IMPLEMENTASI SISTEM OTENTIKASI PADA PENGGUNA JARINGAN *HOTSPOT* DI UNIVERSITAS KANJURUHAN MALANG GUNA MENINGKATKAN KEAMANAN JARINGAN KOMPUTER

Yusriel Ardian
Universitas Kanjuruhan Malang
Jl. S. Supriyadi 48 Malang. Telepon: (0341) 801488
Email: acilnet@yahoo.com

ABSTRAK: Semakin banyaknya aplikasi yang menggunakan *client server* baik *desktop* maupun *WEB Application* membuat setiap user harus memiliki banyak *user id* dan *password* yang harus dihapalkan, karena setiap aplikasi pasti membutuhkan otentikasi agar dapat memanfaatkan aplikasi tersebut dengan alasan keamanan. Selain itu perkembangan media jaringan juga semakin berkembang baik penggunaan kabel maupun nirkabel. Dari penjelasan diatas teknologi RADIUS sangatlah dibutuhkan dalam kasus yang telah dijelaskan diatas, karena dengan metode RADIUS ini memungkinkan seorang user cukup memiliki satu *user id* untuk mengakses ke beberapa aplikasi, baik *desktop* maupun *WEB application*. Metode RADIUS juga dapat diintregasikan terhadap media kabel dan nirkabel.

Kata kunci: Nirkabel, WEP, otentikasi, RADIUS, *database, server, client*

Abstract: *The number of client server applications using both desktop and WEB Application makes every user must have a lot of user id and password that must be memorized, because each application must require authentication in order to utilize the application for security reasons. Besides the development of network media is also growing use of both wired and wireless. From the above explanation RADIUS technology is desperately needed in the case described above, since the RADIUS method allows a user simply has a userID for access to multiple applications, both desktop and WEB application. RADIUS can also integrated method of wired and wireless media.*

Keywords*:* Wireless, WEP, authentication, RADIUS, database, server, client

PENDAHULUAN

Penggunaan jaringan saat ini pada umumnya tanpa adanya otentikasi pengguna. Dengan tanpa adanya otentikasi pengguna ini maka jaringan dapat diakses oleh siapa saja ketika pengguna bergabung dalam jaringan.

Untuk media transmisi menggunakan *wireless access point* otentikasi menggunakan *Wired Equivalent Privacy* (WEP). *Key* pada WEP harus dipasang pada tiap *access point* dan tiap *client access point*, sehingga merepotkan administrator karena harus mendatangi masing-masing client. *Key* WEP juga bersifat statik sehingga mudah diketahui dengan melihat komputer *client* yang lain. Sekarang sudah ada beberapa aplikasi yang bisa membaca *key* WEP sehingga pengguna yang tidak berhak bias masuk ke jaringan, yang bisa membahayakan sistem di dalamnya.

Otentikasi WEP hanya diberikan kepada jalur koneksi untuk staf, sedangkan jalur koneksi untuk mahasiswa (*hostspot*) yang menggunakan media transmisi *wireless access point* tanpa menggunakan otentikasi sehingga dapat diakses oleh siapa saja. Pada media transmisi kabel yang menggunakan HUB sebagai pemecah koneksi tidak menggunakan otentikasi, sehingga dengan menancapkan kabel kita bisa langsung terhubung ke jaringan. Oleh karena itu dalam penelitian ini dibuat sistem untuk otentikasi pengguna, baik yang menggunakan media transmisi kabel maupun nirkabel.

Tujuan penulisan adalah untuk:

1) Pengembangan manajemen sistem keamanan jaringan yang lebih baik
2) Mengintregasikan manajemen *user* untuk beberapa aplikasi

TINJAUAN PUSTAKA

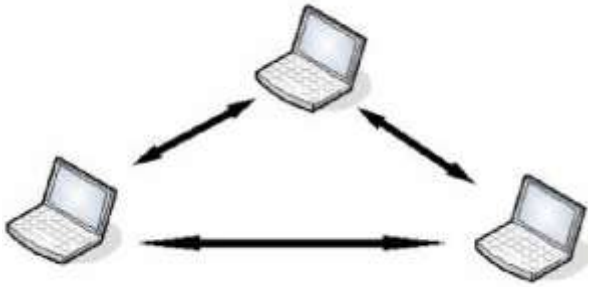
Jaringan Wireless

Jaringan *Wireless Local Area Network* (WLAN) merupakan salah satu bentuk jaringan *wireless*. Jaringan WLAN adalah jaringan yang memungkinkan dua mesin atau lebih untuk berkomunikasi menggunakan protokol jaringan standar tetapi tanpa

menggunakan media transmisi kabel. Media transmisi yang digunakan komunikasi pada jaringan WLAN adalah gelombang elektromagnetik yang dapat berupa sinar infra-merah (*infrared,* IR), gelombang mikro (*microwave*) atau gelombang radio (*radio frequency*, RF). Mode Jaringan WLAN, antara lain:

