SARI

Pesatnya perkembangan dunia jaringan memberikan keuntungan dalam segi ekonomi, akan tetapi hal tersebut juga memberikan dampak yang lain. Pengelolaan pengguna yang semakin komplek menjadi salah satu dari kendala yang harus dihadapi. Salah satu solusi yang bisa digunakan adalah dengan mekanisme direktori terpusat. Mekanisme ini menawarkan sistem jaringan yang terpusat sehingga memudahkan dalam pengolahannya. Teknologi yang biasa digunakan dalam hal ini adalah *Lightweight Directory Access Protocol* (LDAP). LDAP merupakan protokol komunikasi yang memberikan fleksibilitas pada data yang bisa disimpan dalam direktori LDAP. Salah satu hal yang patut disayangkan bahwa standar keamanan dari LDAP masih melewatkan *username* dan *password* dalam jaringan. Oleh karena itu diperlukan suatu mekanisme otentikasi yang mampu memberikan *layer* keamanan tambahan diwaktu pengaksesan direktori LDAP.

Perancangan sistem yaitu dengan menambah layer otentikasi bagi pengaksesan LDAP menggunakan Kerberos. Ha yang dilakukan dalam penelitian antara lain konfigurasi Kerberos sesuai dengan tujuan penelitian. Selain konfigurasi pada Kerberos, dilakukan juga konfigurasi pada LDAP untuk pengelolaan informasi *user*. Kedua fungsi tersebut diintegrasikan dengan SASL GSSAPI. Selanjutnya dilakukan analisis terhadap kinerja sistem diwaktu menggunakan Kerberos dengan sistem tanpa Kerberos.

Penelitian ini berhasil mengembangkan sistem otentikasi LDAP dengan menggunakan Kerberos. Pengujian dilakukan terhadap sistem otentikasi LDAP yang menggunkan Kerberos dan sistem otentikasi LDAP tanpa Kerberos. Hasil dari pengujian tersebut menunjukkan bahwa sistem otentikasi LDAP dengan Kerberos lebih aman karena *user* tidak perlu mengirimkan *user*name dan password diwaktu mengakses direktori LDAP, akan tetapi waktu yang dibutuhkan membutuhkan waktu akses yang relative lebih lama dibandingkan dengan sistem otentikasi tanpa adanya Kerberos.

Kata kunci :

Sistem Otentikasi Lightweight Directory Access Protocol Menggunakan Kerberos