BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan merupakan hal yang sangat penting dalam dunia teknologi dan informasi. Jumlah serangan siber terus meningkat seiring berjalannya waktu, baik di dunia maupun di indonesia. Hal tersebut dapat dilihat dari data Badan Siber dan Sandi Negara, jumlah serangan yang terjadi pada tahun 2018 tercatat di angka 12.895.554 serangan, dan serangan *malware* tercatat di angka 513.863 serangan [1]. Seperti ditunjukkan pada Gambar 1.1.

Gambar 1.1 Data Serangan Siber Tahun 2018

(Sumber Gambar: https://bssn.go.id [2])

Tidak mungkin untuk melindungi jumlah serangan yang meningkat secara eksplosif dengan cara yang sempurna. Tetapi penting untuk meminimalkan akibatnya dengan mendeteksi sumber serangan dan menerapkan reaksi yang sesuai. Ponemon Institute mengatakan bahwa dibutuhkan biaya rata-rata $8.76 juta untuk menangani serangan [3].

Sebagai solusi untuk menangani masalah tersebut, di butuhkan *tools* untuk membaca serangan yang mencoba masuk kedalam server. *Honeypot* merupakan salah satu *tools* dalam keamanan komputer yang biasa digunakan, honeypot merupakan sistem yang dirancang untuk menjebak penyerang dengan harapan penyerang akan masuk dan mengeksploitasi server. *Honeypot* mempunyai keunggulan dalam investigasi untuk menganalisis ancaman, intensitas dan kerentanan keamanan server. Administrator sistem dapat menganalisa serangan menggunakan *honeypot*. secara garis besar, *honeypot* memiliki tiga tingkatan, yaitu interaksi rendah, interaksi menengah dan interaksi tinggi. Tingginya intensitas serangan pada *honeypot*, maka *log* yang dapat dianalisis semakin besar dan risiko yang diterima semakin besar pula [4].

Bertepatan dengan tidak mudahnya menganalisa *log* yang di peroleh oleh honeypot, maka di butuhkan *tools* untuk memvisualisasikan sehingga memudahkan dalam menganalisa *log honeypot dengan* cepat. Log management tools yang digunakan pada penelitian ini adalah *Grafana Loki* dan *ELK Stack*, hasil catatan *log honeypot* di visualisasi menggunakan kedua platform tersebut, dimana *Grafana loki* ini merupakan kombinasi dari *Grafana, loki dan promtail* dan *ELK Stack* merupakan kombinasi dari *Elasticsearch, Logstash,* dan *Kibana.*

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka pokok permasalahan yang akan diteliti adalah banyaknya langkah-langkah yang harus dilakukan untuk menganalisis log dari honeypot, sehingga mengakibatkan proses analisis log semakin sulit, platform monitoring dan manajemen log dibutuhkan untuk mempermudah proses analisis. Oleh karena itu diperlukan membandingkan platform *Grafana Loki* dengan *ELK Stack* untuk mengetahui performa CPU dan

Memori dari kedua platform tersebut. Dalam mengatasi permasalahan di atas, maka perlu di diimplementasikan kedua platform tersebut untuk mengetahui kelebihan dan kekurangannya sehingga dapat membantu administrator dalam memilih platform yang sesuai dengan kebutuhannya.

1.3 Batasan Masalah

Adapun Batasan – batasan dibuat untuk mempersempit pembahasan dalam skripsi ini sebagai berikut:

a. Sistem dirancang menggunakan *Digital Ocean* dan *Ubuntu Server 18.04*, sebagai server. *Cowrie, Grafana Loki, ELK Stack*.
b. Sistem menggunakan Cowrie, Suricata, Dionaea sebagai *honeypot*.
c. Jenis serangan yang digunakan yaitu *DoS, MS17-10, Brute Force*
d. Sistem menggunakan *ELK Stack* dan *Grafana Loki* sebagai *Log Event Managemen tools*.
e. Perbandingan hasil Analisa *Log* menggunakan *Grafana Loki* dan menggunakan *ELK Stack*
f. Penelitian mencakup, perancangan, dan percobaan terhadap honeypot server untuk melihat log yang berhasil tercatat kemudian visualisasi pada *ELK Stack* dan *Grafana Loki*
g. Penelitian ini mencakup analisis performa pemakaian *CPU* dan *Memory* dari platform *Grafana Loki* dan *ELK* Stack saat terjadi serangan.
h. Performa yang dianalisis hanya dari *services* utama dari kedua platform tersebut yaitu Loki, Grafana, untuk Grafana Loki , Logstash, Elasticsearch, Kibana untuk ELK Stack.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk membandingkan performa CPU dan Memori *Grafana Loki* dan *ELK Stack* sebagai platform yang digunakan untuk manajemen log dan sebagai acuan untuk mempermudah Sistem administrator memilih platform yang sesuai dengan kebutuhannya.

1.5 Sistematika Penulisan

Bab I Pendahuluan, berisi: latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

Bab II Landasan Teori, berisi: hasil penelitian sejenis yang sudah pernah dilakukan sebelumnya, teori penunjang, dan referensi berupa buku, jurnal, dan laporan skripsi/tesis.

Bab III Metodologi Penelitian, berisi: penjelasan mengenai metode penelitian yang digunakan untuk memahami dan mengeksplorasi objek penelitian, hasil observasi / pengumpulan data, masalah yang terdapat pada objek, dan gambaran umum proyek atau objek penelitian, hingga Rencana Alur Penelitian.

Bab IV Pembahasan, berisi: rancangan proyek, implementasi *coding* dan desain, serta evaluasi rancangan. Selanjutnya alur pengerjaan proyek, metode testing, hingga hasil akhir penelitian dan pembahasan analisis hasil akhir penelitian, termasuk pembahasan hasil-hasil uji coba (testing). Data hasil akhir pengujian dapat berupa grafik, table, data monitoring, log system, dan lain-lain, dengan pembahasan.

Bab V Penutup, berisi kesimpulan dari hasil akhir penilaian proyek, dan saran.