Seguridad de la Información, Modelos de comportamiento, una Alternativa Para Mejorar la Detección de Intrusos

Roberto Camilo Choque Apaza
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
choqeapaza@gmail.com

***Resumen*—Estudiando el actual contexto de seguridad en la red y la existencia de sistema de detección de intrusos, este artículo introduce la tecnología de minería de datos en la detección de ataques de red y el modelo de comportamiento de patrones. Los datos son la recopilación de siete semanas de tráfico TCP de red, los conjuntos de datos contienen 22 tipos de ataques, se seleccionó el modelo de predicción (Farthest first, y simple K-means) de Weka capaz de diferenciar el comportamiento normal de malicioso. Todo con el fin de minimizar los ataques de red que diariamente causa tantos inconvenientes a nivel local, regional y mundial.**

Palabras clave—minería de datos, patrones, modelo, intrusión.

I. INTRODUCCIÓN

Las tecnologías irrumpen en todos los aspectos de vida. Tal es el nivel de cambio que algunas de estas tecnologías conllevan, que se han llegado a describir como disruptivas. Así, por ejemplo, el fenómeno del internet de las cosas, las NTIC, el cloud computing son tecnologías disruptivas, que están revolucionando la forma en la que funciona nuestro mundo [1].

Los servicios de internet ofrecen servicios de alta velocidad, "esta facilidad de intercambiar información multiplica la capacidad de los ataques a las redes, mismas que promueven a usuarios maliciosos y crackers a buscar objetivos vulnerables, como los sistemas operativos no actualizados, sistemas infectados con virus a través de correos electrónicos, navegación por páginas web, descargas de datos, ejecución de servicios inseguros o puertos abiertos" [2].

Así también, los sistemas informáticos y de comunicación sufren repetidamente ataques de seguridad y privacidad, a lo que invierten cantidades considerables de dinero en mejorar la seguridad y privacidad de su red mismas que afectan la confidencialidad, integridad, disponibilidad.

Sobre la investigación realizada se ha buscado estudios relacionados en cuanto a la detección de ataques en la red, mismas que se señalan a continuación:

Se tiene en primer lugar, un estudio de los distintos "Sistemas de Detección de Intrusos-IDS (por sus sigla en inglés Intruder Detection System)" como ser: las técnicas de detección de anomalías a cambios imprevistos, los sistemas basados en métodos estadísticos como el modelo de series temporales, los sistemas expertos que tienen el conocimiento codificado mediante reglas, detección de firmas que incorpora a la base de datos una firma nueva por cada nuevo tipo de ataque o vulnerabilidad descubierta [4].

Segundo, se tiene una investigación que ayudó en la comprensión de los procesos de la minería de datos aplicada a la detección de intrusos para el análisis de comportamientos que no son fácilmente perceptibles, y en especial, la detección de anomalías en los registros, con el fin de detectar los factores que ponen en peligro la confidencialidad, integridad, disponibilidad y no repudio de los datos [2].

Finalmente, un estudio que conduce y orienta la investigación a la detección de intrusos con minería de datos, de los "protocolos (TCP, UDP, ICMP), IP de origen, IP destino, y puerto de destino, puerto origen" el algoritmo k-medias para agrupar los datos en grupos normales, anormales y detectar el tráfico de falsos positivos presentes en los datos [5].

Estos antecedentes permiten direccionar el trabajo para un mejor sustento científico teórico, producto del éxito de la aplicación de la minería de datos para el mejoramiento del nivel de seguridad en la red; situación que está siendo vulnerada. Así como el caso de una red en entornos militares de la Fuerza Aérea de los EEUU. De los tres estudios mencionados el tercero, se acerca a la investigación que se pretende realizar desde un análisis de intrusiones en la red.

El problema radica en la existencia de falsos positivos, "durante las operaciones de alto tráfico en una red, un IDS puede generar un gran número de falsos positivos con mucha frecuencia" [5] y falsos negativos, es decir, un IDS no puede detectar una actividad maliciosa y declara que es una actividad correcta, lo que no garantiza la seguridad de la información en la red.