1. Mode Ad-Hoc

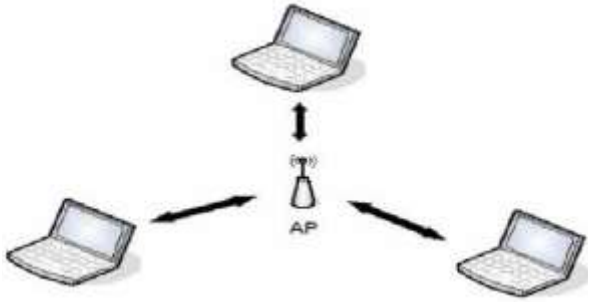
Mode Ad-hoc sering disebut sebagai jaringan *peer to peer* atau disebut juga jaringan *point to point*. Mode Ad-hoc memungkinkan hubungan antar komputer pada jaringan WLAN tanpa melalui suatu *access point*.



Gambar 1. Mode Ad-hoc

2. Mode Infrastruktur

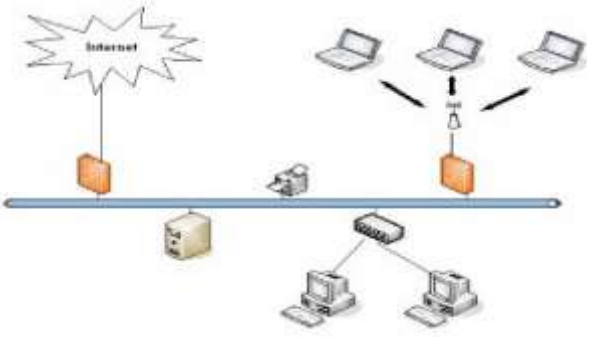
Untuk menghubungkan banyak komputer jaringan WLAN harus dijalankan menggunakan mode Infrastruktur. Pada mode Infrastruktur diperlukan peralatan tambahan berupa *wireless access point* (WAP) atau disebut secara singkat dengan *access point. Access point* berlaku seperti HUB atau *switch* pada jaringan kabel, sehingga *access point* akan menjadi pusat dari jaringan WLAN



Gambar 2. Mode Infrastruktur

Jaringan WLAN dan Ethernet

Jaringan WLAN yang bekerja pada mode Infrastruktur dapat dihubungkan dengan jaringan lain misalnya jaringan Ethernet. Untuk berhubungan dengan jaringan lain diperlukan *bridge*. *Access point* yang beredar di pasaran umumnya sudah dapat difungsikan sebagai *bridge*.



Gambar 3. Jaringan WLAN dan Ethernet

Protokol Rute (Routing Protocol)

Routing adalah proses membawa paket data dari satu host asal ke host tujuan melalui satu atau beberapa *host node* lainnya. Secara umum mekanisme koordinasi routing dapat dibagi menjadi dua, yaitu routing statis dan routing dinamis, dengan penjelasan sebagai berikut:

1. Routing Statis

Pada routing statis, entri-entri dalam *forwarding* tabel routing diisi dan dihapus secara manual sedangkan pada routing dinamis perubahan dilakukan melalui protokol routing. Routing statis adalah pengaturan routing paling sederhana yang dapat dilakukan pada jaringan komputer. Menggunakan routing statis murni dalam sebuah jaringan berarti mengisi setiap entri dalam *forwarding* table di setiap router yang berada dalam jaringan tersebut.

Penggunaan routing statis dalam sebuah jaringan yang kecil bukanlah sebuah masalah hanya beberapa entri yang perlu diisikan pada *forwarding* table di setiap router. Sebaliknya jika harus melengkapi *forwarding* table di setiap router yang jumlahnya tidak sedikit dalam jaringan yang besar.

