BAB I PENDAHULUAN

Dalam bab ini akan mencakup gambaran umum dalam penelitian seperti latar belakang penelitian, perumusan masalah, tujuan penelitian, batasan masalah dan metodologi penelitian.

I.1 Latar Belakang

Perkembangan teknologi yang semakin canggih menciptakan kemudahan dalam berbagai kegiatan manusia. Dengan berkembangnya teknologi dan ditemukannya jaringan internet, manusia menjadi lebih mudah dalam mengakses informasi dan membagikan data ke seluruh dunia. Kemudahan yang ditawarkan pasti sepadan dengan risiko yang dapat muncul dari berbagai hal**.** Urgensitas pemilihan topik ini adalah untuk mengatasi tantangan signifikan dalam keamanan siber yang dihadapi oleh lembaga publik, khususnya dalam melindungi data sensitif dan integritas sistem informasi. Mengingat peningkatan frekuensi dan kerumitan serangan siber, analisis keamanan yang mendalam pada *website* Dinas Perpustakaan dan Kearsipan Kota Surabaya menjadi krusial untuk memastikan perlindungan data pengguna dan menjaga kepercayaan publik. Ancaman di dunia digital, terutama *website,* dapat mempengaruhi sistem secara keseluruhan, selain itu di dunia digital, ancaman dapat berasal dari berbagai sumber, seperti serangan peretas *(hacker)* yang berusaha merusak atau mencuri data sensitif, dan *malware* yang dapat merusak integritas sistem secara keseluruhan. Mengingat banyaknya informasi penting yang disimpan dan diakses melalui *website*, pengembang dan administrator *website* harus memastikan bahwa sistem keamanan yang kuat dan terkini diterapkan untuk melindungi data dan privasi pengguna (Ary et al., 2020).

Website adalah kumpulan dokumen yang terstruktur dengan berbagai tautan yang menghubungankan satu dokumen ke dokumen lainnya (Wardhana and Seta, 2021). Dengan menggunakan *browser* pada *smartphone* atau komputer, pengguna dapat mengakses *website* dari mana saja dan kapan saja. Website ini menjadi pilihan terbaik untuk memudahkan pekerjaan manusia sehari-hari (Wardhana and Seta, 2021). Berdasarkan publikasi *International Telecommunication Union* (ITU) menyebutkan bahwa *Global Cybeer Security*

Index Indonesia pada tahun 2020 berada pada peringkat ke-24 dari 194 negara (Badan siber dan sandi negara, 2021). Hal ini belum tentu dapat merefleksikan kebebasan yang sesungguhnya dalam kapabilitas warga negara Indonesia untuk melindungi data-data pribadi dan mendapatkan jaminan proteksi yang aman untuk dapat beraktivitas di ruang siber. Perlindungan data tiap warga negara wajib dilaksanakan, namun pada faktanya ada beberapa peristiwa yang belum lama ini terjadi seperti kebocoran data BPJS dan Kementerian Kesehatan, kebocoran data E-KTP serta diretasnya situs Badan Intelijen Negara (BIN) kemudian dijual belikan pada sebuah forum jual beli data, sehingga banyak yang mempertanyakan peran dan kemampuan negara dalam menjaga integritas dan kerahasiaan data pribadi(Aji, 2023). Akhir-akhir ini seseorang *hacker* bernama Bjorka menjadi topik yang sangat diperbincangkan di seluruh dunia internet, bahkan di publik tanah air. Selama beberapa bulan dari akhir Agustus hingga awal September 2022, Bjorka diketahui telah menyebarkan sejumlah data sensitif seperti angka telepon, angka kartu identitas, dan angka kartu keluarga . Statistik sensitif warga Indonesia diperoleh Bjorka melalui berbagai sumber asli, seperti operator internet *Indihome*, biaya pemilihan umum (KPU), dan prosedur pendaftaran kartu SIM (Aji, 2023).

Sebuah studi serta analisis yang dilakukan oleh DAKA *Advisori* diperkirakan kerugian yang disebabkan oleh kejahatan siber di Indonesia, yakni sebesar $895 milyar yang artinya mencapai 1,20% dari total keseluruhan perkiraan kerugian akibat kejahatan siber global, yaitu $71,620 milyar (Indah et al., 2022). Oleh karena itu pada penelitian kali ini akan dilakukan analisis keamanan menggunakan *Black Box Testing* berupa uji penetrasi terhadap *website* Dinas Perpustakaan dan Kearsipan (Dispusip), terutama mengingat adanya indikasi kerentanan yang dapat mengancam integritas sistem, seperti kurangya enkripsi data, belum adanya mekanisme login yang memadai, dan potensi risiko terhadap data sensitif yang disimpan dan diakses melalui *website* tersebut. *Black Box Testing adalah* Sebuah metode pengujian yang berfokus pada *spesifikasi fungsional* dari perangkat lunak, penguji dapat mendefinisikan kumpulan kondisi *input* dan melakukan pengetesan pada *spesifikasi fungsional program* (Shadiq et al., 2021). Pengujian menggunakan *Black box* digunakan karena mempertimbangkan waktu penelitian yang sangat singkat dan akses informasi yang didapatkan sangat terbatas (Shadiq

