Rancang Bangun Sistem Pengelolaan Akses User Berbasis Web Menggunakan *FreeRADIUS* (Studi Kasus SMK NU Kaplongan)

Sulhan Qidri[1)],Marsani Asfi*[2)],Ridho Taufiq S.[3)],Muhammad Hatta[4)]
[1)3)] Prog. Studi Teknik Informatika, Fak. Teknologi Informasi, Universitas Catur Insan Cendekia
[2)4)] Prog. Studi Sistem Informasi, Fak. Teknologi Informasi, Universitas Catur Insan Cendekia
Jalan Kesambi No. 202, Kota Cirebon-Propinsi Jawa Barat
[1)] sulhanqidri@gmail.com
[2*)] marsani.asfi@cic.ac.id
[3)] ridho.taufiq@gmail.com
[4)] muhammad.hatta@cic.ac.id

Abstrak

Aplikasi pengelolaan user untuk autentikasi hak akses jaringan di SMK NU Kaplongan masih menggunakan sistem dari router mikrotik. Pengguna baru yang akan menggunakan akses internet harus didaftarkan oleh administrator. Oleh karena itu diperlukan suatu sistem yang dapat membantu dalam pengelolaan akses user sehingga tidak lagi pengelolaan akses user melalui router.Penelitian ini bertujuan mengimplementasikan sistem autentifikasi dan otorisasi untuk proses login ketika akan menggunakan internet. Implementasi system dibuat dalam aplikasi web berbasis PHP dengan mengoptimalkan penggunaan dari freeRadius. Metodelogi yang digunakan adalah menganalisa kebutuhan system, desain dan perancangan system serta implementasi dan pengujian sistem.Sistem yang dibuat terdiri dari tahapan mengkonfigurasi FreeRADIUS dan web server sehingga dapat berkomunikasi dengan radius server. Selanjutnya adalah mengembangkan dan mengimplementasikan aplikasi pengelolaan pengguna berbasis web dengan bahasa pemrograman PHP dan basis data MySQL. Sistem selanjutnya diuji sistem otorisasi dan autentifikasi pengguna. Hasil dari penelitian menunjukkan bahwa aplikasi web berbasis PHP yang dibuat dapat diintegrasikan pengelolaannya dengan membangun sistem autentifikasi dan otorisasi dengan FreeRADIUS.

Kata kunci: autentifikasi, *freeRadius*, pengelolaan user, jaringan, *router*.

Abstract

Authenticating network process access rights at SMK NU Kaplongan still uses the system from the Mikrotik router. Users who will use internet access must be registered by the administrator. So, we need a system that can be assist in managing user access without mikrotik router. This study aims to implement an authentication and authorization system for the login process when using the internet. The system implementation is made in a PHP-based web application by optimizing the use of freeRadius. The methodology used is analyzing system requirements, system design and design as well as system implementation and testing. The system created consists of configuring FreeRADIUS and the web server so that it can communicate with a radius server. Next is to develop and implement a web-based user management application with the PHP programming language and MySQL database. The system is then tested for user authorization and authentication systems. The results of the study indicate that the PHP-based web application that is created can be integrated in its management by building an authentication and authorization system with FreeRADIUS.

Keywords: *authentication, freeradius, management of users, networks, routers*

1. PENDAHULUAN

Autentikasi hak akses pada jaringan komputer sangatlah rentan terhadap penyadapan (*Sniffing*). *Sniffing* merupakan proses penyadapan data pada suatu jaringan komputer [1]. Proses sniffing yang sering kali terjadi adalah *sniffing* pada jaringan untuk mencari *user autentikasi* hak akses jaringan pada

DOI: 10.34128/jsi.v6i2.243 *Received: October 5th, 2020*
Accepted: November 20th, 2020

mikrotik. Berdasarkan hasil observasi, objek studi kasus penelitian dilaksanakan di SMK NU Kaplongan Indramayu diperoleh informasi bahwa selama ini pengelolaan *user* untuk hak akses jaringan masih menggunakan bawaan dari *router* mikrotik. Bagi pengguna baru yang akan mengakses internet harus terdaftar pada sistem yang didaftarkan oleh administrator. Administrator juga harus mendaftarkan *user* di *router* yang ada di *router* mikrotik. Administrator juga akan membedakan antara pengguna siswa, guru dan staff. Pada tahun ajaran baru banyak siswa baru yang belum terdaftar pada sistem *autentikasi* hak akses jaringan. Administrator akan *mengimport* data siswa baru agar terdaftar pada sistem autentikasi hak akses jaringan sehingga user dapat menikmati layanan internet yang ditetapkan oleh sekolah untuk mencari materi, tugas dan sebagainya. Proses menonaktifkan *user autentikasi* untuk hak akses jaringan juga masih manual untuk *user* siswa, guru ataupun staff yang keluar atau tidak diizinkan untuk menggunakan internet. *User autentikasi* hak akses jaringan secara *default* tidak menggunakan enkripsi apapun untuk pengamanan *user autentikasi* akses jaringan. Administrator dapat mengetahui *user* dan *password* semua user yang terdaftar pada sistem.

