BAB 1
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi yang sangat cepat telah membawa manusia memasuki kehidupan yang berdampingan dengan informasi dan teknologi itu sendiri. tetapi tidak hanya memberikan sejumlah fasilitas yang canggih. Namun, teknologi informasi juga memiliki sejumlah masalah yang berhubungan dengan keamanan. salah satunya adalah penyadapan, ancaman keamanan yang disajikan oleh penyadapan adalah kemampuan mereka untuk menangkap semua lalu lintas masuk dan keluar, termasuk *password* dan *username* atau bahan sensitif lainnya. Tidak seorang pun ingin mengirim data pribadi mereka melalui internet kecuali mereka memiliki jaminan bahwa hanya penerima dimaksud yang akan menerimanya. Keamanan data pada komunikasi di jaringan merupakan hal utama yang begitu penting dalam kerahasian informasi.

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. HTTPS adalah HTTP yang menggunakan *secure socket layer* (SSL). *SSL* adalah *protokol enkripsi* dipanggil melalui *web server* yang menggunakan HTTPS. *SSL* adalah jenis *sockets communications* berada diantara *transmision control protocol/internet protocol (TCP/IP)* dan *application layer*. *SSL* biasanya digunakan antara *server* dan *client* untuk mengamankan sambungan. Akan tetapi studi lebih lanjut untuk menguji keamanan transaksi *protokol SSL* sendiri perlu dilakukan untuk melihat sejauh mana protokol *SSL* dapat mengamankan data di jaringan Ketika komputer mengirimkan data melalui jaringan tersebut.

Dinas Kominfo Bangka Selatan adalah dinas komunikasi dan informatika yang berada di kota Toboali ini merupakan dinas yang mengurus bagian

komunikasi dan informatika, Aktivitas yang dilakukan oleh para pegawai dalam bekerja salah satunya adalah mengakses *website* kantor tetapi belum menerapkan protokol *https* pada *web server* tersebut.

Dengan menerapkan keamanan pada *website* di dinas Komunikasi dan Informatika Bangka Selatan sehingga tidak akan ada data dan informasi yang di curi atau dirusak oleh orang-orang yang tidak bertanggung jawab. oleh karena itu, dibutuhkan metode untuk meningkatkan keamanan transfer data melalui *HTPPS*, yaitu dengan mengimplementasi keamanan *transfer* data pada *web server* menggunakan *OpenSSL* di mana terdapat konfigurasi tertentu untuk mengamankan data ketika suatu file di *transfer*.

Beberapa penelitian yang terkait dengan penulis lakukan diantaranya, penelitian, Bayu Arie *Nugroho* (2012)[1], mengenai *"Analisis Keamanan Jaringan Pada Fasilitas Internet (wifi) Terhadap Serangan Packet Sniffing"*. penelitian, Aprianti Putri Sujana (2014)[2], mengenai "*Perangkat Pendukung Forensik Lalu Lintas Jaringan".* Penelitian, Pranata, H.dkk. (2015)[3], mengenai *"Analisis Keamanan Protokol Secure Socket Layer (SSL)".* penelitian M. Ferdy Adriant. (2015)[4]. mengenai "*Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan".* Penelitian, Adzan Abdul Zabar (2015)[5]. Mengenai "*Keamanan Http Dan Https Berbasis Web Menggunakan Sistem Operasi Kali Linux*".

Berdasarkan masalah yang ada, maka penulis mengangkat judul pada Skripsi ini yaitu : *"Implementasi Keamanan Transfer Data Pada Web Server Menggunakan OpenSSL Di Dinas Komunikasi Dan Informatika Bangka Selatan".*

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah diatas pada rumusan masalah yang didapat sebagai berikut :

1. Bagaimana mengimplementasikan metode *SSL (Secure Socket Layer)* pada *Web Server?*
2. Bagaimana mengintegrasikan metode yang terkait dengan system keamanan pada *Web Server* tersebut?
3. Bagaimana uji coba *login* di pantau menggunakan aplikasi *Wireshark*?

1.3. Batasan Masalah

Untuk mempermudah dan membatasi ruang lingkup masalah dalam penelitian ini, maka diberikan batasan-batasan sebagai berikut:

1. *Server* ini di buat di *Linux Debian versi 9.8.0*
2. Pengujian pada penelitian ini hanya dilakukan semulasi login dari pengguna ke *web server.*
3. Penelitian ini tidak membahas *Algoritma Kriptografi* yang di gunakan oleh *OpenSSL*.

1.4. Tujuan Dan Manfaat Penelitian

1.4.1. Tujuan Penelitian

Adapun Tujuan Implementasi Keamanan Transfer Data Pada *Web Server* Menggunakan *OpenSSL* adalah sebagai berikut :

1. Untuk membangun Sistem Kemanan *Transfer Data* Pada *Web Server* tersebut.
2. Untuk melindungi keamanan informasi-informasi dan *Transfer Data* terhadap akses, penggunaan, pengungkapan, gangguan, modifikasi atau pengancuran.
3. Untuk mempermudah pegawai dalam keamanan mentransfer data dari setiap instansi kantor ke *server.*

1.4.2. Manfaat Penelitian

Adapun Manfaat Implementasi Keamanan *Tranfer* Data Pada *Web Server* Menggunakan *OpenSSL* adalah sebagai berikut :

1. Dapat menjaga informasi sensitif selama dalam proses pengiriman melalui internet dengan cara dienkripsi, Sehingga hanya penerima pesan yang dapat memahami dari hasil *enkripsi* tersebut. *SSL* memberikan *enskripsi* data melalui HTTPS yang akan melindungi data pengunjung *website* pengguna, memberikan integrits data sehingga pengguna mengetahui bahwa data atau *website* tersebut tidak mampu dimodifikasi atau dirusak.

2. Dapat melindungi pencurian data dalam bentuk pemalsuan yang dikirim oleh seorang kriminal yang mencoba untuk meniru tampilan *website* tersebut.
3. Dapat mempermudah semua instansi dalam *transfer* data

1.5 Sistematika Penulisan Laporan

Agar laporan penelitian ini dapat dipahami dengan lebih jelas, maka sistematika penulisan laporan ini di bagi menjadi sub bab dimana tiap sub babnya terdiri dari pokok pembahasannya sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, manfaat dan tujuan penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menjelaskan mengenai definisi dan teori-teori dari berbagai sumber dan referensi yang membahas tentang Implementasi keamanan *transfer data* pada *web server* menggunakan *OpenSSL*.

BAB III ORGANISASI

Bab ini berisi tentang latar belakang, profil, sejarah, struktur organisasi, dan visi dan misi dari tempat penelitian.

BAB IV PEMBAHASAN

Memaparkan dari hasil-hasil tahapan penelitian, mulai dari analisis, desain, hasil *testing* dan implementasinya.

BAB V PENUTUP

Bab ini adalah bab terakhir yang menguraikan kesimpulan serta saran yang didapat dari seluruh hasil penelitian pada tempat penelitian.