Pengembangan multi-stage detection method berbasis machine learning untuk meningkatkan akurasi dan efisiensi intrusion detection system (IDS) pada sistem monitoring keamanan jaringan internet Indonesia = Development of machine learning based multi-stage detection method for improving accuracy and efficiency of intrusion detection system (IDS) on Indonesia internet security monitoring system

Bisyron Wahyudi, author

Abstrak

ABSTRAK
Salah satu komponen penting dalam Sistem Monitoring Keamanan Jaringan adalah Intrusion Detection System IDS yang berfungsi untuk mendeteksi setiap potensi serangan yang mengancam keamanan jaringan. Keunggulan sebuah IDS ditentukan oleh kemampuannya untuk mendeteksi serangan siber secara akurat dan mudah beradaptasi terhadap perubahan lingkungan sistem yang terus berkembang. Sebuah IDS yang akurat mampu mendeteksi berbagai jenis serangan secara tepat dengan sedikit kesalahan deteksi false alarm .Penelitian ini merancang dan mengimplementasikan metode machine learning ke dalam IDS yang digunakan untuk mendeteksi serangan dalam jaringan sebenarnya secara akurat dan cepat. Dalam pengembangan model machine learning untuk IDS ini digunakan dataset KDDCUP rsquo;99 dan NSL-KDD. Dengan melakukan analisis pemilihan fitur diperoleh subset 28 fitur dari total 41 fitur dataset KDD yang paling relevan dan dapat diimplementasikan dalam jaringan sebenarnya. Dalam pengembangan model machine learning diperoleh hasil bahwa metode terbaik adalah menggunakan SVM.Pada tahap implementasi digunakan metode multi-stage detection yang memberikan hasil deteksi serangan yang lebih cepat dan akurat. Hasil ujicoba model IDS yang telah dikembangkan menggunakan metode machine learning dengan implementasi multi-stage detection mampu mendeteksi serangan dengan tingkat akurasi sampai 99,37 . Lebih jauh lagi, kecepatan proses deteksi meningkat dengan rata-rata 24 pada data testing dan rata-rata 10 pada lingkungan jaringan sebenarnya.
<hr />
ABSTRACT
An important component in Network Security Monitoring System is Intrusion Detection System IDS . IDS serves to detect any potential attacks that threaten network security. The reliability of an IDS is determined by its ability to detect cyber attacks accurately, and to dynamically adapt to ever-evolving system environment changes. An accurate IDS is able to detect different types of attacks appropriately with minimum false alarm.This research designs and implements machine learning method into IDS to detect actual network attacks accurately and quickly. In the development of machine learning model for IDS, KDDCUP 39;99 and NSL-KDD dataset are used. By performing feature selection analysis, a subset of 28 most relevant features of a total of 41 features of KDD dataset is obtained and can be implemented in the actual network. In the development of machine learning model it is found that the best method for our approach is by using SVM.In the implementation phase the proposed multi-stage detection method provides faster and more accurate attack detection. The experiments also show that combining machine learning method with multi-stage detection implementation improves detection accuracy up to 99.37 . Further, the

proposed method increases the average speed of detection process up to 24 in data testing and up to 10 average in the real network environment.