

RANCANG BANGUN SISTEM HOTSPOT MENGGUNAKAN CAPTIVE PORTAL

¹Agus Supriyono (07018184), ²Imam Riadi (0510088001)

¹Program Studi Teknik Informatika

²Program Studi Sistem Informasi

Universitas Ahmad Dahlan

Prof. Dr. Soepomo, S.H., Janturan, Umbulharjo, Yogyakarta 55164

¹Email:

²Email: imam_riadi@uad.ac.id

ABSTRAK

Pengelolaan jaringan hotspot yang tidak teratur merupakan kendala pada clients hotspot ketika mengakses jaringan yang salah satunya pemakai password yang dapat dipakai secara bersama-sama. Permasalahan utama pada jaringan yang telah ada di Pimpinan Pusat Muhammadiyah Yogyakarta berupa pengawasan client hotspot (pemakai internet) terhadap akses jaringan serta gangguan saat satu password digunakan secara bersama sehingga server yang diakses mengalami kelambatan. Maka diperlukan penelitian untuk mengidentifikasi jaringan hotspot yang telah ada.

Subjek dalam penelitian ini adalah rancang bangun sistem hotspot menggunakan captive portal. Pengumpulan data dalam penelitian ini menggunakan metode observasi, wawancara, metode studi literatur. Sistem yang dibangun adalah captive portal menggunakan aplikasi freeradius dan chillispot. Penyusunan meliputi dengan prosedur antara indentifikasi masalah, analisis kebutuhan, perancangan jaringan, perancangan sistem, serta implementasi jaringan hotspot menggunakan metode captive portal, sedangkan pengujian sistem dilakukan dengan black box dan alpha test.

Hasil penelitian dapat bekerja dengan optimal pada rancang bangun sistem hotspot menggunakan captive portal dan sistem yang mampu meningkatkan keamanan akses jaringan pada Pimpinan Pusat Muhammadiyah Yogyakarta. Sehingga mempermudah karyawan dalam memantau kegiatan client yang sedang memakai jaringan hotspot. Berdasarkan hasil uji coba tersebut dapat disimpulkan bahwa sistem captive portal ini dapat diterapkan pada sistem hotspot di Pimpinan Pusat Muhammadiyah Yogyakarta.

Kata Kunci : Captive portal, Chillispot, Freeradius, Internet, Hotspot.

1. PENDAHULUAN

Perkembangan teknologi komputer meningkat dengan cepat, hal ini terlihat pada era tahun 80 an jaringan komputer masih merupakan teka-teki yang ingin dijawab oleh kalangan akademisi, dan pada tahun 1988 jaringan komputer mulai digunakan di universitas-universitas, perusahaan-perusahaan, sekarang memasuki era *milenium* ini terutama *world wide internet* telah menjadi realitas sehari-hari jutaan manusia di muka bumi ini.

Perangkat keras dan perangkat lunak jaringan telah benar-benar berubah, di awal perkembangannya hampir seluruh jaringan dibangun dari kabel *koaxial*, kini banyak telah diantaranya dibangun dari serat optik (*fiber optics*) atau komunikasi tanpa kabel (*wireless*). Perkembangan ilmu pengetahuan dan teknologi, berkembang pula karakteristik masyarakat *modern* yang memiliki mobilitas tinggi, mencari layanan yang *fleksibel*, serba mudah dan memuaskan, serta mengejar efisiensi di segala aspek. Dan tulang punggung jaringan informasi dan komunikasi khususnya di Indonesia pada kenyataannya membutuhkan infrastruktur *backbone* yang handal, murah dan dapat dibangun sesuai kebutuhan akan dukungan ICT (*Information Electrical and Electronics Engineer*) dan *ETSI-HiperLAN*. Kebutuhan masyarakat semakin bertambah, khususnya kebutuhan akan akses *internet* dan ditunjang dengan semakin berkembangnya dunia teknologi, maka teknologi *Wi-Fi* mulai dirasa kurang dapat memenuhi kebutuhan masyarakat tersebut. Hal ini dikarenakan ditemukannya beberapa kekurangan pada teknologi *Wi-Fi* tersebut. Jaringan komputer untuk mengartikan suatu himpunan interkoneksi sejumlah komputer yang *autonomous* adalah dua buah komputer dikatakan terinterkoneksi bila keduanya dapat saling bertukar informasi. Bentuk koneksinya tidak harus melalui kawat tembaga saja melainkan dapat menggunakan serat optik, gelombang mikro, atau satelit komunikasi. Pada layanan hotspot dengan sebuah area yang menyediakan koneksi internet *wireless* yang dapat diakses melalui *Notebook*, PDA maupun perangkat lainnya yang mendukung teknologi tersebut.

