BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkanan analisis hasil penelitian pada bab sebelumnya, maka dapat ditarik kesimpulan bahwa:

1. Dengan memanfaatkan LDAP *server* yang sebagai *datastore credential* pengguna telah dapat ditampung dan dipusatkan hal ini dapat dicapai dengan merancang *Directory Information Tree* atau DIT sesuai dengan kebutuhan sistem.
2. Dengan memanfaatkan Freeradius sebagai RADIUS *server* yang telah dikonfigurasi dengan menyisipkan sebuah *schema* bernama *Freeradius.schema* kedalam LDAP *server* sehingga data di dalam LDAP *server* dapat dibaca oleh RADIUS *server*. Serta konfigurasi pada Modul LDAP pada RADIUS *server* seperti pada pembahasan di atas sehingga RADIUS *server* dapat menggunakan data pada LDAP *server* dalam melakukan otentikasi.
3. Dengan membangun CAS-*server* sesuai dengan configurasi pada RADIUS *server* maka CAS-*server* sebagai pemberi layanan tiket pada sistem Single Sign On ini dapat menggunakan RADIUS sebagai *Authenticator*. Hal ini dapat diwujudkan dengan mengganti *authenticator* standar CAS dengan

RADIUS *authenticator aDAPter* yang didefinisikan pada file *Web*.xml di dalam CAS-*server*.

4. Dengan melakukan konfigurasi *Secure Socket Layer* atau SSL pada tomcat *Web-server* dimana CAS *server* akan di implemetasikan sehingga data-data yang dipertukarkan dalam jaringan akan melalui protokol *SSL /HTTPS*, walaupun tingkat keamanan yang ditawarkan masih dapat ditembus dengan berbagai cara salah satu dengan *ARP-HTTPS Poisoning* yang telah dilakukan pada pengujian di atas.
5. Pada sistem yang telah dibangun didapat beberapa kelemahan pada sistem ini antara lain.
    a) *Credential* yang disimpan pada LDAP *server* harus berupa data static, hal ini dikarenakan keterbatasan LDAP *server* dalam melayanin proses transaksi.
    b) Fungsi RADIUS *server* yang digunakan pada sistem ini hanya fungsi *Authentication* dan *Authorization.*
    c) Keamanan pada koneksi antara LDAP dan RADIUS *server* rentan terhadap *proses Sniffing.*
    d) Keamanan pada Koneksi CAS-*server* ke CAS-*client* masih dapat ditembus dengan *ARP-Poisoning.*
    e) Sistem tidak mempunyai *error hendler* jika salah satu *server* mati/down.

f) Sistem tidak dapat berjalan dalam jaring yang melakukan *filtering* pada *port* 389,1812,8443.

5.2 Saran

Saran pada penelitian ini adalah antara lain:

1. Perlu diperhatiakan dimana sistem ini akan diimplemetasikan dalam hal batasan sumberdaya jaringan seperti tersedianya *port* pada *server* dan layanan DNS *server* yang merupakan salah satu faktor pendukung berfungsinya sistem ini.
2. Perlu diperhatikanya keamanan dari *server-server* yang bersangkutan dari sisi fisik mau logic hal ini dikarenakan sistem ini tidak dapat berjalan jika salah satu komponen pembentukanya tidak berfungsi sebgai mana mestinya.