BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Id-SIRTII/CC (*Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center*) merupakan pertahanan pertama untuk melindungi user-user di Indonesia dari kejahatan yang mungkin terjadi di dunia maya berupa sebuah tim yang bertugas untuk menjaga keamanan informasi data di Indonesia, terutama dari serangan *cracker* iseng yang banyak menyerang web dan server internet di Indonesia.

Berdasarkan wawancara dengan staf *Laboratorium Data Mining Deputy of Research and Development* Id-SIRTII/CC pada tanggal 10 September 2012, kasus atau insiden yang menimpa sistem informasi dan teknologi pendukung pemilu 2004 di Indonesia membuka mata masyarakat umumnya dan Id-SIRTII/CC khususnya, akan besarnya ancaman keamanan yang dapat menimpa berbagai sistem berskala nasional apapun yang ada di tanah air. Bila eksploitasi tersebut diabaikan dan terjadi pada obyek vital yang ada di Indonesia, seperti pada sistem pembayaran nasional, sistem distribusi listrik, sistem persenjataan militer, sistem pelabuhan udara, dan lain sebagainya, akan melumpuhkan semua aktifitas yang sedang dilakukan.

Dalam hal ini, jika terjadi insiden web yang telah disusupi oleh peretas, staf *Laboratorium Data Mining Deputy of Research and Development* Id-SIRTII/CC mencari informasi di situs Zone-h (http://www.zone-h.org) dan Indonesian Defacer (http://indonesiandefacer.org). Data tersebut digunakan untuk *traffic monitoring* insiden. Adapun tujuan dilakukan *traffic monitoring* adalah untuk mempermudah melihat website berdomain Indonesia yang telah disusupi oleh peretas. Saat ini, proses penyajian data masih dilakukan secara manual dan belum tervirtualisasi dengan baik, sehingga pada saat proses *monitoring* mengalami kesulitan saat akan melakukan analisis insiden dari berbagai kondisi.

Dari permasalahan tersebut, maka *Laboratorium Data Mining Deputy of Research and Development* di Id-SIRTII/CC membutuhkan alat bantu kerja

berupa piranti lunak untuk memonitoring insiden web berbasis protokol internet di Indonesia yang nantinya dapat menyimpan rekaman transaksi (*log file*).

1.2 Perumusan Masalah

Dari latar belakang diatas, masalah dapat dirumuskan menjadi bagaimana cara membangun piranti lunak untuk memonitoring insiden web yang terjadi di Id-SIRTII/CC.

1.3 Maksud dan Tujuan

Berdasarkan permasalahan yang diteliti, maka maksud dari penulisan tugas akhir ini adalah untuk membangun virtualisasi data *traffic monitoring* insiden berbasis web di Id-SIRTII/CC.

Sedangkan tujuan yang akan dicapai dalam penelitian ini adalah memudahkan melakukan pemantauan website berdomain Indonesia yang disusupi oleh peretas dan peringatan terhadap ancaman serta gangguan pada website yang berdomain Indonesia.

1.4 Batasan Masalah

Mengingat luasnya permasalahan yang dihadapi, maka perlu pembatasan masalah agar memudahkan pembahasan selanjutnya, sehingga tidak menyimpang dari permasalahan yang akan dibahas. Batasan masalah tersebut adalah sebagai berikut :

1. Sumber data insiden hanya web yang berdomain Indonesia dan berasal dari *Laboratorium Data Mining Deputy of Research and Development* Id-SIRTII/CC.
2. Untuk pengolahan data menggunakan teknik *Data Mart*.
3. Data yang akan ditampilkan adalah data web domain Indonesia yang telah disusupi oleh peretas berdasarkan jenis domain dan waktu kejadian.
4. Output virtualisasi yang dihasilkan adalah berupa informasi laporan insiden web domain Indonesia dalam bentuk grafik.

5. Metode analisis yang akan digunakan dalam pembangunan piranti lunak ini adalah analisis terstruktur.
6. Perangkat lunak yang akan dibangun berbasis web.

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan untuk membangun virtualisasi data *traffic monitoring* insiden berbasis web di Id-SIRTII/CC ini menggunakan metode analisis deskriptif yaitu suatu metode yang bertujuan untuk mendapatkan gambaran yang jelas tentang hal-hal yang diperlukan, melalui tahap pengumpulan data dan tahap pembangunan perangkat lunak.

1.5.1 Tahap Pengumpulan Data

Metode pengumpulan data adalah tahap awal dalam melakukan suatu penelitian. Metodologi yang digunakan dalam mengumpulkan data yang berkaitan dengan penyusunan laporan dan pembuatan perangkat lunak ini adalah sebagai berikut:

1) Studi Literatur

   Studi literatur adalah tahap pengumpulan data yang diperoleh dengan cara mempelajari Teori *ETL* termasuk penerapan *Data Mart* dan monitoring.

