BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sementara itu, masalah keamanan ini masih sering kali kurang mendapat perhatian, seringkali masalah keamanan ini berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan (Rahardjo, 2002).

Keamanan server pada sebuah perusahaan *Internet Service Provider* (ISP) adalah salah satu faktor penting yang harus menjadi perhatian serius bagi sebuah perusahaan ISP. Kondisi dengan tingkat keamanan yang terjamin, sebuah perusahaan ISP dapat menghindari kerugian yang disebabkan oleh serangan terhadap sistem keamanan jaringan perusahaan ISP tersebut.

Salah satu cara untuk meningkatkan keamanan server dalam jaringan 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. 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.*

Intrusion Detection System diimplementasikan dengan penerapan proses *sniffing,* pengamatan trafik data, dan analisa log trafik. Dengan demikian, seorang administrator dapat mengambil keputusan berdasarkan hasil pengamatan trafik untuk menentukan pengaturan keamanan jaringan yang dikelolanya.

Salah satu perangkat IDS yang sering digunakan pada sistem server adalah *Snort*. *Snort* adalah perangkat lunak berbasis IDS yang pertama kali dibuat dan dikembangkan oleh Martin Roesch, kemudian menjadi sebuah proyek *open source*.

Beberapa keunggulan *Snort* dibandingkan software IDS lain adalah kode sumber yang berukuran kecil, dapat digunakan pada banyak sistem operasi, cepat dan mampu mendeteksi serangan pada jaringan dengan kecepatan hingga 100Mbps, mudah dikonfigurasi dan terutama *Snort* ini bersifat gratis (Geovedi, 2006).

Berdasarkan beberapa pertimbangan di atas, maka akan lebih bermanfaat jika penelitian dilakukan dengan tema Implementasi *Snort* sebagai Tool *Intrusion Detection System.*

B. Rumusan Masalah

Berdasarkan beberapa pertimbangan di atas, maka dapat dirumuskan beberapa rumusan masalah sebagai berikut:

1. Bagaimana langkah implementasi software *Snort* sebagai tool *Intrusion Detection System* pada server ISP?
2. Bagaimana hasil implementasi *Snort* sebagai *Intrusion Detection System* dapat digunakan untuk meningkatkan keamanan sebuah server pada perusahaan ISP?

C. Batasan Masalah

Penelitian ini diharapkan dapat mencapai sasaran dan tujuan, sehingga permasalahan tersebut dibatasi sebagai berikut:

1. Pengamatan trafik data hanya dilakukan pada sisi server pada perusahaan ISP dengan Sistem Operasi *FreeBSD* di PT. Power Telecom cabang Solo.
2. Software yang digunakan untuk melakukan monitoring trafik data dalam penelitian terbatas pada software *Snort*.
3. Pengujian terhadap sistem yang diteliti dilakukan dengan simulasi *virus test* dengan *EICAR virus test file*, simulasi *ping*, *scanning port server*, *SQL Injection*, dan pengaksesan database.
4. Trafik data yang diamati dalam penelitian ini dibatasi pada paket data yang mengarah pada server IDS Snort yang berhubungan dengan keamanan server.

D. Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah:

1. Mengimplementasikan *Snort* sebagai tool *Intrusion Detection Sytem* pada server *FreeBSD* pada PT. Power Telecom Solo.
2. Meningkatkan keamanan pada server ISP dengan *Snort* IDS melalui beberapa pengujian, sehingga didapatkan kesimpulan yaitu manfaat penggunaan *Snort* sebagai tool IDS.

E. Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah:

1. Hasil penelitian ini dapat digunakan sebagai masukan terhadap upaya peningkatan kemananan pada perusahaan ISP.
2. Memberikan referensi bagi penulisan Karya Ilmiah selanjutnya dan menambah sumber pustaka bagi pengembangan sistem jaringan berbasis *open source*.
3. Dapat memberikan referensi dalam mengembangkan kemampuan kalangan akademis dalam menerapkan teori keamanan jaringan komputer.

F. Sistematika Penulisan

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.