Resumen

En la actualidad el consumo de la tecnología sigue en crecimiento gracias a la demanda de recursos tecnológicos que ayudan acelerar procesos. De igual manera el uso de software amplía las posibilidades de encontrar vulnerabilidades en los sistemas informáticos. Por tanto, las exigencias en la seguridad de la información es cada vez trascendental aplicarlo en todo ámbito de trabajo, al ser las redes informáticas un punto crítico a analizar, debido a que toda la información fluye a través de las mismas.

Las redes informáticas por lo general tienen diversos mecanismos de seguridad como firewalls, IDS, IPS, entre otros, los cuales implementan diversas técnicas para el análisis de vulnerabilidades. La seguridad de las redes puede mejorar gracias a la aplicación de aprendizaje automático que mejora la detección de amenazas y las referidas vulnerabilidades.

La presente tesis tiene como objetivo desarrollar algoritmos de aprendizaje automático para el análisis y detección de tráfico malicioso, que incluye toda actividad inusual en el flujo de paquetes de datos, tales como los ataques DOS, XSS y ataques de fuerza bruta. Para lograrlo, se aplicó la metodología ágil SCRUM, que permitió generar un artefacto de software que comprende la arquitectura de cuatro capas funcionales con algoritmos de inteligencia artificial para la detección de tráfico malicioso en una red. Adicionalmente, se realizó una evaluación comparativa de algoritmos de machine learning y el desarrollo evolutivo referido. Como resultado, se entrega una solución práctica al CERT académico, que busca generar nuevo conocimiento que permita incrementar los niveles de seguridad cibernética de la universidad y del país.

Palabras clave: Tráfico malicioso, aprendizaje automático, vulnerabilidades, seguridad informática, CERT.

Abstract

Nowadays, technology consumption continues to grow thanks to the demand for technological resources that help speed up processes. In the same way, the use of software increases the possibility of finding vulnerabilities in computer systems. Therefore, the demands on information security are increasingly transcendental to apply in all areas of work, computer networks being a critical point to analyze because all information flows through them.

Computer networks generally have various security mechanisms, such as firewalls, IDS, and IPS, which implement different vulnerability analysis techniques. Network security can improve thanks to the application of automatic learning that enhances the detection of threats and the vulnerabilities mentioned above.

This thesis aims to develop automatic learning algorithms for the analysis and detection of malicious traffic, including any unusual activity in the flow of data packets, such as DOS attacks, XSS, and brute force attacks. The agile SCRUM methodology was applied, allowing the generation of a software artifact that includes the architecture of four functional layers with artificial intelligence algorithms for detecting malicious traffic in a network. Additionally, a comparative evaluation of machine learning algorithms and the referred evolutionary development was carried out. As a result, a practical solution is delivered to the academic CERT, which seeks to generate new knowledge that increases the levels of cyber security of the university and the country.

Keywords: Malicious traffic, machine learning, vulnerabilities, computer security, CERT**.**