1. PENDAHULUAN

1.1 Latar Belakang

Pada masa yang modern ini, teknologi dan internet semakin berkembang dengan pesat. Internet mulai meluas ke seluruh dunia dan digunakan oleh banyak orang mulai dari anak – anak hingga orang dewasa. Selain digunakan secara individu, internet juga sudah digunakan oleh banyak perusahaan, perbankan, bahkan institusi sebagai sarana untuk membantu kelancaran administrasi, memudahkan komunikasi, mempermudah penyebaran informasi, pendidikan dan budaya, serta hiburan.

Namun dengan luasnya jaringan internet, semakin banyak juga oknum – oknum yang ingin mendapatkan keuntungan sendiri dengan melakukan kejahatan melalui internet, contohnya *hacking*. *Hacking* merupakan sebuah aktivitas yang dilakukan dengan tujuan untuk membobol suatu sistem demi mendapatkan hak akses atau data penting dari target yang di bobol. Aktivitas *hacking* tersebut dapat dicegah dengan adanya *firewall*. *Firewall* akan menghasilkan sebuah *log* yang berisikan informasi dari aktivitas yang ada pada sebuah jaringan. Namun hasil *log* tersebut hanya berupa *text* saja sehingga sulit untuk dipantau.

Untuk mengatasi permasalahan diatas, dalam skripsi ini akan diimplementasikan penggunaan *tools* Grafana yang merupakan sebuah analisis *multi-platform* bersifat *open source* dan aplikasi web visualisasi yang bersifat interaktif. Grafana mempermudah pengguna dalam mengumpulkan data log dan menampilkannya kedalam bentuk grafik. Grafana juga memungkinkan pengguna dalam mengatur sebuah peringatan dan mengirimkan notifikasi melalui email, sms, serta berbagai macam aplikasi notifikasi lainnya. Grafana memiliki fitur *plugin* yang memudahkan pengguna untuk menghubungkan aplikasi eksternal ke Grafana. Pada skripsi ini akan digunakan *data source* Grafana Loki yang berguna untuk mengelolah hasil *log* dengan mudah dan juga agen Promtail yang berguna untuk mengirimkan hasil *log* dari *firewall* ke Grafana Loki.

Terdapat penelitian yang berjudul Monitoring Server dengan Prometheus dan Grafana serta Notifikasi Telegram yang dilakukan oleh (Rahman, Amnur, dan Rahmayuni, 2020). Penelitian ini membahas tentang penerapan realtime monitoring system dengan menggunakan aplikasi Prometheus dan Grafana yang diangkat dari masalah ketidakefisienan pada monitoring jaringan dimana administrator diharuskan untuk terus berada di depan layar. Penelitian lainnya yang membahas mengenai implementasi Security Information and Event Management yang dilakukan oleh (Kamal, 2022). Pada penelitian ini penulis bermaksud untuk mengolah *threat log* yang dihasilkan *firewall* milik BSI UII untuk membantu analisis tren ancaman serangan siber. Hal tersebut dilakukan karena ada permasalahan pada situs web UII, yaitu ditemukannya celah keamanan pada

salah satu situs web dan digunakan oleh orang yang tidak bertanggung jawab untuk menyerang web lain di luar UII. Pada penelitian ini penulis melakukan pengumpulan data sekunder yang diperoleh dari pencatatan *log firewall* pada Badan Sistem Informasi Universitas Islam Indonesia.

Dari permasalahan yang sudah dijelaskan dan penelitian – penelitian yang sudah dilakukan sebelumnya, akan diimplementasikan *tools* Grafana. Grafana akan digunakan untuk mengelolah hasil *log* dari *firewall* yang dimiliki UK Petra, kemudian akan di visualisasikan kedalam bentuk grafik. Selain itu, fitur lainnya yang akan dimanfaatkan adalah *data source* Grafana Loki untuk melabelkan hasil *log*, agen Promtail untuk mengirimkan hasil *log* menuju Grafana Loki, dan juga *alerting* yang akan digunakan untuk membuat, mengelola, serta mendiamkan semua peringatan dari *log* yang telah dikumpulkan. *Log* yang berasal dari *firewall* akan disimpan pada *server* dan di *rotating* agar tidak memenuhi kapasitas penyimpanan. Kemudian *log* akan di *push* oleh agen promtail melalui *configuration* agar dapat dibaca oleh *data source* loki.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang ada, dapat dirumuskan permasalahan sebagai berikut:

1. Apakah *tools* Grafana yang digunakan dapat membantu tim keamanan siber dalam memvisualisasikan data *log firewall* Sangfor NGAF ?
2. Apakah tools Grafana dapat memberikan notifikasi peringatan secara lengkap, cepat, dan tepat ?

