BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Akses data untuk sekarang memang lebih mudah daripada teknologi yang berkembang sebelum beralih ke digital, dan sebagian besar data, sangat sensitif pada berbagai tingkat keamanannya. Beberapa data mungkin memiliki kerahasiaan, dimana data tersebut tidak ditujukan untuk umum dan bersifat sangat rahasia. Terutama pada perusahaan yang memiliki kerahasiaan data yang harus diamankan integritas dan keutuhan datanya. Kebocoran data baik disengaja ataupun tidak, bisa menimbulkan banyak kerugian dan integritas dari organisasi / perusahaan tersebut menjadi sangat dipertaruhkan.

Salah satu solusi terbaik untuk menghindari kehilangan data dan menjaga kerahasiaan data adalah dengan menerapkan sistem *Data Loss Prevention* (DLP). DLP merupakan istilah keamanan komputer merujuk pada sistem yang mengidentifikasi, memantau, dan melindungi data yang digunakan (*data in use*) , data yang bergerak (*data in motion*), dan data saat berhenti (*data at rest*) melalui pemeriksaan isi data yang mendalam, dan analisis keamanan kontekstual transaksi dengan kerangka manajemen yang terpusat. Sistem ini dirancang untuk mendeteksi dan mencegah penggunaan yang tidak sah pada pengiriman informasi rahasia. Oleh karena itu dibangun MyDLP, *software data loss prevention* yang bersifat *open source* . MyDLP meminimalkan resiko kehilangan dan kebocoran data melalui *web, mail* dan *instant messenger* dalam *endpoint*. Aliran data – data penting seperti kartu kredit, nomor jaminan sosial, dan nomor rekening IBAN juga dapat diblokir untuk menghindari pencurian data. Sehingga kesengajaan maupun kecerobohan dalam pencurian data bisa dihindari.

Salah satu kelebihan MyDLP adalah sistem ini bisa berperan sebagai *content filter*. Dimana terdapat Postfix di dalamnya yang mampu berintegrasi dengan Postfix dari *mail server*. Ini bisa menjadi pilihan yang tepat saat

perusahaan menggunakan *mail server* yang membutuhkan aspek keamanan data di dalamnya.

Zimbra merupakan salah satu *mail server* yang dibuat untuk mepermudah penggunaan komunikasi *e-mail*. Sifatnya yang *open source* menjadikan Zimbra menjadi salah satu *platform* yang banyak digunakan dan dikembangkan oleh berbagai kalangan secara bebas. Dan ini memungkinkan Zimbra mampu diintegrasikan dengan MyDLP untuk menambahkan aspek keamanan di dalamnya. Namun pembangunan *mail server* berskala besar harus diimbangi dengan jumlah perangkat yang cukup. Dan ini akan menjadikan pengadaannya membutuhkan biaya yang besar.

Dahulu, pembangunan sebuah infrastruktur *server* harus diimbangi dengan kualitas perangkat yang mumpuni. Namun, sekarang era sudah beralih ke teknologi *cloud computing* yang mampu menyediakan layanan pembangunan infrastruktur komputer tanpa harus mengeluarkan biaya untuk penyediaan infrastruktur. Dalam pengembanganya, muncul banyak *platform* yang mampu menyediakan teknologi *cloud computing*, salah satunya adalah *platform* yang dikeluarkan Ubuntu yaitu Ubuntu Enterprise Cloud (UEC). Dan Zimbra pun bisa dibangun pada teknologi *cloud computing* tersebut.

1.2. Tujuan

Adapun tujuan dari penelitian dan pengembangan Tugas Akhir ini adalah untuk merancang dan mengimplemetasikan layanan *mail* dengan menggunakan Zimbra yang dibangun pada jaringan *cloud computing* kemudian mengamankan data yang berada pada *mail server* tersebut untuk mencegah pencurian dan kehilangan data. Diharapkan dengan diaplikasikannya *software* MyDLP tersebut bisa lebih menjamin keamanan dan privasi *user* ketika menyimpan data - data penting pada layanan *mail server* berbasis UEC.

