UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

Desarrollo de un Analizador de Tráfico Inalámbrico para Detección de Ataques MITM

AUTOR

Nowak Moran Joseph Xavier

Proyecto de Integración Curricular

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

TUTOR

Ing. Coronel Suárez Iván Mgt

Santa Elena, Ecuador

Año 2023

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino, Mgt.
DIRECTOR DE LA CARRERA

Ing. Iván Coronel Suárez, Mgt.
TUTOR

Lsi. Daniel Quirumbay Yagual, MSIA.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez. Mgt.
DOCENTE GUÍA UIC

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por JOSEPH XAVIER NOWAK MORAN, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 4 días del mes de Diciembre del año 2024

TUTOR

Firmado electrónicamente por:
IVAN ALBERTO
CORONEL SUAREZ

Ing. Coronel Suárez Iván Mgt

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **JOSEPH XAVIER NOWAK MORAN**

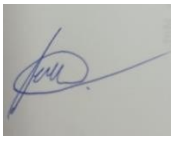
DECLARO QUE:

El trabajo de Titulación, Desarrollo de un Analizador de Tráfico Inalámbrico para Detección de Ataques MITM previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 4 días del mes de Diciembre del año 2024

EL AUTOR



Joseph Xavier Nowak Moran

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Desarrollo de un Analizador de Tráfico Inalámbrico para Detección de Ataques MITM, presentado por el estudiante, JOSEPH XAVIER NOWAK MORAN fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 5%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

CERTIFICADO DE ANÁLISIS
magister

Tesis FINAL FINAL

5%
Textos sospechosos

5% Similitudes
< 1% similitudes entre comillas
< 1% entre las fuentes mencionadas
0% Idiomas no reconocidos
46% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: Tesis FINAL FINAL.docx
ID del documento: 35c5bb53c68257a674decd0ca2121de4718f5ad4
Tamaño del documento original: 1,55 MB
Autores: []

Depositante: IVAN ALBERTO CORONEL SUAREZ
Fecha de depósito: 4/12/2024
Tipo de carga: interface
fecha de fin de análisis: 4/12/2024

Número de palabras: 11.141
Número de caracteres: 78.390

TUTOR

Firmado electrónicamente por:
IVAN ALBERTO CORONEL SUAREZ

Ing. Coronel Suárez Iván Mgt

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

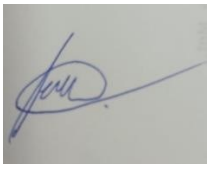
Yo, **JOSEPH XAVIER NOWAK MORAN**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 04 días del mes de DICIEMBRE del año 2024

EL AUTOR



Nombre y Apellidos

AGRADECIMIENTO

En primer lugar, quiero expresar mi más sincero agradecimiento a mi tutor, el Ingeniero Iván Coronel, por su constante apoyo, guía y paciencia durante todo el proceso de desarrollo de esta tesis. Su experiencia y dedicación han sido fundamentales para el logro de este trabajo.

Agradezco también a todos los ingenieros que me han acompañado en este camino, brindándome su conocimiento y colaboración en cada etapa del proyecto. Su trabajo en equipo y compromiso han sido imprescindibles para el éxito de este proyecto.

A mi familia, les doy las gracias por su amor incondicional, comprensión y apoyo en todo momento. Sin su aliento y confianza, este logro no habría sido posible. Su presencia ha sido mi mayor fortaleza.

A mis amigos, quienes siempre estuvieron a mi lado, brindándome su apoyo y motivación en los momentos más desafiantes. Gracias por su paciencia, por ser mi refugio y por acompañarme en cada paso.

Finalmente, a todos aquellos que de alguna manera contribuyeron a este proyecto, su apoyo y ánimo no han pasado desapercibidos. A cada uno, mi más profundo agradecimiento.

Joseph Xavier, Nowak Moran

DEDICATORIA

A mi familia, por su amor incondicional, su apoyo constante y su fe en mí, que me han dado la fuerza para seguir adelante en cada paso de este camino.

A mis amigos, por su compañía, sus risas y su aliento, que hicieron que los momentos difíciles fueran más llevaderos y los buenos aún más especiales.

Y a B, por los aprendizajes compartidos, que siempre llevaré conmigo, y por los momentos que formaron parte de este viaje.

Gracias a todos por ser parte de este logro.

Joseph Xavier, Nowak Moran

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El proyecto **"Desarrollo de un Analizador de Tráfico Inalámbrico para Detección de Ataques MITM"** tiene como objetivo crear una herramienta que identifique de manera temprana ataques Man-in-the-Middle (MITM) en redes inalámbricas, fortaleciendo la seguridad de las comunicaciones. Utiliza algoritmos avanzados de detección basados en aprendizaje automático para analizar patrones de tráfico en tiempo real, detectando anomalías asociadas a dichos ataques. El desarrollo sigue una metodología iterativa e incremental, incluyendo fases de captura de tráfico, diseño de algoritmos, generación de alertas y validación en entornos simulados y reales. Los resultados esperados incluyen una alta tasa de detección, precisión en la clasificación de tráfico y reducción de falsos positivos. La conclusión destaca la efectividad del sistema para prevenir accesos no autorizados, protegiendo la integridad de datos críticos y ofreciendo una solución adaptable para diversos entornos inalámbricos.

Palabras clave: Seguridad inalámbrica, MITM, aprendizaje automático.

ABSTRACT

The "Development of a Wireless Traffic Analyzer for MITM Attack Detection" project aims to create a tool that identifies Man-in-the-Middle (MITM) attacks in wireless networks early on, strengthening communications security. It uses advanced detection algorithms based on machine learning to analyze traffic patterns in real time, detecting anomalies associated with such attacks. The development follows an iterative and incremental methodology, including phases of traffic capture, algorithm design, alert generation, and validation in simulated and real environments. The expected results include a high detection rate, accuracy in traffic classification, and reduction of false positives. The conclusion highlights the effectiveness of the system in preventing unauthorized access, protecting the integrity of critical data, and offering an adaptable solution for various wireless environments.

Keywords: Wireless security, MITM, machine learning.

INTRODUCCIÓN

En la era digital actual, las redes inalámbricas han revolucionado la forma en que las personas y las organizaciones acceden, comparten y procesan información. Su versatilidad y facilidad de uso las han convertido en un elemento esencial en diversos entornos, desde hogares hasta empresas e instituciones gubernamentales. Sin embargo, esta misma accesibilidad las hace vulnerables a amenazas cibernéticas que comprometen la seguridad de los datos transmitidos. Entre las amenazas más peligrosas se encuentran los ataques **Man-in-the-Middle (MITM)**, donde un atacante intercepta y, en algunos casos, altera la comunicación entre dos partes sin que estas lo detecten.

Los ataques MITM no solo exponen datos sensibles, como credenciales de acceso o información financiera, sino que también ponen en riesgo la integridad de las operaciones en sistemas críticos. La detección efectiva de estos ataques se ha vuelto un desafío debido a su sofisticación y la creciente complejidad del tráfico en redes modernas. Aunque existen herramientas de seguridad, muchas no están diseñadas específicamente para redes inalámbricas o generan altos índices de falsos positivos, lo que limita su efectividad.

En este contexto, el presente proyecto propone el desarrollo de un **analizador de tráfico inalámbrico avanzado** que detecte ataques MITM de manera temprana y precisa. La herramienta empleará algoritmos de **aprendizaje automático (Machine Learning)**, capaces de analizar patrones de tráfico en tiempo real para identificar actividades sospechosas. Este enfoque permitirá una detección más eficiente, reduciendo el impacto de estos ataques en entornos donde la seguridad de las comunicaciones es crítica, como empresas, instituciones educativas y organizaciones gubernamentales.

El proyecto sigue una metodología estructurada e incremental, que incluye fases de captura de tráfico, análisis de datos, diseño de algoritmos de detección y generación de alertas. Además, se realizarán pruebas en entornos simulados y reales para validar su efectividad y garantizar su adaptabilidad a diversas configuraciones. Con esta propuesta, se busca no solo fortalecer la seguridad en redes inalámbricas, sino también contribuir al desarrollo de herramientas tecnológicas avanzadas que respondan a las crecientes amenazas de ciberseguridad.

CAPÍTULO 1. FUNDAMENTACIÓN

1.1 Antecedentes

En la era digital actual, la proliferación de redes inalámbricas ha facilitado la conectividad global, pero también ha introducido graves vulnerabilidades. Entre estas vulnerabilidades, los ataques de intermediario (MITM) son una de las amenazas más persistentes y peligrosas para la seguridad de las comunicaciones inalámbricas. En un escenario MITM, un atacante intercepta y potencialmente interrumpe la comunicación entre dos partes sin que ninguna de ellas sea consciente de la presencia del intruso. [1]

A lo largo de los años, se han desarrollado una variedad de métodos y técnicas para mitigar este tipo de ataques, incluido el uso de cifrado sólido, autenticación de extremo a extremo y detección proactiva de anomalías en el tráfico de la red. Sin embargo, debido al continuo desarrollo de técnicas de ataque y la creciente complejidad de la infraestructura de red, la detección eficaz de ataques MITM sigue siendo un desafío importante para los profesionales de la ciberseguridad. [2]

El proyecto se basa en la urgente necesidad de fortalecer las defensas de la red contra amenazas cada vez más sofisticadas, protegiendo así la integridad y confidencialidad de los datos transmitidos a través de redes inalámbricas. En el pasado se utilizaron como estrategias para mitigar estos ataques el cifrado fuerte y autenticación de extremo a extremo, pero los atacantes han evolucionado sus métodos para eludir estas defensas tradicionales. El uso de Machine Learning (ML) ha surgido como una poderosa herramienta pata detectar patrones anómalos en el tráfico de red y predecir posibles ataques con las técnicas de aprendizaje automático para analizar grandes volúmenes de datos en tiempo real y reconocer patrones complejos de comportamiento en la red [3].

Los algoritmos como Random Forests, support vector Machines y redes neuronales han demostrado ser efectivos para identificar patrones sospechosos en el tráfico de red que pueden estar relacionados con un ataque. Estos modelos pueden entrenarse con grandes conjuntos de datos de trafico de red para reconocer señales de

actividad maliciosa, como retrasos inusuales en la transmisión o comportamientos de intercepción que no corresponden a patrones normales. [3]

Una fuente relevante para este proyecto es la publicación NIST SP 800-153 de 2012, la cual además de proporcionar guías específicas para la configuración segura de redes inalámbricas (WLAN) también ofrece recomendaciones para mitigar riesgos asociados a la seguridad de redes. El fin de esta guía es reforzar las prácticas para el monitoreo y configuración de seguridad de los dispositivos inalámbricos que se conectan a la red. Una de sus principales recomendaciones es la implementación de configuraciones estándar de seguridad y evaluar las posibles vulnerabilidades dentro de la red WI-FI, la cual es esencial para la prevención de ataques como los MITM [4]

En los últimos años se ha podido evidenciar un incremento considerable en la frecuencia y sofisticación de los ataques MITM. Según el artículo “People Security Management” realizado por Threatcop, entre los años 2022 y 2023 los ataque MITM crecieron un 35% especialmente aquellos dirigidos a plataformas de correo electrónico y otros servicios en línea. [5]

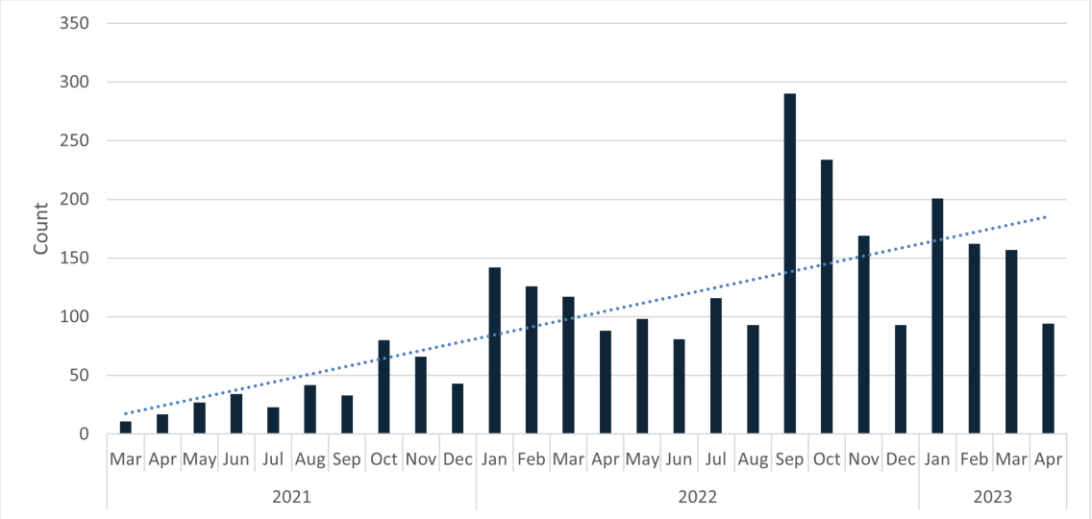


Figura 1 Aumento de ataques MITM años 2018 - 2023 [5]

Las redes inalámbricas son particularmente vulnerables ataques ya que su naturaleza abierta y facilidad con la que un atacante intercepte la comunicación la vuelven un blanco propicio para cualquier ciber-delincuente. Según un estudio realizado por veracode, el 76% de las organizaciones han experimentado algún tipo de ataque MITM en los últimos años [6]. Este incremento en ataques MITM evidencia la necesidad urgente necesidad de herramientas eficaces para su detección.

