ABSTRAK

Single Sign On merupakan sebuah sistem *authentifikasi* terhadap user, dimana user bisa mengakses beberapa aplikasi tanpa harus login dimasing masing aplikasi. Tujuan dari perancangan *Single Sign On* adalah untuk mengabungkan sistem *authentifikasi* dari beberapa aplikasi atau layanan. Dalam perkembangan teknologi informasi secara tidak langsung menuntut pengguna aplikasi untuk mengelola data *account* dengan baik agar tidak disalah gunakan oleh pihak yang tidak bertanggung jawab. Beberapa metode keamanan user *account* telah diusulkan untuk memecahkan masalah-masalah tersebut, diantaranya dengan menerapkan *authentication Single Sign On* dengan menggunakan protokol LDAP.

Pada tugas akhir ini metode yang digunakan untuk menguji keamanan sistem *single sing on* adalah *Man In The Middle Attack*, *LDAP Injection* dan *Brute Force Attack*. Pengujian keamanan sistem dilakukan pada sistem eksisting *Single Sign On*, kemudian dari hasil pengujian sistem eksisting jika terdapat celah keamanan maka dilakukan perbaikan atau modifikasi pada celah keamanan sistem sehingga sistem *single sign on* aman terhadap metode serangan yang telah disebutkan.

Dari hasil pengujian dan analisa yang dilakukan didapatkan hasil bahwa *Man In The Middle Attack* pada sistem eksisting *Single Sign On* berhasil dilakukan, hasil menunjukan bahwa data yang dikirimkan user dapat diketahui dan diindentifikasi menggunakan tools wireshark , cain & abel dan ettercap. Untuk hasil pengujian LDAP *Injection* pada sistem eksisting *Single Sign On* yang menggunakan CAS aman terhadap serangan LDAP *Injection*. Untuk hasil pengujian *Brute Force Attack* berhasil dilakukan pada sistem eksisting *Single Sign On*, sedangkan hasil pengujian pada sistem eksisting *Single Sign On* yang sudah dilakukan perbaikan atau modifikasi sistem dengan penambahan *Captcha* menjadi aman terhadapat serangan *Brute Force Attack*.

Kata Kunci : Keamanan, *Single Sign On (SSO), Authentifikasi, LDAP Injection, Man In The Middle Attack, Brute Force Attack*