ABSTRAK

Seiring berkembangnya teknologi, khususnya keamanan jaringan yang semakin berkembang menuntut agar sistem keamanan untuk dapat mencegah terjadinya sebuah ancaman ataupun serangan terhadap suatu sistem. Seperti halnya berusaha mendapatkan suatu informasi seperti halnya username dan *password*, atau melakukan serangan serangan seperti DDoS *(Distributed Denial of Service), Nmap, HPING3* dan lainya.

Dalam proyek akhir ini dibuat sebuah sistem pencegah serangan yang dapat mengidentifikasi serangan ataupun ancaman yaitu *Intrusion Prevention System* (IPS). Dimana sistem ini merupakan perpaduan beberapa *software* yaitu suricata, snorby, barnyard2 yang saling terintegrasi kemudian diuji dengan DDoS *(Distributed Denial of Service),* Nmap, HPING3 dan lainya. IPS dapat mencegah serangan yang akan masuk ke jaringan local dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor saat serangan teridentifikasi.

Adapun data yang diperoleh : serangan yang paling besar berupa SURICATA STREAM ESHTABLISHED retransmission packet before last ack mencapai 96,28%, SURICAT STREAM ESHTABLISHED SYNK resend dengan presentase 1,89% dan SURICATA STREAM ESHTABLISHED SYNK resend with different ACK dengan persentase 0,98%. *Drop* serangan dilakukan menggunakan *tools* Iptables berhasil dilakukan dengan mendrop sebanyak 543K paket yang terdeteksi sebagai serangan DDoS.

Kata Kunci: *IPS, DDoS*, mendeteksi, mencegah

.