BAB I

PENDAHULUAN

1.1 Latar Belakang

PT Git Solution merupakan perusahaan yang bergerak di bidang perencanaan, pembangunan dan pengembangan serta audit sistem berbasis teknologi, yang memberikan pelayanan antara lain pembuatan *blueprint IT*, audit terhadap implementasi *IT*, analisis dan desain sistem informasi, perancangan dan pembuatan *website*, *training* dan sertifikasi bidang *IT*, desain grafis dan multimedia, perancangan dan pembuatan aplikasi *mobile*, dan pembuatan *games* sebagai media promosi/informasi.

Menurut pengelola PT Git Solution sebagai penyedia layanan, sistem yang berjalan pada *server* harus mampu beroperasi 24 jam penuh, sehingga untuk memantau jalannya *service* pada *server* diperlukan pencatatan dalam bentuk *log event management* yang bersifat *realtime* untuk mencatat aktivitas *service* yang berjalan pada *server*. Namun demikian PT Git Solution belum mempunyai suatu sistem yang dapat menangani data dalam jumlah besar dan menghasilkan detail informasi dari *log*, padahal *log management* sangat dibutuhkan oleh sistem *administrator* untuk dapat mengelola data *log*. Oleh karena itu, perlu adanya sentralisasi yang dapat mengelola *file log* tersebut. Sentralisasi *log* dapat berguna ketika sistem *administrator* mencoba untuk mengidentifikasi masalah pada sebuah *server*, agar dapat membantu sistem *administrator* mencari semua *log* di dalam satu tempat.

Selain itu pada PT Git Solution juga membutuhkan sistem yang dapat memantau dan melakukan deteksi dini terhadap keamanan *server* jika terjadi penyerangan terhadap *server*. Karena mudahnya mengakses jaringan, memungkinkan adanya gangguan dari pihak yang ingin menyerang, merusak, bahkan mengambil data penting. Kurangnya informasi tentang penyerang seperti siapa yang menyerang, metode yang digunakan dalam menyerang, bagaimana mereka menyerang, dan kapan serangan dilakukan.

Berdasar dari latar belakang masalah di atas, maka penulis membuat penelitian dengan judul "IMPLEMENTASI DAN ANALISIS KEAMANAN SERVER MENGGUNAKAN ELK STACK PADA PT GIT SOLUTION". *ELK (Elasticsearch, Logstash, Kibana)* digunakan untuk menampilkan data-data *log* dari *web server*, diharapkan akan mampu mendeteksi serangan yang masuk ke dalam *server*, memberikan rekomendasi berdasarkan uji celah keamanan *server*, dan mempermudah seorang *administrator* untuk memantau jalannya *service* pada *server*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, permasalahan yang dapat dirumuskan adalah sebagai berikut:

1. Bagaimana menerapkan *log management system* menggunakan *ELK (Elasticsearch, Logstash, Kibana)* untuk memudahkan dalam membaca dan menganalisis *log service* pada *server*?
2. Bagaimana mengidentifikasi serangan pada *server* menggunakan *ELK (Elasticsearch, Logstash, Kibana)?*

1.3 Batasan Masalah

1. Hanya membahas tentang implementasi *log event management*.
2. Penelitian ini hanya menggunakan informasi dari *log Apache web server, syslog,* dan *auth log*.
3. Implementasi dilakukan dengan bantuan *server* simulasi.
4. Penelitian hanya menerapkan pada *web server Debian 9*.
5. Rekomendasi yang diajukan adalah melakukan *block ip,* dan *filtered port*.

1.4 Maksud dan Tujuan Penelitian

1. Membuat pemusatan *log* dalam satu *dashboard*.
2. Menampilkan data-data *log* dari *web server*.
3. Mengintegrasi, mengidentifikasi, dan mendapatkan *performance indicator Apache web server*.
4. Mengidentifikasi serangan terhadap *server*.
5. Memberikan rekomendasi keamanan berdasarkan uji celah keamanan *server*.
6. Untuk memenuhi syarat kelulusan Program Strata 1 (S1) di Universitas AMIKOM Yogyakarta.

1.5 Manfaat Penelitian

1. Diharapkan sistem ini mampu mengidentifikasi serangan terhadap *server*.
2. Mempermudah seorang *administrator* untuk melakukan pengawasan terhadap semua kegiatan pada *server*.

1.6 Metode Penelitian

Metode pelaksanaan yang dilakukan selama pembuatan skripsi, meliputi:

1.6.1 Metode Pengumpulan Data

1. **Metode Observasi**

   Metode pengumpulan data dengan melakukan pengamatan dan mempelajari sistem yang berjalan.

2. **Metode Wawancara**

   Pengumpulan data melalui tanya jawab dengan tim terkait dalam kasus ini adalah tim dari PT Git Solution.

3. **Metode Literatur**

   Mengumpulkan data-data dari jurnal penelitian yang memiliki fokus yang sama.

1.6.2 Perencanaan

Perencanaan yang dilakukan yaitu mengidentifikasi masalah-masalah yang ada di PT Git Solution

1.6.3 Analisis

Penulis melakukan analisis terhadap kebutuhan sistem yang ada pada PT Git Solution.

1.6.4 Perancangan

Perancangan sistem ini menggunakan tiga mesin, yaitu *Elasticsearch* yang dipadukan dengan *Logstash* sebagai penyimpanan data dan *Kibana* sebagai visualisasi.

1.6.5 Implementasi

Tahap implementasi berupa proses pembangunan, instalasi, simulasi, dan pengujian terhadap sistem yang telah dibuat untuk mengetahui serangan yang terjadi pada *server*.

1.6.6 Maintance

Seorang *administrator* melakukan pemeliharaan terhadap sistem secara berkala sesuai peraturan dan pembaruan.

1.7 Sistematika Penulisan

Adapun sistematika penulisan skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini menerangkan tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, metode penelitian dan sistematika penelitian.

BAB II LANDASAN TEORI

Berisi tinjauan pustaka dan dasar-dasar teori yang digunakan untuk membangun sistem serta membantu pengolahan berbagai macam laporan yang berkaitan langsung dengan ilmu atau masalah yang diteliti.

BAB III ANALISIS DAN PERANCANGAN

Bab ini menjelaskan tentang analisis dan dasar-dasar teori yang ada pada PT Git Solution, dibuat serta hal-hal yang diperlukan dalam pembuatan sistem *ELK Stack* beserta hasil perancangan yang telah dibuat.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas tentang proses pembangunan dan perancangan, instalasi, pemusatan *log* dan simulasi serangan terhadap *server*.

BAB V PENUTUP

Berisi kesimpulan dan saran yang penulis rangkum selama proses penelitian.