IMPLEMENTASI FREERADIUS PADA JARINGAN HOTSPOT DENGAN MENGGUNAKAN MYSQL DAN EAP-TLS

Apolinarius Gusala[1], Suwanto Raharjo[2], Naniek Widyastuti[3]
[1]Teknik Informatika, FTI, IST AKPRIND, aprykribo007@gmail.com
[2]Teknik Informatika, FTI, IST AKPRIND, wa2n@akprind.ac.id
[3]Teknik Informatika, FTI, IST AKPRIND, naniek_wid@yahoo.com

ABSTRACT

The ease of wireless LAN becomes an attractiveness for computer users to access a computer network or internet. Wireless LAN's users have increased a lot. This increasing is balanced by the increasing of hotspot in public places such as café, mall, airport, office, even in a school or a campus. Hotspot gives much ease for internet users because it doesn't need wire anymore as the connector between modem and internet's client. There are so many hotspot areas, but not all hotspot has security system that can overcome users' problems who don't have a right to use internet.

This research used FreeRADIUS method, MySQL and EAP-TLS to overcome the weakness of Wireless LAN system and as authentic protocol username password and using CA certificate as a security key so that there were no more illegal users could use hotspot network and it also gave ease for network administrator.

Based on the research results, it showed that the use of FreeRADIUS, MySQL and EAP-TLS gave good security for the clients through the process of authentication, authorization and centered account registration with MySQL function as a database for username and password saving. It was also used for CA certificate authentication which was used for securing the connection between the client and the server, so that there were no more illegal internet users.

Keywords: FreeRADIUS, MySQL, EAP-TLS

INTISARI

Kemudahan yang ditawarkan *wireless* LAN menjadi daya tarik tersendiri bagi para pengguna komputer guna mengakses suatu jaringan komputer atau internet. Pengunaan *wireless* LAN mengalami peningkatan pengunaan yang pesat. Peningkatan penggunaan ini juga di imbangi dengan peningkatan jumlah *Hotspot* di tempat – tempat umum, seperti kafe, mall, bandara, di perkantoran bahkah di sekolah dan kampus. *Hotspot* memberikan banyak kemudahan bagi para pengguna internet karena tidak membutuhkan kabel lagi sebagai penghubung antara modem dengan *client* yang ingin berinternet. Ada banyak *Hotspot* yang tersedia di banyak tempat, tetapi tidak semua *Hotspot* memiliki sistem keamanan yang dapat mengatasi masalah pengguna yang tidak berhak untuk menggunakan internet.

Penelitian ini menggunakan metode FreeRADIUS, MySQL dan EAP-TLS untuk mengatasi kelemahan sistem Wireless LAN dan sebagai protokol otentikasi username password dan menggunakan sertifikat CA sebagai kunci keamanan agar tidak ada lagi pengguna yang tidak sah memakai jaringan *Hotspot* serta memberikan kemudahan pada sisi administrator jaringan.

Berdasarkan hasil penelitian didapatkan bahwa pengunaan FreeRADIUS, MySQL dan EAP-TLS memberikan keamanan yang baik untuk client melalui proses otentikasi, otorisasi dan pendaftaran *account* secara terpusat dengan fungsi Mysql sebagai database tempat penyimpanan username dan password serta proses otentikasi sertifikat CA yang berfungsi untuk mengamankan koneksi antara *client* dan server sehingga tidak ada lagi penguna internet yang tidak sah.

Kata kunci: FreeRADIUS, MySQL, EAP-TLS

PENDAHULUAN

Salah satu perubahan utama di bidangang komputer, yang lebih dikenal dengan *wireless LAN (WLAN)*. Kemudahan-kemudahan yang ditawarkan *wireless* LAN menjadi daya tarik tersendiri bagi para pengguna komputer menggunakan teknologi ini untuk

mengakses suatu jaringan komputer atau internet. Beberapa tahun ini pengunaan *wireless* LAN mengalami peningkatan yang pesat. Peningkatan pengguna ini juga dibarengi degan peningkatan jumlah *Hotspot* di tempat –tempat umum, seperti kafe, mal, bandara, di perkantoran bahkah di sekolah-sekolah dan kampus.

