

INTISARI

Pada penelitian ini membahas tentang performa keamanan pada saat autentikasi data user di ldap pada *file server* yang di amankan dengan algoritma kriptografi menggunakan protokol *SSL/TLS*. Dengan adanya protokol *SSL/TLS* maka proses autentikasi menjadi aman dari *snifing*. Metode penelitian yang di gunakan yaitu metode eksperimen. Hasil uji coba pada autentikasi tanpa menggunakan keamanan, data pengguna dapat di lihat pada packet yang di capture *wireshark*, dan setelah menggunakan keamanan, data pengguna yang sebelumnya dapat di lihat pada *wireshark* di enkripsi dengan algoritma kriptografi, sehingga data pengguna yang melakukan autentikasi pun menjadi aman. Kecepatan waktu *request* tanpa menggunakan keamanan lebih cepat dibandingkan kecepatan waktu *request* setelah menggunakan keamanan.

Kata kunci : *file server, ldap, SSL/TLS, wireshark*

ABSTRACT

This research discusses the safety performance during user data authentication in *Idap* in file server protected by cryptographic algorithm using *SSL/TLS*. The authentication process using *SSL/TLS* protocol makes it safe from sniffing. The method applies in this research is the experimental method. User data in the authentication try out without safety performance can be seen in the package captured by *wireshark*, while user data using safety performance is encrypted with cryptographic algorithm, therefore the authentication is safe. The request speed without safety performance is faster than with the safety performance.

Keywords: *File server, Idap, SSL/TLS, wireshark*

