BAB IV
ANALISA DAN PERANCANGAN

Bab ini berisi tentang analisa kebutuhan yang akan digunakana mulai dari *software* hingga analisa kebutuhan *hardware* serta bab ini juga akan berisi tentang rancangan sistem yang akan digunakan dan juga rancangan pengujian untuk mengetahui seberapa efektif dan efisien nantinya sistem ini digunakan dalam penelitian.

4.1 Analisis Kebutuhan

Pada tahapan ini, peneliti akan melakukan analisa terhadap kebutuhan yang akan digunakan dalam penelitian mengenai Perancangan dan Implementasi Dashboard Monitoring dan Analisa Serangan Aplikasi Web Menggunakan ELK Stack, dari analisa ini nantinya akan dibagi menjadi 2 yaitu analisis kebutuhan terhadap *software* dan analisis kebutuhan terhadap *hardware*.

4.1.1 Analisis Kebutuhan *Software*

Dari analisis ini peneliti mendapatakan beberapa *software* yang akan digunakan dalam penelitian diantaranya sebagai berikut ;

Tabel 4. 1 Detail *Software*

Perangakat Lunak	Versi	Deskripsi
Snort	3.1.18	Perangkat yang bertugas sebagai IDS pada aplikasi web pada penelitian ini
Java	11.0.17	Perangkat yang bertugas untuk menjalankan aplikasi berbasis Java
Elasticsearch	7.14.2	Perangakat yang bertugas sebagai mesin pencarian data dan analisa data secara real time
Kibana	7.14.2	Perangkat yang bertugas untuk memvisualisasikan data yang tersimpan pada elasticsearch

Perangakat Lunak	Versi	Deskripsi
Logstash	7.14.2	Perangkat yang bertugas sebagai sistem pengolahan data dalam skala besar

4.1.2 Analisis Kebutuhan *Hardware*

Berdasarkan analisa terbahadap *software* dan infrastruktur yang akan digunakan maka perlu adanya pengoptimalan terhadap *hardware* atau mesin yang akan digunakan sebagai penunjang kebutuhan dari *software* dan infrastruktur. Penggunaan *hardware* nantinya akan dibangun pada lingkungan virtualisasi, yaitu cloud. Penggunaan *hardware* ini nantinya akan disesuikan dengan minimum requirenment dari ELK Stack yang didapatkan dari official aktivitas ELK Stack dan Snort. Berikut minimum requirenmentnya :

1. Processor : 2 Core
2. Memory : 8 GIB
3. Storage : SSD Storage

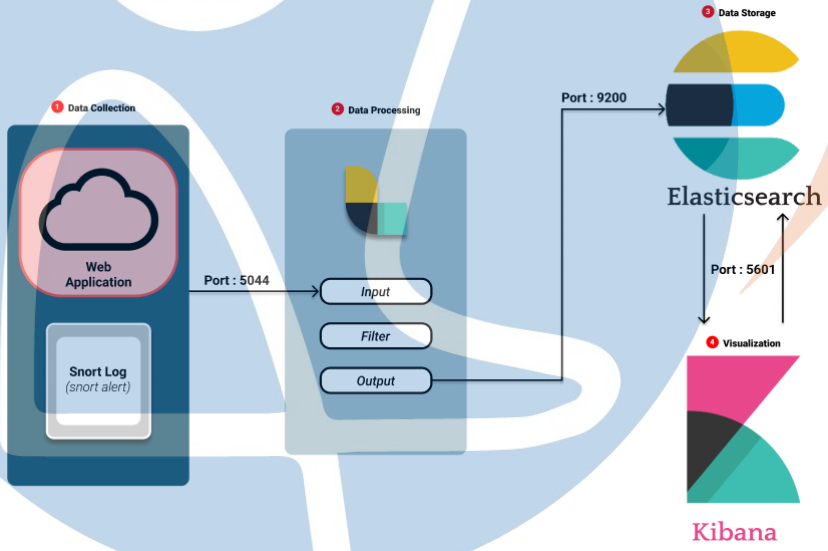
Dalam penelitian ini, penulis akan menggunakan perangkat yang dipasangkan dalam lingkup virtualisasi (cloud) dengan spesifikasi yang sudah dioptimalkan dari standar minimum yang diberikan oleh ELK Stack, berikut spesifikasi dari server yang digunakan :

