Abstract

The increasing development of advanced technologies has made security of information very essential. New problems on network security emerge as the growth of information itself. One of those threats is sniffing which tracks down user activities on networks. The other one is “man in the middle” (MITM) which illegally permit attacker to intercept in the middle of communication so they can freely listen or change the conversation between two parties.

Kerberos is a network authentication protocol designed to provide strong authentication. Kerberos allows the client and server to authenticate each other before making a connection [8]. Whilst, HTTP over SSL, which is usually implemented with HTTPS, is an HTTP protocol that uses Secure Socket Layer (SSL) as a sub-layer under the HTTP so it can be much more secure [9].

Through this thesis, an analysis and comparison of network security is performed on the authentication mechanism using Kerberos and HTTP over SSL. Each authentication mechanism was tested using MITM attacks and sniffing attacks. Thus the comparison of security authentication is able to note, in this case is the threat of attacks, from the usage of Kerberos and HTTP over SSL as the authentication protocol.

The test results showed that the Kerberos and HTTP over SSL is relatively vulnerable to attacks using certain tools. Both Kerberos and HTTP over SSL still has security holes that may be exploited by attackers.

Key words : *kerberos, HTTP over SSL, sniffing, MITM* attack