BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dinas Komunikasi dan Informatika Kabupaten Tangerang (DISKOMINFO Kab.Tangerang) berdiri sejak Februari 2014. Suatu Organisasi pemerintahan yang mengelola jalannya komunikasi dan informasi yang pada umumnya menggunakan *platform* berbasis *website*. Dengan adanya *website* DISKOMINFO, alur komunikasi, pengelolaan data secara online dapat dilakukan dengan mudah. Adapun fungsi utama dari *website* yang di kelola Dinas Komunikasi dan Informatika Kabupaten Tangerang adalah sebagai pengelolaan data secara online untuk setiap dinas dan sebagai penyedia layanan informasi resmi pemerintahan kepada masyarakat tentang kegiatan yang dilakukan pemerintah daerah, menjadi tolak ukur bagaimana aktif atau tidaknya kegiatan pemerintahan, dan memudahkan rakyat untuk mengenal sosok pemimpin Kabupaten Tangerang menggunakan website ini sebagai media informasi. Akan tetapi dibalik itu semua, adanya suatu kerentanan yang terdapat pada sistem/aplikasi yang di kelola Dinas Komunikasi dan Informatika Kabupaten Tangerang. Hal ini dapat membahayakan data dan informasi yang bersifat terbuka maupun tidak terbuka.

Berdasarkan hasil wawancara pada 2 oktober 2017 bersama Bapak Cecep khaerudin salah seorang petugas di bidang telematika Dinas Komunikasi dan Informatika Kabupaten Tangerang, beliau menegaskan bahwa sebelumnya pada tahun 2016 telah terjadi beberapa serangan yang mengakibatkan kinerja *website* tersebut menurun. Dan membutuhkan waktu sekitar satu bulan untuk *website* agar bisa pulih kembali, dalam proses maintenance yang dilakukan pada akhir mei sampai dengan pertengahan juni 2016 beliau menegaskan kembali bahwa terdapat beberapa celah keamanan berupa *sql-injection,xss,ddos* hal itu diketahui setelah ditemukannya artifak sisa - sisa penyerangan yang terdapat didalam sistem database dan trafik tinggi yang terdapat pada situs portal dari Dinas Komunikasi dan Informatika Kabupaten Tangerang. Akibat dari serangan ini beberapa akun admin dan user kehilangan hak istimewa (*privileges*) dan situs portal harus ditutup

untuk sementara waktu. Berdasarkan kejadian ini pihak Dinas Komunikasi dan Informatika Kabupaten Tangerang memutuskan untuk menambah suatu keamanan berupa validasi terhadap *website* yang terkena serangan pada tahun 2016 dan beberapa *website* lainnya, hal ini dilakukan guna untuk menghindari kelanjutan dari serangan yang sudah terjadi sebelumnya. Akan tetapi meskipun dengan adanya suatu keamanan yang sudah diterapkan pada sistem di Dinas Komunikasi dan Informatika Kabupaten Tangerang ini tidak menutup kemungkinan bahwa masih terdapat celah – celah keamanan pada sistem yang mereka kelola, hal seperti ini masih memungkinkan bagi seorang *attacker* memanfaatkan celah tersebut untuk medapatkan akses ilegal agar bisa masuk kedalam sistem DISKOMINFO Kabupaten Tangerang.

Berdasarkan hasil penelitian dapat dijabarkan bahwa, perlu dilakukan *selftest* pada *website* Dinas Komunikasi dan Informatika Kabupaten Tangerang yang akan mengeluarkan hasil *cheklist* berupa celah – celah keamanan yang masih terdapat pada sistem tersebut. Dan juga penerapan *monitoring sistem* berdasarkan metode *Information Systems Security Assessment Framework* (*ISSAF*). *ISSAF* dikeluarkan oleh *Open System Security Information Group* (*OSSIG*) adalah suatu *framework* terstruktur yang mengkategorikan penilaian keamanan sistem informasi berdasarkan hasil penelusuran pada domain dan rincian kriteria evaluasi atau pengujian khusus untuk masing-masing domain.

Berdasarkan masalah yang dialami Dinas Komunikas dan Informatika Kabupaten Tangerang adalah diperlukannya suatu bentuk laporan dari hasil pengujian, yaitu berupa ceklist celah – celah keamanan yang akan digunakan untuk dokumentasi guna untuk pemantauan dan meningkatkan keamanan pada *website* DISKOMINFO Kabupaten Tangerang.

