Anomalías en Redes Informáticas

Mayta Quispe Azael Jholyem, Mamani Mamani Miriam, Mamani Charca Lady Patricia

amaytaq@est.unap.edu.pe, *mirmamanimam@est.unap.edu.pe*, *lamamanich@est.unap.edu.pe*

***Resumen*— Junto al crecimiento exponencial de las redes informáticas y las aplicaciones de red en todo el mundo, han aumentado también los ciberataques. Por esta razón, se crearon conjuntos de datos cómo CSE-CIC-IDS2018, este conjunto fue creado en el 2018 por el Instituto Canadiense de Ciberseguridad (CIC) en AWS (*Amazon Web Services*) para brindar la posibilidad de desarrollar modelos predictivos para la detección de intrusiones y anomalías basadas en la red a través de varios enfoques de aprendizaje automático.**

Una detección temprana de intrusiones basado en anomalías de la red se vuelve muy importante para la protección de redes informáticas y en conjunto con el desarrollo del aprendizaje automático y su capacidad para extraer características de alto nivel con alta precisión, la detección de anomalías tiene gran oportunidad para evitar ataques maliciosos a las redes informáticas.

En nuestro trabajo describimos brevemente el conjunto de datos de intrusión CSE-CIC-IDS2018, el cual fue previamente analizado y posteriormente fue utilizado para entrenar un modelo de detección de intrusiones en la red basado en aprendizaje automático.

Palabras clave: Detección de intrusiones, intrusiones en redes, aprendizaje automático, CSE-CIC-IDS2018.

***Abstract*-- Along with the exponential growth of computer networks and network applications around the world, cyberattacks have also increased. For this reason, data sets such as CSE-CIC-IDS2018 were created, this set was created in 2018 by the Canadian Institute of Cybersecurity (CIC) on AWS (*Amazon Web Services)* to provide the possibility of developing predictive models for detection of network-based intrusions and anomalies through various machine learning approaches.**

An early intrusion detection based on network anomalies becomes very important for the protection of computer networks and in conjunction with the development of machine learning and its ability to extract high-level features with high precision, anomaly detection has great opportunity to prevent malicious attacks on computer networks.

In our work we briefly describe the CSE-CIC-IDS2018 intrusion data set, which was previously analyzed and later used to train a network intrusion detection model based on machine learning.

Keywords: Intrusion detection, network intrusions, machine learning, CSE-CIC-IDS2018.

Glosario:

IDS (Intrusion Detection System o Sistema de Detección de Intrusiones).
NDIS (Network Intrusion Detection System o Sistema de Detección de Intrusiones en Redes).
SQL (Structured Query Language o Lenguaje de consultas estructuradas)
DoS (Denial of Service o Denegación de servicio)
DDoS (Distributed Denial of Service o Denegación de servicio distribuida)

Universidad Nacional del Altiplano -Puno

Introducción

El crecimiento de las redes informáticas ha abierto a los usuarios una nueva serie de posibilidades; sin embargo, éstas traen consigo toda una serie de nuevos y, en ocasiones, complejos tipos de ataques o intrusiones en este entorno. Dichos ataques pueden ser caracterizados como anomalías en el comportamiento usual del flujo de datos de una red de comunicaciones.

El objetivo de la detección de intrusiones en la red es identificar y monitorear actividades maliciosas, esto es posible mediante un sistema de detección de intrusiones en la red (NIDS), este tiene un papel fundamental en la resolución de los desafíos de seguridad, ya que puede monitorear el tráfico de la red para detectar cualquier actividad sospechosa y tras analizar la información del tráfico es posible detectar brechas de seguridad, que comprenden intrusiones y anomalías.

Las técnicas basadas en inteligencia artificial (IA) tienen una ventaja para resolver los problemas de detección de anomalías y para el desarrollo de NIDS. En este trabajo propusimos un enfoque de aprendizaje automático con Regresión Logística al conjunto de datos cibernéticos CSE-CIC-IDS2018 que incluye siete tipos ataques, junto con flujos etiquetados que cubren más de 80 características.