Tabel 4. 2 Server Snort & ELK stack

No	Size	Spesifikasi			OS	Jumlah
1	Standard D2s v3	vCPUs	vRAM	Storage	Ubuntu 20.04	1
		2 Core	8 GIB	SSD 30 GIB		

4.2 Rancangan Sistem

Tahapan ini bertujuan untuk memberikan penjelasan umum terkait sistem yang akan dibuat dan diusulkan. Tahapan ini, penulis akan melakukan perancangan arsitektur sistem yang memiliki sistem operasi ubuntu 20.04 dan didalamnya akan terdapat snort dan ELK Stack. Tahapan ini akan membantu proses pengembangan sistem terutama pada komponen sistem yang akan dibangun dan harapannya perancangan sistem ini dapat membantu pengembangan sistem kedepannya. Penulis akan melampirkan diagram untuk memudahkan dalam pemahami system Dashboard monitoring Snort dengan ELK Stack;



Gambar 4. 1 Perancangan sistem dashboard monitoring Snort & ELK Stack

Penjelasan dashboard monitoring ELK Stack :

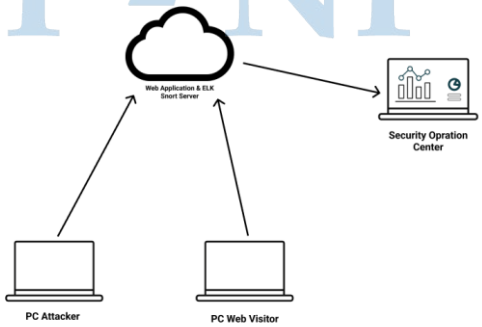
- Snort akan dijadikan sebagai perangkat IDS yang melakukan scanning pada *address* dari aplikasi web
- Logstash akan melakukan penerimaan log yang sudah didapat kan oleh snort apabila terejadinya suatu anomaly atau serangan melalui port yang sudah ditentukan yaitu 5044
- Elasticsearch akan menerima data log dari logstash melalui port 9200 untuk berkomunikasi dan menyimpan data log tersebut, selanjutnya kibana akan

memvisualisasikan semua data yang sudah tersimpan pada elasticsearch dalam bentuk dashboard monitoring.

Perancangan sistem dibuat untuk memperjelas cara dan metode pengumpulan data log snort yang dijadikan data untuk visualisasi oleh ELK Stack. Kemudian dilakukan pengukuran efektivitas sebagai log analisa dalam proses pengimplementasian ELK Stack sebagai dasbord monitoring.

4.3 Perancangan sistem fisik

Tahapan ini merupakan gambaran dari keseluruhan mengenai proses analisa secara fisik. Nantinya dalam skenario sebuah serangan akan melakukan percobaan serangan terhadap aplikasi web yang sudah dipasang. Pada server apikasi web tersebut sudah dipasangan snort dengan jenis *hostbase IDS* yang artinya snort ini akan melakukan pendeteksian secara menyeluruh dari server aplikasi web terhadap lalu lintas jaringannya. Kemudian, saat terjadi pecobaan serangan terhadap wesbite tersebut snort ini akan merekam aktifitas yang masuk sesuai dengan rule yang digunakan. Saat serangan dan proses pendeteksian terjadi penggunalain aplikasi web yang bukan merupakan seorang penyerang, masih tetap bisa menggunakan wesbite tesebut. Selanjutnya data serangan yang sudah terdeteksi akan dikirimkan kedalam server dari ELK, untuk server ini nantinya jaringannya akan dibuat private atau khusus dengan metode penyesuaian firewall dengan menggunakan atau mengganti port yang akan digunakan oleh kibana.