Untuk membuat sebuah jaringan terkoneksi ke internet yang aman dan user *friendly*, dapat di buat dengan membuat sebuah sistem menggunkan *Radius Server.* Penggunaan autentifikasi *server* ditujukan untuk mendukung keamanan proses autentifikasi jaringan untuk dapat menjadi lebih baik karena *server* yang akan bertindak langsung untuk mengontentikasi *dial-in* pengguna dan mengotorisasi *request* ke layanan yang disediakan. Disamping itu , *Remote Acces Dial-In User* (RADIUS) *SERVER* juga memiliki sistem user manajemen yang memberikan kemudahan dalam pengelolaan profil pengguna dengan menggunakan database serta mengatur kebijakan tertentu terhadapap data profil pengguna. Selain dari metode autentifikasi *server*, pengguaan MYSQL yang berfungi sebagai tempat penyimpanan data informasi secara terpusat dan melakukan pencarian informasi menjadi terintegrasi dan sangat mudah . dan EAP-TLS yang menggunakan sertifikat untuk membuat EAP_TLS cocok untuk mengamankan jaringan *wireless*.

TINJAUAN PUSTAKA

Dalam melaksanakan penelitian ini digunakan beberapa referensi yang berhubungan dengan obyek penelitian. Referensi di ambil dari penelitian sebelumnya yang berhubungan dengan penelitian :

- Implementasi Roaming dan manajemen AAA pada wifi *Hotspot*. (Kusuma, 2007). Penelitian yang dilakukan adalah menjelaskan tentang perancangan dan implementasi hostpot berbayar dengan membuat sebuah hostpot access *server*. Kekuranganya adalah manajemen keamananya belum dibahas lebih lanjut.
- Perancangan dan Implementasi Infrastruktur *Hotspot* Di Smk Yasmu Manyar Gresik (Mafidah, 2009). Perancangan *Hotspot* yang diharapkan dapat menunjang mobilitas guru, karyawan dan siswa akan informasi yang cepat dan actual dalam pembelajaran di sekolah. SMK Yasmu Manyar Gresik berencana memberikan fasilitas *Hotspot* untuk para guru dan siswa dimana hampir semua guru dan siswa memiliki notebook/laptop atau bahkan sebuah handphone yang memiliki fasilitas koneksi wireless dan tidak dipusingkan lagi dengan banyaknya kabel.Implementasi *Hotspot* yang terdiri dari satu buah access point, satu buah antena E-goen, *switch* serta modem ADSL *Speedy*. Antena kentongan E-goen berfungsi untuk memperluas *coverage* area hingga beberapa kilometer. Kekuranganya adalah tidak menggunakan sistem autentikasi database yang terpusat dan sistem keamanan juga tidak di bahas.
- Implementasi Sistem Auntentikasi Jaringan *Hotspot* Universitas Udayana dengan Menggunakan Open Source Freeradius (Sudiarta, 2010). Mengimplementasikan sistem autentikasi terpusat menggunakan open source freeradius dan mysql sebagai database user serta mengimplementasikan manajemen sistem yang berbasis web interface untuk memudahkan administrator atau operator dalam mengelola user. Kekuranganya adalah tidak dibahas tentang keamananya tetapi hanya membahas tentang autentikasi database yang terpusat.

Landasan teori yang digunakan dalam penelitian ini adalah penjelasan teori dari buku yang berhubungan dengan penelitian ini, diantaranya :

1. Pengertian MySQL
   MySQL merupakan database yang paling digemari dikalangan Programmer Web, dengan alasan bahwa program ini merupakan database yang sangat kuat dan cukup stabil untuk digunakan sebagai media penyimpanan data.Sebagai sebuah *database server* yang mampu untuk memanajemen database dengan baik, MySQL terhitung merupakan database yang paling banyak digunakan dibandingkan *database*lainnya. (Nugroho, 2013)
2. Pengertian Databases
   Databases merupakan kumpulan file-file yang mempunyai kaitan antara satu file dengan file yang lainsehingga membentuk satu bagunan data untuk

menginformasikan satu perusahaan, instansi dalam batasan tertentu. Bila terdapat file yang tidak dapat dipadukan atau dihubungkan dengan file yang lain berarti file tersebut bukalah kelompok dari satu database, ia akan dapa membetuk satu database sendiri (Kristanto, 2004)

