BAB I
PENDAHULUAN

1.1 Latar belakang

Aplikasi web merupakan sebuah sistem yang saat ini sangat berperan penting digunakan manusia. Aplikasi web dapat membantu mobilitas dari manusia itu sendiri seperti belajar yang tidak harus di sekolah, berbelanja tidak harus ke pusat perbelanjaan, hingga menjelajahi dunia tanpa membutuhkan waktu yang lama.

Namun, apabila aplikasi web ini dapat diakses melalui internet maka besar kemungkinan terjadinya suatu serangan akan meningkat dikarenakan siapa saja diseluruh dunia yang terhubung internet bisa mengakses aplikasi itu sendiri. Oleh karena itu, aplikasi web sangat penting untuk dilakukan pemantauan atau *monitoring* terhadap sistem keamanan jaringannya agar apabila terjadi suatu serangan yang dilakukan oleh seseorang dapat terdeteksi dan segera dilakukan penanganan terkait keamanan aplikasi web itu sendiri.

Selain itu, visualisasi dan analisa dari data serangan juga menjadi suatu hal yang penting, agar pemilik dari aplikasi web dapat mengetahui bahwa aplikasinya memiliki kerentanan dan jenis serangan apa saja yang digunakan untuk menyerang aplikasinya agar dikemudian hari pemilik dari aplikasi web dapat meningkatkan keamanan aplikasi untuk menghindari terjadinya serangan yang secara berulang kali.

Untuk melakukan sebuah pendeteksian terhadap aktivitas yang mencurigakan dan serangan dalam jaringan nantinya penulis akan menggunakan *tools* IPS/IDS, alat ini merupakan teknologi yang digunakan dalam melakukan pecegahan dan merekam aktivitas dari suatu lalu lintas jaringan, contoh aplikasi ini yaitu snort, suricata, OSSEC, Cisco Firepower dan masih banyak lagi. Untuk penelitian kali ini peneliti akan menggunakan salah satunya itu snort. Snort adalah sebuah *tools* untuk mendeteksi sesuatu yang mencurigakan dalam jaringan [1]. Namun, *tools* ini hanya menampilkan log atau data mentah dari

sebuah serangan oleh karena itu diperlukan sebuah *tools* untuk melakukan pengolahan data sehingga data tersebut dapat divisualisasikan dan dianalisa.

Terdapat beberapa sistem untuk melakukan visualisasi dan pengolahan data, diantaranya ELK Stack, Grafana ,dan Prometheus. Disini penulis akan menggunakan ELK Stack, ini merupakan sebuah sistem dimana didalamnya terdapat Logstash yang akan untuk mengelola aktivitas dari sebuah log, Elasticsearch akan menjadi mesin pencari dari sebuah data log yang tertampung dalam Logstash, dan Kibana sebagai dashboard untuk memvisualisasikan data dari Elasticsearch [2]. Nantinya data yang sudah terdeteksi menggunakan *tools* Snort atau *Suricata* akan dipakai dalam ELK Stack.

Karena pentingnya sebuah alat pendeteksi dan sistem dashboard untuk melakukan sebuah visualisasi serta analisa serangan aplikasi web. Maka dari itu penulis akan melakukan penelitian serta perancangan dashboard monitoring untuk melakukan pendeteksian terhadap serangan aplikasi web. Dengan adanya penelitian ini nantinya diharapkan pendeteksian, visualisasi serta analisa terhadap serangan aplikasi web akan menjadi lebih mudah dan membantu pengembang aplikasi web untuk menjadikan aplikasinya menjadi lebih aman digunakan dan mudah diatasi saat terjadinya suatu serangan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan penulis, maka rumusan masalah pada tugas akhir ini adalah :

1. Bagaimana rancangan dashboard monitoring menggunakan ELK Stack ?
2. Bagaimana efektifitas dari rancangan dashboard monitoring aplikasi web menggunakan ELK Stack ?

1.3 Tujuan dan Manfaat Penelitian

Tujuan penelitian ini antara lain yaitu :

1. Melakukan perancangan sistem monitoring dan sistem dashboard untuk pendeteksian serangan aplikasi web

2. Mengetahui efektifitas dari rancangan sistem *monitoring* dan sistem dashboard dalam hal melakukan pendeteksian serangan aplikasi web

Manfaat penelitian ini antara lain yaitu :

1. Untuk memudahkan proses *monitoring* terhadap serangan jaringan aplikasi web
2. Untuk membantu pengembang aplikasi web dalam mengingkatkan keamanan terhadap aplikasinya
3. Untuk dijadikan sebuah rujukan pihak lain apabila nantinya ada penelitian yang terkait

1.4 Batasan Masalah

Batasan masalah penelitian ini antara lain yaitu :

1. Pendeteksian ini tidak memperdulikan apakah serangan tersebut berhasil atau tidak
2. Pendeteksian ini hanya akan melakukan pendeteksian pada pola 4 serangan yang dapat terjadi pada Aplikasi web diantanyan yaitu, *SQL Injection*, *Cross Site Scripting* (XSS), dan Ddos Attack.
3. Pendeteksian hanya melakukan pendeteksian serangan pada *website* simulasi atau bukan *website* production.
4. Penelitian ini tidak akan menjelaskan terkait dengan cara melakukan serangan ke aplikasi web dan tidak juga menjelaskan terkait tools yang digunakan untuk melakukan serangan aplikasi web.

1.5 Sistematika Penulisan

Tugas akhir ini ditulis menggunakan sistematika sebagai berikut :

1. BAB I PENDAHULUAN, Bab ini akan memberikan gambaran terkait penelitian, yang terdiri dari latar belakang, perumusan dari masalah penelitian, tujuan dan manfaat, batasan masalah, serta sistematika penulisan penelitian.

2. BAB II KAJIAN LITERATUR, Bab ini memberi penjelasan secara detail terkait teori dan literatur yang digunakan dalam penelitian
3. BAB III METODOLOGI PENELITIAN, Bab ini memberi penjelasan terkait tahapan – tahapan dalam penelitian, mulai penelitian yang sudah dilakukan hingga yang akan dilakukan.
4. BAB IV ANALISA DAN RANCANGAN, bab ini memberikan penjelasan terkait analisa dan perancangan sistem dashboard mitoring terhadap serangan jaringan aplikasi web
5. BAB V IMPLEMENTASI DAN PENGUJIAN, bab ini memberikan penjelasan terkait dari hasil implementasi dan pengujian dari sistem yang telah dibuat
6. BAB VI KESIMPULAN DAN SARAN, bab ini memberikan penjelasan terkait dari kesimpulan dari penelitian dan saran bagi penulis untuk dijadikan