I. Estado del arte

En la investigación de [1] González Peralta, titulada “El análisis de anomalías detectadas en las pruebas de software: una vía para mejorar el ciclo de vida” realizada por Ramón E. González P. nos muestra un aspecto de mejora continua al proceso de prueba a los requisitos, que consiste en la aplicación de un procedimiento para el análisis y clasificación de las anomalías detectadas, según la naturaleza del error, para identificar los principales problemas cometidos por los desarrolladores e identificar medidas correctivas, contribuyendo, como lo muestran los resultados de esta investigación, a “mejorar” el ciclo de vida.

Rivero Pérez [2] en su investigación titulada “Técnicas de aprendizaje automático para la detección de intrusos en redes de computadoras” realizada por Jorge Luis R. donde nos muestra el desarrollo de sistemas de detección de intrusos en redes de computadoras, constituye un reto para los investigadores, debido a que, con el crecimiento de las redes de computadoras, aparecen, constantemente nuevos ataques basados en contenido. Se describe la taxonomía de los NIDS y un esquema de clasificación de atributos de conexiones. En la detección de anomalías a partir de técnicas de aprendizaje automático varios son los conjuntos de datos empleados, siendo KDD Cup 99 el más utilizado. Atendiendo a esto se describe ese conjunto de datos y se exponen resultados obtenidos sobre el mismo a partir de algunas técnicas de preprocesamiento de datos como selección y discretización. Son expuestos novedosos enfoques que hibridan algoritmos de búsqueda basados en inteligencia de enjambre con algoritmos de aprendizaje automático, lo que posibilita elevar los índices de detección y mejoran la detección de ataques basados en contenido.

Noblejas Sampedro [3] En la investigación titulada “Estudio de algoritmos de detección de anomalías y su aplicación a entornos de ciberseguridad” realizada por Raquel N. busca encontrar un modelo general que englobe todos los posibles casos de entradas no deseadas al sistema y que sea capaz de aprender para detectar intrusiones futuras. Por lo cual estudia la relevancia de las técnicas utilizadas para el almacenamiento de la información. Big Data ilustra los elementos esenciales necesarios para el almacenamiento de los datos con un formato único identificable y unos atributos característicos que los definan, para su posterior análisis. El método de almacenamiento elegido influirá en las técnicas de análisis y captura de valor utilizadas, dado que existe una dependencia directa entre el formato en el que se almacena la información y el valor específico que se pretende obtener de ella. En segundo lugar, se examinarán las distintas técnicas de análisis y captura de datos actuales, y los diferentes resultados que se pueden obtener.

Peña Casanova [4] En la investigación titulada “Sistema para detección y aislamiento de fallas” realizado por Msc. Mónica Peña Casanova1, Lic. Joaquim Lauriano da Silva, Dr. Orestes Febles Díaz, Dra. Caridad Anías Calderón donde nos brinda soluciones encaminadas a detectar y corregir fallas, de manera temprana, en el equipamiento activo de las redes. Estas funcionan solo a partir del monitoreo de la red y no están exentas de generar falsos positivos o múltiples alarmas que desorientan a los administradores sobre el origen y la localización de las fallas. La detección tardía implica la degradación de los servicios que se ofrecen provocando el incumplimiento de los acuerdos de nivel de operación y de servicio. Las herramientas existentes, resultan insuficientes para correlacionar el impacto asociado a la ocurrencia de fallas para automatizar las tareas relacionadas a la solución de las mismas.

2.1 IDS

Sistema de detección de intrusos (o IDS por sus siglas en inglés, *Intruder Detection System*) según Villalón Huerta [7] es una herramienta de seguridad encargada de monitorear los eventos que ocurren en un sistema informático en busca de intentos de intrusión. Se define intento de intrusión como cualquier intento de comprometer la confidencialidad, integridad, disponibilidad o evitar los mecanismos de seguridad de una computadora o red [17]. Las intrusiones se pueden producir de varias formas: atacantes que acceden a los sistemas desde el Internet, usuarios autorizados del sistema que intentan ganar privilegios adicionales para los cuales no están autorizados y usuarios autorizados que hacen un mal uso de los privilegios que se les han asignado [13].

