BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Sistem keamanan komputer adalah salah satu hal yang sangat penting harus dimiliki sebuah komputer *server* yang terkoneksi dalam jaringan intranet dan internet untuk melindungi data dari para peretas. Salah satu *server* yang banyak diakses adalah *web server*. Hal ini dilakukan bukan tanpa dasar, dikarenakan berdasarkan sebuah artikel yang dikeluarkan oleh Acunetix pada tanggal 12 Februari 2007[27], menginformasikan bahwa sejak tahun 2006 telah dilakukan analisis atas s*ampling website* sebanyak 10.000 dimana 3.200 yang telah dilakukan pengecekan, dinyatakan bahwa rata-rata *website* memiliki tingkat kerentanan sampai 70% dan beresiko serius terjadinya peretasan, dan dikhawatirkan dapat dimanipulasi oleh para *hacker* untuk mencuri data-data yang sensitif.

Atas dasar informasi tersebut, hal ini menjadi perhatian utama oleh PT. Indotama Palapa Nusantara dikarenakan PT. Indotama Palapa Nusantara adalah sebuah perusahan *switching service*, dimana *core* bisnis bersifat *transactional*. Sebagian besar layanan *transactional* PT. Indotama Palapa Nusantara dijalankan berbasiskan *web*, jika tidak dikembangkan dengan baik dan tidak di *monitoring* secara berkala untuk *updating* sistem dikarenakan ada *bug* pada bisnis proses dan kelemahan pada sisi *security*, aplikasi *web* dapat menjadi aplikasi yang rentan terhadap tindakan peretasan seperti *scanning*, dan *injection*. Akibatnya, bagi perusahaan dimana didalamnya terdapat data berharga akan mengalami kerugian dan mendapat penilaian buruk dari mitra usaha.

Untuk itu PT. Indotama Palapa Nusantara perlu melakukan analisis permasalahan dari prosedur yang ada, untuk melakukan pencegahan atas tindakan peretasan. Pada penelitian ini tidak menggunakan aplikasi yang sudah ada seperti Snort atau sejenisnya yang dapat diakses dan digunakan secara umum. PT Indotama Palapa Nusantara menginginkan perangkat lunak atau sistem *Intrusion Detection* dan *Prevention System* yang bersifat lebih independen untuk

menghidari *trigger botnet*, *zombie script*, atau *rootkit*, dan aplikasi bersifat terpusat, serta mampu dijalankan pada protokol jaringan yang aman.

Berdasarkan permasalahan tersebut, untuk mengatasi kelemahan pada sisi *security*. Penelitian ini membuat perangkat lunak pencegahan akses ke *network*. Perangkat lunak yang dikembangkan secara independen, dimana memiliki kemampuan untuk melakukan IDS (*Intrusion Detection System*) dan IPS (*Intrusion Prevention System*) pada *server*. Bersifat terpusat, yaitu mampu melakukan *detection* dan *prevention* lebih dari satu *server* dalam satu sesi, baik *server* berada di *intranet* ataupun *internet*. Dalam pengamanan pertukaran data, aplikasi menggunakan SSH (*Secure Shell*) sebagai protokol jaringan untuk pembacaan data, kemudian data tersebut di analisa oleh aplikasi menggunakan metode *signature-base* sebagai metode untuk pengenalan deteksi intrusi yang dapat diprediksi dan metode *anomaly-base* untuk kasus yang tidak bisa ditangani oleh metode *signature-base*.

Penggunaan kedua metode tersebut dalam aplikasi yang dikembangkan sangat penting untuk dilakukan, dikarenakan kedua metode tersebut memiliki mekanisme berbeda dalam menganalisa intrusi. Metode *signature-base* menganalisa berdasarkan parameter yang berbentuk karakter *string* yang dapat dibaca kemudian dicocokan dengan *rule* yang telah di inisiasi, sedangkan metode *anomaly-base* menganalisa dari sisi *traffic*, yaitu dengan menghitung setiap *hit* yang masuk ke *server web* apakah adanya temuan bersifat *scanning* atau tindakan *brute force* yang tidak dapat dideteksi oleh metode *signature-base*, dengan target penggunaan kedua metode tersebut dapat meningkatkan ketepatan dalam proses pendeteksian intrusi. Dalam pengaplikasian metode tersebut, aplikasi menjalankan metode *signature-base* dan *anomaly-base* dijalankan bersamaan tetapi tidak secara konkuren. Selain dari penerapan dua metode berbeda, aplikasi ditargetkan untuk mampu melanjutkan hasil pada proses *detection* ke tahap *prevention* dengan memberi perintah pada Router untuk mendaftarkan *IP Address* yang dianggap berbahaya untuk segera di *drop*, dan dilanjutkan dengan adanya mekanisme memberi informasi *alert*, berupa SMS ke Manager.

