SARI

Server menjadi hal yang perlu mendapat perhatian lebih mengenai tingkat keamanannya. *Server* yang memiliki celah kelemahan dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Data-data yang seharusnya bersifat pribadi bisa saja disalahgunakan oleh pihak yang tidak bertanggung jawab. Administrator harus memastikan bahwa sistem benar-benar aman. Salah satu cara menjaga keamanan *server* yaitu dengan pendeteksian intrusi yang dianggap berbahaya menggunakan *Intrusion Detection System* (IDS). Sistem pendeteksian intrusi dibangun berdasarkan aturan yang telah disimpan dalam sebuah *database* (*signature-based*). Snort merupakan salah satu perangkat lunak yang berfungsi untuk mengetahui adanya intrusi. Paket-paket data yang melalui lalu lintas jaringan akan dianalisa terlebih dahulu. Paket-paket data yang terdeteksi sebagai intrusi akan memicu sebuah *alert* yang kemudian disimpan dalam *file log*. Dengan begitu, administrator dapat mengetahui intrusi yang terjadi pada *server*. Namun, administrator perlu menganalisa pada komputer *server* tersebut. Adanya aplikasi *instant messaging* dapat membantu administrator untuk memperoleh pemberitahuan secara *real time.* Salah satunya menggunakan Telegram dimana administrator mendapatkan informasi singkat dan laporan dokumentasi adanya intrusi pada *server*. Intrusi yang terdeteksi tidak hanya disimpan dalam *file log*, tetapi dapat dilihat pada antarmuka berbasis *web*. Dengan menerapkan IDS, maka sistem dapat memberikan pemberitahuan secara *real time* melalui aplikasi *instant messaging* sebagai solusi untuk mempermudah administrator dalam pencegahan serangan pada *server* sehingga *server* tetap terhindar intrusi dari pihak yang tidak bertanggung jawab.

Kata kunci : *Intrusion Detection System*, Snort, Telegram.