Berdasarkan hasil observasi pada sistem hotspot dikantor Pimpinan Pusat Muhammadiyah Yogyakarta menggunakan tiga buah ISP (*Internet Service Provider*) yaitu paket *ISP Citra Net*, *ISP Speedy* dan *ISP UAD* serta satu buah *router* yang langsung menghubungkan ke HUB (*Head Up Butt*) dan tiga buah *access point*. Media hotspot tersebut yang selalu menjadi sarana untuk mengakses berbagai informasi bagi anggota dikantor Pimpinan Pusat Muhammadiyah Yogyakarta. Media *internet* merupakan *barometer* kemajuan teknologi informasi dan pada dasarnya area *hotspot* di Pimpinan Pusat Muhammadiyah Yogyakarta masih mempunyai berbagai masalah yang menjadi kendala pada sistem hotspot diantaranya adalah kurangnya pengelolaan dan peninjauan terhadap kegiatan hotspot, tidak adanya perekayasaan dalam jaringan, tidak ada sistem yang memonitoring kegiatan dalam jaringan serta hotspot masih bersifat terbuka atau umum dengan *login* menggunakan *password* yang sama dan dapat digunakan banyak *users* atau pemakai media hotspot, jadi semua permasalahan tersebut yang sering mengganggu kegiatan hotspot yang semestinya stabil atau lancar menjadi lambat dan sering terjadi kegagalan dalam *login user* untuk mengakses internet di Pimpinan Pusat Muhammadiyah Yogyakarta. Sistem seperti inilah yang membuat pemakai hotspot merasa bahwa kurang optimal dalam penggunaannya.

Berdasarkan latar belakang diatas, maka dibutuhkan sebuah sistem yang dapat mengontrol dan memonitoring akses *hotspot* serta sistem yang mampu mengamankan jaringan *hotspot* di Pimpinan Pusat Muhammadiyah Yogyakarta. Oleh karena itu akan

dilakukan sebuah penelitian dengan obyek penelitian “Rancang Bangun Sistem *Hotspot* Menggunakan *Captive Portal*”.

Pada penelitian ini menitikberatkan pada perancangan sistem *hotspot captive portal* menggunakan sistem operasi *Ubuntu* dan *freeradius* serta *chillispot* sebagai aplikasinya. Disini peneliti akan menekankan pada sistem *autentikasi* menggunakan *server radius*, *easyhotspot* untuk *management hotspot* dan *chillispot* sebagai *captive portal*. Dengan harapan sebagai solusi untuk meningkatkan keamanan jaringan pada sistem *hotspot* yang efektif dan efisien diPimpinan Pusat Muhammadiyah Yogyakarta.

2. KAJIAN PUSTAKA

Gesit singgih febyatmoko [1], Sistem Otentikasi Otorisasi dan pelaporan koneksi *user* pada jaringan *wireless Chillispot* dan *server Radius*. Pada penelitian ini dilakukan terhadap level keamanan *WLAN* dan pembagian akses layanan yang dapat menjadi lebih baik. Penggunaan layanan jaringan yang dapat dimonitor oleh *administrator* melalui aplikasi berbasis *web* dan pengaksesan basis data. Pada penelitian ini menggunakan server *UAM (Universal Access Method)* dengan *chillispot*. Konfigurasi *server Radius* menggunakan *software Freeradius* dan pembangunan aplikasinya menggunakan Sistem Administrasi *Hotspot* berbasis *web* menggunakan bahasa pemrograman *PHP* [1].

