BAB I

PENDAHULUAN

1.1 Latar Belakang

Dunia teknologi informasi saat ini mengalami perkembangan dan kemajuan yang sangar pesat. Khususnya teknologi jaringan komputer, saat ini sudah berkembang semakin cepat. Perkembangan teknologi ini memudahkan para pengguna untuk melakukan berbagai pekerjaan, seperti bertukar informasi, mencari data, juga sebagai media penghubung antara seseorang dan yang lainnya.

Semakin bertambahnya pengguna dalam sebuah jaringan semakin besar pula risiko keamanannya. Masalah keamanan merupakan salah satu aspek terpenting pada sebuah sistem informasi. Namun masalah keamanan sering kali kurang mendapat perhatian dari perancang dan pengelola sistem informasi serta berada diurutan setelah tampilan *interface*, atau bahkan diurutan terakhir dalam komponen yang dianggap penting. Apabila mengganggu performa sistem seringkali masalah keamanan tidak begitu dipedulikan bahkan ditiadakan.

UPT Laboratorium Universitas Amikom Yogyakarta merupakan unit pelaksana teknis yang menangani bidang sarana dan prasarana laboratorium komputer untuk menunjang perkuliahan di Universitas Amikom Yogyakarta. Terdapat 17 ruangan laboratorium komputer yang ditangani oleh UPT yaitu meliputi Laboratorium *Hardware & Software*, *Programing*, Sistem Operasi, Jaringan Komputer, Multimedia, serta Laboratorium *Green Screen & Broadcasting*.

Namun masalah baru timbul ketika jaringan yang sudah dikatakan cukup besar dengan level pelayanan mencakup sebuah Instutisi perguruan tinggi namun

belum dibangun sebuah sistem monitoring keamanan jaringan untuk melindungi data-data penting serta mencegah adanya tindakan-tindakan yang membahayakan seperti penyerangan attau *attacking* yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab.

Menurut administrator jaringan yang bertanggungjawab di UPT Laboratorium Universitas Amikom Yogyakarta aktifitas mencurigakan sering terjadi, sebagai contoh percobaan masuk sistem *router*, *ssh*, dan beberapa aktifitas mencurigakan lainnya, dan disinyalir masih banyak lagi aktifitas mencurigakan dan membahayakan lainnya namun masih belum bisa dibuktikan dikarenakan belun dibangunnya sistem monitoring keamanan *server* dan jaringan yang khusus menangani kasus seperti itu.

Berdasarkan latar belakang diatas serta dari hasil observasi di tempat dan melakukan wawancara secara langsung kepada administrator maupun pihak yang bertanggung jawab atas jaringan yang ada di UPT Laboratorium Universitas Amikom Yogyakarta maka dapat diambil kesimpulan bahwa diperlukannya sistem keamanan jaringan *server* untuk mengamankan data-data serta layanan yang ada di *server* tersebut. Serta untuk membantu pekerjaan administrator untuk menanggulangi dan mengurangi ancaman serta kerusakan yang dapat ditimbulkan akibat aktivitas-aktivtas hacking oleh orang yang tidak bertanggung jawab.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan diatas, maka dapat diambil suatu rumusan masalah sebagai berikut:

Bagaimana membangun sebuah sistem keamanan *server* dan jaringan komputer dengan metode *Intrusion Prevention system (IPS)* untuk mencegah serta mengatasi terjadinya serangan terhadap *server* di UPT Laboratorium Universitas Amikom Yogyakarta.

