funciones.

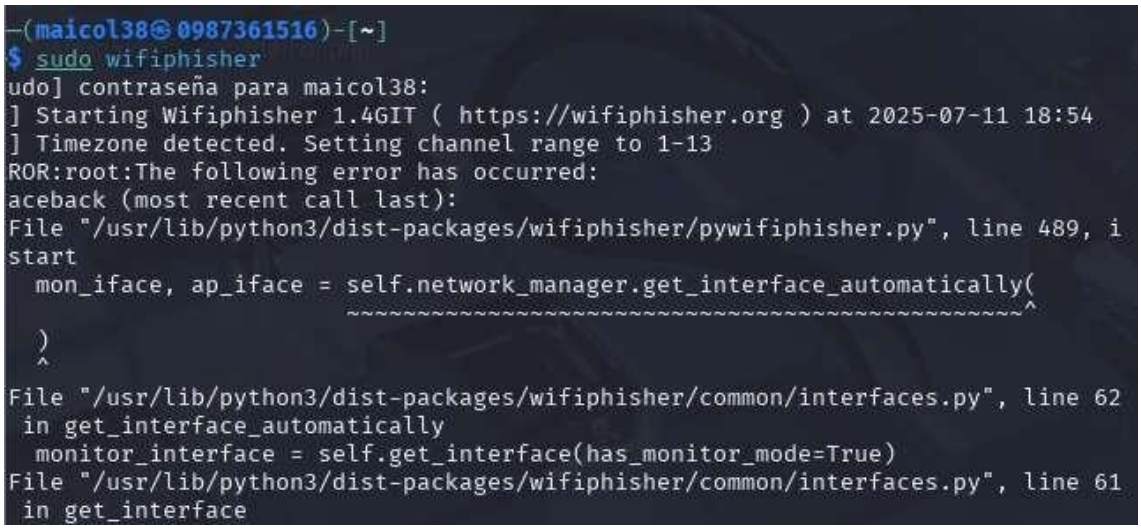
Fue desarrollada como reemplazo moderno de la herramienta iwconfig, con soporte completo para nl80211, el nuevo estándar de comunicación con el kernel de Linux para

interfaces inalámbricas. Se usa ampliamente desde 2010 en distribuciones como Ubuntu, Debian y Kali.

WIFIPHISHER

Figura 23

Versión de WIFIPHISHER al ser ejecutado desde la terminal



Elaborado por: Michael Michay, 2025.

Es una herramienta de línea de comandos, de código abierto y escrita en Python, especializada en la ejecución de ataques de ingeniería social contra redes Wi-Fi. Es ampliamente utilizada en auditorías de seguridad inalámbrica, particularmente para la creación de puntos de acceso falsos (Evil Twin) y la captura de credenciales mediante técnicas de phishing.

Pasos a seguir:

1. Para iniciar el proceso de auditoría, es necesario colocar la tarjeta de red inalámbrica en modo monitor, lo cual permite capturar paquetes que circulan por el aire sin necesidad de estar conectado a una red. Este procedimiento se realiza utilizando los siguientes comandos en la terminal:

sudo ip link set wlan0 down

sudo iw dev wlan0 set type monitor

sudo ip link set wlan0 up

Este método es directo y eficiente, ya que no crea interfaces adicionales, a diferencia de otras herramientas como airmon-ng

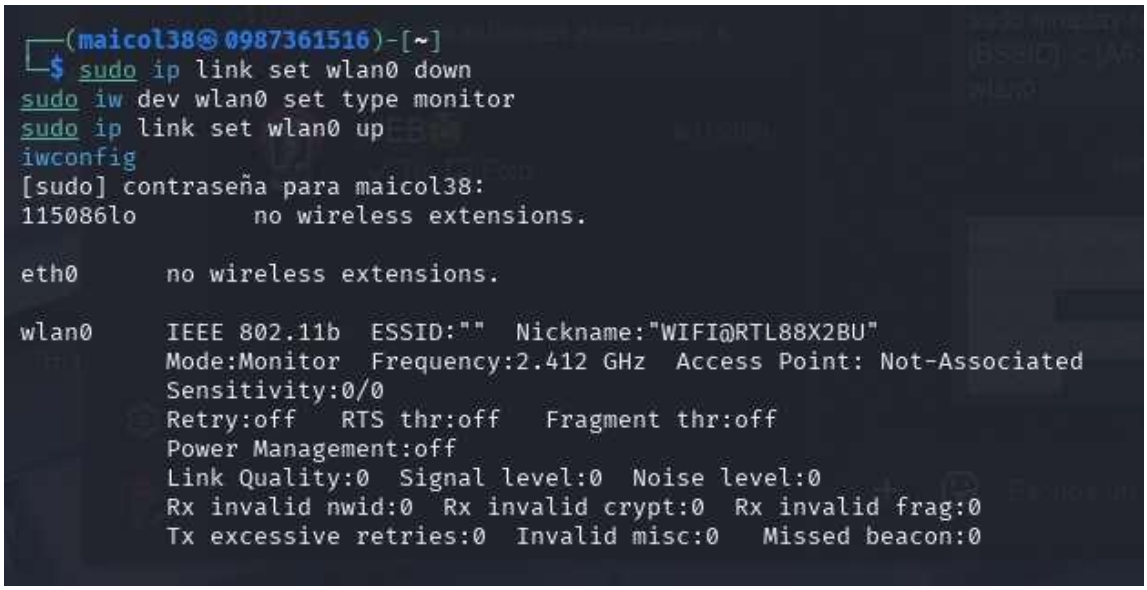
2. Una vez cambiada la interfaz a modo monitor, verifica su estado con:

iwconfig

Esto confirma que la tarjeta está operando en el modo adecuado para capturar paquetes inalámbricos

Figura 24

Verificación del modo monitor en la tarjeta de red inalámbrica usando el comando iwconfig



Elaborado por: Michael Michay, 2025.

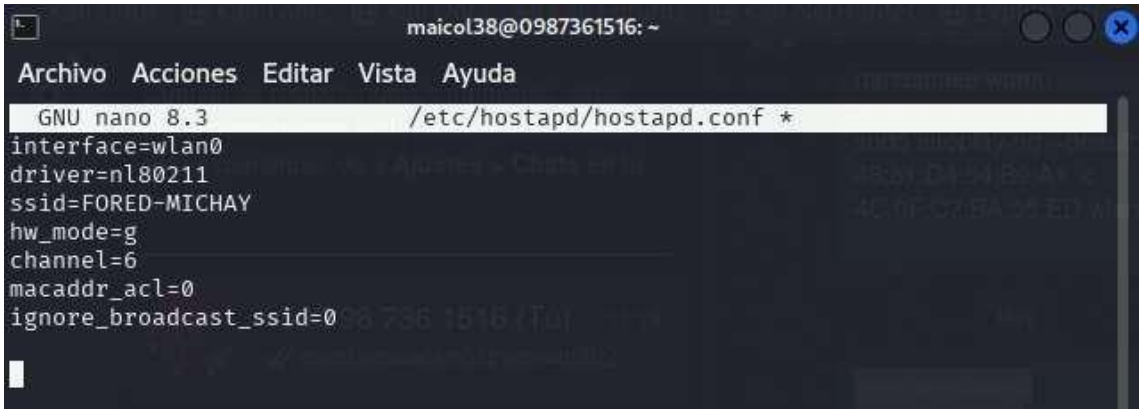
3. Para empezar el ataque, se ejecuta Wifiphisher desde la terminal con permisos de superusuario con el siguiente comando:

sudo wifiphisher

Una vez iniciado, la herramienta comienza a escanear las redes Wi-Fi cercanas. Luego muestra una lista de redes disponibles para que el usuario elija una como objetivo.

Figura 25

Ejecución de WIFIPHISHER desde la terminal de kali linux



Elaborado por: Michael Michay, 2025.

Wifiphisher hace todo de forma automática:

- Desconecta a los usuarios que están conectados a esa red
- Crea un punto de acceso falso con el mismo nombre de la red real.
- Cuando los usuarios intentan conectarse, son redirigidos a una página falsa.
- En esa página, se les pide que ingresen su contraseña o algún dato, y si lo hacen, la herramienta captura esa información.

Figura 26

Lista de redes WIFI cercanas al ejecutar el ataque Wifiphisher



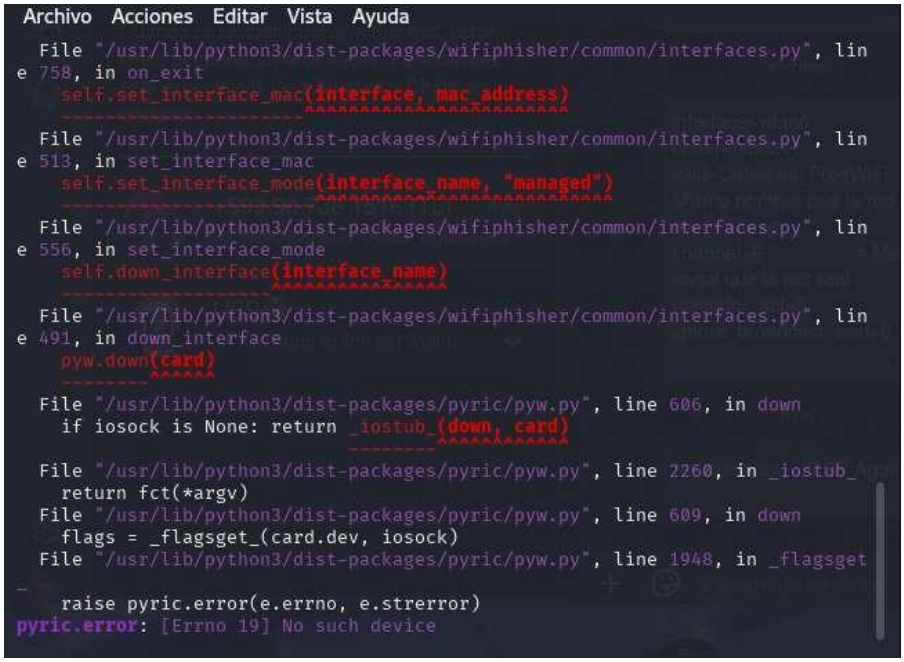
Elaborado por: Michael Michay, 2025.

4. Durante la ejecución del ataque, se utilizó una tarjeta de red TP-Link Archer T4U v3, equipada con el chipset Realtek RTL88x2BU. Sin embargo, se presentaron varias dificultades técnicas que impidieron completar el ataque correctamente:

El chipset no soporta completamente el modo monitor lo cual genero errores como pyric.error: [Errno 22] Invalid argument al no logrór levantar correctamente el punto de acceso gemelo ni completar la fase de redirección.

Figura 27

Error generado por incompatibilidad del chipset RTL88x2BU.



Elaborado por: Michael Michay, 2025.

El ataque no pudo completarse con éxito debido a incompatibilidades técnicas del adaptador Wi-Fi utilizado. A pesar de múltiples intentos y ajustes en la configuración, la herramienta no logró ejecutar correctamente el ataque por las siguientes razones principales:

El adaptador TP-Link Archer T4U v3, equipado con el chipset RTL88x2BU, presenta limitaciones en cuanto al soporte para modo monitor, inyección de paquetes y cambio de canal, funciones esenciales para el correcto funcionamiento de Wifiphisher.

Además, es importante destacar que muchos de los adaptadores de red inalámbrica más recientes no cuentan con compatibilidad plena para estas operaciones avanzadas, lo que dificulta significativamente la realización de ataques como Evil Twin. Esta situación se ve agravada por la limitada disponibilidad y elevado costo de adaptadores compatibles en el mercado ecuatoriano, lo que representa una barrera para profesionales y entusiastas de la ciberseguridad que desean llevar a cabo auditorías inalámbricas efectivas.

5. Resultado de ataque de desautenticación

El ataque de desautenticación (Deauth Attack) es una técnica utilizada en auditorías de seguridad Wi-Fi para forzar la desconexión de los dispositivos conectados a una red inalámbrica. Aprovecha una vulnerabilidad del protocolo IEEE 802.11, donde los mensajes de control como la autenticación y desautenticación no están cifrados.

Aunque fue diseñado originalmente como parte del funcionamiento legítimo del protocolo Wi-Fi (por ejemplo, para que un punto de acceso pueda expulsar a un cliente), este comportamiento puede ser explotado con fines maliciosos o de prueba.

Este tipo de ataque es conocido desde hace más de una década. Se popularizó como una técnica eficaz para:

Forzar la captura del handshake WPA/WPA2.

Preparar ataques de tipo Evil Twin.

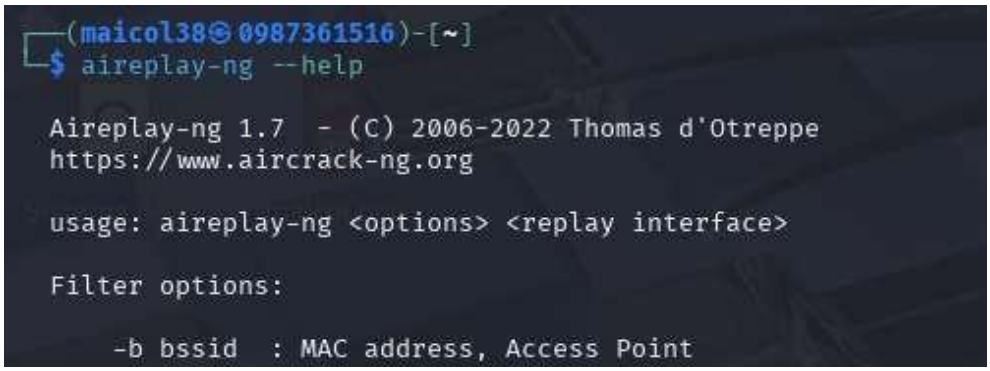
Interrumpir el servicio de conexión de una red inalámbrica.

Herramienta utilizada

AIREPLAY-NG

Figura 28

Versión de AIRODUMP-NG al ser ejecutado desde la terminal



Elaborado por: Michael Michay, 2025.

Es una herramienta diseñada específicamente para realizar inyecciones de paquetes en redes Wi-Fi. Su funcionalidad principal incluye ataques de autenticación y desautenticación (deauth), así como la reinyección de paquetes ARP para generar tráfico útil en la red objetivo.

Desde sus inicios, aireplay-ng ha sido una pieza fundamental en auditorías de seguridad inalámbrica. Inicialmente se popularizó durante la era del cifrado WEP, gracias a distribuciones como BackTrack, y ha mantenido su relevancia en pruebas contra redes WPA/WPA2, siendo actualizada y utilizada ampliamente en entornos de pruebas de penetración y análisis forense de redes Wi-Fi.

Pasos a seguir:

1. Para iniciar el proceso de auditoría, es necesario colocar la tarjeta de red inalámbrica en modo monitor, lo cual permite capturar paquetes que circulan por el aire sin necesidad de estar conectado a una red. Este procedimiento se realiza utilizando los siguientes comandos en la terminal:

sudo ip link set wlan0 down

sudo iw dev wlan0 set type monitor

sudo ip link set wlan0 up

Este método es directo y eficiente, ya que no crea interfaces adicionales, a diferencia de otras herramientas como airmon-ng

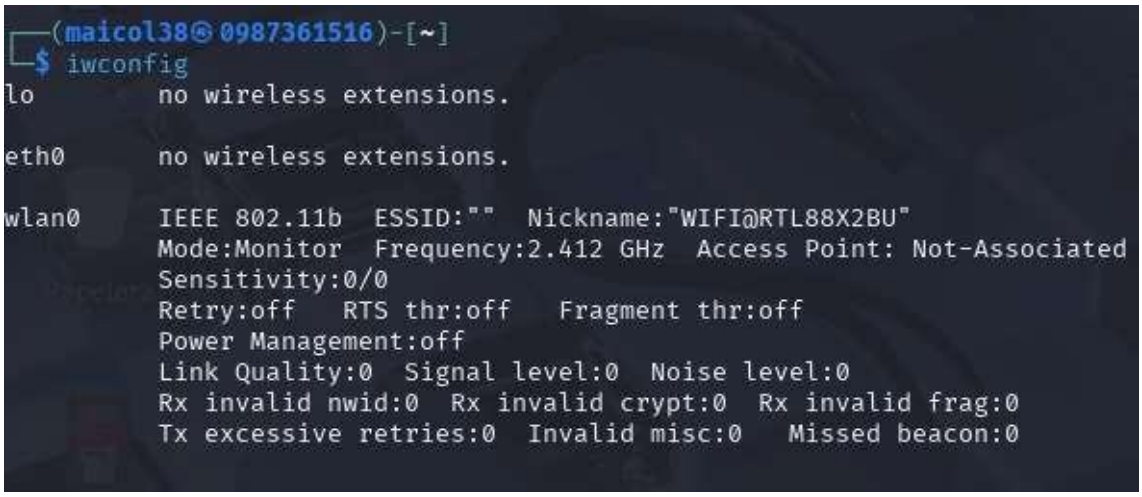
2. Una vez cambiada la interfaz a modo monitor, verifica su estado con:

iwconfig

Esto confirma que la tarjeta está operando en el modo adecuado para capturar paquetes inalámbricos

Figura 29

Verificación del modo monitor en la tarjeta de red inalámbrica usando el comando iwconfig

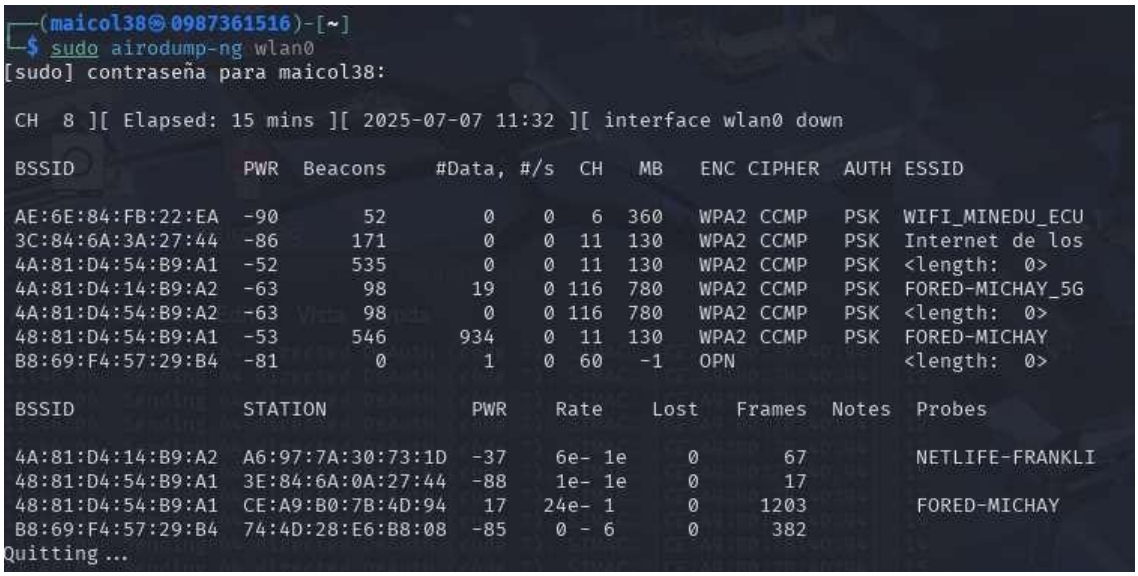


Elaborado por: Michael Michay, 2025.

