INTISARI

ANALISIS PERBANDINGAN KINERJA DETEKSI SERANGAN PADA IMPLEMENTASI *SURICATA* DAN *SNORT* SEBAGAI *HOST INTRUSION DETECTION SYSTEM* DI *UBUNTU SERVER*

Perkembangan teknologi informasi yang cepat menuntut peningkatan sistem keamanan yang memadai. *Intrusion Detection System* (*IDS*) merupakan salah satu pilihan yang difungsikan untuk meningkatkan keamanan jaringan baik jaringan intranet maupun internet. Penerapan *IDS* digunakan sebagai salah satu solusi yang dapat digunakan untuk membantu seorang administrator dalam memantau dan menganalisis paket-paket berbahaya yang dikirimkan ke *server*. Terdapat berbagai macam jenis *IDS* yang tersedia, antara lain *snort* dan *suricata* yang merupakan *open source IDS* dan dapat diterapkan pada sebuah *server*.

Analisis perbandingan aplikasi *IDS* antara *suricata* dan *snort* bertujuan untuk mengukur kinerja deteksi dari sebuah serangan yang menuju ke *host*, dengan parameter jumlah deteksi, kecepatan deteksi serangan serta penggunaan sistem *resource* pada *host* yang terpasang *IDS*. Pengukuran dilakukan dengan simulasi menggunakan mesin virtual dan serangan berasal dari aplikasi *pytbull*. Deteksi serangan ditampilkan pada *web snorby*. Hasil dari pengujian, kinerja *Suricata* lebih baik dalam jumlah serangan yang berhasil terdeteksi dan kecepatan deteksi secara umum. *Snort* lebih efisien dalam penggunaan *resource* sistem.

Kata kunci: *intrusion detection system*, *snorby*, *snort*, *suricata*, *ubuntu*.

ABSTRACT

ANALYSIS OF DETECTION PERFORMANCE COMPARISON ON SURICATA AND SNORT IMPLEMETATION AS HOST INTRUSION DETECTION SYSTEM ON UBUNTU SERVER

The rapid development of information technology demands an adequate security system. Intrusion Detection System (IDS) is one option that is enabled to improve network security both on intranet and internet networks. IDS application is used as one solution that can be used to help an administrator in monitor and analyze malicious packages sent to the server. There are various types of IDS, namely snort and suricata are open source IDS that can be applied to server.

Analysis comparison of IDS applications between suricata and snort aims to measure the level of detection performance of an attack to the host, with parameter total and speed of detection and system reseources used by IDS in a host. Measurements with simulation using virtual machines and attack from pytbull. Attack detection displayed with snorby web framework. As a result of test, Suricata performance is better in the number of detected attacks and detection speed in general. Snort is more efficient in using system resources.

Keywords: intrusion detection system, snorby, snort, suricata, ubuntu.