BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

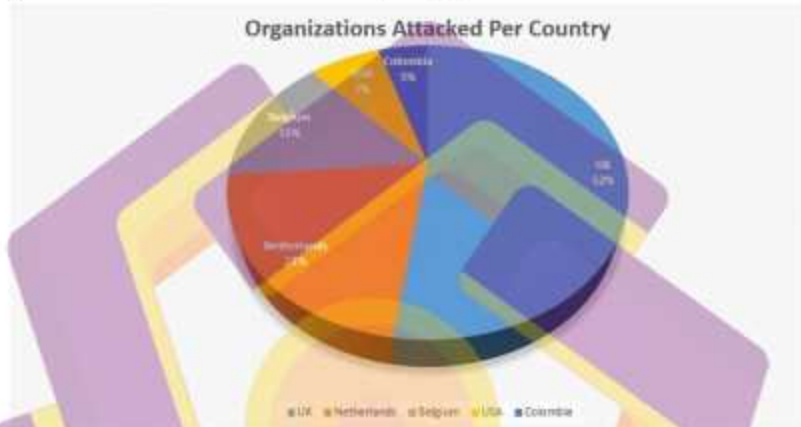
Semakin berkembangnya teknologi komunikasi antar perangkat mengalami perkembangan yang sangat signifikan. Kehadiran teknologi dengan inovasi baru merupakan awal dari perubahan hidup manusia yang dengan kehadiran teknologi dapat dipercara mampu mempermudah pekerjaan manusia dari segala sisi.

Salah satu contoh kemajuan teknologi yaitu dengan majunya teknologi komunikasi antar manusia, manusia dapat berkomunikasi dari manapun dan kapanpun. Seperti yang sekarang dengan pengguna terbanyak dengan sebutan media sosial yaitu WhatsApp, Telegram, Twitter, Facebook, Instagram, dan masih banyak lagi[1].

Tidak hanya dengan menggunakan media sosial, saat ini kita dapat berkomunikasi melalui jaringan dengan memanfaatkan teknologi yang disebut Voice over Internet Protocol (VoIP). VoIP merupakan salah satu aplikasi yang cepat berkembang. Manfaat VoIP dapat digunakan sebagai jaringan komunikasi yang diimplementasikan dengan aplikasi Asterisk sebagai server[2]. Fungsi utama asterisk untuk mengimplementasikan pertukaran telepon, teknologi ini dapat mengurangi biaya dan memaksimalkan hasil telepon. Dibalik semakin majunya teknologi asterisk semakin banyak pula yang mencoba menyerang sistem tersebut[3]. Untuk itu penulis melakukan analisa pada log asterisk.

Banyaknya serangan dari seluruh dunia yang menargetkan VoIP (Voice over Internet Protocol), yang khususnya pada Session Initiation Protocol (SIP) secara global. Pada tahun 2019 terdapat CVE-2019-19006 yang memanfaatkan kerentanan pada Sangoma PBX, yang memberikan akses admin kepada penyerang ke sistem dan memberikan semua akses kontrol hingga dapat mengunggah file PHP yang disandikan dan menyalahgunakannya. Serangan terhadap VoIP menjadi lebih imajinatif dan benyak serangan dapat menyebabkan kerusakan, misalnya Server yang digunakan overload, rusak, kerugian keuangan karena tagihan telepon meningkat dratis. Salah satu serangan pada VoIP yaitu BruteForce, yaitu penyerang

mencoba mengidentifikasikan nama pengguna dan kata sandi dari akun SIP yang valid[4]. Untuk serangan BruteForce penyerang mengirim kombinasi karakter acak ke SIP dan juga mengidentifikasikan akun yang mungkin mendapatkan respon. Dalam 5 tahun terakhir terdapat 822 juta serangan termasuk serangan Bruteforce pada SIP dari 5.591 sumber di 187 Negarasi[5].



Gambar 1 Serangan VoIP dari beberapa Negara

(Sumber Gambar https://research.checkpoint.com)

Membaca log yang sangat banyak dalam satu hari bisa sampai ratusan bahkan sampai jutaan baris log, apalagi jika sampai misalnya 10 hari. Tidak mungkin untuk membaca log serangan yang meningkat secara eksplosif. Namun hal yang penting adalah meminimalkan pengecekan dengan menemukan penyebab serangan dan menerapkan respon yang tepat. Menurut Institut Ponemon dibutukan waktu sekitar 210 hari untuk mendeteksi serangan dan 70 hari untuk menekan insiden[6].

Untuk meringankan pengecekan pada log tersebut, dibutuhkan tools untuk membaca log pada asterisk. Dengan memusatkan log dapat membantu pengecekan log dengan mudah. ELK Stack merupakan salah satu tools open source yang dapat digunakan sebagai pengolahan data yang sangat besar. ELK dapat menganalisis berbagai log dari berbagai sumber termasuk asterisk server[7].

Selain Menggunakan tools ELK Stack, salah satu tools lain yaitu Splunk. Splunk merupakan salahsatu tools monitoring yang banyak dipakai untuk memantau, mencari, menganalisis, dan memvisualisasikan data yang dihasilkan oleh sistem secara realtime[8]. Splunk menyediakan akses data yang mudah untuk didiagnosa dan solusi yang mudah dalam berbagai masalah. Splunk terbagi menjadi 2 yaitu Splunk Entrerprise & Splunk Hunk. Splunk Enterprise dapat mengumpulkan data log dari seluruh sistem dan dapat dianalisis sedangkan Splunk Hunk merupakan cara baru untuk mengindeks dan menjalankan query data Hadoop dengan mudah dan menampilkan dashboard.

1.2 Rumusan Masalah

Berdasarkan dari latar belakang tersebut, maka bagaimana performa platform ELK Stack dan Splunk dalam membaca log serangan bruteforce pada log Asterisk?

1.3 Batasan Masalah

Adapun batasan-batasan masalah untuk mempersempit pembahasan dalam skripsi ini sebagai berikut:

a. Sistem menggunakan server dari Google Cloud dan Ubuntu server 18.10.
b. Server asterisk menggunakan Debian versi 10
c. Menggunakan Asterisk versi 16.18 LTS
d. Platform yang digunakan ELK Stack dan Splunk
e. Perbandingan kecepatan membaca log menggunakan ELK Stack dan Splunk

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah membandingkan kecepatan ELK Stack dan Splunk dalam membaca log asterisk dan mempermudah administrator memilih metode sesuai dengan kebutuhan.

1.5 Sistematika Penulisan

Bab I Pendahuluan, berisi: latar belakang, rumusan masalah dan hipotesis, 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 mengexplorasi obyek penelitian, hasil observasi / pengumpulan data, masalah yang terdapat pada obyek, dan gambaran umum proyek atau obyek 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.