BAB 1

PENDAHULUAN

1.1. Latar Belakang

Perkembangan internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif. Tidak dapat dipungkiri bahwa teknologi internet membawa dampak negatif yang tidak kalah banyak dengan manfaat yang ada (Hilda, 2015).

Internet membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian dan penipuan kini dapat dilakukan dengan menggunakan media komputer Secara *online.* Resiko tertangkap yang sangat kecil oleh individu maupun kelompok dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun negara disamping menimbulkan kejahatan-kejahatan baru (Freddy, 2008).

Website merupakan sebuah cara untuk menampilkan diri di internet. Karena website adalah sebuah tempat di internet siapa saja di dunia ini dapat mengunjunginya. Keamanan merupakan salah satu indikator penting dalam membangun sebuah website, mengingat akses ke internet yang terbuka bebas bagi masyarakat umum. Bahkan tidak ada website yang dapat dikatakan benar-benar aman.

Berbicara tentang keamanan website tentu banyak sekali cara yang dilakukan *hacker* dalam menembus pertahanan sistem. Untuk menghindari kemungkinan serangan yang dilakukan *hacker* bisa menggunakan cara pendeteksian serangan salah satunya dengan cara digital forensik.

Digital forensik memainkan bagian penting dalam penyelidikan kejahatan yang melibatkan peralatan elektronik. Misalnya bukti digital yang dikumpulkan di TKP harus dianalisis terlebih dahulu untuk menemukan bagaimana sebuah kejahatan digital dilakukan dan siapa yang melakukan kejahatan tersebut.

Investigasi adalah Upaya penelitian, penyelidikan, pengusutan, pencarian, pemeriksaan dan pengumpulan data, informasi, dan temuan lainnya untuk mengetahui/membuktikan kebenaran atau bahkan kesalahan sebuah fakta yang kemudian menyajikan kesimpulan atas rangkaian temuan dan susunan kejadian (Karman, 2009).

Dalam proses Investigasi memerlukan waktu khusus, Dengan menyajikan sebuah kerangka kerja digital forensik yang meliputi penyelidikan proses model yang didasarkan pada TKP fisik *procedures*. Dalam investigasi ini, setiap perangkat digital dianggap TKP digital, yang termasuk dalam TKP fisik di mana pelaku berada (Sri Marini, 2012).

Serangan dengan *SQL Injection* merupakan hal paling sering disukai oleh *hacker* dan juga peretas *database*. Biasanya terjadi pada website berbasis PHP dan MySQL. Metode *SQL Injection* yang dipakai oleh *hacker* biasanya memanfaatkan form-form di dalam website yang tidak dilengkapi dengan script pengamanan khusus.

Teknik *SQL Injection* ini sudah dikenal dalam dunia *hacking* sebagai salah satu teknik *web hacking*, namun baru muncul lagi sekarang karena sifatnya yang dapat merusak *database* dari suatu website. Teknik yang digunakan dalam *SQL injection* adalah dengan jalan menginput perintah-perintah standar dalam *SQL*

(DDL, DML, DCL) seperti *create, insert, upate, dorp, alter, union* dan *select* beserta perintah-perintah lainnya yang tak asing lagi bagi anda yang sudah mengenal *SQL* secara mendalam maupun yang baru saja belajar.

SQL singkatan dari *Structured Query Language* yang merupakan bahasa komputer standar yang ditetapkan oleh *ANSI* (*American National Standard Institute*) untuk mengakses dan memanupulasi sistem *database*. *SQL* bekerja dengan program *database* seperti *MS Access, DB 2, Informix, MS SQL Server, Oracle, Sybase* dan lain sebagainya. *SQL injection attack* merupakan salah satu teknik dalam melakukan web *hacking* untuk menggapai akses pada sistem *database* yang berbasis *SQL*.

Teknik *SQL Injection* memanfaatkan kelemahan dalam bahasa pemrograman *scripting* pada *SQL* dalam mengolah suatu sistem *database*. Hasil yang ditimbulkan dari teknik ini membawa masalah yang sangat serius. Kasus *SQL Injection* terjadi ketika seorang penyerang dapat memasukkan serangkaian pernyataan *SQL* ke *query* dengan memanipulasi data input ke aplikasi (Anley, 2002).