et al., 2021). Beberapa keunggulan dari pengujian *Black Box* adalah penguji diposisikan sebagai pihak *eksternal* atau penyerang yang tidak memiliki pengetahuan *internal* tentang informasi dan data yang ada pada *website* (Shadiq et al., 2021). Hal ini membantu untuk dapat mengevaluasi seberapa baik sistem dapat bertahan terhadap serangan dari luar, selain itu *Black Box* testing lebih efektif dalam menemukan kerentanan atau celah keamanan yang tidak terdeteksi oleh tim pengembang dari pihak ketiga bersama tim *internal* pihak Dinas Perpustakaan dan Kearsipan Kota Surabaya yang sudah terbiasa dengan struktur *website* (Sirait, 2020). *Website* Dispusip merupakan sarana publikasi untuk menyampaikan informasi dan gambaran terkait Dinas Perpustakaan dan Kearsipan Kota Surabaya dalam melaksanakan pelayanan kepada masyarakat di bidang Perpustakaan dan Kearsipan, selain itu *website* ini juga berisi data penting seperti data arsip perpustakaan dan data pengguna *website* yang akan melakukan peminjaman buku, oleh karena itu pada menu *login* ini tidak boleh diakses oleh orang luar dan hanya boleh diakses oleh pihak yang berwenang. Permasalahan pada *website* ini adalah masih banyak sistem yang masih belum menerapkan keamanan yang layak, seperti belum adanya menu *login* pada bagian registrasi tamu yang ingin mengakses *website* tersebut diharuskan untuk memilih opsi untuk memasukkan data seperti, KTA (Kartu Tanda Anggota Perpustakaan), KTP (Kartu Tanda Penduduk), KTM (Kartu Tanda Mahasiswa) dan Kartu Pelajar. Selain itu kurangnya enkripsi data dalam menjaga identitas dan privasi pelanggan dan belum pernah melakukan uji coba keamanan karena keterbatasan pengetahuan dan sumber daya pegawai sehingga pihak Dinas Perpustakaan dan Kearsipan Kota Surabaya tidak mengetahui celah dan kerentanan yang ada pada *website* ini. Akibat dari permasalahan ini adalah tingginya risiko terhadap keamanan data pengguna, kemungkinan pencurian identitas, dan kerusakan integritas sistem, yang dapat menurunkan kepercayaan publik serta menimbulkan kerugian finansial dan reputasi bagi instansi tersebut (Kade et al., 20), dalam hal ini termasuk bagi pihak Dispusip. Dasar inilah yang mendorong agar dilakukan analisis keamanan pada *website* Dispusip guna mengetahui celah dan kerentanan yang ada pada *website* tersebut, selain itu terdapat data penting berupa data pengunjung dan Arsip dari Dinas Perpustakaan dan Kearsipan Kota Surabaya oleh

karena itu pengujian untuk mengetahui celah keamanan sangat diperlukan. Pengujian akan dilakukan dengan menggunakan metode *Penetration testing. Penetration testing* merupakan sebuah simulasi serangan yang terkendali dengan tujuan untuk melakukan identifikasi kerentanan terhadap aplikasi, *website*, jaringan dan cabang sistem informasi (Andriyani, et al., 2023). Hal ini dilakukan agar jika terdapat celah keamanan, maka akan dapat teridentifikasi serta ditangani lebih awal sebelum celah tersebut dimanfaatkan oleh orang yang tidak bertanggung jawab (Andriyani et al., 2023).

