BAB I
PENDAHULUAN

1.1 Latar Belakang masalah

Dinas Komunikasi dan Informatika Kota Bandung merupakan sebuah instansi yang bertanggung jawab atas pengolahan informasi dilingkungan kota Bandung. *Website* pun merupakan kebutuhan yang sangat penting di instansi pemerintah khususnya Dinas Komunikasi dan Informatika kota Bandung. Dengan adanya *Website* DISKOMINFO, aliran informasi, komunikasi dan transaksi antara masyarakat dan pemerintah dapat dilakukan dengan mudah. Manfaat *Website* DISKOMINFO diantaranya: sebagai media penyampaian informasi secara resmi dari pemerintah kota Bandung kepada masyarakat, sebagai media interaksi dengan masyarakat, menjadi tolak ukur bagaimana aktif atau tidaknya kegiatan pemerintahan, sebagai tempat masyarakat menyampaikan aspirasinya, memudahkan rakyat untuk mengenal pemimpinnya dan sebagai media promosi. Tetapi, dibalik berbagai macam manfaat, terdapat beberapa kelemahan. Hal ini dapat berbahaya berhubung informasi dan data yang dimiliki suatu instansi khususnya instansi pemerintah tidak semuanya bersifat terbuka.

Tetapi, dibalik banyaknya manfaat, terdapat juga ancaman-ancaman yang dapat terjadi. Berdasarkan data yang di dapat dari Direktorat *Cyber Crime* Indonesia, pada tahun 2015-2016 di Indonesia terdapat 2880 kasus *Cyber Crime* [1]. Pada bulan Mei 2017, terjadi sebuah serangan siber *Ransomware Wannacry* yang menyebabkan gangguan pada perusahaan dan rumah sakit di lebih dari 150 negara [2]. Serangan tersebut membuka mata dunia dan menjadi langkah awal untuk bekerja sama dalam keamanan siber.

Berdasarkan hasil wawancara dengan seorang pegawai Dinas Komunikasi Dan Informatika Kota Bandung, terdapat kurang lebih 105 *Website* yang memiliki keterkaitan dengan Dinas Komunikasi Dan Informatika. Dipaparkan bahwa pada sepanjang tahun 2016 terdapat beberapa kali serangan terhadap *Website* yang memiliki keterkaitan dengan Dinas Komunikasi Dan informatika Kota Bandung. Hal ini memberikan kesadaraan bahwa terdapatnya kerentanan pada *Website*

DISKOMINFO, yang jika tidak segera ditanggulangi, akan mengakibatkan kerusakan pada data yang ada di *Website* tersebut.

Sistem Keamanan Komputer dapat dikatakan sebuah cara yang dibuat untuk mengamankan fungsi, data, performa, atau proses yang ada pada sebuah sistem komputer. Sebuah percobaan harus dilakukan untuk mengetahui apakah sebuah *website* aman atau tidak dari aksi-aksi berbahaya yang dilakukan oleh penyerang [3]. Salah satu cara untuk mengetahui apakah sistem kita aman atau tidak ialah dengan melakukan *Penetration Testing.*

Penetration Testing dapat dikatakan sebuah cara yang legal dan resmi untuk menemukan dan mengeksploitasi sistem komputer yang bertujuan untuk menjadikan sistem tersebut lebih aman [4]. Tetapi pada beberapa kasus, kerentanan yang didapat dari *Penetration Testing* justru dimanfaatkan oleh pihak yang tidak bertanggung jawab. Oleh karena itu sangat penting untuk meminta izin kepada pihak yang ingin di *Penetration Testing* [5].

Penetration Testing Execution Standard (PTES) belakangan muncul sebagai salah satu *Framework* untuk *Penetration Testing.* Walaupun *Framework* ini masih dalam tahap pengembangan, menyediakan sebuah metode yang sangat terstruktur untuk memotivasi komunitas yang bertujuan untuk mengidentifikasi apa itu *Security Assesment.*

Information Systems Security Assessment Framework (ISSAF). merupakan sebuah *framework* terstruktur dari *Open Information System Security Grop* yang mengelompokkan penilaian informasi keamanan sistem kedalam beberapa domain dan menilai detail secara spesifik atau kriteria pengujian setiap domain [6].

