BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada perkembangan teknologi komputer seperti internet sekarang, keamanan merupakan aspek penting dari suatu sistem. Saat ini hampir seluruh kalangan masyarakat dapat menggunakannya untuk mendapatkan informasi yang luas dan beragam dari seluruh dunia. Banyak kalangan sering kali tidak bertanggung jawab dalam menggunakan teknologi internet saat ini, yang sering kali menyebabkan kerugian. Hal ini pula yang menyebabkan munculnya serangan-serangan di dalam suatu jaringan komputer yang tentunya merugikan. Serangan yang terjadi ini bisa disebut sebagai anomali trafik dimana dapat terjadi *flash-crowd* atau karena serangan *flooding* trafik seperti *Denial of Service* (Dos) dan *Distributed Denial of Service* (DDoS).

Denial of Service (DoS) dan *Disributed Denial of Service* (DDoS) merupakan bentuk serangan *flooding* yang berusaha membuat suatu *host* atau *service* menjadi tak dapat diakses oleh pengguna yang berhak. Sasaran serangan oleh DoS/DDoS adalah *link/bandwidth* untuk membuat sumber daya bandwidth penuh dan sumber daya komputasi pada server agar sistem pengolah kehabisan sumber daya yang berujung oleh jaringan *down* atau *crash*. Sedangkan *flashcrowd* adalah kejadian yang tidak dapat diprediksi dan akan mengakibatkan peningkatan akses secara dramatis/tinggi ke suatu server karena suatu kejadian seperti bencana alam, peluncuran produk, *breaking news*, dll.

Dalam mendeteksi dan mengatasi serangan di jaringan komputer, dikenal istilah *Intrusion Detection System* (IDS). Pada *Intrusion Detection System* (IDS) dikenal 2 metode yang sering digunakan yaitu *intrusion signature* dan *traffic anomaly based* yang berfungsi untuk mengenali serangan yang terjadi. Pada saat ini penanganan yang ada untuk masalah *anomaly traffic* hanya secara *offline* atau tidak *realtime*. Oleh karena itu dibutuhkan penelitian ini untuk menganalisa adanya anomali trafik pada suatu jaringan secara *realtime* atau *stream*.

1.2 Rumusan Masalah

Terdapat berbagai macam anomali trafik yang sudah ditemukan dimasa sekarang ini. Beriringan dengan hal tersebut, cara mendeteksi dan mengatasinya pun sudah bervariasi, misalnya [7] menggunakan metode peninjauan pada alamat IP source dan hasilnya sederhana namun tepat, akan tetapi masih diperlukan training pada perangkat lunak yang digunakan.

Dalam penelitian ini akan dibentuk perancangan sistem untuk deteksi anomali pada aliran trafik secara *streaming* serta sistem dapat memperoleh nilai akurasi yang tinggi dan *false positive* rate yang rendah dan mengimplementasikan algoritma clustream untuk pengelompokan trafik berdasarkan grup.

1.3 Tujuan

Pada penelitian ini akan mengimplementasikan metode deteksi anomali trafik dengan algoritma clustream berdasarkan grup agar didapat tingkat akurasi tinggi dengan *false positive* yang rendah.

1.4 Batasan Masalah

Adapun batasan masalah pada tugas akhir ini, yaitu:

a. Menggunakan sistem operasi *Linux Ubuntu*.
b. Menggunakan *Python IDS Tools*.
c. Menggunakan *Dataset KDDCup99* untuk referensi fitur yang digunakan.
d. Menggunakan Algoritma Clustream berdasarkan grup yakni 30 paket.
e. Diuji menggunakan ping normal dan *ping flood*.
f. Fitur yang diolah oleh sistem antara lain: *paket size, time interval, counter paket, counter TCP, counter UDP,* dan *counter ICMP*.
g. Hasil keluaran hanya berupa deteksi serangan dengan mengelompokan trafik normal dan trafik anomali, tidak mengklasifikasikan dan tidak berupa pencegahan.
h. Ruang Lingkup jaringan yang dideteksi adalah LAN (*Local Area Network*).

1.5 Metodologi Penyelesaian Masalah

Pada peneltian yang telah dilakukan, terdapat beberapa tahapan hingga didapatkan hasil akhir yang diinginkan. Berikut tahapan-tahapan tersebut:

1.5.1 Studi Literatur

Tahap mencari materi dan referensi pendukung untuk pembuatan tugas akhir, seperti mencari jurnal terkait algoritma clustream, mempelajari penggunaan *IDS Tools* serta membaca dan me-*review* jurnal internasional yang berkaitan dengan topik tugas akhir.

1.5.2 Pengumpulan Data

Pengumpulan data dilakukan dengan men-*generate* trafik jaringan agar didapat data trafik yang akan diolah oleh algoritma clustream.

1.5.3 Perancangan Sistem

Merancang sistem deteksi yang akan dibuat seperti *flowchart* sistem deteksi, *flowchart* algoritma clustream tahapan dari awal trafik masuk hingga diolah menjadi kelompok trafik normal dan trafik anomali.

1.5.4 Pengujian Sistem

Pada tahap ini dilakukan pengujian terhadap sistem deteksi yang telah dibuat. Pengujian berupa penghitungan nilai akurasi dari hasil deteksi *stream traffic*.

1.5.5 Analisis Pengujian

Dari tahap pengujian yang telah dilakukan sebelumnya, dilakukan analisis terhadap keakuratan dari sistem dalam mendeteksi *stream traffic*.

1.5.6 Penyusunan Laporan

Pada tahap ini dilakukan penyusunan laporan akhir dan pengumpulan dokumentasi yang diperlukan dengan mengikuti format laporan yang telah ditetapkan oleh universitas.

1.6 Sistematika Penulisan

Sistematika pada penulisan ini terbagi menjadi beberapa tahapan. Setiap bagian menjelaskan langkah demi langkah dalam pengerjaan Tugas akhir ini. Berikut adalah bagian tersebut:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang dari pembuatan sistem, rumusan masalah, tujuan dan batasan masalah dari judul tugas akhir ini. Serta metodologi penelitian dan sistematika penulisan yang digunakan dalam tugas akhir ini.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang penjelasan teori-teori terkait yang digunakan dalam perancangan sistem yang dibuat untuk tugas akhir ini. Teori-teori tersebut bersumber dari jurnal, buku, maupun artikel resmi dari internet.

BAB III PERANCANGAN SISTEM

Bab ini membahas mengenai semua hal yang berkaitan dengan proses pemodelan, perancangan sistem, pengerjaan dan penyelesaian sistem, serta alur dari algoritma yang digunakan untuk sistem yang dibuat.

BAB IV PENGUJIAN DAN ANALISIS

Bab ini menjelaskan tentang kinerja sistem dan pengujian-pengujian yang dilakukan pada sistem. Dari setiap hasil pengujian akan dilakukan analisis dan menarik kesimpulan dari hasil analisis tersebut.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan akhir dari perancangan, pengujian dan analisis yang telah dilakukan serta saran dan harapan untuk pengembangan lebih lanjut.