ABSTRAK

Perkembangan keamanan jaringan sangat dibutuhkan seiring berkembangnya teknologi saat ini. Meningkatnya teknologi yang semakin canggih menimbulkan berbagai tindak kejahatan Banyaknya penyerang yang tidak bertanggung jawab seperti merusak sistem, melakukan pencurian data serta pemalsuan data yang dapat merugikan pemiliknya. Dengan hal ini keamanan jaringan membutuhkan sistem yang dapat mendeteksi serta mencegah adanya serangan seperti *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS). Berdasarkan permasalahan tersebut, pada penelitian ini melakukan pengamanan dengan aplikasi Snort3 sebagai NIPS untuk mengamankan PC *Server*. Dalam hal ini, IPS yang berada pada PC *Router* juga dilengkapi *Demilitarized Zone* (DMZ) yang digunakan sebagai jalur komunikasi paket data. Rancangan tersebut dilakukan untuk diuji coba menggunakan serangan *brute force*, *Man-in-The-Middle* (MiTM) dan *Distributed Denial of Service* (DDoS). Pengujian yang dilakukan berupa mendeteksi dan mencegah serangan yang sudah terdaftar di *rules* serta serangan yang tidak terdaftar atau dapat disebut sebagai anomali. Selain itu melakukan perbandingan penggunaan sumber daya saat serangan tanpa pengamanan dan setelah adanya pengamanan. Hasil dari penelitian ini bahwa aplikasi Snort3 dapat mencegah dari serangan dengan akurasi sebesar 100%, serta dapat melakukan deteksi dan pencegahan serangan yang bersifat anomali menggunakan pemantauan *checksum filter* paket berbahaya.

Kata kunci: *Network-based Intrusion Prevention System* (NIPS), Snort3, *Demilitarized Zone* (DMZ), *brute force, Man-in-The-Middle* (MiTM), *Distributed Denial of Service* (DDoS).