Gambar 4. 2 perancangan sistem fisik

4.4 Rancangan Visualisasi

Pada tahapan ini, peneliti akan melakukan visulisasi dengan menggunakan data log serangan aplikasi web dan dijadikan sebagai sebuah dashboard monitoring. Dashboard tersebut nantinya akan digunakan sebagai visualisasi data serangan jaringan agar dapat dianalisa dengan mudah karena data log yang sebelumnya masih berupa susunan kata dari file log diubah kedalam bentuk diagram grafik dan char yang keduanya didapatkan dari log serangan yang dikirimkan kedalam logstash lalu dilakukan indeksing oleh elasticsearch yang akan menghasilkan JSON lalu dari JSON diubah kembali menjadi bentuk diagram grafik dan chart. Berikut diagram - diagram yang akan digunakan adalah sebagai berikut :

Tabel 4. 3 Rancangan Visualisasi

No	Nama Visualisasi	Jenis Visualisasi	Informasi	Sumber
1	*Total of Attacks*	*Gauge*	Statistik seluruh percobaan serangan yang terjadi pada aplikasi web	- count
2	*Variety of Attacks*	*Pie Chart*	Statistik jenis - jenis serangan terhadap aplikasi web	- msg.keyword
3	*City of Attacker*	*Horizontal Bar*	Statistik data lokasi kota penyerang	- geoip.city_name. keyword
4	*Country of Attacker*	*Donuts*	Statistik data lokasi provisi penyerang	- geoip.country_ name.keyword

No	Nama Visualisasi	Jenis Visualisasi	Informasi	Sumber
5	*Top Attack*	*Tag Cloud*	Statistik data lokasi negara penyerang	- msg.keyword
6	*Source IP of Attacker*	*Table*	Statistik data IP penyerang	- src.addr. keyword
7	*Filter*	*Filter Options*	Filter data serangan pada dashboard	- Fitur Kibana

4.5 Rancangan Pengujian

Pada tahapan ini, penulis akan melakukan perancangan uji coba untuk digunakan dalam melakukan pengujian terhadap sistem dashboard monitoring yang dibuat. Pada tahapan ini penulis akan menggunakan metode pengujian Black box Testing. Dengan metode pengujian ini penulis akan melakukan pengujian terhadap fungsionalitas dari sistem yang dibuat agar dapat mengetahui kesesuaian dari rancangan sistem yang dibuat . berikut skenario pengujian pada alat pendetksian dan sistem dashboard monitong ini :

4.5.1 Pengujian Efektitifas

Tahapan ini dilakukan untuk menyimpulkan dan menjawab pertanyaan dari rumusan masalah, apakah efektif dashboard monitoring serangan aplikasi web menggunakan ELK Stack atau setidaknya sistem ini bekerja dengan tepat. Tahapan pengujian dilakukan dengan tepat mengenai analisa log bermacam serangan yang dihasilkan dari snort lalu dikirimkan kedalam ELK Stack untuk dijadikan dashboard monitoring. Untuk mengetahui berapa nilai efektifitas dari dashboard yang dibuat maka perlu dilakukan perhitungan dari jumlah serangan yang dilakukan dan yang dideteksi serta dari jumlah serangan dan log yang diterima

Efektifitas = (jumlah serangan ÷ jumlah log yang diterima / jumlah yang dideteksi) x 100%

Rata rata efektifitas = (Efektifitas ÷ jumlah pengujian)

Nantinya hasil dari ini yaitu rata rata efektifitas akan dijadikan kesimpulan apakah sistem yang dibangun sudah efektif atau belum cukup efektif

