BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring dengan makin berkembangnya penggunaan *internet*, pertukaran informasi dari berbagai belahan dunia menjadi semakin cepat dan lancar. Isu ketidakamanan kemudian mencuat karena terjadinya beberapa kasus, seperti manipulasi data pada *database* dan pencurian *username* dan *password*. Hal ini juga terjadi pada *web-site* KPU (Komisi Pemilihan Umum) indonesia pada tahun 2004, dimana isi dari *web-site* tersebut diacak-acak oleh pihak yang tidak bertanggungjawab. Sehingga data-data dan tampilan dari *web-site* tersebut menjadi tidak jelas dan kacau, hal ini dikarenakan bahwa *administrator web-site* tersebut kurang memperhatikan mengenai masalah keamanan.

Salah satu teknik untuk menangkal serangan tersebut adalah dengan menggunakan keamanan *JDefender*. Keamanan ini bekerja dengan mendeteksi dan mengeblok dari setiap serangan yang masuk dari para *cracker*, seperti *Flood* (Banjir data di jaringan), *SQL Injection* dan *PHP Injection. JDefender* dapat mengeblok *ip address, login* dan memfilter string-sting yang dianggap berbahaya dengan menggunakan *regular expressions* sehingga para *cracker* tidak dapat masuk sebagai *administrator* yang mana dapat melakukan pencurian *username* dan *pasword* serta manipulasi data pada *database*.

Keamanan *JDefender* ini selanjutnya akan mengirimkan *email alerts* kepada *administrator* apabila telah mendeteksi serangan yang masuk. Pemberitahuan berupa pengiriman *email* ini sangat penting, karena sebagai konfirmasi kepada *adminstrator web-site* agar dengan segera waspada dan tetap siaga terhadap beberapa serangan membahayakan yang masuk. Hal ini terjadi apabila *domain* dari *web-site* telah dihosting dan kalau belum

dihosting tidak akan terjadi pemberitahuan berupa pengiriman *email* kepada *administrator*.

1.2 Rumusan Masalah

Permasalahan utama yang menjadi pembahasan pada Proyek Akhir ini adalah:

1. Bagaimana cara kerja *JDefender* ?
2. Apa kelemahan *JDefender* ?

1.3 Tujuan

Adapun tujuan dari penulisan proyek akhir ini adalah sebagai berikut:

1. Mempelajari sistematika kerja *JDefender*.
2. Menguji sistem keamanan *JDefender*.

1.4 Batasan Masalah

Adapun batasan masalah dalam Proyek Akhir ini adalah sebagai berikut:

1. Aplikasi yang digunakan untuk membangun *web-site* ini adalah *Joomla* versi 1.0.15.
2. Tidak membahas lebih lanjut dan secara detail tentang aplikasi pembuat *web-site*, yaitu Joomla versi 1.0.15.
3. Melakukan teknik penyerangan *SQL Injection*, *Flooding* dan *PHP Injection* untuk menguji kekuatan dan mencari kelemahan dari sistem keamanan *JDefender*.
4. Keamanan informasi yang dimaksud bukan menyangkut *cryptography* dan *steganography*.
5. Keamanan dari sebuah *web-site* yang digunakan adalah *JDefender* versi 1.6.
6. Tidak mengulas lebih lanjut perihal standar protokol komunikasi data.

7. Pengujian dilakukan pada *platform* Sistem Operasi Windows XP.
8. *Web server* yang digunakan adalah XAMPP versi 1.6.1.
9. Menggunakan *Database* MySQL versi 5.0.37.
10. Menggunakan PHP versi 5.2.

1.5 Metodologi Penelitian

Metodologi penelitian Proyek Akhir ini berisi tentang metodologi yang akan digunakan Penulis sebagai pendukung dalam proses pengerjaan. Pengerjaan Proyek Akhir ini terdiri dari beberapa tahap pengerjaan, yaitu :

1.5.1 Studi Literatur

Studi literatur yaitu mempelajari tentang teknik penyerangan menggunakan *SQL Injection, Flooding* dan *PHP Injection* dengan metode menyisipkan string-string ke dalam alamat *URL*, *form login*, memberikan *request* berupa *ping* secara terus menerus kepada komputer yang diserang dan menyisipkan *script* PHP *Injection* yang tersimpan didalam *text editor* kedalam alamat URL korban. Sumber literatur yang digunakan antara lain buku, artikel, dan dari internet. Perkiraan waktu yang diperlukan adalah 1 bulan yaitu pada bulan Mei.