Las consecuencias de este tipo de ataques suelen ser devastadoras para la entidad que la sufre, como el robo de información confidencial, la alteración de datos y el acceso no autorizado a sistemas críticos. Según la Comisión Federal de Comercio, los ataques MITM han causados pérdidas financieras significativas y más importante, daños a la reputación de las organizaciones afectadas [7]. La capacidad de detectar estos tipos de ataques de manera temprana es crucial para mitigar sus efectos y proteger la integridad de las comunicaciones.

En la actualidad existen una cantidad diversa de herramientas de seguridad, pero muchas de ellas no están diseñadas para para detectar ataques MITM en redes inalámbricas o no son lo suficiente efectivas. Un análisis comparativo análisis comparativo de diversas herramientas de detección de amenazas revela que muchas soluciones no abordan de manera óptima el tráfico de redes inalámbricas o tiene una enorme taza de falsos positivos. Desarrollar un analizador que aproveche estos avances tecnológicos representa una mejora significativa respecto a las soluciones existentes.

Dado este contexto, donde se ha evidenciado que el desarrollo de un analizador de tráfico inalámbrico eficaz debe abordar las vulnerabilidades mencionadas y contribuir a mejorar las practicas actuales de seguridad en las redes WI-FI, tomando en cuenta fuentes normativas como el NIST y demás organismos especializados en ciberseguridad.

1.2. Descripción del Proyecto

El presente proyecto se centra en el desarrollo de un analizador de tráfico inalámbrico diseñado para la detección temprana y precisa de ataques de tipo Man-in-the-middle. Este tipo de ataques representa una de las más graves amenazas en el ámbito de las redes inalámbricas, ya que un atacante puede interceptar y modificar la comunicación entre dispositivos sin que los afectados sean conscientes de la intervención. [8]

El objetivo principal de este proyecto es la creación de una herramienta robusta que ayude a fortalecer la seguridad dentro de las comunicaciones inalámbricas, mitigando el impacto dañino de los ataques MITM y protegiendo la confidencialidad e integridad de los datos transmitidos.

El analizador propuesto empleara algoritmos avanzados de detección que serán capaces de identificar patrones sospechosos en el tráfico de red que indiquen la presencia de un ataque de esta índole. Técnicas como el análisis de paquetes y detección de anomalías serán utilizadas para ofrecer una solución efectiva a este problema. Además, se evaluará el desempeño del analizador en entornos de redes simuladas para garantizar su efectividad y eficiencia. [9]

Se espera realizar la creación de una solución funcional para estos tipos de ataques, el analizador debe ser capaza de detectar ataques MITM de forma eficaz y a su vez ayude a fortalecer la seguridad en redes inalámbricas, especialmente en entornos donde las comunicaciones son altamente sensibles, como instituciones gubernamentales, empresas, etc.

Fase	**Incremento 1: Captura de tráfico**	**Incremento 2: Algoritmos de detección**	**Incremento 3: Generación de alertas**	**Incremento 4: Optimización y validación**
Análisis	Revisión de tecnologías de captura de tráfico (Wireshark, tcpdump, etc.).	Estudio de algoritmos de detección (Machine Learning, reglas basadas en tráfico).	Análisis de eventos que activarán alertas por ataques MITM.	Revisión de los resultados obtenidos en incrementos anteriores.
Diseño	Definir estructura del módulo de captura de paquetes.	Diseño de algoritmos de detección optimizados para entornos inalámbricos.	Especificación del módulo de alertas y su integración con la detección.	Diseño de mejoras para la optimización del sistema y su validación.
Desarrollo	Implementación del módulo de captura de tráfico.	Desarrollo de algoritmos de detección de MITM (basado en anomalías y patrones).	Desarrollo del sistema de generación de alertas en tiempo real.	Implementación de mejoras para optimización del rendimiento.
Implementación	Despliegue del módulo en entorno controlado de red.	Integración de algoritmos en el sistema para la detección de patrones MITM.	Implementación de alertas automáticas en el sistema (por ejemplo, SNMP, email).	Despliegue de todo el sistema en un entorno de red real.
Pruebas	Validación del módulo de captura en redes simuladas.	Pruebas de detección en redes simuladas con ataques MITM.	Pruebas del sistema de alertas en escenarios simulados con tráfico anómalo.	Pruebas finales de optimización y evaluación de rendimiento en entornos reales.

Tabla 1: Metodología incremental

1.3. Objetivos del Proyecto

1.3.1 Objetivo general

Desarrollar un analizador de tráfico inalámbrico capaz de detectar ataques de tipo Man-in-the-Middle (MITM) para fortalecer la seguridad de las comunicaciones inalámbricas, utilizando el lenguaje de programación Python y sus bibliotecas.

1.3.2 Objetivos específicos

1. Implementar algoritmos de detección avanzados para identificar patrones de ataques MITM con precisión.

2. Evaluar la efectividad del analizador en entornos de redes inalámbricas reales para que se compruebe su precisión y rendimiento en la detección de ataques MITM bajo condiciones operativas reales.

3. Mejorar la capacidad de respuesta del analizador mediante la implementación de ajustes técnicos específicos y la adopción de prácticas de gestión orientadas a la detección temprana y la mitigación eficaz de amenazas.

1.4. Justificación

La preocupación por la seguridad en redes inalámbricas cada vez es mayor, esto se debe al incremento en la frecuencia y en lo sofisticados que son los ataques cibernéticos. Entre estos ataques el MITM destaca por su capacidad para interceptar y manipular las comunicaciones entes dos partes sin que estas caigan en cuenta que están siendo víctimas de este ataque. La implementación de un analizador de tráfico inalámbrico para la detección de ataques MITM representa un avance crucial para mejorar la seguridad en redes inalámbricas, donde los ataques que explotan vulnerabilidades en las redes inalámbricas son cada vez más sofisticados y su frecuencia es alarmante. De acuerdo con estadísticas recientes,

los ataques MITM han representado un 35% de las explotaciones de vulnerabilidades en las redes, una tendencia que va en aumento día tras día. [10]

Uno de los principales beneficios del desarrollo de un analizador de tráfico especializado es la mejora en la seguridad dentro de las comunicaciones inalámbricas, las cuales hoy en día son ampliamente utilizadas en industrias como la banca, el comercio electrónico y las redes empresariales y universitarias. En específico lo ataques MITM suelen aprovecharse de las redes públicas con poca o nula seguridad, como conexiones WI-FI abiertas. La detección en tiempo real de patrones anómalos en el tráfico de red puede reducir significativamente la exposición involuntaria a estas amenazas Según Threatpost, los ciberdelincuentes emplean diversas técnicas en ataques MITM, como la suplantación de direcciones IP, DNS y "SSL Stripping" [10]

Además de mejorar la detección de ataques, el analizador también será capaz de reducir el tiempo de respuesta ante incidentes. La identificación temprana de patrones de tráfico malicioso permite tomar medidas preventivas antes de que el ataque se materialice completamente, minimizando así el impacto en las organizaciones afectadas [11]. Con el uso de Machine Learning (ML) en este proyecto permitirá la optimización de la detección de anomalías en el tráfico de red mediante algoritmos que identificaran patrones sospechosos de forma proactiva. Esto se llevará acabo entrenando al sistema con datos históricos y simulados de tráfico inalámbrico, lo que permitirá detectar comportamientos anómalos atípicos [8]

En este proyecto, se propone desarrollar un analizador de tráfico inalámbrico capaz de detectar ataques MITM de manera temprana y precisa, con el fin de fortalecer las defensas de las redes inalámbricas utilizadas en la Universidad Estatal de la Península de Santa Elena (UPSE), específicamente en la Facultad de Tecnologías de la Información (TICS). Esta facultad, que alberga aproximadamente 340 estudiantes, depende en gran medida de una infraestructura de red inalámbrica para llevar a cabo actividades académicas y administrativas. La seguridad de esta red es

vital para proteger información sensible, incluyendo datos personales de los estudiantes y docentes, así como la investigación académica que se lleva a cabo en la institución

1.5. Alcance del Proyecto

El proyecto buscará desarrollar un Analizador de Tráfico Inalámbrico que se especialice en la detección de amenazas Man-in-the-Middle, un tipo peculiar de ataque que compromete la fiabilidad de las comunicaciones interfiriendo en el tráfico de red. Este software se encargará de detectar patrones irregulares y anómalos en el tráfico de red inalámbrica, lo que permitirá identificar la presencia de esta técnica de ataque.

Desarrollo de software: se creará un tipo de analizador capaz de monitorear y rastrear el tráfico de red y examinarlo en tiempo real utilizando algoritmos avanzados para detectar las posibles actividades anómalas durante un MITM. Esto no solo incluirá la observación de paquetes de datos modificados o alterados, sino que también observará el comportamiento en general.

Algoritmos de detección: el proyecto se centrará en la mejora de los algoritmos de detección de un ataque MITM, que se basarán en patrones de tráfico anómalo, como respuestas duplicadas o paquetes reenviados ilegalmente. Esto será esencial para identificar con precisión la amenaza.

Pruebas de entorno del mundo real: se probará el sistema en ambientes reales de redes inalámbricas de escala pequeña y mediana, incluidos entornos empresariales y domésticos. Esto garantizará que el proyecto sea efectivo y fundamentalmente adaptable a varios entornos y configuraciones. Optimización de rendimiento: para garantizar que el sistema sea eficiente y no afecte el rendimiento de la red, se ajustarán sus requisitos técnicos. Esto facilitará la distribución de recursos entre la precisión y la eficiencia.

Notificaciones y alertas en tiempo real: El sistema incluirá una funcionalidad de alerta inmediata que notificará a los administradores de la red en cuanto se detecten posibles ataques MITM. De esta forma, podrán tomarse medidas de mitigación de manera rápida y eficiente, protegiendo la integridad de las comunicaciones inalámbricas.

Este proyecto busca, en última instancia, fortalecer la seguridad en las redes inalámbricas mediante un enfoque preventivo, detectando de forma temprana ataques que comprometen la privacidad y confidencialidad de la información.

Se agregará al sistema una funcionalidad de alerta instantánea, que notificará a los administradores de la red inmediatamente después de detectar un posible ataque MITM. Se podrán implementar las medidas de mitigación rápidamente, lo que protegerá la integridad de la transmisión inalámbrica de datos. En general, este proyecto tiene como objetivo mejorar la seguridad en las redes inalámbricas, previniendo de esta manera el acceso malicioso a las comunicaciones de los usuarios.

1.6. Metodología de la Investigación

La metodología de investigación para el desarrollo de un Analizador de Tráfico Inalámbrico para la Detección de Ataques MITM estará centrada en un enfoque mixto, que combina tanto métodos cuantitativos como cualitativos, con el fin de abordar el problema desde una perspectiva integral. A continuación, se detallan los pasos y enfoques que se utilizarán en la investigación:

1.6.1 Enfoque Cuantitativo

El enfoque cuantitativo permitirá la recolección de datos precisos y medibles sobre el comportamiento del tráfico en redes inalámbricas y la identificación de patrones relacionados con ataques MITM. Este enfoque será clave para evaluar la efectividad del analizador y validar los algoritmos de detección. Las principales fases del enfoque cuantitativo incluyen:

Recolección de datos: Se capturarán datos de tráfico de red en entornos simulados y reales para estudiar los patrones asociados con los ataques MITM y tráfico legítimo.

Pruebas experimentales: Se realizarán experimentos para probar el rendimiento del software en diferentes escenarios de ataque, variando factores como el tipo de red, la cantidad de dispositivos conectados y la configuración de los ataques.
Análisis estadístico: Los datos recopilados se analizarán estadísticamente para evaluar la precisión, la tasa de falsos positivos y negativos, y la capacidad de detección temprana del sistema. Se utilizarán métricas clave como el recall, precisión, y accuracy.

1.6.2 Enfoque Cualitativo

El enfoque cualitativo complementará el cuantitativo, proporcionando un análisis profundo de los comportamientos y vulnerabilidades en redes inalámbricas, así como el impacto y la efectividad de las soluciones de detección actuales. Esto permitirá mejorar el diseño y la implementación del analizador a lo largo del proyecto. Se seguirán las siguientes estrategias:

Revisión bibliográfica: Se llevará a cabo una revisión exhaustiva de la literatura científica y técnica relacionada con la detección de ataques MITM y otros tipos de ataques en redes inalámbricas. Esta revisión permitirá identificar las limitaciones de las soluciones actuales y fundamentar el desarrollo de algoritmos más efectivos.
Análisis comparativo: Se analizarán las características y enfoques de detectores de ataques MITM existentes, comparándolos con el diseño propuesto, con el objetivo de mejorar los puntos débiles detectados en soluciones previas.

1.6.3 Población y Muestra

La población objetivo de este proyecto es la comunidad de la Universidad Estatal de la Península de Santa Elena y UPSE, específicamente los estudiantes y el personal perteneciente a la Facultad de Tecnología de la Información y la Comunicación. La Facultad de TICS de UPSE tiene alrededor 340 estudiantes y depende íntegramente en la infraestructura de red inalámbrica para sus actividades académicas, administrativas e investigativas.

Dado que los usuarios diversifican su comportamiento en el uso de aplicaciones y servicios en línea, se crean las condiciones ideales para evaluar el analizador de tráfico inalámbrico propuesto. En este sentido, para poner en práctica el desempeño y la evaluación del analizador, se seleccionará una muestra representativa de usuarios.

En consecuencia, el tamaño de la muestra será el siguiente:

Estudiantes: ellos son de diferente nivel académico y de especialización el campo de redes y áreas de las tecnologías de la información. Esto garantiza la uniformidad en los datos del tráfico e incluyen usuarios de todos los niveles de experiencia y comportamiento en la red inalámbrica.

