BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Di era industri 4.0 ketergantungan dunia terhadap layanan daring semakin tinggi. Dengan demikian kebutuhan akan layanan-layanan berbasis internet semakin meningkat. Seiring dengan kebutuhan, *traffic*, dan layanan yang semakin tinggi, semakin meningkat juga ancaman siber yang terjadi. Ancaman-ancaman tersebut antara lain :

1. Ancaman terhadap penyedia layanan

   Ancaman ini adalah ancaman yang dihadapi dari penyedia layanan ancaman ini dibagi menjadi 2 yaitu :

   - Ancaman pada sisi komputer server : *SQL Injection, Command Injection, Command Execution, File inclusion, server take over*
   - Ancaman pada sisi *internet provider / ISP* : Serangan-serangan *DDOS*, Serangan *smurfing*, *ARP poisoning, BGP attacking*

2. Ancaman terhadap pengguna layanan

   Ancaman yang dimaksud di sini adalah ancaman yang didapat dari pengguna layanan ancaman contoh nya adalah *Client-side hacking, XSS, CSRF injection*, Virus Trojan, dll

3. Social Engineering

Social engineering adalah kegiatan untuk mendapatkan informasi rahasia/penting dengan cara menipu pemilik informasi tersebut. *Social engineering* umumnya dilakukan melalui telepon dan Internet. *Social engineering* merupakan salah satu metode yang digunakan oleh *hacker* untuk memperoleh informasi tentang targetnya,. Contoh nya adalah penipuan-penipuan *XSS*.

CIS Security adalah sebuah metoda yang dikembangkan oleh CIS, yang memiliki misi untuk identifikasi, pengembangan, validasi, promosi, dan mempertahankan solusi terbaik untuk pertahanan *cyber*, membangun mindset masyarakat untuk meningkatkan lingkungan terpercaya di dunia maya. Metode yang dikembangkan adalah model *crowdsourcing* (pelibatan pihak lain dalam pengembangan konten dan sumber daya/source). CIS menerapkan *crowdsourcing* secara tertutup (*closed contribution*).

CIS Security memiliki program pada lingkungan-lingkungan :

CIS Control

CIS Benchmark

CIS Communities

CIS Cybermarket

PT Solusi Kampus Indonesia (eCampuz) adalah sebuah perusahaan yang bergerak dalam bidang teknologi informasi dan komunikasi yang menawarkan pengelolaan manajemen perguruan tinggi yang menyeluruh, terintegrasi dan sesuai dengan regulasi DIKTI. eCampuz menyediakan layanan berupa eCampuz Cloud yaitu layanan *SaaS* bagi perguruan tinggi di Indonesia. Sebuah layanan *SaaS* memerlukan tingkat keamanan yang tinggi. Untuk meningkatkan keamanan sistem dilakukan dengan mengimplementasikan CIS Benchmark.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka dapat dirumuskan pemasalahannya sebagai berikut :

1. Bagaimana cara meminimalisir resiko serangan dan ancaman siber?
2. Bagaimana pemanfaatan CIS Security jika diimplementasikan pada *system auditor.*
3. Bagaimana implementasi *system auditor* menggunakan CIS Benchmark dari CIS Security untuk mengaudit suatu layanan *SaaS*?
4. Bagaimana implementasi *system auditor* menggunakan CIS Benchmark dapat mempermudah evaluasi instalasi suatu layanan *SaaS*?
5. Bagaimana cara merancang sebuah aplikasi *scoring* yang dapat memudahkan proses evaluasi dari *system auditor*?

1.3 Ruang Lingkup

Adapun ruang lingkup yang menjadi acuan dalam pengerjaan penelitian ini sebagai berikut :

1. Menggunakan *Bash script* untuk menjalankan bahasa *bash* atau *shell* yang akan melakukan audit di server.
2. Memberikan keluaran berupa tampilan pada layar sesuai dengan data dari hasil audit berdasarkan CIS Benchmark yang telah dijalankan.
3. Menggunakan *framework* Bootstrap untuk membuat tampilan (*frontend*).
4. Membuat visualisasi berupa *Scoring* audit yang menampilkan data dari hasil audit berdasarkan CIS Benchmark yang telah dijalankan.
5. Menyediakan link download berupa *Scoring* dan paparan data dari hasil audit berdasarkan CIS Benchmark yang telah dijalankan.

Implementasi *Security Auditor* untuk Standardisasi Instalasi Server pada Layanan *SaaS* eCampuz Menggunakan CIS Benchmark dilakukan untuk mendukung *System Adminstrator* dalam:

1. Mengetahuai konfigurasi dari instalasi kita mendapatkan nilai berapa berdasarkan CIS Benchmark
2. Menentukan hal apa saja yang perlu dievaluasi pada suatu instalasi *SaaS* berdasarkan CIS Benchmark.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian tentang Implementasi *Security Auditor* untuk Standardisasi Instalasi Server pada Layanan *SaaS* eCampuz Menggunakan CIS Benchmark sebagai berikut:

1. Mendapatkan data *ceklist* kemanan pada layanan *SaaS* eCampuz sesuai dengan CIS Control menggunakan CIS Benchmark
2. Menigkatkan kemanan pada layanan *SaaS* eCampuz dengan mengimplemtasikan standardisasi CIS Control dari CIS Security
3. Diharapkan dapat mengimplemntasikan ISO 27001 berdasarkan CIS Control pada layanan *SaaS* eCampuz
4. Diharapkan dapat membantu *System Administrator* dalam melakukan evaluasi dari instalasi layanan *SaaS* yang bersifat rutin.

1.5 Manfaat Penelitian

Manfaat Implementasi *Security Auditor* untuk Standardisasi Instalasi Server pada Layanan *SaaS* eCampuz Menggunakan CIS Benchmark sebagai berikut:

1. Memberikan data *ceklist* keamanan pada sistem berdasarkan CIS Benchmark.
2. Meminimalisir adanya konfigurasi yang membawa *vurnability* pada sistem.
3. Membantu meningkatkan keamanan siber pada sistem berdasarkan CIS Benchmark yang sesuai dengan tren dari serangan siber terkini.
4. Membantu melakukan pencatatan dokumentasi instalasi sistem secara tersetruktur dan sistematis sehingga dapat mengurangi *human error*.