terdapat dalam website sistem informasi. Untuk mengetahui celah keamanan yang ada peneliti menggunakan metode *penetration testing* dengan *framework* ISSAF.

Berdasarkan uraian di atas maka penulis ingin melakukan penelitian mengenai keamanan *website* untuk mengetahui sejauh mana keamanan yang dimiliki oleh situs *web*. Maka dari itu penulis tertarik untuk melakukan penelitian dengan judul "Analisis Kualitas Keamanan *Website E-ticketing* Indonesia Menggunakan Metode Uji Penetrasi *Information Systems Security Assessment Framework* (ISSAF)" Penelitian ini menggunakan metode *Penetration Testing* berjenis *Information System Security Assessment Framework* (ISSAF) melakukan pengujian terhadap *website ticketing online* Indonesia untuk mengukur sejauh mana keamanan yang dimiliki oleh *website ticketing online*.

1.2 Rumusan Masalah

Rumusan masalah ini disusun berdasarkan latar belakang yang telah dibahas sebelumnya, berikut ini merupakan rumusan masalah yang telah disusun:

1. Bagaimana proses uji penetrasi keamanan *website e-ticketing* Indonesia menggunakan metode *information systems security assessment framework* (ISSAF**)**?
2. Bagaimana hasil pengujian keamanan *website e-ticketing* Indonesia menggunakan metode *information systems security assessment framework* (ISSAF**)**?

1.3 Batasan Penelitian

Guna memastikan tercapainya tujuan utama penelitian, pembahasan tidak meluas, dan permasalahan tidak menyimpang, maka ditetapkan batasan masalah penelitian tugas akhir ini, antara lain:

1. Penelitian ini melakukan analisis kualitas keamanan *website* terhadap *website e-ticketing* Indonesia pada domain *Ticket.com, Traveloka.com, PegiPegi.com, Booking.com,* dan *Agoda.com.*

2. Penelitian dilakukan dengan mengacu pada metodologi *Penetration Testing* berjenis *Information System Security Assessment Framework* (ISSAF) melakukan pengujian terhadap *website e-ticketing* Indonesia.
3. Analisis kualitas keamanan dilakukan berdasarkan tahapan *Fase planning and preparation, Fase assessment dan Fase reporting*
4. Analisis penetrasi mencangkup pengujian pada *information gathering, network mapping, vulnerability identification, penetration testing* dan aspek-aspek lain yang terkait dengan pengalaman pengguna.
5. Tools yang digunakan untuk memperoleh data adalah Whois Domain, IP Lookup Scanner, SSL Labs, What CMS, NMap, dan OwaspZap.

1.4 Tujuan Penelitian

Tujuan penelitian analisis kualitas keamanan menggunakan metodologi *Information System Security Assessment Framework* (ISSAF) adalah untuk melihat sejauh mana kualitas keamanan pada aplikasi *web e-ticketing* Indonesai. Tujuan spesifik dari penelitian analisis kualitas keamanan *website e-ticketing* Indonesia yaitu:

1. Mengetahui proses uji penetrasi keamanan *website e-ticketing* Indonesia menggunakan metode *information systems security assessment framework* (ISSAF**)**
2. Mengetahui hasil pengujian keamanan *website e-ticketing* Indonesia menggunakan metode *information systems security assessment framework* (ISSAF**)**

1.5 Manfaat Penelitian

Manfaat dari penelitian mengenai Analisis Kualitas Keamanan *Website e-ticketing* Indonesia Menggunakan Metode *Information Systems Security Assessment Framework* (ISSAF**)** adalah:

1. Bagi Peneliti
   a. Untuk mengetahui kualitas keamanan dari lima *website e-ticketing* serta mengetahui bagaimana penggunaan metode penetrasi testing berjenis *Information System Security Assessment Framework* (ISSAF)

b. Untuk mengetahui *website* mana yang lebih aman digunakan pada saat memesan tiket secara *online* pada lima domain *website* Indonesia (Tiket.com, Traveloka.com, Pegipegi.com, Booking.com, dan Agoda.com) yang telah diuji keamanannya.

2. Bagi Perusahaan

   Sebagai anjuran dan penjelasan tambahan pada perusahaan ataupun pihak berkepentingan lainnya yang ada didalam perusahaan, dan juga dapat dimanfaatkan sebagai bahan peninjauan untuk mengadakan pembaharuan terhadap *website e-ticketing.*

3. Bagi Penelitian Selanjutnya

   Penelitian ini dapat diaplikasikan untuk masukkan ataupun tambahan referensi. Selain itu juga sebagai bahan untuk membandingkan dengan hasil penelitian lain bagi peneliti berikutnya yang ingin melakukan penelitian pada bidang yang sama di kemudian hari.

BAB II
TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 Keamanan Sistem informasi

Keamanan sistem informasi merupakan keamanan informasi yang terdapat pada komputer atau jaringan. Keamanan komputer bertujuan membantu pengguna agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang berbasis informasi. Informasinya sendiri memiliki arti nonfisik. Keamanan komputer adalah suatu cabang teknologi yangdikenal dengan nama keamanan informasi yang diterapkan pada komputer.Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasiterhadap pencurian atau korupsi, atau pemeliharaan ketersediaan, seperti dijabarkan dalam kebijakan keamanan.

Penerapan *computer security* dalam kehidupan sehari-hari berguna sebagai penjaga sumber daya sistem agar tidak digunakan, modifikasi, interupsi dan diganggu oleh orang yang tidak berwenang. Keamanan dapat diidentifikasi dalam masalah teknis, manajerial, legalitas dan politis. Keamanan komputer berfungsi untuk melindungi berbagai informasi yang terdapat di dalam komputer dari tindakan *cyber-crime* atau *cyber-attack*. Komputer dikatakan aman jika bisa diandalkan dan perangkat lunaknya bekerja sesuai dengan yang diharapkan. Keamanan komputer memiliki 5 tujuan, yaitu *Availability, Integrity, Control, Audit, Confidentiality*. (Rosadi, 2022)

2.1.2 Penetration Testing

Penetration testing adalah metode untuk menguji kerentanan dalam sistem, identifikasi konfigurasi sistem yang buruk, kecacatan perangkat keras dan perangkat lunak serta kelemahan teknis pada sistem informasi yang diujikan (Hussain, 2017). *Penetration testing* merupakan suatu kegiatan berupa simulasi yang dilakukan oleh pihak yang sudah memiliki izin untuk melakukan eksploitas suatu sistem berdasarkan celah keamanan yang ada. *Penetration testing* berbeda