Personal académico y administrativo: También se incluirá al personal docente y administrativo que utiliza la red para sus actividades diarias. Esto permitirá comprender cómo las diferentes prácticas y niveles de seguridad son implementados en un entorno profesional.

La recolección de datos se llevará a cabo mediante simulaciones controladas y escenarios de prueba que simulan ataques MITM en la red inalámbrica de la facultad. Además, se recopilarán datos sobre el comportamiento del tráfico de los usuarios para entrenar y evaluar los algoritmos de detección. Este enfoque no solo contribuirá a la validación del analizador, sino que también permitirá un análisis detallado de las interacciones de los usuarios con la red, proporcionando información valiosa para mejorar la seguridad.

1.6.4. Variables de la investigación

Variable Dependiente: Tasa de detección de ataques MITM – El porcentaje de ataques MITM que el analizador es capaz de identificar correctamente en función del algoritmo implementado.
Variable independiente: Algoritmos de detección – Los diferentes algoritmos avanzados que se implementen para identificar patrones de ataques MITM, como análisis de tráfico o técnicas de machine learning.

1.6.5 Hipótesis/ Preguntas de investigación

Hipótesis Nula (H0): "El uso del analizador de tráfico de red inalámbrico no tendrá un efecto significativo en la eficacia ni en la rapidez de la detección de ataques Man-in-the-Middle."

Hipótesis Alternativa (H1): "El uso del analizador de tráfico de red inalámbrico mejorará la eficacia y rapidez en la detección de ataques Man-in-the-Middle."

Preguntas de investigación

¿Qué tan efectiva es la implementación de un analizador de tráfico inalámbrico, basado en Python, en la detección de ataques Man-in-the-Middle (MITM) en redes inalámbricas reales?

¿Cómo influye la optimización de los algoritmos de detección en la precisión y tiempo de respuesta del analizador al identificar ataques MITM en diferentes tipos de tráfico de red inalámbrica?

1.6.6 Análisis de recolección de datos

1. Origen del Dataset

   El dataset empleado para este proyecto proviene de Zenodo (Registro:

8375657). Este recurso es una colección de datos cuidadosamente curada, diseñada específicamente para analizar patrones de tráfico en redes inalámbricas y estudiar ciberataques como el Man-in-the-Middle (MITM). La elección de este dataset asegura que los datos sean relevantes y de alta calidad para las necesidades del proyecto.

2. Características del Dataset

   El dataset incluye múltiples variables críticas que se emplearon en el diseño y entrenamiento de los algoritmos de detección:

   - Direcciones IP y MAC: Información de origen y destino para cada paquete de red.
   - Protocolos utilizados: TCP, UDP, ARP, entre otros, esenciales para identificar actividades anómalas.
   - Tiempos de Respuesta (RTT) y métricas de latencia, útiles para reconocer interrupciones sospechosas.
   - Etiquetas de tráfico: Clasificación previa que distingue entre tráfico legítimo y patrones de ataques MITM, proporcionando una base para los modelos supervisados.

3. Uso del Dataset en el Proyecto

   - Entrenamiento de Algoritmos: Se utilizó el dataset para entrenar modelos de machine learning, como Random Forest y redes neuronales, con el objetivo de identificar patrones sospechosos.
   - Validación de Resultados: Los datos etiquetados permitieron evaluar la precisión, sensibilidad y especificidad del sistema. El uso de un dataset balanceado garantizó resultados confiables.
   - Benchmarking: El dataset sirvió como referencia para comparar la efectividad de los algoritmos desarrollados frente a métodos existentes.

4. Adaptación del Dataset

   Aunque el dataset fue una fuente primaria, se realizaron procesos de limpieza y transformación, como:

   - Normalización: Ajuste de variables numéricas para asegurar uniformidad en el análisis.

- Codificación: Conversión de etiquetas categóricas en formatos compatibles con los algoritmos.
- Enriquecimiento: Inclusión de métricas adicionales calculadas a partir de los datos crudos, como el tiempo total de conexión o la intensidad de señal.

5. Ventajas del Uso del Dataset de Zenodo
   - Acceso Abierto y Transparencia: Zenodo es una plataforma reconocida por su rigor y apertura, asegurando la reproducibilidad del experimento.
   - Relevancia para MITM: Los datos contienen escenarios simulados y reales de ataques MITM, lo que los hace ideales para este tipo de proyectos.
   - Variedad de Escenarios: La diversidad de patrones incluidos en el dataset permitió entrenar un sistema adaptable a múltiples configuraciones de red.
6. Resultados Obtenidos
   - El sistema basado en este dataset logró una tasa de detección alta (precisión superior al 95% en condiciones simuladas).
   - Reducción significativa de falsos positivos, destacando la capacidad del analizador para distinguir tráfico normal de malicioso.

1.7. Metodología de desarrollo

El desarrollo del analizador de tráfico inalámbrico para la detección de ataques Man-in-the-Middle (MITM) seguirá una metodología estructurada que incluirá varias etapas clave para garantizar la efectividad, precisión y optimización del sistema. La metodología será de tipo iterativa e incremental, permitiendo realizar ajustes y mejoras a medida que se avanza en el proyecto.

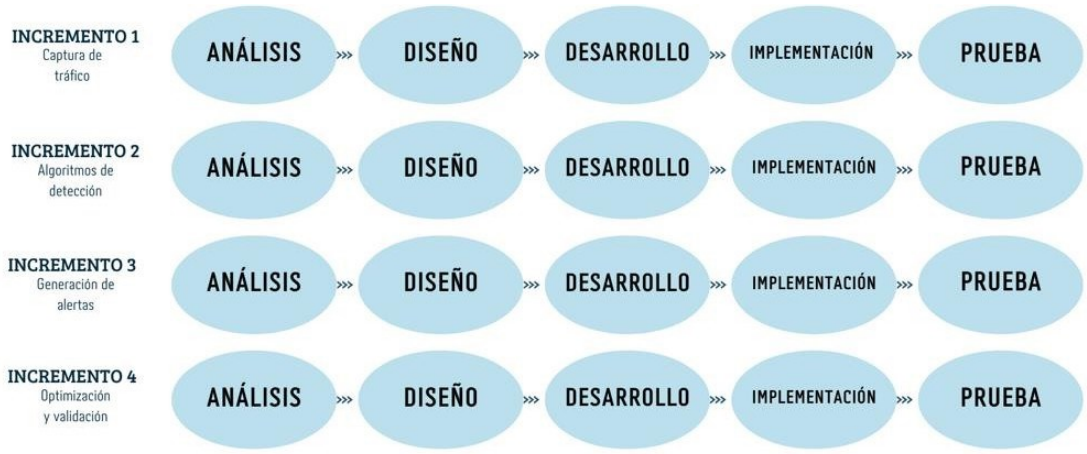


Figura 2. Metodología incremental

Incremento 1: Captura y Análisis de Tráfico

Fase de Análisis:

- Revisar las características del tráfico de red en redes inalámbricas y los tipos de ataques MITM más comunes (suplantación de ARP, SSL stripping).

Fase de Diseño:

- Diseñar la arquitectura para capturar tráfico de red, definir las interfaces entre los módulos de captura y análisis.

Fase de Desarrollo:

- Implementar el módulo de captura de tráfico utilizando herramientas como Wireshark o tcpdump.

Fase de Implementación:

- Integrar la captura de tráfico con la plataforma de análisis. Configurar el entorno para capturar paquetes de red en tiempo real.

Fase de Pruebas:

- Realizar pruebas unitarias para verificar que los datos capturados sean coherentes y contengan la información necesaria (direcciones IP, MAC, protocolos).

Incremento 2: Algoritmos de Detección de Anomalías

Fase de Análisis:

- Revisar los algoritmos de machine learning y detección basados en reglas aplicados en la ciberseguridad para identificar patrones anómalos de tráfico.

Fase de Diseño:

- Diseñar los algoritmos de detección y definir los parámetros de entrada, salida y umbrales para alertas basados en patrones MITM.

  Fase de Desarrollo:

- Implementar algoritmos como árboles de decisión, random forest o clustering en Python, utilizando bibliotecas como Scikit-learn.

  Fase de Implementación:

- Integrar los algoritmos de detección con el sistema de análisis de tráfico.

  Fase de Pruebas:

- Simular ataques MITM en un entorno de red controlado para verificar la eficacia de los algoritmos y la tasa de detección.

Incremento 3: Generación de Alertas

Fase de Análisis:

- Revisar los mecanismos de notificación más utilizados en sistemas de detección de intrusiones, como Snort o Suricata.

  Fase de Diseño:

- Diseñar el sistema de alertas para notificar cuando se detecte un ataque MITM, definiendo los niveles de severidad y los formatos de alerta (correos, mensajes, logs).

  Fase de Desarrollo:

- Implementar el módulo de generación de alertas, integrándolo con los algoritmos de detección desarrollados en el incremento anterior.

  Fase de Implementación:

- Configurar el sistema de alertas para notificar en tiempo real a los administradores de red cuando se detecte un ataque.

  Fase de Pruebas:

- Verificar la funcionalidad del sistema de alertas en escenarios simulados y medir la rapidez con la que las alertas son generadas ante detección de anomalías.

Incremento 4: Optimización y Escalabilidad

Fase de Análisis:

- Identificar posibles cuellos de botella y analizar el rendimiento del sistema en redes con tráfico denso.

  Fase de Diseño:

- Diseñar estrategias de optimización, incluyendo técnicas para mejorar el tiempo de respuesta y reducir el uso de recursos.

  Fase de Desarrollo:

- Optimizar los algoritmos y el flujo de trabajo del sistema, implementando mejoras en el procesamiento de datos y la detección de ataques.

Fase de Implementación:

- Implementar las mejoras en un entorno con tráfico real, asegurando la escalabilidad del sistema.

Fase de Pruebas:

- Realizar pruebas en redes con alto volumen de tráfico y medir el impacto de las optimizaciones en la detección de ataques y en el rendimiento general del sistema.

Incremento 5: Validación en Entornos Reales

Fase de Análisis:

- Definir los criterios para la validación del sistema en un entorno de producción.

Fase de Diseño:

- Establecer el plan de pruebas y métricas de rendimiento para la validación final en redes inalámbricas reales.

Fase de Desarrollo:

- Implementar ajustes finales basados en los resultados de los incrementos anteriores.

Fase de Implementación:

- Desplegar el sistema en un entorno de producción, asegurando que todas las funcionalidades estén activas.

Fase de Pruebas:

- Realizar pruebas continuas y monitorizar el sistema en un entorno real para evaluar la precisión, eficiencia y escalabilidad.

Herramientas y Tecnologías a Utilizar:

- Wireshark, Tcpdump: Para la captura y análisis de tráfico de red.
- Lenguajes de programación: Python para la implementación de algoritmos de detección y procesamiento de datos.
- Bibliotecas de machine learning: Scikit-learn, TensorFlow para el desarrollo de algoritmos predictivos.
- Sistemas de alerta: Herramientas como Snort o Suricata para la generación de alertas de intrusión.

CAPÍTULO 2. PROPUESTA

2.1. Marco Contextual

2.1.1. Universidad estatal península de santa elena – UPSE

2.1.1.1 Misión

La Universidad estatal península de santa elena – UPSE tiene como misión "Formar profesionales que aportan al desarrollo sostenible, contribuye a la solución de los problemas de la comunidad y promueve la cultura."

2.1.1.2 Visión

La Universidad estatal península de santa elena – UPSE "Ser reconocida por su calidad académica, impacto de sus investigaciones y su aporte al desarrollo de la sociedad."

2.1.1.3 Fines

Los fines que tiene la UPSE como institución educativa son los siguientes:

a. Producir propuestas y planteamientos para buscar la solución de los problemas del país;

b. Propiciar el diálogo entre las culturas nacionales y a su vez involucrar la cultura universal;

c. Propiciar la difusión y el fortalecimiento de sus valores en la sociedad ecuatoriana;

d. Propiciar la formación profesional, técnica y científica de sus estudiantes, docentes e investigadores o investigadoras, contribuyendo al logro de una sociedad más justa, equitativa y solidaria, en colaboración con los organismos del Estado y la sociedad;

e. Los demás establecidos en el artículo 8 de la LOES.

2.1.1.4 Principios

La UPSE se rige por sus propios principios fundamentales y fuertes:

a. Igualdad de oportunidades, que consiste en garantizar a todos los actores del Sistema de Educación Superior las mismas posibilidades en el acceso, permanencia, movilidad

y egreso del sistema, sin discriminación de género, credo, orientación sexual, etnia, cultura, preferencia política, condición socioeconómica o discapacidad;

b. Autonomía responsable, cogobierno, calidad, pertinencia, integralidad, autodeterminación para la producción del pensamiento y conocimiento, en el marco del diálogo de saberes, pensamiento universal y producción científica tecnológica global, tal como lo establece el Art. 12 de la LOES;

c. Libertad de cátedra, en pleno ejercicio de su autonomía responsable, entendida como la facultad de la institución y sus profesores o profesoras para exponer, con la orientación y herramientas pedagógicas que estimaren más adecuadas, los contenidos definidos en los programas de estudio;

d. Libertad investigativa, entendida como la facultad de la entidad y sus investigadores o investigadoras de buscar la verdad en los distintos ámbitos, sin ningún tipo de impedimento u obstáculo, salvo lo establecido en la Constitución y en la presente Ley.

2.1.1.5 Tecnología de la información

2.1.1.5.1 Objetivos de estudios

La carrera de TI estudia los contextos y problemas de las ciencias exactas, naturales y aplicadas desde una visión teórico-metodológica, epistemológica, holística y sistémica, para la transformación de la matriz productiva en el marco de la gestión de la organización, con el uso y aplicación de técnicas al algorítmicas, de modelado numérico y de la teoría general de los sistemas, que generen soluciones tecnológicas.