Pengujian ini akan menggunakan *framework The Information System Security Assesment* (ISSAF). ISSAF merupakan kerangka terstruktur yang mengategorikan penilaian keamanan sistem informasi dalam berbagai domain dan rincian kriteria (Prasetyo et al., 2021). *Framework* ISSAF sendiri terbagi atas 3 tahapan besar, pertama pengumpulan semua informasi terkait *website* yang akan dianalisis kerentanannya. Kedua mencari kerentanan yang ada pada *website* tersebut, dan yang terakhir pihak penguji akan membuat laporan terhadap *website* yang diuji (Prasetyo et al., 2021). *Framework* ISSAF memiliki kelebihan yaitu penggunaan ISSAF memiliki kesesuaian untuk memenuhi persyaratan penilaian keamanan organisasi dan dapat dijadikan acuan untuk memenuhi persyaratan keamanan informasi lainnya sehingga membantu dalam menentukan prioritas dan rekomendasi perbaikan keamanan (Rohim et al., 2023). Selain itu ISSAF dipilih karena bersifat *opensource*, bebas digunakan oleh siapa saja, tidak mengharuskan untuk menggunakan suatu *tools* tertentu, melainkan memberikan pilihan *tools* yang dapat digunakan sesuai dengan tujuan dan sasaran penelitian. Jika dibandingkan dengan salah satu metode lainnya seperti OWASP, OWASP tidak memiliki tahapan yang sistematis sehingga harus menentukan sendiri langkah-langkah yang akan digunakan sesuai dengan tujuan penelitian (Thamrin et al., 2023). Fokus penelitian ini adalah pengujian keamanan sistem *website* Dispusip yang dilakukan menggunakan metode *penetration testing* berdasarkan *framework* ISSAF, Pengujian testing dilakukan dengan lebih dari 1 metode penyerangan sehingga kemungkinan gagal atau tidak ditemukannya kerentanan sangat kecil, dan apabila tidak ditemukan celah kerentanan sama sekali maka akan tetap dilakukan prosedur atau tahap yang sesuai dengan metode ISSAF yaitu pembuatan

laporan. Tujuan dari penelitian ini adalah untuk menemukan aspek kerentanan pada *website* berdasarkan *framework* ISSAF, sehingga penelitian ini dapat memberikan rekomendasi perbaikan untuk meningkatkan keamanan pada *website* Dinas Perpustakaan dan Arsip Kota Surabaya (Aldo Fajarino 2023; Umar et al. 2023).

I.2 Perumusan Masalah

Dari permasalahan pada latar belakang dapat diambil rumusan masalah sebagai berikut:

1. Bagaimana tahapan *penetration testing* dapat bekerja sesuai dengan *framework* ISSAF pada *website* Dinas Perpustakaan dan Kearsipan Kota Surabaya?
2. Apakah terdapat celah keamanan yang ditemukan pada *website* Dinas Perpustakaan dan Kearsipan Kota Surabaya?
3. Apa saja rekomendasi perbaikan yang dapat disarankan untuk meningkatkan keamanan *website* Dinas Perpustakaan dan Kearsipan Kota Surabaya?

I.3 Tujuan dan Manfaat

Berdasarkan rumusan masalah maka terdapat tujuan penelitian, yakni sebagai berikut:

1. Menyusun tahapan *penetration testing* yang bekerja sesuai dengan *framework* ISSAF pada *website* Dinas Perpustakaan dan Kearsipan Kota Surabaya.
2. Menganalisis celah keamanan yang ada pada *website* Dinas Perpustakaan dan Kearsipan Kota Surabaya.
3. Merumuskan rekomendasi perbaikan berdasarkan uji penetrasi (*penetration testing*) untuk meningkatkan keamanan *website* Dinas Perpustakaan dan Kearsipan Kota Surabaya.

Adapun manfaatnya yaitu sebagai berikut:

1. Penelitian ini dapat membantu pihak Dinas Perpustakaan dan Kearsipan Kota Surabaya untuk mengidentifikasi dan memperbaiki celah keamanan yang ada, meningkatkan keamanan data dan informasi yang ada pada *website.*
2. Penelitian ini dapat menjadi bahan referensi dan studi kasus bagi pihak kampus, terutama dalam pengembangan kurikulum dan literatur terkait keamanan siber.
3. Penelitian ini meningkatkan pengetahuan dan keterampilan peneliti dalam bidang *penetration testing* dan keamanan informasi. Melalui penelitian ini juga, peneliti mendapatkan pengalaman berharga yang menjadi nilai tambah dalam dunia pekerjaan.

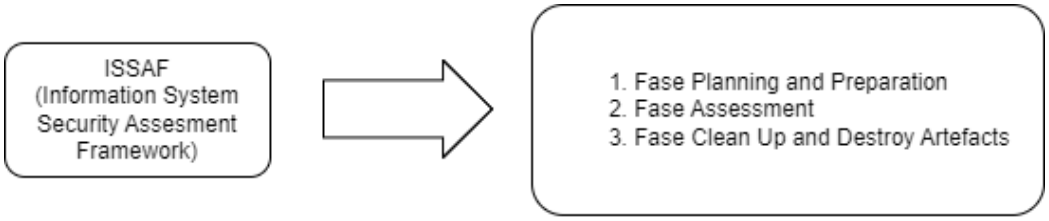
I.4 Batasan Masalah

Adapun batasan masalah sebagai berikut:

1. Metode *penetration* testing hanya dilakukan dengan *frameworf* ISSAF dan pengujian *black box* dari sisi pengunjung *website* Dispusip.
2. Penelitian ini akan dilakukan dalam kurun waktu tertentu agar relevan dengan tujuan penelitian, serta untuk memastikan fokus dan kedalaman analisis yang optimal.
3. Hasil penelitian berupa rekomendasi perbaikan untuk pihak Dins Perpustakaan dan Kearsipan Kota Surabaya.

