BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Dinas Komunikasi, Informatika dan Statistika Kabupaten Bandung merupakan sebuah instansi yang bertanggung jawab atas pengolahan informasi di lingkungan kabupaten Bandung. *Website* pun merupakan kebutuhan yang sangat penting di instansi pemerintah khususnya Dinas Komunikasi, Informatika dan Statistika Kabupaten Bandung. Dengan di sediakannya *website* Pemerintahan alur Komunikasi dan transaksi antara masyarakat dan pemerintah dapat dilakukan dengan mudah.

Namun dengan semakin banyaknya fasilitas *website* yang disediakan untuk mendukung program kerja Diskominfo Kabupaten Bandung dalam melayani masyarakat, Ancaman akan kejahatan dunia maya pun menjadi salah-satu masalah yang harus dihadapi secara seksama. Berdasarkan data yang didapat dari Indonesia *Security Incident Response Team on Internet and Infrastructure/Coordination Center* (Id-SIRTII/CC) yang merupakan badan yang dibentuk untuk melakukan pengawasan keamanan jaringan telekomunikasi berbasis protokol internet. Diketahui dari data yang diolah oleh Direktorat *Cyber Crime* Indonesia kasus *Cyber Crime* yang terjadi di indonesia pada tahun 2016 adalah 2880 kasus [1]. Dampak kejahatan di dunia maya yang mempengaruhi sektor ekonomi berdasarkan data dari Norton *Symantec* selama tahun 2015 sampai dengan Februari 2016 di Indonesia menimbulkan total kerugian Rp 194.6 miliar [2]. Oleh karena itu penanggulangan terhadap *Cyber Crime* perlu ditanggulangi secara seksama.

Berdasarkan hasil wawancara dengan pihak dari Dinas Komunikasi, Informatika dan Statistika Kabupaten Bandung, bidang TIK bagian Keamanan Informasi, beliau menegaskan bahwa sudah pernah terjadi *Cyber Attack* yang di lakukan terhadap *website* Pemerintahan Kabupaten Bandung. Eksploitasi ini

terjadi 2 kali di tahun 2017 dengan tipe eksploitasi berupa *web deface,* diduga penyerangan ini dilakukan individual untuk melakukan eksploitasi dan menampilkan *skill* yang dimiliki para penyerang dalam menyerang *website-website* rentan akan eksploitasi, sehingga dibutuhkannya analisis kerentanan pada *website-website* yang dikelola oleh Dinas Komunikasi, Informatika dan Statistika Kabupaten Bandung, dengan tujuan agar dapat mengetahui kerentanan yang terdapat pada *website-website* tersebut, sehingga dapat mengurangi penyerangan terhadap *website* yang dikelola Diskominfo Kabupaten Bandung dan. *National Institute of Standards and Technology* (*NIST*) merupakan badan non-regulator dan bagian ari administrasi teknologi dan departemen perdagangan Amerika Serikat. Misi dari organisasi ini adalah untuk membuat dan mendorong pengukuran , standar dan teknologi untuk meningkatkan produktivitas, mendukung perdagangan dan kualitas hidup. Empat bidang utama organisasi ini adalah bioteknologi, nanoteknologi, teknologi informasi dan manufakturing moderen. NIST mengeluarkan beberapa seri publikasi yang ditujukan ke keempat bidang tersebut dan salah satunya yang menjurus ke dalam bidang teknologi informasi adalah *NIST SP 800-115 Techincal Guide to Information Security Testing and Assessment,* metodologi yang dikhususkan untuk membatu organisasi dalam melakukan perencanaan tes keamanan informasi [3].

Berdasarkan masalah yang terjadi di Dinas Komunikasi Dan Informatika Kabupaten Bandung maka dilakukan penelitian dengan judul "**Analisis Kerentanan Website Menggunakan Metode NIST SP 800-115 dan OWASP di Diskominfo Kabupaten Bandung**" dengan harapan dapat membatu membantu menanggulangi penyerangan terhadap *website* yang dikelola oleh Dinas Komunikasi, Informatika dan Statistika Kabupaten Bandung.

1.2 Identifikasi Masalah

Dari latar belakang kita dapat jabarkan masalah-masalah yang dihadapi oleh Dinas Komunikasi, Informatika dan Statistika Kabupaten Bandung :

1. Masih terdapatnya *website* pemerintahan yang memiliki kerentanan dan berhasil di *deface* sehingga menimbulkan kerugian.
2. Masih terdapat beberapa website yang belum melakukan pengujian S*ecurity Assessment*
3. Belum adanya panduan/prosedur untuk menangani *website* yang memiliki kerentanan.