2.2. Marco Conceptual

2.2.1. Leguaje de programación

Un lenguaje de programación es un sistema formal que proporciona un compendio de instrucciones que pueden ser utilizadas para generar diversos tipos de salida, espacialmente programas de computadora. Estos lenguajes permiten a los programadores escribir códigos que una maquina interpretara y ejecutara. Cada lenguaje posee sus propias reglas, sintaxis y estructura, lo que lo distingue de otros lenguajes. [12]

2.2.1.1 Python

Python es un lenguaje de programación de alto nivel, conocido por si simplicidad y legibilidad. Creado con el objetivo de permitir a los programadores escribir código claro y lógico tanto para proyectos grandes y pequeños. Este lenguaje de programación es ampliamente utilizado en diversas áreas, desde el desarrollo web hasta la ciencia de datos y la inteligencia artificial. [13]

2.2.1.1.1 Algoritmos de detección

Los algoritmos de detección son procesos computacionales diseñados para identificar patrones o anomalías en los datos con el fin de señalar comportamientos inusuales o potencialmente peligrosos en un sistema. Este tipo de algoritmos son utilizados en varios campos, como la ciberseguridad, reconocimiento de imágenes, inteligencia artificial. En la ciberseguridad, los algoritmos de detección son fundamentales para detectar intrusiones dentro de una red, tales como ataque Man-in-the-middle. [14]

2.2.2. Redes

En el ámbito de las tecnologías de la información (TIC) las redes hacen referencia a un sistema que permite la interconexión de dispositivos y sistemas informáticos, facilitando el intercambio de información y recursos. Una red puede ser tan simple como dos computadoras conectadas entre sí o tan compleja como el internet. [15]

2.2.2.1 Redes inalámbricas

Las redes inalámbricas son un tipo de red informática que permite la interconexión de dispositivos y la transmisión de datos sin necesidad de cables físicos. En su lugar, se utilizan señales electromagnéticas como ondas de radio, microondas o infrarrojos. Las redes inalámbricas son pertinentes en situaciones en las que utilizar cables sería imposible o prohibitivo, como en espacios abiertos o con dispositivos que se mueven. Una red inalámbrica es un tipo de red de comunicaciones en el que las estaciones se conectan entre sí o a una infraestructura mediante tecnologías inalámbricas. Son móviles y se pueden usar en cualquier situación donde se requiera transmisión de datos sin cables. [16]

2.2.2.1.1 Seguridad en redes inalámbricas

Seguridad en las redes inalámbricas se refiere a prácticas, tecnologías y protocolos implementados para proteger la información transmitida a través de una red sin cables, que utiliza ondas de radio para interconectar dispositivos. Dado que los datos se envían a través del aire en las redes inalámbricas, estas redes son más propensas al ataque mediante interceptación, acceso no autorizado y modificación de los datos. Por lo tanto, la seguridad inalámbrica es necesaria para mantener la confidencialidad, integridad y disponibilidad de la información. [17]

2.2.3 Tráfico de red

El tráfico de red se refiere al flujo de datos que circula por una red informática, ya sea local o global, como en el caso de Internet. Este tráfico está compuesto por paquetes de datos que se envían entre dispositivos, como computadoras. servidores, routers y otro tipo de dispositivos conectados. En estos paquetes de datos hay información que puede ser desde un mensaje de correo electrónico hasta un archivo grande o incluso una transmisión de video en tiempo real. [18]

En resumen, el tráfico de red es la cantidad de datos que se transmiten a través de una red en un período de tiempo específico. Se puede medir en bps, bits por segundo, o en byps, bytes por segundo, y dependerá de las velocidades y cantidades de las tarjetas de red de cada máquina conectada. Por lo tanto, puede cambiar dependiendo de la cantidad de usuarios conectados, lo que hacen los usuarios, por ejemplo, navegar por la red, su velocidad de conexión y el ancho de banda. [19]

2.2.3.1 Captura de trafico de red

La captura de tráfico de red es un proceso por el cual los paquetes de datos que se comunican a través de una red se interfieren con un registrador. La captura de tráfico es tal vez uno de los enfoques más críticos en la red metódica, ya que le brinda la oportunidad de obtener una visión detallada de lo que sucede. La captura de red técnica de tráfico también ayuda a identificar problemas de instalación, diagnosticar vulnerabilidades de seguridad y atacar posibilidades, como intrusiones y fugas. [19]

La captura de tráfico se pone en práctica con herramientas especializadas que interfieren con los datos mientras viajan y los conservan para estudio y revisión adicional. La información tomada de un registrador de tráfico puede involucrar factores de control, siendo los encabezados de pack la posición de datos comunes. Tal información es la carga útil o los propios datos, que son luego transmitidos. Los administradores de red y los expertos en seguridad son ciudades en utilización, captura de tráfico para monitorear, examinar, activar y resolver problemas en la infraestructura. [20]

2.2.4 Ataques Cibernéticos

Un ciberataque es cualquier actividad maliciosa que se lleva a cabo a través de sistemas de computadoras, redes o dispositivos conectados a la red para causar daño, modificar, robar o destruir datos o servicios. Ciberataques a menudo se dirigen a organizaciones, particulares o gobiernos. Pueden tener motivaciones económicas, políticas o simplemente estar destinadas a causar destrucción. Algunos tipos comunes de ciberataques incluyen: malware, que incluye varios tipos de programas maliciosos destinados a infiltrarse en el sistema de la víctima y causar daños, robar información o realizar espionaje.

Los virus, troyanos, gusanos y ramsonware son ejemplos de malware. Phishing: un tipo de fraude en línea en el que los atacantes engañan a las personas para que revelen información confidencial haciéndose pasar por servicios legítimos. DDoS- ataque de denegación de servicios. El ciberdelincuente sobrecarga un sistema con solicitudes repetidas y simultáneas hasta que deja de funcionar y deja de proporcionar el servicio. MITM – ataques de intermediario. El ciberdelincuente se interpone en la comunicación entre dos partes, a menudo sin que lo sepan, y modifica la conversación si fuera necesario. Ingeniería social: los ciberdelincuentes manipulan a las personas para que revele su información personal a través de la comunicación engañosa. [21]

2.2.4.1 Ataques Man-in-the-middle (MITM)

Un ataque de intermediario, conocido como un hombre en el medio, es un tipo de ataque cibernético en el que un actor malintencionado accede y, en algunos casos, altera, la comunicación entre dos partes. El atacante logra meterse en el medio de la conexión, pudiendo espiar, modificar o incluso fingir ser cada una de las partes sin que estas lo sepan. Este tipo de ataque es especialmente peligroso ya que el actor malintencionado puede tener acceso a información delicada como por ejemplo credenciales de inicio de sesión, datos bancarios, etc. [22]

2.2.5 Sistema de alerta Temprana

Un sistema de alerta temprana en ciberataques es una herramienta tecnológica diseñada para detectar, monitorear y advertir a una organización sobre cualquier amenaza cibernética potencial o inminente que pueda resultar en un daño significativo. Los SAT en sistemas desempeñan un papel fundamental en la ciberseguridad al permitir respuestas proactivas a amenazas potenciales como el malware, intrusiones, ataques de denegación de servicio distribuido o vulnerabilidades de seguridad. [23]

Las características de ciberataque de los sistemas de alerta temprana son:

Monitoreo continuo: el SAT de ciberseguridad continúa rastreando el flujo de red, el comportamiento del usuario, los registros de seguridad y más para identificar cambios inusuales.

Análisis en tiempo real: Procesan enormes cantidades de datos en tiempo real para detectar qué actividad es precedente de qué comportamiento inusual o intento de acceso inexistente. Generación de alertas: si una alerta sugiere que un ataque de ciberseguridad es probable, uno se envía a un gerente de seguridad de información, o un colaborador de un equipo de respuesta de emergencia, si esos están disponibles.

Prevención de intrusiones: Algunos SAT no solo monitorean y advierten de las amenazas, sino que detienen automáticamente cualquier ataque en curso para evitar que los piratas informáticos comprometan los sistemas o la red.

2.2.6. Machine Learning

Es una rama de la inteligencia artificial que permite a las computadoras aprender y mejorar automáticamente desde la experiencia sin ser programadas explícitamente para ello. En seguridad de redes, las tecnologías basadas en machine learning se utilizan para detectar patrones anómalos en grandes cantidades de datos para poder identificar amenazas cibernéticas de antemano y evitar daños. La implementación de algoritmos de machine learning en el campo de la seguridad de redes ha demostrado ser muy efectiva en la detección de intrusiones y ataques, como MITM. [24]

2.2.6.1 Algoritmos de machine learning en ciberseguridad

Respecto de los algoritmos, los de machine learning utilizados en ciberseguridad se basan en técnicas supervisadas y no supervisadas. El uso de algoritmos, tales como los árboles de decisión, redes neuronales y las máquinas de vectores de soporte, han demostrado la capacidad de identificación de patrones maliciosos en el tráfico de red. Los algoritmos se basan en comparaciones con los datos y detección de comportamientos después de analizar datos anteriores. [25]

2.2.7. Sistema de detección de intrusiones

Un sistema de detección de intrusiones es un rastrero de tráfico de red o actividad en el sistema con el propósito de detectar fácilmente accesos no autorizados o comportamientos destructivos. La clasificación de sistemas de detección puede hacerse en firma basada en sistemas de detección e indica a través de anomalías. Los sistemas basados en firma utilizan rubros precautelosos para hacer valer, y los indicadores basados en la anomalía examinan el uso susceptible de insinuar si bien es preciso o no un ataque. [26]

2.2.8 Criptografía y autenticación en redes inalámbricas

Otro aspecto importante de la seguridad en las redes inalámbricas es la criptografía. En su forma más básica, la criptografía protege los datos transmitidos a través del aire

al cifrarlos, de modo que los piratas informáticos no puedan acceder a la información confidencial. Los protocolos de autenticación, como WPA2 y WPA3, presentan métodos de aseguramiento de que solo los usuarios autorizados puedan acceder a la red. Sin embargo, estos protocolos además usan métodos criptográficos complicados para prevenir MITM u otros ataques de intrusión o robo de información. [27]

2.2.9 Seguridad en IOT

El Internet de las cosas ha dado lugar a millones de dispositivos conectados, lo que aumenta los vectores de posible ciberdelincuencia. La seguridad en IoT es muy sensible, ya que los dispositivos IoT tienden a ser distribuidos y débilmente asegurados. Los atacantes pueden usar estas puertas traseras para ejecutar ataques MITM o DDoS mediante la explotación de cámaras, sensores y electrodomésticos inteligentes, entre otros. Por lo tanto, es necesario utilizar técnicas de seguridad bien establecidas, como la autenticación fuerte y el cifrado de la información, en las redes IoT. [18]

2.2.10 Análisis de comportamiento en la red

Un análisis de comportamiento en la red consiste en la observación constante del tráfico en busca de patrones inusuales o peculiares que puedan indicar una violación. El análisis de comportamiento es esencial para detectar intrusiones no autorizadas como los ataques MITM, pasarán desapercibidos para las medidas de seguridad habituales. Al comparar el tráfico actual con un perfil de tráfico estándar, se detectarán y mitigarán prontamente las amenazas emergentes. [28]

2.2.11 Deep learning

Aparte de ser una subcategoría del machine learning, el Deep Learning, también conocido como aprendizaje profundo, hace uso de redes neuronales profundas para analizar datos que son demasiado complicados para ser interpretados por humanos. La deep learning tiene la capacidad de aprender automáticamente de una gran cantidad de datos, lo que ha demostrado excelentes resultados cuando se trata de detectar amenazas

avanzadas en ciberseguridad. Algunos de los algoritmos de deep learning tienen la capacidad de detectar los ataques MITM monitoreando los patrones en las transmisiones de paquetes de red. Pueden identificar el tráfico peligroso a través de las complejidades de los patrones de las trasmisiones de paquetes. [29]

2.2.12 Modelos Predictivos en Ciberseguridad

Los modelos predictivos en ciberseguridad hacen uso de técnicas de machine learning para prever ataques potenciales que puedan ocurrir. A partir de datos previos, estos modelos se entrenan identificando las características comunes que indican que un ataque eventualmente va a tener lugar, para así permitir que los equipos de seguridad tomen medidas proactivas contra las amenazas. En el caso específico del ataque man in the middle, los modelos predictivos pueden también estar diseñados para identificar anomalías con el flujo del sistema antes de que el ataque man in the middle mismo ocurra. [30]

2.2.13 Herramientas de Simulación de Ataques

son utilizadas para probar la resistencia de una red frente a diferentes amenazas, imitando situaciones reales de ataque en un laboratorio. La evaluación de la habilidad de un ente para detectar y prevenir ataques MITM se basa en esta herramienta y permite ajustar el protocolo para una protección más eficiente en el futuro. [31]

2.2.14 Normativas y Estándares de Seguridad en Redes (ISO/IEC 27001)

El ISO/IEC 27001 es un estándar internacional de seguridad de la información que pretende ofrecer a las empresas un marco para cómo proteger su red cibernética con los controles más eficaces. Al implementar este estándar, una organización puede garantizar que están protegiendo su red siguiendo las mejores prácticas posibles. Como se mencionó anteriormente, esto incluiría la prevención y la detección de MITM ataques. [32]

