BAB I. PENDAHULUAN

1.1. Latar Belakang

Sebagian masyarakat Indonesia dari kalangan bawah hingga kalangan atas, mulai dari anak muda hingga orang tua sudah pasti menggunakan internet. Ini terlihat dari hasil survey pada tahun 2017 yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet (APJII) dimana masyarakat Indonesia yang menggunakan internet mencapai 171,17 juta jiwa dari total 264,16 juta jiwa. Terlebih lagi pada tahun 2020, pandemi COVID-19 membuat pengguna internet bertambah pesat. Hal tersebut terjadi karena masyarakat dipaksa untuk melakukan *Work from Home* (WFH) dan para pelajar diminta untuk mengikuti kelas secara *online* yang berakibat pada penggunaan internet yang semakin bertambah.

Dengan adanya kelas *online,* banyak *website* sekolah dan *website* kampus yang akan digunakan dalam proses pembelajaran. Hal tersebut dapat berakibat baik maupun buruk. Akan berakibat baik apabila digunakan untuk mengumpulkan tugas hingga memberikan informasi sebagaimana mestinya. Tetapi, akan berakibat buruk apabila keamanan sistem informasi *website* tersebut terlalu lemah dan dimanfaatkan oleh oknum-oknum yang tidak bertanggung jawab. Dengan bertambahnya masyarakat yang menggunakan internet maka akan bertambah juga oknum-oknum yang akan mencoba untuk melakukan peretasan atau *hacking* terhadap *website-website* tersebut. Hal tersebut dapat terjadi karena adanya serangan yang dilakukan oleh *hacker* dengan tujuan untuk memperoleh data sensitif yang ada.

Terdapat beberapa cara yang dapat dilakukan untuk menghindari sebuah peretasan. Salah satu pencegahan yang dapat dilakukan adalah dengan cara mengevaluasi keamanan sistem informasi *website* yang ada [1]. Keamanan sistem sendiri adalah bagaimana cara mencegah atau mendeteksi adanya kerusakan pada suatu sistem informasi, pencurian data informasi, serta perubahan pada suatu sistem informasi. Selain itu, perlu juga dilakukan evaluasi keamanan sistem informasi pada suatu *website*. Tujuan dari dilakukannya evaluasi adalah untuk

meminimalisir terjadinya penyalahgunaan suatu aset atau data yang ada pada *website* tersebut. Untuk mengevaluasi keamanan sistem informasi dapat digunakan dengan cara pengujian kerentanan atau *Penetration Testing* (pentest). Pentest merupakan kegiatan yang bertujuan untuk mengeksploitasi dan mengidentifikasi kerentanan yang ada [2].

Sistem Informasi Akademik adalah suatu sistem informasi yang dibangun untuk memberikan kemudahan kepada pengguna dalam kegiatan administrasi akademik kampus secara online, seperti proses Penerimaan Mahasiswa Baru (PMB), pembuatan kurikulum, pembuatan jadwal kuliah, pengisian Kartu Rencana Studi (KRS), pengisian nilai, pengelolaan data dosen dan mahasiswa. Sistem ini juga dapat berfungsi sebagai pendukung untuk analisis data dalam menentukan keputusan kampus. Karena berbagai macam informasi penting terdapat di dalam sistem informasi tersebut, maka perlu dilakukannya pentest ini. Bahaya dari melakukan pentest adalah penguji akan melakukan peretasan dan penggalian celah yang terdapat dalam *website*, sehingga bisa dikategorikan sebagai kejahatan *cyber*. Maka dari itu, sebelum melakukan pentest, perlu adanya izin terlebih dahulu kepada pihak yang terkait.

Dalam pentest ini digunakan beberapa alat seperti WHOIS, whatweb, Nmap, dan Nessus *Web Vulnerability Scanner*. Pengujian ini memiliki tujuan untuk melakukan eksploitasi dan identifikasi terhadap kerentanan suatu server web. Tingkat pengujian yang dilakukan terbagi menjadi tiga tingkat yaitu *low risk, medium risk,* dan *high risk* [3]. Setelah mengetahui tingkat kerentanan suatu server web, selanjutnya adalah mencoba untuk mengeksploitasi suatu kerentanan tertentu, hanya saja akses yang didapat mungkin dibatasi. Dari pengujian ini diharapkan dapat mengetahui tingkat keamanan yang ada pada *website* Universitas Atma Jaya Yogyakarta (UAJY) dan melakukan analisis mengenai celah keamanan pada *website* tersebut. Maka dengan demikian pengujian pentest ini dianggap penting dan layak untuk dijadikan kajian skripsi.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang yang telah disampaikan, terdapat beberapa rumusan masalah yang terdapat dalam pengujian ini, seperti:

1. Bagaimana cara melakukan pengujian keamanan terhadap *website* kuliah.uajy.ac.id milik Universitas Atma Jaya Yogyakarta?
2. Celah keamanan apa saja yang terdapat pada *website* kuliah.uajy.ac.id milik Universitas Atma Jaya Yogyakarta?