3. Una vez que la tarjeta está en modo monitor, se utiliza airodump-ng para escanear todas las redes inalámbricas disponibles dentro del alcance.

Figura 30

Captura del tráfico de la red objetivo mediante airodump-ng.



Elaborado por: Michael Michay, 2025.

4. Antes de realizar el ataque, es necesario fijar el canal en el que se encuentra la red objetivo. Esto permite que la herramienta aireplay-ng funcione correctamente, ya que debe operar en el mismo canal que el punto de acceso. Se lo realiza con el siguiente comando.

sudo iwconfig wlan0 channel [número de canal]

Figura 31

Captura del canal fijado con el comando sudo iwconfig wlan0 channel 11



Elaborado por: Michael Michay, 2025.

5. Una vez fijado el canal, se lanza el ataque para desconectar a un cliente específico de la red seleccionada. Usando el siguiente comando.

sudo aireplay-ng --deauth 10 -a 48:81:D4:54:B9:A1 -c CE:A9:B0:7B:4D:94 wlan0

Figura 32

Captura de salida en pantalla donde se muestra el envió de paquetes indicando que el ataque está activo



Elaborado por: Michael Michay, 2025.

6. En la imagen anterior se evidencia en consola la ejecución del ataque de desautenticación, donde se muestran múltiples líneas con el mensaje

Sending 64 directed DeAuth (code 7). STMAC: [MAC_cliente]

Esto indica que los paquetes de desautenticación fueron enviados correctamente al cliente objetivo. La efectividad del ataque se corrobora visualmente en la Figura 31, donde se muestra el dispositivo móvil víctima sufriendo la desconexión repentina de la red Wi-Fi.

Figura 33

Dispositivo víctima muestra desconexión repentina de la red Wi-Fi tras la ejecución del ataque.



Elaborado por: Michael Michay, 2025.

El ataque de desautenticación se llevó a cabo con éxito, ya que se logró desconectar al dispositivo de la red Wi-Fi seleccionada. En la consola del atacante se pudo observar que se estaban enviando los paquetes necesarios para forzar esa desconexión. Al mismo tiempo, en el dispositivo víctima se evidenció la pérdida de conexión, ya que el ícono de Wi-Fi desapareció y la red dejó de estar visible por unos momentos. Esto confirma que el ataque funcionó correctamente y que fue posible interrumpir la conexión de manera temporal o incluso indefinida, dependiendo de la cantidad de paquetes enviados y la duración del proceso.

6. Resultado de ataque de punto de acceso falso

El Ataque de Punto de Acceso Falso, también conocido como Fake AP, es una técnica de ingeniería social y suplantación de redes utilizada para engañar a los usuarios haciéndoles

creer que están conectados a una red Wi-Fi legítima, cuando en realidad están conectados a una red creada y controlada por el atacante.

Este ataque permite capturar información sensible de los usuarios, como credenciales, datos de navegación o realizar un ataque del tipo Hombre en el Medio (MITM). Es comúnmente utilizado en entornos de pruebas de penetración para evaluar la conciencia de seguridad de los usuarios y la protección de los dispositivos frente a redes no confiables.

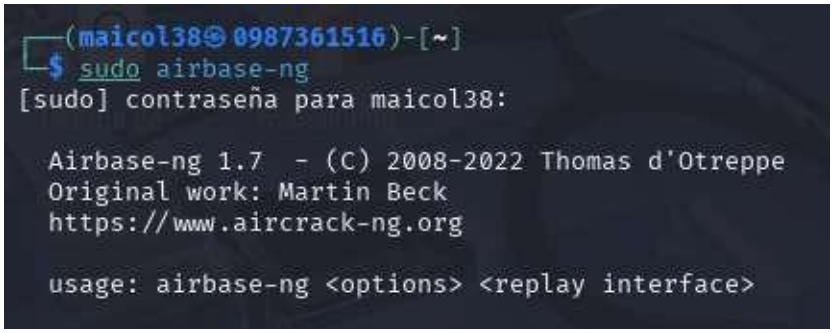
Los ataques de Punto de Acceso Falso se conocen desde principios de los años 2000, cuando se evidenció que muchos dispositivos se conectaban automáticamente a redes abiertas con nombres conocidos (SSID). Con el tiempo, herramientas como Airbase-ng, hostapd, y Wifiphisher facilitaron la automatización del proceso, integrando portales cautivos falsos y servidores de captura para realizar ataques más complejos de manera sencilla.

Herramienta utilizada

AIRBASE-NG

Figura 34

Versión de Airbase-ng al ser ejecutado desde el terminal



Elaborado por: Michael Michay, 2025.

es una herramienta de la suite Aircrack-ng que permite crear puntos de acceso Wi-Fi falsos (Fake APs). Se utiliza para simular redes inalámbricas legítimas con el fin de atraer a los dispositivos cercanos.

DNSMASQ

Figura 35

Versión de Dnsmasq al ser ejecutado desde el terminal



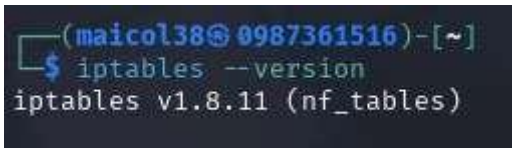
Elaborado por: Michael Michay, 2025.

Es un servicio ligero que actúa como servidor DHCP y DNS. Se utiliza para asignar direcciones IP automáticamente a los dispositivos que se conecten al punto de acceso falso, y también para resolver nombres de dominio, redirigiendo cualquier intento de acceso web hacia la dirección IP del atacante.

IPTABLES

Figura 36

Versión de Iptables al ser ejecutado desde el terminal



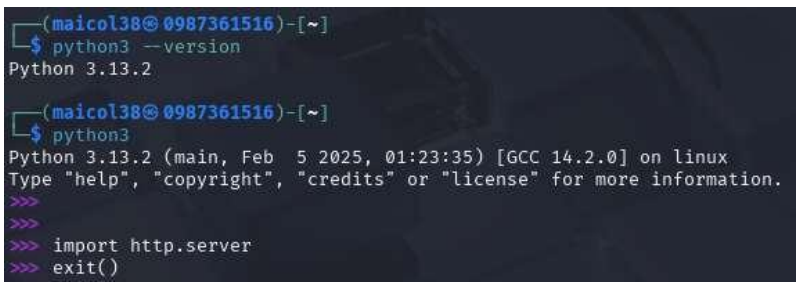
Elaborado por: Michael Michay, 2025.

Es una herramienta de configuración de reglas de firewall en Linux. Permite controlar el tráfico de red, redirigirlo, bloquearlo o modificarlo. En este contexto, se utiliza para redirigir automáticamente todo el tráfico HTTP (puerto 80) hacia el portal falso alojado localmente en el sistema del atacante.

IPTABLES

Figura 37

Versión de Python(http.server) al ser ejecutado desde el terminal



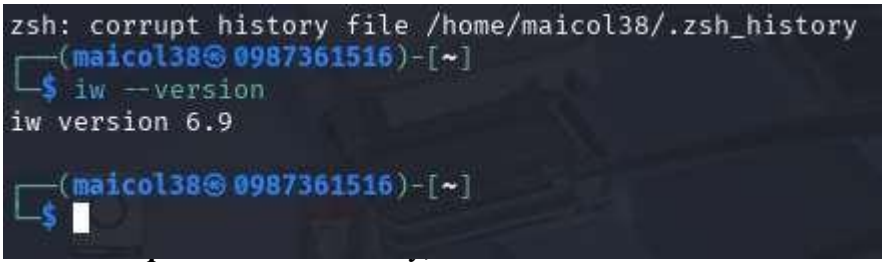
Elaborado por: Michael Michay, 2025.

El módulo http.server de Python permite levantar un servidor web básico de forma rápida y sencilla, sin necesidad de instalar software adicional. Este servidor puede alojar páginas HTML simples, como un portal de inicio de sesión falso.

IW

Figura 38

Versión de IW al ser ejecutado desde la terminal



Es una herramienta de línea de comandos utilizada para configurar dispositivos inalámbricos en sistemas Linux. Permite cambiar modos de operación (como de managed a monitor), ver información del adaptador, cambiar el canal, entre otras funciones.

Pasos a seguir:

1. Para iniciar el proceso de auditoría, es necesario colocar la tarjeta de red inalámbrica en modo monitor. Este procedimiento se realiza utilizando los siguientes comandos en la terminal:

sudo ip link set wlan0 down

sudo iw dev wlan0 set type monitor

sudo ip link set wlan0 up

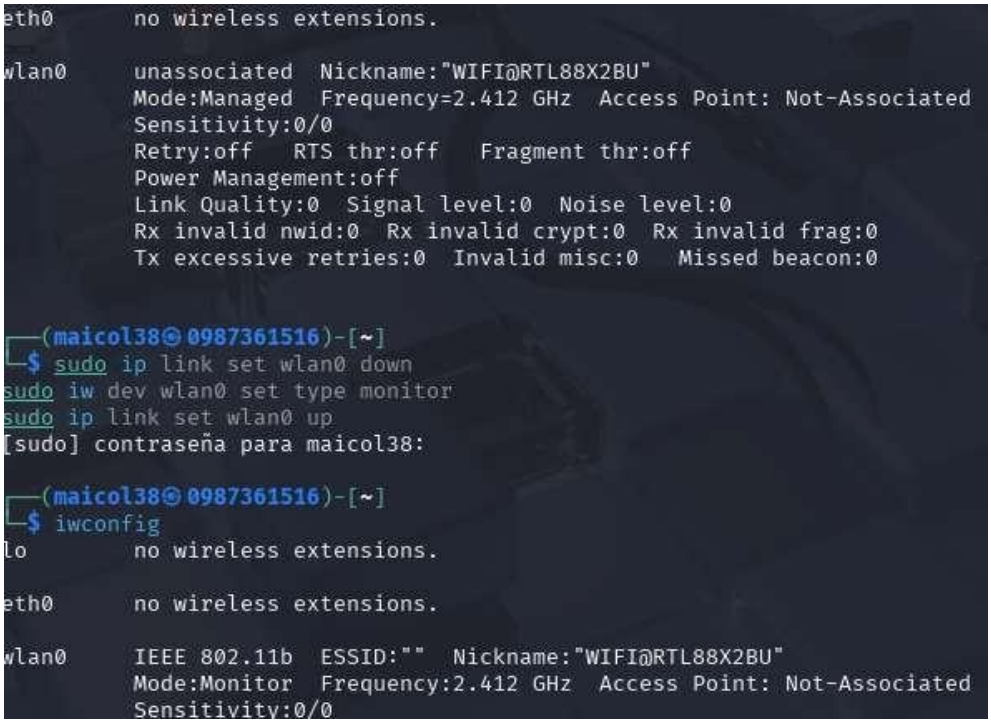
2. Una vez cambiada la interfaz a modo monitor, verifica su estado con:

iwconfig

Esto confirma que la tarjeta está operando en el modo adecuado para capturar paquetes inalámbricos

Figura 39

Verificación del modo monitor en la tarjeta de red inalámbrica usando el comando iwconfig



Elaborado por: Michael Michay, 2025.

3. Luego se procede a crear el AP falso con airbase-ng la cual crea una red WiFi falsa con el SSID deseado usando el siguiente comando:

Sudo airbase-ng –e “FORED-MICHAY-FALSO” –c 11 wlan0

Figura 40

Ejecución del comando airbase-ng para crear un punto de acceso falso con el SSID "Red_Legítima_Falsa". En la terminal se muestra la creación de la interfaz virtual at0, indicando que la red Wi-Fi falsa ya está activa y lista para atraer víctimas.



Elaborado por: Michael Michay, 2025.

Figura 41

Lista de redes wifi junto a red Falsa en la pc y teléfono.

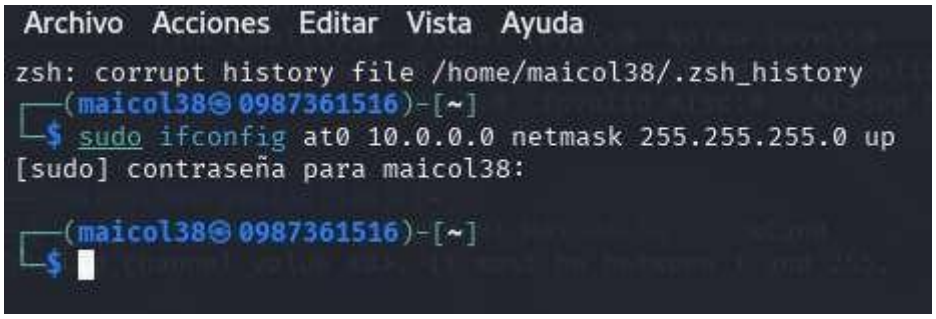


Elaborado por: Michael Michay, 2025.

4. Asignación de dirección IP estática a la interfaz virtual at0 generada por airbase-ng. Esta configuración es fundamental para que los dispositivos conectados a la red falsa reciban respuesta.

Figura 42

Configuración de IP en la interfaz at0



Elaborado por: Michael Michay, 2025.

5. Seguido se configura el dnsmasq.conf donde se asigna la dirección ip a los clientes conectados al AP falso.

Figura 43

Ejecución de dnsmasq para asignar IPs a dispositivos conectados.



Elaborado por: Michael Michay, 2025.

6. Seguido se redirige el tráfico HTTP entrante hacia el servidor web que contiene el portal falso. Esta redirección es clave para interceptar peticiones de los usuarios conectados. Con el siguiente comando:

sudo iptables --flush

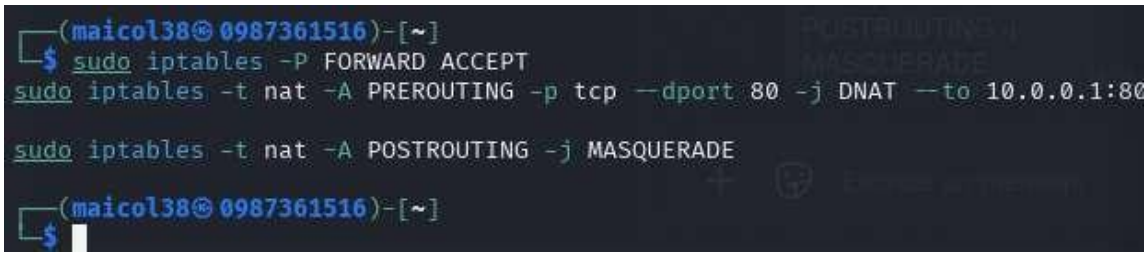
Figura 44

Ejecución de redirección con iptables.



Figura 45

Crear redirección del tráfico HTTP hacia tu servidor local:



Elaborado por: Michael Michay, 2025.

7. Se procede a crear el portal web falso lo cual se procede con la creación del archivo index.html que simula una página de inicio de sesión para acceder a la red Wi-Fi. Esta interfaz visual engaña al usuario para que introduzca credenciales.

Luego se realiza la ejecución del servidor HTTP local utilizando http.server de Python en el puerto 80. Esta acción permite que el archivo index.html esté accesible para los dispositivos conectados a la red falsa.

Figura 46

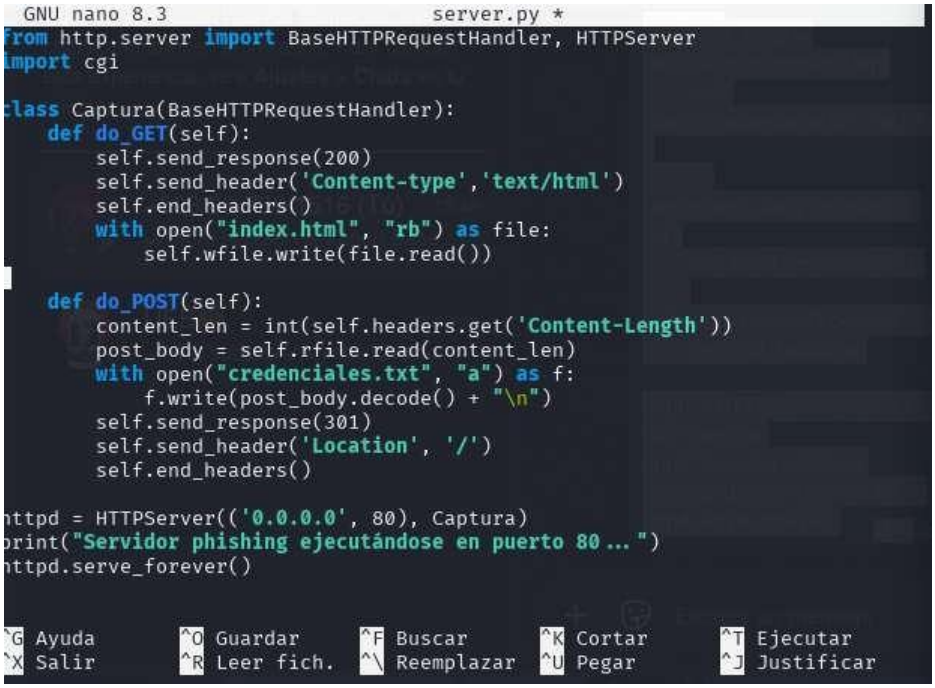
Visualización del Código del portal web falso creado en HTML.