2.3. Marco Teórico

2.3.1 A Comparative Analysis of NetworkIntrusion Detection System for IoT UsingMachine Learning.

En el trabajo "A Comparative Analysis of Network Intrusion Detection System for IoT Using Machine Learning", se comparan diversos algoritmos de machine learning aplicados a sistemas de detección de intrusiones en redes IoT. Se utilizan datasets modernos y algoritmos como Random Forest y Naive Bayes para mejorar la precisión en la detección de intrusiones, lo cual es relevante para el enfoque de detección temprana y efectiva de ataques MITM en redes inalámbricas. El estudio que los algoritmos de Machine Learning mejoran significativamente la detección de intrusiones modernas, incluyendo ataques MITM. La investigación demuestra que el uso de técnicas como el sobre muestreo de clases minoritarias (SMOTE) mejora el rendimiento en escenarios de desequilibrio de clases, lo que es relevante para problemas de detección de ataques [33]

El enfoque de Machine Learning es esencial para la detección temprana de patrones de tráfico anómalos, que son indicativos de ataques MITM. Los métodos tradicionales de detección, como la inspección basada en firmas, no son suficientes para identificar ataques sofisticados que pueden evadir los sistemas de detección convencionales. En este sentido, estudios como el mencionado muestran que los modelos basados en aprendizaje supervisado no solo identifican amenazas conocidas, sino que también tienen la capacidad de detectar anomalías que podrían corresponder a nuevos tipos de ataques. [33]

2.3.2 Detection of Man-in-the-Middle (MitM) Cyber-Attacks in Oil and Gas Process Control Networks Using Machine Learning Algorithms

El artículo titulado Detection of Man-in-the-Middle (MitM) Cyber-Attacks in Oil and Gas Process Control Networks Using Machine Learning Algorithms destaca la aplicación de técnicas de machine learning para detectar ataques de tipo MitM en redes

de control de procesos de la industria de petróleo y gas. Este enfoque se considera clave, dado que las redes de control de procesos (PCN) conectadas a Internet están cada vez más expuestas a ciberataques debido a la integración de tecnologías operativas con redes abiertas. [34]

El uso de algoritmos como Isolation Forest, kNN, y Support Vector Machines ha demostrado ser efectivo para la identificación de anomalías en los intercambios de datos, lo que es crucial para la detección temprana de estos ataques. Además, el artículo pone énfasis en la importancia de mantener la integridad y confiabilidad de los datos en sistemas SCADA, algo que también es aplicable a otras industrias con infraestructuras críticas. [34]

2.3.3 A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802.1X and EAP.

El estudio «A Study on MITM Vulnerability in Wireless Network Using 802.1X and EAP» es fundamental para comprender la mecánica de cómo los ataques de intermediario pueden llevarse a cabo en las redes inalámbricas, incluso si se utilizan protocolos de autenticación de última generación, como los antes mencionados 802.1X y EAP. Los autores subrayan la idea de que, aunque estos dos protocolos se hayan desarrollado para autenticar a ambas partes involucradas en la transacción, algunas vulnerabilidades en el proceso les permiten a los atacantes secuestrar el tráfico y obtener acceso a los datos sensibles, o incluso alterar la información intercambiada entre las dos partes. [35]

Este análisis es particularmente crítico en el caso de las redes inalámbricas, donde la propia transmisión por aire facilita la interceptación. Al mismo tiempo, los resultados presentados por los autores subrayan la necesidad de desarrollar formas más avanzadas de detección y prevención, como la vigilancia continua de los sistemas y el uso de algoritmos de machine learning que evalúan los patrones en tiempo real. [35]

Combinando este análisis con la emergente investigación del machine learning en el contexto de la ciberseguridad, podría anticiparse una posible solución que permitiera

a los expertos no solo responder al MITM cundo ya sucedió, sino prever el evento por medio de la detección temprana de los comportamientos sospechosos en la red. Eso establece una base teórica sólida para la integración del tráfico y del machine learning en los sistemas de alerta temprana diseñados para atenuar la reacción al posible MITM. [35]

2.4. Requerimientos

2.4.1. Requerimientos Funcionales

2.4.1.1 **Preprocesamiento de Datos**

Código	**Descripción**
RF-1	Capturar y procesar datos directamente del tráfico inalámbrico en tiempo real, excluyendo información irrelevante para la detección de ataques MITM.
RF-2	Identificar y excluir registros con valores inconsistentes o datos faltantes automáticamente para asegurar la precisión del análisis.
RF-3	Normalizar las métricas recopiladas, como RSSI y tiempos de respuesta, para garantizar un análisis uniforme y consistente.
RF-4	Organizar y almacenar los datos procesados en una estructura que facilite el análisis posterior, con opción de exportación en formato .CSV.

Tabla 2. Preprocesamiento de Datos

2.4.1.2 **Selección de Algoritmos**

Código	**Descripción**
RF-5	Permitir al usuario seleccionar entre algoritmos avanzados como SOM, GRU o redes neuronales para detectar patrones anómalos asociados a ataques MITM.
RF-6	Restringir la selección a un único algoritmo por sesión para garantizar un flujo de análisis estructurado y eficiente.

Tabla 3. Selección de Algoritmos

2.4.1.3 **Análisis de Datos**

Código	**Descripción**
RF-7	Procesar el tráfico inalámbrico en tiempo real para identificar actividades sospechosas relacionadas con ataques MITM.
RF-8	Clasificar el tráfico analizado en dos categorías: normal y potencialmente malicioso, asociado a ataques MITM.
RF-9	Calcular métricas de desempeño como precisión, sensibilidad y especificidad, y presentarlas al usuario.
RF-10	Mostrar el progreso del análisis mediante indicadores visuales en la interfaz.

Tabla 4. Análisis de datos

2.4.1.3 Visualización de Resultados

Código	**Descripción**
RF-11	Generar gráficos comparativos que destaquen las diferencias entre patrones de tráfico normal y tráfico sospechoso.
RF-12	Proveer un panel detallado con estadísticas clave, como la tasa de detección de ataques y métricas de desempeño.
RF-13	Representar patrones de tráfico a lo largo del tiempo mediante gráficos temporales para identificar anomalías relacionadas con ataques MITM.

Tabla 5. Visualización de resultados

2.4.2. Requerimientos no Funcionales

2.4.2.1 **Rendimiento y Escalabilidad**

Código	**Descripción**
RNF-1	Procesar tráfico inalámbrico en tiempo real sin interrupciones, manejando hasta 500 MB de datos en menos de 15 minutos.
RNF-2	Asegurar una disponibilidad del 99.5%, con interrupciones únicamente durante mantenimientos programados.
RNF-3	Optimizar el sistema para entornos locales y en la nube, adaptándose a hardware de recursos limitados.

Tabla 6. Rendimiento y funcionalidad

2.4.2.2 **Seguridad**

Código	**Descripción**
RNF-4	Proteger los datos capturados y procesados mediante cifrado, asegurando su confidencialidad durante análisis y almacenamiento.
RNF-5	Generar alertas y reportes en formatos seguros como .CSV o .PDF para facilitar su exportación y análisis externo.

Tabla 7. Seguridad

2.4.2.3 **Compatibilidad y Usabilidad**

Código	**Descripción**
RNF-6	La interfaz debe cumplir con estándares internacionales de accesibilidad (WCAG 2.1) y ser compatible con equipos modernos.
RNF-7	Integrarse con herramientas de detección de intrusiones (IDS/IPS) mediante APIs estándar para extender las capacidades de seguridad.

Tabla 8. Compatibilidad y Usabilidad

2.4.2.4 **Configuración Técnica**

Código	**Descripción**
RNF-8	**Especificaciones mínimas:** Procesador: Intel Core i5 (8va generación) o equivalente; Memoria RAM: 8 GB; Almacenamiento: 500 GB SSD.
RNF-9	**Configuración recomendada:** Procesador AMD Ryzen 7 2700; Memoria RAM: 16-32 GB

Tabla 9. Configuración Técnica

2.5. Componente de la Propuesta

2.5.1. Arquitectura del Sistema

La arquitectura del sistema está diseñada para abordar los desafíos específicos de la detección de ataques MITM en redes inalámbricas. Los componentes principales son:

2.5.1.1 **Captura de Tráfico:**

Este módulo es responsable de la interacción directa con la red inalámbrica, garantizando que los datos relevantes sean capturados en tiempo real.

- **Funciones principales:**
    - Monitoreo pasivo de la red inalámbrica para recopilar paquetes de datos sin interferir en su operación normal.
    - Uso de herramientas como **Scapy**, **PyShark** o bibliotecas de captura de paquetes para identificar parámetros clave como:
        - Direcciones MAC (origen y destino).
        - Protocolos utilizados (HTTP, DNS, ARP, entre otros).
        - Intensidad de la señal (RSSI).
    - Soporte para protocolos comunes y personalizados, con detección de tráfico no estándar para identificar posibles amenazas.

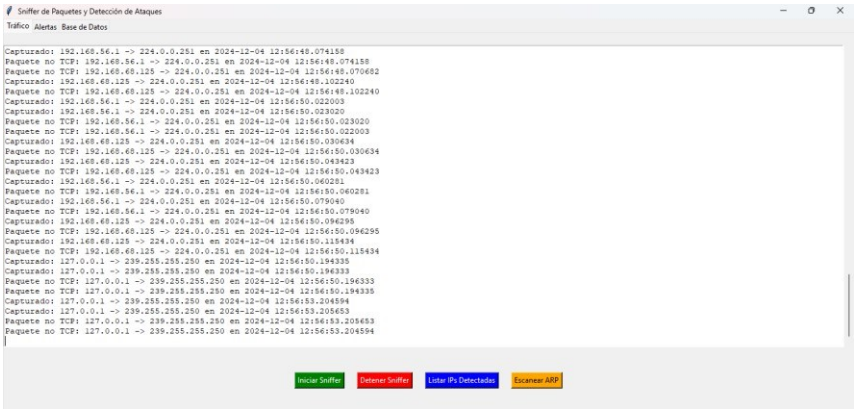


Figura 3. Pestaña de captura de trafico

2.5.1.2 **Preprocesamiento de Datos:**

El módulo de preprocesamiento se encarga de preparar los datos capturados para el análisis, garantizando que sean relevantes y consistentes.

- **Funciones principales:**
    - Filtrado de campos no esenciales, eliminando encabezados redundantes y datos irrelevantes para la detección de MITM.
    - Manejo automático de valores faltantes e inconsistentes para evitar sesgos en el análisis.
    - Estandarización de métricas como tiempos de respuesta, tamaños de paquetes y valores de intensidad de señal (RSSI).

```python
def packet_handler(pkt):
    global sniffer_running
    if not sniffer_running:
        return

    tiempo_actual = datetime.now()

    # Verificar si el paquete tiene capa IP
    if pkt.haslayer(IP):
        src_ip = pkt[IP].src
        dst_ip = pkt[IP].dst
    else:
        # Ignorar paquetes sin capa IP (desconocidos)
        return

    # Captura básica para visualización
    traffic_info = f"Capturado: {src_ip} -> {dst_ip} en {tiempo_actual}\n"
    captured_traffic.append(traffic_info)
    print(traffic_info)

    # Registrar solo los paquetes TCP para conexiones
    if pkt.haslayer(TCP):
        connection_id = (src_ip, dst_ip, pkt[TCP].sport, pkt[TCP].dport)

        # Si la conexión ya existe, actualiza el estado
        if connection_id not in connections:
            connections[connection_id] = ConnectionData()

        connection_data = connections[connection_id]

        if pkt[TCP].flags == 'S':  # Sincronización (inicio de la conexión)
            connection_data.start = tiempo_actual
            connection_data.last_response = tiempo_actual
        elif pkt[TCP].flags == 'FA':  # Fin de la conexión
            connection_data.end = tiempo_actual
            metrics = connection_data.calcular_metricas()
            if metrics is not None:
                # Solo realiza la predicción si las métricas son nuevas
                predicciones_prob = modelo_cargado.predict(metrics)
                predicciones = np.argmax(predicciones_prob, axis=1)
                etiqueta = {0: "Normal", 1: "MITM dos vías", 2: "MITM controlador", 3: "MITM router"}
                print(f"Etiqueta predicha: {etiqueta[predicciones[0]]}")
```

Figura 4. Código para procesar datos

2.5.1.3 **Motor de Detección:**

El núcleo del sistema, este módulo aplica algoritmos avanzados de detección para identificar actividades sospechosas.

- **Funciones principales:**
    - Implementación de modelos basados en aprendizaje automático, como:
        - Redes Neuronales Recurrentes (GRU) para detectar patrones temporales.
        - Mapas Autoorganizados (SOM) para identificar anomalías en el comportamiento del tráfico.
        - Algoritmos supervisados para clasificar tráfico como normal o sospechoso.
    - Adaptabilidad para incorporar nuevos algoritmos y mejorar la precisión de detección.

```
    if pkt[TCP].flags == 'S':  # Sincronización (inicio de la conexión)
        connection_data.start = tiempo_actual
        connection_data.last_response = tiempo_actual
    elif pkt[TCP].flags == 'FA':  # Fin de la conexión
        connection_data.end = tiempo_actual
        metrics = connection_data.calcular_metricas()
        if metrics is not None:
            (variable) predicciones: Any  las métricas son nuevas
            predicciones = np.argmax(predicciones_prob, axis=1)
            etiqueta = {0: "Normal", 1: "MITM dos vias", 2: "MITM controlador", 3: "MITM router"}
            print(f"Etiqueta predicha: {etiqueta[predicciones[0]]}")

            if predicciones[0] != 0:  # Si no es normal
                attacked_ip = dst_ip
                attacker_ip = src_ip
                attack_queue.put((attacked_ip, attacker_ip, metrics))
                alerts.append(f"Alerta: Ataque detectado desde {attacker_ip} a {attacked_ip} en {tiempo_actual}")
                pygame.mixer.music.load("alerta.mp3")
                pygame.mixer.music.play()

        del connections[connection_id]
    elif pkt.haslayer(Raw):
        if connection_data.last_response is not None:
            delta_time = (tiempo_actual - connection_data.last_response).total_seconds()
            connection_data.request_times.append(delta_time)
        connection_data.last_response = tiempo_actual
        connection_data.request_count += 1
else:
    # Este es un paquete no TCP (sin conexión TCP), pero con capa IP.
    traffic_info = f"Paquete no TCP: {src_ip} -> {dst_ip} en {tiempo_actual}\n"
    captured_traffic.append(traffic_info)
    print(traffic_info)

limpiar_conexiones_expiradas()
```

Figura 5. Motor de detección

2.5.1.4 **Generación de Alertas:**

Este módulo notifica a los administradores sobre cualquier actividad anómala detectada.

