BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan pada teknologi informasi yang setiap saat berubah pesat membantu pekerjaan berjalan dengan sangat efisien dan efektif. Dengan semakin bertumbuhnya teknologi informasi, maka akan terjadi peningkatan penggunaan teknologi (Mahdi Maulana Lubis et al., 2022). Dalam penggunaan aktivitas media sosial serta layanan *internet* saat ini, dapat dilihat dari hasil survey laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) di tahun 2012 terdapat 63 juta pengguna *internet* di Indonesia yang terus meningkat sebesar 24,23 dari tahun sebelumnya. Hingga pada tahun 2019-2020 jumlah pengguna *internet* di Indonesia sebanyak 196,71 juta jiwa atau 73,7% dari keseluruhan penduduk Indonesia (APJII, 2020).

Seiring dengan berjalannya perkembangan teknologi, maka keamanan sistem informasi menjadi salah satu isu penting yang harus diperhatikan agar proses bisnis dapat berjalan dengan semestinya. Melindungi aset organisasi dari ancaman serangan peretas dengan menggunakan pendekatan yang komperehensif serta terstruktur dari ancaman resiko kebocoran data. Peretas merupakan individu yang menguasai kemampuan illegal dalam meretas jaringan komputer untuk kepentingan pribadi. Sering terjadi kasus peretasan di Indonesia, antisipasi dapat dilakukan dalam mengamankan *server* agar tidak terjadi kebocoran data hingga *ransomware.* Jika hal itu terjadi, maka dapat menyebabkan kerugian secara materi yang diakibatkan oleh peretas (W et al., 2021). Menurut Badan Siber dan Sandi Negara (BSSN) 361 juta serangan siber yang masuk ke Indonesia dalam kurung waktu 1 Januari-26 Oktober 2023. Telah tercatat tiga jenis serangan siber dengan *traffic* tertinggi, yaitu *malware activity* dengan jumlah 42,79%, kemudian *trojan activity* dengan jumlah 35,40%, dan yang terakhir *information leak* sebesar 9,35%. Data kerugian akibat serangan siber mencapai RP 14,5 triliun pada tahun 2023 (Pohan et al., 2021a). Peretasan juga pernah terjadi pada *website E-Learning* yang digunakan oleh MTs dan Ma Husnul Khotimah yang dinaungi oleh Pondok Pesantren Husnul Khotimah Kuningan, Jawa Barat. Aksi peretasan dengan jenis serangan *defacement website* ini terjadi pada hari Rabu 24 Maret 2021 yang menyebabkan proses

pembelajaran jarak jauh (PJJ) sempat terganggu selama 4 hari. Dimana pihak peretas yang mencoba untuk meretas situs *website* dan mengganti isi konten dengan pesan pribadi mereka. Pesan yang ditunjukkan dapat mengandung unsur agama, politik, atau konten yang tidak seharusnya, hingga pemberitahuan bahwa *website* tersebut telah diretas (Fathurahman et al., 2022).

Website XYZ dengan domain https://XYZ/ *website* pintu utama bagi calon mahasiswa baru sehingga menyediakan informasi dan layanan terkait proses pendaftaran mahasiswa baru, menyimpan data pribadi calon mahasiswa baru, menyajikan informasi mengenai jadwal tes, wawancara, dan kegiatan terkait yang menjadi bagian dari proses seleksi penerimaan mahasiswa baru di Universitas XYZ. Begitu banyak tugas dan fungsi yang harus dikerjakan melalui situs XYZ, dan apabila terjadi peretasan pada *website* tersebut dapat mengakibatkan kebocoran data mahasiswa baru sehingga data pribadi tersebut dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab, seperti pembuatan akun palsu, pinjaman *online,* dan terjadi kasus penipuan. Selain itu, pihak Universitas XYZ juga mengalami kerugian dari segi finansial, waktu hingga kepercayaan. Maka dari itu diperlukan analisis keamanan sistem informasi untuk mencegah dan mengontrol akses yang mencurigakan yang terjadi dalam *website* XYZ. Berdasarkan hasil wawancara dengan responden yang menjabat sebagai ketua divisi IT XYZ bahwa sejak didapatkan daripihak ketiga pada tahun 2013 *website* belum pernah dilakukan *maintenance* dari sisi *user,* dan pihak Universitas XYZ pernah mendapatkan laporan dari mahasiswa bahwa terdapat indikasi potensi serangan *phising*. Hal ini terlampir pada **Lampiran Wawancara.** Oleh karena itu Universitas XYZ meenginginkan adanya kegiatan *penetration testing* yang bertujuan untuk mencegah dan mengantisipasi adanya serangan dari pihak luar dan juga akan digunakan sebagai bahan evaluasi terhadap kebijakan keamanan sistem informasi *website.*

Salah satu *framework* yang dapat digunakan yaitu *Information System Security Assessment Framework* (ISSAF). ISSAF merupakan kerangka kerja yang digunakan untuk melakukan penilaian kemana sistem informasi dan dirancang untuk membantu para ahli keamanan informasi, *auditor*, dan penilai risiko untuk

secara sistematis mengevaluasi dan mengidentifikasi kelemahan pada keamanan dalam suatu sistem (Sanjaya, Sasmita, & Arsa, 2020).

