BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi saat ini sudah berkembang sangat pesat, termasuk dalam teknologi penyimpanan. Media penyimpanan merupakan salah satu teknologi yang sudah berkembang sangat maju, sehingga *data* tidak hanya dapat di simpan pada penyimpanan lokal tetapi juga dapat di simpan pada sebuah *database server*. Perkembangan teknologi ini juga diiringi dengan berkembangnya ancaman, sehingga diperlukannya sebuah sistem yang dapat mengetahui kapan terjadinya ancaman pada sistem yang digunakan.

Saat ini, sudah banyak sekali perusahaan yang menggunakan sistem penyimpanan *data* secara daring. Sistem ini biasanya disebut dengan *server*. *Server* sering digunakan oleh perusahaan karena sistem ini dapat diakses secara bersamaan oleh banyak pengguna, sehingga karyawan di perusahaan dapat mengambil, menyimpan, dan bahkan dapat mengolah *data* secara fleksibel. *Server* saat ini sedang marak digunakan oleh seluruh perusahaan, karena kondisi dunia yang sedang mengalami pandemi COVID-19 sehingga mengharuskan para pekerja untuk bekerja dari rumah, oleh karena itu *server* ini sangat membantu dalam memperlancar pekerjaan [1].

Seperti yang sudah dijelaskan pada paragraf sebelumnya, penggunaan sistem ini tidak luput dari sebuah ancaman. Meskipun sudah banyak *server* yang memiliki sistem perlindungan, masih tetap terjadi pencurian *data* yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Hal ini menyebabkan kepercayaan masyarakat dan perusahaan terhadap sistem *server* dapat berkurang[2].

Pengamanan sistem *database server* harus terus dilakukan, karena sudah mulai banyak yang menggunakan teknologi ini. Penggunaan sistem pendeteksi ancaman pada *server* sangat penting apabila perusahaan menyimpan *data* pada *database server*, oleh sebab itu sistem pendeteksi ini dibutuhkan agar dapat mendeteksi ancaman meskipun pemilik *data* sedang tidak membuka *database server* mereka.

Dalam mengatasi masalah ini, pada penelitian ini akan diterapkan sistem pendeteksian ancaman yang menggunakan ELK *Stack*. ELK *Stack* (*Elasticsearch*,

*Log*stash, *Kibana*) merupakan aplikasi yang dapat mendeteksi *log* pada *database server* apakah tingkat kerentanan yang dimiliki tinggi atau rendah, setelah sistem penilaian yang dilakukan oleh *Log*stash maka akan ditampilkan pada menu *Kibana*. Maka dari itu diharapkan penggunaan ELK *Stack* dapat memperkecil ancaman yang terjadi pada *database server*[3].

1.2 Rumusan Masalah

Pada penelitian ini didapat rumusan masalah sebagai berikut :

1. Bagaimana sistem ELK *Stack* dapat mengetahui ancaman keamanan akan terjadi?
2. Bagaimana sistem ELK *Stack* dapat memberikan informasi kepada pemilik *data* apabila akan terjadi sebuah ancaman?
3. Apakah sistem ELK *Stack* cukup efektif untuk mengatasi ancaman pada *dataset* berisi DDoS?

1.3 Tujuan dan Manfaat

Adapun tujuan ini dari penelitian ini yaitu :

1. Mengetahui cara kerja ELK *Stack* saat mendeteksi ancaman.
2. Mengetahui apakah sistem pemberitahuan ancaman dapat bekerja dengan baik dan menghindari ancaman terjadi .
3. Mengetahui apakah ELK *Stack* aman dan efektif untuk digunakan.

Adapun manfaat dari penelitian ini yaitu :

1. Menambah keamanan dari *server* yang telah dipasangi ELK *Stack.*
2. Mengurangi terjadinya ancaman kerentanan *data* pada *database server* dengan pemberitahuan yang muncul kepada admin.
3. Memastikan ancaman yang terjadi dapat dideteksi sehingga dapat diperbaiki.

1.4 Batasan Masalah

Berikut merupakan batasan masalah yang ada pada penelitian ini :

1. *Data* yang akan digunakan berasal dari *dataset* berisi serangan DDoS.
2. Alat yang digunakan yaitu ELK *Stack.*

3. Penelitian ini berfokus pada penggunaan ELK *Stack* yang diaplikasikan untuk mendeteksi *dataset*.

1.5 Metode Penelitian

Pada penelitian ini, metode penelitian yang digunakan sebagai berikut :

1. Studi Literatur
2. Perancangan sistem
3. Implementasi sistem
4. Pengujian dan analisis sistem
5. Penarikan kesimpulan
6. Pembuatan laporan Tugas Akhir