INTISARI

Klasifikasi Alarm *Intrusion Detection System* Berdasarkan Tingkat Potensi Kerusakan Jaringan Mengsgunakan Metode *Machine Learning*

Oleh

Muflihanto
16/398522/PA/17483

Snort adalah sebuah *packet sniffer* dan *logger* yang dapat digunakan sebagai sistem deteksi intrusi jaringan (NIDS). *Snort* dapat melakukan analisis protokol, pencarian/pencocokan konten, dan dapat digunakan untuk mendeteksi berbagai serangan dan *probe*. Mode NIDS Snort menghasilkan laporan log alarm yang berisi detail serangan serta label prioritas dari setiap serangan. Dalam pengujian menggunakan *Metasploit framework* pada jaringan, *Snort* menghasilkan laporan dengan tingkat alarm *false positive* sebesar 56,2%.

Machine Learning adalah sebuah metode yang dapat digunakan untuk menghasilkan ekspresi pengklasifikasian yang cukup sederhana untuk dipahami dengan mudah oleh manusia. Sejumlah penelitian menggunakan beberapa jenis model *machine learning* untuk meringkas dan mengategorikan alarm intrusi. Beberapa model yang digunakan adalah *Decision Tree*, *Support Vector Machine* (SVM), *AdaBoost* dan *XGBoost*.

Penelitian ini menjabarkan analisis komparasi performa beberapa model *machine learning* yaitu *Decision Tree*, *Support Vector Machine* (SVM), *AdaBoost* dan *XGBoost* dalam mengelompokkan alarm *Snort* saat mendeteksi serangan dalam *dataset* ISCXIDS2012. Pada percobaannya, dilakukan pengelompokan alarm *Snort* dengan dan tanpa alarm *false positive*.

Dari hasil penelitian yang diperoleh, didapatkan bahwa penerapan metode *machine learning* dapat digunakan untuk mengelompokkan alarm *Snort* dan mengurangi tingkat *false positive*. Alarm *Snort* dapat dikelompokkan ke dalam 3 kelas prioritas serangan dan 1 kelas alarm *false positive*. Akurasi model dalam mengelompokkan alarm ke dalam 3 kelas prioritas dan 1 kelas alarm *false positive* berkisar antara 90,6% hingga 98,4%. Pada *dataset* laporan *Snort* dengan tingkat *false positive* 26,77%, sebuah model *XGBoost* yang merupakan *classifier* dengan performa terbaik mampu menurunkan tingkat alarm *false positive Snort* hingga mencapai angka 0,39%.

Kata kunci: pembelajaran mesin, IDS, sistem deteksi intrusi, snort, decision tree, support vector machine, adaboost, xgboost

ABSTRACT

Classification of Intrusion Detection Systems Alarm Based on The Level of Potential Network Damage Using Machine Learning Methods

By

Muflihanto

Snort is a packet sniffer and logger that can be used as a network intrusion detection system (NIDS). Snort can perform protocol analysis, content searching/matching, and can be used to detect various attacks and probes. Snort NIDS mode generates alarm reports containing attack details as well as priority labels of each attack. In a test using the Metasploit framework on the network, Snort produced a report with a false positive alarm rate of 56.2%.

Machine learning is a method that can be used to produce classification expressions that are simple enough to be understood easily by humans. Several studies use several types of machine learning models to summarize and categorize intrusion alarms. Some of the models used are Decision Tree, Support Vector Machine (SVM), AdaBoost and XGBoost.

This study describes a comparative analysis of the performance of several machine learning models namely Decision Tree, Support Vector Machine (SVM), AdaBoost and XGBoost in grouping Snort alarms when detecting attacks in the ISCXIDS2012 dataset. In the experiment, Snort alarm grouping was done with and without false positive alarms.

From the results of the research obtained, it was found that the application of machine learning methods can be used to group Snort alarms and reduce false positive alarm. Snort alarms can be grouped into 3 attack priority classes and 1 false positive alarm class. The accuracy of the model in grouping alarms into 3 priority classes and 1 class of false positive alarms ranges from 90.6% to 98.4%. In the Snort report dataset with a false positive rate of 26.8%, XGBoost model that is the best performing classifier is able to lower the Snort false positive rate to 0.39%.

Keywords: machine learning, IDS, intrusion detection system, snort, decision tree, support vector machine, adaboost, xgboost.