BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Universitas adalah sebuah perguruan tinggi yang terdiri dari beberapa fakultas, yang menyelenggarakan pendidikan ilmiah dalam beberapa disiplin ilmu tertentu. Adanya universitas tentu tidak dapat terpisahkan dari keberadaan orang-orang yang berperan di dalamnya, salah satunya adalah mahasiswa. Dengan banyaknya mahasiswa yang ada di dalam suatu universitas, pengelolaan data mahasiswa menjadi sangat penting agar dapat terorganisir dengan baik.

Data mahasiswa biasanya disimpan pada server universitas. Selain dibutuhkan kapasitas yang cukup untuk menyimpan data, server juga harus memiliki keamanan yang tinggi. Keamanan dari data tersebut menjadi urgensi yang tidak dapat diabaikan. Data mahasiswa harus dilindungi dari pihak yang tidak berhak mengaksesnya. Keamanan secara umum dinilai berdasarkan tiga faktor utama, yaitu *Confidentiality*, *Integrity*, dan *Availability* atau yang biasa disingkat CIA.

Berdasarkan informasi dari portal berita BBC, ancaman keamanan berupa serangan siber pada tahun 2020 telah terjadi di beberapa universitas, sekolah, dan bahkan rumah sakit. Salah satu kasus serangan siber menimpa *University of California, San Francisco* (UCSF). Peretas berhasil menyerang server universitas dan mendapatkan data penting berupa data penelitian Fakultas Kedokteran tentang Covid-19. Awalnya peretas meminta tebusan kepada universitas sebanyak US$ 3 juta untuk mendapatkan kunci dekripsi yang dapat mengembalikan data yang telah dienkripsi oleh peretas. Kemudian universitas melakukan negosiasi dengan peretas yang telah mengunci setidaknya tujuh server milik universitas. Universitas terkonfirmasi membayar peretas dengan jumlah penawaran terakhir dari negosiasi tersebut yaitu sebesar US$ 1,14 juta (Tidy, 2020).

Kasus tersebut membuktikan bahwa data penting yang terletak pada server sebuah organisasi bisa saja diretas dan diakses oleh orang yang tidak berhak. Peretas memiliki tujuan tertentu untuk melakukan penyerangan, seperti mencuri

informasi penting, merusak sistem, bersenang-senang, dan juga melakukan pemerasan seperti yang terjadi pada UCSF. Peretas meminta sejumlah uang kepada organisasi, dengan ancaman jika tidak diberi uang tebusan maka data korban yang telah dimiliki oleh peretas tidak akan dikembalikan, atau bahkan sampai disebarluaskan.

Salah satu cara untuk menghindari terjadinya peretasan adalah dengan menutup celah-celah keamanan yang mungkin dimiliki sistem. Sebelum menutup celah keamanan, kita harus mengetahui celah keamanan tersebut dengan melakukan pengujian seperti yang dilakukan oleh peretas, namun dengan prosedur yang telah disetujui. Untuk mencegah peretas meretas sistem universitas, penulis melakukan penelitian untuk melakukan simulasi serangan terhadap server eksternal sebuah universitas. Penelitian yang dilakukan berjudul Uji Penetrasi Server Universitas PQR Menggunakan Metode *National Institute of Standards and Technology* (NIST SP 800-115).

1.2 Perumusan Masalah

Pada penelitian ini terdapat beberapa permasalahan yang dibahas yaitu:

1. Bagaimana melakukan pengujian penetrasi terhadap keamanan data pribadi mahasiswa pada server Universitas PQR?
2. Jenis kerentanan apa saja yang terdapat pada server Universitas PQR?
3. Bagaimana cara memitigasi kerentanan yang terdapat pada server Universitas PQR?

1.3 Ruang Lingkup Penelitian

Supaya penelitian ini menjadi lebih terarah serta mengurangi adanya penyimpangan, perlu adanya ruang lingkup penelitian. Ruang lingkup yang ada pada penelitian ini yaitu:

1. Penelitian ini dilakukan dengan menggunakan Sistem Operasi Linux, distro Kali Linux 2020.1 untuk pengujiannya. Serta beberapa *tools* uji penetrasi, yaitu Metasploit 5.0.99, NMAP 7.91, Nessus 8.14.0, SSL Scan 2.0.0-static, dan Wireshark 3.2.5.

