

# BAB I

## PENDAHULUAN

### 1.1. Latar Belakang Masalah

Dewasa ini aplikasi berbasis web berkembang dengan amat pesatnya. Hal ini disebabkan karena sumber pembelajaran yang mudah ditemui. Namun perkembangan web dan kemudahan pembuatannya ini tidak diimbangi dengan analisa keamanan yang baik. Sehingga menyebabkan aplikasi web menjadi sangat rentan terhadap serangan yang dilakukan oleh para *attacker*.

Terdapat banyak cara untuk melindungi aplikasi dan server web dari serangan *attacker* yang tidak bertanggung jawab. Diantaranya adalah melakukan pengujian terhadap aplikasi yang hendak *dipublish*. Namun, hal ini tidak menjadi jaminan bahwa aplikasi dan server akan aman. Hal ini dikarenakan teknik *attacking* terus berkembang seiring dengan makin tingginya pengamanan dari aplikasi. Disamping itu, administrator tidak selalu tahu serangan-serangan apa saja yang masuk.

*Intrusion Prevention System* disingkat IPS hadir dengan memberikan sebuah solusi dari permasalahan ini. *Intrusion Prevention System* adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan (anomali) dalam sebuah sistem atau jaringan. *Intrusion Prevention System* dapat melakukan inspeksi terhadap lalu lintas inbound dan

outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan) kemudian dilakukan tindakan pencegahan jika ditemukan sesuatu yang mencurigakan.

### 1.2. Perumusan Masalah

Masalah-masalah yang timbul dalam penyusunan Tugas Akhir ini antara lain:

1. Bagaimana mengetahui suatu kegiatan dikenali sebagai sebuah tindakan anomali dan berpotensi menimbulkan kerusakan pada aplikasi web?
2. Bagaimana IPS dapat melindungi sebuah aplikasi dan server web dari server dan dampak yang diakibatkan olehnya.
3. Bagaimana meminimalkan *false positive* dan *false negative*?

### 1.3. Batasan Masalah

Ruang lingkup dalam penyusunan tugas akhir ini dibatasi pada:

1. IPS diterapkan pada aplikasi web yang menggunakan teknologi Linux, Apache, MySQL, PHP.
2. Sistem Operasi yang digunakan adalah openSUSE Linux.
3. Perangkat lunak pemrograman menggunakan Perl sebagai *Core Engine* IPS dan PHP sebagai antarmuka *Front-End*.
4. Jenis intrusi yang akan diperiksa adalah intrusi berbasis aplikasi seperti *Injection Flaws*, *XSS (Cross Site Scripting)* dan *Malicious File Execution*.

#### 1.4. Tujuan Tugas Akhir

Tujuan dari pembuatan Tugas Akhir ini adalah menerapkan teknologi *Intrusion Prevention System* sebagai pemantau dan melindungi aplikasi web terhadap tindakan *attacking*. *Intrusion Prevention System* akan mendeteksi tindakan *attacking* yang ditujukan kepada aplikasi dan sistem, untuk kemudian melakukan tindakan yang diperlukan. Dengan cara kerja seperti ini, diharapkan dapat meminimalisir kerusakan yang diakibatkan dari tindakan *attacking*.

#### 1.5. Manfaat Penelitian

Adapun manfaat dari penelitian yang dilakukan antara lain:

1. Memantau dan melindungi aplikasi web dari para *attacker* yang tidak bertanggung jawab.
2. Memudahkan administrator sistem dan programmer dalam mengevaluasi aplikasi dan sistem yang sedang berjalan.
3. Meminimalisir kerusakan yang diakibatkan atas tindakan *attacking*.

#### 1.6. Metodologi Penyusunan

Dalam menyelesaikan Tugas Akhir *Intrusion Prevention System* untuk Aplikasi Berbasis Web, digunakan beberapa langkah atau metode, antara lain:

1. Metode studi pustaka, mempelajari referensi yang berasal dari internet, cd dan buku literatur.
2. Analisis dan perancangan, melakukan analisis dan perancangan terhadap

kebutuhan perangkat lunak maupun perangkat keras yang digunakan untuk membangun *Intrusion Prevention System* untuk Aplikasi Berbasis Web.

3. Pembuatan aplikasi dan menerapkan hasil analisis berdasarkan rancangan yang dibuat.
4. Melakukan pengujian terhadap aplikasi *Intrusion Prevention System* untuk Aplikasi Berbasis Web.
5. Pengambilan kesimpulan dari hasil pengujian dan analisa kemudian memberikan saran-saran untuk pengembangan selanjutnya.

#### 1.7. Sistematika Pembahasan

Penyusunan Tugas Akhir ini dibagi menjadi lima bab, yang terdiri dari:

##### **BAB I. PENDAHULUAN**

Bab ini membahas mengenai latar belakang masalah, perumusan masalah, batasan masalah, tujuan Tugas Akhir, metodologi penyusunan, dan sistematika penyusunan laporan.

##### **BAB II. DASAR TEORI**

Pada bagian ini akan dijelaskan mengenai teori-teori yang berhubungan dengan *Intrusion Prevention System* untuk Aplikasi Berbasis Web yang digunakan sebagai bahan kajian dalam melakukan analisis dan perancangan dan penerapan Tugas Akhir.

##### **BAB III. ANALISIS DAN PERANCANGAN**

Bab ini membahas mengenai analisis masalah yang akan digunakan

sebagai sarana yang memudahkan pembuatan aplikasi *Intrusion Prevention System* untuk Aplikasi Berbasis Web.

#### **BAB IV IMPLEMENTASI DAN PENGUJIAN PERANGKAT LUNAK**

Pada bagian ini dijelaskan penerapan dan pengujian perangkat lunak.

#### **BAB V KESIMPULAN DAN SARAN**

Bab ini berisi kesimpulan terhadap perangkat lunak yang berdasarkan dari hasil pengujian dan analisa yang telah dilakukan serta-saran yang bermanfaat untuk pengembangan lebih lanjut.

##### **1.8. Jadwal Penelitian**

Jadwal penelitian, pembuatan program aplikasi *Intrusion Prevention System* untuk Aplikasi Berbasis Web adalah sebagai berikut:

**Tabel 1.1 Timeline penelitian**

| No | Kegiatan        | Bulan   |   |   |   |       |   |   |   |     |   |   |   |      |   |   |   |  |  |
|----|-----------------|---|---|---|---|-------|---|---|---|-----|---|---|---|------|---|---|---|--|--|
|    |                 | Maret   |   |   |   | April |   |   |   | Mei |   |   |   | Juni |   |   |   |  |  |
|    |                 | 1   | 2 | 3 | 4 | 1     | 2 | 3 | 4 | 1   | 2 | 3 | 4 | 1    | 2 | 3 | 4 |  |  |
| 1  | Studi Literatur | 1. Menentukan permasalahan (latar belakang, rumusan, batasan, tujuan dan manfaat) |   |   |   |       |   |   |   |     |   |   |   |      |   |   |   |  |  |
|    |                 | 2. Memahami cara kerja IPS.   |   |   |   |       |   |   |   |     |   |   |   |      |   |   |   |  |  |
|    |                 | 3. Mengumpulkan landasan  |   |   |   |       |   |   |   |     |   |   |   |      |   |   |   |  |  |

