BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Pada era globalisasi saat ini, teknologi informasi (TI) telah berkembang dengan pesat, terutama dengan adanya jaringan internet yang memudahkan orang atau masyarakat dalam berkomunikasi dengan pihak lain. Selain itu, para pengguna (*user*) dapat mengakses dan menggali seluruh informasi yang dibutuhkan, baik itu informasi yang bersifat umum (*public*) maupun bersifat pribadi (*private*).

Dengan berbagai macam sistem operasi yang digunakan pada saat sekarang ini, baik yang *free* (gratis) maupun berbayar, seperti linux yang berbasis *open source*, Windows, MAC OS dan lain sebagainya. Sistem operasi merupakan perangkat lunak (*software*) yang bertugas mengontrol manajemen perangkat keras, dan juga operasi-operasi dasar lainya. Berbagai aplikasi dan fitur-fitur (*utility*) yang berjalan baik di sistem Windows, atau sistem Linux (*open sources*) semua menjalankan data yang akhirnya berakhir pada subuah berkas file yang dinamakan dengan istilah "*Log*". *Log* merupakan bagian penting dari setiap sistem, *Log* mencatat setiap kegiatan yang berjalan didalam sistem. Peroses pencatatan didalam sistem sering disebut dengan istilah "*Logging*".

Pencatatan yang dilakukan untuk memeriksa kebutahan yang ada pada sistem, jika terjadi kesalahan (*error*) maka seorang *administrator* dapat lebih mudah mencari sumber kesalahan, karena informasi yang tercatat lebih rapi.

Demikian pula jika terjadi penyalah gunaan fasilitas, maka dapat diketahui (*monitoring*) siapa yang melakukanya dan apa saja yang dilakukanya.

Masalah yang sering dihadapi oleh penulis atau *administrator* jaringan server adalah tidak adanya manajemen sistem sebuah *log*, karena *administrator* akan kesulitan mencari file *log* jika terjadi sebuah kesalahan pada sistem, karena memiliki fungsi yang banyak pada sistem Linux yang berbasiskan *open source* yaitu salah satunya adalah sebagai, *web server*, *database server*, *email server* dan lain sebagainya.

Karena pencatatan data yang banyak dan yang berbeda-beda ini akan menyulitkan dan membingungkan para pelaku yang bergerak dalam bidang *networking* terutaama *administrator* jaringan server, karena harus mencari berkas file *log* yang jumlahnya sangat banyak dan tempat penyimpanannya (*hardisk*) yang tidak tertata secara formatnya , shingga muncul fasilatas yang penulis gunakan dengan program "*syslog*".

Oleh karena itu untuk mengidentifikasi masalah yang pada sebuah server atau aplikasi unix (*open source*), untuk membantu para *network scurity administrator* untuk mngidentifikasi dan menyelesaikan permasalahan yang ada pada server serta dapat mengkorelasikan *log* dalam jangka waktu tertentu. Selain itu juga perlu adanya file-file *log* selama ini.

1.2. Rumusan Masalah

Dari latar belakang yang telah penenulis uraikan diatas, ditemukan beberapa masalah yang dapat dirumuskan dalam satu rumusan masalah yaitu:

1. Bagaimana manajemen *log* dengan *logstash*, *kibana* dan *elasticsearch* pada *centos server*.
2. Bagaimana menganalisa dan mencatat file-file *loggin* yang *error* dengan *kibana* pada Centos Server.

1.3. Batasan Masalah

Batasan-batasan yang akan peneliti singgung dari uraian yang telah dipaparkan dilatar belakang ialah:

1. Penelitian difokuskan pada sistem monitoring *syslog* pada jaringan Centos Server.
2. Mengembangkan sistem keamanan data pada Centos Server.
3. Mengembangkan pendeteksian dengan menggunakan ELK.

1.4. Maksud dan Tujuan Penelitian

Berdasarkan permasalahan diatas, maka penulis bermaksud manjemen keamanan *log* untuk monitoring *syslog* berbasis *open source* pada centos server dengan tujuan sebagai berikut :

1. Memudahkan administrator untuk menganalisa jaringan server bila terjadi *error* dengan membaca file *log* server.
2. Memvisualisasikan *Log Pad* Centos Server.
3. Membuat *Log* manajemen dengan manggunakan *logstash*, *kibana* dan *elasticsearch* pada Centos Server.

