IMPLEMENTASI RADIUS (REMOTE AUTHENTICATION DIAL IN USER SERVICE) BERBASIS SISTEM OPERASI LINUX PADA JARINGAN WLAN

TUGAS AKHIR

Oleh:

IRVANI JUWITA
BP. 06092032

PROGRAM STUDI TEKNIK KOMPUTER

JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK UNIVERSITAS ANDALAS

2010

ABSTRAK

Salah satu masalah terbesar dalam penyelenggaraan layanan akses Internet untuk publik dalam jaringan *wireless fidelity* (Wi-Fi) adalah akses kontrol terhadap penggunanya. Akses kontrol ini dipergunakan untuk menentukan siapa saja yang berhak menggunakan layanan ini.

Tugas Akhir ini mencoba mendesain dan mengimplementasikan sistem yang lebih aman untuk layanan akses Internet dalam jaringan Wi-Fi. Untuk dapat membangun sistem Wi-Fi tersebut diperlukan protokol yang digunakan untuk otentikasi, otorisasi dan akutansi. Protokol Remote Authentication Dial-In User Service (RADIUS) merupakan protokol yang menyediakan *framework* untuk otentikasi, otorisasi dan akutansi. Untuk menunjang kinerja protokol RADIUS digunakan Chilispot sebagai pemberi otentikasi dan otorisasi , MySql sebagai *database billing* dan PhpMyPrepaid sebagai aplikasi *Web base* untuk manajemen *user* dan *billing*.

Hasil dari Tugas Akhir ini adalah penyedia layanan dapat memiliki kemudahan dalam memantau penggunaan layanan akses Internet Wi-Fi dan pada *client*, saat ingin mengakses Internet harus terlebih dahulu melakukan otentikasi ke server baru setelah itu diberi otorisasi. Setelah *client* keluar dari jaringan, pada database server akan tercatat apa saja yang dilakukan oleh *client*.

Kata Kunci : RADIUS, Wi-Fi.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Kurang dari setengah abad, perkembangan komputer maupun jaringannya sungguh luar biasa. Komputer yang awalnya berukuran besar sekarang sudah lebih kecil. Tidak hanya berubah di ukurannya, tetapi juga kecepatan dan penggunaanya yang lebih mudah dari pada tahun tahun awal komputer dikeluarkan. Sedangkan di bidang jaringan, jaringan komputer diawali dengan penghubungan 2 buah PC dan sekarang penghubungan seluruh PC yang ada di dunia. Ini disebabkan karena berkembangnya media *transmisi*. Dahulu kabel digunakan untuk menghubungkan banyak PC dan sekarang ada cara lain yaitu dengan menggunakan gelombang radio . Teknologi gelombang radio ini disebut dengan *wireless*.

Tidak hanya Internet yang memakai gelombang radio sebagai media transmisi. Tetapi pada *Local Area Network* (LAN), teknologi ini juga bisa diterapkan, yang lebih dikenal dengan sebutan *wireless* LAN (WLAN). Teknologi ini memberikan kemudahan bagi pengguna jaringan komputer, khususnya penyedia layanan Internet (ISP). Pengguna tidak takut lagi adanya tabrakan data, gangguan jaringan yang disebakan kerusakan kabel dan hal lain yang bersifat fisik.

Dari kemudahan yang ditawarkan teknologi *wireless* di atas tidak menutup kemungkinan adanya masalah pada jaringan WLAN. Keamanan data menjadi

salah satu permasalahan yang ada. Adanya pengguna WLAN yang tidak bertanggung jawab menyebabkan permasalahan ini timbul.

System keamanan WLAN yang paling umum di gunakan adalah metode enkripsi, yaitu *Wired Equivalent Privacy* (WEP). WEP ini menggunakan satu kunci enkripsi yang digunakan bersama-sama oleh para pengguna WLAN. Hal ini menyebabkan WEP tidak dapat diterapkan pada *hotspot* yang dipasang di tempat-tempat umum. Karena lubang keamanan yang dimiliki WEP cukup banyak, sehingga mudah dibobol oleh pihak ketiga yang tidak berhak.

Sistem keamanan lainnya adalah *Wi-Fi Protected Access* (WPA), yang menggeser WEP dan menghasilkan keamanan yang lebih baik dari WEP. Implementasi WPA menggunakan 802.1x dan *Extensible Authentication Protocol* (EAP) menghasilkan proses otentikasi pengguna yang relatif lebih aman. Pada proses ini pengguna harus melakukan otentikasi ke sebuah *server* otentikasi, misalnya RADIUS, sebelum terhubung ke *wireless* LAN atau Internet. Pada umumnya proses otentikasi ini menggunakan nama-pengguna dan *password*.

