BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan *website* yang semakin cepat dengan berbagai macam fungsi dan kebutuhan, menuntut meningkatnya kualitas keamanan jaringan *webserver*. Terutama dengan semakin terbukanya pengetahuan *hacking* dan *cracking*, didukung dengan banyaknya *tools* yang tersedia dengan mudah dan -kebanyakan-*free*, semakin mempermudah para *intruder* dan *attacker* untuk melakukan aksi penyusupan ataupun serangan.

Pencegahaan yang paling sering dilakukan untuk masalah ini adalah dengan menempatkan seorang *administrator*. Seorang *administrator* bertugas untuk mengawasi dan melakukan tindakan *preventif* ketika terjadi aksi penyusupan dan serangan.

Masalah timbul ketika *sang administrator* sedang tidak berada pada posisi siap sedia, misalnya sakit, berada di luar jam kerja, atau adanya kepentingan mendadak. Sedangkan serangan terhadap *server* bisa terjadi kapan saja.

Maka, dari permasalahan tersebut, *administrator* membutuhkan suatu sistem yang dapat membantu mengawasi jaringan, menginformasikan serangan, dan mengambil tindakan tepat untuk pencegahan yang akan membantu mengautomatisasi fungsi kerja dasar *administrator*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan di atas, maka dapat ditarik rumusan permasalahan sebagai berikut :

1. Bagaimana membuat sistem yang dapat mengawasi lalu lintas jaringan pada *webserver* secara rutin?
2. Tindakan apa yang tepat dilakukan oleh sistem dalam mengatasi berbagai macam penyusupan ataupun serangan?
3. Bagaimana informasi mengenai ancaman dan serangan pada server dapat sampai dengan cepat kepada *administrator security?*

1.3 Batasan Masalah

Agar ruang lingkup permasalahan tidak melebar, maka diperlukan parameter batasan masalah, antara lainnya adalah :

1. *Intrusion Prevention System* (IPS) merupakan sistem keamanan jaringan yang mampu ditempatkan di berbagai macam lalu lintas jaringan, tetapi dalam penelitian kali ini, IPS akan ditempatkan pada sebuah *webserver.*
2. Core IPS yang dipakai menggunakan Snort, sehingga *rule* yang dipakai kemudian adalah *rule – rule* Snort.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

- Membantu *administrator* dalam pengawasan jaringan server.
- Mengautomatisasi tindakan yang diambil ketika muncul gejala intrusi.
- Memberikan informasi yang tepat dan cepat mengenai serangan dan ancaman kepada *administrator*.

1.5 Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini dapat dilihat dari pencapaian tujuan penelitian, yaitu :

- *Administrator* akan terbantu oleh sistem dalam pengawasan jaringan, sehingga tidak akan timbul masalah ketika *administrator* sedang lengah atau berada di luar jam kerja.
- Automatisasi tindakan yang dilakukan oleh sistem akan sangat membantu *administrator* dalam pemilihan tindakan, terutama ketika dibutuhkan tindakan yang cepat.
- Informasi yang diterima oleh *administrator* bisa menjadi bahan pertimbangan untuk perbaikan keamanan jaringan, seperti menutupi celah – celah keamanan yang *vulnerable*.

1.6 Metode Pengumpulan Data

Penyusunan skripsi ini sangat diperlukan sumber-sumber data dan informasi yang benar dan akurat sehingga dapat menjadi masukan yang berguna dalam proses penyusunan skripsi ini. Untuk memperoleh data-data dan informasi-informasi yang benar dan akurat tersebut maka ada beberapa metode yang dapat dilakukan, antara lain:

1. Metode Eksperimental / Uji Coba

   Penulis akan melakukan melakukan uji coba langsung terhadap subjek penelitian. Perbandingan antara sebelum dan sesudah penggunaan sistem akan menghasilkan data penelitian.

2. Metode Kepustakaan

   Penulis akan mengambil data dari *literature*, majalah, artikel, atau buku-buku, baik yang bersifat cetak maupun internet yang berkaitan dengan permasalahan yang akan diteliti.

3. Metode Interview

   Penulis akan melakukan komunikasi langsung dengan para responden yang terkait mengenai masalah yang sedang diteliti.

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini adalah dengan membagi tiap kelompok bahasan menjadi bab dan sub bab yang akan dibahas secara terinci pada tiap – tiap bab. Berikut ini adalah susunan bab dan keterangannya secara singkat :

BAB I PENDAHULUAN

Bab ini akan dijelaskan tentang latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, metodologi penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi teori – teori yang berkaitan dengan penelitian yang akan menjadi landasan penulisan penelitian skripsi ini. Seperti segala dasar teori mengenai keamanan jaringan dan teori lain yang berhubungan dengan perancangan sistem yang akan dibuat.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini dibahas mengenai analisa kebutuhan sistem dan perancangan yang dibuat, serta menganalisa kelebihan dan kekurangan dari sistem, dan menganalisa perbandingan antara sistem yang lama dan sistem yang baru.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini akan menjelaskan mengenai proses – proses yang berkaitan dengan impelementasi, mulai dari tata cara instalasi IDS dan program – program pendukung ke server, konfigurasi yang harus dilakukan, dan pembahasan mengenai pengujian sistem yang bersifat internal maupun eksternal.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran. Menyimpulkan bukti – bukti yang diperoleh dari hasil uji penelitian, serta kemampuan menjawab pertanyaan dari rumusan masalah. Serta saran yang merupakan manifestasi penulis untuk dilaksanakan yang bisa menutupi kelemahan – kelemahan sistem dan berguna dalam pengembangan sistem di kemudian hari.

1.8 Jadwal Rencana Kegiatan

Tabel 1.1 Jadwal Kegiatan

	Kegiatan	Mei 2011				Juni 2011				Juli 2011			
		1	2	3	4	1	2	3	4	1	2	3	4
1	Persiapan												
2	Pencarian Referensi dan Data												
3	Penyusunan Laporan												
4	Perancangan Sistem												
5	Penyelesaian												