ABSTRACT

Single Sign On is a system authentifikasi against user, where user can access multiple applications without having to log in dimasing applications. The objective of designing Single Sign On is to compress the system authentifikasi from multiple applications or services. In the development of information technology indirectly demanding user applications to manage account data properly so as not misused by irresponsible parties. Several methods of user account security has been proposed to solve the problem, including by implementing authentication Single Sign On using the LDAP protocol.

On this final assignment method used to test the security system single sing on was the Man In The Middle Attack, LDAP Injection and Brute Force Attack. System security testing performed on the existing system of Single Sign On, then from the results of testing existing systems if there are security loopholes then do a repair or modification on the system security gaps so that single sign on system secure against attack methods already mentioned.

Results from testing and analysis done obtained the results that the Man In The Middle Attack on the existing Single Sign On system was successfully performed, the results show that data is submitted the user can know and diindentifikasi using the tools of wireshark, cain and abel & ettercap. For LDAP Injection testing results on the existing system of Single Sign On CAS that use secure LDAP Injection attacks against. Test results for Brute Force Attack was successfully performed on existing systems of Single Sign On, while the results of testing on the existing Single Sign On systems that already do the repair or modification of the system with Captcha be safe terhadapat Brute Force Attack.

Keywords: Security, Single Sign On (SSO), Authentifikasi, LDAP Injection, The Man In The Middle Attack, Brute Force Attack