Penelitian ini sendiri akan membuat sebuah antar muka sistem berbasis web yang dapat digunakan untuk mengatur pengelolaan *user autentikasi* akses jaringan. Antarmuka sistem menerapkan algoritma enkripsi pada *password user autentikasi* hak akses jaringan menggunakan MD5. Aplikasi yang dibuat juga mencakup pembuatan *profile* hak akses jaringan yang dapat membedakan apakah pengguna tersebut berstatus siswa, guru ataupun staff dan juga pembeda pembagian *bandwidth* yang akan diberikan. Untuk pengelompokan *user autentikasi* hak akses jaringan berdasarkan status juga disertakan dalam aplikasi karena sistem *router* tidak ada pengelompokan *user*. Pembuatan sistem pengelolaan user tersebut menggabungkan *freeRadius* dengan pemrograman berbasis web melalui PHP dan mysql.

2. TINJAUAN PUSTAKA

2.1 Penelitian Sebelumnya

Beberapa penelitian sebelumnya, bagaimana sistem kerja server radius yang berfokus pada tiga aspek dalam mengontrol akses user, yaitu autentikasi, autorisasi dan pencatatan[2]. Begitu juga penelitian yang mengembangkan jaringan wireless untuk area hotspot menggunakan *Remote Access Dial In User Service*(RADIUS). RADIUS digunakan untuk user authentication yang aman serta user-friendly untuk membedakan user yang diizinkan dan tidak diizinkan. Metode yang digunakan adalah *Network Development Life Cycle* (NDLC). Hasil pengujian menunjukkan bahwa *user authentication* berbasis RADIUS menggunakan perangkat smartphone dan notebook cukup aman dan *user-friendly*[3]. Sistem autentikasi username dan password dari FreeRadius dengan menggunakan security WPA2-EAP dengan algoritma enkripsi sering juga digunakan. Algoritma yang digunakan yaitu AES dan TKIP sebagai protokol dalam authentication, authorization, dan accounting. Access point dihubungkan dengan FreeRadius yang diinstall pada linux Ubuntu 14.04 server. Hasil penelitian menunjukkan algoritma AES dan TKIP (RC4) mengenkripsi password AES terlihat lebih lama sekitar 2,7 sampai 4,1 ms sedangkan RC4 1,8 sampai 2,7 ms [4]. Implementasi lebih lanjut dilakukan dengan sistem otentikasi hotspot yang diintegrasikan dengan database akademik. Selanjutnya dilakukan pengujian sisi koneksi pengguna, pengaturan Bandwidth dan pemantauan serta menguji pengaturan profil jaringan komputer[2]. Penelitian lainnya menggunakan metode FreeRADIUS, MySQL dan EAP-TLS untuk menyelesaikan kelemahan sistem Wireless LAN. Protokol otentikasi username dan password menggunakan sertifikat CA sebagai kunci keamanan. Hasil penelitian didapatkan bahwa pengunaan FreeRADIUS, MySQL dan EAP-TLS memberikan keamanan yang baik untuk client melalui proses otentikasi, otorisasi dan pendaftaran *account* [5].

2.2 FreeRadius

FreeRADIUS adalah RADIUS server yang *Open Source*. *FreeRADIUS* mendukung dengan semua protokol autentikasi dan dilengkapi web administrasi pengguna berbasis PHP yang disebut *dialupadmin*. *FreeRADIUS* dikembangkan oleh Alan Dekok dan Miquel Smoorenburg pada Agustus 1999. Sebelum mengembangkan *FreeRADIUS*, Miquel mengembangkan *Cistron* RADIUS server, namun tidak dikembangkan lagi. Seiring perkembangan waktu *FreeRADIUS*

terus dikembangkan dan suport dengan banyak fitur selain support teks file juga support *LDAP, MySQL, PostgreSQL*, Oracle dan banyak fitur lainnya [6].

Area yang memiliki akses internet atau lebih dikenal dengan hotspot yang saat ini sudah menjadi standar akses internet perangkat-perangkat jaringan. Terutama untuk hotspot jaringan nirkabel (Wi-Fi) sebagai standar sinyal. Namun masalah pada hotspot adalah ketepatan dan keamanan penerapan metode autentifikasi terhadap akses hotspot.

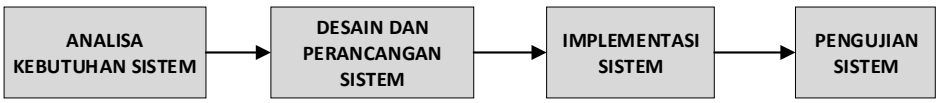
FreeRadius merupakan server Remote Authentication *Dial-In User Service* (RADIUS) yang menggunakan metode portal captative untuk mendapatkan akses hotspot. Metode ini membutuhkan username dan password atau biasa disebut login, freeradius menggunakan protokol AAA (*Authentication, Authorization, Accounting*) melalui data yang tersimpan di dalam database MySql [7].

