ABSTRAK

Web server adalah perangkat yang memberikan layanan berbasis paket data kepada klien melalui protokol HyperText Transfer Protocol (HTTP). Protokol ini memberikan layanan berbagi informasi melalui World Wide Web (WWW) dimana klien akan meminta informasi dari suatu website dan web server akan memberikan informasi yang diminta. Berdasarkan data pengukuran yang dikeluarkan oleh McAfee Labs, selama tahun 2016 36% dari serangan di jaringan menyerang Web Server. Salah satu serangan yang digunakan adalah Denial of Service (DOS) yaitu penyerangan dengan satu *Attacker* dan Distributed Denial of Service (DDOS) yaitu penyerangan dengan lebih dari satu *Attacker* yang bertujuan untuk membuat Server terganggu bahkan dapat merusak *Hardware* dari Server tersebut. Oleh karenanya banyak metode ditawarkan untuk menjaga Server agar tetap stabil, salah satunya adalah Host Intrusion Prevention System (HIPS).

Tugas Akhir ini mengukur kinerja dari HIPS dengan cara membuat implementasinya di jaringan virtual yang juga dilengkapi dengan pertahanan Snort di sisi Server. Penggunaan Snort adalah karena mampu mendeteksi dan melakukan *drop* terhadap paket data yang terindikasi sebagai serangan DOS dan DDOS dengan *tool attack TCP SYN Flood*. Implementasi ini terdiri dari beberapa komponen, Server menggunakan sistem operasi Linux Ubuntu, penyerang menggunakan sistem operasi Linux Kali dan klien yang mengakses informasi pada web server menggunakan sistem operasi Linux Ubuntu.

Dari hasil beberapa pengujian, jumlah rata-rata paket serangan yang dikirimkan ke Server dengan 4 *Attacker* selama 1 menit mencapai 2.454.930. Serangan yang berhasil dideteki dan di*drop* mencapai 97.8 % atau 2.402.626, dan sekitar 2.19 % atau 52.304 paket yang terlewat.

Kata kunci : Web Server, HIPS, DOS, DDOS, Snort dan TCP SYN Flood