BAB I
PENDAHULUAN

1.1 Latar Belakang

Semakin cepat nya perkembangan teknologi sekarang membuat kita bisa merasakan sistem komunikasi jaringan komputer yang dihubungkan melalui perangkat *server*. Pengertian *server* adalah perangkat komputer yang digunakan untuk menyimpan dan mengelola data dalam sebuah jaringan. *Administrator* adalah orang yang mengatur semua aktifitas *server* mulai perawatan sampai perbaikan. menjadi seorang *administrator* merupakan tugas yang berat karena harus menjaga keamanan *server* dari serangan luar. merupakan hal yang sangat penting untuk menjaga keamanan *server* pada sebuah jaringan karena jika *server* pada sebuah jaringan rusak maka jaringan tersebut tidak akan berjalan.

Dalam [1] menyatakan *server* sebagai perangkat utama dalam sebuah sistem komunikasi jaringan yang berfungsi sebagai penyedia layanan harus mampu berjalan selama 24 jam penuh, sehingga untuk memantau jalannya *service* pada *server* diperlukan pencatatan dalam bentuk *log event management* yang bersifat *real time* untuk mencatat aktifitas *service* yang berjalan pada *server*. Dan dalam [2] menyatakan dalam menjaga sebuah *server* akan ada berbagai masalah yang akan dihadapi, salah satunya adalah kerusakan sistem operasi *server*, kerusakan pada *program* aplikasi ataupun terhadap gangguan dari luar sistem seperti serangan *hacker*, *virus*, *trojan* dan lain sebagainya.

CV Lanis IT Support and Maintenance merupakan sebuah Badan Usaha yang bergerak dibidang layanan jasa *support* teknis perangkat teknologi informasi. CV Lanis IT Support and Maintenance masih belum mempunyai suatu sistem yang dapat menangani *data log* dalam jumlah besar dan menghasilkan detail informasi dari *log*, dengan begitu *administrator* akan kesulitan dalam memonitoring *server* jika ada serangan semacam *DDoS (Distributed Denial of Service)*, merupakan serangan yang dapat mengakibatkan sistem keamanan jaringan yang diserang mengalami gangguan. Maka dari itu dibutuhkan suatu

sistem yang dapat membantu *administrator* mencari semua *log* dalam satu tempat. agar *administrator* dapat dengan mudah mengidentifikasi jika terjadi serangan.

ELK (Elasticsearch, Logstash, Kibana) merupakan salah satu solusi *log management* yang dapat mencatat *log* dari seluruh perangkat yang ada di infrastruktur IT secara *real time*. Terdapat banyak *tool* yang dapat melakukan *log management* seperti *Prometheus*, *Splunk* dan lain sebagainya. Peneliti memilih *ELK* karena memiliki beberapa keunggulan dari pada yang lain diantaranya adalah bersifat *Open source*, *Elasticsearch* dapat membantu dan mendistribusikan *data* secara otomatis agar *data* tetap dapat dinilai dan diamankan, dan *ELK* dapat memvisualisasikan semua jenis *data* sumber yang di indeks ke *elasticsearch*.

Pada penelitian ini menggunakan metode pengembangan sistem waterfall. nama model ini sebenarnya adalah "Linear Sequential Model" dimana hal ini menggambarkan pendekatan yang sistematis dan juga berurutan pada pengembangan perangkat lunak, dimulai dengan spesifikasi kebutuhan pengguna lalu berlanjut melalui tahapan-tahapan perencanaan (*planning*), permodelan (*modelling*), konstruksi (*construction*), serta penyerahan sistem ke para pengguna (*deployment*), yang diakhiri dengan dukungan pada perangkat lunak lengkap yang dihasilkan. [3] peneliti memilih metode ini karena :

1. Dengan pelaksanaan yang dilakukan secara bertahap maka sistem yang dihasilkan akan baik
2. Menggunakan proses pengembangan model *fase one by one*, sehingga akan meminimalis kesalahan yang mungkin akan terjadi.

Pembeda penelitian ini dari penelitian serupa adalah selain mengidentifikasi serangan terhadap *server* melalui *log management* pada *server*, penelitian ini juga memberikan rekomendasi keamanan pada *server* tersebut. Dengan menggunakan *ELK stack* yang dapat menjadi solusi *log management*, penelitian ini diharapkan dapat membantu *administrator* dalam mendeteksi serangan yang masuk ke dalam *server*, dan membantu untuk memantau jalanya *service* pada *server*.

1.2 Rumusan Masalah

1. Bagaimana penerapan ELK (Elasticsearch, Logstash, Kibana) untuk membantu *administrator* dalam menganalisis *log service* pada *server*?
2. Bagaimana mengidentifikasi serangan pada *server* dengan cara memonitoring *log service* pada *server* dengan menggunakan *ELK (Elasticsearch, Logstash, Kibana)* ?
3. Bagaimana menguji *ELK (Elasticsearch, Logstash, Kibana)* dengan simulasi serangan *DDoS (Distributed Denial of Service)* ?

1.3 Batasan Masalah

1. Penelitian diterapkan pada *server Ubuntu Server LTS 22.04*.
2. Implementasi menggunakan bantuan simulasi *server*.
3. Belum terimplementasikan di server CV Lanis IT Support & Maintenance.
4. Penelitian hanya menggunakan informasi dari *syslog*, dan *auth log*.
5. Untuk pengujian *ELK Stack* menggunakan enam simulasi serangan yaitu Gagal *Login SSH*, Akurasi ketepatan waktu, Perubahan *package*, Pengujian Create File dan Directory, Perubahan mode akses *directory* dan *DDoS*.

1.4 Tujuan Penelitian

1. Implementasi *ELK Stack* sebagai sistem *monitoring log*.
2. Membantu *administrator* menampilkan aktifitas *log server* pada *dashboard ELK*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah untuk membantu tugas seorang *administrator* dalam menjalankan tugasnya untuk melakukan pengawasan pada *server*.

1.6 Sistematika Penulisan

Dalam penelitian ini, penulis menggunakan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN, berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA, berisi tinjauan pustaka, dasar-dasar teori yang digunakan untuk melakukan penelitian.

BAB III METODE PENELITIAN, berisi tentang analisis pada CV Lanis IT Support and Maintenance , rancangan sistem *ELK Stack* yang akan dibuat dan apa saja yang dibutuhkan untuk melakukan penelitian ini.

BAB IV HASIL DAN PEMBAHASAN, Bab ini berisi tentang proses pembangunan, dan instalasi sistem yang sudah dirancang sebelumnya dan melakukan pengujian terhadap sistem yang telah dibuat.

BAB V PENUTUP, berisi kesimpulan dari penelitian yang telah dilakukan dan berisi saran untuk pengembangan penelitian ini selanjutnya.