Berdasarkan defenisi tersebut, dapat dikatakan bahwa serangan *SQL Injection* sangat berbahaya karena penyerang yang telah berhasil memasuki *database* sistem dapat melakukan manipulasi data yang ada pada *database* sistem. Proses manipulasi data yang dilakukan penyerang dapat menimbulkan kerugian bagi pemilik *website* yang terserang. Kebocoran data dan informasi merupakan hal yang fatal. Data-data tersebut dapat disalah gunakan oleh pihak yang tidak bertanggung jawab.

Keamanan data dan informasi sangat penting dalam menjaga ketahanan sebuah website. Berdasarkan uraian-uraian tersebut, maka dinilai perlu untuk menguji keamanan website terhadap serangan *SQL Injection*. Serta melakukan analisa terhadap kelemahan sistem yang ada, sehingga dapat diperoleh tindakan selanjutnya untuk perbaikan sistem.

Dalam penelitian ini perlindungan website difokuskan pada pencegahan *SQL Injection* dengan metode *scripting* pada bagian *database* akan dikombinasikan atau digabungkan *script* Crawltrack yang akan membantu mengamankan website dari serangan *SQL Injection.* Selain mengatasi serangan *SQL Injection, script* tersebut terdapat interface yang membantu dalam pengoperasian bagi *administrator.* Isi dari interface tersebut terdapat macam-macam fungsi seperti analisis pengunjung website, banyak halaman yang dikunjungi, serta identitas penyerang dari *SQL Injection* akan diketahui secara rinci.

1.2. Rumusan Masalah

Berdasarkan pada latar belakang yang dijelaskan sebelumnya, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana cara melakukan pengujian terhadap keamanan website?
2. Bagaimana melakukan analisa terhadap keamanan website?
3. Bagaimana cara mengetahui metode serangan dari penyerang ?
4. Bagaimana melacak penyerang yang melakukan serangan ?

1.3. Batasan Masalah

Adapun batasan masalah dalam menganalisa dan menyelesaikan suatu masalah, maka perlu diberikan batasan masalah guna mempermudah dalam

pemecahan serta pembahasannya. Adapun batasan – batasan masalah yang telah ditentukan dalam penelitian ini, yaitu sebagai berikut:

1. Pembuatan website sederhana tanpa banyak keamanan didalamnya guna untuk mengetahui website mudah diambil alih oleh penyerang.
2. *Script* keamanan yang dimasukkan dalam *database* berfungsi untuk mengamankan *database* supaya tidak bisa di *inject* oleh penyerang, agar informasi yang dicari penyerang tidak ditemukan.
3. Pengerjaan serangan dilakukan secara real dengan menggunakan Windows 7, kali linux 2 sebagai attacker dan Windows 10 sebagai *control panel* oleh *administrator*.
4. Penggunaan *scripting* berfungsi untuk menganalisis *traffic* website, melihat informasi website¸serta mengetahui dan melacak penyerang melalui *IP address.*
5. Penggunaan *scripting* untuk mengamankan website menggunakan Crawltrack versi 3-2-2.

1.4. Tujuan Penelitian

Adapun tujuan dari penelitian "Investigasi Forensik Serangan Website SQL Injection Menggunakan Metode Scripting Pada Crawltrack" antara lain sebagai berikut:

1. Melakukan pengujian terhadap keamanan website.
2. Melakukan analisa terhadap hasil pengujian keamanan website.
3. Mengetahui metode serangan dan keberadaan IP dari penyerang.

1.5. Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dari penelitian "Investigasi Forensik Serangan Website SQL Injection Menggunakan Metode Scripting Pada Crawltrack" ini adalah:

1. Bagi peneliti:

Dengan dilakukannya penelitian ini diharapkan dapat memberikan pemahaman tentang pentingnya keamanan pada suatu website, serta memberikan pengetahuan dasar tentang script pada *SQL Injection* untuk menyerang *database* MYSQL.