2.2 NIDS

Un *Network Intrusion Detection System* (NIDS) o, en castellano, Sistema de Detección de Intrusiones en Redes, es una herramienta capaz de detectar intentos de acceso no autorizados a una red. Busca detectar anomalías que indiquen un riesgo potencial, tales como ataques de denegación de servicio, escaneadores de puertos o intentos de entrar en un ordenador, analizando el tráfico en la red en tiempo real. Para ello, analiza todos los paquetes, buscando en ellos patrones sospechosos [14].

Los NIDS no sólo vigilan el tráfico entrante, sino también el saliente o el tráfico local, ya que algunos ataques podrían ser iniciados desde el propio sistema protegido [9]. A pesar de la vigilancia, su influencia en el tráfico es casi nula.

2.3 ATAQUES A REDES INFORMÁTICAS

2.3.1 Ataque de fuerza bruta

Un ataque de fuerza bruta ocurre cuando el atacante emplea determinadas técnicas para probar combinaciones de contraseñas con el objetivo de descubrir las credenciales de una potencial víctima y así lograr acceso a una cuenta o sistema [15]. Existen muchas herramientas para realizar ataques de fuerza bruta y descifrar contraseñas, como Hydra, Medusa y Ncrack. Además, existen algunas herramientas como hashcat y hashpump para descifrar contraseñas [7].

2.3.2 Ataques DoS y DDoS

El sitio web de Panda Security, S.L.U., [6] nos habla de este tipo de ataques donde menciona que un ataque de denegación del servicio DoS (*Denial-of-service attack*) es aquel que busca privar a los usuarios de acceso a su red o equipo. Una evolución de esta amenaza son los ataques de negación de servicio distribuido (DDoS) que se provocan al generar grandes cantidades de información desde varios puntos de forma voluntaria, para que el usuario o la organización se vean privados de un recurso [16].

2.3.3 Ataques web

Un ataque web se realiza por parte de un usuario malicioso con el fin de aprovecharse de una vulnerabilidad en el diseño o desarrollo de una aplicación web [10]. Si las aplicaciones web no son seguras, toda su base de datos de información confidencial corre grave riesgo de sufrir un ataque a la aplicación web [11]. Los tipos de ataque de inyección de SQL, que se dirigen directamente a las bases de datos, son el tipo de vulnerabilidad más común y más peligrosa [12].

2.3.4 Ataque Botnet

Un ataque de botnet es un tipo de ataque cibernético llevado a cabo por un grupo de dispositivos conectados a Internet controlados por un actor malintencionado [19]. Las propias botnets son simplemente la red de dispositivos. Cuando los ciberdelincuentes inyectan malware en la red para controlarlos como colectivo, se acostumbran a lanzar [20]. Los ataques de botnet se pueden utilizar para enviar spam, robo de datos, comprometer información confidencial, perpetuar el fraude publicitario o lanzar ataques de denegación de servicio distribuida o DDoS más peligrosos [5].

II. MATERIALES Y METODOS

La investigación fue realizada a partir de la revisión de numerosos artículos relacionados con la detección de intrusos bajo un enfoque de aprendizaje automático, determinando así posibles cuestiones abiertas en esa área, donde se pudiera profundizar y hacer aportes.

La investigación se centra en una revisión de las etapas de preprocesamiento de los datos, en el conjunto de datos más empleado en esta área y en el procesamiento semi-supervisado de los datos para realizar detecciones de ataques maliciosos en redes informáticas.

3.1 Base de Datos CSE-CIC-IDS 2018

La base de datos la elaboró la Universidad de New Brunswick a partir del año 2017 y se siguieron generando nuevas versiones posteriormente, IDS *2018 Intrusion CSVs* (CSE-CIC-IDS2018) [21], esta base de datos se creó en un entorno emulado durante un período de 5 días, contiene tráfico de red en formato de paquetes y los resultados del análisis del tráfico en flujo bidireccional, obtenidos con la herramienta CICFlowMeter y descritos por 80 características (Versión de la base de datos del 02-23-2018) [8].

