Jurnal Computech & Bisnis, Vol. 12, No.2, Desember 2018, 118-130
ISSN (print): 1978-9629, ISSN (online): 2442-4943

USER AUTHENTICATION JARINGAN NIRKABEL BERBASIS *WEB* MENGGUNAKAN RADIUS DI UNIVERSITAS BALE BANDUNG (UNIBBA)

Muchamad Rusdan[1], Asep Ririh Riswaya[2]
Sekolah Tinggi Teknologi Bandung[1], STMIK Mardira Indonesia[2]
rusdan@sttbandung.ac.id[1], asep_ririh@stmik-mi.ac.id[2]

Abstract

In this study, problems arise due to the use of WPA2-based user authentication. Constraints faced in using WPA2 are difficult to distinguish between users of wireless network services that are permitted and not permitted. The purpose of this study is that each wireless network user at Bale Bandung University (UNIBBA) can be distinguished between users who are permitted and not permitted so that wireless networks become safe, comfortable and user-friendly. UNIBBA is one of the educational institutions in Bandung Regency, which makes wireless networks a standard facility provided to students, lecturers, and employees that can be accessed through mobile devices that support wireless networks. The research method used is the waterfall method. The results of this study created a web-based wireless network user authentication system using RADIUS that is safe and user-friendly, by testing on the RADIUS server side and web login form.

Keywords:*user authentication, RADIUS, waterfall, wireless network*

Abstrak

Pada penelitian ini timbul kendala permasalahan yang dihadapi dikarenakan penggunaan user authentication berbasis WPA2. yang menjadi Kendala yang dihadapi dalam penggunaan WPA2 sulitnya membedakan pengguna layanan jaringan nirkabel yang diijinkan dan tidak diijinkan. Tujuan penelitian ini adalah supaya setiap pengguna jaringan nirkabel di Universitas Bale Bandung (UNIBBA) dapat dibedakan antara pengguna yang diizinkan dan tidak diizinkan supaya jaringan nirkabel menjadi aman, nyaman dan user-friendly. UNIBBA merupakan salah satu institusi pendidikan yang berada di Kabupaten Bandung, yang menjadikan jaringan nirkabel sebagai fasilitas standar yang diberikan kepada mahasiswa, dosen, dan karyawan yang dapat diakses melalui perangkat mobile yang mendukung jaringan nirkabel. Metode penelitian yang digunakan metode waterfall. Hasil penelitian ini terciptanya sistem user authentication jaringan nirkabel berbasis web menggunakan RADIUS yang aman dan user-friendly, dengan melakukan pengujian pada sisi RADIUS server dan web login form.

Kata Kunci : user authentication, RADIUS, waterfall, jaringan nirkabel

PENDAHULUAN

Jaringan nirkabel merupakan teknologi komunikasi data yang saat ini sudah banyak digunakan secara luas diberbagai tempat, tanpa terkecuali pada institusi pendidikan atau kampus (Darmadi, 2018). Jaringan nirkabel menjadi alternatif terbaik dalam membangun jaringan komputer yang fleksibel, praktis, skalabilitas, dan mobilitas tinggi. Sebagian besar kampus menggunakan jaringan nirkabel untuk mendukung jaringan kabel yang sudah ada, yang bertujuan supaya pengguna layanan bisa melakukan akses *internet* dan pencarian informasi. Jaringan nirkabel memberikan fleksibel, praktis, skalabilitas, dan mobilitas tinggi serta nyaman untuk digunakan. Selama berada dalam wilayah area cakupan sinyal jaringan nirkabel, pengguna dapat mengakses *internet*(Tenggario & Lukas, 2011). Untuk membuat jaringan nirkabel terkoneksi ke *internet* dengan aman, nyaman, dan *user-friendly*, maka perlu dibuat sistem *user authentication* yang berbasis *Remote Access Dial In User Service* (RADIUS) *Server* yang dapat digunakan untuk *Authentication, Authorization, dan Accounting* (Sikarwar & Saxena, 2017).

Universitas Bale Bandung (UNIBBA) merupakan salah satu institusi pendidikan yang berada di Kabupaten Bandung, yang menjadikan jaringan nirkabel sebagai salah satu fasilitas standar yang diberikan kepada mahasiswa, dosen, dan karyawan yang dapat diakses melalui *laptop, smartphone, tablet*, dan perangkat *mobile* lainnya yang mendukung jaringan nirkabel. Fasilitas tersebut sangat membantu mahasiswa dan dosen dalam proses perkuliahan dan pencarian referensi untuk kebutuhan perkuliahan, sedangkan karyawan mempergunakannya sebagai media komunikasi dan informasi. Setiap mahasiswa, dosen, dan karyawan dapat menggunakan layanan jaringan nirkabel yang ada dengan cara memasukkan user authentication yang masih berbasis *Wi-Fi Protected Access II* (WPA2) pada perangkat *mobile* yang mereka miliki. Kendala yang dihadapi dalam penggunaan WPA2, sulitnya untuk membedakan pengguna layanan jaringan nirkabel yang diijinkan dan tidak diijinkan. Dengan adanya permasalahan tersebut maka, alternatif solusinya perlu dikembangkan *user authentication* yang aman dan *user-friendly* yang mampu membedakan pengguna yang diijinkan dan tidak diijinkan menggunakan RADIUS berbasis *web* pada jaringan nirkabel UNIBBA.

TINJAUAN PUSTAKA

User Authentication

Authentication merupakan proses pemeriksaan identitas pengguna sistem melalui proses login ke dalam sistem dan pengguna yang lolos pemeriksaan identitas merupakan pengguna yang memiliki otoritas atas sistam (Rahardja, Harahap, & Fresandy, 2017). *User authentication* yaitu, seseorang yang diizinkan mengakses suatu sistem atau sumberdaya (Dano, Wowor, & Lantang, 2015). *User authentication* hanya memberikan keputusan antara diizinkan dan tidak diizinkan.