2. Routing Dinamis

Routing dinamis adalah cara yang digunakan untuk melepaskan kewajiban mengisi entri-entri *forwarding* table secara manual. Protokol routing mengatur router-router sehingga dapat berkomunikasi satu dengan yang lain dan saling memberikan informasi routing yang dapat mengubah isi *forwarding* table, tergantung keadaan jaringannya. Dengan cara ini, router-router mengetahui keadaan jaringan yang terakhir dan mampu meneruskan datagram ke arah yang benar.

RADIUS (*Remote Authentication Dial-In User Service*)

RADIUS adalah sebuah protokol keamanan komputer yang digunakan untuk melakukan otentikasi, otorisasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan. RADIUS didefinisikan di dalam RFC 2865 dan RFC 2866, yang pada awalnya digunakan untuk melakukan otentikasi terhadap akses jaringan secara jarak jauh dengan menggunakan koneksi dial-up. RADIUS, kini telah diimplementasikan untuk melakukan otentikasi terhadap akses jaringan secara jarak jauh dengan menggunakan koneksi selain dial-up, seperti halnya VPN (*Virtual Private Networking)*, *access point* nirkabel, *switch* Ethernet, dan perangkat lainnya.

Server RADIUS menyediakan mekanisme keamanan dengan menangani otentikasi dan otorisasi koneksi yang dilakukan pengguna. Pada saat computer *client* akan menghubungkan diri dengan jaringan maka server RADIUS akan meminta identitas pengguna (*username* dan *password*) untuk kemudian dicocokkan dengan data yang ada dalam *database server* RADIUS untuk kemudian ditentukan apakah pengguna diijinkan untuk menggunakan layanan dalam jaringan komputer. Jika proses otentikasi dan otorisasi berhasil maka proses pelaporan dilakukan, yakni dengan mencatat semua aktifitas koneksi pengguna, menghitung durasi waktu dan jumlah transfer data yang dilakukan oleh pengguna. Proses pelaporan yang dilakukan server RADIUS bisa dalam bentuk waktu (detik, menit, jam) maupun dalam bentuk besar transfer data (*Byte, KByte, Mbyte*).

WEP

WEP (*Wired Equivalent Privacy*) adalah suatu metode pengamanan jaringan nirkabel, disebut juga dengan *Shared Key Authentication*. *Shared Key Authentication* adalah metode otentikasi yang membutuhkan penggunaan WEP.

Enkripsi WEP menggunakan kunci yang dimasukkan (oleh administrator) ke *client* maupun *access point.* Kunci ini harus cocok dari yang diberikan akses point ke *client,* dengan yang dimasukkan client untuk otentikasi menuju *access point*.

RANCANGAN SISTEM

Kebutuhan Perangkat Keras (Minimal)

1. Motherboard x86 300 MHZ Pentium
2. RAM 64 MB
3. Hardisk 40 GB

Kebutuhan hardware untuk menginstal Router OS, dalam hal ini menggunakan MikrotikOS
1. CPU dan motherboard 100 MHz Pentium.
2. RAM 32 MB
3. Hardisk ATA/IDE 1 GB.

Kebutuhan Perangkat Lunak

Media instalasi Linux Ubuntu dan MikroTik adalah:
- CD Linux Ubuntu Server 8.04 LTS
- CD MikroTik
- Software FreeRADIUS Server
- Software LAMP (Linux Apache MySql Php)

Kebutuhan Pengguna

Pada dasarnya, Pengguna melihat bahwa jaringan yang diperlukan cukup sederhana dan tidak rumit. Ini dikarenakan client memandang jaringan hanya digunakan untuk share informasi yang umum dan koneksi internet.

Berikut ini adalah ringkasan dari kebutuhan pengguna dilihat dari beberapa parameter. Ringkasan ini didapatkan dari pemegang kebijakan kampus terhadap pengembangan jaringan:

Tabel 1. *Kebutuhan Pengguna*

Parameter	Kebutuhan Pengguna
Waktu Akses Staf	Jam kerja (08.00 – 15.00)
Waktu Akses Mahasiswa	Jam kuliah (07.00 – 21.00)
Waktu Respon	5 Menit
Realibilitas Tampilan	Sistem selalu di- *maintenance* oleh administrator WEB Base
Keamanan	Jaminan keamanan pengguna dan *device*
Dukungan Layanan	Aplikasi mudah digunakan oleh pengguna

Analisa Aplikasi

Aplikasi yang ada di jaringan Universitas Kanjuruhan Malang dibedakan menjadi beberapa kategori yaitu:

Aplikasi Desktop

Aplikasi *Desktop* adalah suatu aplikasi yang dapat berjalan sendiri atau independen tanpa menggunakan *browser* pada suatu komputer otonom dengan sistem operasi tertentu. Penggunaan aplikasi desktop dengan cara meng-*install* aplikasi ini pada masing-masing pengguna.