Los ataques que incluye el dataset son ataques DOS, DDoS, fuerza bruta, Heartbleed, Botnet, infiltración y ataques web, la la siguiente tabla se muestran, así como su duración y las herramientas utilizadas.

TABLA I

TIPOS DE ATAQUES DE LA BASE DE DATOS CSE-CIC-IDS 2018

Ataques	**Instrumentos**	**Duración**	**Atacante**	**Víctima**
Bruteforce attack	FTP - Patator SSH - Patator	1 día	Kali Linux	Ubuntu 16.4 (Web Server)
DoS attack	Hulk, GoldenEye, Stowloris, Slowhttptest	1 día	Kali Linux	Ubuntu 16.4 (Apache)
DoS attack	Heartleech	1 día	Kali Linux	Ubuntu 16.4 (Open SSL)
Web attack	*Damn Vulnerable Web App (DVWA) *In - house selenium framework (XSS and Brute - force)	2 días	Kali Linux	Ubuntu 16.4 (Web Server)
Infiltration attack	*First level:Drop box download in a windows	2 días	Kali Linux	Windows and Macintosh

	machine *Second Level: Nmap and postscan			
Botnet attack	* Ares (developed by Python):remote shell, file upload/download, capturing *Screenshots and key logging	1 día	Kali Linux	Windows V.7, 8.1, 10 (32-bit) and 10 (64-bit)
DDoS + PortScan	Low Orbit Ion Canon (LOIC) for UDP, TCP, or HTTP requests.	2 días	Kali Linux	Windows V.7, 8.1, 10 (32-bit) and 10 (64-bit)

3.2 Regresión Logística

La regresión logística es una técnica analítica que nos permite relacionar funcionalmente una variable dicotómica, es decir, una variable que puede adoptar un número limitado de categorías con un conjunto de variables independientes o también llamadas predictoras [18].

Fue necesario seleccionar hiperparámetros para mejorar la precisión del modelo, se optó por determinarlos mediante la técnica de malla o grid search para obtener la mejor combinación y se dividieron los tres conjuntos de datos en un 70% para el entrenamiento y un 30% para realizar las pruebas.

III. Resultados y discusión

Fue necesario reducir el tamaño del conjunto de datos original CSECIC-IDS2018, pues procesar la magnitud del conjunto (6GB) tomaría tiempo significativo; se dividió en tres muestras definidas como Smple 2 , Sample 3 y Sample 4, las cuales estuvieron balanceadas con la misma cantidad de ataques maliciosos y benignos. Se realizaron tres modelos de Regresión Logística aplicados a cada muestra, en la siguiente tabla se muestran dichos modelos entrenados.

TABLA II

Modelos entrenados con el dataset CSE-CIC-IDS2018.

Nombre	**Sample**	**% de original**	**GridSearch**	**Tiempo**
LogReg1	Sample 2	8%	{1,10}	1 h
LogReg2	Sample 3	4%	{0.01,0.1,1,10,100,1000,10000}	30 min
LogReg3	Sample 4	1%	{0.01,0.1,1,10,100,1000,10000}	15 min

Se consideraron pocos hiperparámetros debido al coste de tiempo de ejecución, sin embargo estos mostraron buenos resultados.

Al realizar las pruebas de cada muestra con sus respectivos conjuntos de test, los tres modelos mostraron comportamientos similares. A continuación, se muestran los datos del segundo modelo (Sample 3) LogReg2.

La matriz de confusión del modelo muestra buenos resultados de verdaderos positivos y verdaderos negativos y en cuanto a los falsos positivos y falsos negativos son pocos los casos en los que tuvo fallas, el cual representa solo al 7% del conjunto de prueba.

TABLA III

MATRIZ DE CONFUSIÓN DEL MODELO LOGREG2 ENTRENADO SOBRE EL CSE-CIC-IDS2018.

