BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Berkat teknologi kini informasi, data, surel, maupun berkas dapat diakses melalui server secara jarak jauh. Pada umumnya server dipakai oleh hampir seluruh perusahaan maupun perseorangan untuk memenuhi kebutuhannya dalam penggunaan sehari-hari. *Server* atau peladen adalah seperangkat komputer yang berisi program-program yang mampu menghasilkan informasi dan informasi tersebut didistribusikan kepada komputer *client* yang mengaksesnya [1].

Berkaitan juga dengan *Web Server* untuk memenuhi kebutuhan pengguna yang merupakan sebuah *software* (perangkat lunak) yang memberikan layanan berupa data, berfungsi untuk menerima HTTP atau HTTPS dari *client* atau yang kita kenal *web browser* (*Chrome, Firefox*) yang selanjutnya ia akan mengirimkan respons atas permintaan tersebut kepada *client* dalam bentuk halaman *web* [2].

Rentan keamanan pada *Web Server* semakin tinggi seiring perkembangan zaman agar melindungi para pengguna dari ancaman *cyber.* Dengan dari itu tujuan dari penelitian Tugas Akhir ini bermaksud untuk menganalisis *vulnerability assessment tools* dengan menggunakan ELK *Stack* guna meminimalisir angka serangan *cyber*. Berdasarkan *Honeywet Report* rata-rata tingkat *cyber-attack* di Indonesia sebesar 1.074.630, tahun berikutnya pada tahun 2019 meningkat menjadi 8.317.363 *cyber-attack* per bulan, selanjutnya tahun 2020 kembali meningkat hingga 26.347.313 per bulannya, dan pada tahun 2021 terjadi peningkatan yang sangat signifikan yaitu hingga 103.537.972 *cyber-attack* per bulannya [3].

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat disimpulkan rumusan masalah *vulnerability assessment tools* menggunakan ELK *Stack* pada *log web server* sebagai berikut.

1. Bagaimana cara kerja *vulnerability assessment* menggunakan ELK *Stack*?
2. Bagaimana analisis yang bisa dilakukan pada *vulnerability assessment* yang diterapkan dengan ELK *stack*?

3. Bagaimana hasil analisis *vulnerability assessment* dengan menggunaka ELK *stack* dengan menggunakan implementasi *dataset* serangan DDoS pada *web server*?

1.3 Tujuan dan Manfaat

Berdasarkan latar belakang dan rumusan masalah di atas, maka tujuan dari Tugas Akhir ini ialah.

1. Mengetahui cara kerja *vulnerability assessment* dengan menggunakan ELK stack.
2. Mengetahui proses analisis yang bisa dilakukan pada vulnerability assessment yang diterapkan dengan menggunakan ELK stack.
3. Melakukan analisis *vulnerability assessment* dengan menggunakan ELK *stack* pada *dataset log web server*.
4. Mengetahui hasil analisis pada *dataset* dengan menganalisis pada ELK *stack*.

Berikut manfaat dari Tugas Akhir ini sendiri adalah:

1. Mengurangi adanya human *error* pada sektor keamanan dari *log web server*.
2. Meningkatkan keamanan pada *log web server* dengan menggunakan ELK *stack*.

1.4 Batasan Masalah

Menurut rumusan masalah di atas, maka batasan masalah pada Tugas Akhir ini sebagai berikut:

1. Pengimplementasian ELK *Stack* dilakukan pada *dataset log web server*.
2. Penerapan *vulnerability assessment* menggunakan ELK *Stack*.
3. ELK *Stack* hanya berfokus pada keamanan *dataset log web server.*
4. Dataset yang digunakan adalah data trafik yang ditangkap pada sebuah web server ketika terjadi serangan dan ketika tidak ada serangan.

1.5 Metode Penelitian

Metode penelitian yang digunakan pada Tugas Akhir ini adalah sebagai berikut.

1. Studi Literatur

   Serangkaian aktivitas pengumpulan data pustaka dan materi dari beberapa sumber berupa jurnal, buku, penelitian, dan artikel.

2. Analisis dan Perancangan Sistem

   Merancang sistem yang akan dibuat pada Tugas Akhir ini, dan menganalisis hasil dari rancangan sistemnya.

3. Pengujian dan Evaluasi Sistem

   Menguji hasil dari perancangan sistem yang sudah dibentuk, dan melakukan evaluasi jika terdapat kekurangan dalam perancangan sistem.

4. Penyusunan Laporan Tugas Akhir

   Menyusun laporan Tugas Akhir dari penelitian yang sudah dibuat berdasarkan pengujian dan evaluasi sistem.