Dengan bertitik tolak kepada faktor di atas penulis ingin melakukan sebuah percobaan dan analisa untuk melakukan otentikasi kepada pengguna *wireless* guna menghindari kerusakan-kerusakan yang akan diperbuat oleh "orang-orang ilegal" dalam sebuah jaringan WLAN. Yang mana ide tersebut akan dibuat dalam sebuah tugas akhir yang berjudul: **"Implementasi RADIUS (Remote Authentication Dial In User Services) Berbasis Sistem Operasi Linux Pada Jaringan WLAN"**

1.2 Rumusan Masalah

Karena banyaknya jaringan WLAN pada saat sekarang ini, maka makin banyak pula kesempatan para "tamu-tamu ilegal" yang bertujuan kurang baik bahkan sampai merusak jaringan yang dimasukinya. Untuk itu dilakukannya otentikasi kepada pengguna yang akan masuk kedalam sebuah jaringan WLAN merupakan langkah yang baik untuk meminimalisasikan kerusakan-kerusakan serta pencurian data yang akan terjadi.

Penulis menggunakan protokol RADIUS untuk mengatur pemakai legal saja yang bisa masuk dalam sebuah jaringan WLAN.

1.3 Tujuan

Adapun tujuan dari pembuatan tugas akhir ini adalah :

a. Mengetahui cara untuk mengatasi atau meminimalisasikan gangguan bahkan kerusakan yang akan terjadi dalam sebuah jaringan WLAN.
b. Memahami tentang kinerja protokol yang berhubungan dengan RADIUS *server* dalam melakukan otentikasi kepenggguna jaringan WLAN.

1.4 Batasan Masalah

Untuk lebih memahami analisa dan pembahasan pada Tugas Akhir ini, maka diperlukan batasan – batasan dan ruang lingkup yang lebih kecil dalam penyusunan tugas akhir ini. Batasan dan ruang lingkup ini, meliputi :

a. Membangun sebuah RADIUS server yang akan digunakan untuk *authentication* (pembuktian keaslian), *authorization* (otoritas/pemberian hak) dan *accounting* (akutansi) bagi user yang akses ke Internet.

BAB V

PENUTUP

5.1. Kesimpulan

Dari perancangan dan implementasi yang telah dilakukan dapat diambil beberapa kesimpulan diantaranya :

1. Dengan menggunakan Radius Server hanya *user* tertentu saja yang bisa menggunakan layanan jaringan, yaitu *user* yang sudah terdaftar dalam sistem.
2. Dengan mekanisme pelaporan detail tentang koneksi yang dilakukan *user*, memudahkan administrator dalam memonitor penggunaan layanan jaringan.
3. Aplikasi administrasi Radius Server memudahkan administrator dalam mengelola sistem.

5.2. Saran

Untuk pengembangan tugas akhir di masa yang akan datang, penulis menyarankan hal-hal sebagai berikut:

1. Fitur-fitur yang disediakan dalam paket chillispot dan freeradius belum digunakan sepenuhnya, diharapkan pada penelitian selanjutnya, fitur-fitur tersebut digunakan secara maksimal.
2. Sebaiknya menggunakan komputer yang memiliki spesifikasi yang tinggi agar dapat menunjang kinerja dari sebuah Radius Server.
3. Chillispot tidak bisa bekerja apabila jaringan memiliki *proxy server*. Karena chillispot tidak mempunyai konfigurasi untuk mengenali proxy server setelah terotentikasi, sebagai gantinya ada CoovaChilli

DAFTAR PUSTAKA

Arifin, Zaenal, 2008. Sistem Pengamanan Jaringan Wireless LAN Bebasis Protokol 802.1x dan Sertifikat. Yogyakarta: Andi Offset.

Ashari, Ahmad, Bernand Renaldy Suteja, Wilfridus Bambang Triadi Handaya, 2009. Linux System Administrator. Bandung: Informatika Bandung.

Kadir, Abdul. 2002. Penuntun Praktis Belajar SQL. Yogyakarta: Penerbit ANDI.

Sofana, Iwan, 2008. Membangun Jaringan Komputer. Bandung: Informatika.

http://1100060884.blog.binusian.org/2009/06/03/konfigurasi-openssl-pada-centos-53

http://ipangsan.web.id/konfigurasi-access-point-dengan-radius-di-linux

http://jomka.tripod.com/media_transmisi.htm

http://krisgeto.blogspot.com/2008/05/jenis-jenis-jaringan_14.html

http://www.chillispot.info/release.html