	Positivos (%)	**Negativos (%)**
Verdaderos	32.40	7.16
Falsos	4,90	55.54

A continuación, mostramos la precisión del modelo, esta es del 96% y un recall del 91% en ataques benignos, y una precisión del 91% y recall del 96% en ataques maliciosos, este resultado muestra que el modelo es bastante bueno al realizar las predicciones.

TABLA IV

REPORT DEL MODELO LOGREG2 ENTRENADO SOBRE EL CSE-CIC-IDS2018. REFLEJA LOS RESULTADOS OBTENIDOS SOBRE EL CONJUNTO DE TEST.

	Precisión	**Recall**	**F1-score**
Benignos	0.87	0.82	0.84
Ataques	0.89	0.92	0.90

Se utilizó la curva ROC para representar la proporción entre los verdaderos positivos frente a los falsos positivos. El área bajo la curva ROC es 0.93, este resultado confirma que el modelo se comporta adecuadamente sobre el conjunto de prueba.

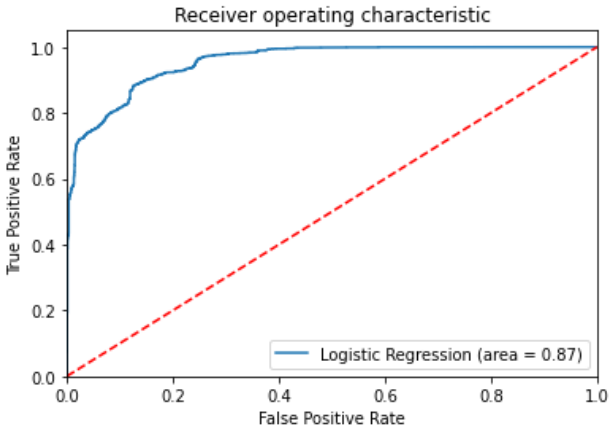

Figura 1. Curva ROC del modelo LogReg2 entrenado sobre el CSE-CIC-IDS2018

Para evitar la posibilidad de que se estuviera produciendo un sobreaprendizaje del modelo, en cuanto a los datos tomados del conjunto de datos del CSE-CIC-IDS2018, se realizaron otras pruebas del modelo sobre otras muestras aleatorias del conjunto de datos original. En estas pruebas, los resultados fueron bastante buenos, similares a los del ROC de la Figura 1.

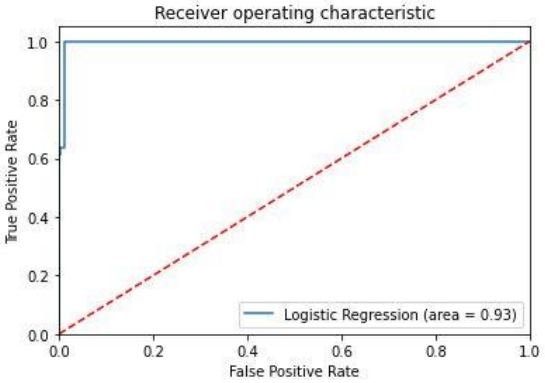

Figura 2. Resultado de probar el modelo LogReg2 sobre una muestra del dataset CSE-CIC-IDS2018.

IV. CONCLUSIONES

Se propuso un método para la detección de intrusiones en redes informáticas mediante la aplicación de una técnica de aprendizaje automático, conocida como Regresión Logística, el método consistió en un preprocesamiento de datos, una definición de datos de entrenamiento y prueba, y el desarrollo, entrenamiento y prueba del modelo.

La precisión de detección del modelo en cuanto a ataques benignos es de 96% y de ataques maliciosos es de 91%, estos resultados de consideran bastante buenos, sin embargo, aún hay desafíos por superar, estos desafíos se centran en: gran tamaño de datos, mayor dimensionalidad y preprocesamiento de datos.

El hecho de no haber probado el modelo con un conjunto de datos diferente al del CSE-CIC-IDS2018 abre las posibilidades de que el modelo propuesto no esté totalmente preparado para ser empleado en otro conjunto de datos, ya que existe bastante dependencia sobre el dataset utilizado, esto quiere decir que no podríamos utilizar los datos del CSE-CIC-IDS2018 para entrenar modelos que funcionen sobre otra infraestructura.