Atas latar belakang tersebut, penulis dalam tugas akhir ini membuat aplikasi dengan judul " PEMBANGUNAN APLIKASI PENCEGAHAN AKSES KE *NETWORK* DENGAN MELAKUKAN PENGAMATAN *LOG* SEBAGAI DETEKSI *INSTRUSION* MENGGUNAKAN METODE *SIGNATURE* DAN METODE ANOMALI DI PT. INDOTAMA PALAPA NUSANTARA ".

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang yang telah dijelaskan, maka dapat dirumuskan masalah yaitu bagaimana membangun sistem keamanan IDS dan IPS di PT. Indotama Palapa Nusantara dengan sistem terpusat, menggunakan protokol komunikasi yang aman sebagai pertukaran data antara aplikasi dan *server* dan perangkat lunak tersebut dikembangkan secara independen, dengan tujuan menghindari adanya *script* yang menjadi *trigger botnet*, *zombie script*, atau *rootkit*.

1.3 Maksud dan tujuan

Maksud dari penulisan tugas akhir ini adalah membangun aplikasi yang bersifat independen, terpusat, dan aman dalam pertukaran data untuk melakukan pencegahan akses ke dalam sistem jaringan komputer di PT. Indotama Palapa Nusantara dengan melakukan deteksi adanya *intrusion* dengan metode *signature-base* dan metode *anomaly-base,* dimana hasil deteksi tersebut menjadi keputusan untuk memberi perintah pemblokiran secara langsung ke Router.

Tujuan yang akan dicapai dalam pembangunan perangkat lunak atau sistem ini adalah :

1. Memudahkan untuk melakukan pengamatan file *log* yang terdapat pada *web server*.
2. Memudahkan untuk melakukan analisa *intrusion detection* dan *intrusion prevention*.
3. Memudahkan dalam implementasi metode *signature* dan metode anomali sebagai pengenalan pola *instrusion* dengan target dari penggunaan kedua metode tersebut dapat meningkatkan ketepatan dan

kecepatan dalam proses pendeteksian *instrusion* untuk menghasilkan *response*, dijalankan bersamaan tetapi tidak secara konkuren.

4. Memudahkan untuk mendapatkan informasi adanya *intrusion* dengan memberi informasi peringatan melalui SMS ke Manager.
5. Memudahkan dalam pengembangan atau *patch* aplikasi, dan *monitoring* beberapa server secara terpusat, dan pertukaran data yang aman dengan menggunakan SSH sebagai protokol jaringan.

1.4 Batasan Masalah

Dalam pembahasan permasalahan penelitian, penulisan tugas akhir ini diperlukan adanya batasan masalah sehingga penyajian lebih terarah dan mencapai tujuan yang ingin dicapai. Batasan-batasan masalahnya adalah sebagai berikut :

1. Pada penelitian ini *platform* yang digunakan berbasiskan aplikasi *desktop* dan *console*.
2. Sumber data dilakukan dengan melakukan pembacaan *log* yang terdapat pada *web server*.
3. Proses pembacaan *log* menggunakan SSH sebagai protokol jaringan.
4. Teknik yang akan digunakan untuk menganalisa *log* menggunakan metode *signature-base* dan *anomaly-base*.
5. Aplikasi melakukan pencegahan akses ke *network* dengan mengirimkan *command drop IP Address* ke Router, dan aplikasi akan memberikan informasi peringatan ke *Manager* berupa SMS.
6. *Tools Modeling* menggunakan UML (*Unified Modeling Language*).
7. Bahasa pemrograman yang digunakan adalah C#.NET.
8. Penggunaan MySQL sebagai media penyimpanan data.

1.5 Metodologi Penelitian

Pada penelitian tugas akhir ini, penelitian menggunakan metode kualitatif. Metode kualitatif lebih menekankan pada aspek pemahaman secara mendalam terhadap suatu masalah daripada melihat permasalahan untuk penelitian generalisasi. Adapun alasan lainnya adalah :

a. Peneliti berinteraksi dengan fakta yang diteliti.
b. Pendekatan induktif, yaitu menekanan pada pengamatan dahulu, kemudian menarik kesimpulan berdasarkan pengamatan tersebut.

1.5.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut :

a. Studi Literatur.