2.3. Enkripsi MD5

MD5 merupakan fungsi hash kriptografik. MD5 menggunakan hash value 128-bit. Dalam standart Internet, MD5 digunakan pada aplikasi keamanan, dan MD5 juga dapat digunakan untuk melakukan pengujian terhadap integritas suatu berkas yang berisi data [8]. Masalah keamanan dalam basis data merupakan salah satu tantangan dalam penelitian basis data. Data yang ada dalam basis data harus terjamin dari sisi keamanan. Pengamanan data dapat dilakukan melalui pengaturan hak akses setiap pengguna atau pengamanan data dari sisi kandungan data yang tersimpan pada basis data. Pengamanan data dari sisi kandungan data dilakukan dengan menggunakan teknik kriptografi MD5. MD5 diharapkan dapat mengamankan data tanpa perlu mengetahui query–query yang perlu diketikkan atau dijalankan. Keamanan dari enkripsi konvensional bergantung pada beberapa faktor [9].

3. METODE PENELITIAN

3.1 Tahapan Penelitian



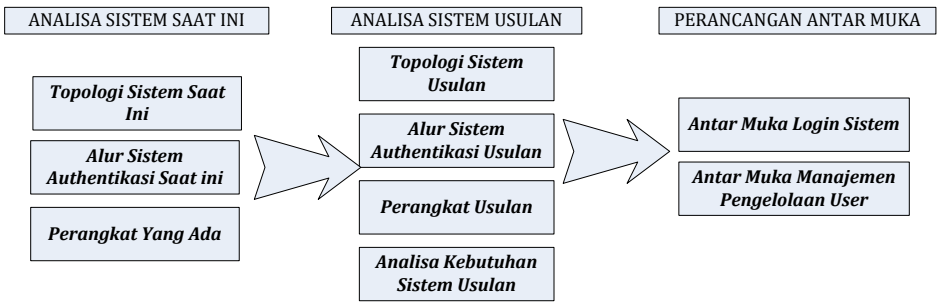
Gambar 1. Metode Penelitian

Dalam penelitian ini metode penelitian yang digunakan mengadopsi dari metode waterfall. Gambar 1 merupakan metode penelitian yang digunakan dengan adaptasi dari metode waterfall. Adapun 3(tiga) tahapan penelitian pada Gambar 1, terdiri dari :

1. Analisa kebutuhan sistem
2. Desain dan perancangan sistem
3. Implementasi sistem
4. Pengujian sistem

3.2 Analisa dan Perancangan Sistem

Penelitian ini mencoba mengimplementasikan tahapan analisa dan perancangan sistem seperti pada Gambar 2.



Gambar 2. Tahapan Analisa dan Perancangan Sistem

Tahapan analisa dan perancangan sistem pada gambar 2, dijelaskan sebagai berikut :

3.2.1 Analisa Sistem Saat Ini

Pada tahapan ini dilakukan analisa untuk topologi sistem yang saat ini digunakan. Tahapan analisa ini berguna untuk mendapatkan alur penggunaan internet yang digunakan di SMK NU Kaplongan. Analisa juga dilakukan untuk mendapatkan alur sistem autentikasi yang berjalan saat ini. Sedangkan informasi perangkat yang digunakan saat ini dijadikan dasar untuk pengimplementasian sistem ketika digunakan dan diujikan. Hasil analisa sistem saat ini diperoleh informasi sebagai berikut:

1. Pada jaringan SMK NU Kaplongan ada jaringan yang diwajibkan menggunakan user authentikasi dan
2. Terdapat jaringan khusus tanpa menggunakan authentikasi yaitu jalur lab komputer.
3. Diperoleh alur sistem akses jaringan dari mulai pertama kali mengakses jaringan sampai pengguna dapat menikmati layanan internet.

3.2.2 Analisa Sistem Usulan

Pada tahapan analisa sistem usulan, berdasarkan analisa sistem saat ini dilakukan hal-hal berikut:

