**BAB I**

**PENDAHULUAN**

**1.1 Latar Belakang**

Penggunaan aplikasi web semakin bertambah seiring dengan kebutuhan akan keamanan pada web setiap tahunnya. Berdasarkan data pada situs IMPERVA jumlah kerentanan yang ada pada aplikasi web pada bulan Januari tahun 2017

adalah sebagai berikut.

**Tabel 1.1 Data Jumlah Kerentanan Aplikasi Web**

|  |  |  |
| --- | --- | --- |
| Bulan | Tahun | Total Jumlah Kerentanan Aplikasi Web |
| Januari | 2016 | 596 |
| 2017 | 922 |

**Sumber** : https://imperva.com

Pada tabel 1.1 pertumbuhan jumlah kerentanan pada bulan Januari tahun 2017 meningkat sebesar 55% dari tahun 2016 sehingga hal tersebut menjadi informasi

yang perlu diperhatikan setiap tahun nya.

Banyaknya kerentanan pada aplikasi web seringkali menjadi sumber kesulitan untuk mengidentifikasikan jenis dari kerentanan tersebut, belum lagi setiap kerentanan memiliki pola, jenis, dan tingkat ancaman yang berbeda, salah satu contoh jenis kerentanan adalah *Insufficient logging and monitoring* yaitu kurangnya upaya dalam melakukan pengawasan, pengelolaan *log* keamanan, dan

respon tepat waktu untuk mendeteksi insiden serangan atau pelanggaran.

Dengan besarnya jumlah kerentanan pada aplikasi web, maka diperlukan peningkatan pada sistem keamanan yang memerlukan suatu teknologi untuk

1

mengumpulkan, mengirimkan dan menyimpan data log dari berbagai perangkat secara terpusat, lalu membuat sebuah manajemen dan pendeteksian kerentanan

berdasarkan jenis kerentanan dari setiap insiden serangan pada aplikasi web.

*Security Information and Event Management* (**SIEM**) adalah sebuah sistem yang mampu memanajemen keamanan pada dunia IT secara menyeluruh, dengan tujuan untuk memberikan analisis secara *realtime* melalui peringatan keamanan yang dihasilkan oleh perangkat keras dan aplikasi jaringan. Terdapat banyak jenis aplikasi **SIEM** yang tersedia.

Pada penelitian ini menggunakan *software Elastic Stack* untuk mengimplementasikan **SIEM. SIEM** juga memerlukan komponen pendukung untuk dapat digunakan dengan maximal salah satu *software* pendukung yaitu **Zeek**. **Zeek** dipilih sebagai *software* dalam pengerjaan penelitian ini, karena tools tersebut bersifat open source, bebas biaya dan juga dokumentasi lengkap yang tersedia di internet. Oleh karena itu peneliti mencoba menggabungkan beberapa sistem dan *software* yang sudah ada saat ini untuk membantu pemilik sebuah situs web untuk memanajemen dan mendeteksi insiden serangan pada situs web.

**SIEM** yang dirancang bertujuan untuk memberikan informasi mengenai respon insiden dan peringatan kepada pemilik situs web tentang jenis-jenis insiden serangan yang sedang terjadi berdasarkan kategori kerentanan yang telah dimuat oleh *The Open Web Application Security Project (****OWASP****) TOP 10 2017*.

Penelitian ini bertujuan untuk mengetahui bagaimana cara mengimplementasikan *Security Information and Event Management* (**SIEM**) menggunakan *software Elastic, Logstash, Kibana* dan **ZEEK** sebagai sistem yang dapat memanajemen

dan mendeteksi jenis-jenis insiden serangan pada situs web.

**1.2 Rumusan Masalah**

Bagaimana mengimplementasikan *Security Information and Event Management (***SIEM***)* menggunakan *Elastic Stack* untuk memanajemen dan

mendeteksi insiden serangan pada aplikasi web?

**1.3 Tujuan Penelitian**

Tujuan dari penelitian ini adalah untuk mengimplementasikan *Security Information and Event Management (***SIEM***)* yang mampu memanajemen dan mendeteksi insiden serangan pada aplikasi web. Serta memaksimalkan *Security Information and Event Management (***SIEM***)* agar dapat digunakan untuk mengidentifikasi setiap insiden serangan berdasarkan kategori atau jenis kerentanan yang mengacu pada *OWASP TOP 10 2017*, dan dapat digunakan

secara fleksibel baik dalam cakupan *personal* maupun instansi.

**1.4 Batasan Masalah**

1. Penelitian ini berfokus pada hasil notifikasi serangan pada aplikasi web*,* dan menggunakan simulasi web sebagai target penyerangan*.*
2. Penelitian ini menggunakan server dan sistem operasi Linux untuk

mengimplementasikan *Security Information and Event Management (SIEM).*

1. Penelitian ini mendeteksi insiden pada aplikasi web yg berjalan pada sistem operasi Linux.
2. Penelitian ini menggunakan metode *Signature Based Detection* untuk

mendeteksi insiden serangan.

**1.5 Manfaat Penelitian**

Manfaat dari Perancangan *Security Information And Event Management* pada

situs Web yang akan dibuat adalah sebagai berikut:

* + 1. **Manfaat Bagi Ilmu Pengetahuan**

Menghasilkan teknik keamanan dalam mendeteksi insiden serangan pada situs web yang berguna untuk mencegah dan memberikan peringatan apakah sebuah data yang melewati suatu situs web tergolong sebagai serangan atau tidak . Sistem ini juga akan memanajemen, *monitoring*, serta mengirim *Log* tentang aktivitas *traffic* yang terjadi pada suatu situs web kepada *System Administrator* secara *real time*.