Penggunaan aplikasi *desktop* di Universitas Kanjuruhan Malang adalah untuk proses administrasi

pada jaringan lokal. Beberapa aplikasi desktop diantaranya adalah bits dosen, bits mahasiswa dan bits akademik. Semua aplikasi tersebut bekerja sebagai client server.

Aplikasi WEB

Beberapa aplikasi berbasis WEB yang ada di Universitas Kanjuruhan Malang adalah *elearning, ebook, ejournal*, WEB *mail client*, perpustakaan *on line*, SIAKAD yang bisa diakses baik melalui jaringan lokal maupun jaringan internet.

Aplikasi Server

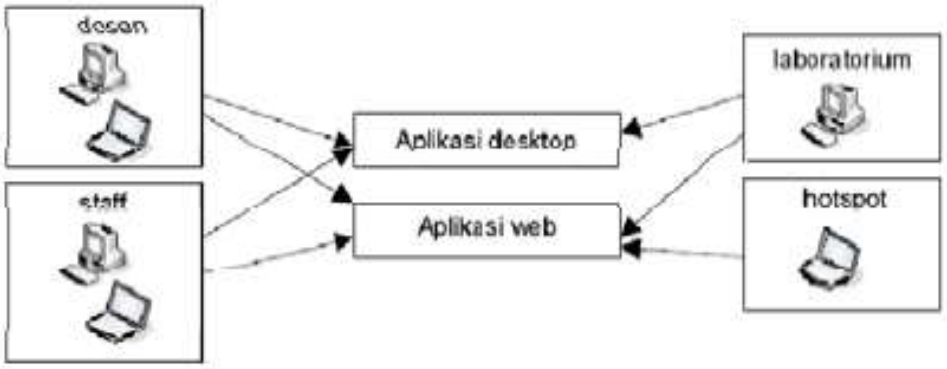
Beberapa aplikasi server yang digunakan di Universitas Kanjuruhan Malang adalah WEB *server*, *database server, mail server*, FTP *server*, DNS *server*, proxy *server* dan *firewall*.

Akses Pengguna

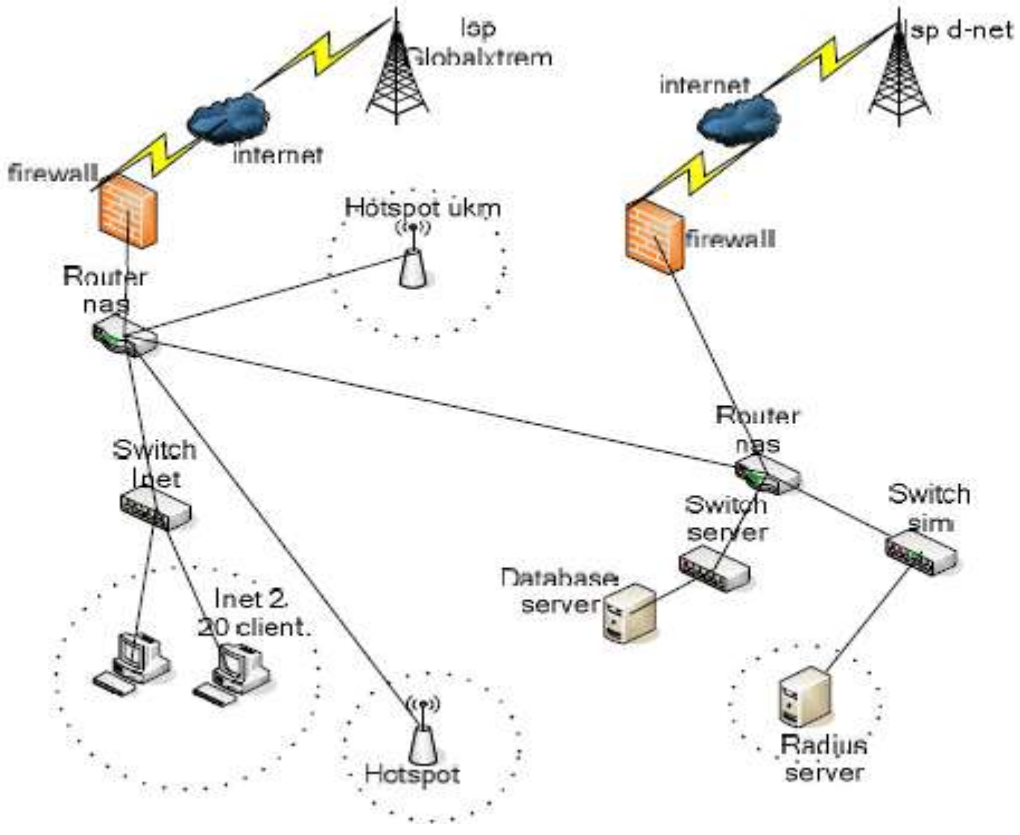
Dari pemaparan diatas dapat digambarkan seperti pada Gambar 4 dimana dosen, staf dan laboratorium dapat mengakses aplikasi *desktop* dan aplikasi WEB, sedangkan *hostspot* hanya mengakses aplikasi WEB saja.

