BAB I

PENDAHULUAN

A. Latar Belakang

Kebutuhan akan informasi dan komunikasi dewasa ini menjadi sangat penting di masyarakat. Seiring kemajuan dan perkembangan teknologi informasi yang semakin canggih dengan perkembangannya yang sangat cepat, maka kebutuhan akan informasi semakin meningkat pula. Teknologi informasi saat ini telah berkembang pesat, salah satunya dalam bidang jaringan komputer.

Jaringan komputer sangat berkaitan erat dengan internet dan telah menjadi suatu sarana untuk membantu dalam melaksanakan aktifitas suatu instansi/perusahaan. Dalam hal ini tidak hanya perusahaan yang bergerak di bidang telekomunikasi saja, akan tetapi juga perusahaan lain yang tidak bergerak di bidang tersebut. Kecenderungan ini disebabkan karena dengan adanya internet akan mendapatkan kemudahan dalam hal komunikasi. Kelebihan inilah yang menjadi kunci dari mengapa dipilihnya fasilitas tersebut. Akan tetapi dibalik kelebihan-kelebihan tersebut, jaringan komputer juga menyimpan banyak kekurangan bagi para penggunanya. Salah satunya adalah dalam bidang keamanan. Setiap komputer yang terhubung ke dalam suatu jaringan dan terkoneksi dengan internet pasti akan sering menghadapi berbagai macam bentuk

serangan yang selalu berusaha mencari celah dari sistem keamanan jaringan komputer yang digunakan.

Kasus yang terjadi bahwa jaringan komputer yang terkoneksi dengan internet sering mendapatkan serangan-serangan yang mengakibatkan kerusakan bahkan kehilangan data yang dimiliki maupun kerusakan-kerusakan *hardware* akibat serangan tersebut. Kerugian karena kasus semacam ini bisa mencapai puluhan juta rupiah yang meliputi kerugian dalam bentuk fisik (*hardware*) maupun non-fisik (data).

Flooding data menjadi salah satu bentuk serangan serangan yang mengakibatkan suatu sistem akan terbanjiri oleh data-data secara terus menerus dalam waktu yang singkat. Hal ini juga mengakibatkan lalu lintas jaringan menjadi sangat padat sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan.

Dalam faktor keamanan ini biasanya perusahaan menempatkan administrator untuk menjaga, tetapi fungsi administrator tentunya akan terbatas waktunya, hanya pada saat jam kerja. Sedangkan suatu serangan ke sistem keamanan bisa terjadi kapan saja. Baik pada saat administrator sedang bekerja ataupun tidak. Dengan demikian dibutuhkan sistem pertahanan didalam *server* itu sendiri yang bisa menganalisa langsung apakah setiap paket yang masuk tersebut adalah data yang diharapkan ataupun data yang tidak diharapkan. Kalau paket tersebut merupakan data yang tidak diharapkan, diusahakan agar komputer bisa

mengambil tindakan untuk mengantisipasi agar serangan yang terjadi tidak menimbulkan kerugian yang besar.

Upaya untuk meningkatkan keamanan jaringan komputer salah satunya adalah dengan *firewall.* Implementasi dari sistem *firewall* ini dapat berupa software ataupun *hardware* yang bersifat aktif dengan melakukan penyaringan paket data yang lewat berdasarkan pengaturan yang diinginkan. Cara lain adalah dengan mengimplementasikan *Intrussion Detection System* (IDS) dan *Intrussion Prevention System* (IPS) pada sebuah Jaringan Komputer. Sedikit berbeda dengan *firewall, Intrusion Detection System* (IDS) adalah sebuah sistem yang digunakan untuk melakukan deteksi adanya usaha-usaha penyusupan terhadap sebuah sistem dengan melakukan pengamatan trafik data secara *real-time.* Sedangkan *Intrussion Prevetion System* (IPS) bertugas untuk mengambil keputusan berdasarkan data yang sudah terekam oleh IDS.

Berdasarkan beberapa pertimbangan di atas, maka akan lebih bermanfaat jika penelitian dilakukan dengan tema Deteksi dan Pencegahan Flooding Data Pada Jaringan Komputer.

B. Rumusan Masalah

Dalam penulisan penelitian ini, kami mencoba memaparkan beberapa permasalahan yang kemudian diusahakan solusi pemecahannya. Beberapa masalah tersebut antara lain :

a. Bagaimana merancang dan membangun sebuah system yang mampu mengenali serangan Flooding data pada suatu jaringan komputer.

b. Bagaimana merancang dan membangun sebuah system yang mampu mengatasi adanya serangan Flooding data pada suatu jaringan komputer.

C. Batasan Masalah

Agar penelitian ini dapat mencapai sasaran dan tujuan yang diharapkan, maka permalasalahan yang ada akan dibatasi sebagai berikut :

a. Sistem yang dibangun hanya digunakan untuk memantau aktivitas jaringan komputer jika terjadi serangan khususnya jika terjadi Flooding data.

b. Sistem yang dibangun adalah menggunakan Snort sebagai *Intrussion Detection System* (IDS) dan *Intrussion Prevention System* (IPS) pada suatu jaringan komputer dengan sistem operasi Linux Ubuntu *Server* 10.04.

c. Trafik data yang diamati dalam penelitian ini dibatasi pada paket data yang mengarah pada *server* IDS dan IPS yang berhubungan dengan keamanan *server*.

D. Tujuan Penelitian

Penelitian ini bertujuan untuk membangun sebuah sistem yang mampu mendeteksi serangan Flooding Data pada jaringan komputer, sehingga secara otomatis mampu mencegah serangan tersebut.

E. Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah:

1 Hasil penelitian ini dapat digunakan sebagai masukan terhadap upaya untuk mengoptimalkan keamanan pada jaringan komputer.

2 Memberikan referensi bagi penulisan Karya Ilmiah selanjutnya dan menambah sumber pustaka bagi pengembangan sistem jaringan berbasis *open source* yang aman.

3 Dapat memberikan referensi dalam mengembangkan kemampuan di kalangan akademis dalam menerapkan perancangan keamanan jaringan komputer.

F. Sistematika Laporan Penelitian

Untuk memudahkan dalam penulisan laporan, maka sistematika penulisan yang digunakan dalam penelitian adalah sebagai berikut:

I. PENDAHULUAN

Bab ini berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penelitian yang digunakan dalam penelitian.

II. TINJAUAN PUSTAKA

Bab ini berisi tentang telaah penelitian terdahulu yang berhubungan dengan penelitian serta landasan teori yang berkaitan dengan masalah yang diteliti dalam penelitian.

III. METODE PENELITIAN

Bab ini berisi tentang jenis penelitian yang dilakukan, sumber data yang digunakan, teknik pengumpulan data, serta analisa masalah yang diteliti.

IV. PEMBAHASAN

Bab ini berisi tentang penyelesaian masalah meliputi langkah-langkah penelitian, hasil tahapan dari penelitian, tahap perancangan dan konfigurasi, tahap pengujian dan implementasi, dan tahap analisa hasil penelitian.

V. PENUTUP

Bab ini berisi tentang kesimpulan dan saran dari hasil kegiatan penelitian.