Identificación visual de ciberataques mediante técnicas de reducción de la dimensionalidad y visualización de la información

Nicolas R. Enciso, Jorge E. Camargo
Grupo de Investigación UnSecure Lab
Universidad Nacional de Colombia – Sede Bogotá

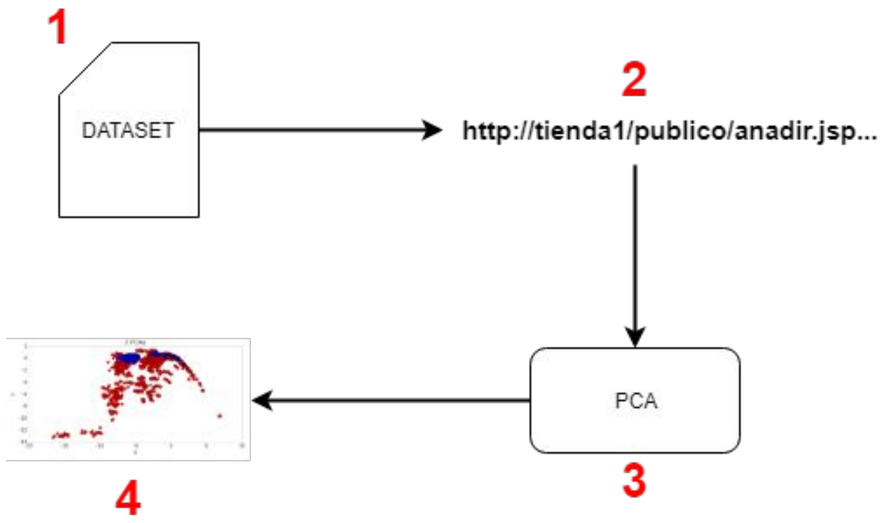

Figura 1. Metodología utilizada

Descripción

Debido a los grandes avances de Internet y la computación, la sociedad está cada vez más conectada digitalmente mediante diferentes tipos de dispositivos y sistemas de información. Esto hace que se generen mayores riesgos de recibir ciberataques [1].

Propósito:
En este trabajo se presenta un método para identificar automáticamente ciberataques a partir del contenido de los *headers* de paquetes HTTP. El método utiliza un conjunto de datos en el que se cuenta con paquetes normales y con paquetes de diferentes tipos de ciberataques tales como XSS, SQL Injection y CRLF.

Metodología

1. **Dataset**: Se obtiene un conjunto de datos más de 60.000 casos, de los cuales 25.000 son ciberataques [2].
2. **Extracción de características**: A partir de la URL de cada *header*, se construye un vector con características tales como cantidad de caracteres especiales, sentencias SQL, longitud, similitud de distribución en el lenguaje, entre otras.
3. **Reducción de la dimensionalidad**: Se utiliza el algoritmo PCA (*principal component analysis)* para reducir la dimensionalidad y encontrar los 2 componentes principales.
4. **Visualización en 2D**: Se visualiza cada paquete en un plano coordenado en donde (x,y) corresponden a los dos componentes principales, discriminando por color paquetes normales (rojo) y ciberataques (azul).