Perancangan Sistem

Perancangan sistem otentikasi pengguna jarringan di Universitas Kanjuruhan Malang memanfaatkan protokol RADIUS dan protokol TCP/IP (*Transfer Control Protocol/ Internet Protocol*). Untuk dapat



Gambar 4. Akses Pengguna



Gambar 5. Desain Topologi RADIUS

terhubung ke dalam jaringan pengguna harus memasukan *username* dan *password*.

Topologi Jaringan

Pada saat ini, jaringan Universitas Kanjuruhan Malang digunakan untuk administrasi dan akses internet, sebagaimana ditampilkan dalam Gambar 4. Jaringan Universitas Kanjuruhan menggunakan media transmisi kabel dan nirkabel. Untuk menghubungkan antar gedung kabel yang digunakan adalah kabel STP (*Shield Twister Pair*). Untuk menghubungkan *client* dalam satu ruangan digunakan media transmisi kabel UTP (*Unshield Twister Pair*) dan *wireless*. Sedangkan media transmisi untuk *hostspot* area bagi mahasiswa digunakan *wireless*.

Untuk memecah antar *client* digunakan HUB yang diletakan ditiap gedung atau ruangan disesuaikan dengan jumlah *client*.

Desain Topologi RADIUS

Secara sederhana desain topologi dengan RADIUS *Server* seperti pada Gambar 5. *Server* RADIUS berfungsi menyimpan username dan password secara terpusat. Pengguna memasukan username dan password melalui *interface* yang disediakan oleh NAS (*Network Access Server*), selanjutnya NAS akan menanyakan ke RADIUS server apakah *username* dan *password* ada dalam *database*. Jika *username* dan *password* ada maka pengguna akan diijinkan menggunakan jaringan.

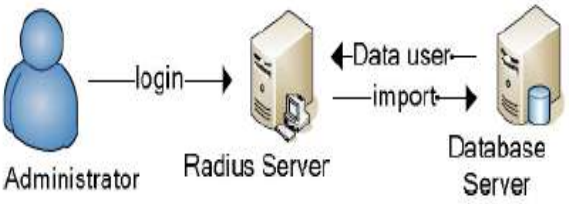
Arsitektur Sistem

Arsitektur Pengambilan Data Pengguna Arsitektur pengambilan data pengguna dari *database* akademik ke dalam RADIUS *Server* seperti terlihat pada gambar dibawah ini.

Gambar 6 menggambarkan arsitektur pengambilan data pengguna dari *database* akademik ke dalam RADIUS *server*. Administrator mengambil data pengguna dari Database *Server* untuk dimasukan ke RADIUS *Server*. Data yang diambil adalah data mahasiswa yang telah registrasi pada semester berjalan. Data yang dimasukkan ke RADIUS *Server* adalah NIM (Nomor Induk Mahasiswa), *password*, nama dan program studi.