Jaringan Nirkabel

Jaringan nirkabel mengacu pada penggunaan sinyal gelombang frekuensi radio untuk berbagi informasi dan sumber daya antar perangkat seperti smartphone, notebook, PDA, dan wireless sensor (Jyoti & Saini, 2017). Jaringan nirkabel berkembang pesat, karena kemampuannya melakukan pengiriman data dan komunikasi data (Rohman, 2008).

Standardisasi yang diciptakan untuk jaringan nirkabel berkode IEEE 802.11. Standar diciptakan agar setiap perangkat jaringan nirkabel yang berbeda vendor tetap dapat berkomunikasi. Dengan penggunaan perangkat jaringan nirkabel pengguna dapat terhubung ke jaringan tanpa perlu menggunakan kabel (Julianto,

Migunani, & Efendi, 2013). Standar jaringan nirkabel yang berlaku saat ini dapat dilihat pada tabel 1.

Tabel 1Standar IEEE

Standar	Kecepatan	Frekuensi	Tahun
IEEE 802.11	2 Mbps	2,4 GHz	1997
IEEE 802.11a	54 Mbps	5 GHz	1999
IEEE 802.11b	11 Mbps	2,4 GHz	1999
IEEE 802.11g	54 Mbps	2,4 GHz	2002
IEEE 802.11n	300 Mbps	2,4 GHz	2009
	600 Mbps	5 GHz	
IEEE 802.11ac	450 Mbps	2,4 GHz	2013
	1300 Mbps	5 GHz	

Keamanan Jaringan Nirkabel

Keamanan bertujuan agar terhindar dari penyadapan dan pencurian yang tidak diharapkan. Keamanan menjadi sangat penting untuk tujuan melindungi komunikasi data supaya terjamin kerahasiaanya (*confidentiality*), keutuhannya (*integrity*), dan ketersediaanya (*availability*) (Suprianto & Riswaya, 2018).

Media transportasi jaringan nirkabel memiliki potensi lebih tinggi untuk diserang daripada media kabel sehingga meningkatkan ancaman terhadap jaringan nirkabel. Keamanan jaringan nirkabel sebagai kombinasi dari keamanan saluran nirkabel dan keamanan jaringan. Tantangan jaringan nirkabel seperti gangguan sinyal frekuensi radio, kerahasiaan data, keutuhan data, dan ketersediaan data (Ochang, Irving, & Ofem, 2016).

Protokol Enkripsi Jaringan Nirkabel

Wired Equivalent Privacy (WEP) adalah protokol nirkabel IEEE 802.11, yang menyediakan algoritma keamanan untuk data selama transmisi nirkabel berlangsung. WEP menggunakan Vektor Inisialisasi (IV) 24 bit untuk membentuk *streamchipper* dan CRC -32 *checksum* untuk integritas transmisi nirkabel. WEP 64 bit menggunakan kunci 40 bit, WEP 128 bit menggunakan kunci 104 bit, WEP 256 bit menggunakan ukuran kunci 232 bit (Pavithran, 2015).

WiFi Protected Access (WPA) merupakan metode penyandian data untuk jaringan nirkabel berdasarkan standar 802.11. WPA dikembangkan setelah WEP untuk menyediakan enkripsi yang lebih kuat dengan mengonfigurasi dua cara yang berbeda yaitu, mode *pre-shared key* dan mode *enterprise*. WPA terdiri dari dua pilihan enkripsi yaitu, *Advanced Encryption Standards* (AES) lebih kuat daripada RC4 dan *Temporal Key Integrity Protocol* (TKIP). Ada dua versi mode WPA, mode *personal* yang dimiliki WPA *authentication* PSK dan enkripsi TKIP, WPA *enterprise* memiliki *authentication* EAP dan TKIP enkripsi (Gali & Mustafa, 2015).

Solusi yang disarankan untuk masalah keamanan WEP adalah beralih ke WPA2. WPA adalah solusi perantara untuk perangkat keras yang tidak dapat mendukung WPA2. Baik WPA dan WPA2 jauh lebih aman daripada WEP. Ada dua versi mode WPA2, mode WPA personal memiliki *authentication* PSK dan enkripsi AES/CCMP, mode WPA2 enterprise memiliki *authentication* EAP dan enkripsi AES/CCMP (Dhiman, 2014).

Web

Web atau *World Wide Web* (WWW) adalah sebuah penyebaran informasi melalui *internet*. Web merujuk pada sekumpulan halaman yang memuat informasi teks, gambar, video, animasi, dan suara (Sundari, 2016). Setiap halaman pada *web* membentuk satu rangkaian yang saling berkaitan, berhubungan melalui jaringan-jaringan halaman.

Web merupakan keseluruhan isi halaman *web* yang tersimpan pada sebuah domain yang menyimpan informasi. Domain merujuk pada nama unik yang dimiliki oleh sebuah institusi, perusahaan, atau perorangan yang dapat diakses melalui jaringan internet (Simangunsong, 2018).

Web dapat juga berarti media publikasi elektronik yang terdiri dari kumpulan halaman yang saling terhubung satu dengan yang lain

menggunakan *hyperlink* yang disematkan pada suatu teks atau gambar. Tim Barners Lee pertama kali membuat *web* pada tahun 1990. *Web* menggunakan bahasa Hypertext Markup Language (HTML) dan protokol Hypertext Transfer Protocol (HTTP) (Rosadi, 2016).