Oleh karena itu, berdasarkan latar belakang dan referensi, penulis ingin melakukan penelitian dengan judul "Analisis Keamanan Sistem Informasi Berdasarkan Pendekatan ISSAF Pada *Website* XYZ" untuk mengetahui sistem keamanan yang terdapat pada situs *website* XYZ tersebut. Hal ini perlu dilakukan untuk mengembangkan strategi yang matang dalam pengelolaan dan pemeliharaan sistem teknologi informasi agar tetap terjaga, aman, dan sesuai dengan norma hukum yang berlaku. Hasil dari penelitian ini berupa dokumen rekomendasi perbaikan yang bertujuan untuk pengembangan sistem *website* XYZ

1.2. Rumusan Masalah

Berdasarkan latar belakang yang sudah dijelaskan, maka diperoleh rumusan masalah dalam penelitian ini, yaitu:

1. Bagaimana tingkat keamanan pada *website* XYZ menurut pendekatan ISSAF?
2. Bagaimana skala prioritas perbaikan sistem hasil dari *penetration testing*?
3. Bagaimana rekomendasi yang diberikan dari hasil *penetration testing* berdasarkan *framework* ISSAF kepada pihak Universitas XYZ

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah yang sudah dijelaskan diatas, maka diperoleh tujuan penelitian, yaitu:

1. Mengidentifikasi proses cara kerja *penetration testing* berdasarkan *framework* ISSAF berdasarkan sistem XYZ.
2. Memberikan rekomendasi perbaikan yang telah sesuai dengan hasil *penetration testing* berdasarkan *framework* ISSAF kepada pihak XYZ.
3. Menentukan skala prioritas dalam perbaikan sistem berdasarkan hasil tingkat kerentanan *penetration testing* yang telah dilakukan.

1.4. Batasan Penelitian

Berdasarkan topik permasalahan yang penulis ajukan, maka diperoleh batasan masalah dalam penelitian ini, yaitu:

1. Studi kasus yang digunakan dalam penelitian ini yaitu *website* XYZ pada *domain* https://XYZ/.
2. Menggunakan *penetration testing* berdasarkan pendekatan ISSAF

3. Menggunakan metode *black box testing.*

1.5. Manfaat Penelitian

1. Memberikan pemahaman lebih lanjut terhadap tingkat keamanan sistem *website* XYZ yang dapat membantu pihak Universitas XYZ untuk melakukan identifikasi peningkatan keamanan sistem.
2. Memberikan pandangan terhadap implementasi ISSAF dalam dunia pendidikan, sehingga dapat membuat peluang untuk evaluasi di bidang lain.

1.6. Sistematika Penulisan

Penelitian ini akan melewati berbagai tahapan yang telah dilakukan observasi dan rancangan. Pada tahap pertama akan berfokus dengan pengumpulan data *website* XYZ, Melakukan studi literatur dengan sebagai sumber referensi merujuk pada *paper*, jurnal, dan sumber referensi sebagai pendukung penelitian. Tahap kedua akan dilakukan analisis *website* yang bertujuan untuk mendapatkan informasi mengenai sistem dan evaluasi keamanan sistem informasi yang ada. Tahap selanjutnya yaitu akan diterapkan identifikasi *vulnerability* sebagai deteksi celah potensi kelemahan keamanan yang bisa dimanfaatkan oleh pihak yang tidak diinginkan. Kemudian, yaitu dilakukan uji penetrasi yang berdasarkan standar ISSAF dengan metode *black box* yang bertujuan untuk mengetahui tingkat keamanan pada *website* XYZ. Tahap akhir dalam penelitian ini yaitu akan dilakukan analisis hasil dari seluruh uji penetrasi yang telah dilakukan pada tahap sebelumnya dan ditentukan skala prioritas perbaikan melalui *Common Vulnerability Scoring System* (CVSS). Hasil analisis akan menghasilkan sebuah buku rekomendasi perbaikan yang dapat membantu meningkatkan keamanan sistem *website* XYZ. Setelah melalui berbagai tahapan pengujian, diharapkan penelitian ini dapat memberikan kontribusi terhadap keamanan sistem *website* XYZ.