REFERENCIAS

[1] R. E. González Peralta, «El análisis de anomalías detectadas en las pruebas de software: una vía para mejorar el ciclo de vida,» Revista Española de Innovación, vol. 5, nº 2, p. 8, 2009.

[2] J. L. Rivero Pérez, «Técnicas de aprendizaje automático para la detección de intrusos en redes de computadoras,» Revista Cubana de Ciencias Informáticas, vol. 8, nº 4, oct- dic 2014.

[3] R. Noblejas Sampedro, «Estudio de algoritmos de detección de anomalías y su aplicación a entornos de ciberseguridad,» Archivo Digital UPM, 2016.

[4] M. M. Peña Casanova, «SISTEMA PARA DETECCIÓN Y AISLAMIENTO DE FALLAS,» Revista Cubana de Ciencias Informáticas, vol. 12, nº 2, 2018.

[5] CDNetworks, «Ataques de Botnet: Todo lo que necesita saber,» 17 Mayo 2021. [En línea]. Available: https://www.cdnetworks.com/cloud-security-blog/botnet-attacks/.

[6] Panda Security, S.L.U., «Ataques DoS y DDoS,» [En línea]. Available: https://www.pandasecurity.com/es/security-info/network-attacks/. [Último acceso: 25 08 2021].

[7] A. Villalón Huerta, SEGURIDAD EN UNIX Y REDES, the Free Software Foundation, 2002.

[8] T. M. «Building an intrusion detection system using deep learning.,» [En línea]. Available: https://towardsdatascience.com/.

[9] C. Jiménez Galindo, «Diseño y Optimización de un Sistema de Detección de Intrusos Híbrido,» 2009.

[10] J. M. Andrade Guzmán, «Ataques Web,» Seguridad, 2018.

[11] M. I. Romero Castro, «INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES,» 2018. [En línea]. Available: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf.

[12] «Fluid Attacks,» 2021. [En línea]. Available: https://try.fluidattacks.com/bo/sql/?gclid=CjwKCAjw4KyJBhAbEiwAaAQbEyYPXzI2ihuAvNc7DfsgOPj5ysQfXJVw_LXp31aq7bZMic3DAltRjhoC_UQQAvD_BwE.

[13] M. Olguin Carbajal, I. Rivera Zarate y P. Perez - Romero, «Sistemas de Detección de Intrusos (Ids), Seguridad en Internet,» redalyc.org, nº 34, p. 33, 2006.

[14] C. A. Ocampo y Y. Castro Bermúdez, «Sistema de detección de intrusos en redes corporativas,» Redalyc.org, vol. 22, nº 1, marzo 2017.

[15] E. A. Maya O., «Aplicación de técnicas de fuerza bruta con diccionario de datos, para

vulnerar servicios con métodos de autenticación simple “Contraseñas”, pruebas de concepto con software libre y su remediación,» Maskana, 19 06 2016.

[16] R. D. Narváez, «Evaluación de ataques de Denegación de servicio DoS y DDoS, y mecanismos de protección,» GEEKS DECC - REPORT, vol. 2, nº 1, 2010.

[17] S. Leacock, «Evaluación de ataques de Denegación de servicio DoS y DDoS, y mecanismos de protección,» Backtrack Academy, 10 04 2018.

[18] L. Camarero, A. Almazán y B. Mañas, Regresión Logística: Fundamentos y aplicación a la investigación sociológica, 2013.

[19] J. U. Santillán Arenas y J. R. Sánchez Soledad, «BOTNETS,» Seguridad - Cultura de prevención para TI, 2018.

[20] G. Calvo Ortega, «https://revista.seguridad.unam.mx/numero-05/botnets,» MISTIC, 01 2018.

[21] «IDS 2018 Intrusion CSVs (CSE-CIC-IDS2018),» 2018. [En línea]. Available: https://www.kaggle.com/solarmainframe/ids-intrusion-csv?select=02-14-2018.csv.