4.5.2 Pengujian pendeteksian serangan *SQL Injection*

Berikut adalah contoh table pengujian *SQL Injection*

Tabel 4. 4 pengujian pendeteksian serangan *SQL Injection*

Pengujian Ke	Jumlah Serangan	Jumlah log yang diterima

4.5.3 Pengujian pendeteksian serangan *Cross Site Scripting*

Berikut adalah contoh table pengujian *Cross Site Scripting*

Tabel 4. 5 pengujian pendeteksian serangan *Cross Site Scripting*

Pengujian Ke	Jumlah Serangan	Jumlah log yang diterima

4.5.4 Pengujan pendeteksian serangan DDoS Attack

Berikut adalah contoh table pengujian DDoS Attack

Tabel 4. 6 pengujian pendeteksian serangan DDoS Attack

Pengujian Ke	Jumlah Serangan	Jumlah log yang diterima

Pengujian Ke	Jumlah Serangan	Jumlah log yang diterima

4.5.5 Pengujian pengiriman log snort kedalam ELK Stack

Pengujian ini yaitu menyangkut pengujian yang dilakukan dengan mengirim log yang sudah diterima snort dari hasil melakukan pendeteksian serangan ke dalam ELK stack. Pengiriman log snort kedalam ELK Stack hingga dapat divisualisasikan akan memerlukan beberapa tahap yaitu, memastikan file log dari snort sudah bekerja dengan baik dengan dapat menyimpan log dari serangan, selanjutnya menyiapkan konfigurasi dari logstash dimana nantinya diletakan *path location file* dari snort log, dan yang terakhir yaitu memastikan log tersebut sudah dapat tergenerate oleh elasticsearch menjadi index dikibana.

4.5.8 Rancangan Pengujian Hasil Visualisasi Kibana

Tahapan ini merupakan hasil visualisasi dari penelitian ini yaitu hasil dari log serangan jaringan yang diterima oleh snort yang sudah dianalisa melalui elasticsearch. Kemudian kibana akan menampilkan visualisasi dengan data yang sudah diterima oleh elasticsearch dan memastikan apakah data yang diterima sudah benar sesuai dengan data yang ada pada log snort dan sudah analisa pada elasticsearch

Tabel 4. 7 Rancangan Uji Visualisasi

No	Nama Visualisasi	Jenis Visualisasi	Hasil Uji	Presentase
1	*Total of Attacks*	*Gauge*	Berhasil Tergambarkan	100 %
2	*Variety of Attacks*	*Pie Chart*		

No	Nama Visualisasi	Jenis Visualisasi	Hasil Uji	Presentase
3	*City of Attacker*	*Table*		
4	*Country of Attacker*	*Table*		
5	*Top Attack*	*Vertical Bar*		
6	*Source IP of Attacker*	*Table*		
7	*Filter*	*Filter Options*		

4.5.8.1 Rancangan Uji Efektifitas Visualisasi

Pada tahapan ini akan dilakukan pengujian terhadap penggunaan apakah dashboard monitoring ini sudah efektif untuk dijadikan sebagai sebuah sistem pemantauan suatu serangan jaringan. Pengujian dilakukan dengan melibatkan beberapa orang yang bekerja dalam bidang khususnya IT dalam mengoprasikan dashboard monitoring ini dengan menggunakan beberapa skenario pengujian untuk dapat mengetahui tingkat penggunaan dan pemahaman dalam penggunaan dashboard monitoring ini. Berikut skenario uji efektivitas penggunaan pada yang akan dilakukan:

Tabel 4. 8 Rancangan Uji Efektivitas Penggunaan

No	Skenario Uji Efektivitas Penggunaan	SS	S	M	SM
1	Membuka halaman dashboard monitoring				
2	Menampilkan visualisasi data dari hasil serangan				
3	Melakukan filter serangan berdasarkan waktu				

No	Skenario Uji Efektivitas Penggunaan	SS	S	M	SM
4	Melakukan filter serangan berdasarkan nama serangan				

Keterangan :

SS : Sangat Sulit
S : Sulit
M : Mudah
SM : Sangat Mudah

Setelah itu akan diberikan sebuah skenario uji efektivitas kelayakan dashboard kepada user yang telah melakukan percobaan dashboard monitoring ini untuk mengetahui tingkat dari kelayakan dan efektivitas dari dashboard monitoring serangan jaringan ini

Tabel 4. 9 Rancangan Uji Efektivitas Kelayakan

No	Skenario Uji efektivitas Kelayakan	STS	TS	S	SS
1	Tampilan dashboard yang disajikan untuk sebuah aktivitas monitoring nyaman untuk digunakan				
2	Diagram - diagram pada dashboard tersebut masuk akal dan sudah tepat digunakan				
3	Fitur filter pada dashboard membantu proses penyaringan data serangan				
4	Mudah untuk menyimpulkan serangan yang terjadi				

Keterangan :

STS : Sangat Tidak Setuju
TS : Tidak Setuju
S : Setuju
SS : Sangat Setuju