ABSTRAK

IT Telkom Jakarta sebagai suatu institut Pendidikan memandang bahwa optimalisasi penggunaan website menjadi prioritas tersendiri ditambah lagi IT Telkom Jakrta memiliki beberapa bisnis proses yang mengandalkan data digital antara lain data akademik yang tersimpan dalam satu server. Melihat dari pentingnya website maka diperlukan peningkatan keamanan untuk website ini. Apalagi website IT Telkom Jakarta yang dapat diakses oleh banyak user melalui jaringan Local Area Network (LAN) berbasis wired maupun wireless fidelity (Wifi). Maka dari itu menjaga keamanan pada web diperlukan untuk mengatasi user yang melakukan serangan dan melindungi web dari ancaman informasi yang sangat beragam. Untuk menjaga keamanan terhadap serangan keamanan tersebut, dibutuhkan sistem yang dilengkapi dengan firewall dan *Intruction Detection System* (IDS). IDS yang digunakan adalah OPNsense, dimana pada OPNsense ini terdapat Suricata. Suricata ini merupakan salah satu solusi terkait permasalahan keamanan. *Suricata* adalah perangkat lunak pendeteksi dan sekaligus pencegah gangguan atau *Intrusion Detection and Prevention System* (IDPS) *open source* yang merupakan generasi lanjutan dari IDS/IPS. Hasil dari implementasi OPNsense Suricata yaitu Suricata dapat mencegah serangan dengan cara memblokir serangan. Dimana pada saat melakukan scanning dan pengujian DDOS maka di sistem OPNsense akan mencatat loh serangan, mengirimkan notifikasi serngan dan memblokir serangan.

Kata kunci : OPNsense, DDOS, Suricata, Website, IDS, Firewall.

ABSTRACT

IT Telkom Jakarta as an educational institute views that optimizing the use of the website is a priority, plus IT Telkom Jakarta has several business processes that rely on digital data, including academic data stored on one server. Seeing the importance of the website, it is necessary to increase security for this website. Moreover, the IT Telkom Jakarta website can be accessed by many users via a wired or wireless fidelity (Wifi)-based Local Area Network (LAN). Therefore, maintaining security on the web is needed to overcome users who carry out attacks and protect the web from various information threats. To maintain security against these security attacks, a system equipped with a firewall and an Instruction Detection System (IDS) is needed. The IDS used is OPNsense, where in this OPNsense there is Suricata. Suricata is one solution related to security problems. Suricata is an open source Intrusion Detection and Prevention System (IDPS) which is the next generation of IDS/IPS. The result of the implementation of OPNsense Suricata is that Suricata can prevent attacks by blocking attacks. Where when scanning and testing DDOS, the OPNsense system will record attacks, send attack notifications and block attacks.

***Keywords**:* OPNsense, DDOS, Suricata, Website, IDS, Firewall.