

Abstrak

File Transfer Protocol atau FTP adalah salah satu protokol yang digunakan untuk pertukaran file baik berupa upload file maupun download file. Sayangnya FTP masih meninggalkan lubang keamanan dimana data yang dikirimkan masih dapat dibaca dengan jelas. Selain itu, tidak adanya mekanisme autentikasi server, membuat client dapat beresiko untuk mengakses FTP server palsu.

Penelitian ini menguji Secure FTP dan FTPS, kedua metode keamanan yang diterapkan pada FTP untuk mengatasi celah-celah keamanan yang ditinggalkan oleh FTP. Aspek keamanan yang diuji mencakup confidentiality (kerahasiaan data) dan authentication (autentikasi). Selain itu, penelitian ini juga menguji kedua metode tersebut dari segi performansi. Aspek performansi yang diujikan mencakup delay, throughput, dan utilitas CPU serta memori pada single transfer dan multiple transfer, dan juga dari kompleksitas pemakaian metode tersebut.

Dari hasil pengujian didapatkan kesimpulan bahwa FTPS mempunyai tingkat keamanan yang lebih tinggi dibandingkan Secure FTP. Selain itu, pada aspek performansi, meskipun Secure FTP unggul pada performansi single transfer namun pada pengujian lain, FTPS mempunyai hasil yang lebih baik dibanding Secure FTP. Dari pengujian kedua aspek tersebut, dapat disimpulkan bahwa FTPS mempunyai kemampuan lebih baik daripada Secure FTP baik dari segi keamanan maupun performansi.

Kata Kunci: keamanan, performansi, FTP, Secure FTP, FTPS