Lilik Suheri [2], Analisis Manajemen *Hotspot* dengan *Captive portal*. Pada penelitian ini membahas penggunaan dan menerapkan aplikasi *Captive Portal* pada jaringan nirkabel pada *hotspot area*, serta memberikan jaminan keamanan terhadap pengguna jaringan nirkabel, dan untuk mempermudah perawatan *account* jaringan nirkabel. Sistem *accounting* pengguna yang digunakan oleh aplikasi *Captive Portal* dalam penelitian ini adalah dengan menggunakan protokol *Remote Authentication Dial-In Services (RADIUS)* [2].

Permadhi santhosa [3], Perancangan *Prototype RADIUS Server* dan *Chillispot* untuk Otentikasi Pengguna Jaringan *Wireless*. Pada penelitian ini membahas perancangan *radius server* untuk mempersempit celah keamanan yang dapat di gunakan oleh pengguna yang ingin mengakses jaringan secara *illegal* dan membatasi hak akses setiap pengguna yang akan mengakses jaringan *wireless* [3].

Yuswira effendi [4], Desain dan Implementasi autentikasi jaringan *hotspot* menggunakan *Chillispot* autentikasi sistem dan *Radius server* pada debian *GNU/Linux 4.0 r3 ETCH*. Pada penelitian ini membahas tentang pembatasan akses diwilayah area *hotspot* dan memonitori semua jaringan untuk memaksimalkan layanan pada setiap komputer yang mengakses *hotspot* akan menghadapi halaman *web* utama yang mengharuskan *user* untuk mendaftar atau *login* terlebih dahulu sebelum memakai layanan *hotspot*. Penelitian ini memanfaatkan *Debian GNU/Linux 4.0r3 ETCH* sebagai sistem operasi pengganti *windows* untuk komputer *server* dan memakai *Chillispot* sebagai sistem autentikasi *web login* untuk proses *user wireless client*[4].

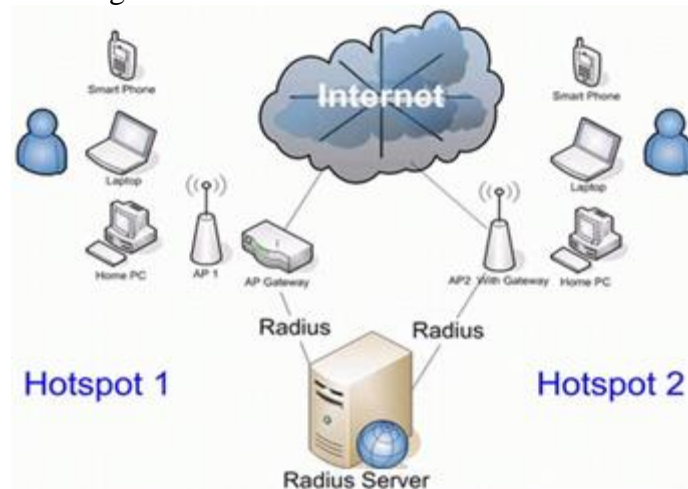
Widhargo [5], Autentikasi Jaringan *Lan* dan *Wireless Lan* menggunakan *Raouter Pfsensi Radius*. Pada penelitian ini menggunakan *router pfsense* yang memiliki fasilitas *captive portal* untuk *redirect user* agar masuk ke halaman *login* sebelum menggunakan *internet* baik pada jaringan *LAN* maupun *wireless LAN* dan pada penelitian ini menggunakan *windows server 2003* sebagai *server radius authentication* [5].

Pada penelitian ini menitik beratkan pada perancang membangun *captive portal* menggunakan *freeradius* sebagai aplikasinya. Disini peneliti akan menekankan optimasi

dalam pelaporan atau penyaringan semua koneksi yang masuk dan menolak koneksi yang tidak diinginkan (tidak terdaftar sebagai *client*) dengan harapan sebagai solusi untuk meningkatkan kinerja keamanan jaringan komputer yang efektif dan efisien.

