BAB I

PENDAHULUAN

I.1 Latar Belakang

Berkembangnya teknologi informasi khususnya jaringan komputer dan layanan-layanannya di satu sisi mempermudah pekerjaan-pekerjaan manusia sehari-hari, akan tetapi di sisi lain timbul masalah yang sangat serius, yakni faktor keamanannya. Di satu sisi manusia sudah sangat tergantung dengan sistem informasi, akan tetapi di sisi lain statistik kejahatan *cyber* meningkat tajam. Hal ini secara umum terjadi karena kepedulian terhadap keamanan sistem informasi masih sangat kurang.

Untuk mencegah terjadinya kejahatan *cyber*, seperti menyerang suatu jaringan komputer, menyusup kedalam suatu jaringan untuk mengambil data – data yang bersifat rahasia dan melumpuhkan suatu sistem jaringan, maka perlu dilakukan langkah – langkah pengamanan pada suatu sistem jaringan komputer dengan membuat suatu sistem keamanan yang dapat menangkal serangan dan usaha penyusupan baik dari sisi *external* dan *internal* suatu sistem jaringan komputer.

Network Operation Center Universitas Kristen Maranatha, sebagai suatu biro yang melakukan pemeliharaan terhadap jaringan komputer di Universitas Kristen Maranatha juga membutuhkan suatu sistem keamanan jaringan yang baik terhadap serangan dan penyusupan baik dari sisi *external* maupun *internal.* Sistem keamanan yang selama ini dimiliki hanya dapat mendeteksi adanya serangan yang dilakukan oleh *user*, virus maupun Trojan tanpa bisa mencegah dan mengatasi serangan – serangan yang ada, serta belum dimilikinya suatu sistem pembaharuan pada *knowledge base* dan anti virus, sehingga pada *client* yang berada dalam satu jaringan lokal di Universitas Kristen Maranatha berada dalam kondisi yang aman

sehingga tidak terdapat virus maupun Trojan yang dapat melakukan serangan pada sisi *server*.

I.2 Identifikasi Masalah

Dalam kehidupan sehari – hari, ketergantungan *user* akan suatu sistem informasi haruslah ditunjang dengan keamanan sistem informasi tersebut. Banyaknya ancaman kejahatan *cyber*, seperti usaha penyusupan pada suatu sistem jaringan komputer, serangan pada sistem jaringan komputer yang bertujuan untuk membuat suatu sistem tersebut down dan ancaman dari sisi *internal* seperti ancaman serangan virus dan trojan terhadap *server* yang masuk melalui *client side*, menuntut adanya suatu sistem keamanan yang dapat menangkal ancaman – ancaman tersebut. Suatu sistem yang dapat mendukung kebutuhan itu adalah sistem yang mampu melakukan deteksi dan kemudian pencegahan terhadap usaha penyusupan dan serangan, serta sistem yang mampu melakukan pembaharuan pada jaringan *internal* di *client side*.

I.3 Perumusan Masalah

Perumusan masalah yang akan dibahas dalam tugas akhir ini adalah bagaimana merealisasikan suatu sistem keamanan yang dapat menangkal serangan dan usaha penyusupan terhadap suatu sistem jaringan komputer, baik dari sisi *external* maupun sisi *internal*? Dan sistem tersebut dapat melewati *penetration test* yang sesuai dengan standar yang diujikan.

I.4 Tujuan

Tujuan yang akan dicapai dalam tugas akhir ini adalah untuk membuat sistem yang mampu melakukan deteksi dan pencegahan terhadap usaha penyusupan dan serangan serta sistem untuk pembaharuan *virus definitions* pada software anti virus dan server *operating sistem update* menggunakan *knowledge base* pada jaringan *internal* di *client side*. Sistem keamanan tersebut juga harus dapat melewati *standard operation procedure* dari suatu *penetration test* yang diujikan.

I.5 Pembatasan Masalah

Pembatasan masalah pada tugas akhir ini dibatasi oleh :

1. Sistem IPS/IDS yang direalisasikan memberikan report kepada System Administrator melalui web application.
2. Jenis serangan yang diujikan pada penetration test adalah serangan yang biasa dilakukan pada suatu jaringan komputer.
3. Sistem keamanan yang dirancang dan diimplementasikan disesuaikan dengan kebutuhan dan sistem yang telah ada pada jaringan Universitas Kristen Maranatha.

I.6 Spesifikasi Sistem

1. Server untuk IPS/IDS menggunakan Ubuntu 8.04 dan menggunakan software Snort 2.8.4. Server untuk Symantec Endpoint Protection Update Server dan Windows Update Services menggunakan Windows 2003 R2 SP2 yang dijalankan di Virtual Machine menggunakan GSX.
2. Sistem keamanan terdiri dari 4 buah server, 2 buah server untuk sistem pencegahan dan pendeteksi penyusupan serta serangan, 1 buah server untuk pembaharuan *virus definitions* dan 1 buah server untuk pembaharuan *knowledge base* pada *client side*.

I.7 Sistematika Penulisan

Laporan tugas akhir ini disusun dengan sistematika sebagai berikut:

- **Bab I**

  Membahas latar belakang masalah, identifikasi masalah, tujuan dibuatnya makalah ini, batasan-batasan masalah, serta sistematika penulisan laporan ini.
- **Bab II**

  Menjelaskan teori-teori yang diperlukan dan menjadi landasan dalam melakukan tugas akhir ini, seperti teori OSI Layer, TCP/IP .
- **Bab III**

  Membahas mengenai perancangan sistem keamanan dan cara kerja dari sistem keamanan yang dibuat.
- **Bab IV**

  Membahas hasil pengujian beserta analisis dari pengetesan terhadap sistem keamanan menggunakan Standart Opersional Prosedur pada Penetration Test.
- **Bab V**

  Merumuskan kesimpulan dan saran.