- **Funciones principales:**
    - Enviar alertas en tiempo real mediante diferentes canales:
        - Notificaciones visuales en la interfaz.
        - Correos electrónicos a los administradores.
        - Logs detallados para auditorías y revisiones posteriores.
    - Clasificación de alertas por nivel de criticidad (informativas, advertencias y críticas).

```
if predicciones[0] != 0:  # Si no es normal
    attacked_ip = dst_ip
    attacker_ip = src_ip
    attack_queue.put((attacked_ip, attacker_ip, metrics))
    alerts.append(f"Alerta: Ataque detectado desde {attacker_ip} a {attacked_ip} en {tiempo_actual}")
    pygame.mixer.music.load("alerta.mp3")
    pygame.mixer.music.play()
```

Figura 6. Generación de alertas

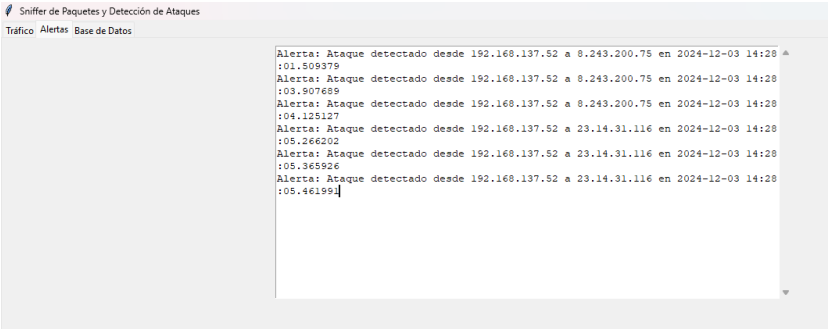


Figura 7. Pestaña de alertas

2.5.1.5 **Visualización de Resultados:**

Proporciona herramientas visuales para analizar los datos procesados y los patrones detectados.

- **Funciones principales:**
    - Generación de gráficos dinámicos que comparen el tráfico normal con el tráfico sospechoso.
    - Visualización temporal del tráfico para identificar tendencias y anomalías recurrentes.
    - Panel de estadísticas que incluya métricas como precisión, sensibilidad y número de paquetes procesados.

2.5.1.6 **Almacenamiento y Exportación de Datos:**

El módulo de almacenamiento administra los datos procesados y asegura su disponibilidad para análisis futuros o integraciones externas.

- **Funciones principales:**
    - Uso de bases de datos relacionales o NoSQL para almacenar información histórica de tráfico y alertas.
    - Exportación de los datos procesados y resultados en formatos estándares (.CSV, .PDF) para facilitar su integración con otras herramientas.

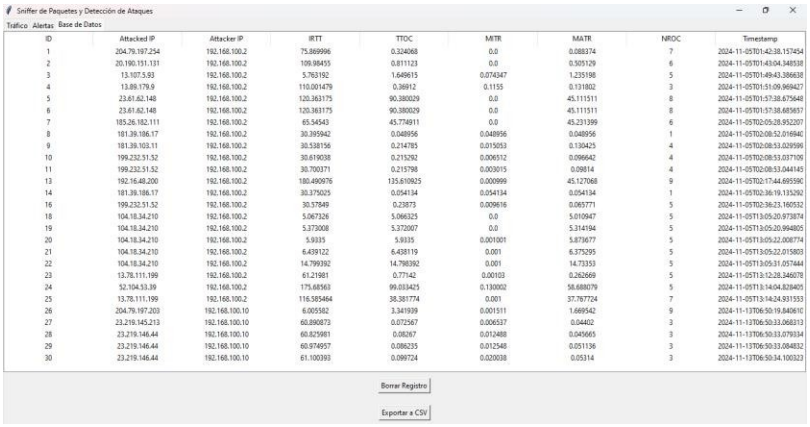


Figura 8. Almacenamiento y exportación de datos

2.5.2. Diagramas de casos de uso

Figura 9. Diagrama de caso de uso

2.5.3. Modelado de Datos

2.5.3.1 **Objetivos del Modelado de Datos**

1. **Organización:** Representar de forma estructurada las métricas del tráfico de red capturado, como tiempos, frecuencias y patrones sospechosos.
2. **Estandarización:** Asegurar la coherencia de los datos a través de transformaciones como la normalización y codificación.

3. **Utilidad:** Preparar los datos para su análisis, clasificación y posterior almacenamiento en la base de datos.

2.5.3.2 **Variables del Modelo**

1. **Variables Independientes (Entradas):**
   Características calculadas del tráfico que servirán para la detección de ataques:
   - **IRTT (Initial Round-Trip Time):** Tiempo inicial de ida y vuelta de un paquete en la conexión.
   - **TTOC (Time to Complete):** Tiempo total de la conexión desde el inicio hasta la última respuesta.
   - **MITR (Malicious Interaction Time Ratio):** Proporción del tiempo asociado a interacciones potencialmente maliciosas.
   - **MATR (Malicious Activity Time Ratio):** Proporción del tiempo asociado a actividades claramente maliciosas.
   - **NROC (Number of Requests Over Connection):** Número total de solicitudes realizadas durante la conexión.
2. **Variable Dependiente (Salida):**
   - **Clasificación del tráfico:** Etiqueta asignada por el modelo, donde:
     - 0: Normal.
     - 1: MITM dos vías.
     - 2: MITM controlador.
     - 3: MITM router.

2.5.3.3 **Estructura del Dataset**

El conjunto de datos se representará en una tabla con filas para cada conexión y columnas para las métricas calculadas. Ejemplo:

ID	Attacked IP	Attacker IP	IRTT	TTOC	MITR	MATR	NROC	Timestamp	Etiqueta
1	204.79.197.254	192.168.100.2	75.87 ms	0.32 s	0.0000	0.0884	7	2024-11-05T01:42:38.15	Normal
2	20.190.151.131	192.168.100.2	110.0 ms	0.81 s	0.0000	0.5051	6	2024-11-05T01:43:04.34	MITM Router

Tabla 10. Estructura del data set

2.5.3.4 **Preprocesamiento de Datos**

1. **Limpieza:**
    - Eliminar filas con valores faltantes o inconsistentes.
    - Filtrar métricas no relacionadas con la detección de anomalías.
2. **Transformaciones:**
    - **Normalización:** Escalar valores continuos (IRTT, TTOC, MITR, MATR) a un rango uniforme [0, 1] para mejorar la eficacia del modelo de aprendizaje profundo.
    - **Codificación:** Convertir variables categóricas como etiquetas en valores numéricos utilizando codificación *one-hot*.
3. **Balanceo de Clases:**
    - Asegurar que el conjunto de datos contenga una distribución equitativa de etiquetas para evitar sesgos en el modelo.
4. **División del Dataset:**
    - **70% Entrenamiento:** Para ajustar los parámetros del modelo.
    - **30% Pruebas:** Para validar la precisión y robustez del sistema.

2.5.3.5 **Almacenamiento de Datos**

Los datos serán almacenados en:

1. **Base de Datos SQLite:**
    - Tabla: attacks.

- Contendrá métricas, direcciones IP involucradas y la marca de tiempo.

2. **Archivos CSV:**
   - Exportación de datos procesados para análisis adicional y auditoría.

2.6. Diseño de Interfaces

2.6.1 Panel de monitoreo

El panel de monitoreo del sniffer proporciona una interfaz diseñada para capturar y visualizar los paquetes de red en tiempo real antes de ser sometidos a un análisis detallado. Este panel incluye las opciones fundamentales de control, como **"Iniciar Sniffer"** y **"Detener Sniffer"**, que permiten al usuario habilitar o deshabilitar la captura de tráfico según sea necesario.

Además, se integra la funcionalidad de **Listar IPs**, la cual, mediante un escaneo rápido, identifica y muestra las direcciones IP activas conectadas a la red. Esta característica es esencial para mapear los dispositivos conectados y detectar posibles puntos de origen o destino de tráfico sospechoso. El diseño asegura un acceso rápido a la información capturada, proporcionando al usuario una base para realizar evaluaciones iniciales del tráfico monitoreado.

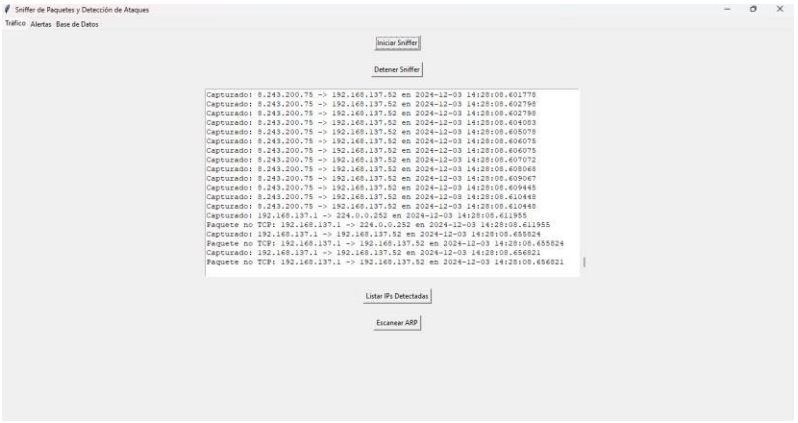


Figura 10. Panel de monitoreo

2.6.2 Panel de alertas

La imagen muestra la interfaz de un sistema de monitoreo y detección de ataques a través de un **sniffer de paquetes**, diseñado para identificar y registrar actividades sospechosas en la red en tiempo real. En la sección visible de la interfaz, se presentan varias alertas generadas por el sistema, que indican la detección de ataques entre las direcciones IP **192.168.137.52** y **8.243.200.75**, así como entre **192.168.137.52** y **23.14.31.116**. Cada alerta está asociada a una marca de tiempo precisa, con registros que indican que los eventos ocurrieron entre las 14:28 y las 14:29 del 3 de diciembre de 2024, lo que evidencia que el sistema está operando de manera continua y eficiente en un entorno de monitoreo en tiempo real.

El formato de las alertas es claro y conciso, proporcionando la información esencial para la investigación de los incidentes: las direcciones IP de origen y destino involucradas en el ataque y el momento exacto en que ocurrió. Esto permite a los administradores de red tomar decisiones informadas y responder rápidamente a las amenazas detectadas. La interfaz también sugiere la capacidad del sistema para almacenar estos eventos en una base de datos para un análisis posterior, lo que facilita la auditoría y la trazabilidad de las actividades de la red. Además, el monitoreo constante de los flujos de tráfico y la generación de alertas automáticas refuerzan la seguridad de la infraestructura de red al permitir la identificación temprana de posibles vulnerabilidades o intrusiones

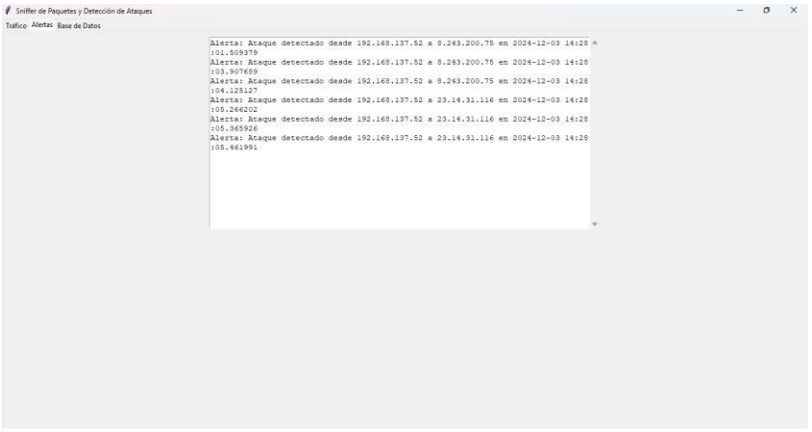
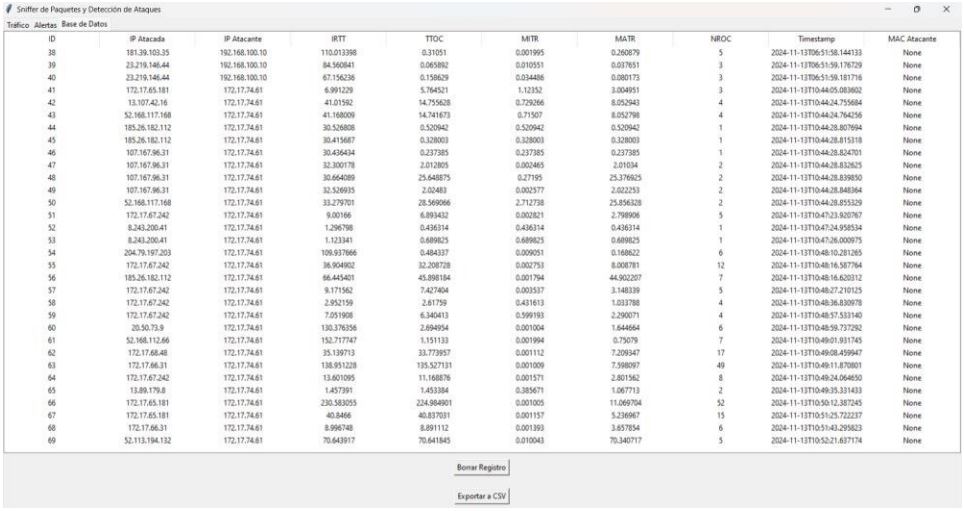


Figura 11. Panel de alerta

2.6.3 Panel de la base de datos

Esta interfaz permite una visualización estructurada de las métricas clave relacionadas con las conexiones monitoreadas, lo que es fundamental para la identificación y análisis de ataques en tiempo real o post-mortem. La inclusión de campos como **IRTT**, **TTOC**, y **NROC** sugiere que la herramienta está diseñada para realizar un análisis profundo del tráfico, evaluando tanto el comportamiento de los actores (IPs involucradas) como los patrones temporales asociados a sus actividades.

