

# BAB 1

## PENDAHULUAN

### 1.1 Latar Belakang Masalah

Studi Independen pada PT Gama Multi Usaha yang berada dalam naungan UGM (Universitas Gadjah Mada) Yogyakarta bekerja sama dengan MSIB membuka Studi Independen atau Magang Independen dengan judul "Skill yang dibutuhkan data *protection officer* dalam menjaga keamanan *cloud computing infrastructure*". Dalam studi independen ini, peserta magang diajarkan oleh dosen dari berbagai kampus seluruh Indonesia seputar *cyber security*. Peserta magang dijelaskan materi langsung oleh ketua mentor dari PT Gama Multi Usaha itu sendiri dan dijelaskan tugas mingguan yang harus dikerjakan. Tugas yang diberikan bermacam-macam tiap minggunya, sesuai dengan materi pada minggu itu. Dari tugas itu yang telah diajarkan pada peserta magang, ilmu itu akan digunakan oleh peserta magang untuk melakukan tugas akhir. Tugasnya ada yang diminta menenkripsi dekripsi pesan email, meretas sebuah web, mendekripsikan *password* menggunakan beberapa aplikasi, mencari kerentanan dari sebuah IP dan masih banyak lagi. Perminggu juga ada sesi mentoring. Mentoring ini dilakukan per kelompok. Setiap mentor memegang 23 - 24 mahasiswa - mahasiswi. Sesi *mentoring* ini peserta bisa bertanya ke para dosen yang menekuni bidang *cyber security*. Kelompoknya dibagi per abjad. Perminggu juga ada sesi Zoom *Soft Skill* yang dibawakan langsung oleh mantan rektor UGM yaitu Professor Sudjarwadi. Dalam pertemuan *online* itu Profesor Sudjarwadi menjelaskan pentingnya memiliki *soft skill* dalam perjalanan hidup.

Dalam tugas akhir studi independen ini, mahasiswa dan mahasiswi akan diminta mencari kerentanan dalam sebuah *website* atau bisa disebut dengan melakukan pentest atau *penetration test* yang sudah ditentukan oleh pihak dari PT Gama Multi Usaha Mandiri. Project ini dilakukan secara berkelompok yang terdiri dari 4 - 5 anggota. Peserta magang akan menggunakan ilmu yang telah diajarkan melalui tugas-tugas yang telah diberikan kepada peserta magang untuk menyelesaikan tugas akhir ini yaitu melakukan *penetration test*. Keamanan siber merujuk pada kumpulan perangkat, kebijakan, pengaturan, langkah-langkah perlindungan, pendekatan manajemen risiko, jaminan keamanan, pelatihan, praktik terbaik, serta teknologi yang digunakan untuk melindungi aset organisasi, terutama

data dan informasi yang berada dalam ruang siber[1].Perkembangan teknologi informasi telah membawa perubahan besar pada konsep keamanan. Interaksi sekarang tidak hanya terbatas pada ruang fisik, tetapi juga meluas ke dunia maya. Akibatnya, negara harus menyesuaikan diri dengan perkembangan ini, dan konsep keamanan dunia maya perlu diakui sebagai salah satu "wilayah" yang harus dilindungi oleh negara, seperti kewajiban negara dalam menjaga wilayah teritorialnya. Terlebih lagi, serangan siber tidak hanya menargetkan institusi publik, tetapi juga menyerang institusi pemerintah[2]. Pada zaman sekarang, penting sekali dengan namanya keamanan atau *security*. Penggunaan *website* sudah banyak sekali digunakan sebagai media penyebaran informasi oleh berbagai instansi. Namun, dengan semakin banyaknya penggunaan *website* muncul beragam kejahatan maya yang berusaha mencuri data dari sebuah *website*. Situs web dapat dibuat dan dikelola oleh individu, kelompok, bisnis, atau organisasi untuk melayani berbagai tujuan. Keamanan *website* itu sangat penting karena siapapun pasti tidak ingin *website* miliknya diretas atau dibobol. Jika sebuah *website* diretas atau bahkan diblokir, hampir tidak mungkin *website* miliknya akan kembali dikarenakan data *traffic*nya sudah hilang dan itu akan berdampak buruk bagi sang pemilik website ataupun yang orang-orang yang bersangkutan pada *website* tersebut. Karena itulah keamanan *website* sangat penting[3]. Ada beberapa faktor yang menyebabkan kurangnya tingkat keamanan pada aplikasi *website*, diantaranya adalah kesalahan penulisan kode program dan *misconfiguration*. Kesalahan pada penulisan kode program dalam pembuatan aplikasi berbasis *website* sering dimanfaatkan oleh penyerang, dalam hal ini serangan yang dapat sering dimanfaatkan oleh penyerang diantaranya adalah SQL Injection, *Authentication*, dan XSS[4].

## 1.2 Maksud dan Tujuan Kerja Magang

Maksud dari Studi Independen ini adalah untuk memberikan pengalaman dan ilmu bagi mahasiswa - mahasiswi semester 6 dari kampus di seluruh Indonesia. Tujuan dari Studi Independen ini sendiri adalah untuk mengajarkan lebih dalam lagi kepada mahasiswa dan mahasiswi seputar IT di bidang *Cyber Security*. Diajarkan cara meretas sebuah *website* dengan beberapa metode yang memungkinkan, mengenkripsi dan deskripsi pesan lewat email, mencari tahu masalah dalam sebuah web atau aplikasi dan sebagainya.

### 1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Waktu pelaksanaan Studi Independen ini *full Online* melalui Zoom yang dimana Zoom ini dilaksanakan 3x seminggu yang dimana ada Lecture setiap Senin atau Selasa, Zoom *soft skill* yang dilaksanakan setiap hari rabu dan Zoom mentoring pada hari Jumat. Untuk jamnya tidak menentu karena tergantung kapan mentor dapat meluangkan waktunya.