2.1 Captive Portal

Captive portal adalah suatu teknik autentikasi dan pengamanan data yang lewat dari *network internal* ke *network eksternal*. *Captive Portal* dapat diartikan sebagai mesin *router* atau *gateway* yang memproteksi atau tidak mengizinkan adanya trafik, sampai user melakukan *registrasi* terlebih dahulu ke dalam sistem. Biasanya *Captive Portal* digunakan pada *infrastruktur wireless* seperti *hotspot* area, tapi tidak menutup kemungkinan diterapkan pada jaringan kabel. Pada *managemant hotspot* berbasis *captive portal* dapat dilihat digambar 1 dibawah ini:



Gambar 1. *Managemant hotspot* berbasis *captive portal*

2.2 Radius Server

Merupakan suatu mekanisme akses kontrol yang mengecek dan mengautentifikasi (*authentication*) user atau pengguna berdasarkan pada mekanisme autentikasi dengan menggunakan metode *challenge / response*. *Remote Access Dial In User Service (radius)* merupakan protokol *connectionless* berbasis UDP yang tidak menggunakan koneksi langsung. Satu paket *radius* ditandai dengan *field* UDP yang menggunakan *port* 1812. *Radius* menggunakan lapisan *transport* UDP dan *radius* memiliki tempat yang paling penting pada layanan *internet*, pada pengaturan, otorisasi, dan rinci *accounting* pengguna baik yang diperlukan atau diinginkan [2].

2.3 Chillispot

Chillispot adalah *Wireless Access Point Controller* berbasis *open source*. *Chillispot* merupakan *software captive portal* yang digunakan untuk autentikasi *user Wireless LAN*. Cara kerja *Chillispot* adalah dengan cara *capture request* halaman *web client* dan kemudian di-*redirect* ke halaman *web Chillispot* untuk *login* autentikasi. Data *user* dan *password* yang dimasukkan *user* akan ditransfer ke *server RADIUS* untuk proses autentikasi dan otorisasi hak akses. Apabila data *user* dan *password* terautentikasi oleh *server Radius* maka *user* dapat mengakses halaman *web* di *internet*. *Chillispot* dikembangkan pada *platform* sistem operasi *Linux* tetapi juga dapat di-

compile pada sistem operasi *FreeBSD*, *OpenBSD*, *Solaris*, dan bahkan *MAC OS X*. *Chillispot* dikembangkan menggunakan bahasa pemrograman *C* untuk meningkatkan portabilitas *platform* sistem operasi yang digunakan. Beberapa fitur yang dimiliki oleh *Chillispot* antara lain *server UAM*, layanan *DHCP*, dan *captive portal*. [3].

3. METODE PENELITIAN

Subyek penelitian ini adalah Rancang bangun sistem hotspot menggunakan *Captive Portal* dan sistem yang dibangun menggunakan aplikasi *freeradius* dan *chillispot* digunakan sebagai *captive portal*. Pada sistem hotspot captive portal diPimpinan Pusat Muhammadiyah Yogyakarta menggunakan sistem operasi *Ubuntu*.

3.1. Metode Pengumpulan Data

Pengumpulan data merupakan suatu usaha yang dilakukan untuk memperoleh data atau dokumentasi yang dibutuhkan dalam penelitian. Data yang diperoleh kemudian diproses sesuai dengan kebutuhan penelitian. Penelitian ini menggunakan metode pengumpulan data antara lain :

3.1.1. Studi Literatur

Studi Literatur merupakan cara pengumpulan data dengan membaca buku referensi atau dokumentasi yang berhubungan dengan penelitian, *browsing* atau *searching* merupakan cara pengumpulan data dengan cara *browsing* di *Internet* untuk mencari data atau dokumentasi yang berhubungan dengan obyek yang diteliti.

