BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam perkembangan *cybercrime* jenis penyerangan bukan hanya sebatas merusak dan melumpuhkan suatu sistem, saat ini *silent attack* merupakan jenis penyerangan yang berbahaya seperti *Unauthorized Access to Computer System*[1]. *Unauthorized Access to Computer System* merupakan kejahatan yang dilakukan dengan memasuki atau menyusup kedalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pengelola sistem tersebut. Pelaku kejahatan (peretas) melakukannya dengan tujuan memata-matai ataupun pencurian informasi penting dan rahasia, dalam praktiknya ada beberapa pola dan teknik yang digunakan peretas untuk masuk kedalam sebuah sistem dan setelah berada didalam sistem target, peretas tinggal menyisipkan file *backdoor shell* pada lokasi yang sulit untuk ditemukan pengelola sistem/website.

Backdoor shell [2] merupakan kumpulan kode-kode atau *script* yang pada umumnya berbasis PHP yang dimanfaatkan oleh peretas untuk memperoleh akses pada *file stored* di *web server* target. Sehingga peretas dapat melakukan manipulasi data dan mengambil data rahasia pada *web server* target. Jika pengelola website tidak dapat mendeteksi keberadaan *backdoor shell* maka dapat menimbulkan efek jangka panjang. Peretas dengan mudah mendapatkan data-data rahasia pada sistem secara berkala. Dan saat pengelola website menyadari ada file penyusup didalam sistem, pengelola website dapat melakukan *restore* file *backup* namun cara ini tidak efektif untuk *file store* yang berkapasitas besar dan juga pengelola tidak mengetahui lama waktu sistem telah terinfeksi oleh *backdoor shell*.

Berdasarkan data survei yang telah dilakukan terdahap 56 orang responden yang mengelola website seperti profil perusahaan/instansi, website pribadi dan online shop 59% dari responden pernah mengalami gangguan terhadap website yang berupa *deface, xss, sql injection* dan beberapa teknik lainnya. dan dalam

penanggulangannya 25% responden sangat setuju dan 30% responden setuju bahwa sangat sulit untuk mencari file *backdoor shell* pada file *store*.

Saat ini ada beberapa tools yang dapat digunakan pengelola web server untuk melakukan pencarian backdoor shell seperti *Grep, NeoPI* [3] dan *PHP Shell Detector* [4], *Grep* dan *NeoPi* merupakan *unix command* untuk mencari file dengan cara pencocokan *string*. Hal ini membuat pengelola web yang tidak familiar dengan sistem operasi *unix/linux* kesulitan dalam menggunakannya, hasil dari pencarian masih berupa list pada terminal sehingga pengguna harus melakukan pencarian manual pada web server sesuai alamat yang telah ditemukan dan tentunya hal ini membutuhkan waktu dalam pengecekannya, dan juga list yang ditampilkan tidak hanya file *backdoor shell* melainkan file legal yang memiliki fungsi sama ikut ditampilkan. Sedangkan *PHP Shell Detector* merupakan *script* berbasis php yang sudah memiliki GUI untuk mempermudah pengguna. Namun *PHP Shell Detector* melakukan pencarian file berdasarkan list telah terdaftar sebelumnya sehingga kelemahannya saat jenis file *backdoor shell* baru menginfeksi, tools ini tidak dapat mendeteksi keberadaan backdoor shell tersebut.

Berdasarkan hal tersebut, maka muncullah sebuah ide untuk membangun sebuah aplikasi pendeteksi *backdoor shell*. Aplikasi pendeteksi *backdoor shell* merupakan sebuah aplikasi pencarian yang akan dibangun untuk menjadi solusi dari permasalahan yang dipaparkan sebelumnya. Dimana dengan aplikasi ini pengelola website dapat mencari file *backdoor shell* dengan mudah karena aplikasi ini menggunakan tampilan yang *user friendly*, meningkatkan akurasi pencarian, dan mengimplementasi *Basic Static Code Analysis Techniques* dalam mendeteksi *script* untuk mengoptimalkan identifikasi file *backdoor shell* atau tidak.

1.2 Rumusan Masalah

Berdasarkan pemaparan latar belakang masalah, maka perumusan permasalahan yang terdapat pada penelitian ini adalah bagaimana cara mendeteksi *backdoor shell* pada *web server* dengan menggunakan *Basic Static Code Analysis Techniques.*

1.3 Maksud dan Tujuan

Berdasarkan penelitian yang dibahas, maka maksud dari penelitian tugas akhir ini adalah untuk membangun aplikasi pendeteksi pada *web server*. sedangkan tujuan dari penelitian ini adalah:

1. Mempermudah pengelola website untuk menemukan file *backdoor shell* pada *web server* yang terinfeksi.
2. Meningkatkan akurasi dalam proses pencarian *backdoor shell* pada *web server*.

1.4 Batasan Masalah

Agar dalam pembahasannya lebih terarah dan sesuai dengan tujuan yang akan dicapai maka diperlukan batasan masalah. Adapun batasan masalah dalam pelaksanaan penelitian ini adalah

1. Perangkat lunak ini dibangun berbasis website.
2. Perangkat lunak ini menggunakan database MySQL.
3. Pendekatan analisis perangkat lunak menggunkan analisis terstruktur.
4. Perangkat lunak ini menggunakan *Basic Static Code Analysis Tehcniques*.
5. Perangkat lunak ini bersifat publik.
6. Ruang lingkup pencarian perangkat lunak ini pada direktori *web server* (cpanel).
7. String matching dapat mendeteksi backdoor shell dengan format php, asp, jsp, vb, aspx, pl, py dan bsh.
8. Sedangkan taint analysis hanya mendeteksi backdoor shell dengan format php.