1.5.2 Wawancara

Wawancara adalah suatu proses komunikasi interaksional antara dua pihak. Cara ini dilakukan untuk mendapatkan informasi dan pengetahuan dari beberapa pihak yang dianggap pakar dan kompeten di bidangnya untuk membantu dalam hal eksplorasi teoretik perihal topik yang akan dibahas. Perkiraan waktu yang diperlukan adalah 1 bulan yaitu pada bulan Mei.

1.5.3 Pembangunan Model

Pembangunan model adalah perancangan dan pembangunan *web-site* akademik yang diserang dengan teknik *SQL Injection, Flooding* dan *PHP Injection*. Keamanan *JDefender* juga diterapkan di *web-site* ini, guna menangkal dari ketiga serangan diatas. Konsep dari penerapan keamanan *JDefender* dalam *web-site* akademik yang akan dibuat adalah dengan menginstalnya langsung di *server web-site* tersebut, dengan catatan harus *login* terlebih dahulu menjadi *administrator*. *Web-site* akademik ini dibuat dengan menggunakan *Content Management System (CMS)* Joomla versi 1.0.15. Setelah keamanan tersebut selesai terinstal, maka kita uji dengan menyerangnya menggunakan teknik *SQL Injection, Flooding* dan *PHP Injection*. Apa yang akan terjadi jika kita serang *web-site* ini setelah memakai keamanan *JDefender*, apakah akan memunculkan pesan atau *alert* berupa pemberitahuan kepada *administrator* bahwa ada penyerang yang ingin menyusup atau tidak dan juga apakah keamanan ini mampu menangkal dari ketiga serangan tersebut. Perkiraan waktu yang diperlukan adalah 1 bulan yaitu pada bulan Juni.

1.5.4 Implementasi

Implementasi adalah pengujian *web-site* akademik yang telah dibuat dengan menggunakan *Content Management System (CMS) Joomla* versi 1.0.15 yang di dalamnya sudah terinstal keamanan *JDefender* dengan memberikan serangan berupa *SQL Injection, Flooding* dan PHP *Injection*. Apa yang akan terjadi jika *web-site* tersebut diserang dengan ketiga serangan diatas sebelum dan sesudah memakai keamanan *JDefender*. Hal ini untuk mengetahui seberapa kuatkah *web-site* yang sudah terinstal *JDefender* tersebut didalam menghadapi ketiga serangan diatas. Perkiraan waktu yang diperlukan adalah 4 bulan yaitu pada bulan Juni, Juli, Agustus dan September.

1.5.5 Analisis Hasil

Analisis hasil adalah menganalisis kualitas dari keamanan *JDefender*. Parameter yang digunakan adalah perubahan yang terjadi pada *web-site* akademik setelah diserang dengan menggunakan teknik *SQL Injection, Flooding* dan *PHP Injection*. Karena keamanan yang baik adalah yang dapat memunculkan pesan berupa *alert* atau peringatan dan mampu menangkal dari serangan *cracker*. Perkiraan waktu yang diperlukan adalah 2 bulan yaitu bulan Agustus dan September.

1.5.6 Pembuatan Laporan

Pembuatan laporan adalah pendokumentasian seluruh rangkaian pengerjaan Proyek Akhir. Metode yang digunakan adalah menyusun laporan berdasarkan data-data selama pengerjaan Proyek Akhir dengan tata tulis karya ilmiah. Perkiraan waktu yang diperlukan adalah 1 bulan yaitu bulan September.

1.6 Jadwal Pelaksanaan

Tabel 1.6 Jadwal Pelaksanaan

Bulan / Kegiatan	Mei 2010				Juni 2010				Juli 2010				Agustus 2010				September 2010			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Pengumpulan Data																				
Pembangunan Model																				
Implementasi																				
Analisis Hasil																				
Pembuatan laporan																				