   Pengumpulan data dengan cara mengumpulkan literatur, jurnal, paper dan bacaan-bacaan yang ada kaitannya dengan judul penelitian.

b. Observasi.

   Teknik pengumpulan data dengan mengadakan penelitian dan peninjauan langsung terhadap permasalahan yang diambil.

c. Interview.

   Teknik pengumpulan data dengan mengadakan tanya jawab secara langsung yang ada kaitannya dengan topik yang diambil.

1.5.2 Metode Pembangunan Perangkat Lunak

Model yang digunakan untuk proses pengembangan perangkat lunak yang akan dibangun adalah model Waterfall[1], yang terdiri dari tahap-tahap sebagai berikut :

1. Analisis dan Perancangan Sistem

   Tahap analisis merupakan tahap dimana peneliti berusaha menganalisi dan merancang sistem terlebih dahulu sebelum mengerjakan seperti merancang sistem *database* dan *table* apa saja yang akan diambil, bagaimana alur sistemnya, membuat peta situs, membuat jadwal kerja,

mengumpulkan bahan dan sebagainya. Proses ini bisa dianggap sebagai titik utama dari proses pengerjaan aplikasi.

2. Desain Sistem

   Begitu rancangan dari sistem jadi maka tahap berikutnya adalah melakukan perancangan desain, seperti warna, konsep, font huruf, filosofi, dan sebagainya yang dirasa sesuai dengan yang diinginkan.

3. Penulisan Kode

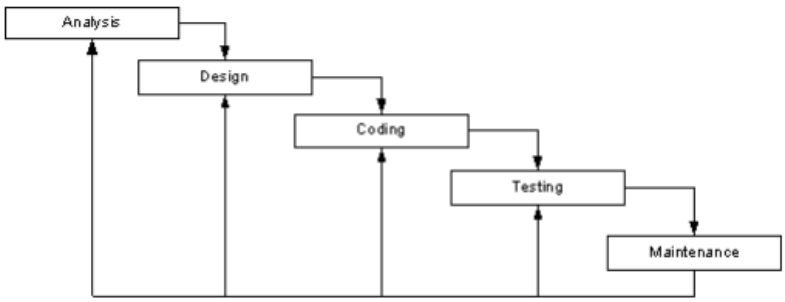
   Dalam Tahap ini merupakan tahap proses yang akan memakan waktu yang cukup lama dan yang paling sulit karena tahap ini berisi barisan perintah (*coding*) yang harus dikerjakan oleh pembuat sistem. Semua tidak akan berjalan tanpa adanya tahap *coding*. Dengan membuat program yang telah dirancang sebelumnya.

4. Integrasi dan Pengujian Sistem

   Unit program atau program individual diintegrasikan dan diuji sebagai sistem yang lengkap untuk menjamin bahwa persyaratan sistem telah dipenuhi.

5. Operasi dan Pemeliharaan

   Sistem dioperasikan (Di-instal dan dipakai). Pemeliharaan mencakup koreksi dari berbagai error (kesalahan) yang tidak ditemukan pada tahap-tahap terdahulu, perbaikan atas implementasi unit sistem dan pengembangan pelayanan sistem, sementara persyaratan-persyaratan baru ditambahkan.



Gambar 1.1 Model Waterfall

1.6 Sistematika Penulisan

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

BAB I PENDAHULUAN

Menguraikan tentang latar belakang permasalahan, mencoba merumuskan inti permasalahan yang dihadapi, menentukan maksud dan tujuan penelitian, yang kemudian diikuti dengan pembatasan masalah, asumsi, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini akan dibahas landasan teori yang berhubungan dengan masalah yang akan dibahas di laporan tugas akhir ini.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Menganalisis masalah dari model penelitian untuk memperlihatkan keterkaitan antar variabel yang diteliti serta model matematis untuk analisisnya.

BAB IV PENGUJIAN DAN IMPLEMENTASI SISTEM

Merupakan tahapan yang dilakukan dalam penelitian secara garis besar sejak dari tahap persiapan sampai pengujian, penarikan kesimpulan, metode dan kaidah yang diterapkan dalam penelitian. Termasuk menentukan variabel penelitian, identifikasi data yang diperlukan dan cara pengumpulannya, penentuan sampel penelitian dan teknik pengambilannya, serta metode atau teknik analisis yang akan dipergunakan dan perangkat lunak yang akan dibangun jika ada.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dari keseluruhan masalah yang telah dibahas pada bab sebelumnya dan dilengkapi dengan saran-saran.