BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan Teknologi Informasi (selanjutnya disebut TI) telah menyebabkan perubahan dan cara pandang hidup manusia dan suatu organisasi. Perkembangan TI yang sedemikian cepatnya telah membawa dunia memasuki era baru yang lebih cepat dari yang pernah dibayangkan sebelumnya. Ssat ini komputer tidak hanya berfungsi sebagai alat pengolahan data saja, namun telah menjadi senjata utama dalam berkompetisi.

Ada banyak survey yang dapat kita jadikan pedoman, di antaranya survey yang dilakukan oleh IDC (International Data Corporation) tahun 2003 yang mengatakan bahwa tantangan utama manajemen perusahaan dalam masalah keamanan sistem informasi adalah kurangnya sumber daya manusia (36%), disusul *monitoring* (19%), tidak adanya kebijakan dan prosedur (17%), serta integrasi antara solusi teknologi keamanan Sistem Informasi (12%)(Stiawan, 2005).

Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya sistem keamanan jaringan komputer harus harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.

Algoritma *Hierarchical clustering* diterapkan pada data traning untuk menentukan banyaknya *cluster* yang diinginkan. Pada algoritma *clustering*, data akan dikelompokkan menjadi *cluster*-*cluster* berdasarkan kemiripan satu data dengan yang lain. Prinsip dari *clustering* adalah memaksimalkan kesamaan antar anggota satu*cluster*dan meminimumkan kesamaan antar anggota *cluster* yang berbeda. Hasil dari clustering tersebut akan menghasilkan pengelompokkan serangan.

Intrusion Detection System yang nantinya akan disebut IDS merupakan usaha mengindetifikasi adanya penyusup yang memasuki system tanpa otoritas (missal *craker*) atau seorang *user* yang sah tetapi menyalahgunakan *privilege* sumberdaya sistem. *Intrusion Detection System* (IDS) atau Sistem Deteksi Penyusupan adalah sistem komputer (bisa merupakan kombinasi *software* dan *hardware*) yang berusaha melakukan deteksi peyusupan IDS akan melakukan pemberitahuan saat mendeksi penyusupan IDS akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap sebagai mencurigakan atau tindakan illegal. IDS efisien dpaat dikembangkan dengan mendifinisak seperangkat aturan yang tepat untuk mengklasifikasikan jaraingan catatan log lalu lintas menjadi normal atau serangan pola. KDD Cup "99 dataset telah digunakan oleh sebagai besar peneliti sebagai test untuk pengembangan IDS efisen dan IPS.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang dijelaskan, dapat dirumuskan sebuah masalah yaitu :

Bagaimana implementasi Algoritma *Hierarchical Clustering* untuk mendeteksi serangan berdasarkan log file dari KDD cup '99.

1.3 Batasan Masalah

Dalam pembuatan pengembangan intrusksi serangan dibuat beberapa batasan masalah agar permasalahan lebih terfokus. Adapun masalahnya sebagai berikut :

1. Aplikasi bisa melakukan clustering namun belum bisa melakukan tindakan aksi pencegahan.
2. Data set log file IDS diambil dari KDDcup Dataset.
3. Serangan berdasarkan data set yang diambil dari KDDcup dataset sebanyak 1000 data.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah untuk mengkluster data menggunakan algoritma Hierarchical Clustering studi kasus data yang digunakan KDDcup Dataset.

1.5 Manfaat Penelitian

Berdasarkan latar belakang di atas, maka manfaat dari penelitian ini dapat diuraikan sebagai berikut :

1. Mengetahui terhadap serangan-serangan aktif berdasarkan kinerja sistem.
2. Mengetahui serangan yang aktif dari dataset setelah dikluster