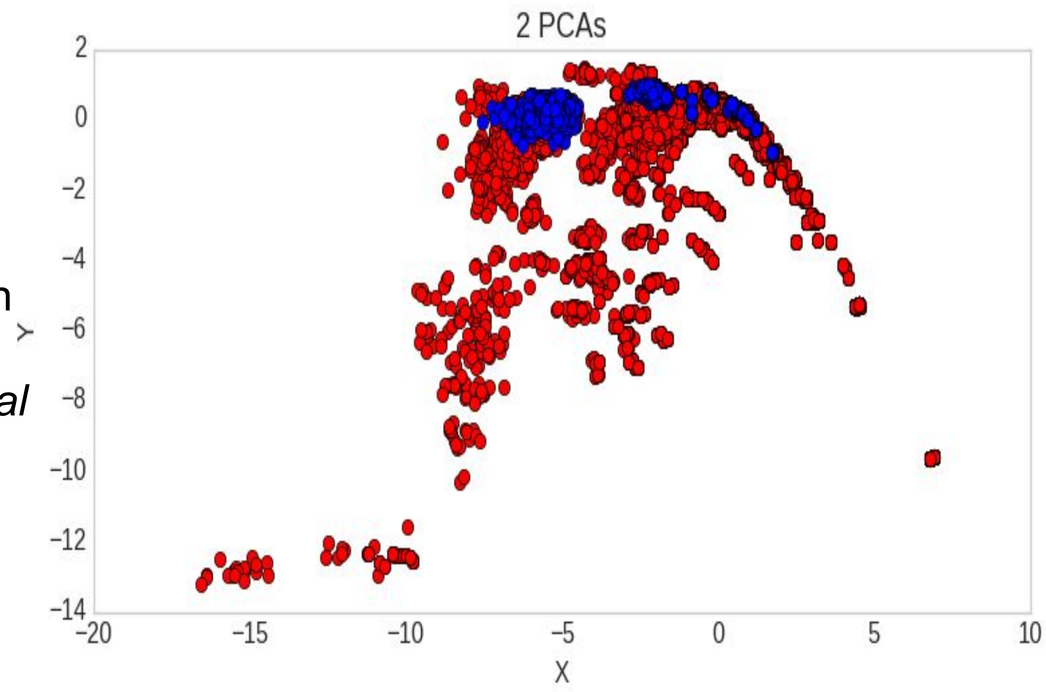

Figura 2. Casos de ataque (azul) y neutrales (rojo) posterior a PCA

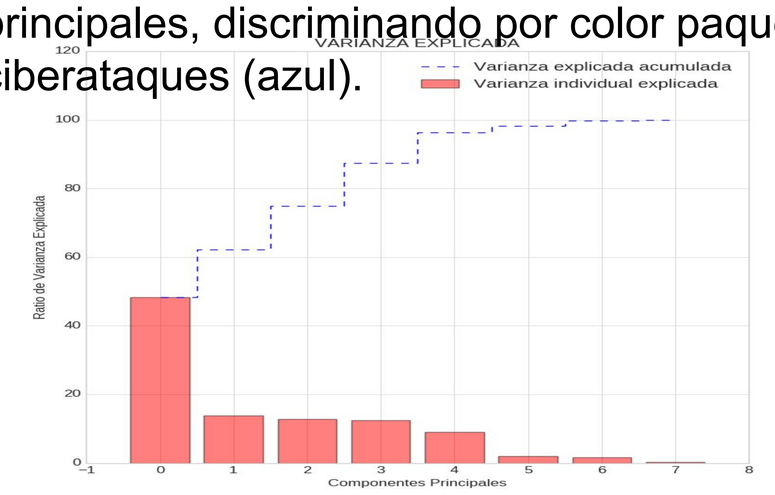

Figura 3. Varianza explicada por reducción PCA

Conclusiones

- El método permite identificar visualmente cuáles paquetes son normales y cuáles son ciberataques.
- Con la simplificación del dataset, y una pérdida no significativa en información, se puede continuar con la etapa de uso de los datos preparados en el presente trabajo, como entrada para algoritmos de clasificación en machine learning.
- Como trabajo futuro se plantea utilizar métodos de Machine Learning tales como clasificación y agrupamiento.

Referencias

[1] Idhammad, M., Afdel, K. & Belouch, M. Semi-supervised machine learning approach for DDoS detection. Applyied Intelligence, (2018) 48: 3193.

[2] Carmen Torrano Giménez, Alejandro Pérez Villegas, Gonzalo Álvarez Marañón.. (2010). HTTP DATASET CSIC 2010 de Consejo Nacional de Investigación, Instituto de seguridad de la Información, gobierno de España Sitio web: http://www.isi.csic.es/dataset/