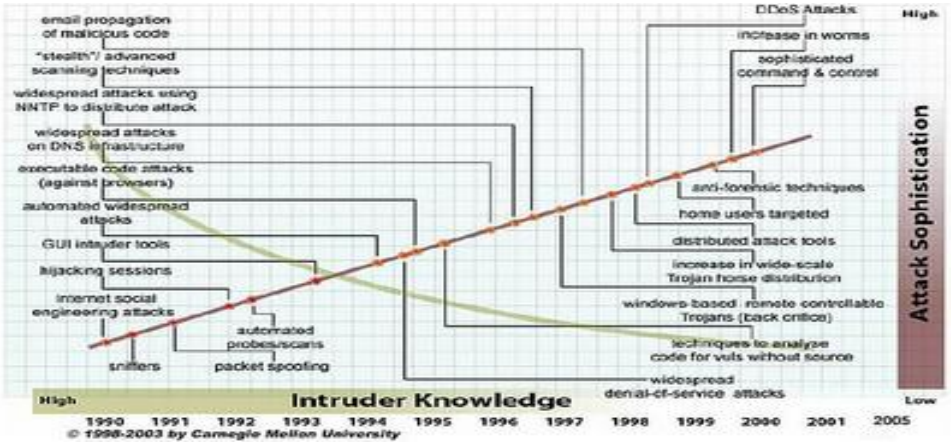
BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Jaringan dalam semua ukuran didesain agar dapat membagi informasi dan keamanan sebagai bagian dari desain tersebut. Sebagian bisnis menggunakan jaringan berbasis IP, seperti *internet* yang digunakan untuk perkantoran yang letaknya jauh, pekerja yang selalu berpindah – pindah, dan relasi bisnis ke dalam lingkup jaringan internal mereka. *Internet* secara terus menerus berkembang dan menghubungkan lebih banyak tempat. Karena daya tahannya terus meningkat, perusahaan dapat menetapkan kembali fungsi aplikasinya. Contoh yang paling jelas adalah hampir segala hal dalam *internet* didasarkan pada HTML. Meskipun hal ini membuat bisnis memiliki interaksi yang lebih luas dengan pelanggan, mempersingkat operasi, mengurangi biaya, dan meningkatkan pendapatan, namun dapat juga menjadi beresiko misalnya mengenai keamanan.

Seiring perkembangan teknologi jaringan komputer tersebut yang membuat kemanan menjadi resiko utama, dimana semakin banyak 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.* Semua serangan ini bersifat sangat merugikan, karena informasi yang seharusnya tidak diketahui pihak lain dapat diambil tanpa adanya *permission*. Masih memungkinkan juga bahwa jenis serangan yang dilakukan akan berkembang dan sangat bervariasi tidak hanya terbatas pada jenis serangan *buffer overflow*. Berdasarkan *www.europa.eu* peningkatan jumlah serangan dari tahun ke tahun semakin meningkat, seperti pada gambar.



Gambar 1.1 Peningkatan jumlah serangan jaringan computer

Oleh karena itu dibutuhkan sebuah sistem pendeteksian serangan yang tidak hanya bisa mendeteksi apakah paket yang lewat termasuk kategori serangan yang ada dan di klaster menjadi kelompok – kelompok tertentu, dan dapat juga mendeteksi serangan – serangan dengan pola yang tidak ada sebelumnya sehingga sistem yang ada menjadi benar – benar aman. *Intrusion Detection System (IDS) Snort* merupakan salah satu solusi dari sistem keamanan jaringan komputer terhadap serangan ataupun usaha penyusupan. Jika terdapat pola serangan baru dan termasuk dalam kategori serangan berbahaya maka aplikasi yang dibuat akan menambahkan pada *rule* IDS *Snort*, sehingga sistem yang di manage akan benar– benar menjadi sistem yang *secure* (aman).

1.2. Rumusan Masalah

Peningkatan *cyber crime* di dunia jaringan komputer sudah sangat pesat . Serangan – serangan seperti DOS *attack*, OS *fingerprinting, scanning, smurf attack,* dan lain – lain menjadi musuh besar para pengguna jaringan komputer. Oleh karena itu dibutuhkan sebuah sistem pendeteksian serangan yang tidak hanya bisa mendeteksi apakah paket yang lewat termasuk kategori serangan yang ada dan di klaster menjadi kelompok – kelompok tertentu, dan dapat juga mendeteksi serangan – serangan dengan pola yang tidak ada sebelumnya sehingga sistem yang ada menjadi benar – benar aman. *Intrusion Detection System (IDS) Snort* merupakan salah satu solusi dari sistem keamanan jaringan komputer terhadap serangan ataupun usaha penyusupan.