3. Pengertian Twisted Pair
   Merupakan jenis kabel paling sederhana dibandingkan dengan lainnya dan saat ini paling banyak digunakan sebagai media kabel dalam membangun sebuah jaringan komputer. *Twisted pair* terdiri dari dua kawat tembaga berselubung yang diatur sedemikian rupa sehingga membentuk pola *spiral*. Satu pasang kawat berfungsi sebagai sebuah link komunikasi. Dalam jarak yang semakin jauh, satu bundle kabel *twisted pair* akan dapat terdiri dari beratus-ratus pasangan, pilinan dari kabel ini akan mengurangi *interferensi* yang terjadi antara kabel. *Twisted pair* dibagiatas 2 jenis yaitu *Unshieded Twisted Pair* (UTP) dan *Shielded Twisted Pair* (STP). (Komputer W. , Konsep Jaringan Komputer Dan Pengembangannya, 2003)
4. Pengertian Wireless
   Wireless atau *nirkabel* merupakan salah satu media penghubung node di jaringan yang tidak terlihat bentuknya. Mengunakan jaringan *wireless,* jaringan komputer akan memiliki banyak keuntugan karena terdapat jaringan komputer yang akan lebih teratur karena tidak adanya kabel-kabel yang berantakan dan sering membuat suasana tidak teratur. (wahana komputer)
5. Pengertian Radius
   RADIUS merupakan singkatan dari Remote Acces Dial in User Service. Pertama kali di kembangkan oleh Livingston Enterprises. Merupakan network protokol keamanan komputer yang digunakan untuk membuat manajemen akses secara terkontrol pada sebuah jaringan yang besar. RADIUS didefinisikan di dalam RFC 2865 dan RFC 2866. RADIUS biasa digunakan oleh perusahaan untuk mengatur akses ke internet atau interner bagi client. (Hassel, 2002)
6. Pengertian FreeRADIUS
   FreeRADIUS diperkenalkan oleh Alan Dekok dan Miquel van Smoorenburg pada bulan Agustus 2005. FreeRADIUS server merupakan modular dan produk open-source paling populer dan paling banyak digunakan di dunia sebagai RADIUS server yang berbasis sistem operasi UNIX. FreeRADIUS mendukung semua protokol umum otentikasi. freeRADIUS berjalan pada platform UNIX 32 bit dan 64 bit. freeRADIUS bersifat gratis dan dapat di download pada alamat http://freeradius.org/download.html . (www.freeradius.org)
7. Pengertian EAP-TLS
   EAP-Transport Layer Security (EAP-TLS) merupakan jenis EAP yang digunakan dalam lingkungan pengamanan berbasis sertifikat. EAP TLS juga merupakan jenis otentikasi yang paling kuat. EAP TLS mengharuskan adanya autentikasi timbal-balik dimana baik *supplicant* dan *server* autentikasi saling membuktikan identitas mereka satu sama lain. EAP-TLS membuat penggunaan kriptografi kunci publik untuk tujuan autentikasi, yang mana melibatkan *smart card* atau sertifikat digital. (Nakhjiri, 2005)

