Abstrak

Perkembangan teknologi yang semakin maju mengakibatkan tingkat kebutuhan terhadap keamanan informasi menjadi penting. Seiring berkembangnya informasi munculah permasalahan baru mengenai keamanan jaringan, contoh ancaman keamanan jaringan yang sering terjadi adalah pengendusan aktivitas di jaringan atau biasa disebut *sniffing*, selain ancaman pengendusan juga terdapat ancaman lainnya seperti *MITM* attack (man in the middle) yang memungkinkan attacker berada di tengah komunikasi bebas mendengarkan atau mengubah percakapan antara dua pihak.

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].

Melalui tugas akhir ini dilakukan analisis dan perbandingan keamanan jaringan pada mekanisme autentikasi menggunakan *kerberos* dan *HTTP over SSL*. Masing-masing mekanisme autentikasi diuji menggunakan serangan sniffing dan MITM attack. Sehingga kita dapat mengetahui bagaimana perbandingan keamanan autentikasi dalam hal ini adalah ancaman serangan dari penggunaan *kerberos* dan *HTTP over SSL* sebagai protokol autentikasi.

Dari hasil pengujian yang dilakukan didapatkan bahwa kerberos dan HTTP over SSL relative masih rentan terhadap serangan menggunakan tools tertentu, baik kerberos maupun HTTP over SSL masih terdapat celah keamanan yang masih mungkin dimanfaatkan oleh para attacker.

Kata kunci : *kerberos, HTTP over SSL, sniffing, MITM* attack