Así mismo, se crean los sistemas de prevención de intrusos "IPS", una versión mejorada de los "IDS", puesto que no solo detectan las intrusiones en la red, sino que las bloquean evitando robo de información, pero sin embargo "como ocurre con cualquier tipo de dispositivo de seguridad que inspecciona paquetes, su uso puede generar potenciales inconvenientes en términos de rendimiento, latencia y disponibilidad" [6].

Para referenciar este artículo (IEEE):

[N] R. Choque, «Seguridad de la Información, modelos de comportamiento, una alternativa para mejorar la detección de Intrusos» *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 83-87, 2020.

Es precisamente por lo expresado anteriormente que la minería de datos basada en una metodología adecuada, puede ser muy útil en el proceso de exploración de datos, para organizar reglas y patrones que permitan clasificar los flujos de datos en la red que afectan la confidencialidad, integridad, disponibilidad, ocasionando daño de datos, denegación de servicios, Fuga de datos, Sabotaje informático entre otros, a fin de mejorar el nivel de seguridad de ataques que no son detectados por antivirus, cortafuegos o sistemas de detección de intrusos y entregar resultados de manera oportuna, que ayude en la toma de decisiones.

II. Marco teórico

A. *Minería de Datos*

Es el conjunto de técnicas encaminadas al descubrimiento de la información contenida en grandes conjuntos de datos. Se trata de analizar comportamientos, patrones, tendencias, asociaciones y otras características del conocimiento inmerso en los datos [7].

Por lo tanto, la minería datos permite analizar grandes volúmenes de datos como ser "logs de ataques de red", para poder descubrir patrones "conocimiento" que se encuentran ocultos en los datos.

B. *Data Warehouse y data mining*

Data warehouse almacena los datos de las bases de datos heterogéneas para que los usuarios consulten sólo un único aspecto. Las respuestas que un usuario consigue a una consulta dependen de los volúmenes de la data warehouse.

Además, data warehouse en general no intenta extraer la información de los datos almacenados, data warehouse estructura y organiza los datos para soportar funciones de administración, mientras que la minería de datos intenta extraer la información útil según el caso, así como predecir las tendencias de los datos. No es necesario construir una data warehouse para hacer data mining, ya que también puede aplicarse data mining a las bases de datos [8].

C. *Intrusión*

El NIST (National Institute of Standards and Technology) [6] define la detección de intrusos como los procesos que monitorizan los eventos en los sistemas de red y procesan dichos eventos en busca de patrones que indiquen anomalías.

Así también se define a la detección de intrusos como la capacidad de detectar ataques en una red, incluyendo dispositivos y computadoras, según [9], la intrusión de red se divide en cuatro categorías principales:

1. ***DoS* (*denial-of-service*):** denegación de servicio. Hace que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecargando los recursos computacionales de su Sistema.
2. **R2L**: acceso no autorizado desde una máquina remota.
3. **U2R**: acceso no autorizado a privilegios de super usuario.
4. **Probing**: vigilancia y otros tipos de sondeo de redes.

Es decir, la implementación de este prototipo computacional ayudará a complementar un nuevo enfoque en la búsqueda a la solución de los ataques de intrusión en la red basado en las cuatro categorías mencionadas anteriormente.

D. *Aprendizaje supervisado y no supervisado*

El aprendizaje supervisado o predictivo se los conoce de esta manera debido a que los valores estimados o calculados son comparados con los resultados conocidos y por lo tanto se tiene una clara medida del éxito o falla de la predicción, por ejemplo, para la detección de aquellos clientes que son más propensos al abandono de una determinada empresa. Algunos algoritmos que se utilizan en estos modelos son los de clasificación y las regresiones.