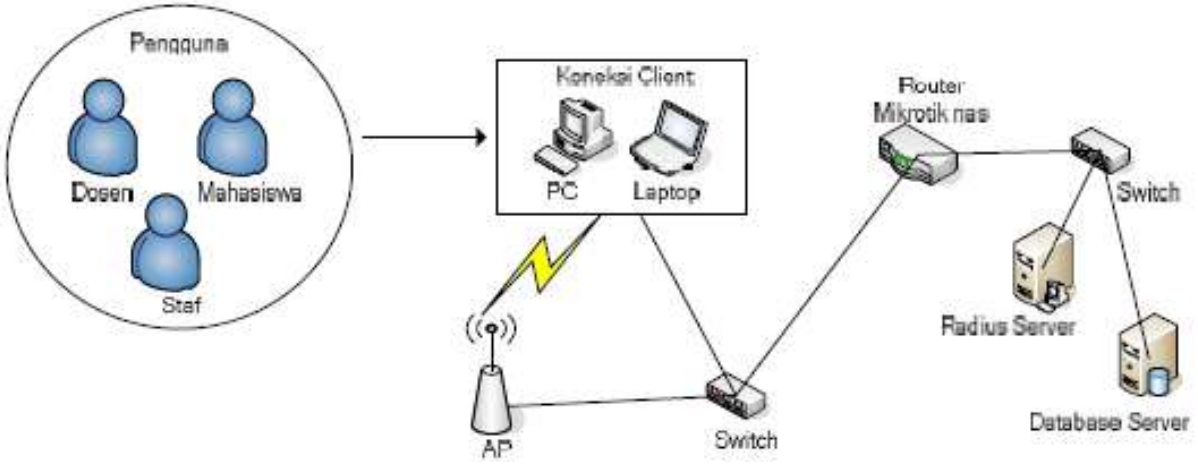
Arsitektur Sistem Otentikasi

Arsitektur sistem otentikasi seperti terlihat pada Gambar 7. Gambar 7 menggambarkan arsitektur sistem otentikasi, terlihat bahwa pengguna terdiri dari dosen, staf dan mahasiswa. Pengguna agar terhubung ke dalam jaringan harus menggunkan PC atau Laptop. Pengguna dapat memanfaatkan jaringan apabila memiliki username dan password pada RADIUS *server*. Apabila pengguna sudah berhasil *login*, maka pengguna bisa terhubung jaringan. *Username* dan *password* yang digunakan untuk login adalah *user* dan *password* yang digunakan untuk *login* pada aplikasi bits mahasiswa.



5

Gambar 6. Arsitektur pengambilan data pengguna



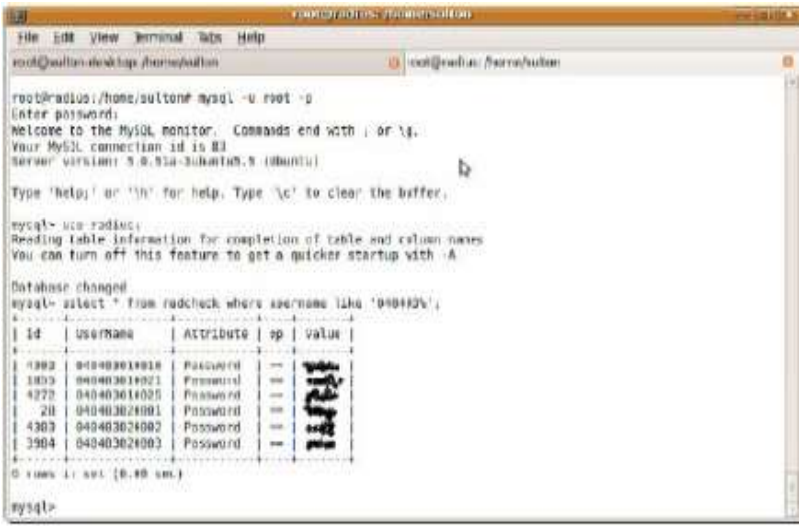
Gambar 7. Arsitektur Sistem Otentikasi

PENGUJIAN PENELITIAN

Pengujian Hasil Tool Importer Pengguna

Tabel 2. Pengujian hasil importer

Test ID		**TR – TS04**	
Tujuan Test		**Mengetahui hasil tool importer**	
Kondisi Awal		**Data belum ter import**	
Prosedur pengujian	**Hasuil yang diharapkan**	**Hasil yang diperoleh**	**Kesimpulan**
	Data berhasil di import		
• Masuk ke server Radius • Gunakan mysql client, ketik mysql -u user -p • Masukkan quary untuk mengecek data sudah masuk atau belum • Query: Select * from radchehk where usename like *040403%	Pada database radius table redcheck berisi data pengguna yang diambil menggunakan importer	Data masuk ke database Radius table radcheck	Tool importer berjalan sesuai dengan rancangan