2. Server yang akan diuji merupakan server eksternal Universitas PQR yang menyimpan data pribadi mahasiswa.
3. Uji penetrasi pada penelitian ini mengacu pada *Penetration Testing* dalam *NIST Special Publication 800-115*.
4. Uji penetrasi dilakukan di atas pukul 6 sore atau setelah jam kantor pada hari kerja dan sepanjang hari pada hari libur.
5. Pengujian pada penelitian tidak mengganggu proses produksi dari Universitas PQR.
6. Alamat IP yang digunakan pada penelitian tidak dipublikasikan demi keamanan sistem Universitas PQR.
7. Pengujian pada penelitian ini tidak menggunakan *Social Engineering*.
8. Penerapan dari rekomendasi akan diserahkan sepenuhnya kepada pihak terkait, yaitu Universitas PQR.

1.4 Tujuan dan Manfaat Penelitian

Tujuan utama dari penelitian ini adalah melakukan pengujian terhadap sistem keamanan pada server yang menyimpan data pribadi mahasiswa di Universitas PQR dengan menerapkan metode *National Institute of Standards and Technology* (NIST SP 800-115) serta mengetahui celah keamanan apa saja yang terdapat pada server tersebut.

Manfaat dari penelitian ini yaitu memberi kontribusi untuk Peneliti, Universitas PQR, dan Pembaca.

1. Bagi Universitas PQR

   Penelitian ini diharapkan dapat membantu Universitas PQR mengetahui celah-celah keamanan apa saja yang terdapat pada server universitas yang menyimpan data pribadi mahasiswa. Selain itu juga hasil penelitian ini dapat digunakan sebagai bahan pertimbangan untuk memperbaiki sistem keamanan server universitas.
2. Bagi Peneliti

   Penelitian ini diharapkan membuat Peneliti memiliki pengalaman tentang ilmu uji penetrasi dengan mengimplementasikan serta mengembangkan lagi ilmu-ilmu yang telah didapat selama di bangku perkuliahan.

3. Bagi Pembaca

   Penelitian ini diharapkan dapat memberikan informasi yang berguna kepada pembaca mengenai uji penetrasi sebagai bagian dari ilmu pengetahuan di bidang Informatika, serta dapat menjadi referensi untuk penelitian yang terkait di masa depan.

1.5 Luaran yang diharapkan

Luaran yang diharapkan dari penelitian ini yaitu diketahuinya kerentanan yang ada pada sistem keamanan server Universitas PQR yang menyimpan data pribadi mahasiswa serta rekomendasi untuk memitigasi kelemahan tersebut, sehingga dapat diatasi dan diantisipasi lebih lanjut oleh pihak universitas.

1.6 Sistematika Penulisan

Dalam menyusun Skripsi ini, sistematika dari pembahasan di dalamnya diatur dan disusun dalam lima bab yang saling berkaitan. Guna memberikan gambaran yang lebih jelas, maka disebutkan secara singkat tentang sistematika penulisan Skripsi pada setiap bab, yaitu sebagai berikut :

BAB I. PENDAHULUAN

Dalam bab ini menjelaskan mengenai latar belakang permasalahan, rumusan masalah, ruang lingkup penelitian, tujuan dan manfaat penelitian, luaran yang diharapkan, serta sistematika penulisan skripsi.

BAB II. LANDASAN TEORI

Dalam bab ini menjelaskan mengenai dasar-dasar teori yang menjadi pendukung selama melakukan penelitian tugas akhir serta referensi jurnal yang digunakan pada penelitian.

BAB III. METODOLOGI PENELITIAN

Dalam bab ini menjelaskan mengenai metode penelitian yang diterapkan, tahap penelitian yang akan dilakukan, alat bantu penelitian, serta jadwal penelitian.

BAB IV. HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan mengenai proses uji penetrasi yang dilakukan, tahapan-tahapan, serta pembahasan tentang hasil yang didapatkan dari pengujian tersebut.

BAB V. PENUTUP

Pada bab ini menjelaskan mengenai kesimpulan dari hasil penelitian yang dilakukan pada bab 4 (empat) serta saran yang dapat dipergunakan untuk pedoman penelitian selanjutnya.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN