

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan. Buku ini diharapkan dapat memberikan gambaran dan informasi bagaimana merancang suatu sistem keamanan untuk melindungi sistem informasi dan dapat membantu para pemilik dan pengelola sistem informasi dalam mengamankan informasinya.

Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah "*information-based society*". Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat. Ini salah satu alasan perusahaan atau organisasi dalam kasus ini Jurusan Teknik Elektro STTTELKOM membuat LAN untuk sistem informasinya dan menghubungkan LAN tersebut ke Internet.

Terhubungnya LAN atau komputer ke Internet membuka potensi adanya lubang keamanan (*security hole*) yang tadinya bisa ditutupi dengan mekanisme keamanan secara fisik. Menurut G. J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya pelanggaran kebijakan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Sehingga dibutuhkan suatu sistem keamanan yang dapat mendeteksi, menganalisa dan bereaksi terhadap serangan tanpa mengurangi performansi servis yang disediakan.

Metode pendekatan yang dapat digunakan untuk mengamankan jaringan adalah dengan menerapkan Adaptive Firewall dengan metode pendekatan *Automated Intelligently Reactive Intrusion Detection System* yang dapat diimplementasikan pada *server* dan *router* berbasis sistem operasi *linux 2.4.x.x*

Sistem keamanan yang dibuat bersifat modular untuk setiap fungsinya, sehingga memudahkan penerapan suatu sistem. Dengan *Linux*, implementasi *network security* dapat diterapkan dengan mengatur dan mengkombinasikan kemampuan-kemampuan yang modular tersebut.

1.2 PERUMUSAN MASALAH

Masalah yang akan dibahas pada tugas akhir ini adalah bagaimana merancang suatu sistem yang aman dan dapat bereaksi secara cerdas terhadap serangan tanpa mengakibatkan degradasi pelayanan sistem informasi dan mampu menampilkan grafik statistik kondisi jaringan untuk memudahkan manajemen keamanan jaringan.

1.3 TUJUAN PENULISAN

Tujuan penulisan tugas akhir ini adalah:

1. Membuat rancangan sistem keamanan yang mampu melindungi sistem informasi pada server database Jurusan Teknik Elektro Stttelkom (ee.stttelkom.ac.id)
2. Sistem keamanan yang dirancang mempunyai kemampuan bereaksi secara cerdas dengan metodologi *Automated Intelligently Reactive Intrusion Detection System*.
3. Mengimplementasikan dan menguji rancangan sistem

1.4 PEMBATAAN MASALAH

Pembatasan masalah untuk tugas akhir ini adalah :

1. Ancaman serangan yang mungkin terjadi diasumsikan hanya berasal dari *internal network* STT Telkom.
2. Pengujian terhadap sistem dibatasi terhadap serangan berbentuk *scanning, exploiting* dan *flooding*

1.5 METODOLOGI PENYELESAIAN

Metodologi yang digunakan dalam tulisan ini adalah:

- Meninjau beberapa aspek pendukung seperti buku, jurnal, majalah dan artikel yang berkaitan dengan topik ini
- Merancang dan mengimplementasikan arsitektur sistem keamanan pada pc *Linux*
- Melakukan percobaan guna menguji implementasi dengan metoda yang diajukan

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan pada Tugas Akhir ini akan mengikuti pola sebagai berikut:

- BAB I PENDAHULUAN**
Berisi tentang latar belakang, tujuan, permasalahan, pembatasan masalah, dan metodologi, dan sistematika penulisan.
- BAB II DASAR TEORI**
Berisi teori yang dibutuhkan dan penjelasan tentang sistem sekuriti jaringan dan TCP/IP.
- BAB III PERANCANGAN DAN IMPLEMENTASI**
Berisi perancangan suatu sistem keamanan pada server database Jurusan Teknik Elektro STT Ttelkom berbasis sistem operasi *Linux* dengan mengimplementasikan arsitektur dan metodologi *Automatically Intelligent Reactive Intrusion Detection System*
- BAB IV ANALISA DATA PERCOBAAN**
Berisi hasil percobaan dari implementasi rancangan Arsitektur sistem keamanan serta pengujian
- BAB V PENUTUP**
Bab ini berisi kesimpulan yang diperoleh dalam analisa tugas akhir ini dan saran-saran yang diperoleh dari pengamatan.