ABSTRAK

Protocol HTTP memiliki versi *secure* yang disebut HTTPS. HTTPS menyandikan data sesi menggunakan *protocol* SSL (*Secure Socket layer*) atau *protocol* TLS (*Transport Layer Security*). Kedua *protocol* tersebut memberikan perlindungan yang memadai dari serangan *eavesdroppers*, dan *man in the middle attacks*(MITM). Penerapan *protocol* https memiliki permasalahan saat diterapkan pada autentikasi *firewall* atau sering disebut *captive portal server* yang mengautentikasi calon pengguna layanan akses internet berbasis web/http. Pada saat autentikasi client dilakukan pada *protocol* https, *browser client* yang berfungsi menampilkan *interface* halaman *login* akan menampilkan *certificate error*. Penelitian ini membahas permasalahan dan penanganan certificate error tsb sekaligus memberikan *alternative* untuk meminimalisir celah keamanan yang ada pada autentikasi *captive portal server.*

Penelitian ini berfokus pada dua metode autentikasi dengan protocol http dan https. Autentikasi https pada captive portal yang menampilkan error sertifikat akan diuji dengan MITM password sniff dan akan dibandingkan dengan autentikasi captive portal dengan protocol http dengan keamanan hash password dengan pengujian yang sama. Hal tersebut akan memberikan gambaran penggunaan protocol yang dapat dipilih oleh seorang teknisi jaringan hotspot untuk mempertimbangkan keamanan dari MITM password sniff dan error sertifikat pada browser *client*.

Kata Kunci : Security, SSL ,HTTPS,TLS , MITM , Man in Middle, Autentikasi, Captive Portal, Firewall.

ABSTRACT

The HTTP protocol has a secure version called HTTPS. HTTPS encodes session data using the SSL (Secure Socket Layer) protocol or TLS (Transport Layer Security) protocol. Both protocols provide adequate protection from eavesdroppers, and man in the middle attacks (MITM). Implementation of the https protocol has problems when applied to firewall authentication or often called a captive portal server that authenticates potential users of web / http web access services. When client authentication is performed on the https protocol, the client browser that displays the login page interface displays a certificate error. This study discusses the problem and handling the certificate error as well as providing an alternative to minimize the existing security gaps in the authentication captive portal server.

This study focuses on two authentication methods with http and https protocols. Https authentication on a captive portal displaying a certificate error will be tested with a sniff MITM password and will be compared with a captive portal authentication with http protocol with password hash security with the same test. This will provide an overview of the use of protocols that a hotspot network technician can take to consider the security of the sniff MITM password and the certificate error in the client browser.

Keywords: Security, SSL ,HTTPS,TLS , MITM , Man in Middle, Authentication, Captive Portal, Firewall.