3.1.2. Metode Observasi

Metode observasi merupakan metode pengamatan secara langsung terhadap sistem *hotspot* yang sudah diterapkan, serta mengetahui kekurangan dari sistem tersebut dan mengetahui segala aktivitas *hotspot* di lingkungan Pimpinan Pusat Muhammadiyah Yogyakarta untuk mempelajari dan mengetahui masalah yang sering terjadi dalam jaringan *hotspot*.

3.1.3. Metode Wawancara

Merupakan metode yang dilakukan dengan mengajukan pertanyaan atau tanya jawab secara langsung kepada pengelola *hotspot* dan *user* atau *clients* di Pimpinan Pusat Muhammadiyah Yogyakarta. Metode ini dilakukan untuk mengetahui masalah yang ada, sehingga diharapkan hasil penelitian dapat membenahi permasalahan tersebut.

3.1.4. Analisis Kebutuhan User

Kebutuhan user untuk mengakses informasi pada media *internet* di Pimpinan Pusat Muhammadiyah Yogyakarta merupakan sarana yang paling penting yang menggunakan akses *hotspot*. Untuk memperlancar sebuah sistem yang dapat meningkatkan kinerja dari sistem *hotspot* yaitu dengan memaksimalkan keamanan serta meningkatkan kenyamanan dalam mengakses, mengelola serta memonitoring dari kegiatan *hotspot*. Hal ini dapat terpenuhi bila sistem yang dibangun memenuhi unsur-unsur yang diperlukan. Dengan melakukan observasi dalam sebuah penelitian maka dapat diambil beberapa hal yang menyangkut kebutuhan *user* dan *administrator* sebagai pengguna dan pengelola *hotspot* adalah:

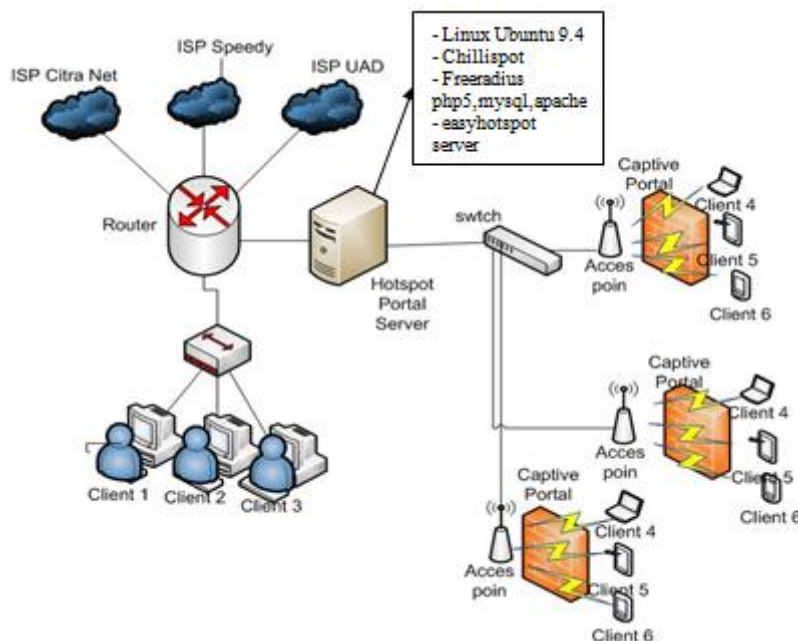
1. Perlunya sistem yang dapat memaksimalkan keamanan pada jaringan *hotspot*.
2. Perlunya sistem yang mampu meningkatkan kenyamanan dalam mengakses *hotspot*.
3. Perlunya sistem yang mampu memantau atau *memonitoring* dari aktifitas penggunaan *hotspot*.

