ABSTRAK

Perubahan besar telah terjadi dalam dunia jaringan komunikasi seiring dengan kemajuan teknologi dalam beberapa dekade terakhir. Salah satu kemajuan yang signifikan adalah adopsi *Software Defined Network* (SDN), yang memberikan tingkat fleksibilitas dan kendali yang tinggi terhadap infrastruktur jaringan. Namun meningkatnya pemanfaatan *SDN* juga membuka potensi risiko keamanan, khususnya terkait serangan *Denial of Service* (DoS). Penelitian ini bertujuan untuk mengatasi tantangan tersebut dengan mensimulasikan Intrusion Detection System (IDS) berbasis *Snort* di SDN menggunakan *Floodlight Controller*. Penelitian ini mengkonfigurasi *Host*, IDS *Snort*, SDN *Controller*. Skenario pada penelitian ini menggunakan 10 skrenario dengan jumlah paket dan ukuran paket yang berbeda. Selanjutnya simulasi serangan DoS menggunakan *flood attack*, parameter penelitian ini diantaranya, waktu respons, Dimana waktu respons disini adalah seberapa lama IDS mendeteksi serangan, akurasi deteksi seberapa akurat IDS mendeteksi serangan, dan beban kerja, seberapa besar *memory*, *Central Processing Unit* CPU, dan bandwidth pada perangkat keras. Hasil penelitian menunjukkan bahwa waktu respons sistem IDS *Snort* meningkat seiring dengan intensitas serangan DoS yang diluncurkan, yaitu dari 2,37 menit pada serangan ringan (100 paket, 64 *Byte*) hingga 11,40 menit pada serangan berat (50.000 paket, 32.768 *Byte*). Meskipun begitu, IDS *Snort* berhasil mendeteksi di semua skenario pengujian. Dalam hal beban kerja, penggunaan memori meningkat dari 54,86 MB hingga 77,27 MB, penggunaan CPU meningkat dari 28,75% hingga 50,53%, dan bandwidth yang digunakan meningkat dari 6.899,40 KBps hingga 74.258,45 KBps. Kesimpulannya, IDS *Snort* terbukti efektif dalam mendeteksi serangan DoS dengan akurasi yang sangat tinggi dan mampu menangani peningkatan intensitas serangan.

Kata Kunci: *Intrusion Detection System*, *Snort*, *Denial of Service*, *Software Defined Network, Floodlight Cobntroller*, Keamanan Jaringan