BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Saat ini teknologi informasi telah berkembang sangat pesat sehingga menjadikan informasi merupakan sesuatu yang sangat penting untuk diperoleh dan dipertahankan. Kebutuhan akan informasi yang terbaru dan dapat dipercaya menjadi hal utama yang harus diperhatikan. Hal ini menyebabkan munculnya kebutuhan akan adanya jaringan komputer yang dapat menghubungkan beberapa komputer pada suatu area tertentu. Penggunaan jaringan komputer ini dapat mempercepat arus informasi dari satu tempat ke tempat lain dan telah banyak memberi kemudahan dalam berkomunikasi kepada para penggunanya.

Penggunaan jaringan komputer baik skala kecil pada LAN (*Local Area Network*) maupun skala besar pada WAN (*Wide Area Network*) memiliki tantangan yang harus dihadapi. Contohnya antara lain: serangan *virus* dan serangan berupa akses dari pihak-pihak yang tidak berkepentingan. Serangan-serangan tersebut harus dapat ditangani dengan baik karena sekecil apapun serangan dapat menimbulkan kerugian finansial dan waktu yang tidak sedikit. Seiring dengan perkembangan dunia informasi maka muncullah ide mengenai IDS *(Intrusion Detection System*) yang dapat mendeteksi serangan-serangan yang ada didalam jaringan. Dengan mengetahui adanya serangan lebih awal, maka dapat dilakukan langkah-langkah pencegahan serangan yang lebih baik. Selain itu dengan adanya IDS, maka informasi mengenai setiap aktivitas di dalam jaringan meliputi siapa, apa, kapan, dan dimana aktivitas itu terjadi dapat diketahui.

1.2 Pokok Permasalahan

Teknik keamanan jaringan juga mengalami perkembangan terus menerus seiring dengan semakin banyaknya jaringan komputer yang ada. Hal ini menyebabkan teknik IDS juga mengalami banyak perkembangan. Ada banyak cara dan peralatan yang dapat digunakan untuk menjaga keamanan jaringan. Implementasi IDS bisa menggunakan aplikasi antara lain: ISS *Real Secure*, *Cisco*, *Tiger*, *Swatch*, dan *Snort*. IDS juga berkembang dengan munculnya teknik IPS (*Intrusion Prevention System)* yang menawarkan solusi keamanan bukan hanya dapat mendeteksi tetapi juga dapat mencegah serangan-serangan tersebut. Akan tetapi hal ini tidak membuat IDS ditinggalkan penggunanya karena dalam suatu sistem selain dibutuhkan IPS sebagai pencegah serangan juga diperlukan IDS yang mendeteksi dan dapat memberikan laporan harian mengenai aktivitas yang terjadi di dalam jaringan.

Permasalahan yang akan dibahas dalam laporan kerja praktek ini adalah bagaimana implementasi IDS menggunakan perangkat lunak aplikasi *Snort* dan BASE (*Basic Analysis and Search Engine*) pada suatu jaringan. Setelah selesai dalam implementasi IDS maka harus diperhatikan juga mengenai serangan apa saja yang berhasil dipantau oleh aplikasi *Snort* sehingga dapat ditentukan langkah-langkah pencegahannya.

1.3 Pembatasan Masalah

Ruang lingkup penelitian yang dilakukan di PT. Broadband Multimedia Tbk. yaitu melakukan implementasi *Snort* dan BASE sebagai IDS hanya pada *Linux Fedora Core* 5. Hal ini dikarenakan sistem operasi yang digunakan pada

server adalah *Linux Fedora Core* 5. Alamat IP yang dapat mengakses BASE juga hanya alamat IP dari *server*. Aplikasi *Snort* yang diinstalasi dan dikonfigurasi harus dapat memantau jaringan selama 24 jam dalam satu hari dan menampilkan laporannya pada BASE.

1.4 Tujuan Penelitian

Adapun tujuan penelitian yang dilakukan di PT. Broadband Multimedia Tbk. adalah sebagai berikut:

1) Mempelajari teknik untuk instalasi dan konfigurasi aplikasi *Snort* dan BASE sebagai IDS.
2) Membangun sistem keamanan jaringan menggunakan IDS.