3.2. Analisis Kebutuhan Sistem

Analisis sistem yang dilakukan meliputi pengamatan dengan cara pengaksesan terhadap *user* yang sedang menggunakan *hotspot*, kapan saja *user* mengalami kegagalan *login*, dikarenakan *password* yang dipakai sedang digunakan oleh beberapa *user* yang mengakses *hotspot*. Pada *server* tidak ada sistem yang memonitoring atau mengontrol aktivitas *hotspot* sehingga pemakai *hotspot* tidak stabil dan banyak pihak yang tidak memiliki hak akses memanfaatkan media *hotspot* yang mengakibatkan akses menjadi lambat. Sehingga dalam penelitian ini, sistem yang dihasilkan nantinya diharapkan dapat mengatasi segala permasalahan-permasalahan yang ada pada sistem *hotspot* di Pimpinan Pusat Muhammadiyah Yogyakarta. Dengan cara membangun sistem *hotspot* menggunakan *captive portal* sehingga dapat mampu meningkatkan keamanan jaringan dan mempermudah pengelolaan pada sistem *hotspot*.

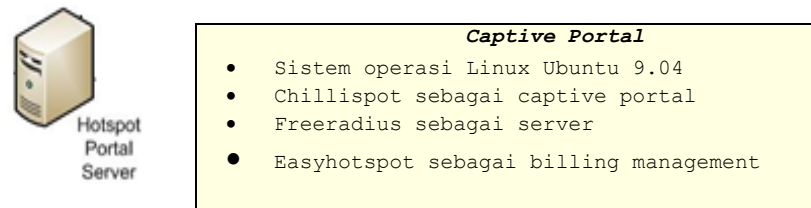
3.3. Perancangan Jaringan

Pada tahap ini dilakukan analisis kebutuhan dan perancangan sistem untuk merumuskan solusi yang tepat dalam pembuatan sistem serta kemungkinan yang dapat dilakukan untuk mengimplementasikan rancangan tersebut. Berikut rencana desain sistem *hotspot* menggunakan *captive portal* yang akan dibuat seperti pada gambar 2 dibawah ini :



Gambar 2. Rancangan sistem *hotspot* menggunakan *captive portal*.

Keterangan pada *hotspot captive portal* seperti tampak pada gambar 3 berikut :



Gambar 3. Keterangan sistem *hotspot captive portal*

Rancangan *captive portal* dapat diuraikan bahwa hal utama yaitu *client* mengakses terhadap *server* yang melalui *access point* selanjutnya akan diteruskan ke switch atau HUB dan akan masuk ke *server*, dengan *router* yang sudah terkoneksi Internet dan bertindak sebagai *gateway* ISP Speedy, ISP Citranet dan ISP UAD. Dalam hal ini *radius* berperan sebagai *server* dan kontroler yang diberi laporan dari *chillispot* yang berperan sebagai *captive portal* sebagai sistem *login*.

4. HASIL DAN PEMBAHASAN

Tahap implementasi menitik beratkan pada rancang bangun sistem hotspot menggunakan *captive portal*. Mempersiapkan komputer yang akan digunakan dalam penelitian, membuat kabel LAN atau *crimping*, instalasi sistem operasi yang digunakan yaitu sistem operasi *Ubuntu* dan konfigurasi beberapa *service* setelah proses instalasi selesai. Tahapan dalam implementasi adalah sebagai berikut:

4.1 Konfigurasi *Ubuntu*

Proses instalasi Sistem Operasi *Ubuntu* versi 9.10 i386 pada tahap ini dimulai dari pemilihan *regional country*, *keyboard layout*, pemilihan partisi *hardisk* yang akan digunakan sebagai *mount point* sampai semua proses instalasi selesai.

4.2 Konfigurasi *Apache Web Server mod Php5*

Proses konfigurasi *apache* dilakukan dengan cara *manual compile*, untuk mencari sebuah paket yang akan dikonfigurasi, *Apache* melingkupi berbagai *library* sebelum ekstraksi file yang akan dikonfigurasi.

4.3 Konfigurasi *chillispot*

Proses konfigurasi *chillispot* dilakukan melalui *ports collection*, untuk mencari sebuah *file* yang akan dikonfigurasi, hasil tersebut menandakan bahwa *file* konfigurasi *chillispot* terdapat pada direktori *nano /etc/chilli.conf*.

