UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

USO DE SOFTWARE LIBRE Y MACHINE LEARNING PARA MEJORAR LA DETECCIÓN DE INTRUSOS EN UNA RED

AUTOR

Carrizo Garcia, Luis Eduardo

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR

Álvarez Galarza, María Daniela

Santa Elena, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Firmado electrónicamente por:
MARIA DANIELA ALVAREZ GALARZA

Ing. María Daniela Álvarez Galarza, Mgtr.
TUTOR

Firmado electrónicamente por:
JAIME BENJAMIN OROZCO IGUASNIA

Ing. Jaime Benjamín Orozco Iguasnia, Mgtr.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
EDISSON POMPILIO QUINTUNA PADILLA

Ing. Edisson Pompilio Quintuña Padilla, Mgtr.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, MSc.
SECRETARIA GENERAL
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

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 Luis Eduardo Carrizo Garcia, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Firmado electrónicamente por:
MARIA DANIELA ALVAREZ GALARZA

María Daniela Álvarez Galarza

Santa Elena, 21 de octubre de 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **LUIS EDUARDO CARRIZO GARCIA**

DECLARO QUE:

El trabajo de Titulación, USO DE SOFTWARE LIBRE Y MACHINE LEARNING PARA MEJORAR LA DETECCIÓN DE INTRUSOS EN UNA RED previo a la obtención del título en Magíster en Ciberseguridad, 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.

Santa Elena, 21 de octubre de 2024

EL AUTOR

Firmado electrónicamente por:
LUIS EDUARDO
CARRIZO GARCIA

Luis Eduardo Carrizo Garcia

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **LUIS EDUARDO CARRIZO GARCIA**

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, 21 de octubre de 2024

EL AUTOR

Firmado electrónicamente por:
LUIS EDUARDO CARRIZO GARCIA

Luis Eduardo Carrizo Garcia

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TEMA

Autor: Luis Eduardo Carrizo Garcia

Tutora: María Daniela Álvarez Galarza

RESUMEN

Este estudio integra técnicas de Machine Learning (ML) con el sistema de detección de intrusiones Snort para mejorar la identificación de ataques DDoS. El objetivo es reducir los falsos positivos y aumentar la precisión en la detección de amenazas en redes complejas. El método consistió en entrenar un modelo Random Forest utilizando el dataset CICIDS2017 y luego implementarlo junto a Snort en un entorno de red controlado. Los resultados mostraron un aumento en la precisión del 52.8% al 70.71%, y en la exactitud del 50.8% al 65.68%, con un incremento del F1-Score de 64.5% a 78.42%. Estos hallazgos demuestran que la integración de ML con Snort mejora significativamente la capacidad de detección y mitigación de incidentes en tiempo real. Se recomienda investigar el uso de otros algoritmos de ML y probar en diferentes escenarios para continuar optimizando el sistema.

Palabras clave: machine learning, detección de intrusiones, Snort, DDoS, ciberseguridad

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TOPIC: USE OF OPEN SOURCE SOFTWARE AND MACHINE LEARNING TO IMPROVE INTRUSION DETECTION IN A NETWORK

Author: Luis Eduardo Carrizo Garcia

Tutora: María Daniela Álvarez Galarza

ABSTRACT

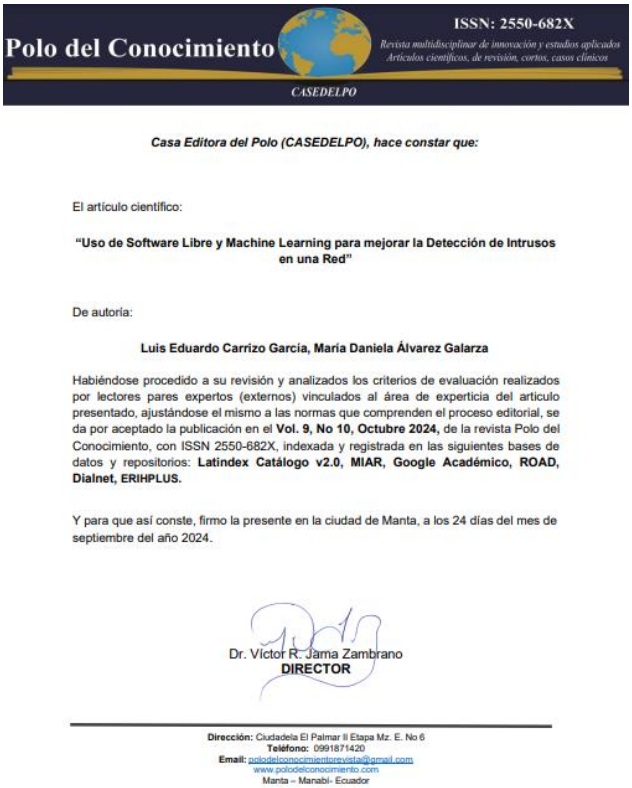
This study integrates Machine Learning (ML) techniques with the Snort intrusion detection system to improve the detection of DDoS attacks. The objective is to reduce false positives and increase detection accuracy in complex network environments. The method involved training a Random Forest model using the CICIDS2017 dataset and implementing it alongside Snort in a controlled network environment. Results showed an increase in precision from 52.8% to 70.71% and accuracy from 50.8% to 65.68%, with an improvement in the F1-Score from 64.5% to 78.42%. These findings demonstrate that the integration of ML with Snort significantly enhances the detection and mitigation capabilities of real-time incidents. It is recommended to explore the use of other ML algorithms and test in different scenarios to further optimize the system.

Keywords: machine learning, intrusion detection, Snort, DDoS, cybersecurity

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

USO DE SOFTWARE LIBRE Y MACHINE LEARNING PARA MEJORAR LA DETECCIÓN DE INTRUSOS EN UNA RED

CERTIFICADO DE ACEPTACIÓN PARA PUBLICACIÓN



Polo del Conocimiento

ISSN: 2550-682X

Revista multidisciplinar de innovación y estudios aplicados
Artículos científicos, de revisión, cortos, casos clínicos

CASEDELPO

Casa Editora del Polo (CASEDELPO), hace constar que:

El artículo científico:

"Uso de Software Libre y Machine Learning para mejorar la Detección de Intrusos en una Red"

De autoría:

Luis Eduardo Carrizo García, María Daniela Álvarez Galarza

Habiéndose procedido a su revisión y analizados los criterios de evaluación realizados por lectores pares expertos (externos) vinculados al área de experticia del artículo presentado, ajustándose el mismo a las normas que comprenden el proceso editorial, se da por aceptado la publicación en el **Vol. 9, No 10, Octubre 2024,** de la revista Polo del Conocimiento, con ISSN 2550-682X, indexada y registrada en las siguientes bases de datos y repositorios: **Latindex Catálogo v2.0, MIAR, Google Académico, ROAD, Dialnet, ERIHPLUS.**

Y para que así conste, firmo la presente en la ciudad de Manta, a los 24 días del mes de septiembre del año 2024.

Dr. Víctor R. Jama Zambrano
DIRECTOR

Dirección: Ciudadela El Palmar II Etapa Mz. E. No 6
Teléfono: 0991871420
Email: polodelconocimientorevista@gmail.com
www.polodelconocimiento.com
Manta – Manabí- Ecuador

Nombre de la revista	POLO DEL CONOCIMIENTO Latindex, catálogo 2.0 https://polodelconocimiento.com/ojs/index.php/es/issue/view/126