BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Diskominfo Provinsi Jabar atau Dinas Komunikasi dan Informatika Provinsi Jawa barat merupakan lembaga teknis daerah yang bergerak dalam bidang sarana komunikasi, informatika, dan hubungan masyarakat[1]. Lembaga tersebut dibentuk untuk membawahi berbagai permasalahan kemasyarakatan dibidang komunikasi. Untuk menjaga keamanan Data Eletronik dan Informasi tersebut maka Diskominfo Provinsi Jawa Barat harus benar-benar memantau dan mengantisipasi pencurian data yang terjadi pada suatu *server* agar keamanan data informasi yang bersifat *confidentional* pada seluruh *server* yang ada di Diskomnfo Provinsi Jawa Barat agar tetap terjaga dari berbagai ganguan yang berasal dari *attacker* baik dari internal maupun *exsternal* yang termasuk kedalam kegiatan *cybercrime*.

Server merupakan sebuah sistem komputer yang menyediakan berbagai jenis layanan dalam sebuah jaringan komputer seperti data *website*, *email*, *ftp*, hingga layanan multimedia yang akan tersimpan didalam *server* untuk dapat diakses dari satu komputer ke komputer lainnya yang terhubung dari suatu jaringan. Komunikasi jaringan melalui *protokol* dan *port* yang mejadi media untuk *transfer* data antara *server* dengan *client* menjadi jalur yang terbuka untuk semua pihak dapat mengakses aliran data di antara kedua sisi tersebut. Demikian juga dengan Diskominfo Provinsi Jawa Barat yang mempunyai beberapa *server* yang digunakan untuk mengelola berbagai data informasi baik yang bersifat data *confidential* maupun data *public*. Dengan mudahnya masyarakat mengakses data tersebut baik dari jaringan *internal* dan *exsternal*, potensi-potensi berbagai jenis serangan terjadi seperti perubahan data maupun potensi untuk menggangu aktifitas pada jaringan *server* tersebut supaya *server* tidak berfungsi sebagai mana mestinya. Menurut *website zone-h.org* dari Maret 2014 sampai Maret 2016 *website* resmi milik pemerintahan di lingkungan Provinsi Jawa Barat telah diretas

sebanyak 70 kali, dua diantaranya berasal dari *website* resmi milik Diskominfo[2], itu karena masih adanya celah di *website* milik diskominfo, sehingga orang yang meretas tersebut bisa dengan sangat mudah merubah semua data yang ada pada *server*.

SIEM (*Security Information And Event Management*) adalah teknologi memberikan keamana yang mengadopsi metodologi dapat digunakan untuk *management log*, peristiwa mengalir dari komputerisasi perangkat, sistem dan layanan terdistribusi dengan baseline keamanan.[3].

Dikarenakan belum adanya *server* untuk *monitoring* di Dinas Komunikasi Dan Informatika Provinsi Jawa Barat maka adanya serangan dan ilegal akses tidak terdeteksi dan tidak ada, untuk itu dengan adanya *server* SIEM dapat membantu untuk merekam semua aktifitas mengenai aspek detail dari *host, network* dan *server* sehingga dapat memberikan informasi kepada *administrator* tentang keamanan jaringan atau sistem. Karena diperusahaan ber skala besar yang banyak *server* biasanya butuh *monitoring*.

Berdasarkan Permasalah di atas, dapat diketahui bahawa di Diskominfo Provinsi Jawa Barat memerluka adanya sebuah kegiatan berupa "**PEMBANGUNAN *SERVER SECURITY INFORMATION MANAGEMENT* UNTUK *MONITORIG* KEAMANAN DI *SERVER* DISKOMINFO PROVINSI JAWA BARAT**" untuk meminimalisir berbagai gangguan penyerangan di *server* Diskominfo Provinsi Jawa Barat.

1.2 Perumusan Masalah

Berdasarkan permasalahan yang telah dikemukakan pada latar belakang dapat dirumuskan, sebagi berikut Bagaimana membangun *server monitoring Security Information And Event Management* di Diskominfo Provinsi Jawa Barat.

1.3 Maksud dan Tujuan

Berdasarkan permasalahan yang telah diuraikan, maka maksud dari penelitian ini tentang Pembangunan *Server Security Management* Untuk *Monitoring* Keamanan Di *Server* Diskominfo Provinsi Jawa Barat.

Tujuan dari penelitian ini adalah memudahkan Administrator dalam melakukan monitoring kemanan di Diskominfo Provinsi. Jawa Barat.