1.3 Batasan Masalah

Untuk menghindari pembahasan masalah yang terlalu luas, maka penulis membarikan batasan-batasan masalah sehingga materi yang disampaikan tepat sasaran. Berikut adalah batasan-batasan masalah tersebut:

1. Server *Intrusion Prevention System* yang dibangun menggunakan *snort* dengan sistem operasi *Ubuntu 16.04*.
2. Sistem Operasi yang digunakan oleh *cliet/attacker* untuk uji coba serangan *Linux Ubuntu 16.04*.
3. Sistem *Intrusion Prevention System* yang akan dibangun menggunakan jenis *network-based IPS (NIPS)*.
4. Sistem keamanan jaringan yang dibangun menggunakan pendekatan *Signature Base Detection*.
5. Uji coba serangan dengan melakukan dua cara, yaitu *Denial of Service* menggunakan program *hping3*, dan pegujian yang kedua yaitu dengan *ssh attack*.
6. Tidak melakukan uji coba menggunakan semua jenis serangan yang dilakukan ke sistem secara lebih mendalam.
7. Metode Pengembangan dalam penelitian ini menggunakan PPDIOO *Network Life-Cycle Approach* namun hanya sampai tahap Implementasi (*Prototyping*).

1.4 Maksud dan Tujuan Penelitian

Maksud dan tujuan penelitian ini berfungsi untuk mengetahui apa yang hendak dicapai dalam penelitian ini. Berikut ini maksud dan tujuan dari penelitian yang di lakukan oleh penulis:

1.4.1 Maksud Penelitian

Adapun maksud dari penelitian adalah untuk memenuhi salah satu syarat kelulusan Strata satu di Universitas Amikom Yogyakarta dengan program studi Informatika di Fakultas Ilmu Komputer.

1.4.2 Tujuan Penelitian

Berikut ini adalah tujuan yang yang hendak dicapai oleh penulis dalam penelitian:

1. Membuat sistem monitoring keamanan jarinagan *server* di UPT Laboratorium Universitas Amikom Yogyakarta.
2. Memberikan informasi yang akurat dan cepat kepada administrator jaringan ketika sedang terjadi intrusi atau serangan melalui *webbase Snorby*.
3. Mengautomatisasi tindakan yang diambil ketika terdapat gejala intrusi.
4. Membantu pekerjaan administrator jaringan dalam menanggulangi ancaman dan serangan pada sebuah jaringan.
5. Mengembangkan penelitian mengenai *Intrusion Prevention System* yang telah dilakukan oleh peneliti sebelumnya.

1.5 Metode Penelitian

Dalam melakukan penelitian ini, penulis menggunakan beberapa metode penelitian untuk menyusun langkah-langkah yang dapat digunakan untuk menyelesaikan penelitian.

1.5.1 Metode Pengumpulan Data

1.5.1.1 Studi Pustaka

Studi Pustaka dilakukan dengan membaca literatur dari buku, *paper*, journal penelitian, dan penelitian sebelumnya yang dapat digunakan sebagai dasar teori dari sistem dalam penelitian yang dilakukan oleh penulis.

1.5.1.2 Observasi

Metode observasi dilakukan dengan cara pengamatan secara langsung di tempat objek penelitian meliputi infrastruktur jaringan serta proses lalu lintas jaringan. Dengan observasi didapatkan data dan informasi aktivitas apa saja yang sedang terjadi dalam sebuah jaringan tersebut.

1.5.1.3 Wawancara

Metode wawancara ini langsung dilakukan kepada administrator jaringan yang bertugas dan bertanggungjawab atas pengelolaan jaringan di UPT Laboratorium Universitas Amikom, sehingga diperoleh data-data yang dibutuhkan oleh penulis dalam menunjang penelitian ini.

1.5.2 Metode Pengembangan

Metode pengembangan pada penelitian yang digunakan penulis yaitu PPDIOO *Network Life-Cycle Approach*. PPDIOO merupakan metode analisis sampai pengembangan instalasi jaringan komputer yang dikembangkan oleh *Cisco* pada

materi *Designing for Cisco Internetwork Solution (DESGN)* yang mendefinisikan secara terus menerus siklus hidup layanan yang dibutuhkan untuk pengembangan jaringan komputer atau teknologi terkait. Adapun tahapan pada PPDIOO terdapat pada Gambar 1.1.

Gambar 1.1 PPDIOO *Network Life-Cycle* [20]

PPDIOO *Network Life-Cycle Approach* memiliki enam tahap dalam setrategi pengembangannya, yaitu *Prepare* (Persiapan), *Plan* (Perencanaan), Design (Perancangan), *Implement* (Penerapan), *Operate* (Pengoperasian), dan Optimize (Potimasi).