Open Web Application Security Project (OWASP) adalah sebuah komunitas yang bebas dan terbuka di seluruh dunia terfokus pada peningkatan keamanan perangkat lunak aplikasi. Misi OWASP adalah untuk membuat aplikasi keamanan "terlihat", sehingga orang-orang dan organisasi dapat membuat keputusan tentang risiko keamanan aplikasi. Hasil yang dilakukan dari pengujian OWASP ini akan dipetakan menggunakan parameter penilaian *Risk Rating*. *Risk Rating* adalah parameter penilaian yang digunakan untuk mengukur tingkat suatu resiko. Pada metodologi ini resiko (*risk*) adalah hasil kali kemungkinan (*Likelihood*) dengan

dampak (*Impact*). Hasil dari pengujian tersebut akan dijadikan parameter penilaian seberapa tinggi tingkat keamanan suatu web.

Berdasarkan masalah yang terjadi di Dinas Komunikasi Dan Informatika Kota Bandung maka penelitian yang diambil ialah "**ANALISIS PERBANDINGAN METODE WEB SECURITY PTES (*PENETRATION TESTING* EXECUTION AND STANDARD), ISSAF (INFORMATION SYSTEMS SECURITY ASSESSMENT *FRAMEWORK*) DAN OWASP DI DINAS KOMUNIKASI DAN INFORMASI KOTA BANDUNG.**"

1.2 Identifikasi Masalah

Dari latar belakang kita dapat jabarkan masalah-masalah yang dihadapi oleh Dinas Komunikasi Dan Informatika Kota Bandung :

1. Adanya kerentanan pada *Website* Dinas Komunikasi Dan Informatika Kota Bandung . dan mencari perbedaan dari 3 *Framework Penetration Testing* yang akan digunakan yaitu PTES (*Penetration Testing Execution Standard*), ISSAF (*Information Systems Security Assessment Framework*) dan OWASP (*Open Web Application Security Project*)
2. Belum adanya panduan dalam pengelolaan resiko pada *Website* yang berkaitan dengan DISKOMINFO Kota Bandung

1.3 Maksud dan Tujuan

Maksud dari penelitian ini adalah untuk menganalisis kerentanan terhadap *Website* yang berkaitan dengan Dinas Komunikasi Dan Informatika Kota Bandung.

Sedangkan tujuan yang akan dicapai pada penelitian yang akan dilakukan adalah sebagai berikut:

1. Melakukan analisis kerentanan pada *Website* Dinas Komunikasi dan Informatika Kota Bandung, dan mendapatkan perbedaan dari 3 *Framework* yaitu PTES (*Penetration Testing Execution Standard*), ISSAF (*Information Systems Security Assessment Framework*) dan OWASP (*Open Web Application Security Project*)

2. Memberikan saran dan rekomendasi serta laporan sebagai acuan untuk keamanan web yang berhubungan dengan DISKOMINFO Kota Bandung

1.4 Batasan Masalah

Dalam penyelesaian proposal tugas akhir ini diberikan batasan masalah agar tujuan dan sasaran yang diinginkan dapat tercapai. Adapun batasan masalah sebagai berikut :

a. *Website* yang diuji adalah ialah *Website* DISKOMINFO kota Bandung
b. Pengujian pada tahap *Exploitation*, akan menggunakan SQL Injecation.
c. Pengujian dilakukan dengan 3 *Framework* , yaitu *Penetration Testing Execution Standard (PTES), Information Systems Security Assesment Framework (ISSAF), dan Open Web Application Security Project (OWASP).*

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan ialah metode penelitian kualitatif, yaitu penelitian tentang riset yang bersifat deskriptif dan cenderung menggunakan analisis.