1.4 Batasan Masalah

Batasanmasalah yang ditentukan pada Pembanguan *Server* Security Management Untuk Monitoring Kemanan Di *Server* Diskominfo Provinsi Jawa Barat, meliputi :

1. Jenis metode yang digunakan dalam pembanguan *server* ini menggunakan jenis metode *Experimental*.
2. Implementasi OSSIM dilakukan pada jaringan komputer di Diskominfo.
3. Menggunakan sistem operasi berupa AlienVault OSSIM 5.3.0 64 bit.
4. Memonitoring Trafik jaringan.
5. Melakukan Pengujian terhadap *Server* OSSIM.

1.5 Metodelogi Penelitian

Dalam melakukan penelitian ini, penulis menggunakan beberapa metode dalam melakukan pengumpulan data, diantaranya :

1.5.1 Studi Pustaka

Penulis mengumpulkan dan mempelajari buku dan *ebook* yang berhubungan dengan tugas akhir yang dilakukan. Untuk melihat referensi selangkapnya terdapat pada halaman daftar pustaka.

1.5.2 Studi Lapangan

Studi lapangan dalam penelitian tugas akhir ini dibagi menjadi 3 bagian, yaitu:

1. Observasi

Pengamatan langsung ke lapangan (observasi) yang dilakukan oleh penulis, tempat pelaksanaannya yaitu di Dinas Komunikasi dan Informatika Provinsi Jawa Barat, Jalan Taman Sari no. 55 Telp. : 022-2502898 Fax : 022-2511505 Kota Bandung 40132.

2. Wawancara

Dalam melakukan pengumpulan data penulis juga melakukan wawancara secara langsung kepada pihak yang terlibat. Wawancara dilakukan kepada Bapak Buddhi Sudrajat, ST selaku Seksi Penyajian Data Informasi di Bidang Pusat Data Elektonik dan Bapak Bambang Indra Rachmawan, A.md selaku *Network Administrator* Dinas Komunikasi dan Informatika Provinsi Jawa Barat .

1.5.3 Metode Pembangunan *Server Monitoring*

Pembangunan *Server* Monitoring ini menggunakan sistem operasi OSSIM sebagai mendia pembangunan *server* dengan menggunakan Metode *Experimental*[3] adapun konsep dan tahapan proses *Experimental* ini,yaitu :

1. Studi Literatur

   Dalam melakukan tugas akhir penulis juga menggunakan literatur sejenis yang digunakan baik berasal dari jurnal-jurnal, prosiding maupun skripsi yang mempunyai topik yang mendekati dengan topik yang dibahas penulis
2. Analisis Sistem

   Menganalisis masalah dan menganalisis sistem yang sedang berjalan
3. Perancangan Sistem

   Perancangan yang dilakukan antara lain perancangan perangkat PC yang akan di jadikan sebagi *Server*, mengkonfigurasi OSSIM, dan memasang aplikasi penunjang agar OSSIM bisa berjalan dengan baik.
4. Implementasi dan Pengujian

   Implementasi dilakukan dengan cara memasang OSSIM dan melakukan pengujian terhadap *server* OSSIM.
5. Kesimpulan

   Kesimpulan dan saran yang sudah diperoleh dari hasil penelitian tugas akhir.

1.6 Sistematika Penulisan

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

BAB 1 PENDAHULUAN

Bab ini berisi latar belakang masalah, identifikasi masalah, maksud dan tujuan penelitian, batasan masalah, metodelogi penelitian dan sistematika penulisan.

Bab 2 LANDASAN TEORI

Bab ini membahas tentang profil tempat studi kasus di Dinas komunikasi dan Informatika Provinsi Jawa Barat dan dan berbagai konsep dasar teori-teori yang berkaitan dengan topik yang sedang dibahas.

BAB 3 ANALISIS DAN PERANCANGAN

Bab ini menguraikan tentang analisis masalah, analisis topologi, analisis kebutuhan komputer pembangunan *server*, analisis pengguna yang sedang terjadi, perancangan sistem , konfiguasi sistem, dan melakuka simulasi pengujian OSSIM.

BAB 4 IMPLEMENTASI DAN HASIL PENGUJIAN

Bab ini merupakan implementasi sistem yang telah dirancang, pengambilan trafik jaringan dan menguji sistem OSSIM menggunakan *DoS Ping Flood.*

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran yang sudah diperoleh dari hasil penelitian tugas akhir. Berdasarkan hasil dari kegiatan pembanguan *server monitoring* yang dapat dijadikan catatan untuk pengembangan selanjutnya.