Elaborado por: Michael Michay, 2025.

Figura 47

Visualización del servidor web activo mostrando el portal falso.



Elaborado por: Michael Michay, 2025.

8. Finalmente se inicia un servidor HTTP en el puerto 80 utilizando Python utilizando el siguiente código

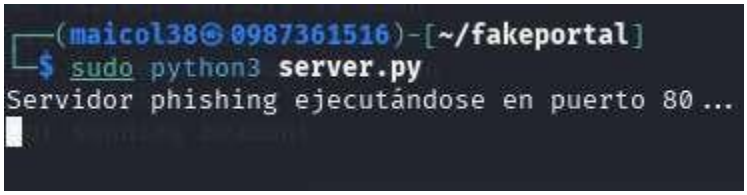
sudo python3 server.py

Este comando levanta un servidor web simple, que sirve el contenido del directorio a través del puerto 80. Dado que previamente redirigen todo el tráfico HTTP hacia la dirección IP local 10.0.0.1, cualquier dispositivo que se conecte al AP falso será automáticamente dirigido al portal falso sin necesidad de escribir una URL específica.

De este modo, al abrir cualquier navegador en el dispositivo víctima, se muestra automáticamente la página falsa de inicio de sesión, simulando una red Wi-Fi que requiere autenticación, lo que aumenta la probabilidad de que el usuario introduzca credenciales sensibles.

Figura 48

Terminal mostrando la ejecución del servidor web en el puerto 80



Elaborado por: Michael Michay, 2025.

Figura 49

Visualización de la página web falsa desde un navegador en un dispositivo conectado a la red falsa. El sitio se carga automáticamente al acceder a cualquier URL, redirigiendo a la IP 10.0.0.1 donde está alojado el portal HTML.



Elaborado por: Michael Michay, 2025.

El ataque de Punto de Acceso Falso**,** evidencia cómo un atacante puede aprovecharse de la confianza del usuario y la falta de validación en redes Wi-Fi para suplantar una red legítima y capturar información confidencial sin necesidad de vulnerar directamente ningún dispositivo.

Este tipo de ataque es altamente efectivo en entornos públicos o donde los usuarios se conectan a redes abiertas o poco seguras, como cafeterías, aeropuertos o centros comerciales. Su ejecución no requiere conocimientos extremadamente avanzados, lo que lo convierte en una amenaza accesible para atacantes con recursos limitados.

7. Resultado de ataque de hombre en el medio

El ataque Hombre en el Medio (Man-in-the-Middle, MITM) es una técnica de interceptación en la que un atacante se posiciona entre dos dispositivos que se están comunicando, generalmente entre un cliente y su puerta de enlace (router), sin que ninguno de los dos tenga conocimiento de la intervención. Desde esa posición, el atacante puede observar, modificar o redirigir el tráfico transmitido, lo que lo convierte en una amenaza crítica para la confidencialidad y la integridad de los datos.

Este ataque ha sido conocido desde los primeros días de las redes TCP/IP, cuando las redes no utilizaban cifrado y la suplantación de identidades (spoofing) era relativamente simple. A lo largo del tiempo, con la introducción de protocolos como HTTPS y mecanismos de autenticación, el ataque MITM ha evolucionado, utilizando métodos como ARP spoofing, DNS spoofing y SSL stripping para seguir siendo efectivo.

En auditorías de seguridad, el ataque MITM es utilizado para detectar vulnerabilidades en redes, identificar malas prácticas de configuración y demostrar la importancia del cifrado de extremo a extremo.

Herramienta utilizada

TEE

Figura 50

Versión de TEE al ser ejecutado desde el terminal



Elaborado por: Michael Michay, 2025.

Es una herramienta de línea de comandos que permite redirigir la salida de un comando y escribirla directamente en un archivo, incluso en archivos de sistema que requieren permisos elevados. Es especialmente útil para habilitar funciones como el reenvío de paquetes modificando archivos protegidos como /proc/sys/net/ipv4/ip_forward.

CAT

Figura 51

Versión de CAT al ser ejecutado desde el terminal



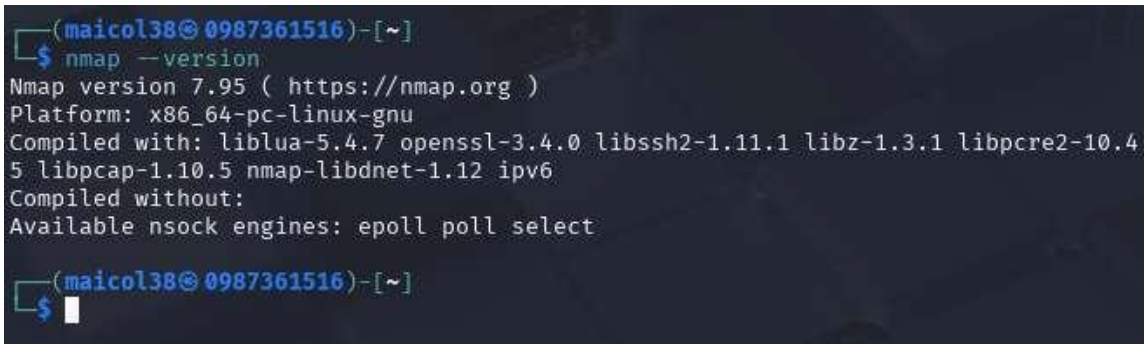
Elaborado por: Michael Michay, 2025.

La herramienta cat se usa comúnmente para visualizar el contenido de archivos en la terminal. En tareas de auditoría, permite revisar configuraciones de red, logs del sistema o archivos capturados por otras herramientas.

NMAP –SN

Figura 52

Versión de NMAP al ser ejecutado desde el terminal



Elaborado por: Michael Michay, 2025.

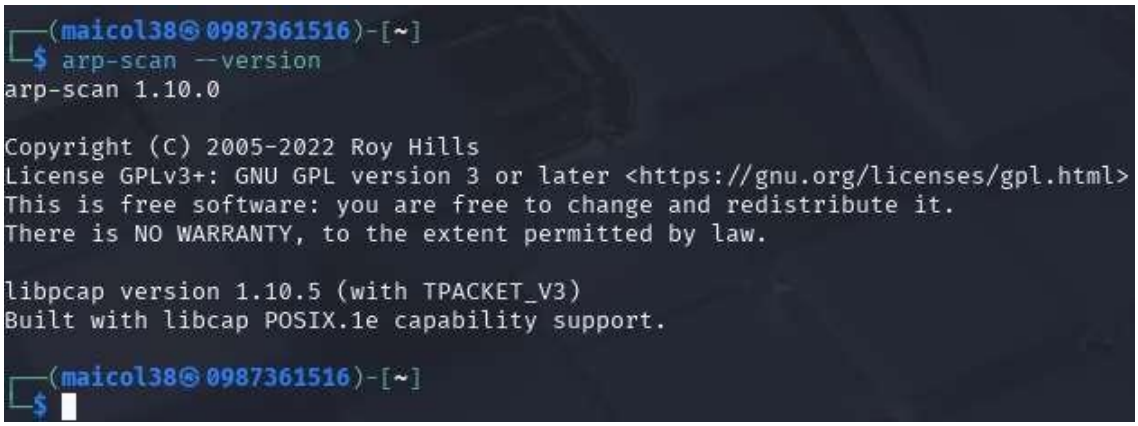
Nmap es una herramienta de escaneo de redes. La opción -sn (ping scan) permite descubrir dispositivos activos dentro de una red sin escanear puertos, útil para mapear

rápidamente la red y encontrar posibles víctimas o el router objetivo antes de lanzar un ataque MITM.

ARP-SCAN

Figura 53

Versión de arp-scan al ser ejecutado desde el terminal



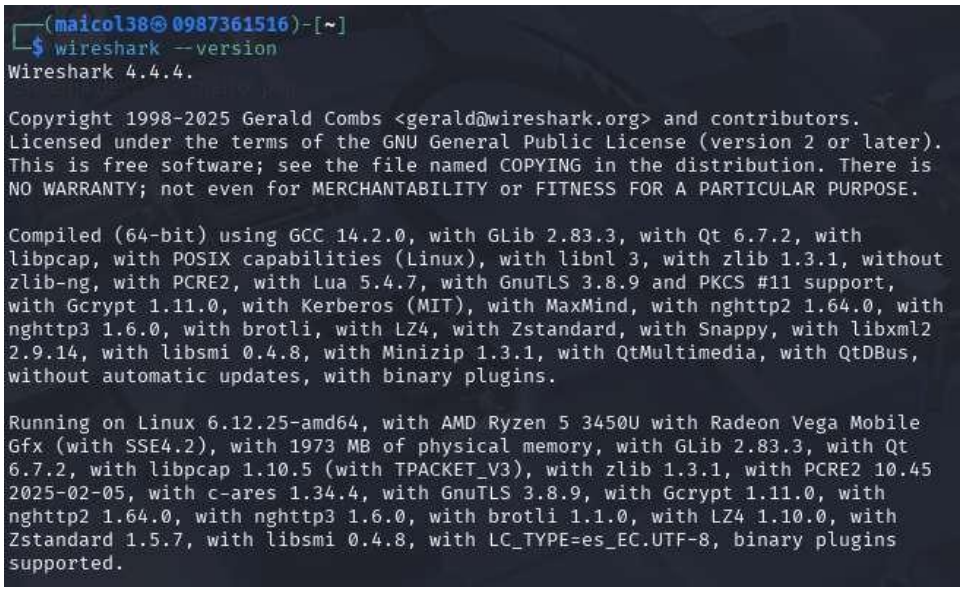
Elaborado por: Michael Michay, 2025.

Es una herramienta que realiza escaneo ARP en la red local, identificando todos los dispositivos conectados mediante su dirección IP y MAC. Es muy preciso para descubrir dispositivos dentro de la LAN y es ideal para ataques basados en ARP spoofing, como MITM.

WIRESHARK

Figura 54

Versión de wireshark al ser ejecutado desde el terminal



Elaborado por: Michael Michay, 2025.

Es un analizador gráfico de protocolos de red. Permite capturar y visualizar en tiempo real el tráfico que circula por la red. Es fundamental en auditorías para identificar credenciales, cookies, peticiones DNS o cualquier tipo de paquete transmitido durante un ataque.

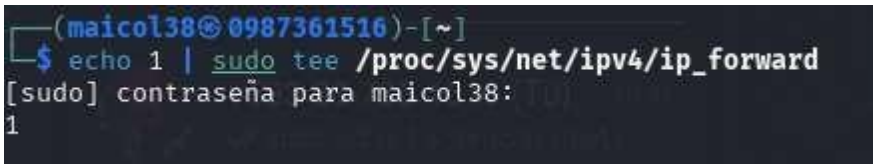
Pasos a seguir:

1. Para realizar el ataque es necesario permitir que los paquetes puedan ser reenviados por el sistema para no interrumpir la comunicación entre la víctima y el router. Utilizando el siguiente comando

echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

Figura 55

Ejecución de sudo desde el terminal



Elaborado por: Michael Michay, 2025.

Figura 56

Verificación del resultado en consola



Elaborado por: Michael Michay, 2025.

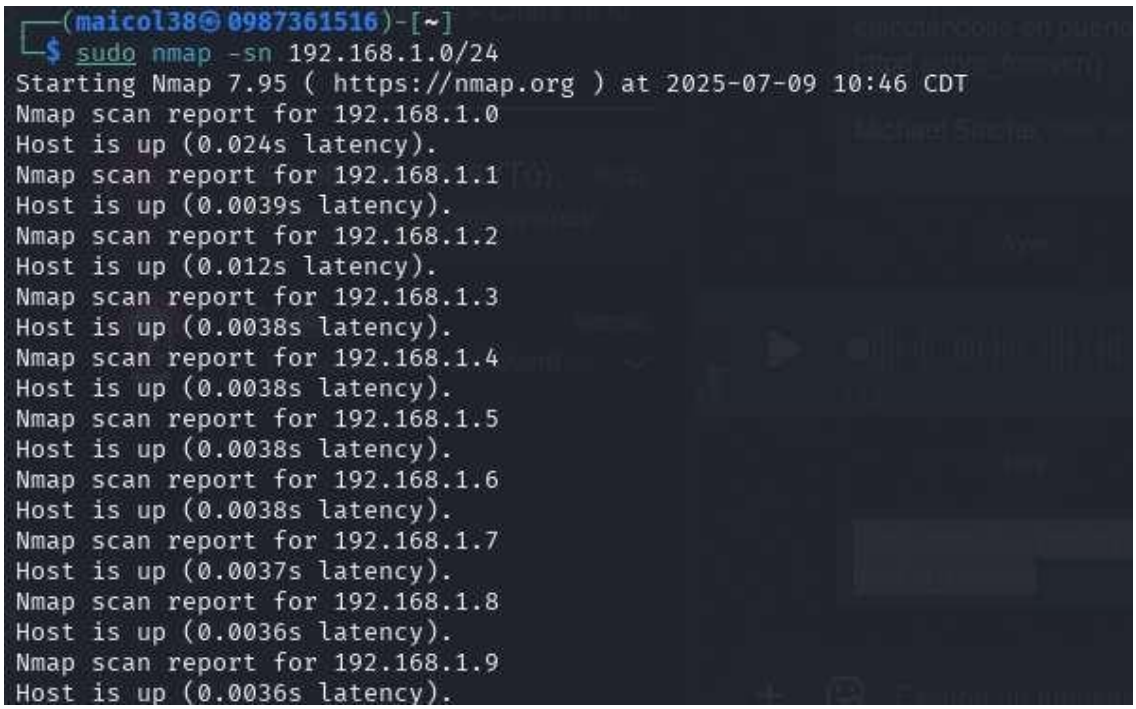
Para la verificación se debe de mostrar el resultado de 1 en consola y se comprueba que el comando se está ejecutando de manera correcta.

2. Posterior mente se procede a realizar un escaneo para determinar qué dispositivos están conectados a la red local y seleccionar las IPs objetivo: el router y un dispositivo víctima. Utilizando el siguiente comando:

sudo nmap -sn 192.168.1.0/24

Figura 57

Listado de redes escaneadas para realizar el ataque.



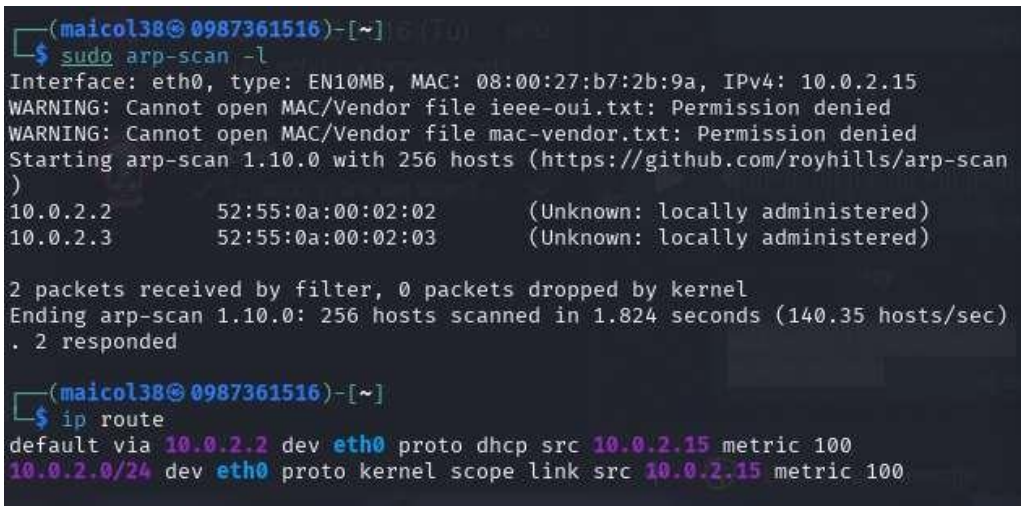
Elaborado por: Michael Michay, 2025.

3. Verificar dispositivos mediante ARP al cual se identificaron con precisión las direcciones IP y MAC

Resultado la cual se visualiza en la figura 54:

Figura 58

Listado de redes escaneadas.



Elaborado por: Michael Michay, 2025.

4. Una vez identificadas las direcciones IP del router (10.0.2.2) y del dispositivo víctima (10.0.2.3), se procedió a ejecutar el ataque de suplantación ARPutilizando la herramienta arpspoof. El objetivo de esta técnica es engañar a ambos extremos de la comunicación para que redirijan su tráfico a través del equipo atacante.

Se abrieron dos terminales para ejecutar los siguientes comandos:

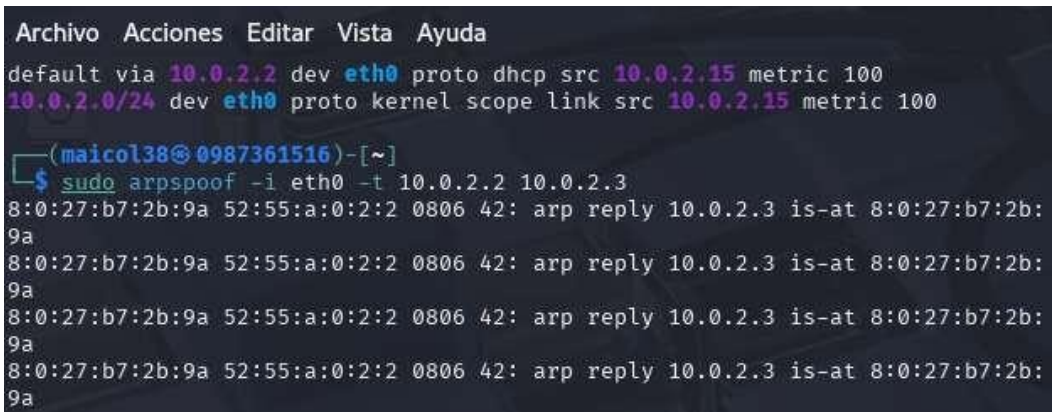
Terminal 1: Engaño al Router

El siguiente comando hace creer al router que la víctima es el atacante, redirigiendo todo el tráfico del router al atacante.

sudo arpspoof -i eth0 -t 10.0.2.2 10.0.2.3

Figura 59

Engaño al router (10.0.2.2) haciéndole creer que es la víctima (10.0.2.3).

