ABSTRAK

Keamanan informasi berfungsi untuk menghindari kerusakan atau kehilangan yang disebabkan oleh aktivitas penyerangan selama proses komunikasi. Aspek keamanan informasi yaitu *Confidentiality, Integrity* dan *Availability. Web server* merupakan penyedia layanan yang digunakan untuk menerima permintaan HTTP yang bekerja pada *port* 80 dimana paling rentan dengan ancaman serangan. Ancaman serangan yang dapat terjadi pada *web server* yaitu *Port Scanning, Brute Force* dan DDoS. *Intrusion Prevention System* merupakan solusi yang dapat menjaga keamanan jaringan dari berbagai serangan. *Intrusion Prevention System* berperan sebagai pelindung pada jaringan dengan mendeteksi sekaligus mencegah jika terdapat trafik yang mencurigakan dalam suatu jaringan. Pada penelitian ini *Intrusion Prevention System* menggunakan *tools* Snort dan *IPTables* serta dengan metode *signature based detection*. Pengujian dilakukan dengan menggunakan dua skenario yaitu sebelum IPS diaktifkan dan sesudah IPS diaktifkan. Hasil dari penelitian yaitu ketiga serangan yang diujikan memiliki karakteristik yang berbeda dari sebab dan akibatnya. Serangan *Port Scanning* dan *Brute Force* dapat dicegah oleh IPS karena karakterisktik kedua serangan tersebut mudah dikenali oleh *rule* pada *database* Snort. Pada serangan DDoS, Snort hanya mempercepat waktu serangan untuk dapat diakses kembali karena karakteristik serangan Slow HTTP yaitu mengirimkan paket tidak lengkap dengan jumlah banyak secara bertahap dan mempertahankan waktu sesi koneksi sehingga sulit dikenali oleh Snort. Pada serangan DDoS dengan *action rule drop, web server* dapat diakses kembali pada detik 160 sedangkan pada *action rule reject* dapat diakses kembali pada detik 145 dimana waktu normal serangan dapat diakses kembali yaitu pada detik 165. Pada penggunaan CPU *usage,* IPS dapat menurunkan penggunaan sebesar 9,2% pada serangan DDoS.

Kata Kunci : *Intrusion Prevention System*, Snort, Triad CIA