BAB 1
PENDAHULUAN

Bab ini berisi uraian singkat mengenai latar belakang tugas akhir, identifikasi masalah dari tugas akhir, tujuan dan maksud dari tugas akhir, lingkup tugas akhir serta metode dan sistematika pembahasan tugas akhir.

1.1 Latar Belakang Tugas Akhir

Seiring dengan perkembangan internet yang semakin cepat serta kemudahan untuk mengakses internet. Banyak orang yang menggunakan *website* sebagai sarana untuk mencari informasi di internet, maka dari itu keamanan website sangatlah penting. Pentingnya keamanan mengharuskan para pengembang *website* untuk menjaga *websitenya*. Salah satunya adalah melindungi informasi-informasi dari para pengguna *website* itu sendiri. Banyaknya kasus pencurian informasi pengguna, menandakan bahwa masih banyaknya *website* yang tidak mengedepankan sistem keamanaan *website*. Terutama sistem keamanan enkripsi yg bertujuan untuk melindungi informasi pengguna sehingga tidak terlihat oleh orang lain. Lemahnya sistem keamaanan enkripsi dimanfaatkan oleh para penyerang untuk memperoleh informasi pengguna yang bersifat *private* (rahasia).

Dengan sistem keamanaan enkripsi yang tidak dan kelalaian pengembang untuk selalu memperbaharui sistem keamanan website merupakan salah satu faktor rentannya kemanan dari *website* tersebut. Selain keamanan internal *website*, dibutuhkan pula sistem keamanan pendukung untuk melindungi informasi-informasi yang ada di *website* tersebut. Maslah timbul ketika, bagaimana sistem keamanan pendukung tidak mampu melindungi informasi-informasi yang ada di *website* terutama informasi-informasi penting dari pengguna. Sebagai contoh *username* dan *password* dari pengguna *website*.

Sebuah *website* yang memiliki sistem keamanan berupa protokol *HTTPS* yang berguna untuk melindungi jalur komunikasi antara pengguna dan *server.* Data pengguna yang dikirim ke *server* secara langsung akan melewati protokol *HTTPS*. Data tersebut akan disimpan di memory sementara server atau yang lebih dikenal dengan istilah *RAM (Random Access Memory)* sebelum disimpan ke *storage server*. Dari sini maka timbul pertanyaan, bagaimana jika *protocol HTTPS* tersebut digunakan oleh penyerang untuk memperoleh data pengguna yang terdapat di memori sementara *server*.

Dari pertanyaan tersebut, penulis akan melakukan penetrasi terhadap *server* untuk membuktikan bahwa protokol *HTTPS* yang digunakan oleh *server* memiliki kelemahan. Penetrasi ini bertujuan untuk mendapatkan informasi yang dikirim oleh pengguna ke *server* yaitu *username* dan *password.* Dari kelemahan yang dimiliki oleh protokol *HTTPS* pada *server* tersebut, penulis juga akan melakukan implementasi ulang *SSL* pada *server* SITU Unpas. *SSL* yang akan diimplementasikkan adalah *OpenSSL*

v1.0.2. Setelah dilakukan pemasangan *OpenSSL v1.0.2* pada *server* penulis akan melakukan pengujian ulang demi memastikan *OpenSSL v1.0.2* yang diimplementasikan aman untuk melindungi protokol *HTTPS*.

1.2 Identifikasi Masalah

Masalah yang didapatkan oleh penulis sebagai salah satu rumusan pada penelitian tugas akhir, maka penulis secara umum mengidentifikasi masalah yang meliputi :

1. Bagaimana cara menanggulangi sistem kemanan *SSL* pada *website* SITU FT Unpas terhadap serangan *heartbleed*?
2. Apakah sistem keamanan *SSL* yang dipakai oleh SITU Unpas sudah menjamin kerahasiaan informasi pengguna?

1.3 Batasan Masalah

Adapun batasan masalah dari penelitian Tugas Akhir ini adalah :

1. Jenis serangan yang dilakukan adalah *Heartbleed*.
2. Tidak membahas *custom script* pada tahap pengujian.
3. Sistem Operasi yang digunakan dalam tahap pengujian adalah *Linux Backtrack*.

1.4 Tujuan Tugas Akhir

Adapun tujuan dan maksud tugas akhir ini adalah sebagai berikut :

1. Menanggulangi serangan *Heartbleed* pada *website* SITU FT Unpas.
2. Menjamin kerahasiaan informasi pengguna SITU Unpas.

