Universitas Indonesia Library >> UI - Skripsi Membership

Deteksi Serangan DOS pada CICIDS 2017 Menggunakan Machine Learning = DOS Attack Detection on CICIDS 2017 Using Machine Learning

Marinus Martin Dwiantoro, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=9999920544911&lokasi=lokal

---

Abstrak

Denial of Service adalah salah satu serangan siber yang dapat mengakibatkan gangguan layanan dan kerugian finansial. Akibat dari serangan DoS tentunya akan memberikan dampak buruk dan sangat merugikan. Untuk dapat menanggulangi dan meminimalisir dampak serangan DoS, dirancanglah sebuah sistem deteksi serangan DoS dan klasifikasi serangan yang terjadi menggunakan machine learning. Pada penelitian ini, akan dilakukan perancangan sistem deteksi serangan DOS melalui pengumpulan traffic data yang dikumpulkan oleh Wireshark dan dikonversi menggunakan CICFlowMeter. Serangan DoS dilancarkan oleh GoldenEye, HULK, dan SlowHTTPTest. Pengklasifikasian diterapkan pada salah satu dataset pada CICIDS2017, menggunakan algoritma Random Forest, AdaBoost, dan Multi-layer Perceptron. Hasil akurasi klasifikasi tertinggi adalah Random Forest sebesar 99,68%, hasil rata-rata Cross-Validation tertinggi juga dipegang oleh Random Forest sebesar 99,67%, dan untuk perbandingan performa antara hasil algoritma yang dilakukan oleh penulis dan paper konferensi DDOS Attack Identification using Machine Learning Techniques yang menjadi acuan, hasil yang paling mendekati adalah Random Forest dengan besar yang sama.

.....Denial of Service is a cyberattack that can result in service disruption and financial loss. The consequences of a DoS attack will certainly have a bad and very detrimental impact. To be able to overcome and minimize the impact of DoS attacks, a DoS attack detection system and classification of attacks that occur using machine learning was designed. In this research, a DOS attack detection system will be designed by collecting traffic data collected by Wireshark and converted using CICFlowMeter. DoS attacks were launched by GoldenEye, HULK, and SlowHTTPTest. Classification was applied to one of the datasets in CICIDS2017, using the Random Forest, AdaBoost, and Multi-layer Perceptron algorithms. The highest classification accuracy result is Random Forest at 99.68%, the highest average Cross-Validation result is also held by Random Forest at 99.67%, and for performance comparison between the algorithm results carried out by the author and the conference paper DDOS Attack Identification using Machine Learning Techniques are the reference, the closest result is Random Forest with the same size.