1. Pendahuluan

1.1 Latar Belakang Masalah

Perkembangan teknologi yang semakin maju mengakibatkan tingkat kebutuhan terhadap keamanan informasi menjadi penting. Seiring berkembangnya informasi munculah permasalahan baru mengenai keamanan jaringan itu sendiri. Contoh ancaman keamanan jaringan yang sering terjadi adalah pengendusan aktivitas di jaringan atau biasa disebut *sniffing*, serangan ini memungkinkan informasi penting seperti password dari suatu account bisa diketahui oleh hecker, selain ancaman pengendusan juga terdapat ancaman lainnya seperti *MITM* attack (man in the middle) yang memungkinkan attacker berada di tengah komunikasi bebas mendengarkan dan mengubah percakapan antara dua pihak dan masih banyak lagi serangan yang ada. Mulailah berkembang anggapan bahwa internet merupakan tempat yang tidak aman. Banyak protokol yang menggunakan internet tidak memberikan sistem autentikasi yang aman pada sistem informasinya. Beberapa system menggunakan firewall untuk mengatasi masalah keamanan jaringan. Tetapi sayangnya, firewall mengasumsikan bahwa ancaman bahaya berasal dari luar, padahal seringkali pada kenyataannya tidaklah demikian. Ancaman bahaya justru sering datang dari dalam.

Karena hal-hal tersebut di atas, maka diperlukan suatu protokol yang dapat diandalkan dalam autentikasi. Terdapat berbagai macam protokol yang bisa digunakan, tetapi tidak semuanya bisa menahan serangan dari penyusup. Dalam Tugas Akhir ini dibahas dua mekanisme autentikasi menggunakan protokol autentikasi *kerberos* dan penggunaan *HTTP over SSL*, baik kerberos maupun *HTTP over SSL* keduanya memiliki kelebihan masing-masing dalam autentikasi dan dari segi keamanan jaringan. Kerberos sudah banyak diterapkan dalam sebuah system yang membutuhkan mekanisme autentikasi efektif dan aman dalam pemenuhan banyak layanan di jaringan. *HTTP over SSL* menyediakan autentikasi yang membutuhkan tingkat keamanan yang tinggi seperti yang telah banyak diterapkan di aplikasi web yang membutuhkan transaksi aman dalam operasionalnya. Antara Kerberos dan *HTTP over SSL* bisa digunakan dalam autentikasi client dan server. Dari hal tersebut dibandingkan penggunaan autentikasi yang komplek dan yang sederhana apakah memiliki pengaruh yang signifikan dalam masalah keamanan di jaringan.

Kerberos merupakan suatu protocol autentikasi jaringan yang dirancang untuk memberikan autentikasi yang kuat, *Kerberos* memungkinkan client dan server untuk saling mengotentikasi sebelum melakukan koneksi [8]**.** Sedangkan *HTTP over SSL* atau yang biasa diimplementasikan dengan HTTPS merupakan protokol HTTP yang menggunakan Secure Socket Layer (SSL) sebagai sublayer dibawah HTTP sehingga keamanan lebih terjamin [9]. Kedua autentikasi tersebut memiliki kelebihan dan kekurangan masing-masing. Dari analisis segi mekanisme kedua sistem autentikasi tersebut, dapat diduga bahwa kerberos bisa diandalkan untuk menjamin keamanan autentikasi di banding menggunakan *HTTP over SSL*

karena dilihat dari mekanisme kerberos yang menggunakan suatu tiket granting dalam prosesnya.

Pada Tugas Akhir ini di implementasikan dan dibandingkan metode mana yang bisa diandalkan dalam proses autentikasi dari segi ketahanan terhadap serangan dari luar seperti sniffing dan MITM attack dengan kata lain dari segi keamanannya.

1.2 Perumusan Masalah

Rumusan masalah yang ada pada Tugas Akhir ini yaitu sebagai berikut :

- Bagaimana ketahanan terhadap serangan pada protokol *kerberos* dan *HTTP over SSL*.
- Bagaimana hasil perbandingan terhadap serangan pada *kerberos* dan *HTTP over SSL*.

Adapun batasan masalah dari Tugas Akhir ini adalah :

- OS yang digunakan dalam pengujian adalah windows server 2003, windows XP karena OS tersebut telah memenuhi resaurce yang dibutuhkan dalam tahap pengujian.
- Hal yang dianalisis adalah dari segi keamanan autentikasi terhadap serangan sniffing
- Skenario uji serangan yang dipakai menggunakan serangan *MITM* attack (man in the middle), Password Attacks karena serangan tersebut berhubungan dengan mekanisme autentikasi.

1.3 Tujuan

Adapun tujuan yang ada pada Tugas Akhir ini adalah sebagai berikut :

- Menganalisis mekanisme autentikasi dari penggunaan *kerberos* dan *HTTP over SSL* sebagai protokol autentikasi.
- Menganalisis perbandingan keamanan autentikasi dalam hal ini adalah ancaman serangan dari penggunaan *kerberos* dan *HTTP over SSL* sebagai protokol autentikasi.