4.4 Konfigurasi *Freeradius*

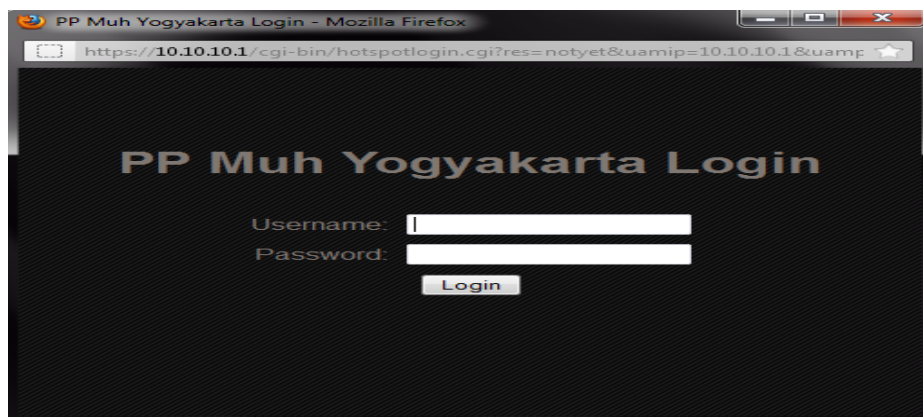
Radius merupakan sebuah protokol keamanan yang digunakan untuk autentikasi terhadap akses jaringan. Pada hal ini konfigurasi *freeradius* merupakan *file* konfigurasi utama yang menggabungkan *file-file* konfigurasi yang terpisah, diantaranya adalah konfigurasi *clients* (*clients.conf*), konfigurasi *sql* (*sql.conf*) dan modul-modul yang dibutuhkan oleh *server freeradius*, pada *file* konfigurasi *freeradius* dapat ditemukan pada *file* direktori *nano /etc/freeradius/radiusd.conf*.

4.5 Easyhotspot

Easyhotspot merupakan *interface* berbasis *PHP* yang dapat berfungsi sebagai *web administrator* dan pengontrol *freeradius*. Pada proses ini ketika penginstalan dan konfigurasi *easyhotspot* telah selesai maka akan dilanjutkan pengeditan konfigurasi *chillispot* yang berada pada menu *dieasyhotspot* yang nantinya akan berperan sebagai halaman *login captive portal* pada *clients* atau *users*.