RADIUS

Remote Authentication Dial In User Service (RADIUS) dikembangkan untuk melakukan akses ke berbagai macam sumberdaya perangkat dari lokasi lain secara *remote*, serta memberikan layanan standar proteksi atas akses sistem dan jaringan. RADIUS dikembangkan pada tahun 1990-an oleh *Livingstone Enterprise* yang sekarang bernama *Lucent Technology*. RADIUS merupakan sebuah protokol yang memungkinkan untuk melakukan *Authentication, Authorization, dan Accounting* (AAA)(Stiawan & Rini, 2009). RADIUS berfungsi untuk menyediakan mekanisme keamanan dan manajemen pengguna pada jaringan komputer (Hermawan, 2012). RADIUS diterapkan dalam jaringan dengan model *client-server*. RADIUS, berisi protokol atau aturan yang mendukung berbagai mekanisme dalam pengiriman data pengguna yang sensitif dari perangkat *client* ke *server authentication* (Yuliansyah, 2011). RADIUS didefinisikan dalam beberapa *Request For Comment* (RFC), daftarnya sebagai berikut:

1) RFC 2865 : *Remote Authentication Dial-In User Service* (RADIUS)
2) RFC 2866 : RADIUS *Accounting*
3) RFC 2867 : RADIUS *Accounting for Tunneling*
4) RFC 2868 : RADIUS *Authentication for Tunneling*
5) RFC 2869 : RADIUS *Extensions*
6) RFC 3162 : RADIUS *over* IP6
7) RFC 2548 : *Microsoft Vendor-Specific* RADIUS *Attributes*

Authentication, Authorization, dan Accounting

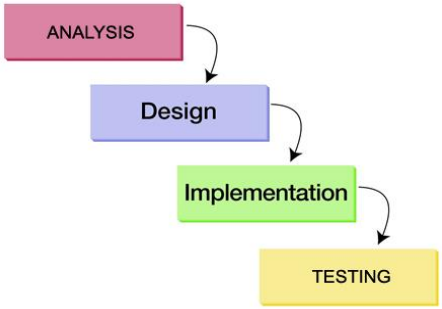
Authentication merupakan proses pemeriksaan identitas pengguna sistem melalui proses login ke dalam sistem dan pengguna yang lolos pemeriksaan identitas merupakan pengguna yang memiliki otoritas atas sistam (Rahardja et al., 2017). *User authentication* yaitu, seseorang yang diizinkan mengakses suatu sistem atau sumberdaya (Dano et al., 2015). *User authentication* hanya memberikan keputusan antara diizinkan dan tidak diizinkan. Cara paling umum untuk melakukan *authentication* dengan menggunakan *username* dan *password*.

Authorization merupakan pemberian alokasi layanan pada pengguna yang berhak mengakses sebuah jaringan. *Authorization* dilakukan ketika pengguna sudah dinyatakan berhak untuk menggunakan jaringan, setelah tahap *authentication* diselesaikan (Pattipeilohy, 2016).

Accounting merupakan proses yang dilakukan RADIUS *server* yang mencatat semua aktivitas pengguna dalam jaringan. Informasi yang diperoleh dari proses *accounting* disimpan pada RADIUS *server* dan dapat dipergunakan untuk berbagai keperluan seperti *billing*, *auditing*, dan *network management*(Muskitta, Yohanes, & Wardana, 2016).

METODE

Metode penelitian yang digunakan metode waterfall, langkah-langkah pelaksanaan metode waterfall dapat dilihat pada gambar 1.



Gambar 1. Metode Waterfall

Berdasarkan Gambar 1 dapat diuraikan sebagai berikut:

1) Analisis

Pada tahap analisis menggunakan teknik observasi dan studi pustaka untuk mendapatkan gambaran tentang kebutuhan sistem *user authentication* jaringan nirkabel berbasis *web* menggunakan RADIUS.

2) Desain

Pada tahap ini desain pada pengembangan *user authentication* jaringan nirkabel berbasis *web* menggunakan RADIUS, didesain dan dirancang sesuai dengan kebutuhan yang sudah didefinisikan pada tahap analisis.

3) Implementasi

Pada tahap ini dilakukan proses *coding, programming* dan pemasangan aplikasi sesuai dengan desain yang telah dibuat, dan sesuai dengan rencana pengembang *user authentication* jaringan nirkabel berbasis *web* menggunakan RADIUS.

4) Pengujian

Tahap pengujian untuk menemukan kesalahan-kesalahan atau kekurangan-kekurangan pada sistem yang akan digunakan. Pengujian bermaksud untuk mengetahui sistem yang dibuat sudah memenuhi kriteria yang sesuai dengan tujuan harapan pengembang *user authentication* jaringan nirkabel berbasis *web* menggunakan RADIUS.

HASIL DAN PEMBAHASAN

Hasil Analisis Sistem

Teknik analisis yang digunakan yaitu, teknik observasi dan teknik studi pustaka, yang menghasilkan analisis kebutuhan fungsional, analisis kebutuhan non fungsional, analisis kebutuhan perangkat keras, analisis kebutuhan perangkat lunak, dan analisis pengguna.

Analisis Fungsional Sistem

Kebutuhan fungsional sistem, yaitu:

a) Sistem manajemen *user authentication* menyediakan fitur *authentication* bagi pengguna jaringan nirkabel.
b) Sistem manajemen *user authentication* harus menyediakan fitur *create, read, update* dan *delete* untuk menambahkan data pengguna yang akan digunakan untuk hak akses ke jaringan nirkabel.
c) Sistem manajemen *user authentication* dapat digunakan untuk memudahkan administrator jaringan untuk mengelola koneksi jaringan nirkabel.
d) Sistem manajemen *user authentication* dapat melakukan pencatatan login pengguna saat pengguna melakukan akses jaringan nirkabel dan menampilkan informasi serta status pengguna.

