ABSTRACT

Web servers are often the target of Denial of Service (DoS) attacks so that they become difficult to access because they run out of resources. This condition makes the client unable to access any data from the server. Application of Intrusion Detection System (IDS) is one solution to overcome this. The selection of the right IDS tools is important before being applied to a computer network, because each tool has its own advantages and disadvantages. The purpose of this research is to measure the performance of IDS tools. Snort and Suricata were chosen to be used in experiments in this study which were tested with three types of Denial of Service (DoS) attacks: syn flooding, XMAS flood, and slowloris. The results of the experiments in this study show that Snort has a better detection performance against xmas flood attacks of 4.9% which was detected from the total packets sent and has a lower CPU usage than Suricata against syn flooding and xmas flood attacks with its usage of 53.05% for syn flooding and 70.42% for xmas flood attacks. Based on the slowloris attack, the best application to detect this attack is suricata, good detection performance in the suricata application is accompanied by lower CPU and memory usage, namely 7.6% CPU usage and 17% memory usage.

Keyword : ***Denial of Service , Intrusion Detecting System, Snort, Suricata, Web Server***

ABSTRAK

Web server sering kali menjadi sasaran penyerangan *Denial of Service* (DoS) sehingga menjadi sulit diakses karena kehabisan sumber daya. Kondisi tersebut membuat *client* tidak dapat mengakses data apa pun dari *server*. Penerapan *Intrusion Detection System* (IDS) merupakan salah satu solusi untuk mengatasi hal tersebut. Pemilihan tools IDS yang tepat, penting dilakukan sebelum diterapkan pada jaringan komputer, karena setiap *tools* mempunyai kelebihan dan kekurangannya masing-masing. Tujuan dari penelitian ini untuk mengukur kinerja tools IDS. *Snort* dan *Suricata* dipilih untuk digunakan pada percobaan dalam penelitian ini yang diuji dengan tiga jenis serangan *Denial of Service* (DoS) : *syn flooding, XMAS flood,* dan *slowloris*. Hasil dari percobaan pada penelitian ini, menunjukan *snort* mempunyai performa deteksi yang lebih baik terhadap serangan *xmas flood* sebesar 4,9% yang terdeteksi dari total paket yang dikirim dan memiliki penggunaan CPU yang lebih rendah dari *suricata* terhadap serangan *syn flooding* dan *xmas flood* dengan penggunaannya sebesar 53,05% untuk *syn flooding* dan 70,42% untuk serangan *xmas flood*. Berdasarkan serangan *slowloris* aplikasi terbaik untuk mendeteksi serangan ini adalah *suricata,* performa deteksi yang baik pada aplikasi *suricata* disertai dengan penggunaan CPU dan memori yang lebih rendah yaitu 7,6% penggunaan CPU dan 17% penggunaan memori.

Kata Kunci : ***Denial of Service , Intrusion Detecting System, Snort, Suricata, Web Server***