BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

PT. Fasa Centra Artajaya merupakan merupakan perusahaan yang bergerak di bidang *financial technology* khususnya sebagai layanan *online payment* yang berdiri sejak tahun 2011 di Yogyakarta. PT Fasa Centra Artajaya mengeluarkan produk FasaPay sebagai layanan uang elektronik (*e-money*) dan transfer dana. Layanan FasaPay mendukung dalam memenuhi kebutuhan penggunanya mulai dari bayar, beli, kirim, dan berinvestasi.

Server merupakan sebuah perangkat sistem yang dapat menjalankan layanan yang mampu menerima perintah dari komputer yang mengeksekusi perangkat lunak. Server dapat menjalankan perangkat lunak yang bisa mengontrol akses untuk masuk ke dalam jaringan.

SIEM (*Security Information and Event Managament*) pada dasarnya adalah layanan untuk membuat manajemen pada sistem serta mengontrol keamanan yang ada pada sistem. SIEM menghubungkan dan menyatukan informasi yang terdapat pada sistem, memungkinkan untuk dapat menganalisis data.

OSSIM (*Open Source Security Information Management*) sebagai sistem pemantauan jaringan berfungsi menyediakan informasi yang terkait dengan keamanan jaringan secara terpusat dan juga berfungsi untuk mengumpulkan log jaringan dan alert yang dihasilkan oleh peralatan keamanan dan bekerja secara real time selama 24/7, sehingga seorang administrator jaringan dapat dengan mudah dan mengetahui lebih cepat kondisi jaringan dalam 24 jam yang terjadi pada server.

Dikarenakan belum adanya sistem atau aplikasi yang dapat monitoring jaringan komputer secara online atau WAN (*Wide Area Network*) pada PT. Fasa Centra Artajaya maka adanya serangan tidak dapat terdeteksi. Dengan adanya layanan SIEM dapat membantu Administrator jaringan untuk

merekam aktifitas pada host, network, dan server. Serta menjaga data nasabah agar dapat tetap aman serta dapat dipercaya oleh klien.

OSSIM dapat memantau semua alat jaringan dalam satu layar atau dashboard. OSSIM mengumpulkan file log dari masing-masing tools tersebut dan melakukan analisa. OSSIM juga menampilkan hasil analisa log ini dengan tampilan yang interaktif, dalam bentuk grafik maupun diagram. Sehingga dapat memudahkan admin dalam memantau jaringan.

Data apa yang ditampilkan juga dapat kita konfigurasi. Selain memudahkan admin, OSSIM juga sangat memudahkan pimpinan Departemen Jaringan dalam memantau kondisi keamanan jaringan di perusahaan. Merekomendasikan OSSIM sebagai aplikasi log monitoring online, serta menggunakan sebuah antarmuka web yang cukup responsif dan dapat di akses oleh administrator jaringan, sekaligus untuk membuat keamanan jaringan.

1.2 Tujuan Penelitian

a. Menciptakan sistem pendeteksi atau sensor terhadap area jaringan menggunakan aplikasi berbasis *open source*, yaitu AlientVault OSSIM.
b. Memberikan laporan kepada administrator sistem mengenai upaya penyerangan terhadap sistem, melalui catatan atau *log* yang dihasilkan oleh aplikasi.
c. Menjadikan laporan dari aplikasi sebagai bukti digital yang mencatat segala upaya penyerangan ke dalam suatu area jaringan perusahaan.
d. Menghadirkan sistem pencegahan penyusupan berdasarkan pola-pola serangan yang ditujukan kepada sistem, sebelum berakibat hilangnya layanan secara keseluruhan.

1.3 Rumusan Masalah

Berisikan pertanyaan-pertanyaan dan solusi yang ditawarkan. Rumusan masalah harus dapat menyimpulkan masalah-masalah yang ada. Masalah yang diajukan hendaknya dirumuskan dalam bentuk kalimat tanya yang tegas

dan jelas untuk menambah ketajaman masalah. Rumusan masalah harus relevan dengan latar belakang masalah.

a. Bagaimana cara membangun sistem yang dapat membuat manajemen log secara real time ?
b. Bagaimana cara melakukan pendeteksian serangan menggunakan aplikasi OSSIM - AlienVault melalui paket data yang melewati area lingkungan jaringan lokal perusahaan ?
c. Bagaimana cara menampilkan log berupa grafik yang mudah di pahami ?
d. Siapa saja yang dapat memantau dan mengoperasikan aplikasi ?

1.4 Batasan Masalah

Untuk mempersempit pembahasan pada tugas akhir ini, maka dibuat batasan-batasan sebagai berikut:

a. OSSIM di rancang menggunakan sistem operasi Debian.
b. Desain OSSIM dari AlienVault menggunakan *web interface* untuk konfigurasi. 9
c. OSSIM menggunakan tools untuk memonitor *log* jaringan.
d. Penelitian mencakup analisis, perancangan dan implementasi aplikasi OSSIM.
e. Pengamanan terhadap *log* jaringan dari serangan *malware* berbahaya.

1.5 Sistematika Penulisan

Sistematika dalam penulisan tugas akhir ini dibagi menjadi lima bab, antara lain sebagai berikut :

BAB I PENDAHULUAN

Dalam bab ini berisi gambaran umum penulisan tugas akhir yaitu tentang Latar Belakang Masalah, Tujuan Penelitian Rumusan Masalah, Batasan Masalah, dan Sistematika Penulisan.

BAB II TINJAUAN PUSTAKA

Dalam bab ini berisikan teori berupa pengertian dan definisi yang diambil dari kutipan buku yang berkaitan dengan penyusunan laporan tugas akhir serta beberapa review yang berhubungan dengan penelitian.

BAB III TINJAUAN UMUM

Berisi penjelasan mengenai obyek penelitian, hasil observasi, masalah yang terdapat pada obyek, dan gambaran umum proyek.

BAB IV PEMBAHASAN

Bab ini menjelaskan tentang implementasi OSSIM, pengujian alat, dan evaluasi pengerjaan proyek.

BAB V PENUTUP

Bab ini merupakan penutup dari penulisan tugas akhir. Terdapat kesimpulan dari penelitian yang dilakukan. Sesuai dengan data data yang sudah diolah.