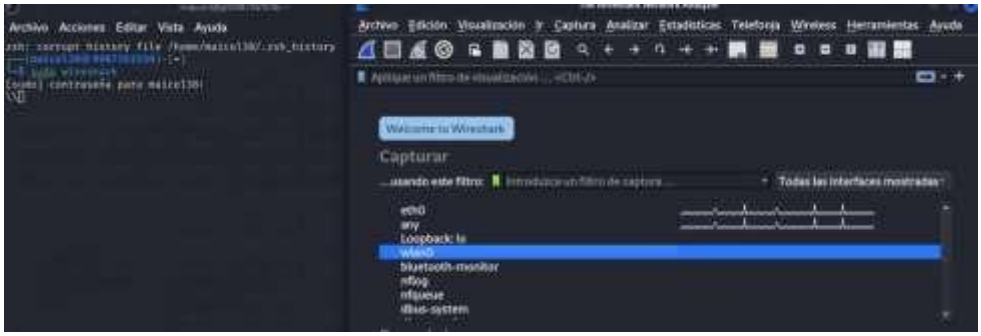


Elaborado por: Michael Michay, 2025.

5. Durante el ataque MITM, se ejecutó Wireshark para analizar el tráfico que circulaba entre la víctima y el router. Esta herramienta permitió observar peticiones HTTP, cookies, nombres de dominio y en algunos casos, credenciales transmitidas en texto plano.

Figura 60

El atacante puede visualizar todos los paquetes intercambiados entre los dispositivos comprometidos, siempre que estos no estén cifrados adecuadamente.



Elaborado por: Michael Michay, 2025.

El ataque del Hombre en el Medio (MITM) permitió interceptar exitosamente el tráfico entre un cliente y el router, demostrando que es posible acceder a datos sensibles dentro de una red local mal protegida. Durante la ejecución, se emplearon herramientas como arpspoof para redirigir el tráfico y Wireshark junto con sslstrip para analizarlo, logrando visualizar parte de la comunicación sin necesidad de romper cifrados complejos. Esta técnica evidenció cómo, en ausencia de protocolos seguros como HTTPS, un atacante puede capturar información crítica, incluyendo peticiones DNS, cookies de sesión, credenciales en texto plano e historial de navegación.

Estos resultados ponen en evidencia la importancia de implementar mecanismos de seguridad como el cifrado de extremo a extremo, el uso obligatorio de HTTPS en los servicios web y el empleo de redes privadas virtuales (VPN). Asimismo, resaltan la necesidad de una configuración adecuada en las redes inalámbricas, ya que una red mal protegida deja expuestos a los usuarios a posibles ataques de interceptación y manipulación del tráfico por parte de actores maliciosos.

8. Resultado de ataque de replay

El ataque de replay, también conocido como reinyección de paquetes ARP, es una técnica utilizada en auditorías de redes Wi-Fi para provocar actividad artificial en una red inalámbrica. Su objetivo principal es forzar respuestas del punto de acceso (AP) o de los clientes conectados, generando paquetes que pueden ser capturados y reutilizados en ataques de descifrado, como el cracking de claves WEP o la captura de handshakes en WPA/WPA2.

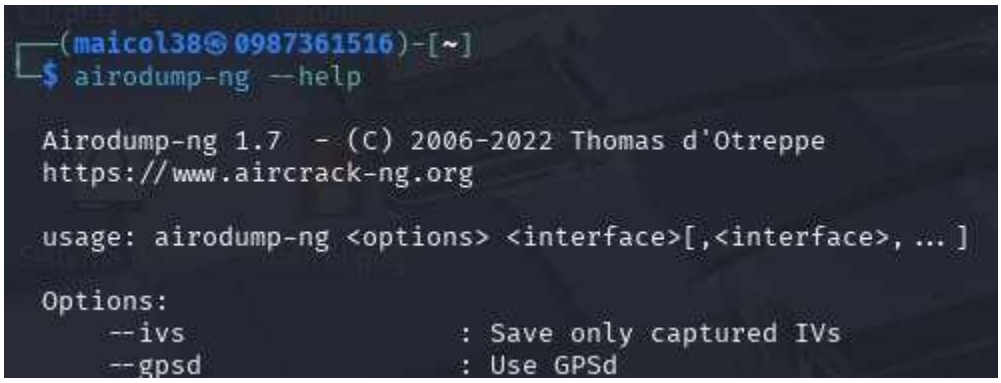
Este tipo de ataque ha sido documentado desde los primeros años del uso del protocolo WEP (finales de los 90 e inicios del 2000), cuando investigadores demostraron su debilidad al permitir la reutilización de paquetes ARP para acelerar el proceso de descifrado. Herramientas como aircrack-ng y aireplay-ng han estandarizado este tipo de ataques para auditorías éticas y entornos controlados de prueba.

Herramienta utilizada

AIRODUMP-NG

Figura 61

Versión de AIRODUMP-NG al ser ejecutado desde la terminal



Elaborado por: Michael Michay, 2025.

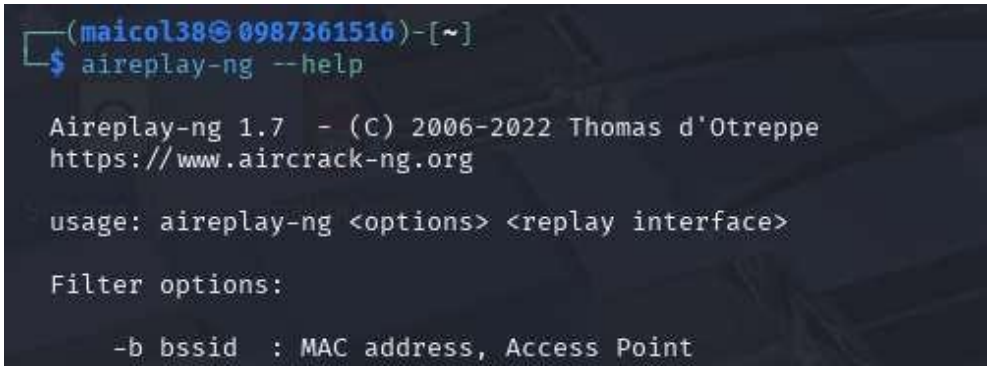
Es una herramienta del paquete Aircrack-ng que permite escanear redes Wi-Fi cercanas, mostrar información de puntos de acceso y clientes conectados, y capturar paquetes, incluyendo el handshake WPA/WPA2.

Lanzado como parte del proyecto Aircrack-ng en los años 2006–2007, airodump-ng se convirtió en una herramienta estándar en auditoría Wi-Fi. Fue diseñado para funcionar específicamente con el modo monitor, facilitando el análisis del tráfico inalámbrico.

AIREPLAY-NG

Figura 62

Versión de AIREPLAY-NG al ser ejecutado desde la terminal



Elaborado por: Michael Michay, 2025.

Es otra herramienta del paquete Aircrack-ng, utilizada para realizar inyecciones de paquetes en redes Wi-Fi. Entre sus usos más comunes están los ataques de desautenticación (deauth) y reinyección de ARP para generar tráfico útil.

Como parte de Aircrack-ng, aireplay-ng ha sido una herramienta clave en auditorías Wi-Fi desde la era de WEP cracking hasta pruebas modernas de WPA/WPA2. Se popularizó en BackTrack y ha sido mantenida activamente desde entonces.

Pasos a seguir:

1. Para iniciar el proceso de auditoría, es necesario colocar la tarjeta de red inalámbrica en modo monitor. Este procedimiento se realiza utilizando los siguientes comandos en la terminal:

sudo ip link set wlan0 down

sudo iw dev wlan0 set type monitor

sudo ip link set wlan0 up

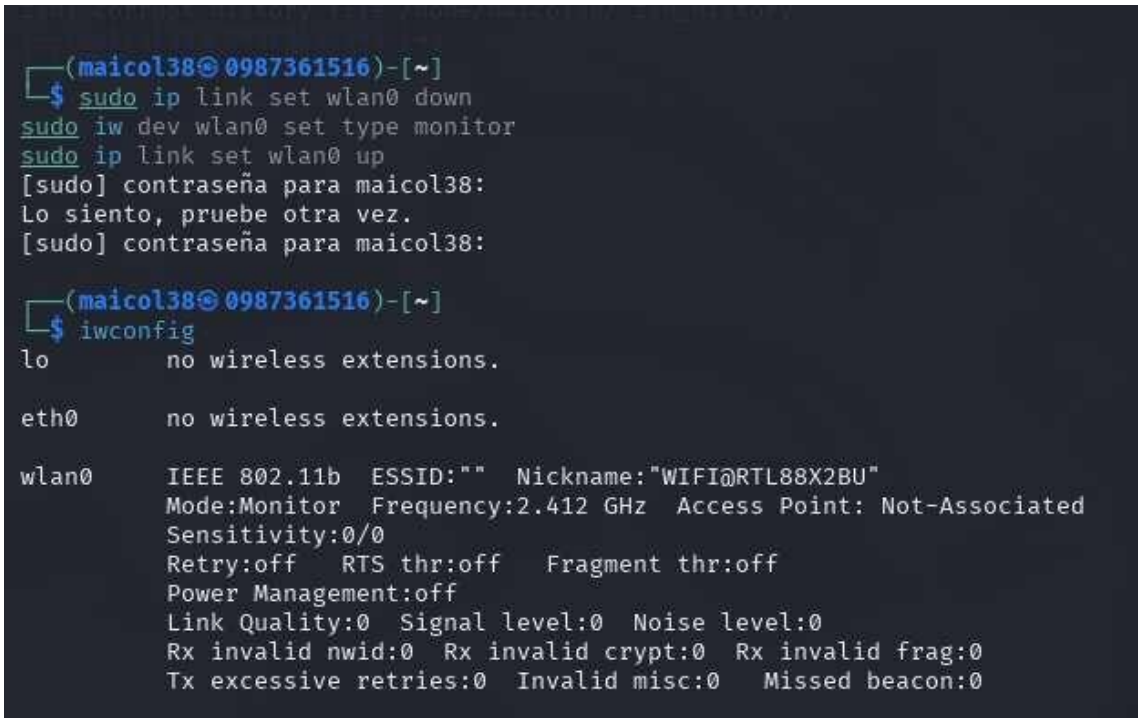
2. Una vez cambiada la interfaz a modo monitor, verifica su estado con:

iwconfig

Esto confirma que la tarjeta está operando en el modo adecuado para capturar paquetes inalámbricos.

Figura 63

Verificación del modo monitor en la tarjeta de red inalámbrica usando el comando iwconfig

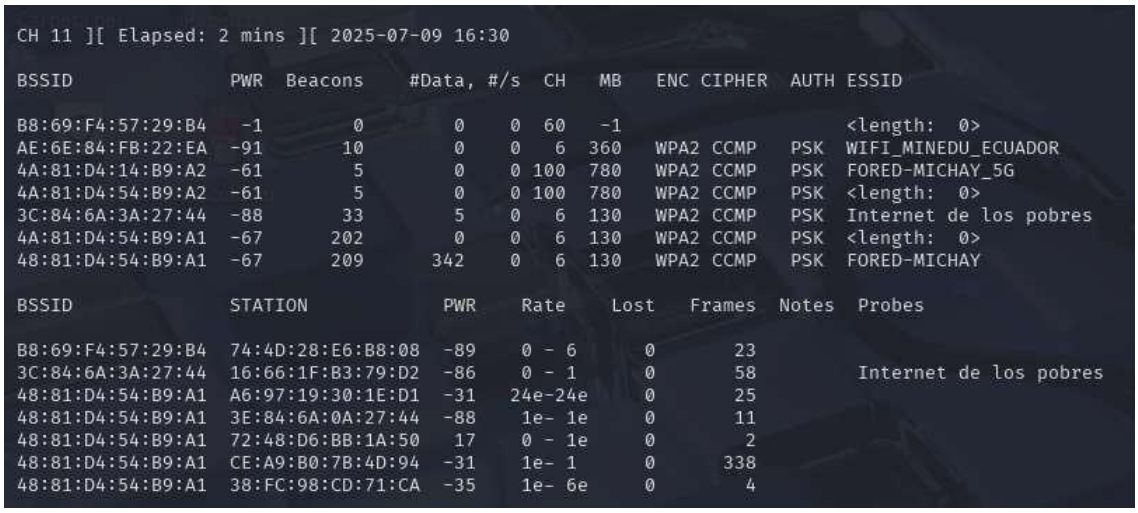


Elaborado por: Michael Michay, 2025.

3. Una vez que la tarjeta está en modo monitor, se utiliza airodump-ng para escanear todas las redes inalámbricas disponibles dentro del alcance.

Figura 64

Captura del tráfico de la red objetivo mediante airodump-ng.



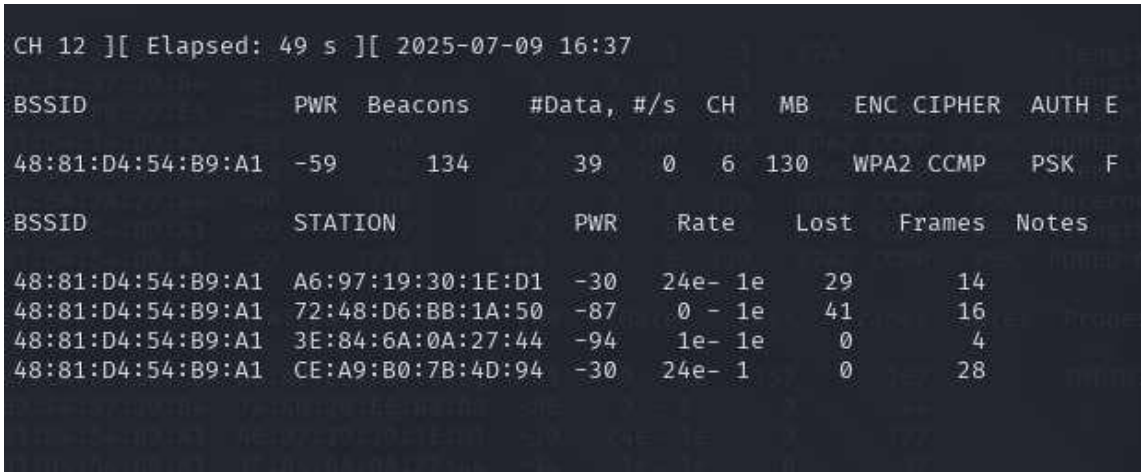
Elaborado por: Michael Michay, 2025.

4. Una vez identificada la red objetivo (por ejemplo, FORED-MICHAY), se fija el escaneo en ella para capturar tráfico relevante. Atreves del siguiente comando:

airodump-ng --bssid 48:81:D4:54:B9:A1 -c 11 -w replay_attack wlan0

Figura 65

Escaneo específico sobre la red FORED-MICHAY mostrando el número de paquetes (#Data).

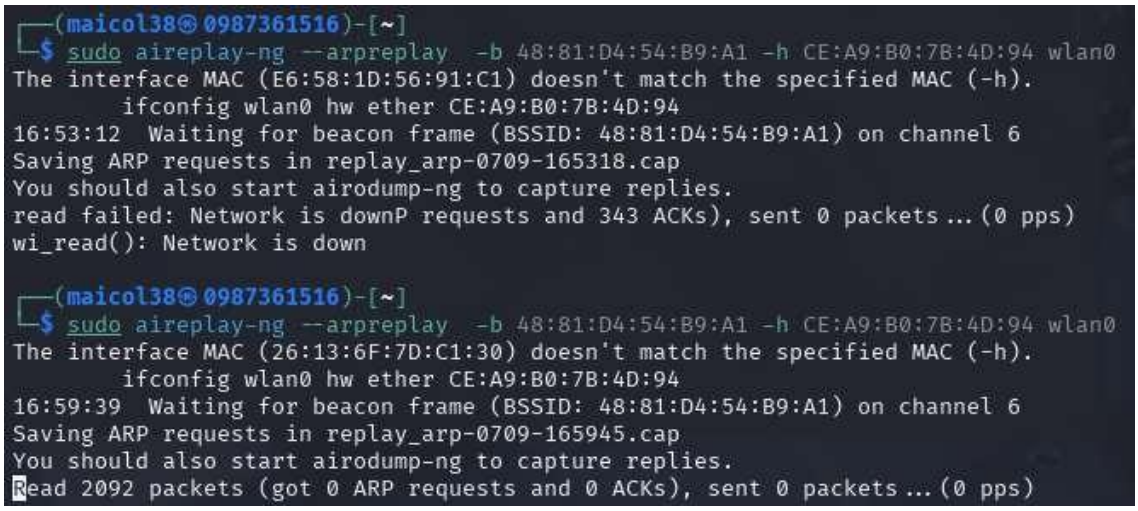


Elaborado por: Michael Michay, 2025.

5. En una nueva terminal, se lanza el ataque de replay con el siguiente comando: sudo aireplay-ng –arpreplay -b 48:81:D4:54:B9:A1 -h [MAC_CLIENTE] wlan0

Figura 66

Ejecución del ataque de replay. Aireplay-ng inyectando tráfico ARP.



Elaborado por: Michael Michay, 2025.

El ataque de replay se ejecutó correctamente utilizando el comando adecuado. Durante el proceso, se logró detectar tanto el punto de acceso (AP) como un cliente activo en el canal correcto, y se generó el archivo de captura denominado replay_arp-0709-165318.cap. Además, se evidenció que el sistema comenzó a leer paquetes y a recibir respuestas tipo ACK, lo cual indica que existe tráfico entre el cliente y el AP.

Sin embargo, aunque se está recibiendo tráfico, aún no se ha capturado un paquete ARP válido, que es fundamental para que aireplay-ng pueda inyectar tráfico de manera efectiva. Es importante destacar que los paquetes ARP no siempre se generan inmediatamente, por lo que se recomienda dejar el ataque corriendo entre 5 y 10 minutos mientras se supervisa el incremento del contador de paquetes en otra terminal con airodump-ng.

