Instituto Tecnológico y de Estudios Superiores de Monterrey

Escuela de Ingeniería y Ciencias

Ingeniería en Ciencias de Datos y Matemáticas

Análisis de Criptografía y Seguridad

Actividad 3.4. Configuración de VPNs basadas en IPSec

Nombre	Matrícula
Julio Avelino Amador Fernández	A01276513
Juan Pablo Echeagaray González	A00830646
Verónica Victoria García De la Fuente	A00830383
Erika Martínez Meneses	A01028621
Emily Rebeca Méndez Cruz	A00830768
Ana Paula Ruiz Alvaro	A01367467

Dr. Alberto Francisco Martínez Herrera

Dr.-Ing. Jonathan Montalvo-Urquizo

Socio Formador: Kaspersky

Monterrey, Nuevo León

10 de junio del 2022

Las respuestas presentadas en este escrito se basan en la presentación, videos y artículo científico *DNS-ADVP: A machine learning anomaly detection and visual platform to protect top-level domain name servers against DDoS attacks* escrito por profesores del ITESM y NIC [Trejo et al., 2019].

1. ¿Cuál es la principal función de la plataforma: DNS-ADVP: DNS Anomaly Detection Visual Platform?

Brindar una medida de contraatacar ciberataques del tipo DDoS que afecten a servidores DNS mediante un modelo visual.

2. ¿Cuáles son las fuentes que generan una alerta en el sistema?

- La actividad de las IP
- Las correlaciones de las actividades de los IP
- La predicción arrojada por el clasificador

3. ¿Cuál es el clasificador utilizado en la plataforma?

El equipo implementó el algoritmo del vecino más cercano (KNN) para clasificar el tráfico en la red como normal o anormal.

4. ¿De qué manera podrías mejorar la plataforma?

4.1. Simplificación o mejora de las visualizaciones

En el video se menciona que las 4 gráficas describen un mismo fenómeno, pero que cada par representa una cara del ataque DDoS; el que haya demasiadas visualizaciones para representar la misma información puede llegar a ser algo redundante y confuso; en especial creo que el gráfico de cuerdas necesita de una explicación a mayor detalle para ser interpretada.

4.2. Realizar PCA en los datos que recibe el modelo

En el video se explica cómo el algoritmo KNN necesita de 174 atributos para realizar el proceso de clasificación con una métrica AUC de 80 %, que en palabras generales nos dice que el modelo tiene un desempeño aceptable para realizar.

Sin embargo, varios de los atributos en el modelo fueron compuestos de atributos que ya se estaban contando, agregando una capa de dependencia que podría mermar la precisión del modelo. De forma tentativa, creo que un PCA podría arrojar luz sobre qué atributos son verdaderamente significativos para el proceso de clasificación.

4.3. Auditoría al código implementado

En la presentación nunca se brinda una liga de acceso al código implementado por el equipo, no existe una manera robusta de brindar críticas constructivas si es que no sabemos cómo es que llevaron a cabo su tarea, un poco de cultura open source nunca es mala cuando se trata de ciberseguridad.

Referencias

[Trejo et al., 2019] Trejo, L. A., Ferman, V., Medina-Pérez, M. A., Giacinti, F. M. A., Monroy, R., and Ramirez-Marquez, J. E. (2019). Dns-advp: A machine learning anomaly detection and visual platform to protect top-level domain name servers against ddos attacks. *IEEE Access*, 7:116358–116369.