BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan dunia teknologi yang semakin canggih membuat pekerjaan berjalan dengan sangat mudah dan cepat. Kemudahan yang ditawarkan teknologi tentunya beriringan dengan bahaya yang dapat disisipkan melalui berbagai hal. Terlebih lagi, jika bahaya tersebut tersistem sehingga membuat pengguna tidak menyadari dengan adanya bahaya yang sudah masuk dan mengintainya. Selain itu, *human behavior* dari mahasiswa maupun karyawan ini sendiri juga perlu dilihat mengingat bahwa pelaku *hacking* ini adalah orang dalam itu sendiri. Terkadang, *human behavior* yang kurang baik ini dapat membawa dampak buruk baik secara langsung maupun tidak langsung.

Dengan semakin majunya ilmu dan teknologi, semakin banyak pula masyarakat yang bergantung pada teknologi tersebut, terutama dalam hal yang berhubungan dengan internet. "Perkembangan dan evolusi dari komputer, internet dan teknologi *web* telah membuat masyarakat lebih bergantung pada layanan jaringan komputer lebih dari sebelumnya" (Shrestha, 2012). Hal ini dapat dilihat dengan semakin banyaknya jumlah pengguna media sosial dan layanan internet yang ada saat ini. Dari hasil laporan Asosiasi Penyelanggara Jasa Internet Indonesia (APJII) pada tahun 2012 menunjukkan sudah terdapat 63 juta pengguna internet di seluruh Indonesia yang mana meningkat sekitar 24,23% dari tahun sebelumnya (Asosiasi Penyelenggara Jasa Internet Indonesia, 2012). Pengguna internet di Indonesia diperkirakan masih akan terus meningkat hingga mencapai 123 juta orang pada tahun 2018 (Emarketer, 2014).

Di seluruh dunia terdapat sekitar 640 *Terabytes* data *transfer* dan 204 juta *email* dikirim melalui jaringan internet setiap menitnya (Rick, 2013). Informasi sendiri menjadi hal penting di era digital ini baik untuk setiap individu ataupun organisasi. Semakin banyak individu yang peduli dengan bagaimana informasi pribadi mereka digunakan dan semakin banyak pula organisasi yang sadar bahwa resiko keamanan informasi dapat memberi dampak buruk pada keberlangsungan proses bisnis, citra publik, relasi, menyebabkan kerugian materil, mempengaruhi hubungan dengan pelanggan atau mitra dan juga dapat menyebabkan masalah dengan pihak berwajib. Oleh karena itu untuk melindungi informasi yang ada diperlukan sistem yang baik.

Sistem dapat didefinisikan sebagai seperangkat komponen (sumber daya) terkait, dengan batas yang jelas dan bekerjasama untuk mencapai tujuan tertentu melalui sebuah inputan dalam proses transfromasi yang teroganisir (Brien dan Marakas, 2010). Sedangkan Sistem Informasi lebih menekankan pada pengelolaan sumber daya (*resource*) yang ada menjadi produk informasi. Jadi, sistem informasi akademik adalah sebuah sistem khusus untuk keperluan pengeloaan data-data akademik dengan penerapan teknologi komputer baik *hardware* maupun *software*.

Universitas XYZ merupakan salah satu universitas dengan jumlah civitas akademik yang banyak. Hal tersebut tentunya mengakibatkan banyaknya informasi yang dipertukarkan dalam organisasi ini. Pertukaran informasi menggunakan jaringan komputer sebagai medianya dimana informasi tersebut dapat berupa informasi penting atau pribadi dimana hak aksesnya hanya diperuntukkan untuk orang-orang tertentu. Mengingat *website* ini dapat diakses secara luas, maka dinilai perlu memperhatikan keamanan *website*. Terdapat beberapa cara yang dapat digunakan untuk melakukan pengujian terhadap kemanan *website*. Salah satunya adalah dengan melakukan *Web Penetration Testing*.