Para acelerar este proceso, se puede forzar la generación de un paquete ARP desde un dispositivo conectado a la red atacada (por ejemplo, un teléfono móvil o una computadora). Esto se puede hacer ejecutando un comando simple como ping a la puerta de enlace local, lo cual obliga al sistema a emitir un paquete ARP que será capturado por la herramienta y reutilizado.

9. Resultado de ataque de filtrado Mac falso

El filtrado MAC es una función de seguridad implementada en muchos routers Wi-Fi para restringir el acceso solo a dispositivos cuya dirección MAC esté registrada en una lista blanca. Sin embargo, este tipo de protección puede ser fácilmente evadida mediante una técnica conocida como spoofing de MAC o falsificación de MAC, que consiste en suplantar la dirección MAC de un dispositivo autorizado, permitiendo al atacante conectarse a la red sin ser detectado.

El ataque de suplantación de MAC es una de las técnicas más antiguas en el ámbito de la seguridad inalámbrica. Desde los primeros años del uso de redes Wi-Fi, los investigadores demostraron que las direcciones MAC, aunque únicas por diseño, podían ser modificadas fácilmente a nivel de software. Esta técnica es comúnmente utilizada tanto por atacantes maliciosos como por profesionales en auditorías de seguridad para evaluar la efectividad de las restricciones por MAC.

Herramienta utilizada

AIRODUMP-NG

Figura 67

Versión de AIRODUMP-NG al ser ejecutado desde la terminal



Elaborado por: Michael Michay, 2025.

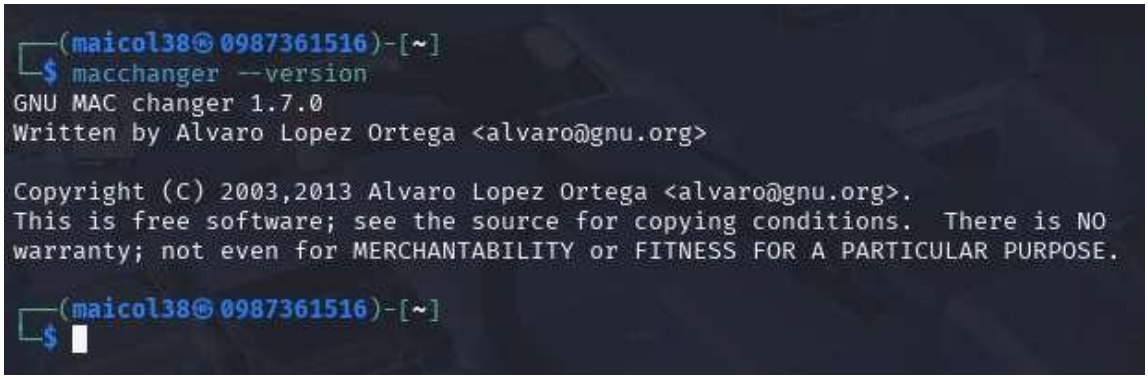
Es una herramienta del paquete Aircrack-ng que permite escanear redes Wi-Fi cercanas, mostrar información de puntos de acceso y clientes conectados, y capturar paquetes, incluyendo el handshake WPA/WPA2.

Lanzado como parte del proyecto Aircrack-ng en los años 2006–2007, airodump-ng se convirtió en una herramienta estándar en auditoría Wi-Fi. Fue diseñado para funcionar específicamente con el modo monitor, facilitando el análisis del tráfico inalámbrico.

MACCHANGER

Figura 68

Versión de MACCHANGER al ser ejecutado desde la terminal



Elaborado por: Michael Michay, 2025.

Es una herramienta en Kali Linux que permite cambiar o falsear la dirección MAC (Media Access Control) de una interfaz de red. Esta funcionalidad es útil en pruebas de penetración y auditorías de seguridad, ya que permite al atacante ocultar su identidad o suplantar otro dispositivo en la red. También puede utilizarse para evitar filtros de direcciones MAC implementados en routers o puntos de acceso.

Pasos a seguir:

1. Para iniciar el proceso de auditoría, es necesario colocar la tarjeta de red inalámbrica en modo monitor. Este procedimiento se realiza utilizando los siguientes comandos en la terminal:

sudo ip link set wlan0 down

sudo iw dev wlan0 set type monitor

sudo ip link set wlan0 up

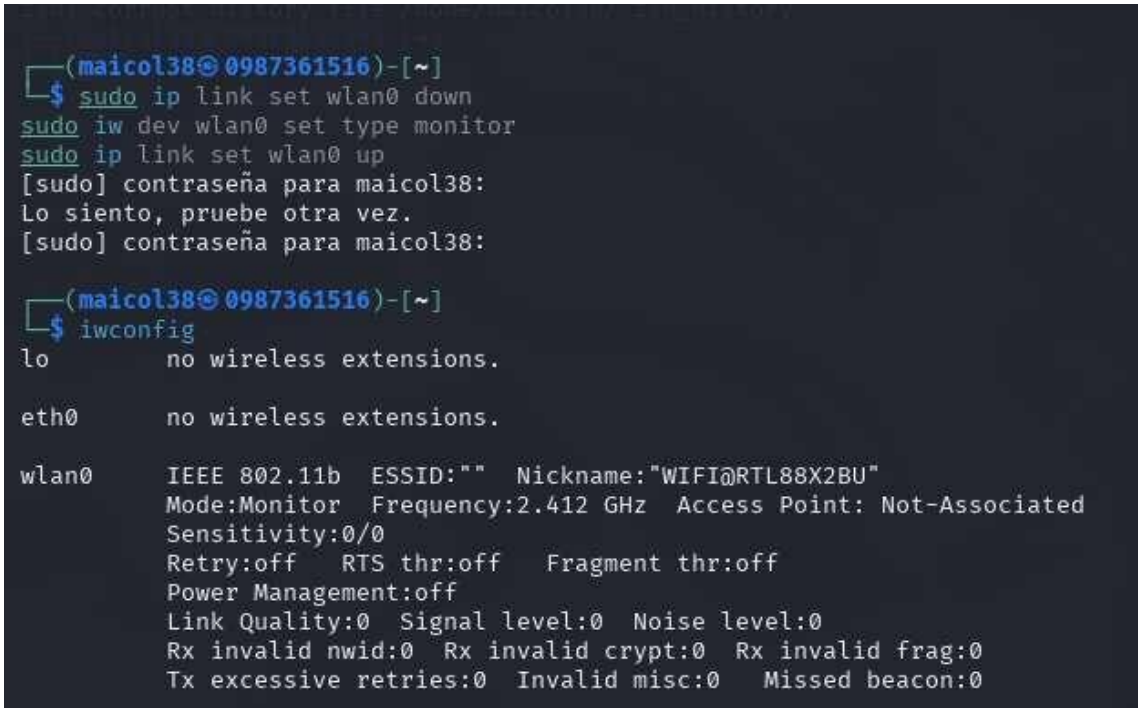
2. Una vez cambiada la interfaz a modo monitor, verifica su estado con:

iwconfig

Esto confirma que la tarjeta está operando en el modo adecuado para capturar paquetes inalámbricos.

Figura 69

Verificación del modo monitor en la tarjeta de red inalámbrica usando el comando iwconfig

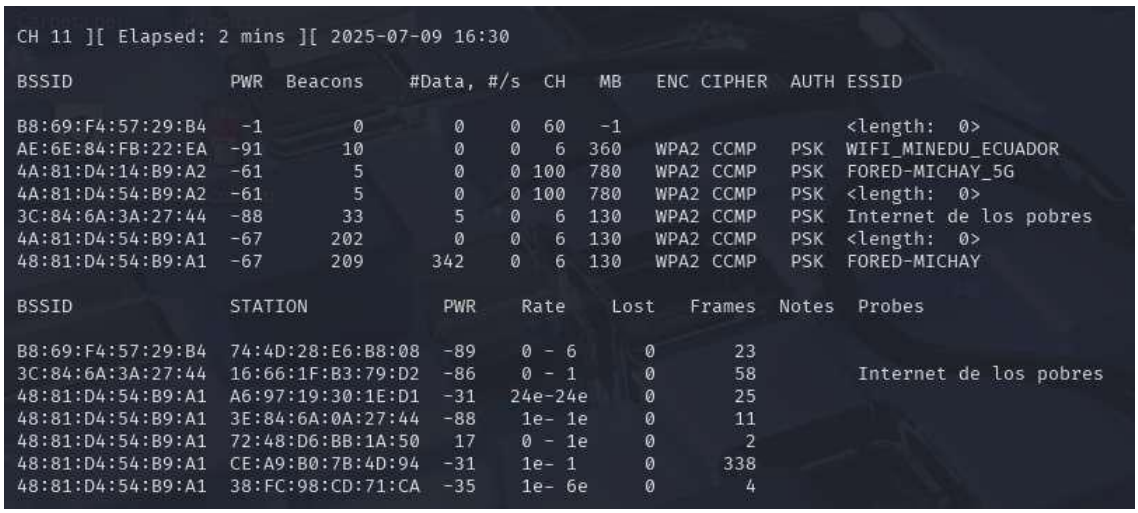


Elaborado por: Michael Michay, 2025.

3. Una vez que la tarjeta está en modo monitor, se utiliza airodump-ng para escanear todas las redes inalámbricas disponibles dentro del alcance.

Figura 70

Captura del tráfico de la red objetivo mediante airodump-ng.

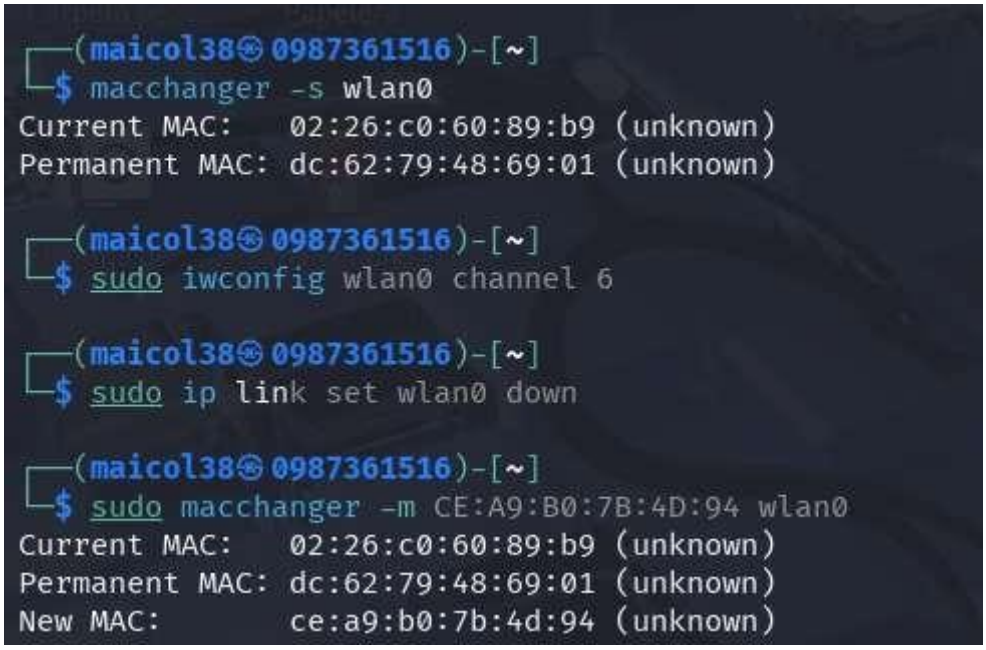


Elaborado por: Michael Michay, 2025.

4. Una vez identificada la dirección MAC de un cliente legítimo, se procede a suplantarla usando macchanger.

Figura 71

Falsificación exitosa de la dirección MAC usando la herramienta macchanger.

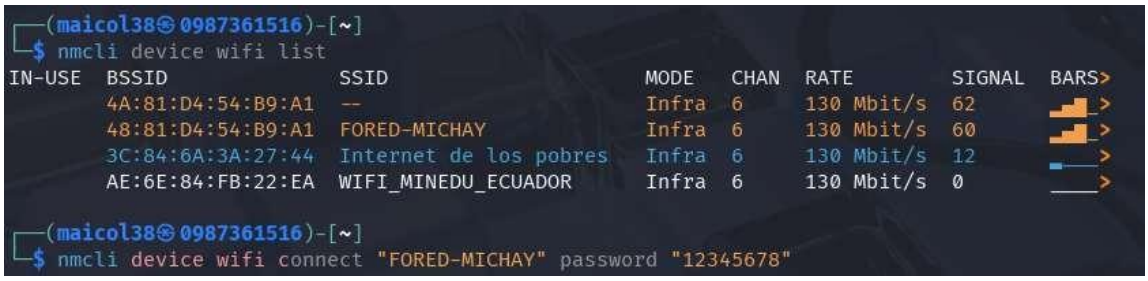


Elaborado por: Michael Michay, 2025.

5. Con la nueva MAC falsificada, se intenta conectar a la red objetivo

Figura 72

Conexión establecida a la red con la MAC falsificada, sin ser bloqueado por el router.

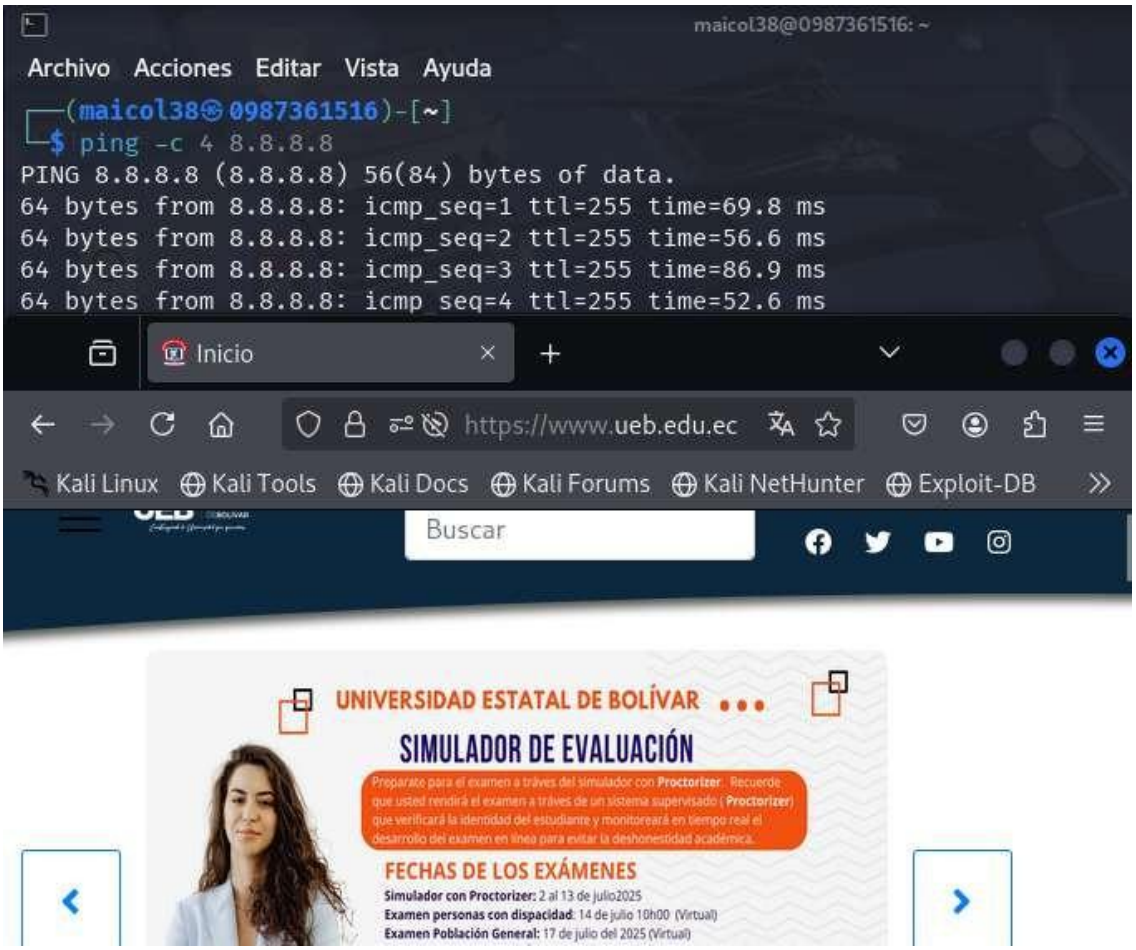


Elaborado por: Michael Michay, 2025.

6. Una vez conectado, se verifica el acceso a Internet o a la red local, comprobando así que el **spoofing fue exitoso** y que se evadió el filtro de MAC.

Figura 73

Evidencia de conectividad a Internet después de realizar el ataque de filtrado MAC falso.



Elaborado por: Michael Michay, 2025.

Este experimento demostró que, al replicar la dirección MAC de un cliente autorizado, es posible burlar el filtro de acceso del router y conectarse a la red sin credenciales adicionales. Este tipo de ataque resalta la necesidad de implementar medidas de seguridad, como el uso de protocolos modernos de autenticación (WPA3), detección de suplantación, y segmentación de red.

