Proyecto Final
Fase 1

DELVALLE
GRUPO EDUCATIVO

Andrei Portales 19825, Christian Perez 19710, Alfredo Quezada 191002, Javier Hernández 19202, Marco Ramirez 19588.

Motivación:

La tecnología avanza exponencialmente hacia un futuro donde la mayoría de actividades y transacciones que realizamos y realizaremos, se encuentran que se dan mediante algún tipo de página o servicio web, es por eso que podemos ver que conforme más se están utilizando estas herramientas, mas se encuentran con la posibilidad de sufrir un ataque, en este caso por mencionar algunos ejemplos, se dan los ataques DoS, DDoS, Brute-Force Web, por mencionar algunos, entonces tomando eso en cuenta, la finalidad de este proyecto es crear un algoritmo o modelo que pueda ser capaz de detectar la posible iniciación de algún tipo de ataque.

Alcance y Objetivos:

Como se mencionó anteriormente, la finalidad que se busca con este proyecto es crear un modelo que sea capaz de determinar un posible ataque, un ataque dirigido a una página web para especificar, para que tanto como futuras empresas o individuales, puedan optar a usar este modelo para prevenir o reaccionar ante un posible ataque, pero para llegar a este fin, nos basamos en los siguientes objetivos generales y específicos:

Generales:

- Crear un modelo funcional
- Identificar ataques conocidos
- Identificar múltiples ataques

Específicos:

- Crear un modelo que sea capaz de determinar ataques dirigidos.
- Crear un modelo que pueda identificar más de un ataque a la vez.
- Ejecutar un modelo adaptativo

Revisión de la literatura

Es importante que cada usuario conozca y comprenda las amenazas a las que se enfrenta en el entorno virtual, así como los riesgos que derivan de ellas, no solo para prevenir ser víctimas de los mismos, sino saber cómo actuar en caso de ser víctimas. Y estar conscientes de la difícil tarea que es en ocasiones ubicar al responsable beneficiado por el anonimato proporcionado por el entorno digital, que deriva en actos de impunidad en ocasiones ajenos incluso al actuar de las autoridades, por lo que el papel preventivo es de suma importancia. También concientizar sobre el uso responsable del internet, sobre todo para evitar que se cometan conductas que causen daño a terceros o incurran en un delito, por el desconocimiento que existe en relación con las afectaciones que conllevan determinadas acciones en el entorno virtual, que si bien parecieran a simple vista inofensivas, tienen grandes repercusiones en las víctimas (Hernández, Canizales & Páez, 2021).

Hay un libro llamado “Machine Learning Algorithms for Network Intrusion Detection” publicado en 2019, habla sobre algoritmos de aprendizaje automático para la detección de intrusiones. Cuenta que la intrusión en la red es una amenaza creciente con impactos potencialmente severos, que pueden dañar de múltiples maneras las infraestructuras de red y los activos digitales e intelectuales en el ciberespacio y el enfoque más comúnmente utilizado para combatir la intrusión en la red es el desarrollo de sistemas de detección de ataques a tráves de técnicas de aprendizaje automático y minería de datos.

En un artículo titulado “Network Intrusion Detection System using Deep Learning” publicado en el año 2021 cuenta que el uso generalizado de la interconectividad y la interoperabilidad de los sistemas informáticos se han convertido en una necesidad indispensable para mejorar nuestras actividades diarias, pero esto abre un camino a vulnerabilidades explotables que van mucho más allá de la capacidad de control humano. Se menciona que se puede usar aprendizaje automático para detectar los ataques en una red. Además, se muestran ciertos patrones que estos sigue para conocer cómo detectarlos.

Limpieza de datos:

https://github.com/AQ-ja/Proyecto-SDS/blob/main/ProyectoR/Limpieza.Rmd

Referencias

Hernández, E. F. T., Canizales, R. R., & Páez, A. V. (2021). La importancia de la ciberseguridad y los derechos humanos en el entorno virtual. *Misión Jurídica*, *14*(20), 142-158.

Li, J., Qu, Y., Chao, F., Shum, H.P.H., Ho, E.S.L., Yang, L. (2019). Machine Learning Algorithms for Network Intrusion Detection. In: Sikos, L. (eds) AI in Cybersecurity. Intelligent Systems Reference Library, vol 151. Springer, Cham. https://doi.org/10.1007/978-3-319-98842-9_6

Lirim Ashiku, Cihan Dagli,Network Intrusion Detection System using Deep Learning, Procedia Computer Science, Volume 185, 2021, Pages 239-247, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.05.025.