1.3 Maksud dan Tujuan

Maksud dari penelitian ini adalah untuk menganalisis kerentanan yang terdapat pada *website* di bawah pengawasan Diskominfo Kabupaten Bandung menggunakan metode NIST SP 800-115 dan OWASP serta saran dalam melakukan penanggulangannya.

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

1. Melakukan analisis terhadap kerentanan *website* yang dikelola oleh Diskominfo Kabupaten Bandung.
2. Melakukan pengujian *Security Assessment* pada *website* yang dikelola Diskominfo Kabupaten Bandung
3. Memberi saran / rekomendasi atau informasi untuk menangani kerentanan yang terdapat pada *website* di bawah pengawasan Diskominfo Kabupaten Bandung.

1.4 Batasan Masalah

Pada penelitian ini terdapat batasan masalah agar tujuan dan sasaran yang diinginkan dapat tercapai. Adapun batasan masalah sebagai berikut :

1. Pengujian dilakukan dalam ruang lingkup aplikasi *website*.
2. Pengujian dilakukan dengan *Black Box Testing.*

3. *Penetration Testing* di lakukan menggunakan Metode *NIST SP 800-115*.
4. *Website* yang diuji berjumlah 5 domain dari daftar domain yang diberikan oleh petugas Diskominfo Kabupaten Bandung termasuk domain yang pernah diserang.
5. *Website* yang diuji adalah *website* yang tersedia secara online
6. Dibangunnya Aplikasi untuk *list* kerentanan dan *Risk Rating.*
7. *Dilakukan tahapan Riks Rating* untuk *website* yang diuji dengan menggunakan perhitungan OWASP *Risk Rating Methodology.*
8. Mekanisme yang menghubungkan Metode NIST SP 800-115 dan OWASP *Risk Rating Methodology* hanya mengcangkup bagian Likelihood OWASP Risk Rating Methodology pada bagian *Vulnerabily Factor* poin *Ease of Disecovery* dan poin *Ease of Exploit*.
9. Hasil dari penelitian ini adalah berupa hasil analisis dan laporan kerentanan dalam bentuk aplikasi yang akan menunjukkan grafik kerentanan dan *Risk Rating* menggunakan bahasa pemogramman *C#*.