2) Studi Lapangan

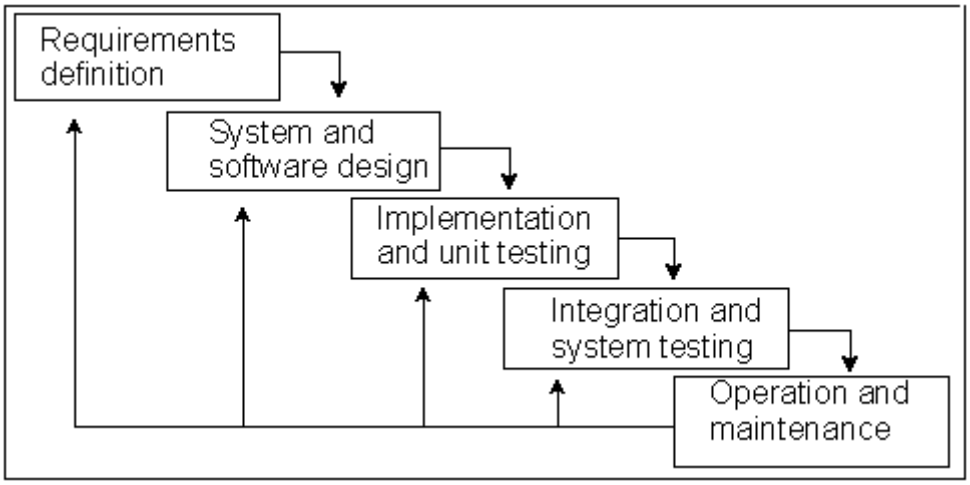
   Studi lapangan adalah tahap pengumpulan data dengan mengadakan penelitian dan peninjauan langsung terhadap permasalahan yang ada di *Laboratorium Data Mining Deputy of Research and Development* Id-SIRTII/CC.

3) Wawancara

   Wawancara adalah tahap pengumpulan data dengan cara tanya jawab langsung dengan staf *Laboratorium Data Mining Deputy of Research and Development* Id-SIRTII/CC terhadap permasalahan yang diambil.

1.5.2 Tahap Pembangunan Perangkat Lunak

Tahap pembangunan perangkat lunak dalam pembutan perangkat lunak ini menggunakan *waterfall*, berikut dapat dilihat pada Gambar 1.1.



Gambar 1.1 *Metode Waterfall* menurut Sommerville

1. *Requirements definition*

   Mengumpulkan kebutuhan secara lengkap kemudian kemudian dianalisis dan didefinisikan kebutuhan yang harus dipenuhi oleh program yang akan dibangun. Fase ini harus dikerjakan secara lengkap untuk bisa menghasilkan desain yang lengkap.
2. *System and software design*

   Desain dikerjakan setelah kebutuhan selesai dikumpulkan secara lengkap.
3. *Implementation and unit testing*

   Desain program diterjemahkan ke dalam kode-kode dengan menggunakan bahasa pemrograman yang sudah ditentukan. Program yang dibangun langsung diuji baik secara unit.
4. *Integration and system testing*

   Penyatuan unit-unit program kemudian diuji secara keseluruhan (*system testing*).

5. *Operation and maintenance*

   Tahapan untuk mengoperasikan program dilingkungannya dan melakukan pemeliharaan, seperti penyesuaian atau perubahan karena adaptasi dengan situasi sebenarnya.

1.6 Sistematika Penulisan

Sistematika penulisan laporan penelitian ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisikan tentang latar belakang masalah, perumusan masalah, maksud dan tujuan, batasan masalah, metodologi penelitian, dan sistematika penulisan untuk menjelaskan pokok-pokok pembahasannya.

BAB II. LANDASAN TEORI

Bab ini membahas tentang profil perusahaan dan landasan teori yang digunakan dan definisinya.

BAB III. ANALISIS DAN PERANCANGAN SISTEM

Bab ini membahas tentang analisis sistem, analisis masalah, analisis OLTP, analisis spesifikasi kebutuhan perangkat lunak, analisis *data mart*, analisis ETL, analisis OLAP, analisis kebutuhan non fungsional, analisis kebutuhan perangkat keras, analisis pengguna, analisis perangkat lunak, analisis kebutuhan fungsional, perancangan arsitektur sistem, perancangan antarmuka sistem.

BAB IV. IMPLEMENTASI DAN PENGUJIAN

Bab ini membahas tentang implementasi atau pengujian dari hasil analisis dan perancangan yang telah disusun ke dalam bentuk program.

BAB V. KESIMPULAN DAN SARAN

Bab ini merupakan penutup penyusunan laporan yang berisi kesimpulan dari implementasi dan uji coba yang dilakukan. Selain itu berisi pula saran yang diharapkan dapat menjadi masukan untuk pengembangan aplikasi di masa yang akan datang.