1.5 Metodologi Penelitian

Metodologi penelitian yang dilakukan adalah melalui metodologi pembelajaran, yaitu studi literatur dan studi lapangan. Studi literatur dengan membaca buku-buku referensi dan dari *Internet*. Studi lapangan dengan bertanya kepada pembimbing dan belajar dari kesalahan-kesalahan (*error*) yang terjadi pada saat pelaksanaan kerja praktek.

Penelitian ini dilaksanakan dalam jangka waktu satu setengah bulan, yaitu mulai dari 1 Juni 2006 sampai dengan 14 Juli 2006, total sebanyak 286 jam. Adapun perincian kegiatan selama penelitian dapat dilihat pada tabel di halaman berikut ini:

Tabel 1. 1 *Time Frame*

No	Kegiatan	Durasi	Minggu Ke-						
			1	2	3	4	5	6	7
1	Pre-Inisialisasi	1 hari							
2	Inisialisasi sistem	1 hari							
3	Instalasi								
a	OS Linux Fedora Core 5	1 hari							
b	Apache, PHP, dan MySQL	1 hari							
4	Studi pustaka	7 hari							
5	Pengenalan server	1 hari							
6	Download aplikasi Snort dan BASE	2 hari							
7	Instalasi dan konfigurasi Aplikasi Snort	3 hari							
8	Instalasi dan konfigurasi BASE	3 hari							
9	Evaluasi hasil konfigurasi	2 hari							
10	Pekerjaan lain	10 hari							
11	Pelaksanaan Project Management	7 hari							
12	Presentasi	1 hari							
13	Penyusunan laporan ke perusahaan	11 hari							

Keterangan:

1) Pre-Inisialisasi

Penelitian ini dilakukan oleh empat orang yang memiliki ruang lingkup penelitian yang berbeda-beda, tetapi pada akhirnya akan digabung menjadi satu projek besar. Oleh karena itu sebelum penelitian dimulai diberikan penjelasan mengenai *job description* masing-masing.

2) Inisialisasi Sistem

Pada tahap ini disiapkan hal-hal yang dibutuhkan dan ruangan khusus untuk melakukan penelitian. Penelitian ini membutuhkan sebuah komputer untuk *server*, sebuah komputer sebagai *Firewall*, sebuah *switch*, dan beberapa komputer sebagai *client*.

3) Instalasi

a) Sistem operasi (OS) *Linux Fedora Core* 5

Pada tahap ini dilakukan instalasi *Linux Fedora Core* 5 sebagai sistem operasi untuk *server*.

b) *Apache*, PHP, dan *MySQL*

Pada tahap ini dilakukan instalasi *Apache* sebagai *web server*, PHP sebagai bahasa pemrograman yang digunakan dan *MySQL* sebagai aplikasi *database*. Proses instalasi *Apache*, PHP, dan *MySQL* biasanya sudah termasuk pada saat instalasi *Linux Fedora Core* 5, sehingga pada tahap ini hanya perlu memeriksa apakah *Apache*, PHP, dan *MySQL* sudah ada atau belum. Jika belum ada maka ulangi tahap instalasi OS *Linux Fedora Core* 5.

4) Studi pustaka

Pada tahap ini dilakukan pencarian dan pembelajaran bahan-bahan mengenai IDS, *Snort* dan BASE sebagai aplikasi dari IDS. Pencarian ini meliputi melalui *Internet* atau buku-buku kuliah yang terkait dengan topik penelitian.

5) Pengenalan *Server*

Pada tahap ini diperlihatkan *server* yang ada pada perusahaan. Hal ini bertujuan agar diperoleh pengetahuan mengenai bentuk dan cara kerja *server*.

6) *Download Snort* dan BASE

Aplikasi *Snort* dan BASE yang akan digunakan harus di-*download* terlebih dahulu dari *website Snort*: http://www.snort.org. Tahap *download* ini dilakukan oleh *administrator* khusus dari perusahaan yang memiliki hak akses untuk melakukan *download* aplikasi *Snort* dan BASE versi terbaru.

7) Instalasi dan konfigurasi *Snort*

Pada tahap ini dimulai pelaksanaan instalasi dan konfigurasi aplikasi *Snort* sebagai IDS yang digunakan. Instalasi dan konfigurasi ini dilakukan pada komputer *server*. Tahap konfigurasi antara lain memilih fasilitas-fasilitas yang mampu dilakukan oleh aplikasi *Snort* sehingga menjadikan aplikasi

Snort berfungsi dengan sebaik-baiknya. Pada tahap ini juga dilakukan pembuatan tabel pada *database MySQL* yang akan menyimpan hasil pantauan *Snort*.