Analisis Non Fungsional Sistem

Kebutuhan non fungsional sistem, yaitu:

a) Availability, jaringan nirkabel harus selalu tersedia.
b) Confidentiality, data pengguna yang tersimpan harus dijamin aman.
c) Integrity, data pengguna yang tersimpan terjaga keasliannya.
d) Sistem manajemen *user authentication* mampu menangani permintaan login dalam jumlah banyak dalam setiap waktu,
e) Sistem manajemen *user authentication* mampu memberikan keamanan dan *user-friendly*

Analisis Kebutuhan Sistem

Analisis kebutuhan sistem meliputi perangkat keras dan perangkat lunak, yaitu:

Tabel 2. Kebutuhan Perangkat Keras

Nama	Qty	Keterangan
Komputer *Server*	1	*RADIUS Server + Web Login + Firewall*
Access Point	3	TP-Link TL-WA7210N Outdoor
	12	TP-Link TL-WR840N Indoor
Switch	3	TP-Link 1Gbps 16 port

Router Firewall	1	MIkrotik RB750G
Kabel UTP	1	Kabel *backboneaccess point*

Adapun alasan pemilihan perangkat keras pada Tabel 2 selain karena merupakan perangkat keras tersebut dibutuhkan dalam menunjang pengembangan *user authentication* berbasis Web menggunakan RADIUS, alasan lainnya karena sebagian perangkat sudah ada.

Tabel 3. Kebutuhan Perangkat Lunak

Nama	Keterangan
Sistem Operasi *Linux Ubuntu*	*Server RADIUS + Web + Firewall*
CoovaChilli	*Web Login* dan DHCP
Apache 2.0	*WebServer*
MySQL	*Database* RADIUS
PHP & Python	Bahasa Pemrograman
FreeRADIUS	Aplikasi RADIUS

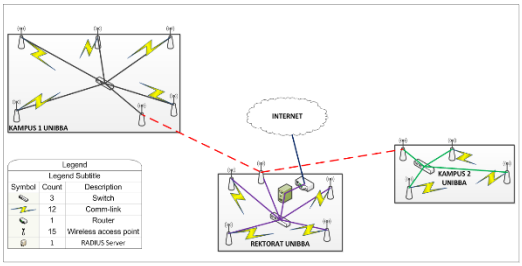
Alasan pemilihan perangkat lunak pada Tabel 3 karena merupakan perangkat lunak *OpenSource* yang bisa didapatkan secara mudah dan dapat dikembangkan sesuai dengan kebutuhan.

Analisis Pengguna

Pengguna yang menggunakan layanan jaringan nirkabel di UNIBBA meliputi mahasiswa, dosen, dan karyawan. Pengguna jaringan nirkabel tersebar dibeberapa titik lokasi yaitu, gedung rektorat, gedung kampus 1, dan gedung kampus 2.

Desain Topologi Jaringan Nirkabel

Desain topologi jaringan dibuat menggunakan aplikasi Microsoft Visio 2016, hasilnya dapat dilihat pada gambar 2.

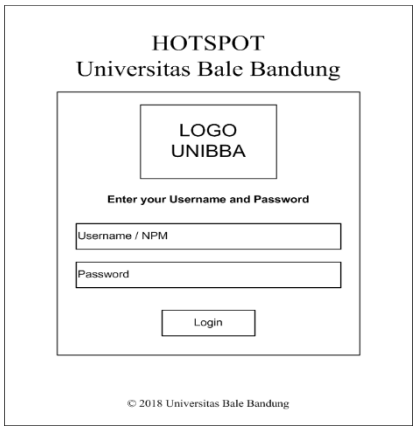


Gambar 2. Desain Topologi Jaringan

Berdasarkan gambar 2, terdapat 3 gedung berbeda lokasi yang harus terhubung dengan jaringan nirkabel yaitu, gedung rektorat, gedung kampus 1 dan gedung kampus 2. gedung rektorat akan menjadi titik pusat pendistribusian sinyal jaringan nirkabel yang akan didistribusikan ke gedung kampus 1 dan gedung kampus 2. Pemilihan gedung rektorat sebagai titik pusat jaringan nirkabel dikarenakan posisinya yang berada di tengah-tengah antara gedung kampus 1 dan 2.

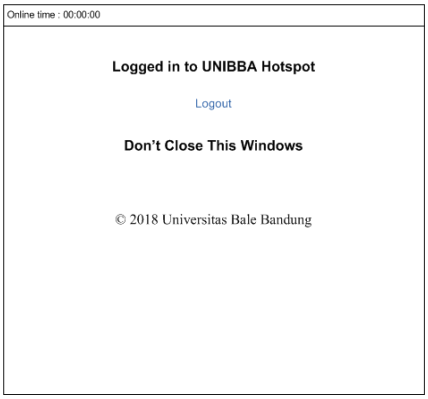
Desain *User Interface*

Desain *user interfacelogin* sistem manajemen *user authentication* berbasis *web* merupakan hasil pengembangan dari *user interfaceformlogin* dan *formlogout* yang dimiliki oleh *CoovaChilli*, yang disesuaikan dengan kebutuhan.



Gambar 3. Desain *Form Login*

Berdasarkan gambar 3 merupakan desain dari *form login* dari sistem *user authentication* berbasis *Web* yang terdapat beberapa bagian yaitu, nama *header*, logo UNIBBA, kolom *username*, kolom *password*, dan tombol Login serta *copyright*.