1.3 Tujuan Skripsi

Skripsi ini bertujuan untuk mengimplementasikan tools Grafana yang berguna untuk mengolah *data log firewall* Sangfor NGAF yang dimiliki oleh UK Petra, kemudian divisualisasikan ke dalam bentuk grafik seperti *time series*, *stat*, *table*, *donut chart*, *bar chart, logs panel, dan alert list* ke dalam satu halaman untuk keperluan *monitoring* serta agar lebih efisien dalam pemantauan. Selain itu, dimanfaatkannya juga fitur *alerting* pada Grafana yang berguna untuk mengirimkan notifikasi peringatan melalui aplikasi peringatan seperti email. Hasil *dashboard* yang dibuat pada Grafana akan dibandingkan dengan *dashboard* pada SOC *NGAF Sangfor Firewall*.

1.4 Ruang Lingkup

Ruang lingkup dibatasi pada:

1. Instalasi *tools* menggunakan *Operating System* Ubuntu
2. Tools akan diinstall pada *server virtual machine* UK Petra
3. Sumber data dari *log firewall* Sangfor NGAF

4. Menggunakan *data source* Loki untuk mengelola dan menampilkan *log* di Grafana
5. Menggunakan Promtail sebagai agen untuk memproses data *log* ke Loki
6. Visualisasi pada Grafana berupa *time series*, *stat*, *table*, *donut chart*, *bar chart, logs panel, dan juga alert list*
7. Visualisasi dibuat untuk *log* IPS dan WAF
8. Memanfaatkan fitur *alerting*
9. Melakukan pengujian *tools* oleh tim keamanan siber UK Petra

1.5 Metodologi Penelitian

Langkah – langkah dalam pengerjaan skripsi:

1. Studi Literatur
   1.1 Studi literatur mengenai Ubuntu
   1.2 Studi literatur mengenai *firewall* Sangfor NGAF
   1.3 Studi literatur mengenai syslog
   1.4 Studi literatur mengenai Grafana
   1.5 Studi literatur mengenai Loki
   1.6 Studi literatur mengenai Promtail
2. Wawancara
   2.1 Melakukan wawancara terhadap mitra
3. Implementasi
   3.1 Implementasi *tools* Promtail
   3.2 Implementasi *tools* Loki
   3.3 Implementasi *tools* Grafana
4. Pengujian dan Analisis
   4.1 Uji coba hasil visualisasi dan *alerting* pada Grafana
5. Kesimpulan
   5.1 Membuat laporan dari hasil pengujian dan analisis

1.6 Manfaat Penelitian

Manfaat yang didapat dari penelitian ini adalah membantu Universitas Kristen Petra dalam mengelola serta memvisualisasikan hasil *log* yang berasal dari *firewall* Sangfor NGAF yang dimiliki UK Petra kedalam bentuk grafik dan juga memanfaatkan fitur *alerting* agar dapat memberikan notifikasi peringatan melalui email.

1.7 Sistematika Penulisan

Bab 1: Pendahuluan

Bab ini berisi judul, latar belakang, perumusan masalah, tujuan skripsi, ruang lingkup, metodologi penelitian, manfaat penelitian, dan sistematika penulisan.

Bab 2: Landasan Teori

Bab ini berisi tinjauan pustaka dan tinjauan studi yang menunjang dalam implementasi sistem

Bab 3: Analisis dan Desain Sistem

Bab ini berisi analisa permasalahan, analisa kebutuhan, desain *flowchart*, dan juga tampilan sistem yang akan diimplementasikan.

Bab 4: Implementasi Sistem

Bab ini berisi implementasi sistem yang akan dilakukan.

Bab 5: Hasil dan Pembahasan

Bab ini berisi penjelasan dari hasil pengujian sistem yang telah diimplementasikan.

Bab 6: Kesimpulan dan Saran

Bab ini berisi kesimpulan terhadap sistem yang telah diimplementasikan berdasarkan hasil pengujian yang dilakukan dan juga berisi saran yang berguna untuk pengembangan sistem selanjutnya.