Berdasarkan definisi dalam modul CEH, *Web Penetration Testing* merupakan metode evaluasi keamanan sistem komputer atau dengan mensimulasikan serangan dari sumber yang berbahaya dan merupakan bagian dari *security audit*. Simulasi serangan yang dilakukan dibuat seperti kasus yang bisa dibuat oleh *black hat hacker*, *cracker*, dan sebagainya. Tujuannya adalah menentukan dan mengetahui macam – macam serangan yang mungkin dilakukan pada sistem beserta akibat yang bisa terjadi karena kelemahan sistem. Dalam melakukan *penetration testing*, diperlukan analisa intensif untuk setiap kerentanan yang diakibatkan oleh kelemahan sistem. Uji penetrasi dalam penelitian ini akan menggunakan *Kali Linux*. *Kali Linux* menggabungkan lebih dari 300 *tools* untuk uji penetrasi dan audit keamanan dengan sistem operasi *Linux*, memberikan sebuah solusi yang memungkinkan *administrator IT* dan profesional keamanan untuk menguji efektivitas keamanan sistem.

Alasan dilakukannya penelitian ini adalah karena peneliti mendengar dari beberapa sumber baik dosen maupun temen mahasiswa, bahwa sistem informasi akademik yang dimiliki oleh Universitas XYZ tidaklah aman atau dapat di *hacking* atau di jebol sewaktu – waktu. Alasan lain mengapa dilakukannya penelitian ini adalah untuk mengetahui pula seberapa tingginya tingkat keamanan sistem informasi akademik yang ada di Universitas XYZ. Oleh karena itu, prioritas utama kebutuhan yang penting saat ini adalah membantu meminimalisir dan mengantisipasi para *hacker* yang ada dari kejahatan *hacking*. Salah satu hal yang dapat dilakukan adalah dengan melakukan uji *Penetration* (*Web Penetration Testing*). Dari hasil pengujian ini, laporan atau hasilnya akan diberikan kepada pihak *administrator IT* agar pengembangan terhadap keamanan sistem bisa dapat dipertahankan atau ditingkatkan kembali.

1.2 Perumusan Masalah

Berdasarkan penjelasan dari latar belakang diatas, maka didapatkan perumusan masalah sebagai berikut:

a. Bagaimana menganalisis tingkat keamanan sistem informasi akademik di Universitas XYZ dengan menggunakan metode *Web Penetration Testing*?
b. Bagaimana hasil dari pengujian tingkat keamanan sistem informasi akademik di Universitas XYZ dengan *Web Penetration Testing*?
c. Bila terdapat kerentanan yang dapat ditembus, apa solusi atau saran untuk menutupi kerentanan tersebut?

1.3 Batasan Masalah

Batasan masalah pada penelitian tingkat keamanan sistem informasi akademik di Universitas XYZ adalah sebagai berikut:

a. Penelitian ini hanya untuk menguji tingkat keamanan sistem informasi akademik yang ada di Universitas XYZ.
b. Hanya menggunakan metode *black – hat* yaitu metode *penetration testing* yang serupa dengan yang dilakukan aslinya karena peneliti hanya diberikan nama perusahaan saja dan informasi mengenai jaringan maupun informasi lainnya harus dicari sendiri oleh peneliti.
c. Uji coba yang digunakan pada penelitian ini adalah menggunakan uji coba non destruktif, yaitu uji coba yang tidak membuat kerusakan sistem.
d. Metodologi *penetration testing* yang digunakan hanya menggunakan metode *Information Systems Security Assessment Framework (*ISSAF*) penetration testing*.
e. Pada tahapan penetrasi, serangan yang dilakukan hanya untuk mengetahui informasi *database* yang digunakan, tidak merubah atau mengambil data

– data yang ada dalam *database* tersebut. Serangan ini biasa disebut dengan *sql injection*.

1.4 Tujuan

Adapun tujuan dari penelitian pengujian tingkat keamanan sistem informasi akademik di Universitas XYZ ini adalah sebagai berikut:

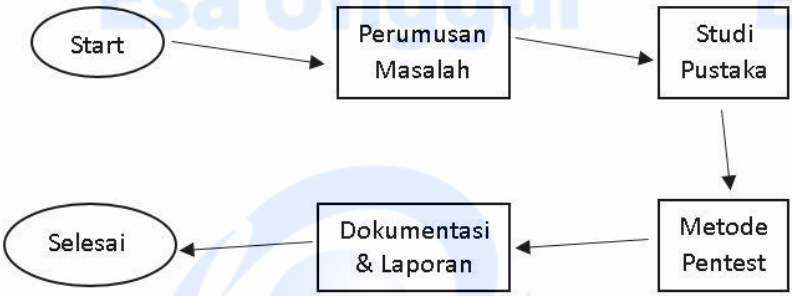
a. Untuk mengetahui tingkat keamanan sistem informasi akademik yang ada di Universitas XYZ.
b. Untuk mengetahui hasil dari pengujian tingkat keamanan sistem informasi akademik di Universitas XYZ.
c. Untuk mengetahui solusi atau saran dari kerentanan yang dapat ditembus selama proses pengujian.