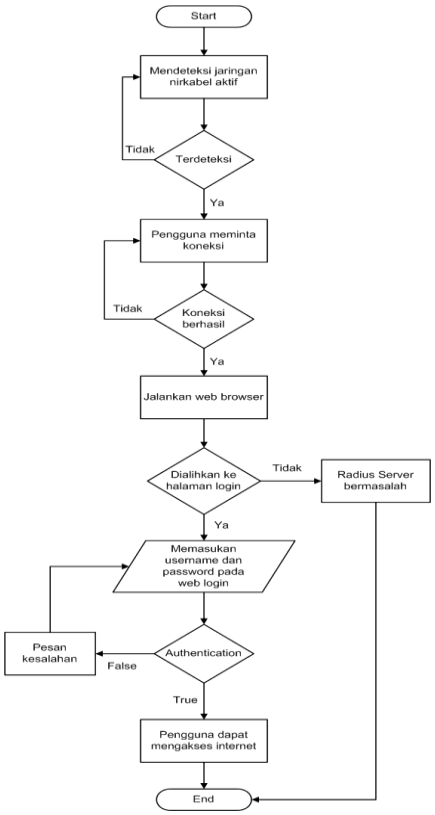


Gambar 4. Desain *Form Logout*

Sedangkan desain *form logout* dapat lihat pada gambar 4. Pada *form logout* tersebut memperlihatkan durasi waktu koneksi dari pengguna, informasi pemberitahuan agar jendela tersebut tidak ditutup sampai koneksi selesai, dan tombol *logout* yang berfungsi untuk mengakhiri layanan jaringan nirkabel di UNIBBA.

Mekanisme *User Authentication*

Web login form digunakan sebagai perantara antara pengguna dan RADIUS *server*. Berdasarkan gambar5 dapat dijelaskan bahwamekanisme *user authentication*sebagai berikut, pertama setiap pengguna yang terhubung jaringan nirkabel kemudian mencoba untuk terhubung ke internet, makaakan dialihkanke halaman *login* yang telah dibuat. Jika *username* dan password diterima maka, pengguna dapat mengakses *internet* melalui jaringan nirkabel, namun jika ditolak maka akan kembali ke halaman *login* dan tidak dapat mengakses *internet* melalui jaringan nirkabel.



Gambar 5. Mekanisme User Authentication

Implementasi *User Authentication* Berbasis *Web*

User authentication merupakan sistem keamanan pada jaringan nirkabel yang mekanismenya meminta pengguna layanan jaringan nirkabel untuk memasukkan *username* dan *password* yang sesuai dengan yang tersimpan pada *database*, pada penelitian ini *database* yang menyimpan informasi *username* dan *password* yaitu *database* RADIUS.

Instalasi dan Konfigurasi Apache dan PHP

Penelitian ini menggunakan model *authenticationCoovaChilli* yang menggunakan *Universal Access Method* (UAM), maka diperlukan *web server* Apache yang dilengkapi dengan modul SSL dan PHP. Langkah pemasangan Apache dan PHP dapat dilakukan dengan perintah :

 # apt-get install –f apache2 php

Setelah proses instalasi Apache dan PHP maka dilanjutkan dengan proses instalasi modul SSL pada Apache yang digunakan untuk mengenkripsi data antara *browser* pengguna dengan w*eb server* Apache. Cara instalasi modul SSL pada Apache dibutuhkan OpenSSL dan konfigurasi ssl-cert, dengan perintah sebagai berikut:

 # apt-get install –f openssl ssl-cert

Langkah selanjutnya adalah membuat alamat khusus untuk akses HTTPS, dengan perintah sebagai berikut:

 # cp /etc/apache2/sites-available/default /etc/apache2/sites-available/ssl

Setelah proses pembuatan alamat HTTPS berhasil, langkah selanjutnya *reload* Apache, supaya perubahan dapat diterapkan, perintahnya:

 # /etc/init.d/apache2 force-reload

Instalasi dan Konfigurasi MySQL

MySQL dibutuhkan untuk mengelola *database* RADIUS yang tersimpan data *username* dan *password* pengguna jaringan nirkabel UNIBBA, instalasi MySQL menggunakan perintah:

 # apt-get update
 # apt-get install –f mysql-server

Setelah proses instalasi MySQL selesai, maka selanjutnya adalah proses konfigurasi pada file my.cnf untuk merubah baris berikut.

bind-address = 127.0.0.1
menjadi
#bind-address = 127.0.0.1

Konfigurasi di atas dimaksudkan supaya server MySQL dapat diakses bukan hanya dari localhost saja. Kemudian lakukan restart pada server MySQL dengan perintah:

 # /etc/init.d/mysql restart

Instalasi RADIUS *Server*

Instalasi RADIUS *Server* dengan menggunakan *software* berbasis *opensource* FreeRADIUS. Cara instalasi dengan menggunakan perintah sebagai berikut:

 # apt-get install –f freeradius freeradius-mysql

Langkah selanjutnya adalah membuat *database* di MySQL yang akan digunakan oleh FreeRADIUS. FreeRADIUS dalam paket instalasinya telah menyediakan skema *database* yang dapat diambil pada direktori ***/usr/share/doc/freeradius/examples/***. Tahapan membuat *database* FreeRADIUS sebagai berikut:

 # mysql -u radius -p testing123
mysql> CREATE DATABASE radius_wifi;
quit;

Langkah selanjutnya adalah memasukkan skema *database* FreeRADIUS ke dalam *database* radius_wifi, perintahnya sebagai berikut:

 # mysql -u root –p radius123 radius_wifi < /etc/freeradius/sql/mysql/schema.sql

 # mysql -u root –p radius123 radius_wifi < /etc/freeradius/sql/mysql/nas.sql

Langkah selanjutnya supaya FreeRADIUS dapat mengakses *database* perlu dilakukan konfigurasi file ***/etc/freeradius/sql.conf,*** seperti berikut:

 # vi /etc/freeradius/sql.conf
server = "localhost"
login = "radius"
password = "testing123"
radius_db = "radius_wifi"
exit;

langkah selanjutnya melakukan set FreeRADIUS *client password*, sebagai berikut:

 # vi /etc/freeradius/clients.conf
client 127.0.0.1 {
secret = testing123
nastype = other
shortname = unibba
}

Langkah selanjutnya melakukan pengetesan terhadap FreeRADIUS yang telah diinstalasi dan dikonfigurasi dengan perintah sebagai berikut:

 # /etc/init.d/freeradius stop
 # freeradius -XXX

Jika FreeRADIUS telah berjalan dengan baik, maka akan tampil pesan seperti dibawah ini:

Debug: Ready to process requests.