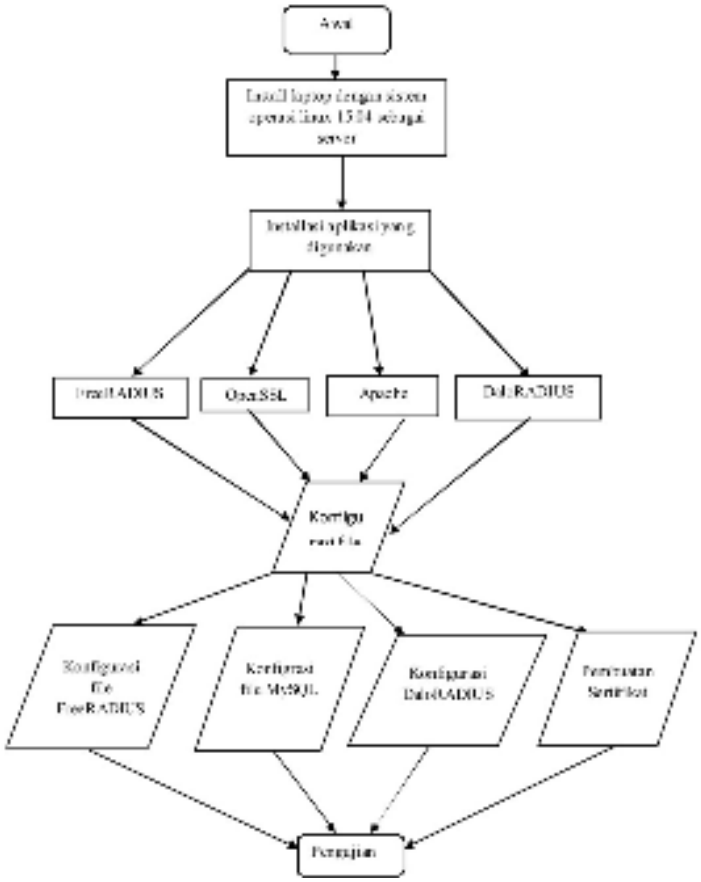
Metode Penelitian

Rancangan penelitian meliputi proses dari perencanaan serta pelaksanaan penelitian yang menghasilkan suatu kesimpulan dimana rancangan penelitian itu adalah catatan yang menjelaskan semua prosedur dari penelitian sejak dari tujuan penelitian hingga menghasilkan suatu kesimpulan. Adapun rancangan penelitian yang dilakukan terdiri dari 4 tahap yaitu :

a. Tahap pertama : Penginstalaan laptop-server dengan menggunakan ubuntu 15.04 sebagai sistem operasi yang digunakan.

b. Tahap kedua : penginstallan aplikasi yang digunakan seperti aplikasi FreeRADIUS, MySQL, DaloRADIUS,OpenSSL
c. Tahap ketiga : Proses konfigurasi dari tiap – tiap aplikasi yang digunakan.
d. Tahap keempat : Melakukan percobaan terhadap aplikasi yang di buat.
e. Tahap terakhir : Membuat kesimpulan dari hasil pengujian yang di lakukan.

Adapun gambar rancangan penelitiannya dapat dilihat pada gambar 1 di bawah ini.



Gambar 1 Rancangan Penelitian

PEMBAHASAN

Tampilan Halaman DaloRADIUS

DaloRADIUS yang berbasis web interface memberikan kemudahan dalam menjalankan aplikasi ini, dengan melalui web browser seperti mozila atau google chroom dan mengaksesnya melalui *ip/daloradius* atau *host/daloradius* pada *address bar.* Saat pertama mengakses akan muncul halaman login DaloRADIUS dan untuk dapat login kedalam aplikasi, username dan password dapat dilogin dengan *username* dan *password default* yang sudah ada dari aplikasi DaloRADIUS yaitu *administrator* sebagai *username* dan *radius* sebagai *password*. Adapun gambar tampilan awal DaloRADIUS seperti gambar 2.

Gambar 2 Tampilan awal DaloRADIUS

Membuat user aplikasi FreeRADIUS

Untuk membuat user baru, dilakukan melalui menu Management > New User dan kemudian mengisi form untuk username dan password berserta tipe dari password tersebut

Gambar 3 Proses pembuatan user dan password baru

Pada gambar 3 Di atas user dan password yang telah di buat dengan nama username tes3 dan password tes3 Serta dengan tipe password yang dipilih yaitu *Cleartext-password*. Dalam aplikasi ini terdapat tiga macam pilihan untuk membuat user yang diantaranya yaitu: *username authentication, MAC address authentication dan PIN code authentication*. Setelah user baru dibuat, maka dapat melihat daftar user yang asda di dalam database melalui pilihan menu *List Users* seperti yang ditunjukkan pada gambar 4 di bawah ini.

Gambar 4 Daftar user.