El aprendizaje no supervisado o descriptivos, es usado en los casos en que no se tiene conocimiento previo del resultado al que se va a llegar, donde el modelo se va ajustando de acuerdo a las observaciones o datos entregados, y se recurre muchas veces a argumentos heurísticos para evaluar la calidad de los resultados. Algunos algoritmos que se utilizan en estos modelos son los de clustering y las reglas de asociación.

E. *Modelos y Algoritmos de minería de datos*

Un algoritmo de Minería de Datos es un procedimiento bien definido que toma los datos como entrada y produce una salida en forma de modelos o patrones.

Es importante notar que no existe un "mejor" modelo o algoritmo de minería de datos, depende del problema en estudio y de los datos disponibles para decir cuál entrega resultados más confiables. Los modelos predictivos requieren ser "entrenados", utilizando un conjunto de datos de entrenamiento cuyo valor de variable objetivo es conocido. La idea es que el modelo entregue resultados en base un aprendizaje, en otras palabras, que se vaya ajustando a la realidad conocida como al problema que se pretende resolver.

TABLA I. Modelos de minería de datos

Modelo	**Técnicas de minería de datos**		
	Aprendizaje	***Técnica***	***Algoritmo***
Modelo	No supervisadas o descriptivos	Clustering	Análisis de clúster Farthest first Simple k-means Reducción de la dimensión Segmentación
Modelo	Supervisadas o predictivas	Predicción	Modelos de regresión Análisis de Varianza Series Temporales Análisis discrimínate Árboles de decisión Redes Neuronales

(*Fuente: Pere4z, 2014*)

La tarea consiste en proteger la red de usuarios no autorizados y construir un modelo de minería de datos (clasificador y agrupador) capaz de diferenciar el comportamiento normal del malicioso.

A. *Farthest first*

El primer algoritmo más lejano propuesto por Hochbaum y Shmoys 1985 tiene el mismo procedimiento que k-medias, esto también elige los centroides y asigna los objetos en grupo, pero con la distancia máxima y las semillas iniciales son valores que se encuentran a la mayor distancia a la media de los valores, aquí la asignación de conglomerados es diferente, en el clúster inicial

obtenemos un enlace con un alto conteo de sesiones, como en clúster-0 más que en cluster-1, y así sucesivamente, es decir:

- Selecciona aleatoriamente el primer centro.
- Para cada punto restante, calcule la distancia al centro actual. Seleccione el punto con la distancia máxima como nuevo centro.
- Asigne los puntos restantes con el cálculo de la distancia a cada centro del grupo y colóquelo en el grupo con la distancia mínima.

$$\min \{\max \text{dist}(p1, p2), \max \text{dist}(p1, p2) \ldots\} \quad (1)$$

B. *Simple k-means*

Es un algoritmo de clustering particional, uno de los métodos de clustering más conocidos y utilizados cuando todas las variables son de tipo cuantitativo. Funciona de forma iterativa, dividiendo óptimamente el conjunto inicial de datos en un número de clusters, el cual se indica como parámetro:

TABLA II. MODELOS DE MINERÍA DE DATOS

Etapa	Descripción
P. 1	Elegir k ejemplos que actúan como semillas (k número de *clusters*).
P. 2	Para cada ejemplo, añadir un dato a la clase más similar.
P. 3	Calcular el centroide de cada clase, que pasan a ser nuevas semillas.
P. 4	Si no se llega a un criterio de aproximación (por ejemplo, dos iteraciones no cambian la clasificación de los ejemplos), volver a 2.

Fuente: (Wunch, 2009)

Los modelos misionados anteriormente son las que dan luz verde a la presente investigación.

III. MÉTODOS

A. *Metodología CRISP-DM*

- Comprensión del negocio: Entendimiento de los objetivos y requerimientos del proyecto y la definición del problema de minería de datos.
- Comprensión de los datos: Obtención conjunto inicial de datos, exploración del conjunto de datos, identificar las características de calidad de los datos y los resultados iníciales.
- Preparación de Datos: Selección de datos y la limpieza de datos.
- Modelamiento: Implementación en herramientas de minería de Datos.
- Evaluación: Determinar si los resultados coinciden con los objetivos del negocio.
- Despliegue: Instalar los modelos resultantes en la práctica y la configuración para minería de datos de forma repetida o continúa.

