BAB I
PENDAHULUAN

1.1 Latar Belakang

PT Jabarmaya Kriya Sentosa adalah perusahaan jasa penyedia layanan internet / Internet service provider yang berada di Bandung. Dari tahun 2018 PT Jabarmaya Kriya Sentosa mulai mengembangkan usahanya ke bidang *software.* Salah satu *software* yang sudah dimiliki adalah aplikasi manajemen data alokasi dana BOS yang bernama SILALA. SILALA (Sistem Laporan Langsung) adalah sebuah sistem informasi berbasis *website* yang dipergunakan sekolah untuk mencatat dan melaporkan data alokasi penggunaan dana Bantuan Operasional Sekolah (BOS) kepada Dinas Pendidikan Kota/Kabupaten.

Berdasarkan wawancara dengan Tri Mur Fridayanto selaku penanggung jawab aplikasi SILALA, dalam aplikasi SILALA terdapat banyak sekali data yang penting dan sensitif, tentu akan menjadi masalah bilamana data – data tersebut disalahgunakan atau dimanfaatkan untuk kepentingan yang tidak bertanggung jawab. Sebagai contoh, bilamana data yang ada dalam aplikasi berubah secara tiba-tiba dan tidak sesuai dengan laporan yang sudah tercatat oleh pihak dinas, maka akan terjadi ketimpangan data yang menyebabkan tersendatnya proses pelaporan data oleh pihak sekolah ke pihak dinas dan pemerintah daerah. Data tersebut juga bisa mempengaruhi pemeriksaan data yang rutin dilakukan oleh BPK, bilamana data tersebut tidak sesuai dengan bukti kwitansi dan laporan yang *real*, maka pihak pengelola dan pengguna bisa saja dirugikan atas hal yang sebenarnya tidak mereka lakukan. Oleh karena itu sangat penting untuk meningkatkan pengamanan terhadap *web server* SILALA untuk memberikan perlindungan *extra* terhadap *web server* aplikasi SILALA ini guna mempertahankan keabsahan data dan terjaganya informasi yang akurat dan terpercaya.

Berdasarkan dari masalah dan penelitian diatas, sebagai solusi dari penelitian ini adalah akan mengimplementasikan dua jenis *honeypot* yaitu *honeypot* web HIHAT untuk melindungi akses dari *port* web dan *honeypot* SSH

KIPPO untuk melindungi akses dari *port* SSH, dan akan menggunakan IPS *Snort* untuk mendeteksi serangan dan akan dibantu oleh *bot* untuk *redirect* secara otomatis ip penyerang yang sudah diketahui ke *web server* palsu (*honeypot*), dan *bot* juga akan mengirim peringatan kepada administrator melalui aplikasi telegram jika sudah ada ip yang di *redirect* ke server *honeypot*.

1.2 Identifikasi Masalah

Berdasarkan latar belakang diatas, berikut permasalahan yang akan dijadikan pokok dalam penilitian ini :

1. Bagaimana mengimplementasikan metode *honeypot* menggunakan *tools* HIHAT dan Kippo serta IPS *snort* menjadi solusi dalam melindungi Server SILALA.
2. Bagaimana mengimplementasikan IPS *Snort* dan *bot* untuk mendeteksi, mengirimkan peringatan kepada administrator, dan *redirect* penyerang ke server *honeypot*
3. Bagaimana cara simulasi penyerangan untuk mencoba sistem yang telah diimplementasikan.

1.3 Maksud dan Tujuan

Maksud dari penelitian ini adalah meingimplementasikan *honeypot* jenis *High Interaction Honeypot* pada server SILALA di PT.Jabarmaya Kriya Sentosa dengan tujuan sebagai berikut :

1. Mengimplementasikan metode *honeypot* menggunakan *tools* HIHAT dan Kippo dan IPS *snort* di PT.Jabarmaya Kriya Sentosa untuk menunjang keamanan Server SILALA.
2. Mengimplementasikan IPS *Snort* untuk mendeteksi serangan dan *bot* untuk membantu dalam *redirect* penyerang ke *server honeypot* dan mengirimkan peringatan kepada administrator.
3. Membuat simulasi penyerangan untuk mengetahui seberapa efektif metode ini berjalan.

1.4 Batasan Masalah

Dalam penelitian ini dibuat beberapa batasan masalah agar pembahasan lebih berfokus dan sesuai dengan tujuan yang akan dicapai. Berikut batasan masalahnya :

1. Implementasi server *Honeypot* menggunakan VPS dengan OS Ubuntu Server.
2. Menggunakan HIHAT dan Kippo untuk *tools* pengelola *honeypot.*
3. Menggunakan IPS *Snort* dan *bot* untuk *redirect* penyerang ke server *honeypot.*
4. Mengirimkan peringatan ke administrator melalui aplikasi telegram
5. Serangan pada jaringan sudah ditentukan yaitu *port scanning*, SSH *brute force* dan DOS *attack*.
6. Serangan dilakukan dengan simulasi.

