ABSTRAK

Keamanan jaringan menjadi hal utama yang dibutuhkan untuk mengamankan data. Karena semakin berkembangnya teknologi informasi maka serangan yang dilakukan oleh penyerang juga sangat bermacam-macam. Untuk mencegah resiko terkena serangan, maka dibutuhkan langkah dalam pencegahan dengan suatu sistem untuk mengamankan jaringan agar data yang dimiliki oleh target tidak disalahgunakan oleh penyerang. Salah satu sistem yang dapat digunakan untuk mencegah resiko terkena serangan yaitu *Intrusion Detection System* (IDS) yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah jaringan.

Metode deteksi *Anomaly-Based* dipilih agar dapat mendeteksi aktivitas yang mencurigakan dan tidak normal bagi sistem yang tidak dapat dilakukan oleh metode *Signatured-based.* Pada penelitian ini dilakukan pengujian serangan menggunakan tiga tools DoS yaitu tools LOIC, Torshammer dan Xerxes dengan scenario pengujian yaitu menggunakan IDS serta tanpa IDS.

Dari hasil pengujian yang telah dilakukan IDS berhasil mendeteksi serangan yang dikirim, untuk pengiriman paket serangan terbanyak berurutan yaitu Torshammer, Xerxes dan LOIC. Pada pendeteksian tools serangan Torshammer kepada target FTP Server didapatkan sebanyak 9525 paket, untuk tools Xerxes yaitu sebanyak 10777 paket dan tools LOIC sebanyak 6166 paket. Sedangkan serangan kepada target Web Server untuk tools torshammer sebanyak 320 paket, untuk tools Xerxes sebanyak 473 paket dan untuk tools LOIC sebanyak 60 paket. Akurasi dari hasil performansi IDS yaitu sebesar 88,66%, presisi sebesar 88,58% serta false positive rate sebesar 63,17%.

Kata kunci: Keamanan Jaringan, *Intrusion Detection System, Anomaly-Based, Denial of Service*