BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin pesat menuntut kemudahan pada berbagai macam aktifitas. Penyediaan layanan sistem informasi sudah tidak hanya diperuntukkan sebagai media pengelolaan data saja, namun juga mulai diperuntukkan sebagai media pendukung keputusan. Berbagai macam istilah dalam bidang sistem informasi pun mulai bermunculan, mulai dari e-bussiness, e-marketing, e-commerce, dan berbagai macam “e” yang lain, seolah ikut menjamur dalam perkembangan teknologi informasi saat ini.

Permasalahan yang timbul adalah setiap sistem informasi harus memiliki jaminan pada keamanan dari informasi yang dimilikinya. Isu tentang celah keamanan yang terdapat pada sebuah sistem informasi bisa menjadi ancaman besar bagi seluruh entitas yang terkait dengan sistem informasi tersebut. *International Organization for Standardization* telah mengeluarkan standarisasi tentang keamanan informasi yaitu pada ISO 27001. Salah satu pokok yang tercantum di dalam ISO 27001 adalah A.12.6 *Technical Vulnerability Management. Vulnerability management* sendiri merupakan siklus dari serangkai tahapan sebagai penanggulangan sebuah kerentanan. Salah satu tahapan yang dilakukan pada siklus *vulnerability management* tersebut adalah tahap pengidentifikasian kerentanan.

Oleh karena itu, demi menunjang aktifitas yang dilakukan pada

siklus *vulnerability management*, diperlukanlah peranti software untuk melakukan pengidentifikasian kerentanan.

1.2 Rumusan Masalah

Dari latar belakang permasalahan di atas maka dapat dirumuskan masalah bagaimana membangun peranti software untuk pengidentifikasian kerentanan pada audit keamanan informasi berdasarkan ISO 27001.

1.3 Ruang Lingkup

Agar pembahasan dapat dilakukan secara terarah dan sesuai dengan yang diharapkan, maka perlu diterapkan batasan-batasan permasalahan yang akan dibahas didalamnya, antara lain :

1. Aplikasi yang dibangun dapat menunjang praktek siklus *vulnerability management* pada ISO 27001 A.12.6 *Technical Vulnerability Management*, yaitu dengan melakukan penidentifikasian kerentanan pada servis yang berjalan di sistem operasi.
2. Aplikasi yang dibangun menggunakan Exploit-DB files.csv sebagai *vulnerability database*.
3. Aplikasi yang dibangun dapat menampilkan informasi tentang kerentanan yang ditemukan sesuai dengan keterangan yang terdapat di dalam *vulnerabilitity database* (yaitu: Exploit-DB files.csv).
4. Pengujian aplikasi dilakukan pada sistem operasi linux dengan target pengujiannya adalah sistem operasi Windows dan Linux.

1.4 Tujuan Penelitian

Dari perumusan masalah di atas peneliti bertujuan untuk membangun aplikasi yang dapat melakukan pengidentifikasian kerentanan pada servis yang berjalan di sebuah sistem operasi.

1.5 Manfaat Penelitian

Berdasarkan dari tujuan penelitian di atas, manfaat dari aplikasi yang akan dibangun dapat difungsikan sebagai penunjang *vulnerability management* pada audit keamanan informasi berdasarkan ISO27001.

1.6 Sistematika Penulisan

Sistematika penulisan pada penilitian ini meliputi :

- BAB I (pendahuluan), berisikan latar belakang masalah, rumusan masalah, ruang lingkup, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.
- BAB II berisikan tinjauan pustaka dan dasar teori yang digunakan sebagai acuan pada penelitian ini.
- BAB III (metode penelitian), berisikan setiap langkah eksperimen yang dilakukan dalam penelitian menggunakan bentuk kalimat pasif.
- BAB IV berisikan impelementasi, uji coba, serta pembahasan sistem.
- BAB V (penutup), berisikan kesimpulan dan saran dari penelitian yang telah dilakukan.