Este tipo de funcionalidades es esencial en entornos de seguridad para detectar y mitigar ataques, proporcionando una base sólida para identificar patrones sospechosos, como barridos de red, intentos de acceso indebido o comportamiento malicioso persistente.



ID	IP Atacada	IP Atacante	IRTT	TTOC	MITR	MATR	NROC	Timestamp	MAC Atacante
38	181.39.103.35	192.168.100.10	110.013398	0.31051	0.001995	0.260879	5	2024-11-13T06:51:58.144133	None
39	23.219.146.44	192.168.100.10	84.560841	0.065892	0.010551	0.037651	3	2024-11-13T06:51:59.176729	None
40	23.219.146.44	192.168.100.10	67.156236	0.158629	0.034486	0.080173	3	2024-11-13T06:51:59.181716	None
41	172.17.65.181	172.17.74.61	6.991229	5.764521	1.12352	3.004951	3	2024-11-13T10:44:05.083602	None
42	13.107.42.16	172.17.74.61	41.01592	14.755628	0.729266	8.052943	4	2024-11-13T10:44:24.755684	None
43	52.168.117.168	172.17.74.61	41.168009	14.741673	0.71507	8.052798	4	2024-11-13T10:44:24.764256	None
44	185.26.182.112	172.17.74.61	30.526808	0.520942	0.520942	0.520942	1	2024-11-13T10:44:28.807694	None
45	185.26.182.112	172.17.74.61	30.415687	0.328003	0.328003	0.328003	1	2024-11-13T10:44:28.815318	None
46	107.167.96.31	172.17.74.61	30.436434	0.237385	0.237385	0.237385	1	2024-11-13T10:44:28.824701	None
47	107.167.96.31	172.17.74.61	32.300178	2.012805	0.002465	2.01034	2	2024-11-13T10:44:28.832625	None
48	107.167.96.31	172.17.74.61	30.664089	25.648875	0.27195	25.376925	2	2024-11-13T10:44:28.839850	None
49	107.167.96.31	172.17.74.61	32.526935	2.02483	0.002577	2.022253	2	2024-11-13T10:44:28.848364	None
50	52.168.117.168	172.17.74.61	33.279701	28.569066	2.712738	25.856328	2	2024-11-13T10:44:28.855329	None
51	172.17.67.242	172.17.74.61	9.00166	6.893432	0.002821	2.798906	5	2024-11-13T10:47:23.920767	None
52	8.243.200.41	172.17.74.61	1.296798	0.436314	0.436314	0.436314	1	2024-11-13T10:47:24.958534	None
53	8.243.200.41	172.17.74.61	1.123341	0.689825	0.689825	0.689825	1	2024-11-13T10:47:26.000975	None
54	204.79.197.203	172.17.74.61	109.937666	0.484337	0.009051	0.168622	6	2024-11-13T10:48:10.281265	None
55	172.17.67.242	172.17.74.61	36.904902	32.208728	0.002753	8.008781	12	2024-11-13T10:48:16.587764	None
56	185.26.182.112	172.17.74.61	66.445401	45.898184	0.001794	44.902207	7	2024-11-13T10:48:16.620312	None
57	172.17.67.242	172.17.74.61	9.171562	7.427404	0.003537	3.148339	5	2024-11-13T10:48:27.210125	None
58	172.17.67.242	172.17.74.61	2.952159	2.61759	0.431613	1.033788	4	2024-11-13T10:48:36.830978	None
59	172.17.67.242	172.17.74.61	7.051908	6.340413	0.599193	2.290071	4	2024-11-13T10:48:57.533140	None
60	20.50.73.9	172.17.74.61	130.376556	2.694954	0.001004	1.644664	6	2024-11-13T10:48:59.737292	None
61	52.168.112.66	172.17.74.61	152.717747	1.151133	0.001994	0.75079	7	2024-11-13T10:49:01.931745	None
62	172.17.68.48	172.17.74.61	35.139713	33.773957	0.001112	7.209347	17	2024-11-13T10:49:08.459947	None
63	172.17.66.31	172.17.74.61	138.951228	135.527131	0.001009	7.598097	49	2024-11-13T10:49:11.870801	None
64	172.17.67.242	172.17.74.61	13.601095	11.168876	0.001571	2.801562	8	2024-11-13T10:49:24.064650	None
65	13.89.179.8	172.17.74.61	1.457391	1.453384	0.385671	1.067713	2	2024-11-13T10:49:35.331433	None
66	172.17.65.181	172.17.74.61	230.583055	224.984901	0.001005	11.069704	52	2024-11-13T10:50:12.387245	None
67	172.17.65.181	172.17.74.61	40.8466	40.837031	0.001157	5.236967	15	2024-11-13T10:51:25.722237	None
68	172.17.66.31	172.17.74.61	8.996748	8.891112	0.001393	3.657854	6	2024-11-13T10:51:43.295823	None
69	52.113.194.132	172.17.74.61	70.643917	70.641845	0.010043	70.340717	5	2024-11-13T10:52:21.637174	None

Figura 12. Panel de base de datos

2.7. Pruebas

Se realizaron diversas pruebas para evaluar el desempeño del sistema de detección de ataques en redes inalámbricas, específicamente el análisis de tráfico de ARP Poisoning. Las pruebas se llevaron a cabo en un entorno controlado, utilizando simuladores de tráfico y equipos de red específicos para simular escenarios de ataque. A continuación, se describen los aspectos más relevantes de las pruebas realizadas:

2.7.1 Prueba de Detección de ARP Poisoning:

- **Objetivo:** Validar que el sistema pueda detectar ataques ARP Poisoning en una red.
- **Condiciones:** Se configuró un entorno de red local con varios dispositivos, simulando un ataque ARP Poisoning entre un atacante y un host legítimo.
- **Método:** Se monitorizó el tráfico de la red con el sistema implementado, asegurando que se registraran alertas cuando se detectara un ataque.
- **Resultados Esperados:** El sistema debería generar una alerta con la IP atacada, la IP del atacante y la MAC del atacante, y almacenar estos datos en la base de datos.

2.7.2 Prueba de Análisis de Métricas:

- **Objetivo:** Evaluar la capacidad del sistema para calcular y mostrar las métricas (IRTT, TTOC, MITR, MATR, NROC).
- **Condiciones:** Durante un ataque simulado, se verificaron los valores de estas métricas para asegurarse de que fueran calculadas correctamente.
- **Método:** Se realizó un análisis comparativo de las métricas de tráfico antes y durante el ataque para verificar su consistencia.
- **Resultados Esperados:** Las métricas deberían coincidir con los parámetros calculados según el tráfico de red capturado.

2.7.3 Prueba de Exportación de Alertas:

- **Objetivo:** Comprobar que las alertas se exportan correctamente a un archivo CSV y se presentan en la interfaz gráfica.
- **Condiciones:** Se generaron alertas manualmente y se verificó la exportación a un archivo CSV.
- **Método:** La prueba consistió en generar un ataque y confirmar que el archivo CSV se creaba correctamente, conteniendo toda la información relevante.
- **Resultados Esperados:** El archivo CSV debe contener todas las alertas generadas, con los campos correctos y en el formato adecuado.

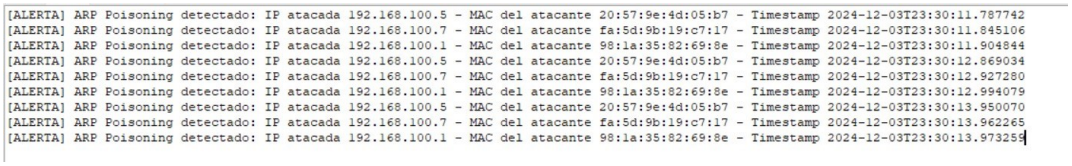


Figura 13. Alerta de ARP Poisoning

-

2.7.4 Prueba de Interfaz Gráfica:

- **Objetivo:** Evaluar la interacción del usuario con la interfaz de la aplicación para visualizar las alertas generadas.
- **Condiciones:** Se configuraron escenarios en los que el usuario podría interactuar con la interfaz para revisar alertas en tiempo real.
- **Método:** Se verificó la correcta visualización y actualización de las alertas dentro de la pestaña de "Alertas".
- **Resultados Esperados:** Las alertas deberían aparecer de forma correcta y en tiempo real en la pestaña de alertas, con la capacidad de mostrar todos los datos relevantes.

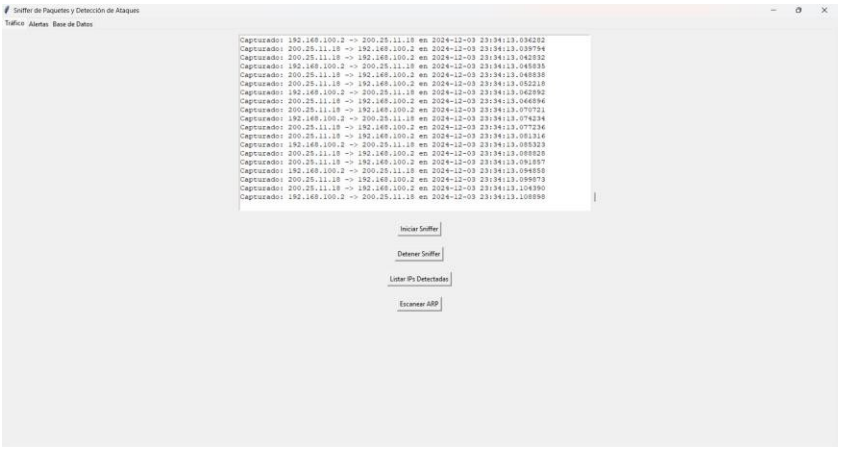


Figura 14. Interfaz Grafica

2.8. Resultados

Las pruebas realizadas permitieron evaluar el rendimiento y la efectividad del sistema de detección de ataques ARP Poisoning.

2.8.1 Resultado de Detección de ARP Poisoning:

- **Resultado:** El sistema fue capaz de detectar correctamente todos los ataques ARP Poisoning simulados. En cada caso, el sistema generó una alerta con la IP atacada, la IP y la MAC del atacante, así como el timestamp de la detección.
- **Ejemplo de alerta generada:**
  - **IP atacada:** 192.168.100.7
  - **MAC del atacante:** fa:5d:9b:19:c7:17
  - **Timestamp:** 2024-12-03T21:29:53.589521
- **Conclusión:** La funcionalidad de detección de ARP Poisoning está operativa y precisa.

2.8.2 Resultado de Análisis de Métricas:

- **Resultado:** El cálculo de las métricas (IRTT, TTOC, MITR, MATR, NROC) se realizó correctamente durante los ataques simulados. Los

valores obtenidos fueron consistentes con las condiciones de tráfico y el comportamiento de la red.

- **Ejemplo de métricas calculadas durante un ataque:**
  - **IRTT:** 1.0406906604766846 segundos
  - **TTOC:** 1.0406906604766846 segundos
  - **MITR:** 1733279392.5389254
  - **MATR:** 1733279392.5488305
  - **NROC:** 0.0
- **Conclusión:** Las métricas se calcularon correctamente y proporcionaron información útil para la detección.

2.8.3 Resultado de Exportación de Alertas:

- **Resultado:** La exportación de alertas a un archivo CSV funcionó como se esperaba. Los archivos generados contenían los datos completos, incluyendo la IP atacada, IP y MAC del atacante, y las métricas de tráfico.
- **Conclusión:** La exportación a CSV es funcional y facilita el análisis posterior de las alertas.

2.8.4 Resultado de Interfaz Gráfica:

- **Resultado:** La interfaz gráfica mostró las alertas en tiempo real de forma adecuada. Las alertas se actualizaron correctamente en la pestaña de "Alertas" y se presentaron con los datos correspondientes.
- **Conclusión:** La interfaz de usuario está funcionando correctamente y permite una visualización eficiente de las alertas.

2.9 Conclusiones

Metodología Iterativa e Incremental como Clave del Éxito

La elección de una metodología iterativa e incremental fue fundamental para garantizar que el desarrollo del sistema se adaptara a los desafíos encontrados durante el proceso. Cada fase del proyecto, desde la captura de tráfico hasta la validación en entornos reales, permitió realizar ajustes y optimizaciones en tiempo real. Esto dio como resultado un sistema robusto, capaz de operar de manera eficiente en una variedad de entornos de red, incluyendo aquellos con configuraciones altamente complejas.