1.2 Identifikasi Masalah

Berdasarkan latar belakang dapat di jabarkan bahwa masalah yang di hadapi Dinas Komunikasi dan Informatika Kabupaten Tangerang, yaitu :

1. Terdapat celah keamanan pada sistem yang di kelola Diskominfo Kabupaten Tangerang.

2. Menerapkan sistem monitoring untuk memantau kerentanan – kerentanan yang terjadi di Dinas Komunikasi dan Informatika Kabupaten Tangerang.

1.3 Maksud dan Tujuan

Maksud dan tujuan dari penelitian ini melakukan analisis terhadap *website* Dinas Komunikasi dan Informasi Kabupaten Tangerang berdasarkan metode *ISSAF*, yaitu :

1. Melakukan *selftest* pada *website* Dinas Komunikasi dan Informasi Kabupaten Tangerang.
2. Dapat membantu mengurangi resiko kerentanan pada *website* Dinas Komunikasi dan Informatika Kabupaten Tangerang.

1.4 Batasan Masalah

Pada proses penelitian yang nanti akan di kerjakan akan ada beberapa batasan masalah, yaitu :

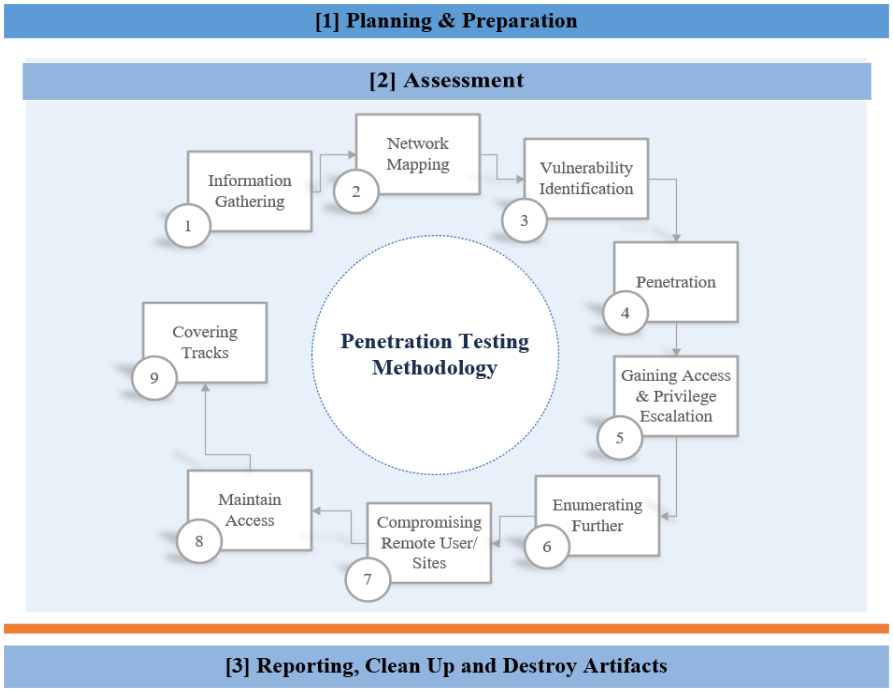
1. *Vulnerability assessment* yang di gunakan adalah metode *ISSAF*.
2. Ruang lingkup untuk *penetration testing* yang diambil adalah web aplikasi.
3. Tahap *clean-up and destroy artefacts* di lakukan secara manual.
4. Pengujian sistem yang di bangun tidak dilakukan di server DISKOMINFO Kabupaten Tangerang.
5. Pengujian dilakukan pada 8 website DISKOMINFO Kab. Tangerang.
6. Penilaian keamanan mengacu pada penyedia layanan penilaian kerentanan *common weakness enumeration* yaitu cwe.mitre.org

1.5 Metode Penelitian

Metode penelitian yang di gunakan yaitu metode kualitatif karena membutuhkan analisis dalam proses *vulnerability assessment* untuk menjalankan prosedur pada metode *ISSAF*.

1.6 Tahapan Penelitian

Berikut ini adalah tahapan penelitian yang dilakukan sesuai dengan modul yang digunakan yaitu *Information System Security Assessment Framework* (ISSAF) *Draft 0.2.1FullRelease* [1]. Modul tersebut dikeluarkan oleh *Open Information System Security Group* (OISSG) pada 30-April-2006. Tahapan – tahapan tersebut akan dijelaskan pada gambar 1.1 Tahapan penelitian.