I.5 Metologi Penelitian

Penelitian ini menggunakan metode ISSAF *(Assessment Framework for Information System Security)*, yang dipilih karena bersifat *opensource* dan dapat diakses oleh siapa saja. Untuk membantu penguji menghindari kesalahan yang sering terjadi metode ISSAF menjelaskan proses pengujian penetrasi yang ideal. Selama uji penetrasi, metode ISSAF memiliki tiga Fase yang harus dilakukan, masing-masing dengan tujuan untuk membantu dan membimbing penguji dapat dilihat pada gambar Gambar I.1.



Gambar I.1 Fase Proses Pengujian Metode ISSAF

Fase *Information System Security Assessment* adalah sebagai berikut :

1. **Fase 1 (*Planning and Preperation*)** terdiri dari *information gathering* dan *network mapping*

   a. Information Gathering

   Pada tahap ini, internet digunakan untuk mendapatkan informasi sebanyak mungkin dari target, yaitu perusahaan atau individu. Metode teknikal *(DNS/WHOIS)* dan non-teknikal *(Search)* digunakan untuk mendapatkan informasi ini. *Engine*, daftar e-mail, dan lainnya. Mengumpulkan informasi tidak dibutuhkan untuk menentukan bagaimana sistem target berhubungan satu sama lain. Sumber-sumber publik seperti internet dan organisasi yang memiliki sumber data publik, seperti perpustakaan dan sumber daya lainnya.

   b. *Network Mapping*

   Pada tahap ini, *"Footprint"* akan diletakkan pada sistem atau jaringan yang diinginkan adalah langkah teknikal yang dapat diambil setelah data telah dikumpulkan. *Network Mapping* harus dilakukan untuk hasil yang lebih baik serta sesuai dengan rencana. Rencana ini mencakup titik potensial terlemah atau yang paling berharga dari perusahaan.

2. **Fase 2 (*Assessment*)** terdiri dari *vulnerability identification, penetration, gaining access, enumerate further, compromise remote user, maintaining access.*

   a. *Vulnerability Identification*

   Penguji akan melakukan berbagai tugas untuk mengidentifikasi kerentanan sistem.

   b. *Penetration*

Penguji akan mencoba mendapatkan akses ilegal dengan mengakali sistem keamanan dan mendapatkan level akses seluas mungkin.

c. Gaining Access & Privilege Escalation

Dalam beberapa keadaan, sistem dapat dievaluasi lebih jauh. Ini memungkinkan penguji untuk memastikan dan mendokumentasikan kemungkinan gangguan dan serangan otomatis. Selain itu hal Ini memungkinkan hasil pengujian yang lebih baik untuk target secara mendalam.

d. *Enumerate Further*

Dalam tahap ini, penguji akan mendapatkan informasi tambahan berdasarkan proses pada sistem.

e. Compromise Remote User/Sites

Tidak peduli seberapa aman sebuah jaringan, satu kerentanan saja cukup untuk membuka akses ke seluruh jaringan. Penguji dapat mencoba menggunakan pengguna jauh untuk mendapatkan akses ke jaringan yang lebih dalam.

f. *Maintaining Access*

Penguji dapat kembali ke dalam sistem, bahkan jika sistem yang diuji tidak ada lagi, dengan *backdoor*, yang dapat dibuat dengan berbagai cara, seperti menggunakan *root-kit* untuk mengizinkan sistem target terkoneksi dengan server penguji, dan sebagainya.

3. Fase 3 terdiri dari *covering track, reporting dan clean and destroy artefacts.*

a. *Covering the Track*

Pada tahap ini, penguji akan menghapus informasi sebelumnya dengan menyembunyikan file dan menghapus file log.

b. *Reporting*

Pada tahap ini, penguji akan menulis laporan yang menjelaskan hasil pengujian bersama dengan rekomendasi saran untuk menyelesaikannya.

c. *Clean and Destroy Artefacts*

Pada tahap ini, semua informasi yang telah dibuat atau disimpan di sistem harus dihapus. Jika ini tidak mungkin dilakukan melalui sistem jauh, hal ini harus diberitahukan kepada pihak yang diuji agar staf IT pihak tersebut dapat menghapus informasi tersebut setelah menerima laporan.