BAB I

PENDAHULUAN

1.1 Latar Belakang

Banyaknya perusahaan atau lembaga yang menggunakan internet sebagai sarana untuk membantu dalam melaksanakan aktifitas rutin perusahaan dan aktifitas rutin lainnya, kemudahan dan kepraktisan merupakan kunci dari mengapa dipilihnya internet ini. Sehingga internet menjadi salah satu daftar penting dalam suatu perusahaan ataupun instansi-instansi pemerintah lainnya.

Disamping kelebihan tersebut, internet juga mempunyai banyak kekurangan yang sangat mengkhawatirkan bagi para penggunanya ataupun instansi instansi perkantoran yang menggunakan internet, seperti kejahatan komputer, yang meliputi pencurian, penipuan, kompetitif, banyak lagi yang lainnya, seperti jatuhnya informasi ke pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. (Ariyus : 2005) Banyak kasus yang membuktikan bahwa perusahaan yang tersambung di internet sering kali mendapatkan gangguan baik dalam data yang dimiliki maupun peralatannya. Kerugian yang diderita akan hal ini bisa dibilang tidak kecil. Kasus pencurian atau manipulasi data perusahaan saja dapat mencapai kerugian sampai jutaan rupiah.

Belum lagi kerusakan peralatan yang digunakan oleh perusahaan tersebut, yang bisa dibidang tidak murah.

Dalam faktor keamanan ini salah satu serangan yang sering muncul adalah data *flooding*. (Soki :2011) Data *flooding* merupakan suatu kejadian di dalam jaringan dimana dalam jaringan tersebut terjadi suatu transfer data dalam jumlah yang besar sehingga mengganggu kinerja komputer yang terhubung di dalam jaringan tersebut, hal ini kemungkinan bisa disebabkan adanya serangan dari luar yang biasa disebut dengan DOS/DDOS (*Denial of Service/ Distributed Denial of Services*) yaitu serangan pada jaringan komputer yang berusaha untuk menghabiskan sumber daya sebuah peralatan komputer, sehingga jaringan komputer menjadi terganggu. Untuk mengatasi hal itu biasanya digunakan 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.

Instansi pemerintah Badan Penanggulangan Bencana Daerah Provinsi Sumatera Selatan yang melakukan aktifitas pertukaran informasi, laporan laporan bencana daerah ke Badan Nasional Penanggulangan Bencana Pusat menggunakan jaringan komputer, maka ancaman terhadap jaringan komputer akan selalu membayangi keamanan jaringan tersebut, terutama ancaman data *flooding* yang bisa terjadi kapan saja. Dalam skripsi ini penulis mencoba menganalisis keamanan

jaringan terhadap ancaman terjadinya data *flooding* pada jaringan komputer pada Badan Penanggulangan Bencana Daerah Provinsi Sumatera Selatan.

1.2 Perumusan Masalah

Rumusan masalah dalam penelitian ini “bagaimana menganalisis keamanan jaringan komputer Badan Penanggulangan Bencana Provinsi Sumatera-Selatan terhadap ancaman data *flooding* ?”

1.3 Tujuan Penelitian

Tugas akhir ini bertujuan untuk mengetahui, menganalisa dan mencegah ancaman terjadinya data *flooding* pada keamanan jaringan komputer Badan Penanggulangan Bencana Daerah Provinsi Sumatera Selatan.

1.4 Batasan Masalah

Dengan adanya rumusan masalah yang telah ada, sehingga untuk menghindari meluasnya masalah, maka penulis akan membatasi ruanglingkup kajian pada implementasi *Intrusion Detektion System* (IDS) menggunakan *monitoring Based* dan sensor *Snort* di data server.

1.5 Manfaat penelitian

Adapun manfaat dari penelitian ini adalah :

1. Mengetahui karakteristik implementasi aplikasi monitoring di server.

2. Meningkatkan sistem keamanan yang dapat di implementasikan, mencegah data *flooding* pada Badan Penanggulangan Bencana Daerah Provinsi Sumatera Selatan.

1.6 Metodologi Penelitian

Dalam penelitian ini penulis menggunakan metode *Action Research* atau penelitian tindakan merupakan salah satu bentuk rancangan penelitian yang mengutamakan tindakan secara langsung ke lapangan guna untuk mengetahui masalah apa yang sedang dihadapi dan upaya apa yang akan dilakukan dalam pemecahan masalah tersebut.

Tahapan yang dilakukan dalam *Action research* yaitu :

1. Melakukan diagnosa (*diagnosing*), dalam tahapan ini yang dilakukan adalah mengidentifikasi masalah keamanan jaringan terhadap ancaman data flooding pada instansi tersebut.
2. Membuat rancangan tindakan (*action planning*), dalam tahapan ini penulis mencoba memahami pokok permasalahan dan kemudian menyusun rencana untuk melakukan penelitian.
3. Melakukan tindakan (*action taking*), dalam tahapan ini penulis melakukan penelitian langsung pada pokok permasalahan yang sudah di diagnosa.
4. Pembelajaran (*learning*), pembelajaran atau *learning* ini adalah tahapan terakhir yang dilakukan penulis. Dalam tahapan ini penulis menganalisa data yang telah diperoleh dari penelitian tersebut.

1.7 Sistematika Penulisan

BAB I PENDAHULUAN

Merupakan pendahuluan yang membahas latar belakang, perumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, metodologi penelitian dan sistematika pembahasan.

BAB II TINJAUAN PUSTAKA

Berisi teori-teori yang berhubungan dengan penelitian yang akan dilakukan dan juga memuat hasil-hasil penelitian sejenis yang menginspirasi atau melandasi pelaksanaan penelitian ini.

BAB III ANALISA DAN PERANCANGAN

Berisikan konsep dasar yang mendukung penelitian.

BAB IV IMPLEMENTASI

Berisikan tahap-tahapan peginstalan sensor Snort monitoring.

BAB V HASIL DAN PEMBAHASAN

Berisi tentang hasil dan pengolahan data yang telah di peroleh pada saat penelitian.

BAB VI PENUTUP

Berisi kesimpulan dan saran dari bab-bab sebelumnya.