Gambar 8. RedCheck

Pengujian Pengguna

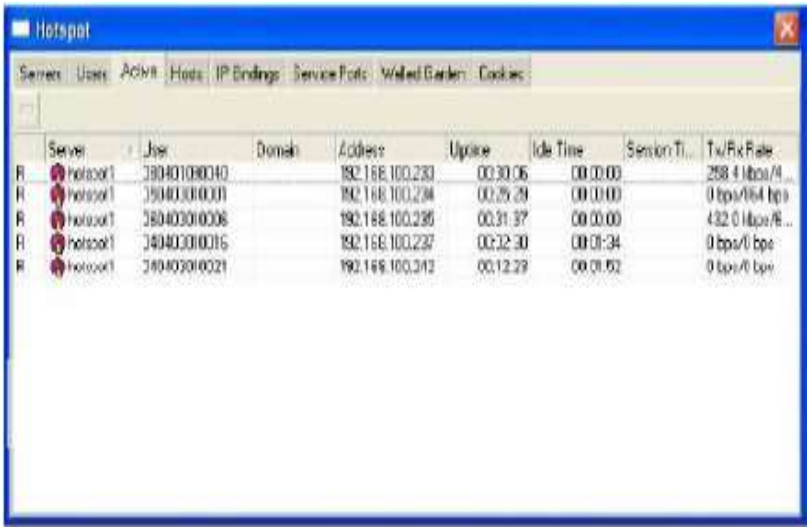
Tabel 3. Pengujian Pengguna

Test ID		**TR – TS05**	
Tujuan Test		**Mengetahui apakah pengguna dapat terhubung Dengan system radius**	
Kondisi Awal		**Pengguna radius kosong**	
Prosedur pengujian	**Hasuil yang diharapkan**	**Hasil yang diperoleh**	**Kesimpulan**
	User radius kosong		
• Masuk ke server Radius • Menggunakan tool radiest • Langkah: radiest pengguna password ipport password • Radiest 04043010016 sult 127.0.0.1.1812 testing123	Rad_recv menampilkan pesan Acess-Accept	Rad_recv menampilkan pesan Acess-Accept	Pengguna sudah dapat terbhubung dengan Radius server
	User tidak bisa terhubung		
• Masuk ke server Radius • Menggunakan tool radiest • Langkah: radiest pengguna password ipport password • Radiest 04043010016 sult 127.0.0.1.1812 testing123	Rad_recv menampilkan pesan Acess-Reject	Rad_recv menampilkan pesan Acess-Reject	Pengguna sudah dapat terbhubung ke radius server karena password yang dimasukkan salah.

Pengujian Mikrotik Hotspot User

Tabel 4. Pengujian Mikrotik hotspot user

Test ID		**TR – TS03**	
Tujuan Test		**Mengetahui fungsi user pada Mikrotik NAS**	
Kondisi Awal		**User tidak ada**	
Prosedur pengujian	**Hasuil yang diharapkan**	**Hasil yang diperoleh**	**Kesimpulan**
	User disable pada Mikrotik		
• Login ke Mikrotik dengan winbox • Masuk menu ip hotspot user • Disable semua user yang ada	User cepat melakukan login	User dapat melakukan login	Komunikasi Mikrotik NAS berjalan dengan normal
	User Aktif pada Mikrotik NAS		
• Login ke Mikrotik dengan winbox • Masuk menu ip hotspot user • Perhatikan user yang ada	List pengguna muncul pada tab active	List pengguna muncul pada tab active	Komunikasi NAS berjalan normal sehingga pengguna dari radius server muncul pada *list active*