Pada metode pengembangan ini menjelaskan tahapan-tahapan pada penelitian, mulai dari tahap awal hingga tahap akhir. Terdapat lima tahapan utama yang dilakukan dalam penelitian yaitu tahap persiapan (*Prepare*), tahap perencanaan (*Plan*), tahap desain (*Design*), dan tahap Implementasi (simulasi *prototyping*). Berdasarkan batasan masalah yang telah ditentukan, penggunaan metode PPDIOO

hanya digunakan sampai tahap simulasi *prototyping*. Penjelasan dari setiap tahapan adalah sebagai berikut:

1.5.2.1 *Prepare* (Persiapan)

Pada bagian *prepare* atau persiapan dilakukan proses penelitian awal terdiri dari identifikasi kondisi yang terdapat pada objek penelitian, identidikasi masalah, yang kemudian dilakukan analisis permasalahan yang ada hingga rencana tindakan penanganan.

1.5.2.2 *Plan* (Perencanaan)

Pada bagian perencanaan dilakukan untuk membuat rincian spesifikasi infrastruktur dan mengidentifikasikan kebutuhan jaringan serta penentuan jadwal penelitian. Tahapan ini juga dilakukan analisa terhadap infrastruktur eksisting, serta memahami apa saja yang dibutuhkan dalam proses pembangunan sistem sehingga didapatkan hasil analisa yang digunakan sebagai dasar dalam perencanaan.

1.5.2.3 *Design* (Perancangan)

Tahap selanjutnya adalah desain atau perancangan dalam tahap pembangunan IPS *Server*. Pada tahap ini terdapat beberapa tahap yaitu rancangan topologi jaringan yang akan diimplementasikan, perancangan sistem IPS meliputi hubungan antar modul dalam sistem, serta alur kerja IPS *Server*.

1.5.2.4 *Implement* (Penerapan)

Pada tahap Implementasi ini akan diterapkan apa yang telah direncanakan dengan dilakukannya pembuatan *prototyping* terhadap desain infrastruktur. Dalam tahap ini mencakup instalasi serta konfigurasi sistem terhadap desain topologi jaringan yang telah direncanakan serta melakukan pengujian terhadap sistem.

1.6 Sistematika Penulisan

Sebagaimana gambaran umum dalam penyusunan skripsi ini sesuai dengan judul, penulis menyusun pembabakan dari ringkasan setiap isi, dan per bab yang dibagi menjadi lima bab yang diawali dari :

BAB I PENDAHULUAN

Pada bab ini penulis mengurai mengenai gambaran umum penelitian yang akan dilakukukan penulis, latar belakang penelitian, perumusan masalah, pembatasan masalah, dan metode penelitian guna menyusun sekripsi ini serta sistematika penulisan yang merupakan panduan dalam menysun landasan teori.

BAB II LANDASAN TEORI

Dalam bab ini akan membahas dan menjelaskan mengenai dasar teori yang berkaitan dengan keamanan jaringan yang menjadi landasan dan mendukung pelaksanaan penelitian dan penulisan skripsi.

BAB III ANALISIS DAN PERANCANGAN.

Menguraikan tentang perancangan dan analisis yang akan digunakan dalam pembuatan sistem, alat-alat yang digunakan, serta sistematika pengujian yang akan dilakukan.

BAB IV IMPLEMENTASI DAN PEMBAHASAN.

Bab ini membahas tentang implementasi sistem yang telah dirancang, pengujian sistem, serta pembahasan sistem keamanan yang telah diterapkan.

BAB V PENUTUP

Berisikan tentang kesimpulan dari seluruh pembahasan yang diuraikan dari Bab 1 hingga Bab 4 serta saran-saran yang dianggap perlu dalam usaha menuju perbaikan dan kesempurnaan untuk penelitian selajutnya.

DAFTAR PUSTAKA

Berisikan referensi yang di gunakan oleh penulis sebagai acuan dan perbandingan landasan teori dalam penulisan skripsi.