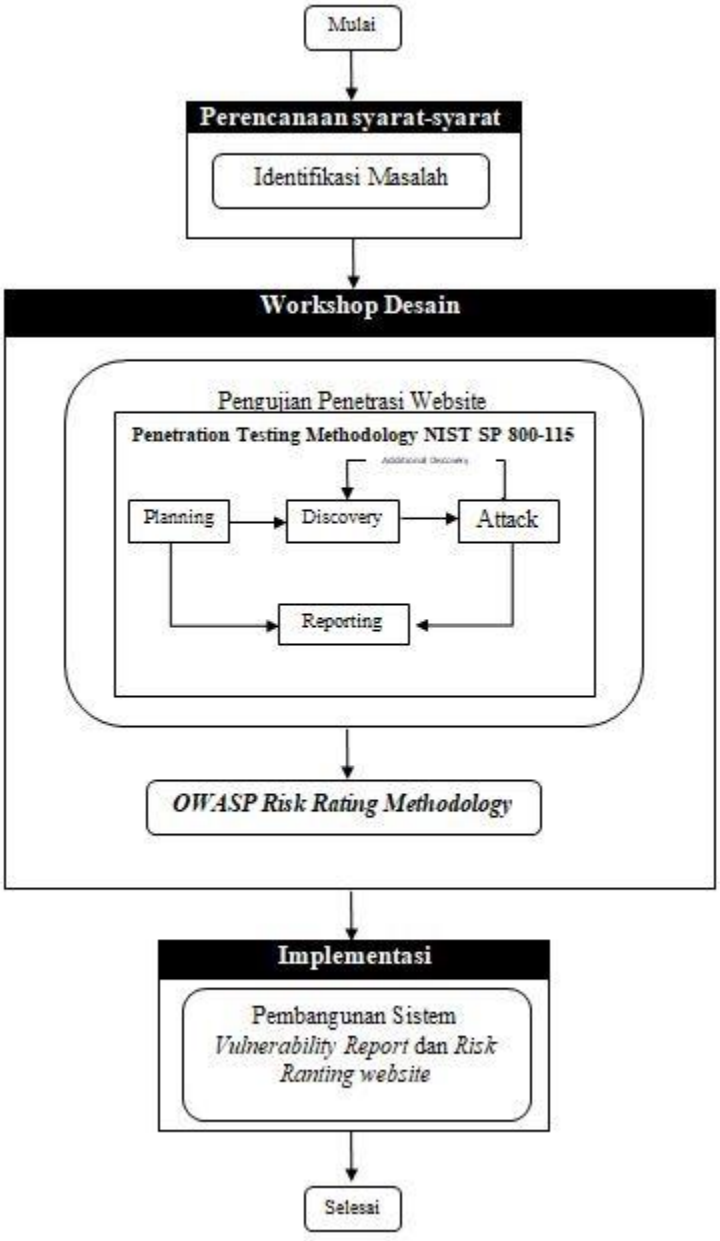
1.5 Metodelogi Penelitian

Metode pengumpulan data yang di gunakan adalah Metode kualitatif karena dibutuhkan wawancara dengan pihak Diskominfo Kabupaten Bandung kemudian dilanjutkan dengan observasi terhadap aplikasi *website* yang diuji dan menganalisis kerentanan yang ditemui di dalam *website* tersebut.

Agar penelitian ini dapat berjalan sebagaimana mestinya maka akan digunakan metode NIST SP 800-115 dalam pelaksanaan *Penetration Testing* yang akan dilanjutkan dengan memberikan peringkat terhadap *website* yang diuji menggunakan OWASP *Risk Rating Methodology*

1.6 Alur Penelitian

Berikut merupakan tahapan penelitian yang dilakukan dalam penelitian ini :



Gambar 1. 1 Alur Penelitian

1. Perencanaan syarat-syarat

Tahapan pertama dalam metode pembangunan perangkat lunak *Rapid Application Development* adalah Perencanaan Syarat-syarat,

dilakukan identifikasi masalah yang berkaitan dengan *website-website* pemerintahan di bawah pengawasan Diskominfo Kabupaten Bandung.

2. *Workshop* Desain

Tahap kedua dalam metode *Rapid Application Development adalah Workshop* Desain. Dalam penelitian ini tahapan *Workshop* Desain terdiri dari analisis kerentanan *website* dengan melakukan tahapan sebagai berikut:

- Pengujian penetrasi pada *website*

  Dalam tahapan ini dilakukan uji penetrasi terhadap *website* yang di kelola oleh Diskominfo Kabupaten Bandung baik yang pernah diserang maupun yang belum diserang. Dalam uji penetrasi ini, metode yang digunakan adalah metode NIST SP 800-115. Metode ini terdiri dari beberapa tahapan sebagai berikut

  1) Planning

  Dalam tahapan *planning* peneliti bekerja sama dengan pihak Diskominfo dalam perizinan penelitian, menetapkan metode, menetapkan aturan keterlibatan peneliti dengan pihak Diskominfo dan ruang lingkup penelitiannya

  2) Discovery

  Dalam tanhapan *Discovery* terdapat dua tahapan yaitu pertama melakukan testing terhadap *website*, *information gathering* dan melakukan *scanning* pada *website*. Tahapan selanjutnya adalah melakukan analisis terhadap kerentanan yang terdapat pada *website*

  3) Attack

  Tahapan *Attack* merupakan inti dari pengujian Penetrasi yang dilakukan pada *website*. Di mana kerentanan akan verifikasi, melakukan eksploitasi dan penyerangan untuk mendapatkan

hak akses dari *website* tersebut. Di dukung dengan *PoC* yang tersedia.

4) Report

Dalam tahapan *Report*, hasil analisis kerentanan yang telah di verifikasi akan dilaporkan kepada pihak Diskominfo Kabupaten Bandung.

- OWASP *Risk Rating Methodologhy*

  Dalam tahapan ini akan dilakukan perhitungan *Risk Rating* menggunakan OWASP *Risk Rating Methodologhy*

3. Implementasi

   Dalam tahapan ini akan dilakukan penerapan berdasarkan hasil pengujian sistem dan analisis kerentanan *website* di bawah pengawasan Diskominfo Kabupaten Bandung ke dalam sistem yang dapat menampilkan laporan mengenai kerentanan *website*, grafik kerentanan dan melakukan proses *Risk Rating*.

1.7 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 TINJAUAN PUSTAKA

Bab ini membahas tentang profil dari Diskominfo Kabupaten 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 analisis *vulnerability assessment* yang meliputi analisis masalah yang terjadi dan *Penetration testing* dalam 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, pengujian sistem yang dibangun serta pembahasan risiko disertai saran/rekomendasi dalam menanggapi kerentanan *website*.

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.