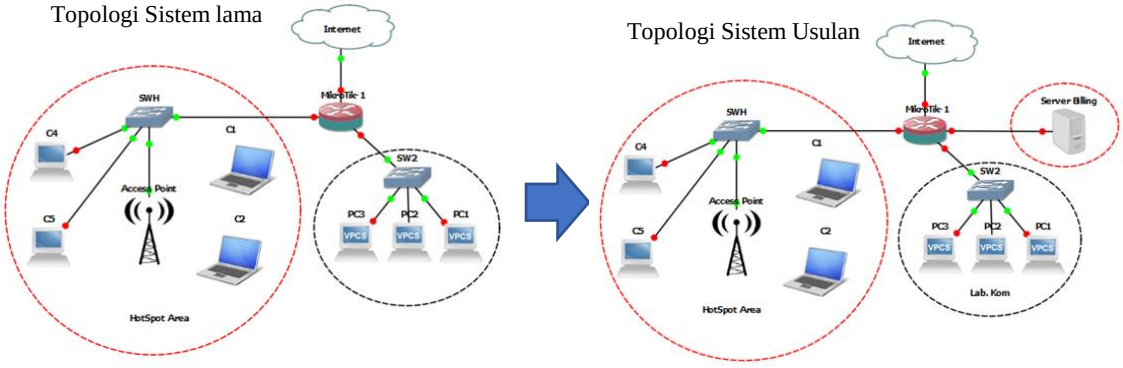
1. Topologi jaringan komputer di SMK NU Kaplongan terbagi menjadi beberapa bagian yaitu jalur khusus server, jalur untuk Laboratorium Komputer dan jalur akses jaringan.
2. Pada penelitian ini hanya dibahas jalur akses jaringan khususunya jalur server saja.
3. Hasil analisa usulan diperlukan tambahan alat yang digunakan yaitu server, server yang akan digunakan untuk mengalihkan proses autentikasi halaman login yakni dari mikrotik ke server dan penyimpanan user akses jaringan.
4. Sistem akses jaringan usulan ketika mengakses jaringan sampai pengguna dapat menikmati layanan internet.

Untuk analisa kebutuhan user, dilakukan konfigurasi untuk 4 file utama dari freeradius, yaitu radiusd.conf, site-enable/default.conf, clients.conf serta sql.conf. File-file tersebut merupakan file konfigurasi utama dari freeRadius. File-file tersebut merupakan modul yang digunakan untuk menjalankan freeRadius. File sql.conf merupakan file konfigurasi yang terkait antara server FreeRadius dapat terkoneksi dengan database MySQL. Konfigurasi pada file berupa pemberian nilai alamat host, username, passowordd an nama databaseyang digunakan oleh database server FreeRadius. File *site-enable/default.conf* merupakan file konfigurasi dari virtual hostserver FreeRadius.

4. PEMBAHASAN

Proses awal dilakukan konfigurasi FreeRADIUS Server serta router mikrotik. Pengujian kinerja dari FreeRADIUS Server dan router mikrotik dilakukan dengan login dan akses internet. Pengujian otentikasi pengguna jaringan hotspot adalah melalui aplikasi yang dikembangkan. Pengujian dilakukan berdasarkan user akses yang telah dibuat pada konfigurasi hotspot.

4.1 Topologi Sistem Usulan



Gambar 4. Topologi Sistem Usulan

Topologi jaringan saat ini terlihat pada Gambar 4 diwajibkan menggunakan user authentikasi dan ada juga jaringan khusus tanpa menggunakan authentikasi yaitu jalur laborarium komputer. Penambahan alat

p-ISSN: 2460-173X
e-ISSN: 2598-5841

yang diusulkan untuk topologi sistem terlihat pada Gambar 4 yaitu server. Server yang diajukan akan digunakan untuk mengalihkan halaman login dari mikrotik ke server dan penyimpanan user akses jaringan. Fokus jaringan tertentunya yaitu akses jaringan dan server yang terlingkar warna merah.

4.2 Konfigurasi Sistem FreeRadius

Konfigurasi koneksi antara FreeRadius dan MySQL dengan mengubah file di "nano /etc/freeradius/mods-enabled/sql". Berikut adalah konfigurasi yang digunakan :

```
sql {
       driver = "rlm_sql_mysql"
       mysql {
            warnings = auto }
 # Connection info:
 server = "localhost"
 port = 3306
 login = "root"
 password = "ucic"
 radius_db = "radius"
```

Kemudian *user* FreeRadius ke database dengan perintah :