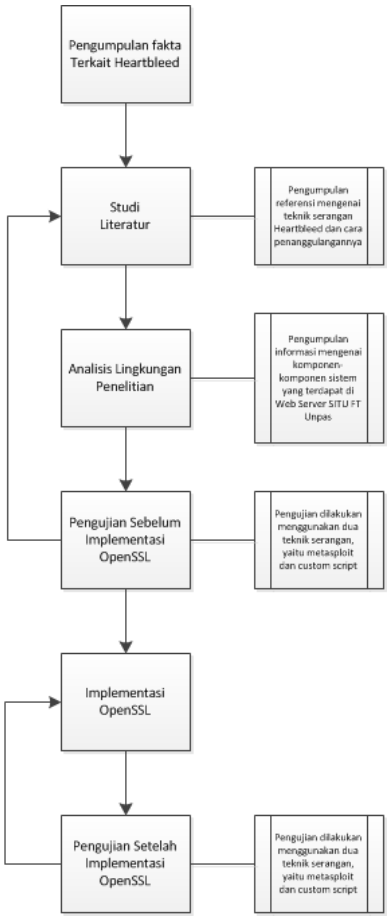
1.5 Lingkup Tugas Akhir

Adapun lingkup masalah pada penelitian Tugas Akhir adalah sebagai berikut :

1. Solusi yang akan dipakai untuh mecegah serangan *Heartbleed* adalah *OpenSSL 1.0.2*.
2. Metode yang digunakan dalam pengujian adalah *metasploi*t dan *custom script.*

1.6 Metodologi Tugas Akhir

Pada pembuatan tugas akhir ini penulis menggunakan metode penelitian sebagai berikut berdasarkan pada gambar 1.1 :



Gambar 1.1 Metodologi Tugas Akhir

Berikut ini merupakan penjelasan pada gambar 1.1 :

1. Tahap Pengumpulan Fakta terkait Heartbleed

   Pada tahap ini penulis melakukan pengumpulan fakta-fakta terkait dengan serangan *Heartbleed*.

2. Tahap Studi Literatur

   Tahap ini adalah tahap pencarian referensi dan sumber-sumber yang berhubungan dengan teknik serangan *Heartbleed*, sistem pencegahan serangan *Heartbleed* dan peng-implementasiannya.

3. Tahap Analisis Lingkungan Penelitian

   Pada tahap ini penulis melakukan analisis terhadap lingkungan penelitian, untuk mengetahui komponen-komponen sistem yang terdapat di *web server* SITU FT Unpas.

4. Tahap Pengujian Sebelum Implementasi OpenSSL

   Tahap pengujian ini dilakukan sebelum implementasi system yang akan dibangun oleh penulis. Pada tahap ini dimaksudkan untuk mengetahui tingkat keamanan sistem yang telah digunakan SITU FT Unpas. Pengujian dilakukan dengan cara melancarkan paket serangan ke sistem yang dilindungi.

5. Implementasi OpenSSL

   Pada tahap ini, akan dilakukan implementasi sistem yang akan dibangun oleh penulis untuk mencegah serangan *Heartbleed*.

6. Tahap Pengujian Setelah Implementasi OpenSSL

   Tahap pengujian ini dilakukan setelah implementasi sistem yang dibangun oleh penulis. Untuk mengetahui tingkat keberhasilan dari sistem yang telah dibangun oleh penulis apakah mampu tahan terhadap serangan *heartbleed*.

1.7 Sistematika Penulisan Tugas Akhir

Secara umum keseluruhan laporan tugas akhir ini terdiri dari lima bab serta terdapat daftar pustaka, penjelasan mengenai tiap babnya adalah sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini berisi uraian singkat mengenai latar belakang tugas akhir, identifikasi masalah dari tugas akhir, tujuan dan maksud dari tugas akhir, lingkup tugas akhir serta metode dan sistematika pembahasan tugas akhir.

BAB 2 LANDASAN TEORI

Bab ini berisi penjelasan tentang dasar – dasar teori mengenai SSL, OpenSSL, Serangan Heartbleed dan cara penanggulangannya.

BAB 3 ANALISIS DAN PENGUJIAN

Bab ini berisi penjelasan tentang analisis dan pengujian serangan *Heatbleed* dimulai dari pengujian menggunakan *tools metaploit* dan *custom script*. kerangkat tugas akhir, skema analisis, skenario pengujian, analisis kebutuhan *hardware* dan *software*.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi tentang implementasi *OpenSSL v1.0.2* untuk kemudian dilakukan pengujian ulang dengan metode yang sama dengan tujuan mengetahui perbedaan hasil dari pengujian sebelum dan sesudah dilakukannya implementasi *OpenSSL v1.0.2*.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan beserta dengan saran selama pelaksanaan dan pengerjaan tugas akhir

DAFTAR PUSTAKA

Daftar pustaka berisi sumber penjelasan di dalam pelaksanaan tugas akhir.

DAFTAR LAMPIRAN

Bab ini menjelaskan mengenai lampiran – lampiran dokumen dan surat yang digunakan dalam pengerjaan tugas akhir.