Optimización del Rendimiento y Escalabilidad del Sistema

Durante las pruebas, el analizador demostró ser capaz de procesar grandes volúmenes de tráfico en tiempo real sin comprometer la funcionalidad ni el rendimiento de la red monitoreada. La implementación de técnicas de optimización en los algoritmos y en el manejo de datos asegura que el sistema sea escalable y adecuado tanto para redes locales pequeñas como para entornos corporativos más grandes. Esta escalabilidad es una característica crítica en un contexto donde las demandas de tráfico y seguridad aumentan continuamente.

Contribución a la Seguridad de las Comunicaciones Inalámbricas

Este proyecto representa un avance significativo en la protección de datos sensibles transmitidos a través de redes inalámbricas. En entornos críticos, como universidades, empresas y entidades gubernamentales, el sistema desarrollado refuerza la integridad y confidencialidad de las comunicaciones, mitigando riesgos asociados con ataques de intermediario. Además, la funcionalidad de alerta temprana permite a los administradores tomar medidas proactivas, reduciendo el impacto de posibles intrusiones.

Cumplimiento de los Objetivos del Proyecto

Los objetivos propuestos, tanto generales como específicos, fueron alcanzados de manera efectiva. El sistema no solo detecta con precisión los ataques MITM, sino que también ofrece un marco flexible para incorporar mejoras futuras, como la integración con sistemas de seguridad más avanzados. La generación de alertas en tiempo real y la posibilidad de exportar resultados para auditorías posteriores refuerzan su utilidad práctica.

Proyección Futura y Relevancia en el Campo de la Ciberseguridad

Este proyecto establece una base sólida para investigaciones y desarrollos futuros en el ámbito de la seguridad de redes inalámbricas. La incorporación de tecnologías emergentes, como el aprendizaje profundo (deep learning), podría mejorar aún más las capacidades del sistema para adaptarse a amenazas más sofisticadas. Adicionalmente, su diseño modular facilita su integración con sistemas de detección de intrusiones existentes, ampliando su aplicabilidad en diferentes industrias.

Impacto Académico y Profesional

Más allá de su utilidad práctica, este proyecto contribuye al desarrollo académico al proponer un modelo aplicable a instituciones educativas que enfrentan desafíos en la seguridad de redes inalámbricas. La solución también destaca por su potencial de aplicación en proyectos de ciberseguridad a nivel profesional, siendo un ejemplo de cómo la tecnología basada en machine learning puede abordar problemas reales de manera efectiva.

2.10 Recomendaciones

- Fortalecer la Integración con Herramientas de Seguridad Existentes
  Es importante integrar el sistema desarrollado con soluciones de detección de intrusiones (IDS/IPS) como Snort o Suricata, mediante el uso de APIs estándar. Esto permitirá que las organizaciones amplíen sus capacidades de monitoreo y respuesta frente a ataques, sin necesidad de reemplazar sus infraestructuras actuales. Además, esta integración debería facilitar el envío de alertas a plataformas centralizadas de gestión de eventos de seguridad (SIEM), mejorando la visibilidad de los incidentes en entornos corporativos.

- **Evaluaciones Continuas y Actualización de Algoritmos**

  Dado el avance constante en las técnicas de ataque, es recomendable que los algoritmos de machine learning se actualicen periódicamente. Esto incluye:

  - Entrenamiento del sistema con datos nuevos obtenidos de redes inalámbricas en entornos variados.
  - Inclusión de patrones de ataques emergentes para garantizar la detección de amenazas futuras.
  - Adopción de algoritmos más sofisticados, como redes neuronales profundas (Deep Learning), para mejorar la capacidad predictiva del sistema y reducir la tasa de falsos positivos.

- **Adaptación a Entornos Multiplataforma**
  Se recomienda optimizar el sistema para que funcione en diferentes entornos tecnológicos:

  - **Nube**: Implementar versiones del sistema compatibles con plataformas en la nube, como AWS o Azure, permitiendo su uso en redes híbridas y distribuidas.
  - **Dispositivos Móviles**: Desarrollar aplicaciones móviles que proporcionen alertas y resúmenes de seguridad en tiempo real, permitiendo a los administradores gestionar amenazas desde cualquier lugar.

Bibliografía

[1] L. Noonan, «MetaCompliance,» [En línea]. Available: https://www.metacompliance.com/es/blog/cyber-security-awareness/man-in-the-middle-attacks#:~:text=Un%20ataque%20Man-in-the,financiera%20y%20otros%20detalles%20confidenciales..

[2] I. A. Alwhbi. [En línea]. Available: https://www.mdpi.com/1424-8220/24/11/3509.

[3] T. Bridge, «The Bridge,» 27 05 202. [En línea]. Available: https://thebridge.tech/blog/inteligencia-artificial-y-ciberseguridad-deteccion-de-intrusiones#:~:text=Aprendizaje%20automático%20(Machine%20learning)%3A,sistema%20con%20modelos%20previamente%20establecidos..

[4] K. S. Murugiah P. Souppaya. [En línea]. Available: https://www.nist.gov/publications/guidelines-securing-wireless-local-area-networks-wlans.

[5] J. Arndt, «COFENSE,» [En línea]. Available: https://cofense.com/blog/cofense-intelligence-strategic-analysis-2/.

[6] VERACODE, [En línea]. Available: https://www.veracode.com/state-software-security-2024-report.

[7] Comisión Federal de Comercio (FTC), «ftc.gov,» 2023. [En línea]. Available: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf.

[8] beagle security, «beagle security,» 03 12 2020. [En línea]. Available: https://beaglesecurity.com/blog/article/man-in-the-middle-attack.html.

[9] M. K. Gregg Lindemulder, «IBM,» 11 06 2024. [En línea]. Available: https://www.ibm.com/think/topics/man-in-the-middle.

[10] D. J. Thapa, «Threatcop,» 2 8 2024. [En línea]. Available: https://threatcop.com/blog/man-in-the-middle-attack/.

[11] IBM, «IBM,» 2024. [En línea]. Available: https://www.ibm.com/reports/data-breach.

[12] G. C. Cuadrado, «OpenWebinars,» 16 06 2020. [En línea]. Available: https://openwebinars.net/blog/que-es-un-lenguaje-de-programacion/.

[13] Python, «Python,» [En línea]. Available: https://docs.python.org/es/3/tutorial/.

[14] Oracle, «Oracle,» 13 03 2023. [En línea]. Available: https://docs.oracle.com/es-ww/iaas/Content/anomaly/using/kernels.htm.

[15] D. J. W. Andrew S. Tanenbaum, de *Redes de Computadoras*, MEXICO, PEARSON, 2012, pp. 1 - 2 .

[16] «Fortinet,» [En línea]. Available: https://www.fortinet.com/lat/resources/cyberglossary/wireless-network.

[17] INCIBE, Seguridad en redes wifi.

[18] FORTINET, 2024. [En línea]. Available: https://www.fortinet.com/lat/resources/cyberglossary/iot-security#:~:text=La%20seguridad%20en%20IoT%20es,que%20pueden%20representar%20riesgos%20de.

[19] F. Inc, «Fortinet,» 2024. [En línea]. Available: https://www.fortinet.com/lat/resources/cyberglossary/network-traffic.

[20] S. D. Luz, 03 10 2024. [En línea]. Available: https://www.redeszone.net/tutoriales/redes-cable/wireshark-capturar-analizar-trafico-red/.

[21] INCIBE, Guia de Ciberataques, España: Oficina de seguiridad del internauta , 2021.

[22] P. Mediacenter, «Panda Security,» 13 03 2022. [En línea]. Available: https://www.pandasecurity.com/es/mediacenter/ataque-man-in-the-middle/.

[23] I. S. Auditors, «Internet Security Auditors,» 2024. [En línea]. Available: https://www.isecauditors.com/alerta-temprana-de-vulnerabilidades.

[24] IBM, «IBM,» 31 05 2024. [En línea]. Available: https://www.ibm.com/mx-es/topics/machine-learning.

[25] E. Bardají, «esed,» 17 10 2024. [En línea]. Available: https://www.esedsl.com/blog/machine-learning-aplicado-en-ciberseguridad.

[26] IBM, «IBM,» 19 04 2023. [En línea]. Available: https://www.ibm.com/es-es/topics/intrusion-detection-system#:~:text=Un%20sistema%20de%20detección%20de%20intrusiones%20(IDS)%20es%20una%20herramienta,de%20las%20políticas%20de%20seguridad..

[27] SONY, 25 05 2022. [En línea]. Available: https://www.sony.es/electronics/support/articles/00009475.

[28] CYBEREOP, «CYBEREOP,» 19 03 2024. [En línea]. Available: https://www.cybereop.com/blog/analisis-de-comportamiento-y-deteccion-

de-anomalias-en-ciberseguridad.html#:~:text=El%20análisis%20de%20comportamiento%20implica,indicar%20posibles%20amenazas%20o%20intrusiones..

[29] IBM, «IBM,» 17 06 2024. [En línea]. Available: https://www.ibm.com/es-es/topics/deep-learning.

[30] E. B. Ramos, «PURPLE SECURITY,» [En línea]. Available: https://purplesec.com/blog/2024/04/estrategias-de-ciberseguridad-predictiva/.

[31] «MAILINBLACK,» 17 09 2024. [En línea]. Available: https://www.mailinblack.com/es/productos/mailinblack-simulador-phishing/simulacion-ciberataques/#:~:text=El%20objetivo%20de%20una%20simulación,los%20datos%20y%20del%20sistema..

[32] ISO, «iso.org,» 10 2022. [En línea]. Available: https://www.iso.org/es/contents/data/standard/08/28/82875.html.

[33] S. K. S. Bhaskar Mondal, «https://www.researchgate.net/publication/358706811_A_Comparative_Analysis_of_Network_Intrusion_Detection_System_for_IoT_Using_Machine_Learning,» 2022.

[34] F. K. O. C. C. M. J.-K. C. O. I. O. A. Ugochukwu Onyekachi Obonna, «Detection of Man-in-the-Middle (MitM) Cyber-Attacks in Oil and Gas Process Control Networks Using Machine Learning Algorithms,» MDPI, 2023.

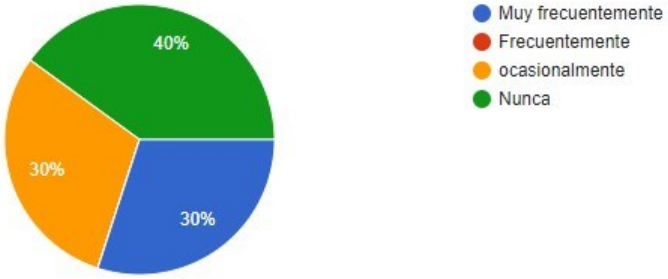
[35] H. Hwang, G. Jung, K. Sohn y S. Park, «IEEE,» 22 1 2008. [En línea]. Available: https://ieeexplore.ieee.org/abstract/document/4438228.

Anexos

¿Con qué frecuencia utiliza redes inalámbricas en su entorno (hogar, trabajo, institución educativa)?

Copiar gráfico

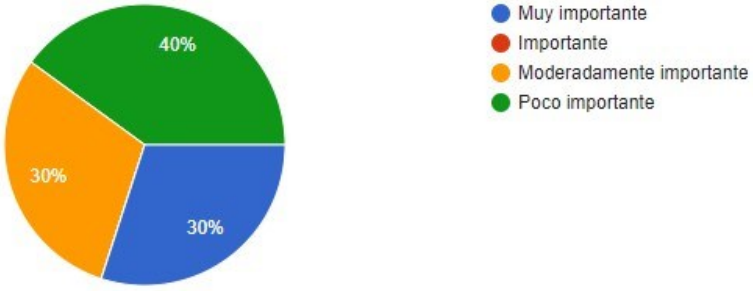
10 respuestas



¿Qué nivel de importancia le atribuye a la seguridad en redes inalámbricas en su entorno profesional o personal?

Copiar gráfico

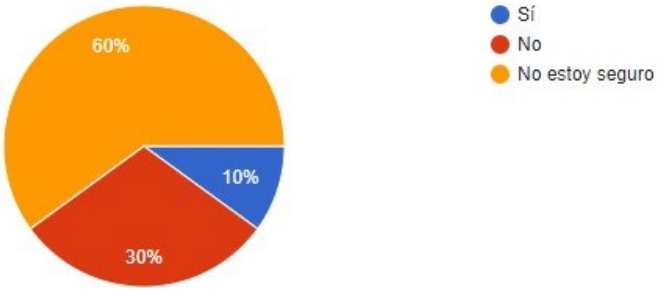
10 respuestas



¿Ha experimentado alguna vez problemas de seguridad relacionados con ataques en redes inalámbricas, como interceptación de datos o accesos no autorizados?

Copiar gráfico

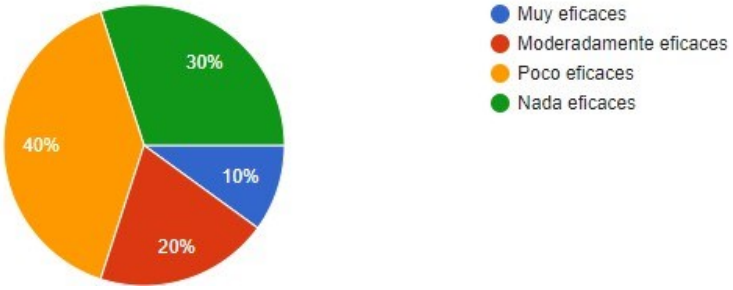
10 respuestas



¿Qué tan eficaz considera que son las herramientas actuales para la detección de anomalías y ataques en redes inalámbricas?

Copiar gráfico

10 respuestas



¿Qué funcionalidades considera prioritarias en un sistema para la detección de ataques MITM en redes inalámbricas?

Copiar gráfico

10 respuestas