

BAB I

PENDAHULUAN

1.1 LatarBelakang

Pada era globalisasi sekarang ini semua yang berhubungan dengan jaringan komputer harus memiliki keamanan yang dapat diandalkan. Dimana sekarang seseorang dalam sebuah jaringan komputer dapat melakukan apapun terhadap sebuah perangkat komputer apabila tidak ada keamanan yang menjaga jaringan tersebut.

Di jaringan Internet tidaklah mudah untuk menjaga keamanan komputer dari serangan-serangan penjahat internet saat ini, karena dalam struktur jaringan internet perangkat komputer bisa di akses dari mana saja. Serangan yang dilakukan ini sangat banyak jenisnya, namun yang paling banyak digemari adalah DDOS karena serangan dengan jenis ini mengakibatkan *server* korban tidak dapat mengakses sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

Salah satu solusi mengenai DDOS *attack* adalah menggunakan IDS yang dapat mendeteksi serangan-serangan tersebut. Tujuan dari IDS sendiri adalah untuk mengingatkan Administrator jaringan bahwa ada serangan yang akan menyerang *system* jaringan miliknya. Dengan adanya IDS Administrator dapat mencegah serangan tersebut dengan berbagai cara yang dimilikinya.

1.2 Perumusan Masalah

Dari latar belakang yang sudah dijelaskan sebelumnya dimunculkan rumusan masalah yaitu:

1. Bagaimana merancang dan membangun HIDS menggunakan SNORT pada network yang tersedia ?
2. Bagaimana mencegah serangan DDOS untuk menjaga server tidak down ?.

1.3 Tujuan dan Manfaat

Berdasarkan rumusan masalah diatas, maka tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. Untuk mengimplementasikan sebuah HIDS yang difokuskan pada pencegahan serangan DDOS menggunakan SNORT.
2. Manfaat yang dihasilkan dari penelitian ini adalah adanya produk sistem HIDS yang nantinya dapat dimanfaatkan *administrator* jaringan untuk mencegah serangan DDOS.

1.4 Batasan Masalah

Agar dalam pembahasan penelitian ini tidak terlalu melebar maka diberikan sebuah batasan masalah yang meliputi:

1. Penelitian ini mengarah pembuatan HIDS pada sebuah *server* yang akan dibangun untuk tujuan mengidentifikasi serangan DDOS, bukan mengarah pada pembuatan IDS untuk segala jenis serangan dan infrastruktur jaringan yang lain.
2. Implementasi sistem menggunakan aplikasi *open source* SNORT.
3. Penelitian ini menggunakan topologi Internet, namun tidak menutup kemungkinan HIDS digunakan di topologi yang lain.
4. Penelitian ini membatasi *tools* serangan yang dipakai yaitu hping3, karena *tools* ini dapat menerapkan banyak tipe serangan.

1.5 Metodologi Pengerjaan Tugas Akhir

Metodologi pengerjaan Tugas Akhir adalah gambaran langkah-langkah yang ditempuh dalam menjalankan penelitian, yakni sebagai berikut:

1. Pengumpulan Data
Pengumpulan bahan-bahan literature yang berhubungan dengan topik serta beberapa sumber yang lainnya yang terkait dengan *Host based Intrusion Detection System*, *Snort*, dan *Distributed Denial Of Service*.
2. Studi Literatur
Pada tahap ini dipelajari bahan-bahan literatur yang didapat pada tahap pengumpulan data. Literatur yang didapat berasal dari buku, jurnal, materi kuliah, dan materi-materi lain yang terkait.

3. Analisis
Melakukan analisis lebih lanjut terhadap masalah yang dikaji serta batasan-batasan masalah tersebut dan analisis terhadap metode *Intrusion Detection* dan *DDOS* yang akan diimplementasikan.
4. Perancangan Sistem
Menentukan perancangan/desain sistem didasarkan pada beberapa teori yang diperoleh dan mempelajari konsep teknologi dari *software* yang ada. Pada tahapan ini dilakukan desain proses-proses yang akan dibuat.
5. Implementasi Sistem
Untuk tahap pengimplementasian desain sistem.
6. Pengujian dan Evaluasi
Pada tahap ini dilakukan uji coba pada program yang telah dibuat, mengamati kinerja sistem yang telah dibuat, apakah sudah sesuai dengan tujuan penelitian, serta melakukan perbaikan apabila terdapat kesalahan ataupun kekurangan.
7. Penyusunan Laporan Tugas Akhir
Penyusunan laporan dilakukan pada tahap akhir sebagai dokumentasi dari pelaksanaan penelitian. Dokumentasi ini dibuat untuk menjelaskan proses penelitian agar memudahkan orang lain yang ingin mengembangkan penelitian ini. Dengan adanya penyusunan laporan diharapkan dokumentasi sistem dan seluruh tahapan penelitian tersusun dengan rapi.

1.6 Sistematika Penulisan

Secara garis besar, penulisan buku Tugas Akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bagian ini dipaparkan tentang hal-hal yang melatar belakangi penelitian, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah, dan metodologi penelitian yang digunakan dalam menyelesaikan Tugas Akhir ini, serta sistematika penulisan dalam penulisan buku Tugas Akhir ini.

BAB II TEORI PENUNJANG

Bab ini membahas tentang teori-teori yang digunakan dalam merencanakan dan menyelesaikan Tugas Akhir ini. Pustaka yang digunakan baik dari buku, jurnal, maupun materi dari internet.

BAB III PERANCANGAN SISTEM

Bab ini membahas tentang rancangan sistem dari keseluruhan sistem yang akan dibuat, yang meliputi pembuatan *System Intrusion Detection*.

BAB IV IMPLEMENTASI PROGRAM

Bab ini membahas tentang implementasi sistem yang telah dirancang pada tahap sebelumnya ke dalam aplikasi program serta berisi penjelasan mengenai bagian-bagian atau fitur-fitur apa saja yang ada dalam aplikasi program tersebut. Serta analisis sistem hasil uji coba.

BAB V PENUTUP

Bab ini menjelaskan tentang kesimpulan hasil uji coba yang diperoleh setelah menyelesaikan penelitian, dan saran-saran yang dapat digunakan sebagai masukan dalam pengembangan penelitian.