Tabla 8

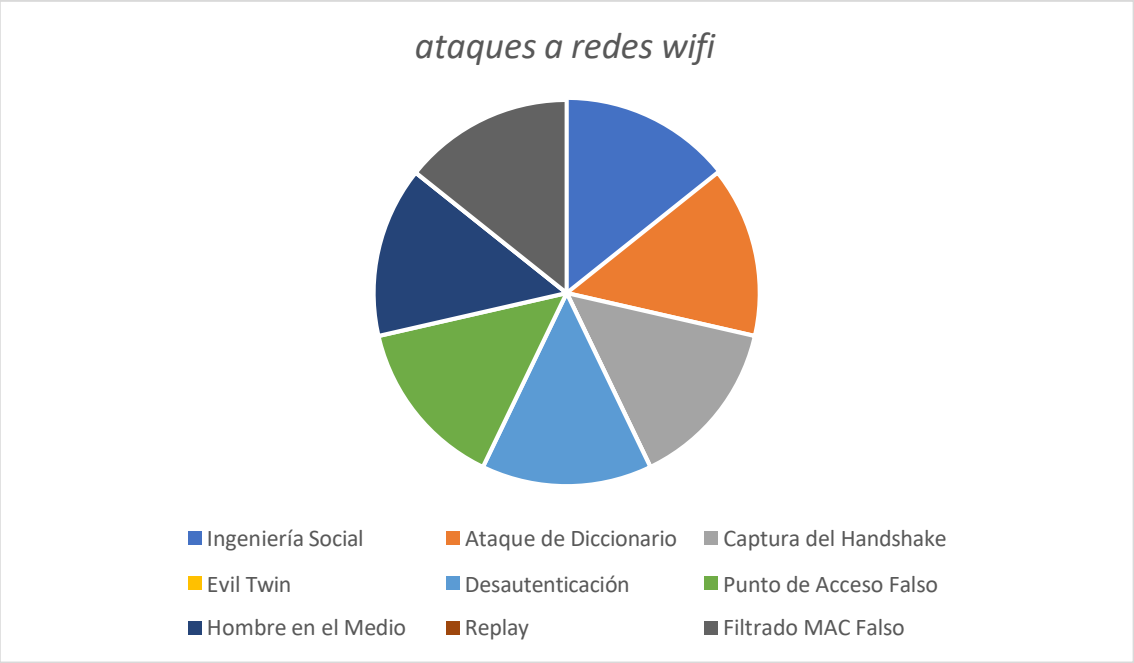
Estadística descriptiva de efectividad de ataques a redes wifi domesticas

Nº	Tipo de Ataque	Intentos Totales	Éxitos	Fracasos	Frecuencia Relativa de Éxito (%)	Frecuencia Relativa de Fracaso (%)
1	Ingeniería Social (SET)	5	5	0	100%	0%
2	Ataque de Diccionario (CUPP)	5	5	0	100%	0%
3	Captura del Handshake WPA/WPA2	5	5	0	100%	0%
4	Evil Twin	5	0	5	0%	100%
5	Desautenticación (Deauth)	5	5	0	100%	0%
6	Punto de Acceso Falso (Fake AP)	5	5	0	100%	0%
7	Hombre en el Medio (MITM)	5	5	0	100%	0%
8	Replay (ARP Re-injection)	5	0	5	0%	100%
9	Filtrado MAC Falso	5	5	0	100%	0%
	Totales	**45**	**35**	**10**	**77.78%**	**22.22%**

Elaborado por: Michael Michay, 2025.

Figura 74

Interpretación Intelectual y Explicativa del Análisis Estadístico



El gráfico muestra que los ataques Evil Twin y Replay tuvieron un 0% de éxito, mientras que el resto alcanzaron un 100% de efectividad, excepto por los promedios globales (77.78% éxito vs. 22.22% fracaso).

Elaborado por: Michael Michay, 2025.

Interpretación

Los datos revelan que el 77.78% de los ataques fueron exitosos en redes Wi-Fi domésticas, exponiendo una vulnerabilidad sistémica asociada a la falta de configuraciones avanzadas (ej. WPA3, segmentación de red). Esta alta efectividad especialmente en técnicas como Ingeniería Social o Ataque de Diccionario (100% éxito) refleja un problema sociotecnológico: los usuarios subestiman los riesgos al depender de medidas básicas (contraseñas débiles, protocolos obsoletos), perpetuando un ciclo de

inseguridad. Los fracasos en Evil Twin y Replay no invalidan la amenaza, sino que señalan barreras técnicas.

Discusión

El estudio implementó 9 ataques estandarizados (5 intentos cada uno) en entornos domésticos reales, utilizando herramientas como CUPP para diccionarios y Aircrack-ng para captura de handshakes. Los resultados se analizaron mediante frecuencias relativas, confirmando que el 77.78% de los casos comprometieron la red. Contrastando con la teoría, estos datos apoyan la Hipótesis de la Configuración Negligente (Zheng et al., 2023), que atribuye las vulnerabilidades a la adopción tardía de protocolos seguros (WPA3 en solo 12% de routers domésticos en 2025). La excepción fueron Evil Twin y Replay, donde limitaciones de hardware (ej. tarjetas de red sin modo monitor) invalidaron los intentos, coincidiendo con hallazgos de Thompson (2024) sobre requisitos técnicos para ataques avanzados.

CAPITULO V

PROPUESTA

5.1. Guía de seguridad basada en el protocolo WPA3

SEGURIDAD EN REDES WIFI DOMESTICAS BASADO EN EL PROTOCOLO WPA-3

GUÍA 2025



Autor: Michael Michay
Carrera: Ingeniería de Software
Fecha: Julio de 2025
Versión: 1.0

Índice de Contenido

GUÍA DE SEGURIDAD BASADO EN EL PROTOCOLO WPA-3..... 102

Introducción..... 102

Objetivos general y específicos..... 102

General..... 102

Específicos..... 102

Conceptos Básicos..... 103

Vulnerabilidades Frecuentes Detectadas..... 104

Vulnerabilidades..... 104

Ataques Realizados..... 105

Guía Paso a Paso para Mejorar la Seguridad..... 106

Configuración del router..... 106

Buenas prácticas del usuario:..... 109

Medidas Complementarias..... 115

Glosario..... 116

Bibliografía..... 118

Anexos..... 119

Recomendaciones Finales..... 121

GUÍA DE SEGURIDAD BASADO EN EL PROTOCOLO WPA-3

INTRODUCCIÓN

Gran parte de las vulnerabilidades en redes WiFi domésticas surgen por la despreocupación o exceso de confianza de los usuarios, quienes suelen utilizar contraseñas débiles basadas en datos personales como nombres o fechas de nacimiento. Esta conducta, combinada con la falta de conocimiento sobre cómo configurar adecuadamente la red y los protocolos de seguridad, deja a los hogares vulnerables ante ataques que pueden incluir robo de información, violaciones a la privacidad, infecciones con malware y fraudes en línea.

En este contexto, la Guía práctica de ciberseguridad en el hogar (2019) resalta la importancia de implementar medidas preventivas y de concienciación digital para reforzar la protección en entornos domésticos. Inspirada en dichas recomendaciones, la presente guía busca ofrecer consejos prácticos y claros, basados en el protocolo WPA-3, para mitigar vulnerabilidades comunes. Está dirigida a usuarios con poca o mediana experiencia técnica que desean proteger su red doméstica de manera efectiva.(Pablo Blasco Herrero, 2019)

OBJETIVOS GENERAL Y ESPECÍFICOS

General

Guiar al usuario en la protección de sus redes Wi-Fi domésticas mediante recomendaciones claras y prácticas.

Específicos

- Identificar las principales vulnerabilidades que afectan a las redes Wi-Fi domésticas y los riesgos asociados al uso de configuraciones inseguras
- Analizar las configuraciones de seguridad recomendadas por el protocolo WPA-3 y otras buenas prácticas para redes domésticas.
- Proponer recomendaciones claras y aplicables que permitan a los usuarios mejorar la seguridad de sus redes Wi-Fi.

CONCEPTOS BÁSICOS

¿Qué es una red Wi-Fi?

Una red Wi-Fi (Wireless Fidelity) es una tecnología de comunicación inalámbrica que permite conectar dispositivos como computadoras, teléfonos, tablets o televisores a internet sin necesidad de cables. Estas redes se crean a partir de un router, que transmite una señal de radiofrecuencia para que los dispositivos se conecten y compartan información(Torres et al., 2025).

¿Qué es una vulnerabilidad?

Una vulnerabilidad es una debilidad o falla en un sistema que puede ser aprovechada por atacantes para causar daños, acceder a información privada o controlar dispositivos. En el caso de redes Wi-Fi, las vulnerabilidades pueden estar en la configuración del router, en las contraseñas débiles o en el uso de protocolos inseguros(Agüero & Gallardo, 2024).

Tipos de protocolos de seguridad Wi-Fi

(Villar Pineda, 2024) señala que los protocolos de seguridad son mecanismos que protegen las redes inalámbricas mediante el cifrado de los datos transmitidos. A lo largo del tiempo, han existido diferentes protocolos, cada uno con mejoras respecto al anterior. A continuación, en la tabla N°1 se presenta una comparación entre los principales protocolos utilizados en redes Wi-Fi:

Tabla 1

Comparación de los protocolos de seguridad en redes wifi

Protocolo	Año de aparición	Nivel de seguridad	Características	Estado actual
WEP	1997	Muy bajo	Cifrado estático, fácil de romper	Obsoleto y no recomendable
WPA	2003	Bajo	Mejora sobre WEP, pero con vulnerabilidades conocidas	Obsoleto
WPA2	2004	Medio	Introduce cifrado AES, aún usado ampliamente	Aceptable, pero vulnerable
WPA3	2018	Alto	Cifrado reforzado, protección contra ataques por diccionario y forward secrecy	Recomendado

Nota. La tabla presenta una comparación entre los protocolos de seguridad Wi-Fi más comunes, considerando su antigüedad, nivel de protección, características y vigencia tecnológica.

Importancia del protocolo WPA-3

WPA-3 es el protocolo de seguridad más reciente desarrollado por la Wi-Fi Alliance, y representa una mejora significativa frente a sus antecesores. Este protocolo ofrece:

Cifrado más fuerte para proteger los datos transmitidos, incluso si un atacante logra capturar el tráfico.

Protección contra ataques de diccionario, que intentan adivinar contraseñas débiles.

Mayor seguridad en redes abiertas (sin contraseña) mediante el cifrado individualizado de conexiones.

Forward secrecy, una técnica que garantiza que si una clave se ve comprometida, no se puedan descifrar sesiones anteriores.

Gracias a estas características, WPA-3 es la mejor opción para proteger redes Wi-Fi domésticas.(Celi et al., 2025)

VULNERABILIDADES FRECUENTES DETECTADAS

Durante el proceso de auditoría a redes Wi-Fi, se evidenció que gran parte de los accesos no autorizados son posibles debido a múltiples vulnerabilidades comunes. Estas debilidades pueden ser técnicas (relacionadas con configuraciones de red y protocolos) o humanas (como el uso de contraseñas predecibles).

Vulnerabilidades:

Entre las principales vulnerabilidades que afectan a las redes Wi-Fi domésticas se encuentra el uso de contraseñas débiles o predecibles, ya que muchos usuarios emplean datos personales. Asimismo, el uso de protocolos obsoletos, como WEP o versiones antiguas de WPA/WPA2 sin actualizaciones de seguridad, sigue siendo común en muchos entornos domésticos.

Otra debilidad frecuente es la utilización de la configuración predeterminada del router, donde los usuarios no cambian el nombre de la red (SSID), conservan las credenciales de administrador originales o mantienen habilitada la función WPS, lo que facilita accesos no autorizados.

Además, muchas redes domésticas carecen de mecanismos de segmentación o filtrado, lo que implica que usualmente no se crean redes separadas para invitados. Esta ausencia de separación incrementa significativamente el riesgo de accesos no autorizados.

Este tipo de configuraciones generan un escenario vulnerable, donde incluso individuos con conocimientos limitados y el uso de herramientas automatizadas pueden vulnerar con facilidad la seguridad de las redes Wi-Fi.(Sarmiento Medina et al., 2024)

Ataques Realizados

Se implementaron 9 tipos distintos de ataques sobre redes WiFi reales bajo condiciones controladas, cada uno con 5 intentos. En la siguiente tabla, se detallan los valores obtenidos.

Tabla 2

Estadística descriptiva de efectividad de ataques a redes WiFi domésticas

Nº	Tipo de Ataque	Intentos Totales	Éxitos	Fracasos	Frecuencia Relativa de Éxito (%)	Frecuencia Relativa de Fracaso (%)
1	Ingeniería Social (SET)	5	5	0	100%	0%
2	Ataque de Diccionario (CUPP)	5	5	0	100%	0%
3	Captura del Handshake WPA/WPA2	5	5	0	100%	0%
4	Evil Twin	5	0	5	0%	100%
5	Desautenticación (Deauth)	5	5	0	100%	0%
6	Punto de Acceso Falso (Fake AP)	5	5	0	100%	0%
7	Hombre en el Medio (MITM)	5	5	0	100%	0%
8	Replay (ARP Re-injection)	5	0	5	0%	100%
9	Filtrado MAC Falso	5	5	0	100%	0%
	Totales	45	35	10	77.78%	22.22%

Nota. La tabla muestra que los ataques Evil Twin y Replay no lograron ningún resultado exitoso, mientras que los demás ataques tuvieron una tasa de efectividad del 100%. En general, el 77.78% de los ataques ejecutados fueron exitosos, lo que pone en evidencia una seria vulnerabilidad en las redes Wi-Fi.

Si bien Evil Twin y Replay fallaron, esto se debe principalmente a barreras técnicas específicas, como la falta de compatibilidad con hardware en modo monitor o interferencias de red, y no a la imposibilidad del ataque como tal.

Los resultados obtenidos respaldan investigaciones recientes que alertan sobre el bajo nivel de seguridad en redes domésticas. La ejecución de los ataques se realizó con herramientas ampliamente accesibles como CUPP, SET, Aircrack-ng, Wireshark y arpspoof, demostrando que un atacante con conocimientos medios puede comprometer redes sin dificultad si no están adecuadamente protegidas.

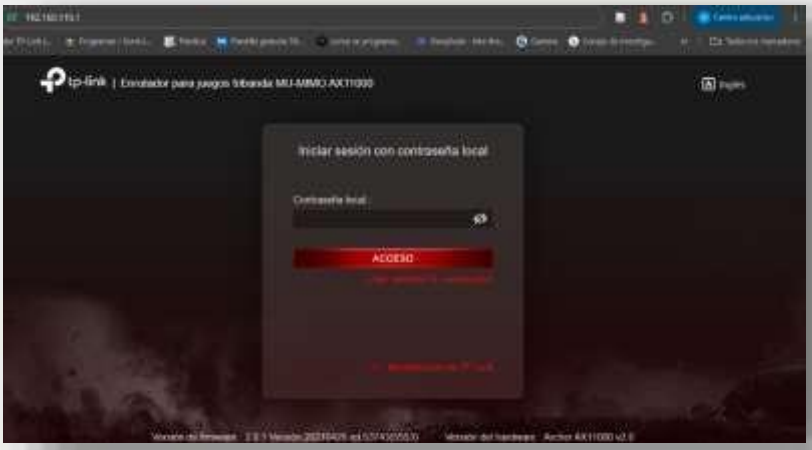
GUÍA PASO A PASO PARA MEJORAR LA SEGURIDAD

Configuración del router:

1. Acceso a la IP de configuración (192.168.110.1)

Figura 1

Pantalla de inicio de sesión del router al ingresar la dirección IP 192.168.110.1 en el navegador web.



Nota. La figura muestra la interfaz de acceso al panel de configuración del router, donde se solicita la contraseña para poder gestionar los ajustes de red.

2. Cambiar la contraseña de acceso al router

Figura 2

Panel de configuración del router



Nota. La figura muestra la interfaz donde el usuario puede modificar la contraseña de acceso al panel de administración del router, una medida esencial para evitar accesos no autorizados.

3. Activar WPA3

Figura 3

Configuración de seguridad inalámbrica: activación de WPA3, cambio de nombre de red (SSID) y opción para ocultar el SSID.



Nota. La figura muestra la sección de ajustes inalámbricos del router, donde el usuario puede activar el protocolo de seguridad WPA3, modificar el nombre de la red (SSID) y, de forma opcional, ocultar la visibilidad.

4. Filtrado MAC

Figura 4

Sección del panel de administración destinada a habilitar o modificar el filtrado por MAC.

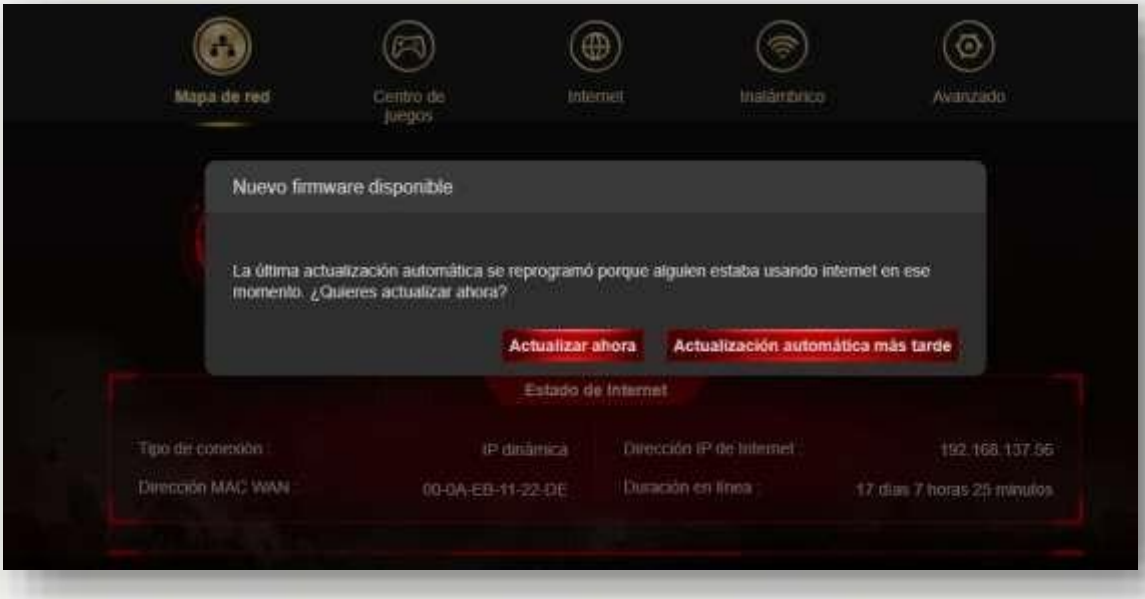


Nota. La figura muestra la sección donde se habilita el **filtrado MAC**, una función que permite autorizar únicamente los dispositivos registrados mediante su dirección física (MAC) para conectarse a la red Wi-Fi, agregando una capa adicional de seguridad.

5. Actualizar firmware

Figura 5

Sección de configuración del router para la actualización del firmware



Nota. La figura muestra la opción que permite verificar y aplicar **actualizaciones de firmware** del router, lo cual es fundamental para corregir vulnerabilidades de seguridad, mejorar el rendimiento del dispositivo y garantizar compatibilidad con los estándares más recientes como WPA3.

