

Abstrak

Proses otentikasi merupakan sebuah mekanisme pengamanan dalam sebuah sistem dengan membuktikan kebenaran identitas dari user. Mekanisme otentikasi berperan dalam keamanan jaringan untuk menghindari akses resource oleh pihak yang tidak memiliki hak.

Protokol Kerberos merupakan protokol otentikasi yang bekerja dalam sebuah jaringan lokal. Salah satu kelebihan protokol Kerberos adalah mendukung mekanisme Single Sign-On dimana client cukup melakukan otentikasi satu kali kepada Key Distribution Center (KDC) untuk dapat mengakses resource pada server – server yang telah ter-kerberized.

Celah keamanan yang masih terdapat pada protokol Kerberos adalah belum dapat mengatasi serangan offline password guessing yang dilakukan attacker setelah mendapatkan paket hasil request otentikasi. Cara untuk menangani celah keamanan tersebut adalah dengan mekanisme pre-authentication dan Flexible Authentication Secure Tunneling (FAST) merupakan salah satu cara pre-authentication yang dapat mencegah serangan offline password guessing.

Selain mempengaruhi segi keamanan dari protokol Kerberos, adanya penambahan mekanisme FAST akan berpengaruh juga terhadap penggunaan resource server, seperti CPU dan memory.

Kata kunci: otentikasi, Kerberos, KDC, FAST, resource