BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Masalah keamanan sebuah jaringan akhir-akhir ini amat sangat rentan terhadap serangan dari berbagai pihak. Alasan dari serangan tersebut tentu saja beragam. Diantaranya yaitu alasan untuk merusak, balas dendam, politik, atau cuma iseng - iseng saja untuk unjuk gigi.Status subkultural dalam dunia *hacker*, adalah sebuah unjuk gigi atau lebih tepat kita sebut sebagai pencarian jati diri. Adalah sebuah aktifitas umum dikalangan *hacker-hacker* muda untuk menunjukkan kemampuannya dan *Denial of Service* (*DoS*) merupakan aktifitas hacker diawal karirnya.Alasan politik dan ekonomi untuk saat sekarang juga merupakan alasan yang paling relevan. Kita bisa melihat dalam *cyber war*, serangan *DoS* bahkan dilakukan secara terdistribusi atau lebih dikenal dengan istilah '*Distribute Denial of Service*'. Beberapa kasus serangan virus semacam 'code-red' melakukan serangan *DoS* bahkan secara otomatis dengan memanfaatkan komputer yang terinfeksi, komputer ini disebut *zombie*. Lebih relevan lagi, keisengan merupakan motif yang paling sering dijumpai.Bukanlah hal yang sulit untuk mendapatkan program-program *DoS*, seperti *nestea, teardrop, land, boink, jolt dan vadim*. Program-program *DoS* dapat melakukan serangan *Denial of Service* dengan sangat tepat, dan yang terpenting sangat mudah untuk melakukannya (Gon, 2012).

Serangan Denial of Services (DoS) adalah salah satu contoh jenis serangan yang dapat mengganggu infrastruktur dari jaringan komputer, serangan jenis ini memiliki suatu pola khas, dimana dalam setiap serangannya akan mengirimkan sejumlah paket data secara terus-menerus kepada target serangannya. Dengan menggunakan metode deteksi anomali, serangan *DoS* dapat dideteksi dengan mengidentifikasi pola-pola anomali yang ditimbulkan (Sucipta, Wirawan, & Muliantara, 2012).

Dalam tugas akhir ini penulis mencoba melakukan pemodelan terhadap lalu lintas paket data dengan menangkap paket data dalam jaringan dan menganalisisnya guna mengetahui karakteristik sebuah serangan *UDP Flood, PING Flood, dan SYN Attack.*

1.2 Perumusan Masalah

Berdasarkan latar belakang diatas, dapat dirumuskan permasalahan yaitu:

1. Bagaimana melakukan identifikasi karakteristik statistik paket data yang mengandung *DoS attack*?
2. Bagaimana melakukan estimasi parameter statistik yang bersesuaian dengan distribusi data yang mengandung *DoS Attack*?

1.3 Pembatasan Masalah

Batasan masalah dari sistem yang dibahas adalah sebagai berikut :

1. Aplikasi yang digunakan untuk mengambil/ menangkap paket data yang lewat adalah *Network Protocol Analyzer.*
2. Menggunakan *Denial of Service attack jenis UDP Flood, PING Flood* dan *SYN Attack.*
3. Serangan Menggunakan *OS Bactrack 5* dan Korban menggunakan *Ubuntu.*

4. Analisis panjang paket menggunakan *SPSS* 14 dan *Matlab* 2009.
5. Menggunakan topologi jaringan yang sudah ditentukan dan 2 modem *Smartfren*.

1.4 Tujuan

Tujuan dari analisa jaringan ini adalah:

1. Melakukan identifikasi karakteristik statistik paket data yang mengandung *DoS attack*?
2 Melakukan estimasi parameter statistik yang bersesuaian dengan distribusi data yang mengandung *DoS Attack*?

1.5 Kontribusi

1. Dari hasil identifikasi karakterisitik statistic paket data yang mengandung *DoS,* diharapkan seorang *Administrator* jaringan bisa mengetahui serangan paket data yang mengandung *DoS* pada *server.*
2. Memberikan analisis pemodelan karakteristik *DoS* jenis *SYN Attack, PING Flood dan UDP Flood* dan pada akhirnya pemodelan ini bisa dijadikan refrensi oleh peneliti lebih lanjut untuk mengatasi serangan *DoS.*

2.1 Sistematika Penulisan

Pada penulisan Laporan Tugas Akhir ini ditulis dengan sistematika penulisan sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini dikemukakan hal–hal yang menjadi latar belakang, perumusan masalah, batasan masalah, tujuan yang ingin dicapai, manfaat serta sistematika penulisan laporan tugas akhir ini.

BAB II : LANDASAN TEORI

Pada bab ini dibahas teori yang berhubungan dengan pemodelan *DoS Attack*, *Network Protocol Analyser*, *Network Attack*, *Security Attack Models*, Proses *Attack*, *Denial of Service Attack*, Statistika, serta Distribusi Probabilitas.

BAB III : METODE PENELITIAN

Pada bab ini dibahas mengenai penjelasan sistem keseluruhan dari proses serangan dengan menggunakan simulasi jaringan, beserta detail dari blok diagram system, yang terdiri dari paket data serangan yang difilter dengan menggunakan *Network Protocol Analyser*, paket data tersebut diolah dengan *SPSS* untuk dicari distribusi frekuensi, selanjutnya membuat interval kelas, jumlah paket, nilai tengah dan frekuensi relative. Selanjutnya mencari rata-rata dari empat serangan yang sama selanjutnya estimasi parameter untuk mencari distribusi probabilitas. Selanjutnya plot histogram data mentah dengan distribusi probabilitas dan yang terakhir adalah menghitung *MSE* untuk mencari

nilai selisih terkecil antara histogram data mentah dengan distribusi probabilitas.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini memaparkan berbagai macam percobaan yang dilakukan, hasil-hasil yang didapatkan berupa plot gambar berupa histogram dan grafik serta nilai dari *MSE*. berserta solusi dari permasalahan yang didapat. Selain itu disertai pula hasil uji coba perbagian dan juga uji coba sistem secara keseluruhan untuk *UDP Attack* melakukan pengujian sebanyak lima kali yaitu *UDP Attack A, UDP Attack B, UDP Attack C, UDP Attack D,* dan*UDP Attack* Rata-rata. Selanjutnya untuk *PING Flood* melakukan pengujian sebanyak lima kali yaitu *PING Flood A, PING Flood B, PING Flood C, PING Flood D,* dan *PING Flood* Rata-rata. Selanjutnya untuk *SYN Attack* juga melakukan pengujian sebanyak lima kali yaitu *SYN Attack A, SYN Attack B, SYN Attack C, SYN Attack D* dan *SYN Attack* Rata-rata.

BAB V : PENUTUP

Pada bab ini dibahas mengenai kesimpulan dari sistem terkait dengan tujuan dan permasalahan yang ada, serta saran untuk pengembangan sistem di masa mendatang.