2. Bagi pengguna:

a. Dari penelitian ini diharapkan dapat memberikan pengetahuan tentang pengamanan website.
b. Dapat mengetahui kelemahan website, apakah sistem rentan terhadap serangan.
c. Dapat mengetahui langkah atau tindakan pencegahan, berdasarkan hasil analisa terhadap pengujian keamanan website serta melacak penyerang yang melakukan serangan dengan *IP address* yang digunakan.

1.6. Metodologi

Metode penulisan yang digunakan dalam melakukan analisa, pengumpulan data serta penyusunan laporan tugas akhir adalah sebagai berikut:

a. Studi Literature

Pada tahap ini melakukan pencarian referensi-referensi yang berkaitan mengenai tema tugas akhir ini. Referensi berasal dari berbagai sumber misalkan artikel berupa e-book, jurnal, skripsi, *thesis* dan buku.

Hasil dari studi *literature* ini adalah terkumpulnya referensi yang relevan dengan perumusan masalah. Tujuannya adalah untuk memperkuat permasalahan serta sebagai dasar teori dalam melakukan studi dan juga menjadi dasar untuk melakukan penelitian.

b. Analisa Kebutuhan

Pada tahap ini melakukan analisa apa saja kebutuhan untuk penelitian tugas akhir. Seperti mengumpulkan data, analisa data dan analisa kebutuhan *hardware* dan *software*.

c. Perancangan Simulasi

Pada tahap ini membuat perencanaan pembentukan komponen-komponen keamanan website yang dibutuhkan untuk menunjang simulasi keamanan website dari serangan *SQL Injection* agar mendapatkan hasil yang diinginkan. Simulasi ini menggunakan virtualbox untuk pengoperasian sistem dan *script* CrawlTrack untuk keamanan website.

d. Analisa dan Implementasi

Pada tahap ini melakukan analisa terhadap perancangan yang telah dibuat dan melakukan implementasi keamanan website dengan *script* anti *SQL Injection* dari CrwalTrack.

e. Evaluasi dan Revisi

Pada tahap ini akan dilakukan evaluasi dari hasil analisa yang sudah dilakukan. Hasil evaluasi menghasilkan suatu kesimpulan dari tugas akhir. Revisi dibutuhkan jika terjadi kesalahan dalam pelaksanaan penelitian sehingga penelitian ini dapat menjadi sumber referensi yang baik.

f. Penyusunan Laporan Tugas Akhir

Pada tahap ini dilakukan penyusunan laporan skripsi. Buku ini disusun sebagai laporan keseluruhan penyusunan skripsi. Laporan ini dibuat untuk memudahkan pembaca untuk mempelajari tentang analisa kinerja keamanan sebuah website dari serangan *SQL Injection*.

1.7. Sistematika Penulisan

Dalam laporan penelitian tugas akhir ini, pembahasan dibagi menjadi lima bab dengan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Berisi latar belakang yang akan menjelaskan tentang alasan serta pentingnya tugas akhir atau penelitian ini dilakukan, dari perumusan masalah, batasan masalah, tujuan, manfaat, metode penulisan dan sistematika penulisan yang digunakan dalam laporan penelitian tugas akhir ini.

BAB II TINJAUAN PUSTAKA

Pada bab ini akan disajikan penjelasan singkat penelitian terdahulu dan beberapa pengertian yang menjadi landasan teori penelitian diantaranya *SQL Injection*.

BAB III METODELOGI PENELITIAN

Pada bab ini akan menjelaskan secara lebih mendalam mengenai keamanan website yang menggunakan metode *scripting* pada CrwalTrack sebagai pendeteksian serangan.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini akan menjelaskan proses keamanan website menggunakan Crwaltrack sebagai pendeteksian serangan *offline* ataupun *online*.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi tentang kesimpulan yang dapat diambil dari keseluruhan isi dari laporan penelitian tugas akhir serta saran - saran yang diharapkan dapat mengembangkan lebih dalam tentang penelitian ini selanjutnya.

DAFTAR PUSTAKA

Pada bab ini berisi bagian yang akan dipaparkan tentang sumber - sumber literatur yang digunakan dalam proses penelitian tugas akhir ini.