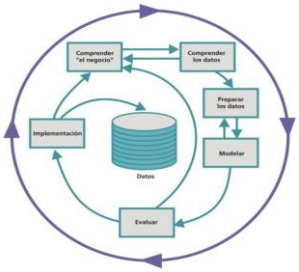

Fig. 1. Modelo de proceso CRISP–DM

B. *Comparación de software para el desarrollo de aplicaciones de minería de datos*

TABLA III. SOFTWARE DE MINERÍA DE DATOS

Características	Modeler	SAS Enterprise Miner	Tariykdd	Weka
Licencia Libre	No	No	Si	Si
Requiere conocimientos avanzados	No	No	No	No
Acceso a SQL	Si	No	Si	Si
Multiplataforma	No	Si	Si	SI
Requiere bases de datos especializadas	No	...	No	No
Métodos de máquinas de soporte vectorial	Si	Si	No	Si
Métodos bayesianos	Si	...	No	Si
Puede combinar modelos	Si	Si	No	Si (no resulta eficiente)
Modelos de clasificación	Si	Si	Si	Si
Implementa arboles de decisión	Si	Si	Si	SI
Modelos de regresión	Si	Si	No	Si
Clusterin	Si	Si	No	Si
Interfaz amigable	Si	Si	Si	Si
Permite visualización de datos	Si	Si	Si	Si

(*Fuente: Vallejo, 2011*)

La herramienta que más se adecua para el desarrollo del prototipo de minería de datos en la detección de intrusos en la red es: Weka, que resulta ser multiplataforma "Windows, Linux, MacOS", de licencia libre, proporciona mayor facilidad al momento de realizar el análisis de datos de ataques de intrusiones en la red según la tabla III.

IV. RESULTADOS

Este trabajo, se centra en la extracción de datos de conexión a la red como un primer paso mismos que se podrían recoger de la mayoría de firewalls y sensores "IDS/IPS" de intrusión en la red, o pueden ser construidos sobre la base de registros de paquetes.

A través del prototipo computacional que ayuda a complementar un nuevo enfoque en la búsqueda a la solución de los ataques de red, debido a que el diseño de las variables a medir estará definido en la capa superior del enlace de datos según el Modelo de referencia OSI, permitiendo complementar los esfuerzos realizados por la comunidad investigativa en la capa

de red, buscando aumentar la eficacia en la detección de ataques de red.

A partir de los modelos "árbol de decisión, Soporte de Máquina Vectorial" y una base de datos de ataques simulados en un entorno de red militar de la Fuerza Aérea de los EE. UU. con una amplia variedad de intrusiones de red realizada para el Tercer Concurso Internacional de Descubrimiento de Conocimientos dirigidos por los laboratorios de MIT Lincoln recopiladas de siete semanas de tráfico de red TCP [3].

Todo con el fin de minimizar este comportamiento anómalo en la red que diariamente causa tantos inconvenientes a nivel local, regional y mundial.

Modelo de detecciones de ataques de red

Se considera la metodología CRISP-DM, la cual permite desarrollar un proyecto de Minería de datos aplicado a un caso real como son las intrusiones en la red. De acuerdo a lo anterior, se formulan los pasos a seguir, que se detallan a continuación:

A. *Selección de fuentes de datos (Entrada)*

Teniendo en cuenta las variaciones de los ataques de red, se utiliza la métrica de las cabeceras de los paquetes IP la cual corresponde al nivel 3, encabezados TCP que corresponde al nivel 4 y los datos de la capa de aplicación como las peticiones HTTP que están representadas en el nivel 7 las cuales están representadas en el modelo de referencia OSI. Esto proporciona un espectro mucho más amplio de datos para analizar y, por lo tanto, una mayor probabilidad de encontrar características que se pueden utilizar para detectar anomalías en el tráfico de la red.

