BAB I

PENDAHULUAN

1.1 Latar Belakang

Seperti kita ketahui media rekam medis dari waktu ke waktu mengalami perubahan dan penyempurnaan, dari mulai media rekam medis yang mengalami perubahan karena pegaruh teknologi seperti dari media kertas sekarang sudah mulai bergeser ke media elaktronik bahkan sudah mulai ke web atau internet, dimana rekam medis sudah dapat diakses dari berbagai tempat dan berbagai Negara, hal ini dapat memudahkan pertukaran informasi kesehatan akan tetapi dengan perlu diwaspadai adanya kebocoran informasi kesehatan yang diakses oleh orang-orang yang tidak bertanggung jawab untuk kepentingan pribadi atau kelompok.

Bagaimana basis data diretas?: Penting untuk menyebutkan bagaimana basis data diretas, mengingat hal ini membantu Anda untuk lebih melindungi mereka. Mari kita hitung beberapa serangan umum.

- Password guessing/brute-forcing: Jika kata sandi kosong atau tidak kuat, mereka dapat dengan mudah ditebak / di-brute force. Setelah akun pengguna yang valid ditemukan, mudah untuk menyelesaikan kompromi basis data, terutama jika basis data adalah Oracle.
- Passwords and data sniffed melalui jaringan: Jika enkripsi tidak digunakan, kata sandi dan data dapat dengan mudah diendus(sniffing).

- Exploiting mis-configurations: Beberapa server basis data terbuka secara default. Banyak fungsi yang diaktifkan dan sebagian besar waktu terkonfigurasi dengan aman.
- Memberikan Trojan: Ini bukan serangan server database umum .Sebuah trojan dapat dikirimkan melalui email, p2p, IM, CD, DVD, pen drive, dll. Setelah dieksekusi pada komputer desktop oleh karyawan perusahaan, ia akan mendapatkan server database dan informasi pengguna secara otomatis dan sembunyi-sembunyi menggunakan ODBC, OLEDB , Koneksi JDBC dikonfigurasi, sniffing, dll. Ketika informasi yang cukup dikumpulkan trojan dapat menghubungkan ke server datatabase, itu bisa mencoba akun default jika perlu. Setelah login berhasil, ia akan mencuri data, itu bisa menjalankan 0 hari untuk meningkatkan hak istimewa untuk memiliki server basis data lengkap dan juga menginstal rootkit basis data untuk menyembunyikan tindakannya. Semua langkah sebelumnya akan berulang pada setiap server basis data yang ditemukan. Trojan dapat mengirim data curian yang dienkripsi ke penyerang melalui email, HTTP, saluran rahasia, dll.
- Memanfaatkan kerentanan yang diketahui / tidak dikenal: Penyerang dapat mengeksploitasi buffer overflows, SQL Injection, dll. Untuk memiliki server database. Serangan dapat melalui aplikasi web dengan mengeksploitasi SQL Injection sehingga tidak diperlukan otentikasi. Dengan cara ini, basis data dapat diretas dari Internet dan firewall selesai dilewati. Ini adalah salah satu metode termudah dan disukai yang

digunakan penjahat untuk mencuri informasi sensitif seperti kartu kredit, nomor jaminan sosial, informasi pelanggan, dll.

- Mencuri disk dan kaset cadangan: Ini adalah sesuatu yang tidak umum disebutkan, perusahaan selalu mengatakan bahwa disk atau cadangan hilang:) Jika file data dan data cadangan tidak dienkripsi, data yang dicuri dapat dengan mudah dikompromikan.
- Menginstal rootkit / backdoor: dengan menginstal rootkit *action* dan objek basis data dapat disembunyikan sehingga administrator tidak akan memperhatikan seseorang meretas basis data dan terus memiliki akses. Backdoor basis data dapat digunakan, dirancang untuk mencuri data dan mengirimkannya ke penyerang dan / atau memberikan penyerang diam-diam akses tidak terbatas pada waktu tertentu.

Rekam medis adalah berkas yang berisi catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan kepada pasien.Rekam medis bermanfaat sebagai dasar dan petunjuk untuk merencanakan dan menganalisis penyakit serta merencanakan pengobatan, perawatan dan tindakan medis yang harus diberikan kepada pasien.