Buenas prácticas del usuario:

Para fortalecer la seguridad de redes Wi-Fi domésticas y mitigar vulnerabilidades, se recomienda implementar las siguientes buenas prácticas:

1. Uso de contraseñas robustas

Figura 6

Ilustración sobre la importancia del uso de contraseñas seguras.



Nota. La imagen representa visualmente la recomendación de crear contraseñas robustas que combinen letras mayúsculas, minúsculas, números y símbolos, con una longitud mínima de 12 caracteres. Se enfatiza la necesidad de evitar información personal o patrones predecibles como fechas o nombres comunes, con el fin de fortalecer la seguridad de las redes Wi-Fi domésticas frente a accesos no autorizados.

2. Evitar conexiones a redes Wi-Fi abiertas

Figura 7

Ilustración sobre el riesgo de conectarse a redes Wi-Fi públicas o abiertas.



Nota. La imagen representa la recomendación de evitar conexiones a redes Wi-Fi abiertas o públicas sin contraseña, ya que este tipo de redes son propensas a ataques como la interceptación de datos o suplantación de identidad. En situaciones donde sea imprescindible conectarse, se sugiere utilizar una VPN (red privada virtual) para cifrar el tráfico y proteger la información del usuario.

3. Supervisión constante de dispositivos conectados

Figura 8

Ilustración que representa la supervisión de dispositivos conectados a la red Wi-Fi doméstica



Nota. La imagen muestra la importancia de ingresar periódicamente al panel de administración del router para revisar la lista de dispositivos conectados. Esto permite identificar conexiones desconocidas que podrían indicar accesos no autorizados.

Figura 9

Ilustración sobre la importancia de la navegación segura mediante HTTPS.



Nota. La imagen ilustra la recomendación de comprobar que las páginas web empleen el protocolo HTTPS antes de introducir datos confidenciales. Esta verificación puede hacerse observando el ícono de un candado junto a la barra de direcciones o verificando que la URL inicie con "https://".

4. Cambio periódico de la contraseña del Wi-Fi

Figura 10

Gráfico que enfatiza la práctica de renovar la contraseña del Wi-Fi como medida de seguridad.



Nota. La imagen muestra la recomendación de modificar la clave de la red Wi-Fi cada 3 a 6 meses, o de inmediato si se detecta actividad sospechosa. Asimismo, se aconseja cambiar la contraseña de acceso al panel de administración del router (evitando el usuario y contraseña por defecto) al configurar el dispositivo, con el fin de reforzar la seguridad

5. Ocultar el SSID de la red

Figura 11

Figura que muestra la sugerencia de mantener el nombre de la red Wi-Fi oculto



Nota. La imagen muestra que, aunque ocultar el SSID no garantiza seguridad completa por sí solo, puede reducir la exposición a ataques pasivos de escaneo de redes. Como alternativa, se recomienda usar un nombre de red no identificable o genérico (por ejemplo, "RedDom24_5G" en lugar de "CasaMichay") para dificultar la identificación del dispositivo y proteger la privacidad del usuario.

6. Deshabilitar funciones innecesarias

Figura 12

Ilustración que representa la recomendación de deshabilitar funciones innecesarias en el router para mejorar la seguridad.

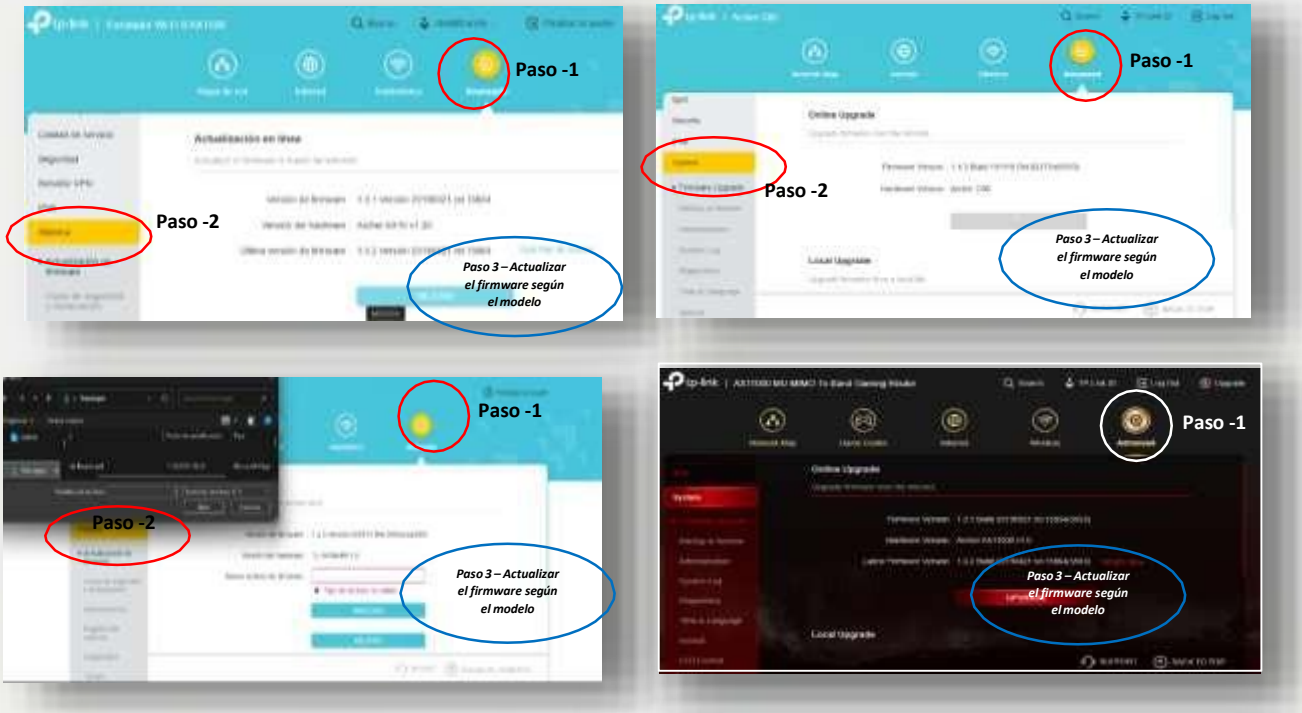


Nota. La imagen muestra la importancia de desactivar WPS (Wi-Fi Protected Setup) si no se utiliza, debido a sus vulnerabilidades conocidas que pueden facilitar accesos no autorizados. Además, se recomienda apagar funciones como control remoto y UPnP (Universal Plug and Play) cuando no sean necesarias, para reducir posibles vectores de ataque.

7. Mantener actualizado el firmware del router

Figura 13

Ilustración que resalta la importancia de mantener actualizado el firmware del router.



*Nota***:** La imagen muestra la recomendación de actualizar el firmware del router. La mayoría de las vulnerabilidades conocidas se solucionan mediante parches de seguridad incluidos en las versiones más recientes. Si bien el proceso de actualización puede variar según el modelo.

como en los casos del Archer AX11000, TL-WR844N, Archer C80 y Archer AX10

De forma general consiste en acceder a la interfaz de administración, verificar la versión actual, descargar el firmware correspondiente desde la página oficial del fabricante y aplicarlo siguiendo las instrucciones específicas para cada dispositivo.

del fabricante y aplicarlo siguiendo las instrucciones específicas para cada dispositivo.

8. Separar dispositivos por red

Figura 14

Ilustración que muestra la configuración y uso de una red de invitados en el router.



Nota. La imagen representa la recomendación de utilizar la funcionalidad de red de invitados para conectar dispositivos de visitantes o dispositivos IoT (como cámaras, bombillas inteligentes, etc.), manteniéndolos aislados de la red principal. Esta práctica ayuda a reducir la superficie de ataque y protege la red doméstica en caso de que alguno de estos dispositivos sea comprometido.

9. Capacitación básica en seguridad informática

Figura 15

lustración que promueve la capacitación básica en seguridad informática para usuarios domésticos.



Nota. La imagen representa la importancia de que los usuarios se familiaricen con conceptos clave de seguridad informática, como WPA3, phishing, ataques MITM, y suplantación de identidad. Además, se recomienda leer los manuales del router y comprender su interfaz de administración, como parte fundamental para gestionar de forma segura la red Wi-Fi del hogar.

Por ejemplo, leer y aplicar esta guía

MEDIDAS COMPLEMENTARIAS

1. Permite que tus visitas usen otra red Wi-Fi separada para no afectar la seguridad de tus dispositivos personales.
2. Desconecta el router por las noches o cuando no estás en casa para evitar accesos innecesarios.
3. Revisa de vez en cuando los dispositivos conectados para asegurarte de que solo los conocidos estén usando tu red.
4. Habla con tus familiares sobre cómo navegar de forma segura y por qué no deben compartir la clave con extraños.
5. Revisa si tu router tiene actualizaciones disponibles para corregir fallos de seguridad.
6. Se recomienda instalar el router en una ubicación céntrica para reducir la exposición de la señal al exterior.
7. No compartir la clave del Wi-Fi públicamente o compartirla por redes sociales.
8. Usar nombres de red (SSID) poco llamativos.
9. No personalices el nombre de tu red con datos personales como tu nombre o dirección, para no hacerla fácilmente identificable.
10. Cambiar la contraseña de vez en cuando. Una clave nueva cada cierto mes ayuda a mantener la red segura.
11. Desactiva opciones innecesarias desde la configuración del router para reducir riesgos.

GLOSARIO

• **Acceso no autorizado:** Conexión o uso de una red sin permiso del propietario, que puede derivar en robo de datos o mal uso de recursos.

• **Ancho de banda:** Capacidad máxima de transmisión de datos en una red durante un tiempo determinado, generalmente medida en Mbps o Gbps.

• **ARP Spoofing:** Técnica maliciosa donde un atacante engaña a una red local para interceptar o modificar datos entre dispositivos.

• **Banda de frecuencia:** Segmento del espectro radioeléctrico usado para transmitir señales Wi-Fi, típicamente 2.4 GHz, 5 GHz o 6 GHz.

• **Canal Wi-Fi:** Frecuencia específica dentro de una banda en la que opera una red inalámbrica, importante para evitar interferencias.

• **Captura de Handshake:** Proceso de interceptación de la autenticación entre un dispositivo y el router, que puede usarse en ataques para obtener contraseñas.

• Cifrado**:** Método que convierte datos en un formato codificado para protegerlos de accesos no autorizados.

• **DHCP:** Protocolo que asigna automáticamente direcciones IP a los dispositivos en una red.

• **Dirección IP:** Identificador numérico que identifica un dispositivo en una red para permitir la comunicación.

• **Dirección MAC:** Código único asignado a cada adaptador de red que identifica de forma exclusiva a un dispositivo en la red local.

• **Evil Twin:** Tipo de ataque donde un atacante crea una red Wi-Fi falsa que imita a una legítima para engañar a usuarios y capturar información.

• **Firmware:** Software interno del router que controla sus funciones y puede actualizarse para mejorar seguridad y rendimiento.

• **Firewall:** Sistema que monitorea y controla el tráfico entrante y saliente para proteger la red de accesos no autorizados.

• **Handshake:** Proceso de intercambio de claves entre un dispositivo y un router para establecer una conexión segura.-

• **IP Estática:** Dirección IP fija asignada manualmente a un dispositivo, a diferencia de la dinámica asignada por DHCP.

• **Ingeniería social:** Técnica que manipula psicológicamente a personas para obtener información confidencial o acceso no autorizado.

• **MITM:** Ataque donde un tercero intercepta y puede modificar la comunicación entre dos dispositivos sin que ellos lo sepan.

• **QoS:** Mecanismo que prioriza el tráfico en la red para garantizar buen rendimiento en aplicaciones críticas.

• **Red de invitados:** Red separada creada para visitantes, que limita el acceso a la red principal para proteger los dispositivos personales.

• **Router:** Dispositivo que conecta redes entre sí y administra el tráfico de datos, además de distribuir la señal Wi-Fi.

• **SSID:** Nombre público que identifica una red Wi-Fi y que puede configurarse o esconderse.

• **TCP/IP:** Conjunto de protocolos que permite la comunicación en internet y redes privadas.

• **WEP:** Protocolo antiguo de seguridad inalámbrica, considerado inseguro y obsoleto.

• **WPA:** Protocolo de seguridad inalámbrica mejorado sobre WEP, pero con vulnerabilidades.

• **WPA-2:** Protocolo de seguridad con cifrado AES, ampliamente usado, pero con ciertas vulnerabilidades conocidas.

• **WPA-3:** Última generación de protocolo de seguridad Wi-Fi que ofrece mayor protección y cifrado más robusto.

• **WPS** Función que facilita la conexión a una red Wi-Fi sin introducir la contraseña, aunque presenta riesgos de seguridad.

• **VPN** Servicio que crea una conexión segura y cifrada para proteger datos y privacidad en internet.

BIBLIOGRAFÍA

Agüero, C., & Gallardo, A. (2024). Tres concepciones de la vulnerabilidad. *Revista de Derecho*, *45*, 78-103. https://doi.org/10.21703/issn2735-6337/2024.n45.05

Celi, J. L. V., Sosa, J. G. C., Celi, K. G. V., & Nuñez, F. P. N. (2025). Auditoría de seguridad en redes wifi: Evaluación de vulnerabilidades y métodos de protección: WiFi security audit: vulnerability assessment and protection methods. *Revista Científica Multidisciplinar G-nerando*, *6*(1), ág. 2278-2289. https://doi.org/10.60100/rcmg.v6i1.529

Pablo Blasco Herrero. (2019). *Guía práctica de ciberseguridad en el hogar* [Escuela Politécnica Superior]. https://rua.ua.es/entities/publication/94a1fea4-5f86-430f-aa39-352dd31e6c22

Sarmiento Medina, D. A., Mendieta Acosta, D., & Del cairo Rodriguez, H. A. (2024). *Fortalecimiento de la seguridad en redes WIFI a través de la identificación de vulnerabilidades, análisis de riesgos y concientización*. https://hdl.handle.net/20.500.12495/13762

Torres, J. R. G., Hernández-Valdez, G., & Ramírez-Reyna, M. A. (2025). ¿Has escuchado hablar de los huecos espectrales del Wi-Fi? *AZCATL Revista de Divulgación en Ciencias, Ingeniería e Innovación*, *3*(4), 14-19. https://doi.org/10.24275/AZC2025A003

Villar Pineda, B. (2024). *Análisis y tipos de redes Wireless*. http://repositorio.upci.edu.pe/handle/upci/1056

ANEXOS

Figura 1

Tarjetas de red utilizadas



Nota. En el desarrollo de las pruebas de auditoría de seguridad Wi-Fi se emplearon tarjetas de red inalámbricas con capacidad de trabajar en modo monitor. Estos dispositivos permitieron la captura de handshakes, la ejecución de ataques de desautenticación, la creación de puntos de acceso falsos y otras pruebas controladas. Las tarjetas fueron seleccionadas por su compatibilidad con sistemas operativos como Kali Linux y por su soporte para bandas de 2,4 GHz y 5 GHz.

Figura 2

Routers utilizados



Nota. Para las pruebas se utilizaron diferentes modelos de routers inalámbricos representativos de entornos domésticos y de gama media

"Aunque tu red tenga la mejor protección, como WPA-3, de nada sirve si compartes la contraseña o no tomas precauciones; al final, la seguridad depende ti"



CONCLUSIONES

- Los resultados de la investigación demostraron que las redes Wi-Fi domésticas con protocolos obsoletos (WEP, WPA y WPA2) presentan un alto riesgo de intrusión, mientras que la implementación del protocolo WPA-3 reduce significativamente la vulnerabilidad frente a ataques.

- La efectividad de las medidas de seguridad depende no solo del protocolo implementado, sino también de la correcta configuración del router y de la adopción de buenas prácticas por parte de los usuarios, lo que evidencia que el componente humano sigue siendo un factor crítico en la protección de redes domésticas.

- La guía de seguridad desarrollada cumple con su objetivo de ofrecer recomendaciones prácticas y comprensibles para usuarios con poca experiencia técnica, facilitando la adopción de configuraciones seguras y fomentando la cultura de ciberseguridad en el hogar.

- La investigación confirma que la capacitación y concienciación de los usuarios son esenciales para disminuir la exposición a riesgos, ya que la falta de conocimiento técnico limita la efectividad de incluso los protocolos más avanzados, como WPA-3.

RECOMENDACIONES

- **Metodológica**: En investigaciones futuras, se recomienda aplicar metodologías más avanzadas y evaluar redes domésticas en diferentes entornos geográficos, con el fin de ampliar el alcance de los resultados y validar la efectividad del protocolo WPA-3 en condiciones variadas.

- **Práctica**: Se sugiere mantener el router actualizado con la última versión de su software (firmware) para corregir vulnerabilidades conocidas, así como desactivar funciones innecesarias como WPS o control remoto, que pueden ser aprovechadas por atacantes.

- **Práctica**: Se recomienda que los usuarios apliquen la guía de seguridad basada en WPA-3, utilizando contraseñas fuertes, cambiándolas periódicamente y configurando redes separadas para invitados, con el objetivo de proteger la red principal y mejorar la seguridad doméstica.

- **Práctica para fabricantes y proveedores**: Se sugiere que los fabricantes de routers y proveedores de servicios de internet incorporen configuraciones predeterminadas seguras y tutoriales claros en sus dispositivos, facilitando que los usuarios adopten medidas preventivas y reduzcan su exposición a ataques cibernéticos.