8) Instalasi dan konfigurasi BASE

Setelah selesai melakukan instalasi aplikasi *Snort*, maka dimulailah tahap instalasi BASE yang berfungsi sebagai GUI (*Graphical User Interface*) yang menampilkan hasil pantauan dari aplikasi *Snort*. Tahap konfigurasi BASE meliputi antara lain: menentukan *database* yang akan ditampilkan, alamat *url* yang akan digunakan oleh BASE, *username* dan *password* yang akan digunakan untuk akses BASE.

9) Evaluasi hasil konfigurasi

Pada tahap ini dilakukan pengamatan terhadap hasil pantauan yang dilakukan oleh aplikasi *Snort* dan BASE. Hasil konfigurasi ini dapat digunakan untuk memantau setiap serangan-serangan yang ada di dalam jaringan. Selain itu setiap *link* yang terdapat pada *website* BASE dicoba apakah dapat menampilkan informasi yang sesuai dengan kebutuhan.

10) Membantu pekerjaan lain

Pada penelitian ini, selain melakukan implementasi IDS juga dilakukan pekerjaan lain yang bertujuan membantu perusahaan tersebut. Pekerjaan yang dilakukan antara lain: melakukan pencatatan nomor *asset* setiap komputer yang ada di seluruh kantor PT. Broadband Multimedia Tbk. untuk keperluan inventaris ulang *database* komputer yang dimiliki oleh perusahaan dan memperbaiki kabel yang digunakan untuk *line* telepon pelanggan Kabel Vision.

11) Pelaksanaan *Project Management*

Pada tahap ini dibuat laporan mengenai *Project Management* yang terdiri dari *Business Requirement* (BR), *Requirement Analysis* (RA), dan *Project Plan* (PP). Tujuan dari pelaksanaan *Project Management* adalah agar benar-benar mengalami melaksanakan suatu projek, mulai dari merumuskan permintaan *client* (pada BR), merumuskan apa yang harus dikerjakan oleh bagian IT (pada RA), dan menetapkan jadwal pelaksanaan projek dari awal hingga selesai (pada PP).

12) Presentasi

Presentasi mengenai apa yang telah dilaksanakan selama kerja praktek. Presentasi ini dilaksanakan di kantor dengan dihadiri oleh pembimbing dan beberapa kepala divisi.

13) Penyusunan laporan ke perusahaan

Pada tahap ini dilakukan penyusunan Laporan Kerja Praktek untuk perusahaan sebagai bahan pertanggungjawaban terhadap apa yang telah dikerjakan selama masa kerja praktek. Penyusunan laporan meliputi hasil aplikasi yang telah dibuat selama kerja praktek.

1.6 Sistematika Penyajian

Sistematika penyajian Laporan Kerja Praktek ini dibagi menjadi beberapa bab sebagai berikut:

Bab I Pendahuluan

Pada bab ini dibahas mengenai permasalahan yang ada sehingga butuh dilakukan penelitian ini. Dalam bab ini juga termasuk tujuan dan metodologi dalam melakukan penelitian ini beserta *time frame* pelaksanaan penelitian.

Bab II Landasan Teori

Pada bab ini dibahas mengenai teori-teori mengenai IDS, mulai dari sejarah penggunaan IDS, teknik-teknik yang dilakukan oleh IDS, tipe-tipe IDS, beserta penjelasan mengenai jenis-jenis serangan yang dapat dideteksi oleh IDS.

Bab III Gambaran Umum Perusahaan

Pada bab ini dibahas mengenai profil perusahaan tempat dilakukan penelitian, gambaran umum perusahaan, layanan yang diberikan oleh perusahaan kepada masyarakat, struktur organisasi pada perusahaan, dan bentuk jaringan yang sudah dimiliki oleh perusahaan.

Bab IV Analisis dan Perancangan

Pada bab ini dibahas kebutuhan sistem untuk pengembangan teknik keamanan menggunakan IDS. Dalam bab ini terdapat tahap pengimplementasian dan informasi mengenai hasil yang telah dicapai.

Bab V Kesimpulan dan Saran

Pada bab ini dibahas kesimpulan dari seluruh Laporan Kerja Praktek ini dan saran-saran yang dapat mendukung perkembangan penelitian lebih lanjut.