1.3. Rumusan Masalah

Permasalahan yang dijadikan obyek penelitian dan pengembangan tugas akhir ini adalah :

1. Bagaimana membangun Ubuntu Enterprise Cloud sebagai arsitektur dasar *cloud computing*?
2. Bagaimana membangun Zimbra sebagai *mail server* yang diimplementasikan di Ubuntu Enterprise Cloud?
3. Bagaimana membuat proteksi terhadap data yang terdapat pada *mail server* berbasis UEC menggunakan MyDLP?
4. Bagaimana perbandingan tingkat keamanan *server Zimbra* serta data *client* dengan MyDLP dan *server* Zimbra serta data *client* tanpa MyDLP?
5. Bagaimana aspek keamanan data yang ada meliputi *privacy*, *confidentiality*, *acces control*, dan *availability*?

1.4. Batasan Masalah

Batasan masalah dalam penelitian dan pengembangan tugas akhir ini adalah:

a. Implementasi *Cloud computing* dengan *Ubuntu Enterprise Cloud* (UEC).

b. Implementasi layanan *mail* menggunakan Zimbra.

c. Layanan yang akan diimplementasikan pada Zimbra adalah layanan data *e-mail*.

d. Jenis serangan dibatasi pada *sniffing* dan *Denial of Service* (DOS).

e. *Tools* penguji yang digunakan dalam pengujian adalah *tool attack* yang umum dan popular yang telah ada dalam bentuk *open source*, bukan dari hasil *coding* penulis.

f. Tidak membahas kalkulasi algoritma enkripsi dan proteksi.

g. Parameter yang dianalisa adalah:

1. Tingkat keberhasilan serangan *sniffing*, dan *denial of service.*
2. Aspek *confidentiality*, *privacy*, *access control* serta *availability* data ketika sistem keamanan diterapkan.

1.5. Metode Penelitian

Metode yang akan digunakan untuk menyelesaikan tugas akhir ini adalah :

a. Studi literature

   Studi literature ini dimaksudkan untuk mempelajari konsep dan teori-teori yang dapat mendukung proses perancangan sistem.

b. Perancangan dan realisasi

Meliputi aplikasi dari konsep dan teori yang telah diperoleh. Melakukan perancangan sebuah sistem untuk nantinya diuji kemampuannya.

c. Pengujian dan analisis implementasi

- ❖ Konfigurasi mail server menggunakan server Zimbra yang dibangun di atas infrastruktur *Cloud computing* menggunakan *Ubuntu Enterprise Cloud*.
- ❖ Konfigurasi MyDLP pada server Zimbra.
- ❖ Simulasi serangan pada server dan *client* Zimbra tanpa MyDLP dan dengan MyDLP.
- ❖ Analisa kemampuan MyDLP dilihat dari aspek keamanan yang didapat.

d. Pengambilan kesimpulan terhadap penelitian yang dilakukan dan penyusunan laporan.

1.6. Sistematika Penulisan

Penulisan tugas akhir ini akan dibagi beberapa bagian sebagai berikut :

Bab I Pendahuluan

Berisi latar belakang, perumusan masalah, batasan masalah, tujuan pembahasan, metodologi penyelesaian masalah dan sistematika penulisan.

Bab II Landasan Teori

Bab ini berisi penjelasan tentang dasar – dasar teori yang berkaitan dengan arsitektur jaringan yang akan dirancang sehingga akan membantu pengerjaan Tugas Akhir ini.

Bab III Perancangan dan Implementasi

Berisi tentang pembahasan perancangan proteksi pada server Zimbra berbasis UEC mengguanakan MyDLP, bagan jaringan, serta proses konfigurasi sistem operasi server dan proteksinya.

Bab IV Pengujian dan Analisis Hasil Implementasi

Bab ini dibahas mengenai pengujian dan analisis hasil implementasi pada Zimbra *mail server* berbasis UEC dengan penambahan keamanan

MyDLP yang telah dilakukan. Pengujian dan analisis ini bertujuan untuk mengetahui tingkat keamanan *server* yang dibangun terhadapa serangan.

Bab V Kesimpulan Dan Saran

Berisi tentang kesimpulan akhir dan saran pengembangan tugas akhir.