* + 1. **Manfaat Bagi Instansi dan Perusahaan**

Dengan adanya sistem ini membuat perusahaan atau instansi diluar sana dapat memonitoring keamanan *website* mereka secara *real-time.* Hal ini karena sistem tidak mengharuskan *System Administrator* untuk selalu memantau keadaan *website* setiap saat, bahkan jika memang sedang tidak dipantau sistem juga dapat memberikan informasi tentang insiden serangan yang dilakukan oleh *Attacker* kepada *System Administrator* sehingga perusahaan atau instansi bisa langsung mengambil tindakan terhadap serangan tersebut.

* + 1. **Manfaat Bagi Masyarakat Umum**

Sistem ini memberikan dan menyampaikan informasi dan memberikan peringatan tentang sebuah data yang melewati suatu situs web dengan mengklasifikasikan dan mendeteksi data tersebut sebagai insiden serangan dengan tipe kerentanan yang telah dimuat di *The Open Web Application Security Project (****OWASP****) Top 10 2017* pada aplikasi situs *web*. sistem ini juga dapat dijadikan media pembelajaran, agar supaya masyarakat lebih paham dan mengerti, bagaimana cara menjaga keamanan pada suatu situs web yang dimiliki, agar

serangan yang dilakukan oleh penyerang dapat diatasi dengan baik dan benar.

**1.6 Metodologi Penelitian**

* + 1. **Tempat Dan Waktu Penelitian**

Lokasi penelitian berada di internet, karena sebagian besar data yang dibutuhkan pada penelitian ini berada di sana. Sedangkan waktu penelitian dilakukan selama enam bulan dengan jadwal seperti yang terlihat pada tabel

berikut:

**Tabel 1.2 Jadwal Penelitian**



* + 1. **Bahan dan Alat Penelitian**

Bahan dan alat pada penelitian ini mencakup *Hardware* dan *Software* antara

lain sebagai berikut:

* *Virtual Private Server(VPS)* : (12GB RAM, 8vCPU, 60 GB Disk, Ubuntu 20.04LTS)
* *Software* : Elastic, Logstash, Kibana, Filebeat, ZEEK, Mozilla Firefox

(Browser)

* Data : Jenis Kerentanan *OWASP TOP 10 2017*
* *Hardware :* MacBook Air (Retina, 13-inch, 2018 , 1,6 GHz Intel Core i5, 8

GB 2133 MHz LPDDR3)

**1.6.3. Pengumpulan Data dan Informasi**

Pada penelitian ini diperlukan beberapa data sebagai bahan. Teknik yang digunakan dalam mengumpulkan data atau informasi yaitu dengan mengunjungi suatu situs web yang menyediakan data-data dan dokumentasi yang dibutuhkan seperti *ZEEK, OWASP* dan *Elastic Stack ( Elastic,logstash & Kibana)*.

**1.6.4. Analisis Data**

Analisis data merupakan suatu cara untuk mengolah data untuk kemudian diproses menjadi informasi. Tujuan tersebut dimaksudkan agar sifat dari data bisa lebih mudah diolah dan dimengerti.

**1.6.5 Prosedur Penelitian**

 Prosedur penelitian yang diambil dalam melaksanakan penelitian ini

tercantum sebagai berikut:

1. Perencanaan

Melakukan pengumpulan data-data dengan mengunjungi beberapa situs yang dibutuhkan dan membahas tentang beberapa perangkat pada penelitian ini seperti situs milik **OWASP**, **ZEEK,** dan **Elastic**.

1. Analisis

Mengkaji beberapa penelitian serupa atau penelitian yang membahas tentang kerentanan suatu situs web terhadap pola serangan yang dimuat di *The Open Web Application Security Project (****OWASP****) TOP 10 2017*.

1. Perancangan

Merancang topologi jaringan, *Flowchart, use case diagram, diagram activity,* dan *sequence diagram* sehingga mampu menghasilkan perancangan *Security Information and Event Management (SIEM)* untuk mendeteksi insiden pada situs web yang dimuat di *The Open Web Application Security Project (****OWASP****) TOP 10 2017* .

1. Implementasi

Mengimplementasikan *Security Information and Event Management (SIEM)* menggunakan *Elastic Stack*, memasang *software Filebeat, dan* **ZEEK** pada *Agent* lalu memasang simulasi aplikasi kerentanan pada web dan membuat manajemen *rule* pada *dashboard* Kibana menggunakan *KQL*.

1. Uji Coba

Pengujian dilakukan untuk mengetahui sistem pendeteksi insiden pada web yang telah dirancang.

**1.6.6 Sistematika Penulisan**

Pada penelitian, sistematika penulisan yang digunakan terbagi dalam 5 bab,

yaitu :

**BAB I Pendahuluan**

Bab ini memaparkan latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, metodologi penelitian dan

sistematika penulisan.

**BAB II Tinjauan Pustaka**

Bab ini menjelaskan tentang konsep-konsep, penelitian sebelumnya, teori-teori yang terkait dan *software* yang mendukung penyelesaian tugas

akhir.

**BAB III Analisa dan Perancangan**

Bab ini berisi tentang uraian masalah, pemecahan masalah, metodologi, desain dan perancangan aplikasi.

**BAB IV Hasil Uji dan Pembahasan**

Bab ini berisi tentang perancangan dan pembahasan aplikasi yang telah dibuat. Proses perancangan yang dilakukan adalah penerapan *Security Information and Event Management (SIEM)* dan dilakukan pengujian.

**BAB V Penutup**

Bab ini memaparkan kesimpulan yang diambil berdasarkan hasil yang

telah dicapai dan saran untuk pengembangan tugas akhir selanjutnya.