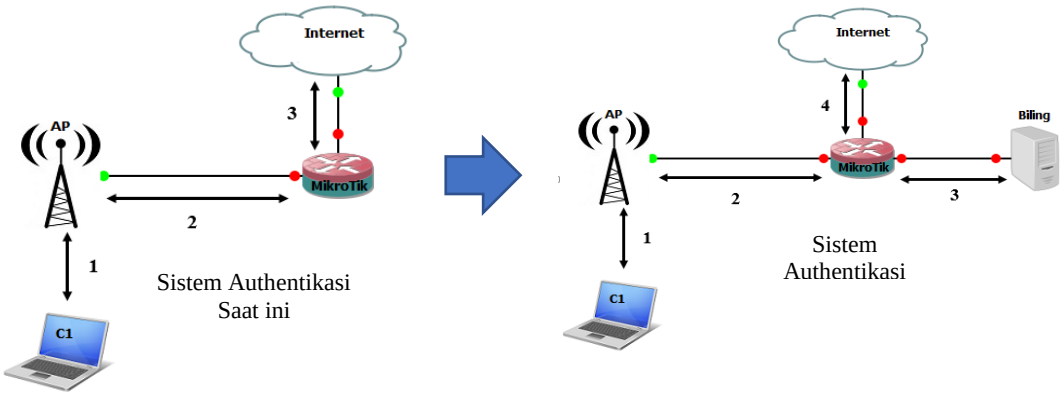
```
mysql -uroot -pucic
use radius;
INSERT INTO radcheck ( id , UserName , Attribute , op , Value )
      VALUES ( NULL , 'sulhan', 'Cleartext-Password', ':=', 'sulhan');
INSERT INTO radreply (username, attribute, op, value)
      VALUES ('sulhan', 'Mikrotik-Rate-Limit', '==', '1024k/1024k');
INSERT INTO radcheck ( id , UserName , Attribute , op , Value )
  VALUES (NULL , 'sulhan', 'Expiration', ':=', '13 Jan 2029 11:00');
INSERT INTO radcheck (username,attribute,op,value)
   VALUES ('sulhan', 'Simultaneous-Use', ':=', '1');
exit
```

Tahap selanjutnya adalah menghentikan service dan melakukan *debugging* dengan perintah "service freeradius stop" dan "*freeradius* -X".

```
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel
Listening on proxy address * port 32772
Listening on proxy address :: port 37562
Ready to process requests
```

Gambar 5. Proses Menghentikan *Service Dan Debugging*

4.3 Alur Sistem Authentikasi Usulan



Gambar 6. Alur Sistem Authentifikasi Usulan

Alur authentifikasi saat ini pada Gambar 6, prosesnya terdiri dari :

1. *Request: Client* mengubungkan media *wireless* laprop/komputer ke aksespoin jika menggunakan media kabel laptop/komputer harus terhubung dengan dengan *switch* yang terhubung dengan kabel. *Reply:* Jika sudah terhubung maka status network adapter aktif.
2. *Request: Client* yg sudah terhubung dengan jaringan tersebut meminta *IP Address* dan *DNS,* kemudian *client* akan diminta untuk memasukan *username* dan *password* pada halaman web. *Reply:* Maka *MikroTik* akan memberikan *IP Address* dan *DNS* kepada *client,* kemudain *MikroTik* juga akan mengalihkan ke halaman *login*, jika *username* dan *password* yang dimasukan pada *client* tidak valid maka akan muncul pesan *username* atau *password* salah jika benar maka akan melanjutkan ke halaman berikutnya.
3. *Request: Client* akan memasukan kata kunci atau URL untuk mengakses internet. *Reply:* Jika *client* sudah melakukan autentikasi dan data yang dimasukan client itu benar maka proses akan dilanjutkan ke *internet*.

Alur sistem authentifikasi yang diusulkan seperti pada Gambar 5 prosesnya sebagai berikut :

1. *Request: Client* mengubungkan media *wireless* laprop/komputer ke aksespoin jika menggunakan media kabel laptop/komputer harus terhubung dengan dengan *switch* yang terhubung dengan kabel. *Reply:* Jika sudah terhubgung maka status network adapter aktif.
2. *Request: Client* yg sudah terhubung dengan jaringan tersebut meminta *IP Address* dan *DNS,* kemudian *client* akan diminta untuk memasukan *username* dan *password* pada halaman web. *Reply:* Maka *MikroTik* akan memberikan *IP Address* dan *DNS* kepada *client,* kemudain *MikroTik* juga akan mengalihkan ke halaman *login*.
3. *Request: MikroTik* akan melanjutkan pengiriman paket data yang telah dikirim dari *client* ke server. *Reply*: Server akan menerima dan melakukan autentikasi apakah *username* dan *password* itu valid apa tidak jika *username* dan *password* yg dimasukan pada *client* tidak valid maka akan *server* akan mengirim data paket ke *MikroTik* dan mikrotik akan melanjutkan pengiriman pesan ke *client* bahwa *username* atau *password* salah jika benar maka akan melanjutkan ke halaman berikutnya.
4. *Request: Client* akan memasukan kata kunci atau URL untuk mengakses internet. *Reply:* Jika *client* sudah melakukan autentikasi dan data yang dimasukan client itu benar maka proses akan dilanjutkan ke *internet*.

4.4 Perangkat Usulan

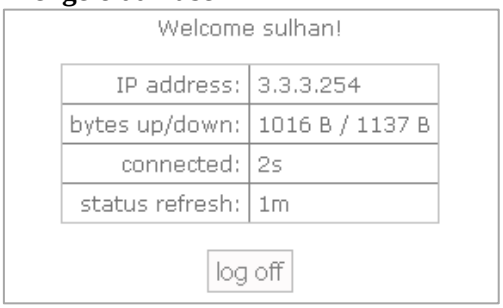
Tabel.1. Perangkat usulan

No.	Nama Alat	Jumlah	Ket.
1	Mikrotik Routerboard	1	
2	Antena sectoral	4	
3	Access Point	10	
4	Antena Omni	2	
5	Switch	8	
6	Server	1	Usulan
Jumlah		26	

Perangkat yang telah ada seperti pada Tabel 1, kemudian di analisa kegunaannya dan menghasilkan penambahan perangkat usulan baru, yaitu 1 buah server.