1.4 Metodologi Penyelesaian Masalah

Metodologi yang akan digunakan dalam menyelesaikan Tugas Akhir ini adalah sebagai berikut :

- Identifikasi
  Kerberos merupakan suatu protocol autentikasi jaringan. Kerberos dirancang untuk memberikan autentikasi yang kuat. Kerberos memungkinkan *client* dan *server* untuk saling mengotentikasi sebelum melakukan koneksi [8]. Beberapa situs menggunakan firewall untuk

mengatasi masalah keamanan jaringan mereka. Tetapi, firewall mengasumsikan bahwa ancaman bahaya berasal dari luar, padahal seringkali pada kenyataannya tidaklah demikian. Ancaman bahaya justru sering datang dari dalam. Kerberos merupakan protokol autentikasi yang bisa diandalkan, kerberos dirancang untuk memberikan autentikasi yang kuat untuk aplikasi client/server dengan menggunakan *secret-key cryptography* [19].

HTTP over SSL atau yang biasa diimplementasikan dengan HTTPS merupakan protokol HTTP yang menggunakan Secure Socket Layer (SSL) sebagai sublayer dibawah HTTP sehingga keamanan lebih terjamin. Dengan HTTPS kita dapat melakukan proteksi data yaitu hanya penerima saja yang dapat membaca data, Kenyamanan (data privacy), memungkinkan identifikasi server ataupun client, otentikasi server dan klien, dan integritas data[9]. SSL adalah protokol yang memiliki tingkat keamanan sangat tinggi [13]. Perkembangan Internet yang cukup pesat membawa pengaruh yang cukup besar bagi pihak-pihak yang memanfaatkan internet untuk melakukan berbagai hal misalnya tukar-menukar data, transaksi online, promosi dan lain-lain. Dengan adanya kejahatan-kejahatan internet ini para pengguna semakin tidak aman dan menjadi intaian para penjahat setiap kali mereka berinternet. SSL menyediakan metode enkripsi yang digunakan untuk mengamankan data dengan mengubah data asli kedalam bentuk unicode dengan aturan tertentu.

- Literatur

  Mempelajari literatur-literatur yang berkaitan dengan konsep Autentikasi, kerberos, HTTP over SSL ,sniffing MITM attack (man in the middle), Password Attacks, hacking kemudian melakukan kajian terhadap materi-materi tersebut.

- Desain Penelitian

  Model autentikasi yang diterapkan adalah menggunakan *kerberos* dan *HTTP over SSL*, dimana untuk setiap protokol autentikasi akan dibuat prototype autentikasinya dengan menggunakan satu platform OS yang sama pada saat tahap pengujian.

  Setelah dibuat prototype dari kedua model autentikasi dilakukan serangan untuk kedua model tersebut. Jenis serangan yang dilakukan adalah *sniffing* dengan *MITM attack* dan Password *attacks.* Pemilihan serangan dilakukan untuk menganalisis paket data yang bisa dimanfaatkan untuk masuk dalam sistem. *MITM attack* dan Password *attacks* merupakan serangan yang dilakukan oleh para hacker dalam menyusup sebuah sistem.

  a. *MITM* attack (man in the middle) yang memungkinkan attacker berada di tengah bebas mendengarkan dan mengubah percakapan antara dua pihak. Man-In-The-Middle Attack adalah sebuah aksi sniffing yang memanfaatkan kelemahan switch dan kesalahan penangannan ARP chache dan TCP/IP [10]. Awalnya adalah menempatkan komputer hacker ditengah dua komputer yang sedang berhubungan sehingga paket data harus melalui komputer hacker dulu agar paket data itu bisa

dilihat atau diintip oleh hacker. Aplikasi yang digunakan adalah Ettercap, ARPSpoof.

b. Password attacks
   Menggunakan teknik brute force dimana serangan dilakukan oleh sebuah aplikasi untuk menyusup pada sistem.

Tujuan dari dilakukan serangan adalah :

a. untuk mengetahui apakah terdapat celah pada sistem keamanan menggunakan kedua protokol tersebut.
b. untuk mengetahui tingkat ketahanan keamanan dari penerapan kedua protokol tersebut terhadap serangan yang dilakukan

- Pengujian
  Pengujian yang dilakukan adalah dari segi autentikasi menggunakan kedua model yang ada kemudian dilakukan serangan untuk tiap model sesuai dengan skenario serangan.
  Metrik pengujian secara kuantitatif dilakukan dengan banyaknya serangan yang berhasil, kemudian pengujian secara kualitatif dimana informasi apa saja yang didapatkan dari proses sniffing untuk tiap protokol yang diuji. Setelah dilakukan pengujian lakukan analisis sesuai tujuan dari dilakukannya serangan.
  Hasil yang diharapkan tercapai adalah :
  a. Mengetahui bagaimana ketahanan terhadap serangan pada protokol *kerberos*.
  b. Mengetahui bagaimana ketahanan terhadap serangan pada *HTTP over SSL*.

- Analisis
  Menganalisis hasil dari pengujian diatas dengan menggunakan sampel pengujian sesuai pada tahap pengujian dengan batasan jumlah serangan attack yang telah ditentukan, kemudian di buat kesimpulan yang ada sesuai dengan tujuan tugas akhir ini.

- Pembuatan Laporan
  Mendokumentasikan tahap-tahap yang telah dilakukan pada bagian metodologi ini mulai dari studi literatur sampai analisis hasil testing yang berisi kesimpulan sebagai bahan literatur penelitian.