Kemudian jalankan FreeRADIUS dengan perintah sebagai berikut:

 # /etc/init.d/freeradius start

Langkah selanjutnya yaitu pengetesan *user* yang telah disimpan di *database* FreeRADIUS, sebagai berikut:

#radtest radius testing123 127.0.0.1 0 testing123

Bilamana semua berjalan dengan baik, maka akan tampil pesan sebagai berikut:

Sending Access-Request of id 182 to 127.0.0.1 port 1812
User-Name = "radius"
User-Password = "testing123"
NAS-IP-Address = 127.0.1.1
NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=182, length=37

Instalasi dan Konfigurasi CoovaChilli

Setelah proses instalasi dan konfigurasi FreeRADIUS maka dilanjutkan dengan instalasi dan konfigurasi CoovaChilli. Cara instalasi dan konfigurasi seperti di bawah ini:

 # wget http://ap.coova.org/chilli/coova-chilli_1.0.13-1_i386.deb

Kemudian lakukan instalasi dengan perintah sebagai berikut:

 # dpkg -i coova-chilli_1.0.13-1_i386.deb

Kemudian salin *file* konfigurasi *default* CoovaChilli dengan perintah sebagai berikut:

 # cp /etc/chilli/defaults /etc/chilli/config
 # mkdir /var/www/hotspot
 # cd /var/www/hotspot
 # cp /etc/chilli/www/* /var/www/hotspot
 # mkdir /var/www/hotspot/images
 # cp /var/www/hotspot/coova.jpg /var/www/hotspot/images/

 # mkdir /var/www/hotspot/uam
 # cd /var/www/hotspot/uam
 # wget http://ap.coova.org/uam/
 # wget http://ap.coova.org/js/chilli.js

Selanjutnya adalah menyalin *file* /etc/chilli/defaults ke *file* baru dengan nama *config* pada *directory* yang sama. Kemudian lakukan konfigurasi pada file **/etc/chilli/config** dengan perintah sebagai berikut:

 # vi /etc/chilli/config

Isi dari file /etc/chilli/config:

 # -*- /bin/sh -*-
 # HS_WANIF=eth0
HS_LANIF=eth1
HS_NETWORK=10.10.1.0
HS_NETMASK=255.255.0.0
HS_UAMLISTEN=10.10.1.1
HS_UAMPORT=3990
HS_TCP_PORTS="80 443"
 # HS_DYNIP=
 # HS_DYNIP_MASK=255.255.255.0
 # HS_STATIP=
 # HS_STATIP_MASK=255.255.255.0
 # HS_DNS_DOMAIN=
HS_DNS2=62.72.64.237
HS_DNS1=192.168.2.1
HS_NASID=nas01
HS_UAMSECRET=testing123
HS_RADIUS=127.0.0.1
HS_RADIUS2=127.0.0.1

HS_RADSECRET=radiussecret
HS_UAMALLOW=10.10.1.1
HS_UAMDOMAINS="radius.org"
 # HS_SSID=<ssid>
 # HS_NASMAC=<mac address>
 # HS_NASIP=<ip address>
HS_UAMSERVER=10.10.1.1
HS_UAMFORMAT=https://\$HS_UAMSERVER/uam/
HS_UAMHOMEPAGE=http://\$HS_UAMLISTEN:\$HS_UAMPORT/www/coova.html
HS_UAMSERVICE=https://10.10.1.1/cgi-bin/hotspotlogin.cgi

Instalasi dan Konfigurasi Firewall

Pembuat *CoovaChilli* sudah membuat aturan *firewall* untuk *IPTables*, namun *script* yang disediakan masih membutuhkan sedikit bantuan untuk dapat berjalan dengan baik. Konfigurasi *IPTables* di *CoovaChilli* dilakukan melalui file /etc/chilli/up.sh yang di jalankan sesudah *interface* tun0 beroperasi. File /etc/chilli/up.sh dijalankan dengan perintah sebagai berikut:

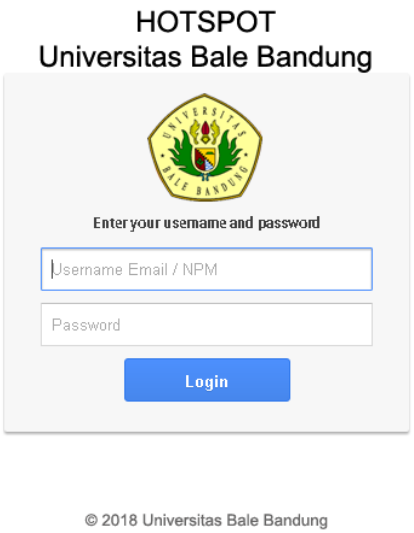
 # sh /etc/chilli/up.sh

Script firewall CoovaChilli dijalankan maka aturan *firewall IPTables* telah terpasang.

Pengujian Sistem *UserAuthentication*

Tahap pengujian sistem*userauthentication* dilakukan menggunakan *Smartphone* dan *Notebook* dengan mencoba terhubung ke jaringan nirkabel UNIBBA yang telah selesai dikembangkan dengan *Service Set Identifier* (SSID): @UNIBBA.*Webbrowser*yang digunakan *GoogleChrome* baik pada *smartphone* dan *notebook*.

Setelah penggunaberhasil terhubung ke jaringan nirkabel UNIBBA dengan mendapatkan IP*Address*dari DHCP*server*, maka selanjutnya pengguna akan dialihkan untuk melakukan *authentication* dengan mengunjungi *web form login.* Seperti dapat dilihat pada gambar 5.5.



