ABSTRAK

Sistem keamanan pada jaringan komputer pada saat ini masih banyak cara untuk melakukan serangan kepada target yang ingin dituju seperti serangan DoS (*Denial of Service*) dan DDoS (*Distribute-Denial of Service*). DoS dan DDoS *attack* merupakan salah satu metode serangan yang dapat mengakibatkan kerugian pada target yang mengalami serangan ini seperti rusaknya beberapa berkas yang ada pada komputer atau laptop, komputer atau laptop berjalan menjadi lambat. Sehingga kita perlu mengetahui segala jenis pertahanan dari serangan DoS dan DDoS menggunakan beberapa metode seperti HIPS Snort dan *firewall* yang nantinya akan menjadi tembok utama sebelum paket-paket yang dianggap tidak aman memasuki jaringan komputer yang kita perlu amankan data atau *file* yang ada pada komputer atau laptop target dari serangan tersebut yang nantinya akan dilakukan analisis dan perbandingan antara beberapa metode pertahanan yang akan saya buat sehingga dapat menyimpulkan metode manakah yang paling efesien untuk melakukan pertahanan dari DoS dan DDoS *attack*.

HIPS (*Host Intrusion Prevention System*) merupakan salah satu saran penulis untuk menjadi pertahanan pada serangan DoS dan DDoS *attack* karena pada metode ini dapat mendeteksi terhadap aktifitas yang tidak normal, IPS (*Intrusion Prevention System*) akan melakukan pencegahan selanjutnya dengan tujuan menjaga agar jaringan tetap aman dan tidak ada gangguan pada jaringan komputer. HIPS Snort dan *firewall* juga dapat membantu untuk mendeteksi dan mencegah berbagai serangan seperti DoS dan DDoS yang masuk pada suatu jaringan komputer.

Dengan adanya metode yang dilakukan berupa HIPS Snort dan *Firewall* sebagai pertahanan dari serangan DoS dan DDoS. Dapat di simpulkan lebih baik HIPS Snort dibandingkan dengan *Firewall*, karena HIPS Snort dapat mendapatkan paket *drop* dengan angka persentase yang mendekati angka 100%, sedangkan pada sisi firewall sederhana tidak dapat menampilkan persentase paket *drop*.

Kata Kunci : HIPS, snort, DoS, DDoS, serangan, pertahanan.