4. Untuk manajemen *log* file agar mudah dipahami melalui *web interface kibana*.

1.5. Metode Penelitian

1.4.1. Metode Pengumpulan Data

Supaya memperoleh informasi yang tepat dan akurat serta mampu menyajikan informasi dengan lengkap maka digunakan beberapa metode pengumpulan data sebagai berikut:

a. Metode Observasi

Metode ini sebuah teknik pengumpulan data dan pengamatan terhadap manajemen keamanan jaringan log pada centos server sebgai monitoring jaringan yang ada.

b. Metode Wawancara

Melakukan dialog dengan para pelaku jaringan untuk mendapatkan informasi mengenai kemanan jaringan.

c. Arsip

Penliti mengambil catatan atau gambaran mengenai rancangan pengembangan sistem yang akan dijalankan.

1.4.2. Metode Perancagan Sistem

Jenis metode pengembangan sistem yang digunakan penulis menggunakan metode *Network Development Life Cycle* (NDLC), dengan beberapa tahapan yaitu: *Analisis*, *Design*, *Simulasi Prototype*, *Monitoring*, dan *Management*.

a. Analisis

Penulis disini mencoba menganalisis loggin user untuk monitoring sistem keamanan pada centos server. Penulis juga mencoba untuk memberikan gambaran grafik statistik dengan menggunakan kibana.

b. Design

Setelah melakukan analisis dari permasalahan diatas penulis mencoba men-design rancangan yang peneliti gunakan untuk mengembangkan system keamanan monitoring syslog untuk mempermudah pengerjaan selnajutnya.

c. Simulasi Prototype

Dalam simulasi prototype ini penulis mencoba langsung untuk membuat logging, dengan menggunakan sistem oprasi linux (*open sources*) agar bisa mendeteksi atau merekam aktifitas dari setiap syslog yang masuk.

d. Monitoring

Setelah melakukan simulasi prototype yang dilakukan, selanjutnya bagaimana mengawasi sistem dengan memantau (monitoring) situasi yang ada dalm *network* (jaringan) didalam penelitian yang dilakukan penulis.

e. Management

dalam peneltian ini setalah tahapan dari analisis samapai tahapan monintoring, selanjutnya untuk menajemen server sesuai dengan rancangan sistem *Network Deplopment Cycle*.

1.6. Sistematika Penulisan

Sistematika penulisan yang dimaksud oleh penulis adalah gambaran yang lebih jelas dan sistematis, Tugas Ahir ini dibagi menjadi lima bab dan tiap bab memiliki sub bab dengan dengan urutan sebagai berikut:

BAB I Pendahuluan

Bab I membahas tentang latar belakang masalah, rumusan masalah, maksud dan tujuan penelitian, dan sistematika penulisan.

BAB II Dasar Teori

Bab II membahas tinjauan pustaka, dimana penulis mengambil dan membaca literature-literatur karya ilmiah yang serupa, baik dari skripsi, tesis, jurnal, maupun buku. Membahas dasar-dasar teori yang sebagai dasar acuan dalam pembahasan penelitian ini

BAB III Analisis dan Perancangan

Pada bab ini menjelaskan maupun mengenai analisis masalah, analisis kelemahan, analisis sistem, analisis kebutuhan dan bagaimana analisis pemacangan sistem yang digunakan

BAB IV Implementasi dan Pembahasan

Bab ini akan menguraikan hasil pengujian manajemen *log* pada Centos Server untuk memudahkan administrator jaringan dalam monitoring *log* yang masuk pada server jaringan.

BAB V Penutup

Bab ini berisi kesimpulan dari hasil yang didapat melalui analisa manajemen keamanan *log* untuk monitoring *syslog* berbasis *open*

sources pada Centos Server dan juga saran pengembangan bagi peneliti terhadap pengembangan sistem keamanan jaringan.