1.3. Batasan Masalah

Supaya pengujian tidak menyimpang dan tetap terarah, maka dibutuhkan batasan masalah. Batasan masalah pada pengujian ini meliputi:

1. Pengujian celah keamanan pada *website* kuliah.uajy.ac.id dan ortu.uajy.ac.id milik Universitas Atma Jaya Yogyakarta menggunakan alat WHOIS, Whatweb, Nmap, dan Nessus *Web Vulnerability Scanner*.
2. Pengujian dilakukan dengan menggunakan beberapa metode serangan *exploit*, *cross-site scripting* (XSS), dan DoS.

1.4. Tujuan Penelitian

Tujuan pengujian yang hendak dicapai adalah:

1. Mengetahui tingkat keamanan yang ada pada *website* UAJY.
2. Melakukan analisis mengenai celah keamanan pada *website* UAJY.

1.5. Metode Penelitian

Beberapa tahapan yang digunakan peneliti dalam melakukan sebuah pengujian keamanan sistem informasi, yaitu:

A. Observasi

Pengujian ini dilakukan pada Sistem Informasi Universitas Atma Jaya Yogyakarta dengan mengumpulkan sejumlah informasi penting sehingga dapat membantu proses pengujian keamanan sistem.

B. Pengumpulan Data

Pengumpulan data dilakukan dengan cara mempelajari situs web dan buku-buku karya ilmiah. Selain itu, pengumpulan data dilakukan dengan melakukan dokumentasi yang berkaitan dengan penelitian yang digunakan oleh penulis sebagai bahan acuan dalam melakukan pengujian keamanan sistem. Dalam menentukan dan guna mengumpulkan data penelitian, dibutuhkan sebuah perbandingan studi literatur. Studi literatur dilakukan dengan maksud untuk mencari referensi metode dan data yang akan digunakan untuk penelitian. Adapun pemanfaatan hasil pencarian dari referensi seperti jurnal, buku, serta internet adalah untuk mendapatkan materi yang berkaitan dengan pengujian ini.

C. Mempersiapkan Alat

Tahap ini merupakan tahap dimana penulis akan mempersiapkan alat-alat yang diperlukan untuk melakukan pengujian. Salah satu alat yang digunakan adalah *scanner*. *Scanner* berfungsi untuk memindai beberapa informasi yang dibutuhkan seperti ip *address*, *port*, *server* dan bahasa pemrograman yang digunakan.

D. *Scanning*

Setelah mendapatkan beberapa informasi mengenai web target, selanjutnya akan melakukan proses *scanning* atau pemindaian yang dimana proses ini akan mencari *port* atau celah keamanan lain pada web menggunakan beberapa alat pengujian.

E. Pengujian

Pengujian terhadap sistem dilakukan dengan menggunakan alat pendukung atau manual. Masalah terhadap keamanan yang ditemukan akan diberitahukan kepada pemilik sistem bersamaan dengan penilaian dan solusi teknis dari setiap kerentanan yang ditemukan. Ada tiga alternatif teknik pengujian, yaitu:

1. *Passive Penetration Testing*

   Teknik pengujian ini melakukan pemetaan dan pengujian terhadap kontrol yang ada pada aplikasi web, *login* dan konfigurasinya, sehingga penguji dapat memetakan target sistem.

2. *Active Penetration Testing*

   Teknik pengujian ini melakukan pengujian terhadap keamanan sistem dengan cara memanipulasi *input* dan melakukan pengujian terhadap kerentanan sebuah sistem.

3. *Aggressive Penetration Testing*

   Teknik pengujian ini melakukan eksploitasi terhadap kerentanan sistem, melakukan *reverse engineering* terhadap perangkat lunak dan sistem, menanamkan *backdoor*, pengunduhan kode, dan mencoba mengambil alih finansial dan informasi yang ada pada server.

F. Penulisan Laporan Akhir

Langkah terakhir adalah penulisan laporan akhir yang berisi hasil dan pembahasan mengenai penelitian yang telah dilakukan.

1.6. Sistematika Penulisan

Di dalam sistematika penulisan akan memberikan gambaran secara luas mengenai topik yang akan dibahas pada setiap bab. Adapun penjelasannya sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan laporan *penetration testing* pada domain uajy.ac.id.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang penelitian-penelitian yang dilakukan

oleh orang lain untuk dijadikan patokan dalam melakukan pengujian ini.

BAB III LANDASAN TEORI

Bab ini berisi landasan teori berisi teori yang akan diterapkan pada *penetration testing*. Di dalam bab ini juga menjelaskan tentang metode dan alat yang akan digunakan untuk pengujian.

BAB IV ANALISIS DAN PERANCANGAN PENGUJIAN

Bab ini berisi tentang hasil dari analisis dan perancangan pengujian.

BAB V HASIL DAN PEMBAHASAN PENGUJIAN

Bab ini berisi tentang hasil yang diperoleh dari proses pengujian keamanan yang dilakukan terhadap web target.

BAB VI PENUTUP

Bab ini berisi kesimpulan yang diambil dari hasil penelitian dan saran untuk membangun pengembangan penelitian selanjutnya.