ABSTRAK

Lalu lintas jaringan sangat penting untuk dijaga keamanannya karena pengiriman dan penerimaan data terjadi pada lalu lintas jaringan. Tidak menutup kemungkinan lalu lintas jaringan lepas dari gangguan serangan. Gangguan dalam penelitian ini disebut *Distributed Denial of Service* atau biasa dikenal DDoS, DDoS membanjiri lalu lintas jaringan sehingga *client* asli tidak dapat mengakses internet. Jenis serangan DDoS yang digunakan pada penelitian ini TCP dan UDP *flood,* serangan TCP membanjiri lalu lintas jaringan dengan mengirimkan data dalam jumlah besar secara terus-menerus, sementara UDP dapat membanjiri *port* pada *host* dengan mengirimkan paket-paket data ke banyak *port*, menyebabkan *host* menjadi tidak responsif. Dibutuhkan sistem keamanan jaringan seperti IDS yang dapat mendeteksi serangan yang masuk. Agar dapat berjalan sesuai fungsinya, IDS harus dijalankan dengan *tools*. Penelitian ini mengunakan zeek dan suricata sebagai *tools*, dan akan dilakukan perbandingan pada *tools* yang digunakan terhadap serangan yang masuk kedalam sistem. Untuk mengetahui tingkat akurasi jumlah serangan yang terdeteksi oleh *tools*, penelitian ini menggunakan parameter *confusion matrix* yang terdiri dari *accuration*, *precision*, dan *recall*. Hasil yang didapatkan suricata lebih unggul dalam mendeteksi serangan TCP *flood* dengan *accuration* 93,36%, *precision* 100%, *recall* 93,36%, namun dalam mendeteksi serangan UDP *flood* Zeek lebih baik dengan nilai *accuration* 63,33%, *precision* 100%, *recall* 63,33%

Kata kunci: DDoS, IDS, Zeek, Suricata, *Confusion Matrix.*