B. *Indicadores de los tipos de Ataques de Red*

A partir de las métricas utilizadas las cuales serán tratadas para clasificar y agrupar los ataques de red mismas que se dividen en cuatro principales categorías que se detallan a continuación (*véase* tabla IV):

TABLA IV. DISTRIBUCIÓN DE LOS ATAQUES DE AED POR CADA CATEGORÍA NSL-KDD

Categoría de Ataque	**Ataques de Red**		
	Nombre del Ataque de Red	***Número de Registro***	***Porcentaje total***
DoS (Anormal)	Back	956	
	Land	18	
	Neptune	41214	
	Pod	201	
	Smurf	2646	
	Teardrop	892	
		45927	36.46
Probe (Anormal)	Satan	3633	
	Ipsweep	3599	
	Nmap	1493	
	Portsweep	2931	
		11656	9.25
R2L (Anormal)	Guess Password	53	
	Ftp write	8	
	Imap	11	
	Phf	4	
	Multihop	7	
	Warezmaster	20	
	Warezclient	890	
	Spy	2	
		995	0.79
U2R (Anormal)	Buffer overflow	30	
	Loadmodule	9	
	Rootkit	10	
	Perl	3	
		52	0.04
Normal		**67343**	53.46
Total		**125973**	

A partir de la estructura de un fichero con formato *.arff "Attribute Relation File Format"*: con cabecera "AtaquesDeRed", la cual acepta como atributos "duración, tipo de protocolo, servicio, numero de accesos, numero de acceso a super usuario, IP origen, IP destino, y el tipo de ataque de red" y que no dan problemas para iniciar el proceso de minería de datos.

C. *Aplicación de modelos de minería de datos en la detección de ataques de red*

Llegando a este punto, tras un tiempo de procesado de todos los datos obtenidos, tenemos nuestro archivo en formato *.arff* de los diferentes datos proporcionados. El proceso de ejecución del algoritmo, dependerá de los datos históricos de los ataques de red, la cual puede llegar a tardar unos segundos dependiendo de la cantidad de datos.

A continuación, se analizan los resultados de dos algoritmos seleccionados de los múltiples algoritmos implementados en *Weka*. La selección de estos modelos ha estado basada en los resultados que se desea obtener.

En este caso, el propósito será detectar intrusiones en la red y proteger la red de computadoras de usuarios no autorizados. La tarea de aprendizaje del detector de intrusos es construir un modelo (clasificador y agrupador).

Después de haber realizado varias pruebas con los datos de ataques de red se representan los comportamientos que llegan a tener los atributos normales y anormales:

En la figura 2, se verifica la existencia de ataques de red DoS con un mayor patrón de agrupamiento, seguido del comportamiento normal, R2L, Probing, y finalmente U2R.

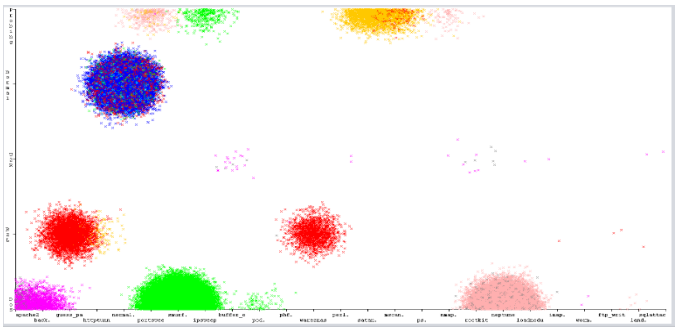

Fig. 2. Comportamiento de patrones de ataques de red y categoría de ataque

En la figura 3, se comprueba los diferentes servicios *"private,auth, ,daytime, discard, domain, ecr_i, efs, ftp, hostnames, http_443, imap4, icmp, netbios, netstat, nntp, ntp_u, other, printer, shell, smtp, sql_net, ssh, telnet, systat, time, vmnet"* donde existe mayor agrupamiento en los ataques de red DoS, seguida de un comportamiento de patrones R2L, Probing, U2R.

