BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada saat ini jaringan internet merupakan jaringan yang paling banyak dipakai oleh semua orang di seluruh dunia. Hal ini terjadi karena internet dapat menyediakan berbagai macam layanan yang dibutuhkan oleh semua orang. Di internet kita dapat bertukar data dengan mudah dan cepat. Selain karena kemudahan dan kecepatannya internet juga dikenal sebagai jaringan yang fleksibel. Sehingga banyak sekali ditemukan hal-hal baru di jaringan internet. Seperti misalnya, aplikasi-aplikasi baru yang dapat menunjang pekerjaan, foto-foto unik, video menarik dan lainnya.

Seiring semakin pesatnya perkembangan teknologi internet sekarang ini semakin banyak pula kegiatan yang memanfatkan internet. Internet dapat menyediakan berbagai macam layanan yang dibutuhkan oleh semua orang. Di internet kita dapat bertukar data dan informasi dengan mudah dan cepat.

Tapi sangat disayangkan ada penggguna- pengguna internet yang tidak bertanggung jawab dengan memanfaatkan internet untuk melakukan kejahatan atau biasa kita sebut dengan *hacker*. Tujuan dari pada kegiatan *hacking* itu sendiri adalah untuk mencuri informasi-informasi penting yang nanti dari informasi penting tersebut akan disalah gunakan atau bahkan tujuan dari *hacking* sendiri selain untuk mrncuri informasi bisa jadi untuk merusak sistem yang telah dibuat sehingga sistem tidak dapat berjalan dengan semestinya. Saat ini para *hacker* tidak mau kehabisan akal untuk selalu membuat attack-attack jenis baru dan lebih mengkahwatirkan. Salau satu *attack* yang biasa digunakan oleh *hacker* yakni Botnet.

Robot Netwrok atau biasa disingkat dengan Botnet adalah suatu kaki tangan yang dikirim dengan cara disisip kan ke komputer target oleh *attacker* dengan cara diam-diam. Setelah *attacker* mensisipkan botnet ke banyak komputer barulah *attacker* mengendalikan komputer korban yang telah terinfeksi botnet.

Penelitian Tugas Akhir ini sangat penting karena keluaran dari penelitian ini adalah berupa sistem deteksi trafik anomali dan klasifikasi serangan BOTNET secara *Real time* sehingga korban dapat dengan cepat mengetahui apakah komputer korban menjadi target dari *ha*cker atau tidak. Untuk sistem deteksi penulis menggunakan Metode *Self-similarity* yang mana metode ini menggunakan pengkarakteristikan dari trafik yang masuk, dan juga metode ini juga harus menggunakan estimasi *hurst exponent* yaitu mencari nilai dari estimasi H. Karakteristik yang digunakan oleh penulis pada metode *self similarity* yaitu proses aggregat. Untuk sistem pengklasifikasian penulis menggunakan algoritma *cumulative sum*. Algoritma *cumulative sum* atau biasa disingkat CUSUM ini merupakan algoritma yang memiliki ide dasar berupa perhitungan statistika. Pada algoritma CUSUM ini

1.2 Formulasi Masalah

Zaman sekarang ini telah banyak sekali ditemukan metode untuk mengatasi serangan anomali trafik dengan metode dan hasil yang berbeda pula. Salah satu penelitianya yaitu [1] menggunakan algoritma *cumulative sum* untuk mendeteksi serangan UDP *flooding.* Pada penelitian ini memberikan hasil yang baik dan cepat dalam melakukan pendeteksian, dan melakukan pendeteksian sedini mungkin, akan tetapi sistem hanya terkhusus untuk serangan UDP *flooding*. Kekurangan dari penelitian sebelumya yaitu sistem masih berupa deteksi dan tidak secara *realtime*. Maka dari itu, pada penelitian ini penulis ingin membuat sistem yang dapat mendeteksi anomali dan juga dapat mengklasifikasi serangan sehingga korban dapat mendeteksi lebih dini serangan**.** Perbedaanya dengan penelitian [1] yaitu apabila pada penelitian sebelumnya menggunakan Algoritma CUSUM untuk sistem deteksi pada tugas akhir ini penulis menggunakan Algoritma sebagai metoda untuk sistem klasifikasi dan sistem deteksi menggunakan metode *Self Similarity*. *Self similarity* digunakan untuk mendeteksi apakah suatu trafik yang datang merupakan normal trafik atau anomali trafik.

Ada pun beberapa masalah pada penelitian ini yaitu untuk melakukan analisis dari *self similarity* kita harus terlebih dahulu mengetahui nilai dari hurst eksponen pada penelitian ini nilai hurst eksponen dicari dengan menggunakan metode R/S. Pada saat dalam kondisi normal suatu trafik akan memberikan nilai *hurst eksponen* antara 0,5 dan 1.

Rumusan masalah selanjutnya yaitu membuat klasifikasi serangan dengan menggunakan Algoritma CUSUM. Dalam menentukan jenis serangan nya dalam penelitian ini mencari nilai *threshold* terlebih dahulu dari setiap serangan botnet. Pada penelitian ini penulis mempunya target untuk dapat membedakan 5 jenis

serangan botnet.

1.3 Tujuan

Tujuan dari penelitian ini adalah :

1. Membuat sebuah sistem deteksi dan klasifikasi dari anomali trafik dengan menggunakan NS2..
2. Membuat sebuah sistem deteksi anomali trafik menggunakan algoritma *self-simliarity* dan sistem klasifikasi serangan dengan menggunakan algoritma CUSUM
3. Menguji keakuratan dari algoritma *Self-similarity* dan Algoritma CUSUM

1.4 Batasan

1. Menggunakan datastream hasil dari NS2.
2. Tidak membahas teknik *hacking*..
3. Menggunakan sistem analisis self similarity dan Algoritma CUSUM.
4. Hasil keluaran hanya berupa deteksi serangan dan klasifikasi tidak membahas mengenai penanggulangan.

1.5 Metodologi Penyelesaian Masalah

Metodologi penelitian yang digunakan adalah:

a. Studi literatur, yaitu mempelajari literatur-literatur yang ada sesuai dengan permasalahan yang akan dibahas meliputi, konsep deteksi anomali trafik, teori serangan *anomaly*, teori estimasi *hurst eksponen*, teori dasar dari karakteristik *self-similarity* proses agregat.

b. Analisis terhadap kebutuhan dan pemodelan sistem untuk proses deteksi da klasifikasi anomali trafik

c. Perancangan dan analisis menggunakan tools untuk sistem deteksi dan klasifikasi anomali trafik.

d. Uji performansi dan analisis hasil penelitian

e. Pembuatan laporan dari hasil penelitian

1.5 Sistematika Penulisan TA

Adapun sistematika penulisan pada Tugas Akhir ini adalah :

BAB I PENDAHULUAN

Berisi tentang latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, metodologi penelitian, dan sistematika penelitian

BAB II TINJAUAN PUSTAKA

Berisi tentang penjelasan mengenai penjelasan mengenai serangan botnet, teori dasar *self-similarity* dan algoritma cusum, penjelasan mengenai *Hurst eksponen*.

BAB III PERANCANGAN SISTEM

Berisi tentang perancangan sistem yang akan dibangun, metode estimasi *hurst eksponen* dan karakteristik dari *self-similarity* yaitu proses agregat. Perancangan dari algoritma cusum.

BAB IV PENGUJIAN DAN ANALISIS

Berisi tentang pengujian performansi dan analisis hasil penelitian

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan dari hasil penelitain yang dilakukan dan rekomendasi untuk penelitian berikutnya