Pengujian user DaloRADIUS terhadap FreeRADIUS *Server*

Pengujian yang dilakukan sama pada saat menggunakan data *user* dalam *file konfigurasi users*, namun pengujian kali ini menggunakan *user* yang sudah dibuat dan tersimpan di dalam *database*. Berikut uji coba yang dilakukan terhadap *user "user P1"* dengan menggunakan *radtest*:

Gambar 5 Proses pengujian Radtest

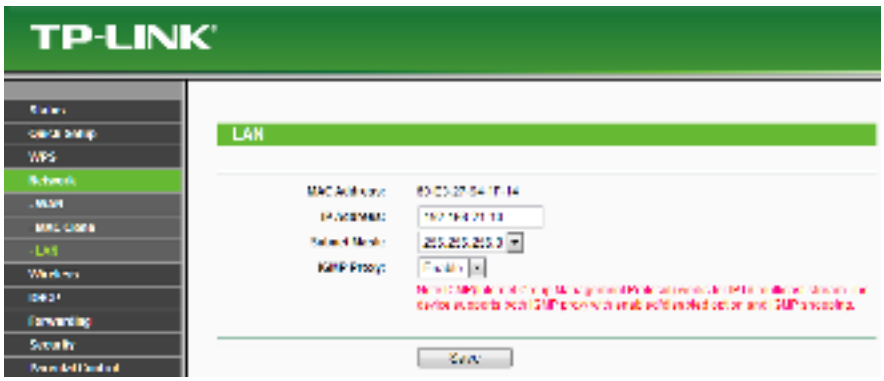
Konfigurasi Router Access Point Tp-Link

Perangkat acces point digunakan untuk membantu menyebarkan koneksi internet dari wifi *Hotspot Server* pada laptop-*server* yang telah dibuat. namun sebelumya perlu dilakukan konfigurasi terhadap perangkat access point agar dapat berkomunikasi ke dalam jaringan laptop-*server*. Adapaun konfigurasi yang di lakukan.

Konfigurasi jaringan perangkat access point

Agar dapat berkomunikasi dengan laptop-*server* , adapun langkah langkah untuk mengkonfigurasi access pointnya :

- Buka browser dan masukan ip access point yang default.
- Masukan username dan password access point
- Ganti IP *access point* yang ada pada menu *Network* > *Lan* menjadi 192.168.21.10 dan kemudian save. Seperti pada gambar 6
-



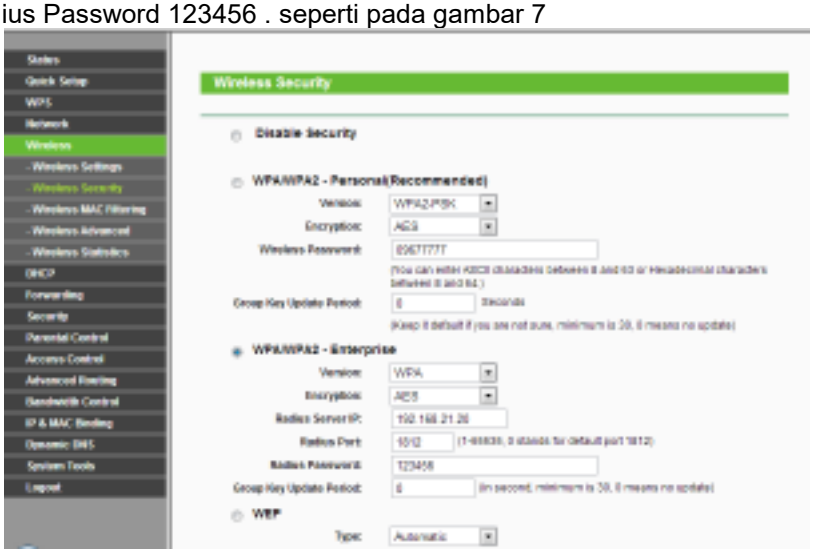
Gambar 6 Proses pemberian IP baru LAN

Konfigurasi Securuty Acces Point

Selanjutnya untuk melakukan konfigurasi selanjutnya, sebelumya samakan kembali Network IP laptop yang terhubung dengan access point agar dapat melanjutkan konfigurasinya.