1.5 Manfaat

Manfaat yang diperoleh dari penelitian pengujian tingkat keamanan sistem informasi akademik di Universitas XYZ ini adalah dapat mengembangkan dan meningkatkan keamanan sistem informasi akademik yang dimiliki oleh Universitas XYZ sehingga kegiatan civitas akademika tetap terjaga kerahasiaan datanya.

1.6 Metodologi

Kerangka pemikiran pada gambar 1 merupakan serangkaian bagan – bagan yang menggambarkan alur dari proses penelitian analisis sistem informasi akademik dengan *web penetration testing* studi kasus Universitas XYZ.



Gambar 1: Kerangka Berfikir

Sumber: Peneliti

a. Perumusan Masalah

Merupakan tahapan awal dari penelitian ini. Masalah yang dirumuskan adalah Bagaimana menganalisis tingkat keamanan sistem informasi akademik di Universitas XYZ dengan menggunakan metode *Web Penetration Testing* dan Bagaimana hasil dari pengujian tingkat keamanan sistem informasi akademik di Universitas XYZ dengan *Web Penetration Testing.*

b. Studi Pustaka

Mencari pengetahuan dasar yang didapat dari buku, jurnal, artikel, internet, karya ilmiah dan media lainnya untuk melengkapi landasan teori dan sebagai acuan dasar dalam menyelesaikan penelitian ini.

c. Metode Pentest

Pada tahapan ini dilakukan pengujian penetrasi tingkat keamanan sistem informasi akademik yang dimiliki oleh Universitas XYZ dengan *web penetration testing* dengan metode pentest yang biasa digunakan. Untuk metode pentest biasanya terdiri dari 3 tahapan yaitu *planning and preparation, assessment, report and result*. Untuk tahapan *assessment* terdiri dari *information gathering, network mapping, vulnerability scanning, penetration*. Penetrasi menggunakan teknik serangan yang hanya untuk mengetahui informasi *database* yang dimiliki oleh sistem tersebut. Jenis serangan ini biasa disebut *SQL injection*. Adapun *tools* pendukung yang digunakan dalam metode tersebut antara lain *who is*, *SSL scan*, *nmap*, *zenmap*, *SQLmap*, *havij*, *skipfish*, *httrack*, *vega*, *maltego*, *owasp zap*.

d. Dokumentasi dan Laporan

Pada tahapan dokumentasi dan pembuatan laporan merupakan tahapan dimana peneliti memaparkan hasil penelitian yang dilakukan dari tahap awal hingga akhir dan diimplementasikan kedalam bentuk skipsi atau proposal tugas akhir. Laporan hasil penelitian diserahkan ke 5 penerima yaitu bagian penanggung jawab IT, dosen pembimbing selama penelitian, dosen penguji ketika sidang, perpustakaan dan fakultas yang bersangkutan.

1.7 Lokasi dan Waktu Penelitian

Pada penelitian ini, peneliti menggunakan beberapa tempat dalam meneliti dan mengolah data – data yang didapat. Lokasi yang digunakan dalam penelitian ini antara lain:

a. Universitas XYZ yang bersangkutan, tepatnya di lantai 5 gedung lama Universitas XYZ.
b. Kosan belakang kampus Universitas XYZ yang bersangkutan
c. Rumah peneliti yang bersangkutan terletak di Perumahan Taman Kirana Surya Solear Kabupaten Tangerang Banten

Dalam penelitian ini, waktu yang digunakan didalam penelitian ini dari tahap awal hingga akhir adalah 11 bulan atau kurang lebih 330 hari. Adapun rincian jadwal tahapan penelitian dari awal hingga akhir adalah sebagai berikut:

Tabel 1: Waktu Penelitian

Waktu / Tahapan	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May
Perumusan Masalah									
Studi Pustaka									
Metode Pentest									
Dokumentasi dan Laporan									

Sumber: Peneliti