ABSTRAK

Denial of Service (DOS) dan *Distributed Denial of Service (DDOS)* adalah bentuk serangan yang kerap terjadi belakangan ini yang memungkinkan terhentinya suatu layanan pada *server* tertentu. Layanan yang sering menjadi target serangan yaitu layer aplikasi (layer 7) seperti layanan HTTP, FTP, SMTP dan lainnya. Layanan-layanan tersebut menjadi bagian vital dari kehidupan di era digital saat ini, pelanggan yang mengakses layanan server tersebut jumlahnnya mencapai jutaan bahkan lebih sehingga keamanan jaringan menjadi salah satu keutamaan dalam menjaga kualitas layanan *server*.

Dalam tugas akhir ini dibuat sebuah jaringan implementasi virtuallisasi dimana akan dilakukan simulasi serangan DOS dan DDOS terhadap *Web server* dengan layanan HTTP yang dilengkapi sebuah pertahanan berbasis *Network Intrusion Prevention System* (NIPS) yaitu Snort. Komponen-komponen yang digunakan kali ini semua bersifat virtual karena terkandung di dalam area *Hypervisor*, mulai dari *Web server* virtual yang dibentuk menggunakan sistem operasi berbasis Debian yaitu Linux Ubuntu, pihak penyerang berupa VM yang dioperasikan dengan sistem operasi Kali Linux, pertahanan yang dibentuk dengan VM Linux Ubuntu, hingga *client* yang berfungsi untuk mengakses konten layanan di kala penyerangan terjadi juga dibentuk dengan VM Linux Ubuntu.

Serangan yang berhasil di deteksi dan ditahan untuk memasuki area DMZ mencapai 1.063.713 serangan dengan beragam tingkat kerusakan, 98 % serangan yang berhasil direkap merupakan serangan torshammer dengan tingkat kerusakan yang tinggi, begitu pula pembebanan kinerja terhadap serangan tersebut lebih besar daripada serangan pertama, Nmap HTTP *Brute Force*, dengan peningkatan pembebanan kinerja *resource* sebesar 30 - 50 %

Kata kunci : DOS, DDOS, Web server, NIPS, Snort, Ubuntu, Kali Linux