- Masukan alamat IP access point 192.168.21.10 ke browser.
- Masuk kemenu Wireless dan pilih wireless security
- Pilih security mode WPA/WPA2-Enterprise
- Masukan IP Radius 192.168.21.20
- Radius Port 1812

- Radius Password 123456 . seperti pada gambar 7



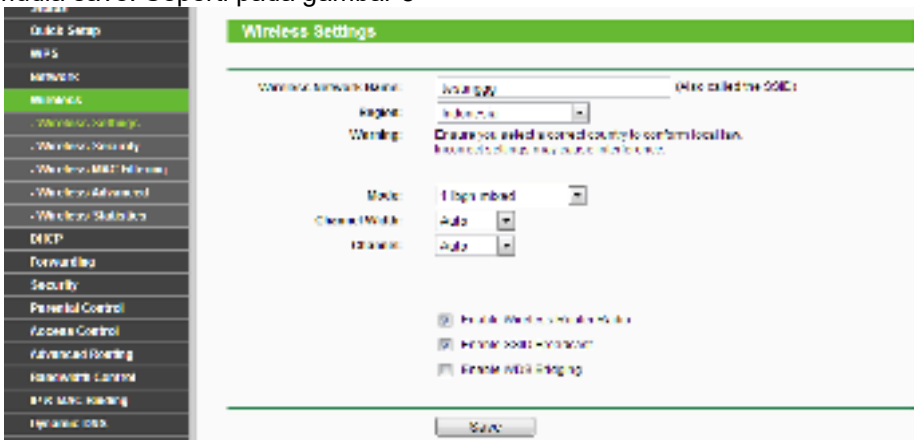
Gambar 7 Proses konfigurasi security

- Kemudian save dan rebot access point agar konfigurasinya dapat berjalan dengan baik.

Konfigurasi SSID Access Point

Pada umunya Access point sudah memiliki nama SSID default. Perlu untuk mengubahnya agar dapat menjadi lebih unik dibandingkan dengan SSID defaultnya. Adapun cara mengubah nama SSIDnya yaitu :

- Masuk ke menu Wireless.
- Pilih wireless setting
- Ubah nama wireless network Name menjadi testing
- Region Indonesia.
- Kemudia save. Seperti pada gambar 8

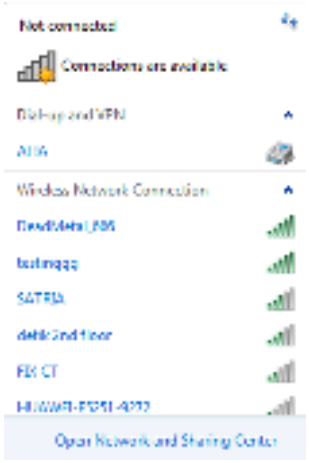


Gambar 8 Proses pemberian nama Access Point

Proses Login Sebelum menginstall Sertifikat CA untuk Client

Pada tahap pertama yang di lakukan setelah melakukan konfigurasi yang telah dilakukan mencoba melogin ke access point dengan nama SSID testinggg yang telah di buat sebelumnya. Adapun langkah langkahnya sebagai berikut

- Pilih nama SSID testing pada Open Network and Shearing Center seperti pada gambar 9.

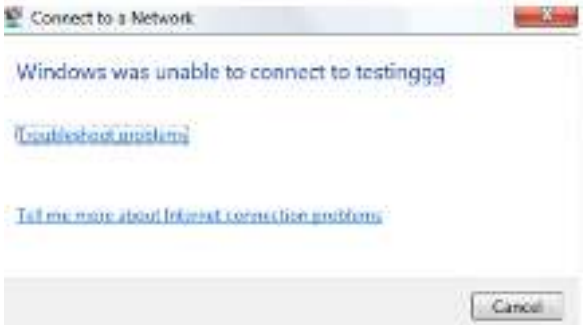


Gambar 9 Nama jaringsn *Hotspot*

- Setelah pilih SSID testinggg , maka akan muncul pesan untuk memasukan username dan password. Untuk mencoba apakah bisa terhubung kejaringanya atau tidak. username dan password yang digunakan menggunakan user dan password yang sudah ada pada database yaitu tes1 sebagai usernamenya dan tes1 sebagai paswordnya. Prosesnya dapat di lihat seperti pada gambar 10.

