BAB 1 PENDAHULUAN

1.1 Latar Belakang

Pesatnya dunia jaringan komputer membawa dampak yang tidak sederhana. Perkembangan dunia jaringan komputer ini juga membawa dampak negatif dalam beberapa hal. Salah satunya dampak negatif tersebut adalah semakin kompleksnya pengelolaan sistem-sistem yang terdapat dalam jaringan, khususnya pada permasalahan pengelolaan *user*. Penambahan *user* baru merupakan pekerjaan yang masih tergolong relatif sederhana ketika jaringan hanya terdiri dari lima server atau bahkan kurang dari jumlah itu. Masing-masing server dapat dengan mudah saling terhubung, melakukan penambahan akun *user* baru dengan tetap menjaga konsistensinya, mengatur password, dan notifikasi *user*. Akan tetapi proses-proses ini menjadi tidak mudah ketika lingkungan jaringan berkembang menjadi sepuluh, lima puluh, seratus server atau bahkan lebih. Pengelolaan jaringan akan semakin sulit karena banyaknya aplikasi-aplikasi yang diimplementasikan dalam jaringan. Semakin banyak sistem dan aplikasinya maka semakin banyak mekanisme login yang diberlakukan. *User* akan disibukkan dengan mengingat banyak kombinasi *userid* dan *password*, atau disulitkan dengan mekanisme login yang berulang-ulang (Garman,2002).

Sistem direktori terpusat telah banyak dimanfaatkan sebagai solusi dari persoalan ini. Sistem direktori terpusat ini menawarkan SingleID dan dapat dimanfaatkan untuk keperluan *single sign on* sehingga pengelolaan jaringan besar menjadi lebih mudah (Christian, 2004).

Single sign on telah banyak dibicarakan sebagai solusi dalam pengelolaan login dalam jumlah besar. Hampir sebagaian besar *user* pada sistem IT yang modern

seperti sekarang ini, akan menghadapi metode *multiple login*. Metode *multiple login* banyak memberikan dampak negatif bagi pihak yang mengimplementasikan. Resiko *multiple login* dari sisi waktu yang dihabiskan yaitu, ketika harus melakukan login berulang-ulang dibandingkan dengan metode single login. Aspek lain yang tidak kalah penting adalah dari segi biaya. Biaya yang dimaksud disini adalah biaya yang dihabiskan ketika *user* menghubungi *help desk* saat *user* lupa akan kombinasi userid dan password miliknya. Selain kedua aspek tersebut, aspek berikutnya adalah dari segi keamanan penyimpanan password. Beberapa *user* memilih untuk menuliskan password pada kertas atau media lainnya yang justru tidak aman karena dapat diketahui pihak lain selain *user* yang bersangkutan (Christian, 2004).

Konsep dasar dari adalah bagaimana agar *user* hanya perlu melakukan login sekali dan untuk kemudian computer akan menggantikan perannya pada login-login berikutnya secara otomatis atas nama *user* tersebut. Senada dengan konsep *Single sign on*, Single ID juga merupakan suatu konsep yang bertujuan memudahkan pengelolaan administrasi jaringan. Single ID ini merupakan konsep dari identitas tunggal untuk banyak aplikasi. Beban *user* untuk mengingat bermacam-macam kombinasi userid dan password dapat dikurangi atau bahkan dieliminasi.

Selain itu, dengan adanya direktori terpusat ini dapat dikembangkan suatu system terdistribusi, baik aplikasi direktori terdistribusi, maupun system terdistribusi lainnya. Salah satu teknologi yang ada untuk keperluan direktori terpusat yaitu *Lightweight Directory Access Protocol* (LDAP). LDAP merupakan protocol yang ditujukan untuk pengaksesan direktori (Wahl,1997).

Lightweight Directory Access Protocol (LDAP) telah banyak dimanfaatkan untuk penggunaan aplikasi-aplikasi direktori yang semakin meningkat seperti *mail server* dan *remote login*. Direktori LDAP digunakan untuk penyimpanan informasi

personal dan aturan-aturan otentikasi. Data yang disimpan bersifat statis sehingga cache bisa digunakan untuk peningkatan kinerja (Uli, 2000).

