ANALISIS SELEKSI FITUR DALAM MENENTUKAN SERANGAN MENGGUNAKAN ALGORITMA *DECISION TREE*

Hidayah Husnul Khotimah

ABSTRAK

Kejahatan siber (*cyber crime*) adalah kejahatan pada dunia maya yang memanfaatkan teknologi dan telekomunikasi sebagai medianya. Salah satu kejahatan siber adalah serangan siber (*cyber attack*). Serangan siber merupakan serangan terhadap sistem informasi, infrastruktur, jaringan komputer, serta sistem keamanan komputer. Oleh karena itu, perlu adanya alat yang dapat digunakan untuk mendeteki serangan yang disebut sebagai *Intrusion Detection System* (IDS). Hasil dari IDS ini berupa *log* serangan yang nantinya akan dianalisa menggunakan *Security Event Management* (SEM) oleh administrator keamanan jaringan. Agar administrator keamanan jaringan lebih mudah dalam menganalisa SEM, diperlukan metode seleksi fitur yang berfungsi untuk menentukan fitur-fitur apa saja yang berpengaruh dalam mendeteksi serangan. Metode yang digunakan dalam seleksi fitur adalah *ranking importance* dengan algoritma klasifikasi *decision tree* sebagai penghitungan akurasi. Dari hasil penelitian didapat fitur-fitur penting, yang terdiri dari *source ip*, *source port*, *signature id*, *rev*, *signature*, *severity*, *source city name*, *destination regional name*, dan *destination city name* dengan akurasi klasifikasi sebesar 99.97%, waktu pelatihan selama 0.021208 s, serta waktu pengujian selama 0.001554 s.

Kata kunci: Kejahatan Siber, Serangan Siber, IDS, SEM, *ranking importance*, *Decision Tree*.

ANALYSIS OF FEATURES SELECTION IN DETERMINING THE ATTACK USING DECISION TREE ALGORITHM

Hidayah Husnul Khotimah

ABSTRACT

Cybercrime is a crime in cyberspace that utilizes technology and telecommunications as its medium. One of the cybercrime is cyber attack. Cyber attack is an attack on information systems, infrastructure, computer networks, and computer security systems. Therefore, there needs to be a tool that can be used to detect an attack called the Intrusion Detection System (IDS). The result of this IDS is in the form of an attack log which will later be analyzed using Security Event Management (SEM) by the network security administrator. To make network security administrators easier to analyze SEM, a feature selection method is needed that functions to determine what features are influential in detecting attacks. The method used in feature selection is importance ranking with the decision tree classification algorithm as an accuracy calculation. From the research results obtained important features, which consist of source ip, source port, signature id, rev, signature, severity, source city name, destination regional name, and destination city name with classification accuracy of 99.97%, training time for 0.021208 s, as well as the testing time of 0.001554 s.

Keyword: Cybercrime, Cyber Attack, IDS, SEM, ranking importance, Decision Tree.