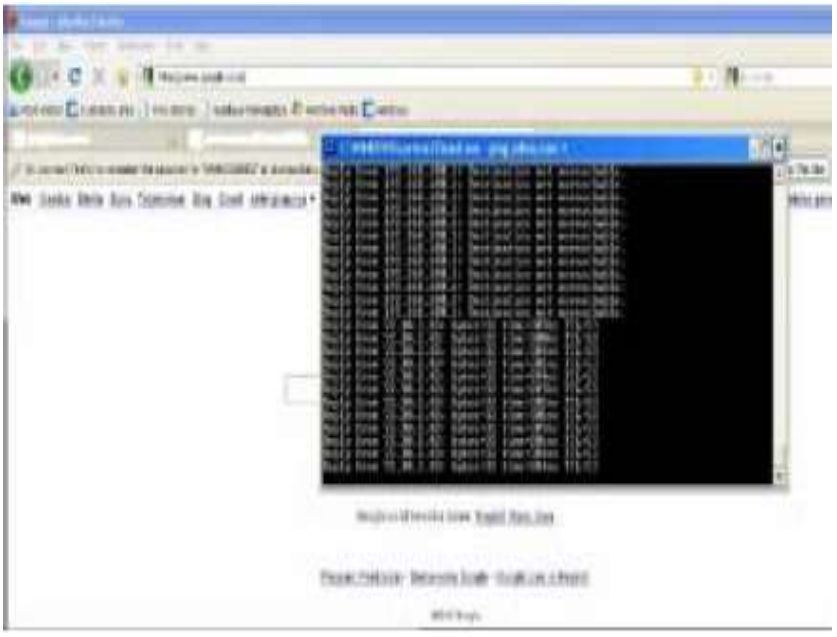


Gambar 9. User aktif pengguna jaringan

Pengujian Interface Login

Tabel 5. Pengujian interface login

Test ID		**TR – TS02**	
Tujuan Test		**Menguji login hotspot**	
Kondisi Awal		**Membuka web brower**	
Prosedur pengujian	**Hasuil yang diharapkan**	**Hasil yang diperoleh**	**Kesimpulan**
	Login Sukses		
• Buka browser • Masukkan alamat web • Misal: google.co.id • Akan dipaksa masuk ke login hotspot	Sebelum sukses login akan di redirect ke halaman login	Client di redirect ke halaman login	Client belum melakukan login
• Buka browser • Masukkan alamat web • Misal: google.co.id • Akan dipaksa masuk ke login hotspot • Masukkan usename dan password • User: 040403020002 password: arif • Login sukses	Clien berhasil login dan masuk ke halaman login	Client di redirect ke halaman login	Client belum melakukan login
	Login Gagal		
• Buka browser • Masukkan alamat web • Misal: google.co.id • Akan dipaksa masuk ke login hotspot • Masukkan usename dan password • User: 040403017 password: sult	Mendapat pesan username atau password salah, pastikan anda sudah registrasi di bau atau hubungi staf sim Univ. Kanjuruan Malang	Client gagal masuk ke halaman google.co.id	Ada kesalahan pada imput username atau password
• Pergunakan 2 komputer • Login dengan user yang sama	Mendapatkan pesan bahwa user sedang aktif	Mendapat pesan bahwa pengguna sedang aktif	Login ganda tidak diijinkan



Gambar 10. Uji coba Login Sukses

KESIMPULAN

Berdasarkan pengujian dan implementasi sistem yang telah dilakukan, dapat disimpulkan bahwa dengan menggunakan RADIUS dengan *software* free RADIUS yang dihubungkan dengan Mikrotik sebagai *network access server* dapat digunakan untuk otentikasi pengguna pada jaringan Universitas Kanjuruhan Malang. Dengan adanya otentikasi user ini diharapkan dapat meningkatkan keamanan jaringan komputer.

DAFTAR PUSTAKA

1. Arifin, Zaenal. 2008. *Sistem Pengamanan Jaringan Wireless LAN Berbasis Protokol 8.02.1x dan Sertfikat*. Penerbit Andi. Yogyakarta.
2. Febyatmoko, dkk. 2006. *Otentikasi, Otorisasi & Pelaporan Koneksi User Wireless Chillispot dan Server RADIUS*. http://journal.uii.ac.id/index.php/mediainformat ika/ article/viewFile/122/83 (akses 20 januari 2010).
3. Kelompok 123P IKI-83408T MTI UI. 2005. *Keamanan Jaringan Komputer*. http://bebas.vlsm.org/v06/Kuliah/MTIKeamananSistem-Informasi/2005/123/123P-03-final1.0-network_security.pdf (akses 20 januari 2010).
4. Linto, Herlambang Moch., dan Catur L. Azis. 2008. *Panduan Lengkap Menguasai Router Masa Depan Menggunakan Mikrotik RouterOSTM*. Penerbit Andi. Yogyakarta.
5. Rigney, et al. 2000. *Remote Authentication Dial In User Service (RADIUS)*. http://www.ietf.org/rfc/rfc2865.txt (akses 19 januari 2010).
6. Wagito. 2007. *Jaringan Komputer Teori dan Implementasi Berbasis Linux*. Gava Media. Yogyakarta.