Pengaksesan direktori menggunakan LDAP memiliki kelemahan dalam sistem keamanannya. Banyak implementasi LDAP tanpa memperhatikan keamanan saat pengaksesan data. Data seperti misalnya userid dan password masih ditranmisikan melalui jaringan pada saat pengaksesan direktori. Hal ini menjadi lubang keamanan yang tidak bisa diremehkan mengingat banyaknya metode kejahatan cyber di era sekarang.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, dapat diambil rumusan yang menjadi permasalah utama dalam tugas akhir ini yaitu :

1. Bagaimana membuat sistem direktori terpusat dengan menggunakan LDAP sehingga dapat dimanfaatkan untuk keperluan *single sign on* sehingga pengelolaan jaringan besar menjadi lebih mudah.
2. Bagaimana membuat sebuah sistem otentikasi yang memberikan keamanan saat pengaksesan direktori LDAP.
3. Menutupi kelemahan dari system otentikasi direktori LDAP dengan menggunakan protokol Kerberos

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telah disebutkan sebelumnya, maka batasan yang diberikan untuk rumusan masalah diatas yaitu :

1. Proses otentikasi, penyimpanan dokumen dan proses backup dilakukan secara terpusat dalam server LDAP.

2. Pengujian sistem otentikasi Kerberos dengan GSSAPI, sebagai mekanisme yang digunakan dalam protokol Kerberos.
3. Dalam penelitian ini hanya akan diadakan sebuah master KDC (*Key distribution center*) tanpa mengadakan replikasinya.

1.4 Tujuan Penelitian

Tujuan dalam melakukan penelitian ini adalah mengembangkan sistem otentikasi yang aman bagi pengaksesan direktori LDAP. Tujuan berikutnya dari penelitian ini yaitu menguji sistem otentikasi LDAP yang menggunakan protokol Kerberos dengan sistem otentikasi LDAP tanpa adanya Kerberos.

1.5 Manfaat Penelitian

Penetian ini diharapkan akan mampu memberikan manfaat, diantaranya :

1. Memberikan kemudahan otentikasi bagi *user* yang mengakses direktori LDAP.
2. Memberikan kemudahan kepada admin jaringan dalam pengelolaan sistem yang menggunakan LDAP sebagai backend jaringannya.
3. Menawarkan keamanan selama pengaksesan sumber informasi yang tersimpan dalam direktori LDAP.

1.6 Metode Penelitian

1.6.1 Studi Pustaka

Pada penelitian ini, langkah-langkah penyelesaian diawali dengan studi pustaka. Studi pustaka, yaitu pengumpulan literatur melalui buku- buku dan sumber lain yang berkaitan dengan penelitian yang dilakukan dalam rangka mencari konsep dasar dari penelitian ini.

Selain itu, langkah ini juga didapat dari pengumpulan literatur melalui internet, yang dilakukan dengan tujuan pemilihan perangkat lunak yang akan diimplementasikan sebagai Sistem *Authentikasi* Kerberos, serta pencarian referensi mengenai tahap dalam implementasi, termasuk kebutuhan *hardware* serta *software* pendukung lainnya agar sistem berjalan dengan baik. Kemudian membahas tentang pengembangan sistem otentikasi menggunakan sistem otentikasi LDAP yang menggunakan protokol Kerberos dengan sistem otentikasi LDAP tanpa adanya Kerberos.