1.5 Metodologi Penelitian

Penelitian ini menggunakan metode penelitian deskriptif, yaitu metode penelitian yang bertujuan untuk mendapatkan gambaran yang jelas tentang hal-hal yang dibutuhkan dan berusaha menggambarkan serta menginterpretasi objek yang sesuai dengan fakta secara sistematis, faktual dan akurat. Adapun metodolgi yang

digunakan dalam penelitian ini menggunakan dua metode, yaitu metode pengumpulan data dan metode pembangunan perangkat lunak.

1.5.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan untuk mengumpulkan data penelitian adalah sebagai berikut :

1. Studi Literatur

   Teknik pengumpulan dengan membaca dan meneliti literatur, jurnal, dokumen-dokumen, buku-buku, artikel, berita dan berbagai referensi yang berkaitan dengan judul penelitian.

2. Kuesioner

   Teknik pengumpulan data dengan cara memberikan angket yang berisi pertanyaan dan pernyataan serta pendapat kepada orang-orang yang terlibat lansung dalam pembuatan maupun pengelolaan website.

1.5.2 Metode Pembangunan Perangkat Lunak

Dalam pembangunan aplikasi ini metode yang digunakan adalah *waterfall* model sebagai tahapan pengembangan perangkat lunaknya. Adapun proses tersebut antara lain :

1. *Requirement analysis and definition*

   Merupakan bagian dari sistem yang terbesar dalam pengerjaann suatu proyek, dimulai dengan menetapkan berbagai kebutuhan dari semua elemen yang diperlukan sistem dan mengalokasikannya kedalam pembentukan perangkat lunak.

2. *System and software design*

   Tahap *system and software design* merupakan tahap mendesain perangkat lunak yang dikerjakan setelah kebutuhan selesai dikumpulkan secara lengkap.

3. *Implementation and unit testing*

   Tahap *implementation and unit testing* merupakan tahap hasil desain program diterjemahkan ke dalam kode-kode dengan menggunakan bahasa

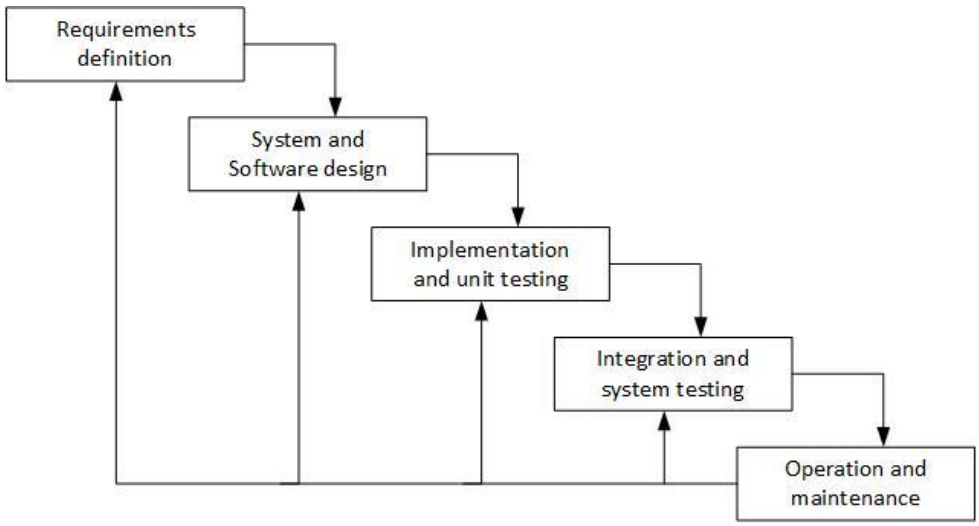
pemograman yang sudah ditentukan. Program yang dibangun lansung diuji berdasarkan unit-unitnya.

4. *Integration and system testing*

Tahap *integration and system testing* merupakan tahap penyatuan unit-unit program kemudian sistem diuji secara keseluruhan.

5. *Operation and maintance*

Tahap *operation and maintance* merupakan tahap mengoperasikan program dilingkungannya dan melakukan pemeliharaan, seperti penyesuaian atau perubahan karena adaptasi dengan situasi yang sebenarnya.



Gambar 1. 1 Metode Waterfall [5]

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab I ini akan membahas tentang latar belakang permasalah, merumuskan inti permasalahan yang di hadapi, menentukan maksud dan tujuan yang kemudian

diikuti batasan masalah, metodologi penelitian yang digunakan serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab II ini akan membahas konsep dasar *Basic Static Code Analysis Techniques* dan teori-teori yang berkaitan dengan topik pembangunan aplikasi yang dilakukan dan hal-hal yang berguna dalam proses analisis pembangunan aplikasi pendeteksi *backdoor shell*. Dan membahas segala sesuatu yang nantinya bisa dijadikan pegangan dalam pembangunan aplikasi pendeteksi *backdoor shell*.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab III ini akan membahas tentang analisis sistem, pengguna, analisis pemecahan masalah, analisis kebutuhan fungsional dan non fungsional, serta perancangan sistem untuk pembangunan aplikasi pendeteksi *backdoor shell* pada *web server.*

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab IV ini akan memaparkan hasil implementasi analisis pada BAB III dan perancangan sistem yang dilakukan, serta hasil pengujian *black box* pada sistem untuk mengetahui apakah aplikasi pendeteksi *backdoor shell* yang dibangun sudah memenuhi kebutuhan.

BAB V KESIMPULAN DAN SARAN

Bab V ini berisi kesimpulan dan saran yang merupakan jawaban yang melatar belakangi masalah pada Bab I, juga saran untuk perbaikan dan menindak lanjuti hasil penelitian yang nantinya akan berguna bagi pengembang perangkat lunak ini kedepannya.