Gambar 10 Proses memasukan username dan password bagian 1

- Setelah memasukan username dan password, sistem langsung melakukan otentikasi pada jaringan. karena belum diinstall terlebih dahulu sertifikat buat client maka proses otentikasi gagal. Adapun proses pengujian ini di lakukan sebanyak 3 kali dan hasil yang di peroleh sama dimana ditunjukan pada gambar 11.



Gambar 11 Proses otentikasi gagal bagian 1

Proses Login Setelah menginstall Sertifikat CA untuk Client dengan User dan Password Benar

Pada tahap sebelumnya sudah dilakukan pengujian login dan proses yang di dapat selama percoban adalah gagal. Pada tahap ini akan dilakukan lagi pengujian terhadap sistem *Hotspot* tetapi dengan user dan password yang benar dan sudah terinstall sertifikat CA. adapun prosess pengujiannya langsung masuk ke dalam proses login tanpa di jelaskan tiap-tiap langkahnya. Adapun prosesnya adalah sebagai berikut.

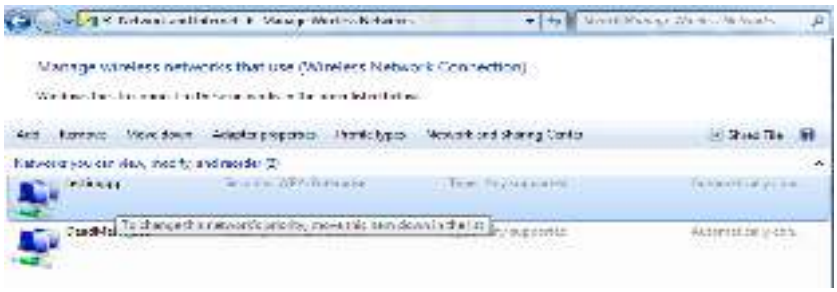
- Pilih SSID testinggg , maka akan muncul pesan untuk memasukan username dan password. masukan username dan password yang sudah ada pada database yaitu tes1 sebagai usernamenya dan tes1 sebagai paswordnya. Prosesnya dapat di lihat seperti pada gambar 12.

Gambar 12 Proses memasukan username dan password bagian 3

- Setelah memasukan username dan password, sistem langsung melakukan otentikasi pada jaringan. karena username dan password sudah ada di database proses otentikasi berhasil. Adapun hasil yang di peroleh sama dimana ditunjukan pada gambar 13.

Gambar 13 Proses otentikasi berhasil

- Jika dilihat pada menu Manager Wireless Networks, SSID testing menggunakan type security WPA-Enterprise yang berrarti proses Eap-Tls berjalan dengan lancer. Adapun gambarnya seperti pada gambar 14.



KESIMPULAN

Kesimpulan yang di ambil dari hasil penelitian adalah :

1. Otentikasi user terpusat memudahkan administrator dan user atau pengguna baik dalam mengatur dan menggunakan sumber daya jaringan.
2. Penerapan protocol EAP-TLS dapat berjalan dengan baik dan dapat digunakan sebagai proses otentikasi.
3. Penggunaan aplikasi FreeRADIUS dapat berjalan dengan lancar dan dapat mendukung aplikasi yang di butuhkan dalam penelitian.
4. Penggunaan MySQL dan EAP-TLS dapat memberi keamanan yang double untuk mengamankan jarigan *Hotspot* meskipun masi ada aplikasi yang mampu masuk kedalam sistem.

Saran

Untuk pengembangan selanjutnya, saran yang dapat diberikan adalah Untuk pengembangan berikutnya untuk proses *auntentikasi* dengan berbasis Radius server ini jangan hanya diterapkan pada jaringan *wireless,* melainkan juga pada jaringan LAN.

DAFTAR PUSTAKA

Hassel, J. (2002). RADIUS Cambridge Massachusetts . O'Reilly Media.

Komputer, W. 2003. *Konsep Jaringan Komputer Dan Pengembangannya*. Jakarta: Salemba Infotek.

Kristanto, I. H. 2004. *Konsep dan Perancangan Database*. Yogyakarta: Penerbit ANDI.

Kusuma, A., 2007, *Implementasi Roaming dan Manajement AAA*, Skripsi, Jurusan Ilmu Komputer dan