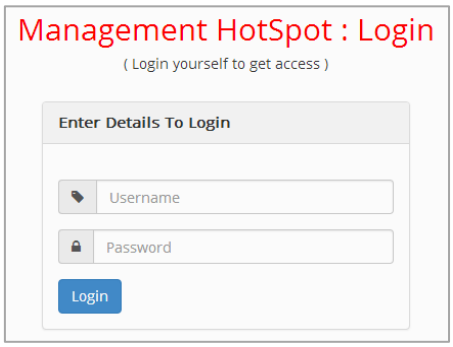
p-ISSN: 2460-173X
e-ISSN: 2598-5841

4.5 Antar Muka Sistem Pengelolaan user



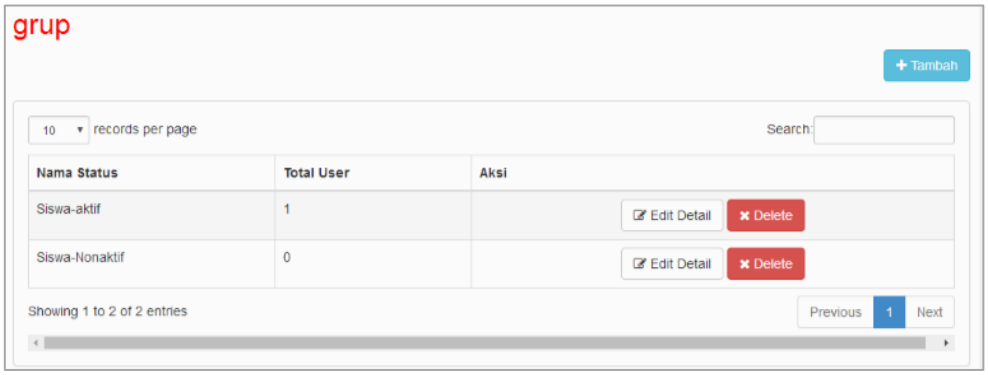
Gambar 7. *Form Status*

Salah satu form seperti pada Gambar 7 merupakan form status untuk menampilkan IP *client* yang digunakan, berapa pemakaian data yang digunakan, berapa lama koneksi ke jaringan dan status refresh



Gambar 8 *Login* ke Sistem

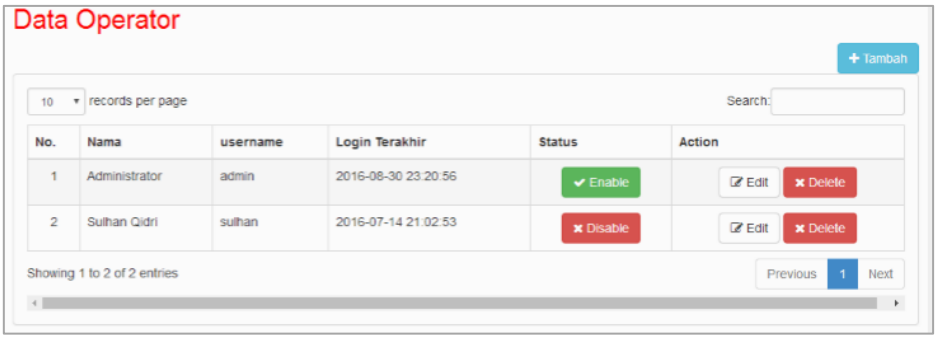
Gambar 8 adalah form login ke sistem utama sedangkan form halaman kelola grup terlihat seperti pada Gambar 9. Form ini digunakan untuk mengelola grup akses jaringan. Pada form ini terdapat tombol tombol tambah grup, tombol edit detail grup untuk mengedit detail grup, dan tombol *delete* akan menghapus data.



