Rancang Bangun Sistem Deteksi Multi-Serangan pada Zeek Network Security Monitor Menggunakan Machine Learning = Design and Implementation of a Multi-Attack Detection System for Zeek Network Security Monitor Using Machine Learning

Zulfikar hadzalic, author

Abstrak

Seiring berkembangnya teknologi, serangan siber menjadi semakin canggih dan beragam, sementara sistem keamanan jaringan tradisional menggunakan aturanaturan tetap yang sulit mendeteksi serangan baru. Penelitian ini bertujuan mengembangkan sistem deteksi serangan siber yang lebih pintar dengan menggunakan Machine Learning untuk meningkatkan kemampuan Zeek Network Security Monitor (NSM) dalam mendeteksi berbagai jenis serangan secara otomatis. Metodologi penelitian menggunakan dataset TOn_IOT yang dilakukan pengolahan data, kemudian membandingkan tiga algoritma Machine Learning yaitu Random Forest, XGBoost, dan LightGBM. Setelah dibandingkan, didapatkan model terbaik yaitu XGBoost dengan tingkat akurasi 93,28% dan F1-score 93,30% dalam mendeteksi sembilan jenis serangan siber seperti DoS, DDoS, scanning, dan ransomware. Model XGBoost kemudian digunakan untuk ekstraksi threshold menggunakan analisis kurva ROC dan presisi-recall untuk menemukan nilai batas optimal yang membedakan aktivitas normal dari mencurigakan, menghasilkan 31 threshold individual dengan rata-rata 3,4 threshold per serangan. Parameter threshold yang diekstrak berhasil diterapkan dalam script Zeek dan diuji pada lingkungan simulasi tiga komputer virtual dengan total 45 percobaan, terbukti mampu mendeteksi 39 dari 45 serangan dengan tingkat deteksi keseluruhan 86,7% dan memberikan peringatan otomatis melalui log Zeek. Penelitian ini membuktikan bahwa penerapan Machine Learning dapat secara signifikan meningkatkan kemampuan sistem keamanan jaringan dalam mendeteksi ancaman siber dibandingkan sistem konvensional, dengan ekstraksi threshold berbasis XGBoost menghasilkan parameter optimal untuk implementasi praktis pada Zeek NSM.

.....As technology advances, cyber attacks become increasingly sophisticated and diverse, while traditional network security systems use static rules that struggle to detect new attacks. This research aims to develop a smarter cyber attack detection system using Machine Learning to enhance Zeek Network Security Monitor (NSM) capabilities in automatically detecting various types of attacks. The research methodology uses the TOn_IOT dataset with data processing, then compares three Machine Learning algorithms: Random Forest, XGBoost, and LightGBM. After comparison, the best model was XGBoost with 93.28% accuracy and 93.30% F1- score in detecting nine types of cyber attacks such as DoS, DDoS, scanning, and ransomware. The XGBoost model was then used for threshold extraction using ROC curve and precision-recall analysis to find optimal boundary values that distinguish normal from suspicious activities, generating 31 individual thresholds with an average of 3.4 thresholds per attack. The extracted threshold parameters were successfully implemented in Zeek scripts and tested in a three virtual machine simulation environment with 45 total trials, proven capable of detecting 39 out of 45 attacks with an overall detection rate of 86.7% and providing automatic alerts through Zeek logs. This research proves that applying Machine Learning can significantly improve network security system capabilities in detecting cyber threats compared to conventional systems, with XGBoost-based threshold extraction producing optimal parameters for practical

implementation on Zeek NSM.