Dalam Permenkes No.269 Tahun 2008 tentang kerahasian rekam medis. Setiap orang harus dapat meminta pertolongan kedokteran dengan perasaan aman dan bebas. Ia harus dapat menceritakan dengan hati terbuka segala keluhan yang mengganggunya, baik bersifat jasmaniah maupun rohaniah, dengan keyakinan bahwa hak itu berguna untuk menyembuhkan dirinya. Ia tidak boleh merasa khawatir bahwa segala sesuatu mengenai keadaannya akan disampaikan kepada

orang lain, baik oleh dokter maupun oleh petugas kedokteran yang bekerja sama dengan dokter tersebut.

Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa di dekripsi (kebalikan dari proses enkripsi) dahulu.

Karena penulis adalah pemula pada bidang enkripsi dan kriptografi maka penulis memilih "Enkripsi kriptografi Vigènere Cipher" sebagai algoritma kriptografi dalam aplikasi ini, karena cara kerjanya mudah dimengerti dan dijalankan, dan bagi para pemula sulit dipecahkan.

Dengan menggunakan Enkripsi kriptografi Vigènere Cipher pada saat data tersimpan kedalam database sudah dalam keadaan terenkripsi, dan diharapkan dapat meningkatkan tingkat keamanan dan kerahasian data rekam medis. Dengan judul "Sistem Informasi Pengelolaan Rekam Medis Dengan Enkripsi Vigenere Cipher", maka dengan website ini diharapkan proses pelayanan pasien dapat memberikan rasa nyaman dan aman bagi pasien.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, maka dapat diambil suatu perumusan masalah yaitu:

1. Bagaimana mengimplementasikan enkripsi vigenere cipher pada sistem informasi pengelolaan rekam medis tsb.

1.3 Tujuan Penelitian

Tujuan dari perancangan sistem ini adalah sebagai berikut:

1. Meningkatkan tingkat keamanan dan kerahasian data.

2. Memberikan rasa aman dan nyaman pada pasien sehingga dapat menceritakan dengan hati terbuka segala keluhan yang mengganggunya, baik bersifat jasmaniah maupun rohaniah,
3. Sebagai media pembelajaran penulis mengenai Enkripsi dan kriptografi

1.4 Batasan Masalah

Pada perancangan dan pembuatan sistem ini mencakup banyak hal. Agar permasalahan tidak meluas maka perlu adanya batasan masalah yang akan dibahas yaitu sebagai berikut :

1. Input tipe text di batasi hanya huruf dan angka saja tanpa karakter dan simbol.

1.5 Sistematika Penulisan

BAB I PENDAHULUAN

Berisikan informasi mengenai latar belakang, rumusan masalah, batasan masalah, tujuan, manfat penelitian, dan sistematika penelitian.

BAB II LANDASAN TEORI

Berisikan tentang software yang diguanakan serta konsep dasar perancangan aplikasi.

BAB III ANALISA SISTEM

Berisikan tentang pembahasan analisa dan perancangan aplikasi, perancangan sistem.

BAB IV PEMBAHASAN

Berisikan tentang spesifikasi kebutuhan perangkat, implementsi system, analisis hasil dan rancangan tampilan sistem

BAB V PENUTUP

Berisikan kesimpulan penulisan dari pembuatan Laporan dan juga saran-saran sebagai tindak lanjut dari penulisan sesuai materi.

1.6 Metoda Penulisan

Dalam metode penulisan, sumber data yang digunakan oleh penulis adalah:

Data sekunder yang digunakan oleh penulis untuk memperoleh data yaitu dengan Penelitian Kepustakaan (Library Research)yaitu dengan mempelajari masalah dan literatur-literatur maupun sumber data lainnya yang berkaitan dengan masalah penulisan laporan akhir ini, sebagai dasar perbandingan dan penganalisaan data penulisan.

Metode Pengumpulan Data Dalam pengumpulan data sebagai dasar penulisan, metode penelitian yang digunakan adalah sebagai berikut:

a) Metode Observasi

Yaitu metode pengumpulan data dengan cara mengadakan pengamatan terhadap suatu hal yang nyata dengan hal-hal atau keadian untuk melengkapi dan mencocokan data yang diperoleh melalui interview atau wawancara.

b) Metode Literatur/ Dokumentasi

Yaitu dengan melakukan pengumpulan data mengenai hal-hal yang berhubungan dengan penelitian, cara ini dilakukan untuk melengkapi datayang dibutuhkan,