1.6.2 Implementasi Perangkat Lunak

Implementasi dilakukan berdasarkan hasil dari langkah pengumpulan literatur yang meliputi :

1. Desain Arsitektur Jaringan dan Alokasi *Account*

   Tahap ini merupakan tahap perancangan arsitektur jaringan komputer yang akan digunakan untuk membangun Sistem *Authentikasi* Kerberos serta pengalokasian *account* pada directory LDAP.
2. Pengadaan *Hardware*

   Tahapan ini merupakan tahap pengadaan perangkat keras untuk Sistem *Authentikasi* server, serta komputer yang menjadi *client* dari Sistem *Authentikasi* Kerberos tersebut. Selain itu diperlukan pula perangkat keras yang digunakan sebagai pendukung keberlangsungan transmisi data *client*.
3. Instalasi dan Konfigurasi *Software*

   Tahapan ini merupakan tahap instalasi *software* pada komputer yang akan dijadikan Sistem *Authentikasi* Kerberos, serta komputer yang akan dijadikan *client*. Kemudian dilanjutkan dengan melakukan konfigurasi *software* pada Sistem *Authentikasi* Kerberos serta *client-client*.

4. Pengujian

   Setelah konfigurasi selesai dilakukan, tahap selanjutnya adalah pengujian kinerja Sistem *Authentikasi* Kerberos tersebut dalam menghadapi adanya penggunaan *account* oleh pihak yang tidak memiliki hak akses. Protokol Kerberos melakukan otentikasi dengan menggunakan *ticket* yang dikeluarkan oleh pihak ketiga dan *authenticator* yang dibuat sendiri oleh *client.* Pada tahap ini, dilakukan uji coba Sistem *Authentikasi* yang menggunkan Kerberos dan Sistem *Authentikasi* yang tidak menggunakan Kerberos

   Dengan dibangunnya protokol Kerberos dapat mengetahui perbedaan keamanan yang menggunakan Kerberos ataupun tidak.

1.7 Sistematika Penulisan

Penulisan laporan tugas akhir akan disusun dalam tujuh bab. Berguna untuk memberikan gambaran tentang permasalahan yang akan dibahas, dibawah ini penulis uraikan sistematika penulisan tugas akhir ini nantinya :

BAB I	PENDAHULUAN Bab ini berisi latar belakang masalah, perumusan masalah, batasan masalah, tujuan dan penelitian, metodelogi penelitian, dan sistematika penulisan.
BAB II	TINJAUAN PUSTAKA Bab ini berisi penjelasan yang memuat uraian sistematis tentang informasi hasil penelitian *Single sign on* yang memanfaatkan LDAP, kemudian penelitian mengenai protokol LDAP yang digunakan sebagai *backend* manajemen suatu jaringan Wi-Fi. Pada bab ini diuraikan pula perbedaan-

	perbedaan antara penelitian-penelitian sejenis sebelumnya dengan penelitian yang dilakukan kali ini.
BAB III	LANDASAN TEORI Bab ini berisi uraian mengenai landasan teori yang harus dipahami sebelum membahas bagian inti dari tugas akhir, yaitu mengenai perbedaan konsep otentikasi dan otorisasi, hal-hal yang berkaitan dengan protokol Kerberos, dan teori-teori tentang LDAP. Sub bab otentikasi dan otorisasi menguraikan definisi otentikasi dan otorisasi, serta menguraikan perbedaan-perbedaan yang mendasar diantara dua konsep tersebut. Sub bab Kerberos memberikan penjelasan mengenai dasar, terminology dan konsep kerja Kerberos. Sub bab LDAP memberikan penjelasan tentang dasar, skema dan konsep kerja LDAP.
BAB IV	ANALISIS DAN PERANCANGAN SISTEM Bab ini menjelaskan tentang perancangan arsitektur dalam sistem otentikasi LDAP menggunakan Kerberos yang akan diimplementasikan, kemudian menerangkan peran Kerberos bagi LDAP serta modul-modul SASL GSSAPI yang akan digunakan untuk keperluan pengimplementasian Kerberos pada direktori LDAP.
BAB V	IMPLEMENTASI Bab ini berisi penjelasan mengenai instalasi dan konfigurasi pada Kerberos dan LDAP berserta modul-modul SASL GSSAPI yang diperlukan untuk mengintegrasikan keduannya.