1.5 Metodologi Penelitian

Metodologi penelitian merupakan suatu proses yang digunakan untuk memecahkan suatu masalah yang logis, dimana memerlukan data-data untuk mendukung terlaksananya suatu penelitian. Dalam rangka mendapatkan data atau informasi pendukung dalam penyusunan laporan ini, metode penelitian yang digunakan adalah:

1.5.1. Metode Pengumpulan Data

Adapun metode pengumpulan yang diterapkan penulis sebagai berikut :

1. Studi Literatur

Studi literatur merupakan kegiatan yang dilakukan untuk mencari dan mengumpulkan data pustaka untuk menunjang penelitian ini, diantaranya buku, artikel, jurnal, laporan akhir yang ada kaitannya dengan penelitian ini.

2. Wawancara

Wawancara dilakukan penulis untuk mengetahui dan mengumpulkan data permasalahan yang ada di perusahaan PT.Jabarmaya Kriya Sentosa yang berkaitan dengan permasalahan yang akan diteliti.

3. Analisis Data

Pada analisa data dilakukannya proses penganalisaan terhadap konsep dan metode yang cocok untuk diterapkan pada permasalahan yang sedang diteliti.

4. Perancangan dan Implementasi

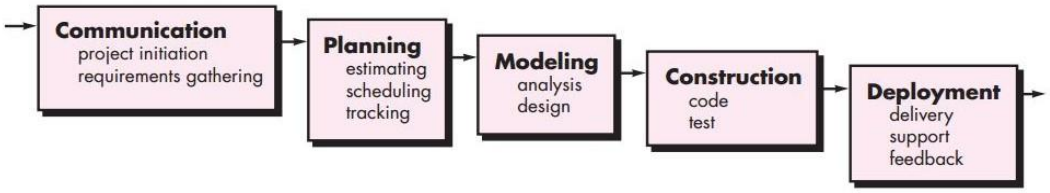
Perancangan dilakukan untuk memudahkan dalam mengimplementasikan rancangan *honeypot* dan untuk memberikan gambaran yang jelas terhadap jenis metode yang akan diterapkan, tentu juga mempermudah implementasi yang nantinya akan dilakukan.

5. Pengujian

Pada pengujian ini akan dilakukan simulasi penyerangan untuk memastikan seberapa efektif metode yang telah diimplementasikan.

1.5.2. Metode Alur Penelitian

Model yang terdapat pada gambar Alur SDLC *Waterfall* dari Winston Royce. Metode pembangunan sistem mengikuti alur SDLC metode *Waterfall*. SDLC adalah tahapan tahapan yang dilalui dalam membangun sebuah sistem atau aplikasi. *Waterfall* adalah tahapan pembangunan sistem atau aplikasi yang dilakukan tahap pertahap secara berutan dari awal sampai akhir. Dalam membangun sistem ini penulis akan melewati tahap *communication, planning, modeling, construction dan deployment*.



Gambar 1.1 Model SDLC Waterfall

Tahap *Communication* merupakan tahap dimana penulis mengumpulkan masalah dan batasan yang akan dibuatkan menjadi suatu sistem. Hal ini bertujuan agar sistem dapat berjalan sesuai dengan kebutuhan.

Tahap berikutnya adalah *Planning*. Pada tahap ini dilakukan perencanaan estimasi, penjadwalan dan pelacakan. Hal iini bertujuan agar proses pembangunan sistem memiliki target yang jelas kedepan.

Berikutnya adalah *Modelling*. Pada tahap ini penulis merancang sistem yang akan dibangun berdasarkan hasil analisis. Dalam merancang sistem penulis juga memikirkan alur dari sistem serta kebutuhan yang diperlukan dalam membuat sistem tersebut.

Tahap *Construction* merupakan tahap dimana penulis menerapkan sistem berdasarkan desain atau perancangan sistem. Dengan kata lain tahap ini merealisasikan dari tahap perancangan. Sehingga sistem yang dirancang bisa diterapkan diruang lingkupnya.

Tahap terakhir adalah *Deployment*. Setelah sistem dibuat atau diimplementasikan, maka diperlukan tahap pengujian. Pada tahap ini pula ketika sistem terdapat masalah maka dilakukan *feedback* terhadap masalah yang ada. Apabila terdapat kesalahan yang harus segera di perbaiki maka kembali ke tahap awal untuk dilakukan penyelesaian masalah tersebut.

1.6 Sistematika Penulisan

Sebagai acuan bagi penulis agar penulisan laporan ini terarah dan tersusun dengan yang diharapkan penulis, maka disusun sistematika penulisan sebagai berikut :

BAB 1 PENDAHULUAN

Pada bab ini berisi uraian latar belakang, rumusan masalah, maksud dan tujuan, batasan masalah, metode penelitian, serta sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Pada bab ini berisi uraian konsep dan teori dasar yang bisa menunjang dan berhubungan dengan penelitian yang dimaksud.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini berisi penjelasan tentang proses analisis dan perancangan sistem atau konfigurasi yang akan dilakukan dalam penelitian yang diambil.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Pada bab ini berisi tentang penerapan metode yang akan diimplemntasikan dan pengujian sistem dengan melakukan simulasi penyerangan.

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dan saran yang sudah diperoleh dari hasil penelitian tugas akhir ini.