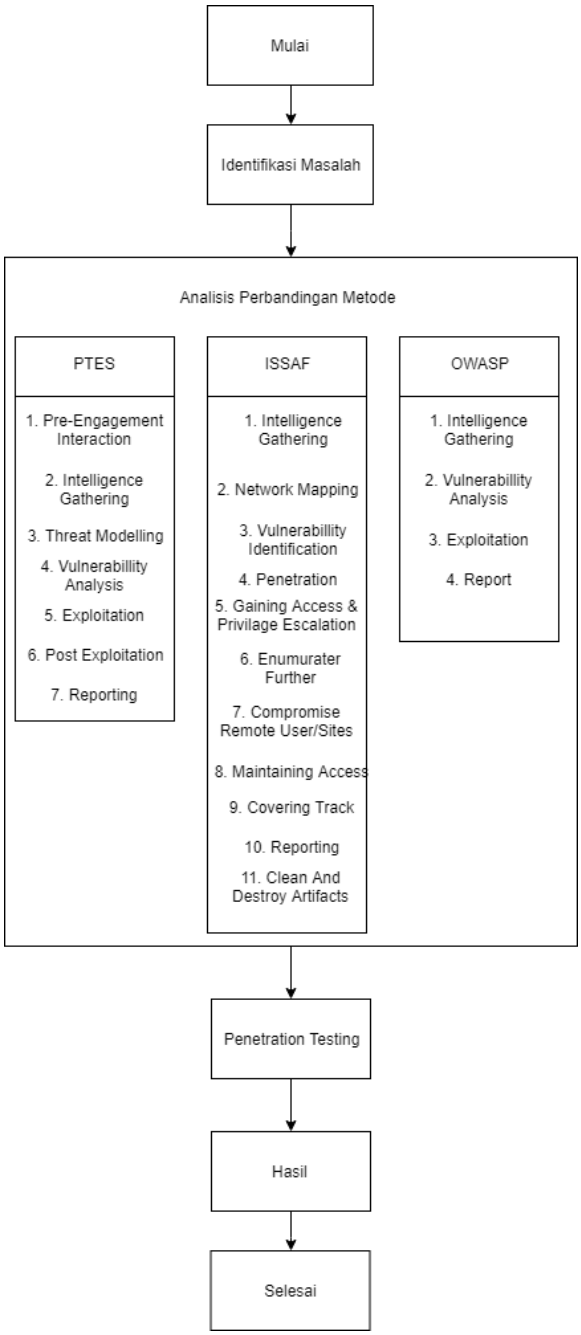
1.6 Metode Pengumpulan Data

Metode pengumpulan data adalah tahap awal dalam melakukan suatu penelitian. Metodologi yang digunakan dalam mengumpulkan data yang berkaitan dengan penyusunan laporan sebagai berikut :

1. Studi Literatur

   Studi literatur adalah tahap pengumpulan data yang diperoleh dengan cara mempelajari keamanan web dan langkah-langkah yang akan ditempuh dalam analisis web security.

1.7 Alur Penelitian



Gambar 1. 1 Alur Penelitian

1. Identifikasi Masalah

   Pada tahap ini, peneliti bekerja sama dengan pihak diskominfo untuk mengidentifikasi masalah – masalah yang terdapat pada *Website* DISKOMINFO Kota Bandung.

2. Analisis Perbandingan Metode

   Peneliti melakukan perbandingan antara ketiga metode yang digunakan.

3. *Penetration Testing*

   Dalam tahap ini peneliti akan melakukan uji kerentanan pada *Website* yang telah ditentukan. Pemeriksaan mengenai kerentanan dilakukan dengan menggunakan *tools* yang akan disesuaikan.

4. Hasil

   Dalam tahap ini, penguji mendapatkan hasil dari perbandingan ke tiga metode dan mendapatkan hasil dari *Penetration Testing*

1.8 Sistematika Penulisan

Sistematika penulisan ini bertujuan untuk memberikan gambaran umum tentang penulisan tugas akhir yang akan dilakukan. Sistematika penulisan tugas akhir ini adalah sebagai berikut.

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang permasalahan, perumusan masalah, menentukan maksud dan tujuan, batasan masalah, metodologi penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas tentang profile dari DISKOMINFO Kota Bandung, struktur organisasi, deskripsi jabatan, dan teori – teori pendukung yang akan membantu di dalam penelitian ini.

BAB III ANALISA DAN PERANCANGAN SISTEM

Bab ini berisi tentang analisis masalah dan skenario analisis vulnerability assessment yang meliputi analisis masalah yang terjadi dan melakukan testing untuk menentukan vulnerability yang terdapat pada sistem.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini merupakan tahap implementasi dan pembahasan hasil yang didapat dari analisis berdasarkan metode yang digunakan.

BAB V KESIMPULAN DAN SARAN

Dalam bab ini berisi mengenai kesimpulan yang dapat diambil dari semua yang telah dikerjakan serta saran yang dapat diberikan untuk proses pengujian berikutnya agar sistem menjadi lebih baik