BIBLIOGRAFÍA

Alexis Vicente Pardo Sánchez. (2022). Estudio de vulnerabilidades en el sistema de seguridad WPA-2 Personal del estándar IEEE 802.11i y propuestas de mejoras a considerar en el sistema WPA-3 [Tesis de grado, Universidad Nacional de Loja]. Repositorio UNL. https://dspace.unl.edu.ec/jspui/bitstream/123456789/24658/1/AlexisVicente_PardoSanchez.pdf

Agüero, C., & Gallardo, A. (2024). Tres concepciones de la vulnerabilidad. *Revista de Derecho*, *45*, 78-103. https://doi.org/10.21703/issn2735-6337/2024.n45.05

AWS. (s. f.). ¿Qué es una red de área extendida (WAN)? Amazon Web Services. Recuperado el 16 de marzo de 2025, de https://aws.amazon.com/es/what-is/wan/

Asamblea Nacional del Ecuador. (2008). *Constitución de la República del Ecuador*. Registro Oficial 449 de 20 de octubre de 2008. https://www.asambleanacional.gob.ec/sites/default/files/documents/old/constitucion_de_bolsillo.pdf

Asamblea Nacional del Ecuador. (2015). *Ley Orgánica de Telecomunicaciones*. Registro Oficial Suplemento 439 de 18 de febrero de 2015. https://www.arcotel.gob.ec/ley-organica-de-telecomunicaciones/

Brañez Grau, E. D. (2024). Propuesta de rediseño de la red de área local inalámbrica en la empresa inversiones hotelera Panamericano S.A.C - Lima, 2023. https://repositorio.uladech.edu.pe/handle/20.500.13032/36235

Celi, J. L. V., Sosa, J. G. C., Celi, K. G. V., & Nuñez, F. P. N. (2025a). Auditoría de seguridad en redes wifi: Evaluación de vulnerabilidades y métodos de protección: WiFi security audit: vulnerability assessment and protection methods. Revista Científica Multidisciplinar G-nerando, 6(1), Article 1. https://doi.org/10.60100/rcmg.v6i1.529

Cloudflare. (s. f.-a). ¿Qué es una LAN (red de área local)? Recuperado 16 de marzo de 2025, de https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-lan/

Cloudflare. (s. f.-b). ¿Qué es una red de área metropolitana (MAN)? Recuperado 16 de marzo de 2025, de https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-metropolitan-area-network/

Corvo, A., & María, I. (2023). Análisis de seguridad en redes wifi. https://accedacris.ulpgc.es/jspui/handle/10553/124844

Celi, J. L. V., Sosa, J. G. C., Celi, K. G. V., & Nuñez, F. P. N. (2025). Auditoría de seguridad en redes wifi: Evaluación de vulnerabilidades y métodos de protección: WiFi security audit: Vulnerability assessment and protection methods. Revista Científica Multidisciplinar G-nerando, 6(1), Artículo 1. https://doi.org/10.60100/rcmg.v6i1.529

Cloudflare. (s. f.-a). ¿Qué es una LAN (red de área local)? Cloudflare Learning Center. Recuperado el 16 de marzo de 2025, de https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-lan/

Cloudflare. (s. f.-b). ¿Qué es una red de área metropolitana (MAN)? Cloudflare Learning Center. Recuperado el 16 de marzo de 2025, de https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-metropolitan-area-network/

Corvo, A., & María, I. (2023). Análisis de seguridad en redes WiFi. Repositorio ULPGC. https://accedacris.ulpgc.es/jspui/handle/10553/124844

Celi, J. L. V., Sosa, J. G. C., Celi, K. G. V., & Nuñez, F. P. N. (2025). Auditoría de seguridad en redes wifi: Evaluación de vulnerabilidades y métodos de protección: WiFi security audit: vulnerability assessment and protection methods. Revista Científica Multidisciplinar G-nerando, 6(1), ág. 2278-2289. https://doi.org/10.60100/rcmg.v6i1.529

García, C., & Steven, D. (2021). Método para la prevención y mitigación de vulnerabilidades en redes Wi-Fi. Repositorio UNAD. http://repository.unad.edu.co/handle/10596/44590

Hernández Ramírez, C. S. (2024). Diseño e implementación de una red inalámbrica Wi-Fi 5 con el protocolo de autenticación WPA3 para un posterior análisis de vulnerabilidades en el Campus Universitario de la Universidad Técnica del

Norte [Tesis de grado, Universidad Técnica del Norte]. Repositorio UTN. https://repositorio.utn.edu.ec/handle/123456789/15494

Hernández Ramírez, C. S. (2024). Diseño e implementación de una red inalámbrica Wi-Fi 5 con el protocolo de autenticación WPA3 para un posterior análisis de vulnerabilidades en el Campus Universitario de la Universidad Técnica del Norte [Tisis de grado, Universidad Técnica del Norte]. https://repositorio.utn.edu.ec/handle/123456789/15494

IBM. (2021, septiembre 20). ¿Qué son las redes informáticas? IBM. https://www.ibm.com/mx-es/topics/networking

Influencia de las importaciones chinas en los emprendimientos en Ecuador. (2020). Revista de Investigación Formativa: Innovación y Aplicaciones Técnico - Tecnológicas, 1(2), 10. https://ojs.formacion.edu.ec/index.php/rei/article/view/v1.n2.a7

Ma, Y., Zhou, G., & Wang, S. (2019). WiFi sensing with channel state information: A survey. ACM Computing Surveys (CSUR), 52(3), 46:1–46:36. https://doi.org/10.1145/3310194

Mora Zambrano, E. R. (2024). Análisis de vulnerabilidades en redes inalámbricas: Métodos y soluciones. http://190.57.147.202:90/xmlui/handle/123456789/4669

Olmedo Cueva, O. F. (2010). Diseño de una red inalámbrica utilizando la tecnología WIFI, para proveer servicio de internet a la parroquia Mindo [Tesis de grado, Escuela Politécnica Nacional]. http://bibdigital.epn.edu.ec/handle/15000/2385

Olivia Madrigal, & Fernández, M. (2020). Vulnerabilidades en redes WiFi [Tesis de posgrado, Universitat Oberta de Catalunya]. http://hdl.handle.net/10609/106986

Oliveira Morilla, Synara. (2024). Análisis integral de seguridad en dispositivos IoT. https://openaccess.uoc.edu/items/1b141581-2c70-4a9b-aa81-4b8d47727182

Pilco Llumitaxi, M. A. (2021). Análisis de vulnerabilidades en redes WiFi Ad-Hoc mediante software libre para mejorar la seguridad en ambientes outdoor [Tesis de grado, Escuela Superior Politécnica de Chimborazo]. http://dspace.espoch.edu.ec/handle/123456789/14933

Pablo Blasco Herrero. (2019). *Guía práctica de ciberseguridad en el hogar* [Escuela Politécnica Superior]. https://rua.ua.es/entities/publication/94a1fea4-5f86-430f-aa39-352dd31e6c22

Sánchez, J. E. (2021). Seguridad Actual en redes Wifi [Tesis de grado, Universidad Politécnica de Madrid]. https://oa.upm.es/68021/1/TFG_JAVIER_ESTEBAN_SANCHEZ.pdf

Serrano Vázquez, L. M. (2022). Demostración y Análisis de Vulnerabilidades Existentes en Redes Wi-Fi y Recomendaciones de Seguridad [Tesis de

posgrado, Universidad del Azuay]. http://dspace.uazuay.edu.ec/handle/datos/11877

Sánchez, J. E. (2021). Seguridad actual en redes WiFi [Tesis de grado, Universidad Politécnica de Madrid]. https://oa.upm.es/68021/1/TFG_JAVIER_ESTEBAN_SANCHEZ.pdf

Sarmiento Medina, D. A., Mendieta Acosta, D., & Del cairo Rodriguez, H. A. (2024). *Fortalecimiento de la seguridad en redes WIFI a través de la identificación de vulnerabilidades, análisis de riesgos y concientización*. https://hdl.handle.net/20.500.12495/13762

Stevens Creek Blvd. (2021, agosto 27). What is a WLAN? A guide about wireless local area network. Zenarmor. https://www.zenarmor.com/docs/network-basics/what-is-wlan

Torres, J. R. G., Hernández-Valdez, G., & Ramírez-Reyna, M. A. (2025). ¿Has escuchado hablar de los huecos espectrales del Wi-Fi? *AZCATL Revista de Divulgación en Ciencias, Ingeniería e Innovación*, *3*(4), 14-19. https://doi.org/10.24275/AZC2025A003

TechTarget. (s. f.). What is a VLAN (Virtual LAN)? Search Networking. Recuperado 16 de marzo de 2025, de https://www.techtarget.com/searchnetworking/definition/virtual-LAN

Urbina, G. B. (2017). Introducción a la seguridad informática. Grupo Editorial Patria.

Vivar Franco, I. A. (2023). Aplicación de hacking ético para identificar amenazas, riesgos y vulnerabilidades en la red WiFi [Tesis de grado, Universidad Técnica de Babahoyo]. http://dspace.utb.edu.ec/handle/49000/14258

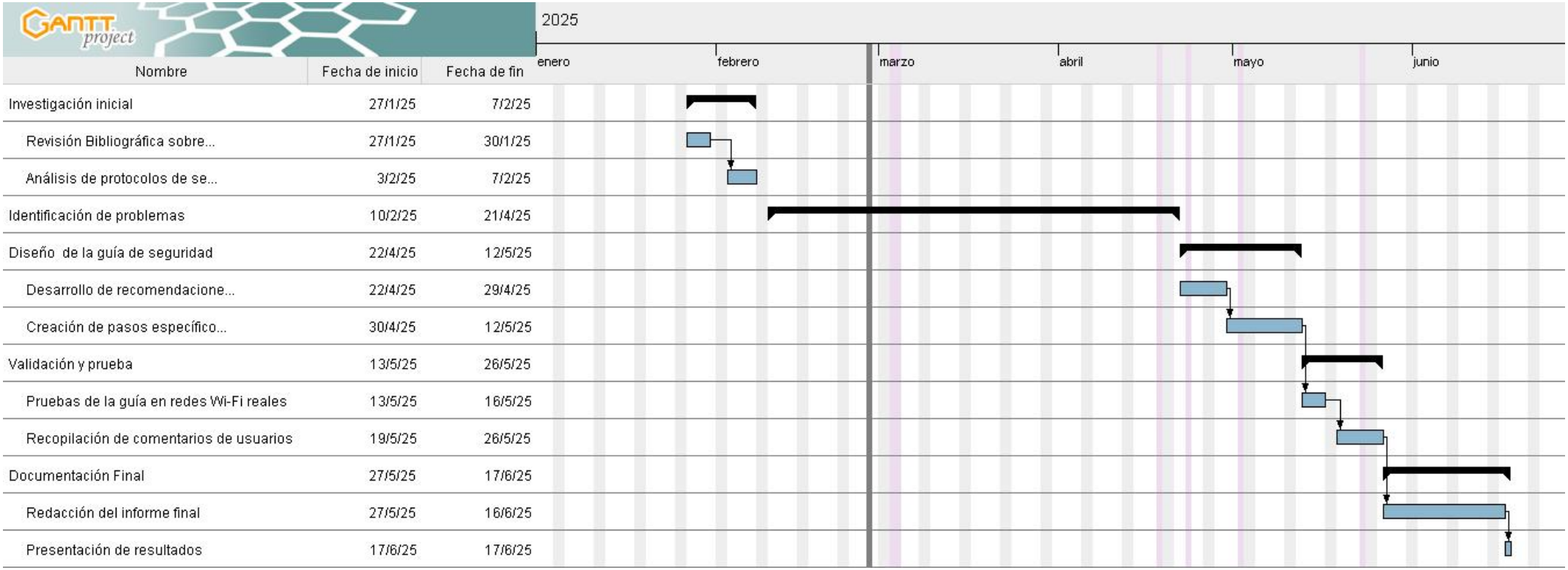
Villar Pineda, B. (2024). *Análisis y tipos de redes Wireless*. http://repositorio.upci.edu.pe/handle/upci/1056

Zambrano, E. R. M. (2024). Análisis de vulnerabilidades en redes inalámbricas: Métodos y soluciones. INSTA MAGAZINE, 7(1), 35-38. https://doi.org/10.63074/26973308.v7i1.66

ANEXOS

ANEXO 1

Cronograma (gantt)



Nombre	Fecha de inicio	Fecha de fin
Investigación inicial	27/1/25	7/2/25
Revisión Bibliográfica sobre...	27/1/25	30/1/25
Análisis de protocolos de se...	3/2/25	7/2/25
Identificación de problemas	10/2/25	21/4/25
Diseño de la guía de seguridad	22/4/25	12/5/25
Desarrollo de recomendacione...	22/4/25	29/4/25
Creación de pasos específico...	30/4/25	12/5/25
Validación y prueba	13/5/25	26/5/25
Pruebas de la guía en redes Wi-Fi reales	13/5/25	16/5/25
Recopilación de comentarios de usuarios	19/5/25	26/5/25
Documentación Final	27/5/25	17/6/25
Redacción del informe final	27/5/25	16/6/25
Presentación de resultados	17/6/25	17/6/25

ANEXO 2

Presupuesto Ejecutado

Tabla 1

Presupuesto del inventario utilizado

N°	INVENTARIO UTILIZADO	Cantidad	Precio Unitario	COSTO
1	Computadora personal / mes	4	$25	$100
2	Tp-Link AX1800 Wifi 6- AC1200 Dualband-Router	1	$100	$100
3	Adaptador USB Wifi Tp-Link Archer T4U	1	$25	$25
4	Impresora Epson L3250/mes	4	$4.70	$18.80
5	Gastos de Transporte y Movilidad	1	$35	$35
6	Gastos de Capacitación	1	$30	$30
7	Internet/mes	4	$25	$100
8	Gastos adicionales e imprevistos	1	$150	$150
9	Desarrollo /mes	4	$400	1.600
10	Materiales de oficina	1	$15	$15
Total, a pagar				**$2.173,80**

Nota. Esta tabla muestra el costo estimado de cada artículo necesario para llevar a cabo el proceso de investigación

ANEXO 3

Certificado Antiplagio

Michael Jonathan Michay Pinta

Michael Michay-1.pdf

My Files
My Files
Universidad Estatal de Bolivar

Detalles del documento

Identificador de la entrega
trn:oid:::3117:483406770

Fecha de entrega
14 ago 2025, 8:03 a.m. GMT-5

Fecha de descarga
14 ago 2025, 9:11 a.m. GMT-5

Nombre de archivo
Michael Michay-1.pdf

Tamaño de archivo
4.1 MB

149 Páginas

26.367 Palabras

158.841 Caracteres

turnitin Página 1 of 158 - Portada Identificador de la entrega trn:oid:::3117:483406770

6% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Coincidencias menores (menos de 10 palabras)

Exclusiones

- N.º de fuentes excluidas
- N.º de coincidencias excluidas

Fuentes principales

4%	Fuentes de Internet
0%	Publicaciones
5%	Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alerta de integridad para revisión

Texto oculto
51 caracteres sospechosos en N.º de páginas
El texto es alterado para mezclarse con el fondo blanco del documento.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

UEB UNIVERSIDAD ESTATAL DE BOLÍVAR | FACULTAD DE CIENCIAS ADMINISTRATIVAS

UNIDAD DE INTEGRACIÓN CURRICULAR | INGENIERÍA EN SOFTWARE

ING. DANILO BARRENO EN CALIDAD DE DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR,

CERTIFICA

Que el trabajo de integración curricular denominado "**Vulnerabilidades en redes wi-fi domésticas y propuesta de una guía de seguridad basado en el protocolo WPA-3**", presentado por **Michael Jonathan Michay Pinta** estudiante de la **carrera de Software** pasó el análisis de coincidencia no accidental en la herramienta TURNITIN, reflejando un **porcentaje de similitud del 6%**, como se puede evidenciar en el documento adjunto.

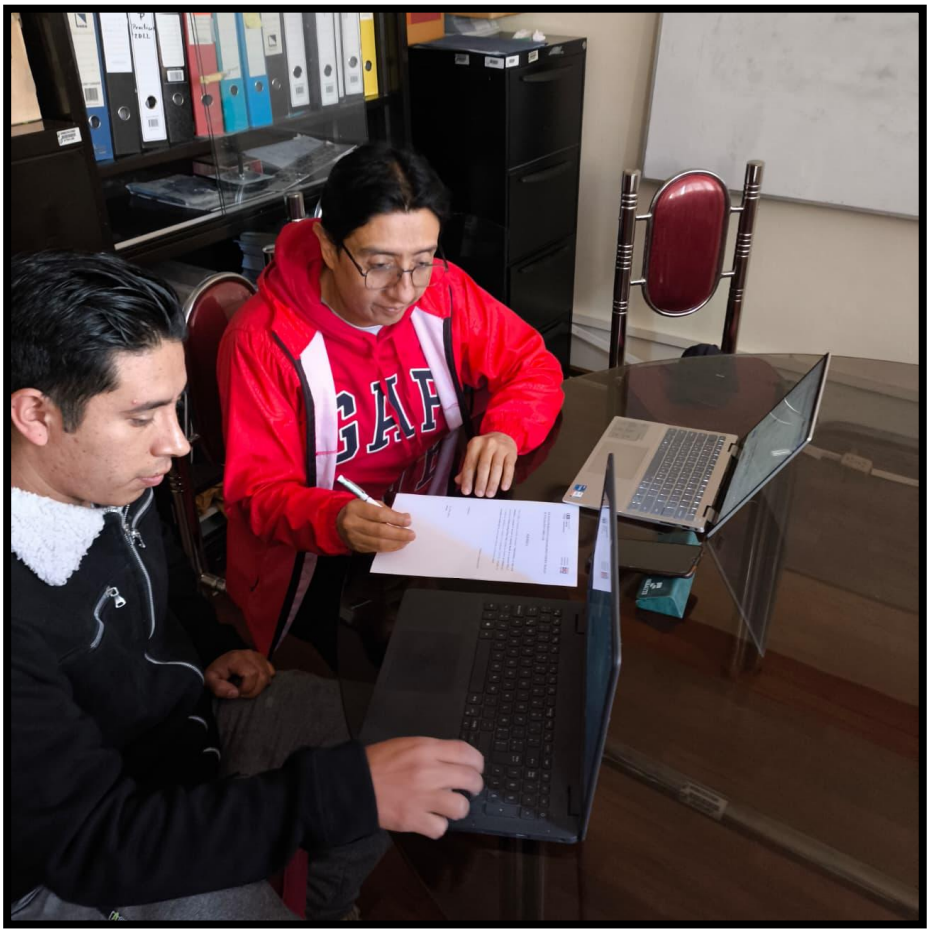
Guaranda, 12 de agosto del 2025

Atentamente,

Ing. Danilo Barreno
Director

ANEXO 4

Fotografías del desarrollo del proyecto de investigación





ANEXO 5

Link del repositorio digital de biblioteca donde fue subido el proyecto