Gambar 1.1 Tahapan penelitian

1) *Planning and Preparation*

Pada tahap ini akan dilakukan pertukaran informasi, rencana dan persiapan untuk pengujian. Sebelum pengujian berlangsung akan dilakukan pertemuan antara penulis dan pihak Dinas Komunikasi dan Informatika Kabupaten Tangerang untuk meminta persetujuan dalam penelitian ini. Aktivitas yang akan di pertimbangkan dalam phase ini adalah :

Mengidentifikasi kontak peneliti dan pihak Diskominfo Kab.Tangerang, pertemuan terbuka untuk meminta konfirmasi ruang lingkup (*scope)*, pendekatan, metode dan meminta persetujuan untuk pengujian.

2) *Assessment*

Pada tahap ini akan dilakukan *penetration testing*. Dalam tahap assessment ini akan terbagi menjadi beberapa tahap, dan setiap tahap memiliki tingkatan informasi yang berbeda-beda.

a) *Information gathering*

Peneliti mengumpulkan informasi mengenai alamat website yang menjadi target dalam penelitian, dimana pada tahap ini, peneliti akan mencoba mengumpulkan data/informasi dan mengidentifikasi target yang akan diuji.

b) *Network mapping*

Mengindentifikasi sistem dan sumber yang berada di dalam ruang lingkup jaringan target yang akan di uji.

c) *Vulnerability identification*

Aktivitas yang dilakukan oleh peneliti untuk mendeteksi kerentanan target.

d) *Penetration*

Mendapatkan akses ilegal dengan menguji keamanan seperti WAF(*web application firewall*) dan mencoba mengambil akses sejauh mungkin.

e) *Gaining access & privilege escalation*

Setelah berhasil meng-*exploit* sistem/jaringan, si peneliti akan mencoba mencari celah untuk mendapatkan akses yang lebih jauh.

f) *Enumerating further*

Mendapatkan informasi tambahan berdasarkan proses pada sistem, dengan tujuan untuk melakukan exploitasi setelah itu.

g) *Compromise remote user/sites*

Exploitasi hubungan koneksi antara *remote user* dan *enterprise user*.

h) *Maintain access*

Dengan menggunakan sesuatu seperti *backdoor*, untuk tetap dapat masuk ke dalam sistem yang sudah di exploitasi.

i) *Covering tracks*

menghapus semua jejak dengan cara menyembunyikan file, hapus log, menghindari pengecekan integritas dan antivirus.

3) *Reporting, clean-up and destroy artefacts*

a) *Reporting*

Setelah menyelesaikan semua pengujian yang berada pada ruang lingkup, menuliskan laporan yang mendeskipsikan hasil lengkap pengujian dan presentasi yang sudah di persiapkan dengan rekomendasi dan penyelesaiannya.

b) *Clean-up and destroy artefacts*

Semua informasi yang dibuat/ disimpan pada pengujian sistem harus di hapus dari sistemnya, jika itu tidak bisa di lakukan dengan *remote sistem* maka harus di beritahukan ke pihak Diskominfo Kab.Tangerang, agar staff IT bisa langsung menghapus informasi tersebut setelah laporan di terima pihak tersebut.

1.7 Sistematika Penulisan

Diisi dengan susunan calon Bab pada skripsi yang akan dilakukan beserta dengan penjelasannya.

BAB I PENDAHULUAN

Pada bab ini akan diuraikan latar belakang masalah mengapa sistem harus diuji, kemudian identifikasi masalah terhadap sistem yang digunakan, maksud dan tujuan diujinya sistem, batasan masalah dalam pengujian sistem lunak, metode penelitian yang dilakukan dalam pengujian sistem dan sistematika penulisan laporan pembuatan perangkat lunak.

BAB II LANDASAN TEORI

Pada bab ini akan diuraikan berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap penelitian-penelitian serupa yang telah / pernah dilakukan sebelumnya termasuk sintesisnya.

BAB III ANALISIS MASALAH

Pada bab ini berisi tentang analisis masalah dan skenario *assessment* pada fase ke dua metode ISSAF menggunakan *blackbox penetration testing* dalam pengujian keamanan terhadap sistem.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini merupakan tahap implementasi dan pembahasan hasil yang didapat dari analisis *assessment* berdasarkan metode ISSAF. serta pembahasan resiko kerentanan yang terdapat pada sistem yang diteliti dalam kasus ini.

BAB V KESIMPULAN DAN SARAN

Pada 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.