Gambar 6.*Web Login Form*

Pengujian sistem *userauthentication*dilakukan dengan dua cara. Cara pertama dilakukan dengan melakukan proses pengujian *authentication* pada sisi RADIUS server dan cara kedua dilakukan pengujian *authentication* pada sisi pengguna jaringan nirkabel melalui *web form login*. *Username* dan *password* yang digunakan untuk melakukan *login* ke jaringan nirkabeldibagi menjadi 3 bagian, yaitu:

a. Mahasiswa, *login* dengan menggunakan Nomor Pokok Mahasiswa (NPM) sebagai *username* dan *password*yang sudah dibuat.
b. Dosen dan karyawan, *login* menggunakan *username* dan *password*yang sudah dibuat.

Pengujian *authentication* pada RADIUS *server* dilakukan untuk memastikan RADIUS *server* dapat berjalan dengan baik dalam melakukan proses *authentication* terhadap data penggunayang tersimpan dalam *database*. Perintah untuk melakukan pengujian *authentication* RADIUS *server* sebagai berikut:

 # sudo radtest radiusradius123 localhost 1812 testing123

Hasil pengujian *authentication* RADIUS *server* secara umum,*server* dapat berjalan dengan baik dalam menangani permintaan *authentication request.* Hal ini dapat diketahui melalui status dari proses *authentication* yang benilai *Access-Accept.*

Langkah selanjutnya,pengujian *authentication* melalui *Web Login Form*yang dilakukan untuk menguji proses *authentication* pada sisi pengguna jaringan nirkabel. Hasil pengujian *authentication* yang dilakukan pada sisi penggunajaringan nirkabelmelalui *web login form*sebagai berikut:

Tabel 4. Hasil Pengujian Authentication Melalui Web Login Form

Kondisi	User name	Password	Proses Login	
			Sukses	Gagal
Database kosong	-	-		√
Data baru	radius	radius123	√	
Ubah password	radius	radius123		√
Password Baru	radius	radius1234	√	
Case sensitive	radius	Radius123		√
Case sensitive	radius	RADIUS123		√
Case sensitive	Radius	radius123		√
Data dihapus	-	-	-	√

Berdasarkan Tabel 4 dari hasil pengujian dapat diuraikan sebagai berikut:

a. *Database* kosong, proses *login username* dan *password* dikosongkan, proses *user authentication* gagal.
b. Data baru, proses *loginusername* dan *password* dibuat dan tersimpan di *database* RADIUS yaitu *username*: radius dan *password*: radius123, maka proses *user authentication*sukses.
c. Ubah *password,username* benar namun *password* yang dimasukkan bukan password yang baru yaitu radius1234, maka proses *user authentication* gagal.
d. Password baru, *login* menggunakan *username* dan *password* menggunakan password yang baru yaitu radius1234, maka proses *user authentication* sukses.
e. *Casesensitive,* ketika proses *login* menggunakan *username* namun dengan *password* salah satu karakternya salah yaitu Radius123 yang seharusnya radius123, maka proses *user authentication* gagal.
f. *Casesensitive,* ketika proses *login* menggunakan *username* namun dengan *password* yang karakternya salah yaitu RADIUS123 yang seharusnya radius123, maka proses *user authentication* gagal.
g. *Casesensitive,* ketika proses *login* menggunakan *username* yang karakternya salah yaitu Radius yang seharusnya radius namun dengan *password* benar yaitu radius123, maka proses *user authentication* gagal.
h. Data dihapus, proses *login username* dan *password* dengan menggunakan*username*: radius dan *password*: radius123, maka proses *user authentication* gagal.

KESIMPULAN DAN SARAN

Kesimpulan

Pengembangan sistem *user authentication* berbasis web menggunakan RADIUS setelah dilakukan pengujian menggunakan perangkat *smartphone* dan *notebook* dapat diambil kesimpulan bahwa *user authentication* menggunakan *RADIUS* dapat dikategorikan aman dan *user-friendly* yang mampu membedakan pengguna yang diizinkan dan tidak diizinkan untuk menggunakan layanan jaringan nirkabel. Kesimpulan tersebut didapatkan dari hasil pengujian yang telah dilakukan dengan cara menguji RADIUS *server* dan pengujian pada sisi pengguna melalui *web login form*. Pengujian *user authentication* pada RADIUS *server* secara umum dapat berjalan dengan baik dalam menangani permintaan *authentication request*, hal ini dapat diketahui melalui status dari proses *authentication* yang benilai *Access-Accept*, sedangkan pengujian *user authentication* melalui *web login*

form yang dilakukan untuk menguji proses *authentication* pada sisi pengguna menggunakan perangkat yang mendukung jaringan nirkabel. Hasil pengujian ketika *username* dan *password* yang digunakan sama dengan yang tersimpan pada *database* RADIUS, maka proses *login* sukses dilakukan, namun ketika *username* dan *password* salah dan tidak tersimpan pada *database* RADIUS proses *login* akan gagal dilakukan.

Saran

Setiap langkah memiliki tujuan, setiap tujuan memperlukan sarana dan prasarana, begitu pun dengan pengembangan suatu sistem sudah pasti membutuhkan sarana dan prasarana. Peningkatan sarana dan prasarana jaringan nirkabel yang telah dibangun diharapkan kedepannya akan dilakukan peningkatan spesifikasi komputer server, peningkatan teknologi standarisasi *Access Point* (AP) menjadi b/g/n/ac, dan peningkatan atau penambahan *bandwidth* yang khusus dialokasikan untuk jaringan nirkabel.

Pemanfaatan *database* RADIUS dapat lebih dioptimalkan, karena selain datanya hanya dipergunakan untuk *user authentication*jaringan nirkabel, database RADIUS dapat dipergunakan untuk membangun sistem *Single Sign On* (SSO).