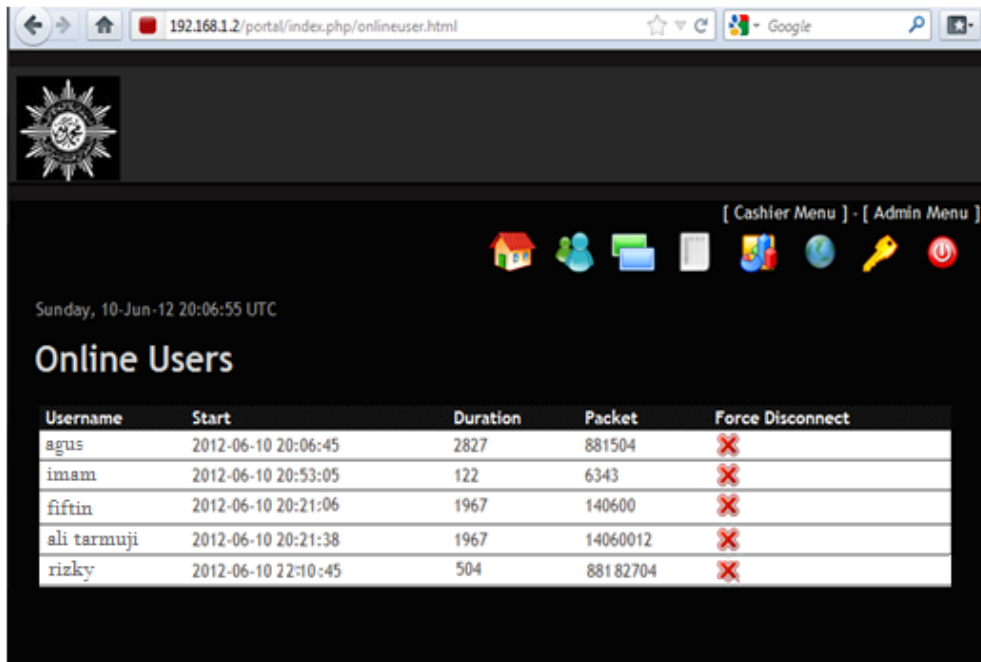
4.6 Pengujian sistem

Pada pengujian ini menitik beratkan apakah sistem *hotspot* menggunakan *captive portal* telah bekerja sesuai dengan yang diharapkan. Pengujian ini dilakukan dengan *user* yang sudah terdaftar dan melakukan *login* pada akses *hotspot* Pimpinan Pusat Muhammadiyah Yogyakarta yang terlihat pada *form login* gambar 4 dibawah ini:



Gambar 4. *Form login user*.

Dengan cara kerja *chillispot* yaitu menangkap permintaan halaman *web client* dan kemudian di *redirect* ke halaman *web chillispot* untuk *login autentikasi*. Data *user* dan *password* akan ditransfer ke *server radius* untuk proses *autentikasi* dan *otorisasi* hak akses sebelum dapat mengakses *internet*. Setelah *client login* dengan mengisi *username* dan *password* yang benar atau telah terotentikasi di *database* maka *chillispot* juga akan menampilkan halaman *logout* yang berfungsi untuk memutuskan koneksi *hotspot*. Pada akses sistem yang sudah terdaftar dan sedang menggunakan *hotspot captive portal* selanjutnya akan dimonitoring di halaman *web administrator*, hal ini dimaksudkan untuk mengetahui apakah *user* yang memakai jaringan *hotspot* dapat terlihat atau terdeteksi dalam menangani permintaan. Setelah masuk ke *web administrator* maka selanjutnya akan mengontrol atau memonitoring *users* yang sedang aktif atau memakai *hotspot captive portal* Hasil monitoring berjalan dengan baik seperti pada gambar 5 dibawah ini:



Username	Start	Duration	Packet	Force Disconnect
agus	2012-06-10 20:06:45	2827	881504	✗
imam	2012-06-10 20:53:05	122	6343	✗
fiftin	2012-06-10 20:21:06	1967	140600	✗
ali tarmuji	2012-06-10 20:21:38	1967	14060012	✗
rizky	2012-06-10 22:10:45	504	881 82704	✗

Gambar 5. Monitoring akses users diweb administrator

5 KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan sebelumnya maka dapat diambil kesimpulan sebagai berikut :

- Pada sistem *hotspot* menggunakan metode *captive portal* diPimpinan Pusat Muhammadiyah yogyakarta telah mampu menjaga keamanan dalam *login* setiap *user* .
- Captive portal* telah bekerja dan mampu menangani semua permintaan *client*, untuk mengakses jaringan *hotspot*.

6 DAFTAR PUSTAKA

- [1], Gesit Singgih Febyatmoko, 2006, "*Sistem Otentikasi Otorisasi dan pelaporan koneksi user pada jaringan wireless Chillispot dan server Radius*", Surabaya, Skripsi
- [2], Lilik Suheri, 2009, "*Analisis Manajemen Hotspot dengan Captive Portal*", Semarang, Skripsi.
- [3], Permadhi Santosa, 2011, "*Perancangan Prototype Radius Server dan Chillispot untuk Otentikasi Pengguna Jaringan Wireless*". Skripsi, Bandung.
- [4], Widhargo, 2009, "*Autentikasi Jaringan LAN dan Wireless menggunakan Raouter Pfense dengan Radius*", Skripsi, Surakarta
- [5], Yuswira Efendi, 2008 "*Desain Dan Implementasi Autentikasi jaringan Hotspot menggunakan Chillispot autentikasi system dan radius server pada GNU/Linux 4.0 r3 ETH*", Surakarta, Skripsi
- [6], <http://ndra.gmib26.net/2010/06/install-easyhotspot-dan-konfigurasi-freeradius-serta-coova-chilli-di-ubuntu-10-04-lts-server-edition>(diakses rabu,30 mei 2012).