Gambar 9. *Form* Halaman Kelola Grup

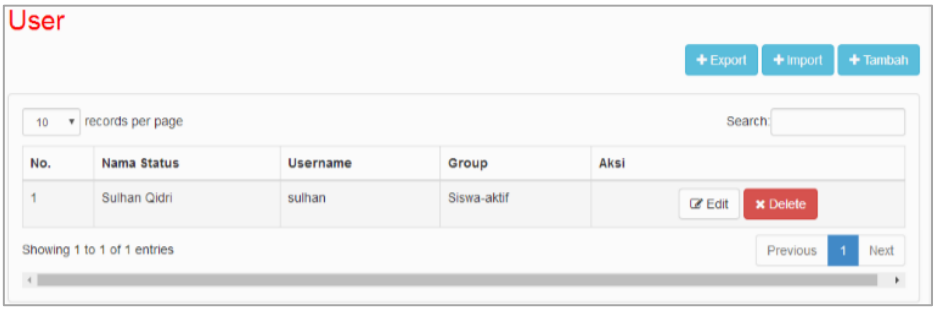
Halaman data operator ditunjukkan seperti pada Gambar 10. Beberapa tombol antara lain tombol tambah untuk menambah operator, tombol *enable/disable* untuk mengaktifkan oeprator dan akan berubah jika awalnya enable maka akan berubah *disable* ataupun sebaliknya, serta menekan tombol *edit* akan mengedit operator. Tombol *delete* akan menghapus data operator.

p-ISSN: 2460-173X
e-ISSN: 2598-5841



Gambar 10. *Form* Data Operator

Halaman user terlihat seperti pada Gambar 11. Pada form ini terlihat beberapa tombol antara lain tombol tambah, *export*, *import*, *edit* dan *delete* user. Jika menekan tombol tambah maka akan masuk ke halaman tambah user, jika menekan tombol *import* maka akan masuk kehalaman *import* data user, jika menekan tombol *export* maka akan men-*download* semua data user akses jaringan. Jika menekan tombol edit maka akan masuk ke halaman *edit* user. Jika menekan tombol *delete* maka akan ada pertanyaan apakah data tersebut akan dihapus jika *yes* data tersebut akan dihapus jika tidak tidak akan terjadi apa-apa.



Gambar 11. *Form* Halaman User

Hasil pengujian menunjukkan bahwa Sistem otentikasi user pengguna hotspot yang dibuat ini dapat membatasi jumlah pengguna dan meningkatkan keamanan dalam hal otentikasi. Tersentralisasinya data dan otorisasiaccount dengan penerapan username dan password untuk tiap user/pengguna.

4.6 Pengujian Sistem

4.6.1 Pengujian terhadap penggunaan freeRadius

Pengujian FreeRadius dilakukan dengan perintah "radtest sulhan sulhan localhost 1812 testing123"

```
root@SRVUCIC:~# radtest sulhan sulhan localhost 1812 testing123
Sent Access-Request Id 137 from 0.0.0.0:58165 to 127.0.0.1:1812 length 76
        User-Name = "sulhan"
        User-Password = "sulhan"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 1812
        Message-Authenticator = 0x00
        Cleartext-Password = "sulhan"
Received Access-Accept Id 137 from 127.0.0.1:1812 to 0.0.0.0:0 length 26
        Session-Timeout = 258549532
```

Gambar 12. Pengujian *freeradius*

Jika proses diatas ada keterangan "Access-Accept" berarti user yang ada di database sudah bisa digunakan. Lanjut ke pengujian menggunakan web dari Autentikasi MikroTik.

Buat koneksi Radius Server ke Radius client, kemudian tambahkan di file "nano /etc/freeradius/3.0/ clients.conf" script ini di bagian paling bawah.

p-ISSN: 2460-173X
e-ISSN: 2598-5841

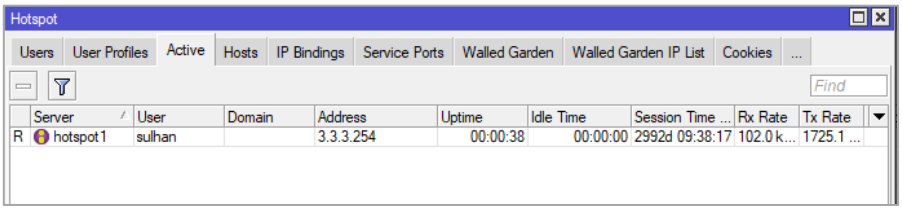
```
  GNU nano 2.2.6       File: /etc/freeradius/3.0/clients.conf

#  will then accept ONLY the clients listed in this section.
#
#clients per_socket_clients {
#       client socket_client {
#               ipaddr = 192.0.2.4
#               secret = testing123
#       }
#}
client mikrotik {
        ipaddr = 2.2.2.1
        secret = ucic
}
```

Gambar 13. Setting Konfigurasi *Freeradius*

4.6.2 Pengujian terhadap proses login ke sistem

Pengujian dilakukan dengan mengecek konfigurasi serta koneksi antara server dengan client apakah dapat berjalan dengan baik. Halaman login dan password pada form login akan ditampilkan terlebih dahulu. Selanjutnya client yang berhasil masuk dapat membuka sebuah situs yang artinya konfigurasi server telah berhasil. Pengujian pada client dilakukan dengan melihat aktifitas koneksi. Jika koneksi sudah tersambung maka saat mengakses internet pada browser akan diarahkan pada halaman login untuk memasukkan user dan password. Gambar 14, merupakan hasil pengujian terhadap akses user.



