BAB I
PENDAHULUAN

1.1. Latar Belakang

Seiring dengan perkembangan teknologi informasi akses untuk segala sesuatu menjadi lebih mudah, salah satunya dalam bidang internet, berbagai perangkat pintar seperti *smartphone, smart* TV dan *device* lainnya saling terhubung satu sama lain sehingga menciptakan fenomena *Internet of Things* (*IoT*) yang terus berkembang. Jaringan perangkat yang dilengkapi dengan teknologi di dalamnya memungkinkan mereka untuk saling berinteraksi satu sama lain ataupun dengan lingkungan di luar. Karena banyaknya jumlah dan macam perangkat yang ada, *IoT* telah menjadi sasaran yang menarik bagi penjahat *cyber*.

Penyerangan perangkat seperti mengganggu, merusak serta mengambil data penting yang ada biasaya ditunjukan dengan beberapa gejala yang terjadi, kurangnya informasi tentang apa, siapa, mengapa, bagaimana dan kapan serangan itu dilakukan menjadi salah satu hal yang patut di perhatikan. Maka dari itu sistem berupa Honeypot *security resource* yang sengaja dibuat untuk diselidiki, diserang, atau dikompromikan digunakan untuk menjebak pelaku *cybercrime* yang hendak mengakses data yang ada didalam sebuah perangkat *IoT*.

Penelitian ini dilakukan untuk dapat menganalisis *log* penyerangan yang sudah terjadi agar mendapat informasi tentang penyerangan dengan menggunakan ELK Stack dan *Regular Expression* sebagai pemantauan dan analisis data *log* yang dihasilkan oleh Honeypot.

1.2. Rumusan Masalah

Berdasarkan topik pada penelitian tugas akhir ini maka rumusan masalah adalah sebagai berikut :

1. Bagaimana cara penerapkan ELK Stack dengan *Regular Expression* pada *log* Honeypot untuk visualisasi dan *monitoring* log Honeypot ?
2. Bagaimana hasil *performance* dan akurasi yang dihasilkan dengan menggunakan ELK Stak dan *Regular Expression* ?

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah dari penelitian yang akan dilakukan yaitu untuk merancang sistem yang mampu menampilkan serangan pada sistem Honeypot. Penelitian ini akan memberikan hasil *log* Honeypot dalam bentuk visualisasi untuk mempermudah dalam meganalisis dan me*monitoring* sistem Honeypot.

1.4. Batasan Masalah

Adapun Batasan dari proposal Tugas Akhir ini adalah:

1. Penelitian ini hanya membahas penggunaan, pengumpulan dan pemerosesan data *log* Honeypot.
2. Penelitian ini berfokus pada bagaimana cara implementasi dan memvisualisasikan hasil *log* Honeypot dengan *Regular Expresession* dan ELK Stack.

1.5. Metodologi Penelitian

Metodologi penelitian yang digunakan pada Tugas Akhir ini adalah:

1. Studi Literatur

Tahap ini dilakukan dengan tujuan untuk mendapatkan informasi dan referensi sebagai dasar dari pengerjaan tugas akhir. Referensi ini dapat berupa *paper*, laporan, jurnal, buku, ataupun artikel dari internet. Informasi yang di dapat berupa berbagai identifikasi, metode yang digunakan, dan Gambaran mengenai bagaimana proses tersebut dapat dilakukan.

2. Analisa Kebutuhan

Analisis kebutuhan dilakukan bertujuan untuk mengetahui kebutuhan apa saja yang mendukung proses implementasi *Regular Expression* dan ELK stack untuk proses *analytic* data.

3. Perancangan *Regular Expression* dan ELK Stack

Pada tahap ini dilakukan perancangan *parse* data yang akan dilkukan oleh *regular expression* untuk mengambil data-data penting pada *log* Honeypot. Lalu dilakukan perancangan *system* ELK stack untuk memproses *log* yang ada.

4. Implementasi *Regular expression* dan ELK stack

Pada tahap ini dilakukan implementasi dari perancangan yang dibuat untuk mengetahui apakah perancangan yang dibuat dapat berjalan sesuai dengan kebutuhan.

5. Pengujian *Regular expression* dan ELK Stack

Pengujian dilakukan dengan dengan cara menghitung akurasi data yang dihasilkan dari proses *string matching* pada *file* JSON menggunakan *Regular Expression* dengan penghitungan manual dan *performance* yang dihasilkan saat proses *string matching* berlangsung. Untuk pengujian Elk stack dilakukan dengan cara melihat apakah data tersebut berhasil di *index* oleh Elasticsearch.

6. Pembuatan Laporan

Pada proses ini dilakukan pembuatan dokumentasi laporan Tugas Akhir yang akan digunakan untuk sidang Tugas Akhir.

1.6. Sistematika Penulisan

Penulisan tugas akhir ini dibagi dalam beberapa bagian. Tiap-tiap bagian menjelaskan langkah demi langkah dalam pengerjaan tugas akhir ini. Berikut adalah bagian tersebut:

1. BAB I PENDAHULUAN

Pada bab ini menjelaskan latar belakang penelitian, rumusan masalah tujuan, dan batasan masalah, dan metodologi penelitian yang dilakukan.

2. BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang tinjauan teori dan sumber-sumber terkait yang digunakan dalam penelitian yang dilakukan.

3. BAB III ANALISIS DAN PERANCANGAN

Bab ini menjelaskan tentang proses analisis pada sistem serta desain dan perancangan aplikasi yang akan dibuat pada tugas akhir ini. Perancangan sistem diGambarkan dengan meggunakan *flowchart,* data *flow* diagram, dan perancangan sistem.

4. BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini membahas proses pengujian yang dilakukan pada aplikasi, dan hasil pengujian dianalisis agar dapat dilakukannya penarikan kesimpulan dalam penelitian ini.

5. BAB V KESIMPULAN DAN SARAN

Bab ini membahas kesimpulan dari hasil pengujian aplikasi yang dibuat dan saran yang membuat hasil penelitian lebih baik untuk kedepannya.