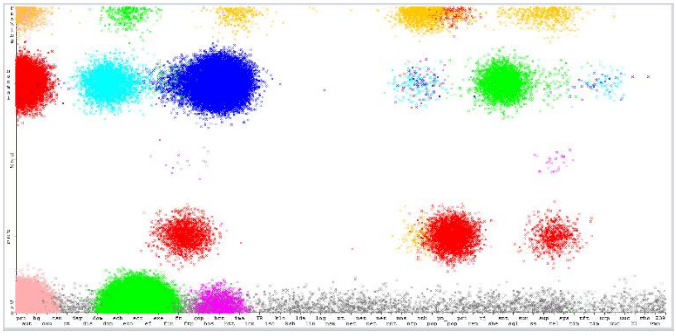

Fig. 3. Comportamiento de patrones de ataques de red y servicio comprometido

D. *Evaluado de los modelos óptimos*

En la siguiente figura, se observa un breve resumen con los datos más relevantes sobre los modelos "algoritmos", que han obtenido mejores resultados:

ALGORITMO	Tiempo de entrenamiento
Simple *K-means*	0.62 s
FasthestFirst	0.32 s

Fig. 4. Comparativa de Resultados de Agrupación

De los experimentos para la prueba se utilizó la Simple K-means, FasthestFirst, los dos modelos presentan una solución razonable, cada una con sus particularidades, pero la segunda realiza la agrupación por similitud en menor tiempo que la primera.

V. DISCUSIÓN

Se ha determinado y obtenido información para establecer indicadores normales y anormales según los tipos de ataques de red más comunes "denegación de servicios (DoS), *Root to local attacks* (R2L), *User to root attack* (U2R), *Probe attacks* (Probing) y el modelo de detección de ataques de red en base a minería de datos mismo que coadyuba a la toma de decisiones.

A partir de la simulación de ataques de red en tiempo real "segundos", del mejor modelo de detección de ataques de red *"Farthest first y simple k-means"* cumplen con las necesidades de detección de ataques de red, misma que ha demostrado ser eficiente, pues genera automáticamente patrones de intrusión *"DoS, R2L, U2R, Probing"* y se adapta a los resultados esperados.

REFERENCIAS

[1] E. Gonzales, Big Data, Privacidad y Protección, Eds. Madrid: Agencia Estatal Boletín Oficial del Estado.

[2] D. Vallejo, Minería de Datos Aplicada en Detección de Intrusos, Colombia, 2011.

[3] Wenke Lee, Sal Stolfo, Phil Chan, Eleazar Eskin, Wei Fan, Matt Miller, Shlomo Hershkop, and Junxin Zhang, Real Time Data Mining-based Intrusion Detection, in Proceedings of The 2001 DARPA Information Survivability Conference and Exposition (DISCEX II), Anaheim, CA, Junio del 2011.

[4] M. I. Garcia. Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral, Almeria, 2008.

[5] Ch. Kumar, Sistema de detección de intrusiones utilizando K-medias de minería de datos, Bangalore, 2017.

[6] Networkworld, Prevención de intrusiones. Web. 01 Mayo 2008. http//www.networkworld.es/seguridad/prevension-de-intrusiones

[7] M. Marquez, Minería de datos a través de ejemplos, 2014.

[8] S. Mukkamala, Detecting denial of service attacks using support vector machines," Fuzzy Systems, 2003. FUZZ '03. The 12th IEEE International Conference on Vol. 2.

[9] J. Mena, Investigative data mining for security and criminal detection, Butterworth-Heinemann, Butterworth-Heinemann, EE.UU, 2003.

[10] Molina, Técnicas de análisis de datos aplicaciones prácticas utilizando Microsoft Excel y weka, Madrid, España, 2012.

[11] Wunch, R. XU, Clustering, Wiley Publishin, 2009.