Gambar 14. *Status* Akses *User*

Pada bagian paling kiri ada tulisan “R” menandakan bahwa user tersebut dari Radius Server, jika tidak ada tulisan “R” berarti dari user local.

Selanjutnya adalah pengujian terhadap aplikasi sistem untuk proses login yang dilakukan dengan metode *blackbox.*

Tabel 1. Pengujian Halaman Login

No.	Jenis	Pengujian	Hasil yang diharapkan	Output	Hasil Uji
1	Login	Username = “admin” Password = “admin”	Halaman status	Halaman status	Berhasil
2	Login	Username=“admin” Password = “adminn”	Pesan kesalahan	Pesan kesalahan	Berhasil
3	Login	username = “” password = “”	Pesan kesalahan	Pesan kesalahan	Berhasil

Tabel 3. Pengujian pada masing-masing menu administrator

No.	Jenis	Pengujian	Hasil yang diharapkan	Output	Hasil Uji
1	Tambah	Pilih Tambah	Halaman Tambah User	Halaman Tambah User	Berhasil
2	Import	Pilih Import	Halaman import	Halaman import	Berhasil
3	Export	Pilih Export	Download file user	Download file user	Berhasil
4	Edit	Pilih Edit	Halaman edit user	Halaman edit user	Berhasil
5	Delete	Pilih Delete	Data akan terhapus	Data akan terhapus	Berhasil

Tabel 2, dan Tabel 3 merupakan beberapa hasil pengujian untuk aplikasi sistem yang telah dibuat. Hasil pengujian menunjukkan bahwa sistem yang dibuat dapat diimplementasikan dan dipergunakan di SMK NU Kaplongan.

5. KESIMPULAN

1. Penelitian yang dilakukan dapat digunakan untuk menyelesaikan proses pendaftaran pengguna pada jaringan *hotspot* Mikrotik dan FreeRadius melalui aplikasi berbasis web.
2. Aplikasi web yang dibuat terdapat sistem pengelolaan user sehingga memudahkan administrator dalam memanajemen user, dan memudahkan admin memonitor user yang memakai layanananya, melihat user yang aktif.
3. Aplikasi web yang dibangun terdiri dua bagian aplikasi yaitu aplikasi berbasis web untuk admininstrator dan user pengguna layanan. Sistem dibangun berbasis web menggunakan.

DAFTAR PUSTAKA

[1] "What Is a Sniffing Attack? - DZone Security." https://dzone.com/articles/what-is-a-sniffing-attack (accessed Aug. 30, 2020).
[2] M. Unik, S. Suryanto, and J. Al Amien, "Wireless Network Authentication System Using RADIUS (Remote Authentication Dial In-User Service) Server (Case Study: Universitas Muhamadiyah Riau)," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 4, no. 2, Mar. 2020, doi: 10.30743/INFOTEKJAR.V4I2.2382.
[3] M. Rusdan and M. Sabar, "ISSN : 2460-1861 Pengembangan Jaringan Wireless Menggunakan User Authentication Berbasis Radius Dalam Industri 4 . 0 (Studi Kasus : Universitas Widyatama) ISSN : 2460-1861," *Infotech J.*, vol. 0, no. January, pp. 44–52, Jun. 2019, doi: 10.31949/inf.v5i1.1449.
[4] R. Setiawan, "Penerapan Sistem Autentikasi Pada Jaringan Wireless Dengan Menggunakan Freeradius Dan Security WPA2-EAP," 2016.
[5] A. Gusala, S. Raharjo, and N. Widyastuti, "Implementasi Freeradius Pada Jaringan Hotspot Dengan Menggunakan MYSQL Dan EAP-TLS," *J. Jarkom*, vol. 4, no. 1, pp. 21–30, Jul. 2016, Accessed: Aug. 26, 2020. [Online]. Available: www.freeradius.org.
[6] "FreeRADIUS." https://freeradius.org/ (accessed Aug. 30, 2020).
[7] M. S. Fauzi, "Manajemen User Dan Login Layanan Hotspot Mikrotik Dengan Logger Menggunakan Server Authentication Freeradius Pada Raspberry PI," Mar. 2018. Accessed: Aug. 26, 2020. [Online]. Available:https://ejournal.itn.ac.id/index.php/jati/article/view/1685.
[8] "MD5 Hash Generator." https://www.md5hashgenerator.com/ (accessed Aug. 30, 2020).
[9] A. T. Arsanto, "Implementasi Pengamanan Basis Data Menggunakan Metode Enkripsi MD5 (Message-Digest Algorihm 5)," *Explor. IT! J. Keilmuan dan Apl. Tek. Inform.*, vol. 5, no. 1, Jun. 2013, Accessed: Aug. 30, 2020. [Online]. Available: https://jurnal.yudharta.ac.id/v2/index.php/EXPLORE-IT/article/view/252.