ABSTRAK

Seiring perkembangan teknologi jaringan komputer yang semakin pesat, semakin banyak pula jenis – jenis serangan bermunculan seperti DOS *attack*, OS *fingerprinting, scanning, smurf attack,* dan lain – lain. Oleh karena itu dibutuhkan sebuah sistem yang bisa mendeteksi *attack* secara *realtime respons.*

Intrusion Detection System (IDS) merupakan suatu aplikasi yang memonitor jaringan komputer dari tindakan *attacker* (serangan) yang terhubung dalam sebuah *Local Area Network (LAN).* Aplikasi ini digunakan sebagai tahap awal proteksi terhadap sumber – sumber di dalam suatu sistem atau jaringan, sehingga mempermudah pengelolaan jaringan oleh administrator jaringan dan pemanfaatan jaringan dapat lebih maksimal. Dalam tugas akhir ini digunakan produk dari *Intrusion Detection System (IDS)* itu sendiri, yaitu *Snort 2.9.0.5* pada sistem operasi Linux.

Pendeteksian serangan berbasis IDS dengan algoritma *clustering k-means* adalah suatu sistem yang mendeteksi serangan berdasarkan data log pada *Snort* dengan cara mengelompokkan atau meng-*cluster* data log tersebut menjadi 3 jenis serangan. Sistem ini menggunakan algoritma *clustering k-means* dimana jumlah *cluster* yang ingin dibentuk ditentukan diawal sebanyak tiga *cluster* yaitu serangan berbahaya, *middle,* dan tidak berbahaya. Sistem ini mendeteksi jenis serangan dengan menggunakan proses pengklasteran data *training* dan data baru yang diperoleh dari data log *snort* secara *realtime.* Metode *k-means* digunakan karena metode *k-means* dapat meng-*cluster* data dengan ukuran besar dan cepat.

Berdasarkan teori dan percobaan yang telah dilakukan dengan lebih dari 100 data *training*, hasilnya memberikan kesimpulan bahwa hasil pengklasteran dengan *k-means* menghasilkan nilai akurasi yang bervariasi tergantung dari hasil *random centroid* awal *cluster*. Perbandingan pengujian dengan pengambilan data yang lebih banyak menghasilkan jumlah klaster yang lebih merata yaitu sekitar 7:6 . Setelah mengklaster serangan – serangan yang masuk kedalam sistem menjadi 3 kategori tersebut, selanjutnya sistem akan melakukan aksi berupa *banned IP source* dan juga tutup *port* yang diserang.

Kata kunci: IDS, *Snort,cluster,k-means.*