Berdasarkan uraian di atas, perumusan masalah yang akan dibahas pada Tugas Akhir ini adalah sebagai berikut:

a. Bagaimana meng-*generate* database log dari *snort*?
b. Bagaimana mengklaster data serangan menggunakan algoritma *clustering k-means* sehingga menjadi klaster dengan kategori serangan berbahaya, serangan sedang, dan serangan tidak berbahaya?
c. Bagaimana melakukan aksi setelah serangan berhasil dideteksi dan diklaster oleh sistem?
d. Bagaimana membuat *interface* dengan membuat aplikasi GUI dengan bahasa pemrograman Java yang mungintegrasikan *snort* dengan algoritma *clustering k-means?*

1.3. Tujuan Penelitian

Berdasarkan pada masalah yang telah diidentifikasikan di atas, maka tujuan dari penelitian ini adalah sebagai berikut :

a. Membuat sebuah aplikasi yang dapat mengklaster data serangan menggunakan metode c*lustering k-means* sehingga menjadi klaster dengan kategori serangan berbahaya, serangan sedang, dan serangan tidak berbahaya.
b. Membuat *rules* baru dari hasil pengklasteran data serangan, dimana *rules* yang akan dibuat adalah serangan dengan *label* bahaya.
c. Membuat aksi berupa *banned IP source* dan sistem tutup *port* setelah serangan berhasil dideteksi dan diklaster oleh sistem.
d. Membuat *interface* dengan membuat aplikasi GUI dengan bahasa pemrograman Java yang mengintegrasikan *snort* dengan algoritma *clustering k-means.*

1.4. Batasan Masalah

Agar dalam penelitian Tugas Akhir ini dapat fokus dan tidak terlalu melebar sehinga menjadi mudah dipahami sesuai dengan tujuan penelitaan yang hendak dilakukan, maka perlu dilakukan pembatasan masalah sebagai berikut:

a. Data serangan yang dipakai hanya yang berasal dari *database log snort* dengan pemilihan data – data yang hanya dibutuhkan sebagai data serangan yaitu data protokol, d_port, size, IP_source dan tcp_flags.
b. *Snort* hanya meng-*scan* komputer server dengan sistem operasi Linux Debiasn 5.0.1.
c. Sistem yang dibangun hanya melakukan pendeteksian dan pengklasteran data – data serangan dari database log *snort* dan membuat *rule* baru serta mengirimkan *alert* (peringatan) jika pola serangan sama dengan *rule snort*.
d. Jumlah *user* yang digunakan dalam pengujian ialah sebanyak 2 *user* .
e. Pengujian dilakukan pada jaringan *Local Area Network (LAN).*
f. Jenis – jenis serangan yang dipilih untuk pengujian system yang telah dirancang adalah *DoS attack, ARP poisoning, Vulnerability scanning,* dan *port scanning.*

1.5. Metodologi Penelitian

Dalam membangun sistem pendeteksian serangan dengan teknik *clustering* ini diperlukan langkah – langkah berikut ini:

1. Melakukan studi pustaka mengenai algoritma *clustering k-means,*IDS, konfigurasi *snort* , mysql, dan konfigurasi Linux Debian 5.0.1 melalui buku referensi, *paper, browsing,* dan jurnal.
2. Melakukan pengumpulan data yang dibutuhkan untuk membangun sistem yang diperoleh dari *database log snort*.
3. Melakukan perancangan sistem yang terdiri dari:
    a. Perancangan model algoritma *clustering k-means* dan optimasi *cluster* dengan menggunakan nilai variansi untuk melakukan pengklasteran pada serangan.
    b. Perancangan aksi yang akan dilakukan setelah terjadi serangan.
    c. Perancangan model aplikasi yang digunakan untuk menampilkan aplikasi yang telah dibuat.
    d. Perancangan model serangan yang digunakan untuk uji coba sistem.
4. Melakukan pembuatan sistem yang meliputi proses mendapatkan data serangan dari hasil seleksi *database* log milik *snort* yang kemudian dilakukan proses pengklasteran dengan algoritma *clustering k-means.*
5. Melakukan perancangan model serangan yang dilakukan untuk men*demo*kan sistem yang telah dibuat.
6. Melakukan uji coba dan analisis terhadap sistem yang telah dibuat dengan data yang telah didapatkan.
7. Penyusunan serta pembuatan laporan.

1.6. Sistematika Penulisan

Sistematika pembahasan dari penyusunan Tugas Akhir ini direncanakan sebagai berikut :

BAB I PENDAHULUAN

Menguraikan secara singkat dan sederhana gambaran dari penelitian yang akan dilaksanakan, terdiri dari latar belakang

penelitian, perumusan masalah, tujuan penelitian, manfaat penelitiaan, pembatasan masalah, metodologi penelitian, dan sistematikan penelitian.

BAB II LANDASAN TEORI

Bab ini membahas mengenai teori – teori dasar yang berkaitan dan menunjang dalam penyelesaian tugas akhir ini

BAB III PERANCANGAN DAN IMPLEMENTASI

Bab ini berisi perancangan dan pembuatan sistem untuk proses pengklasteran data – data serangan yang didapatkan dari database log milik *snort* berdasarkan algoritma *clustering k-means* dengan menggunakan bahasa pemrograman java dan *database* mysql.

BAB IV PENGUJIAN DAN ANALISIS

Dari sistem yang telah dibuat, akan dilakukan pengujian dengan menggunakan data yang sudah di *generate* oleh *snort* yang selanjutnya dikelompokkan berdasarkan algoritma *clustering k-means* dan kemudian hasilnya nanti akan dianalisa. Hal ini dilakukan untuk mengetahui apakah metode pengklasteran ini dapat digunakan untuk proses pendeteksian serangan yang akurat atau tidak dan pengaruhnya terhadap performansi. Selan itu akan dianalisis juga pengaruh aksi yang dilakukan kepada penyerang.

BAB V PENUTUP

Bab ini berisi kesimpulan dari pembahasan pada perencanaan serta analisis pengujian sistem atau program yang diperoleh. Untuk lebih meningkatkan hasil akhir yang lebih baik maka diberikan juga saran – saran untuk perbaikan sera penyempurnaan Tugas Akhir ini.