REFERENSI

Dano, A. B. C., Wowor, H. F., & Lantang, O. A. (2015). Perancangan Web Service Sistem Autentikasi dan Identifikasi Berbasis QR Code Pada Universitas Sam Ratulangi. *E-Journal Teknik Elektro Dan Komputer*, 1–7.

Darmadi, E. A. (2018). Perancangan Sistem Otentikasi Radius Pada Pengguna Jaringan Wireless Untuk. *Jurnal IKRA-ITH Informatika*, *2*(3), 9–16.

Dhiman, D. (2014). WLAN Security Issues and Solutions. *IOSR Journal of Computer Engineering (IOSR-JCE)*, *16*(1), 67–75. Retrieved from https://pdfs.semanticscholar.org/cab d/a6b52dfd269e5e478ddeaa86220ef3abe4ef.pdf

Gali, T. A. B., & Mustafa, A. B. A. (2015). A Comparative Study between WEP , WPA and WPA2 Security Algorithms. *International Journal of Science and Research (IJSR)*, *4*(5), 2390–2391. Retrieved from https://www.ijsr.net/archive/v4i5/SUB154986.pdf

Julianto, A., Migunani, & Efendi, R. (2013). Otentikasi Penggunaan Layanan Wireless Lan Dengan FreeRADIUS DAN CHILLISPOT. *Jurnal Teknologi Informasi Dan Komunikasi*, *4*(2), 1–10. https://doi.org/Achmad Julianto1, Migunani2, Rissal Efendi3

Jyoti, & Saini, H. (2017). A Study on Networks and Comparison of Wired, Wireless and Optical Networks. *International Journal of Innovative Research in Computer*, *5*(3), 3801–3809. https://doi.org/10.15680/IJIRCCE.2017

Muskitta, Y. J., Yohanes, B. W., & Wardana, H. K. (2016). Implementasi Protected Extensible Authentication Protocol (PEAP) menggunakan Remote Access Dial In User Service (RADIUS). *Techné Jurnal Ilmiah Elektroteknika*, *15*(2), 91–100.

Ochang, P. A., Irving, P. J., & Ofem, P. O. (2016). Research on Wireless Network Security Awareness of Average Users. *International Journal of Wireless and Microwave Technologies*, *6*(2), 21–29. https://doi.org/10.5815/ijwmt.2016.02.03

Pattipeilohy, W. F. (2016). Analisis dan Perancangan User Manager pada Mikrotik Router dengan Sistem Pembelian Kredit Voucher. *Jurnal SISFOKOM*, *05*(01), 64–69.

Pavithran, M. (2015). Advanced Attack Against Wireless Networks Wep , Wpa / Wpa2-Personal And Wpa / Wpa2- Enterprise. *International Journal of Scientific & Technology Research*, *4*(08), 147–152. Retrieved from http://www.ijstr.org/final-print/aug2015/Advanced-Attack-Against-Wireless-Networks-Wep-Wpawpa2-personal-And-Wpawpa2-enterprise.pdf

Rahardja, U., Harahap, E. P., & Fresandy, G. (2017). Penerapan Sistem Autentikasi Sertifikat Sebagai Pengambil Keputusan Validasi Sertifikat Pada Perguruan Tinggi. *Technomedia Journal (TMJ)*, *2*(1), 17–25.

Rohman, N. (2008). Sistem Pendistribusian Informasi Jadual Ujian Stmik Mardira Indonesia Dengan Menggunakan Layanan Protocol Data Unit (PDU Type). *Jurnal Computech & Bisnis*, *2*(2), 80–95. Retrieved from http://jurnal.stmik-mi.ac.id/index.php/jcb/article/view/25

Rosadi, D. (2016). APLIKASI SOCIAL LEARNING NETWORKS BERBASIS WEB (STUDI KASUS DI STMIK MARDIRA INDONESIA) Dadi Rosadi. *Jurnal Computech & Bisnis*, *10*(2), 72–77. Retrieved from http://jurnal.stmik-mi.ac.id/index.php/jcb/article/view/148/171

Sikarwar, A. P. S., & Saxena, P. (2017). An Analytical and Experimental Study of AAA Model with Special Reference to RADIUS and TACACS +. *International Journal of Computer Applications*, *169*(9), 6–10.

Simangunsong, A. (2018). Sistem Informasi Pengarsipan Dokumen Berbasis Web. *Jurnal Mantik Penusa*, *2*(1), 11–19.

Stiawan, D., & Rini, D. P. (2009). Analisis Perbandingan Sistem Keamanan WEP/WPA/RADIUS Pada Jaringan Publik Wireless Hotspot. In *Seminar Nasional Electrical, Informatics, And It's Educations* (pp. 1–5). Palembang.

Sundari, J. (2016). Sistem Informasi Pelayanan Puskesmas Berbasis Web. *Indonesian Journal on Software Engineering Sistem (IJSE)*, *2*(1), 44–49.

Suprianto, & Riswaya, A. R. (2018). Sistem Pengkodean Data Pada File Teks Untuk Keamanan Informasi Dengan Menggunakan Metode Skipjack. *Jurnal Computech & Bisnis*, *12*(1), 59–72. Retrieved from https://pdf.lemlit.com/wp-content/uploads/2018/08/06-Suprianto.pdf

Tenggario, R. P., & Lukas, J. (2011). Manajemen Jaringan Wireless Menggunakan Server Radius. *Jurnal Teknik Komputer*, *19*(9), 80–87.

Yuliansyah, H. (2011). Optimalisasi Radius Server Sebagai Sistem Otentikasi Dan Otorisasi Untuk Proses Login Multi Aplikasi Web Berbasis Php. In *Seminar Nasional Informatika 2011 (semnasIF 2011)* (Vol. 2011, pp. 17–23).