Jurnal Sain Informatika
Sistem dan Teknologi Informasi

Penerapan Sistem Autentifikasi dan Pengamanan pada Jaringan Hotspot Berbasis Captive Portal di Universitas Prof. Dr. Hazairin, SH

Elviza Diana[1*)], Ade Fitrah Putra Akhir [2], Yulia Darmi [3]
[1] Program Studi Informatika, Fakultas Teknik, Universitas Prof.DR. Hazairin,SH, Bengkulu
[2] Program Studi Informatika, Fakultas Teknik, Universitas Prof.DR. Hazairin,SH, Bengkulu
[3] Program Studi Informatika, Universitas Muhammadiyah, Bengkulu
[1,2] Jln Jend. A. Yani No. 1, Kebun Ros, Kec. Tlk. Segara, Kota Bengkulu, Bengkulu 38115
[3]Jln. Bali, Kp. Bali, Kec. Tlk. Segara, Kota Bengkulu, Bengkulu 38119
email : [1]elvizaunihaz@gmail.com,[2]adefitrah.af@gmail.com,[3]yuliadarmi10juli@gmail.com

Abstract **- Prof. Dr University. Hazairin.SH seeks to utilize ICT by providing hotspot services for students, lecturers, employees and foundations. However, the use of hotspots is experiencing problems due to the ease with which the general public can connect to the Hotspot network at Prof. Dr. Hazairin, SH University (UNIHAZ) Bengkulu, Lack of security on the Hotspot network at UNIHAZ. The purpose of this research is the implementation of Captive Portal makes it easier to manage and monitor users in the hotspot area at UNIHAZ. Improved security with user management on the UNIHAZ Hotspot network. With the existence of a data security system using a captive portal, which was developed to make it easier for administrators to monitor and control users connected to the network and can limit bandwidth usage.**
Keywords ***: Autentifikasi, Hotspot, Captive Portal***

Abstrak- Universitas Prof. Dr. Hazairin. SH berupaya untuk memanfaatkan TIK dengan menyediakan layanan hostspot bagi mahasiswa, dosen, karyawan maupun yayasan. Akan tetapi pemakaian hostspot tersebut mengalami permasalahan dikarenakan mudahnya orang umum terhubung dengan jaringan Hotspot di Universitas Prof. Dr. Hazairin, SH (UNIHAZ) Bengkulu, kurangnya keamanan pada jaringan Hotspot di Universitas Prof. Dr. Hazairin, SH. Tujuan dari penelitian ini adalah implementasi Captive Portal mempermudah dalam memanagement dan memonitoring user di area hotspot di Universitas Prof. Dr. Hazairin, SH Peningkatan keamanan dengan manajemen user pada jaringan Hotspot Universitas Prof. Dr. Hazairin, SH. Dengan adanya sistem pengaman data menggunakan captive portal ini yang dikembangkan memudahkan administrator dalam memantau dan mengontrol user-user yang terhubung ke jaringan serta dapat membatasi penggunaan bandwidth.
Kata Kunci : **Autentifikasi, Hotspot, Captive Portal**

1) **penulis**: Elviza Diama
Email: elvizaunihaz@gmail.com

I. PENDAHULUAN

Pada Universitas Prof. Dr. Hazairin, SH Bengkulu saat ini dikembangkan program sistem keuangan dan akademik secara online, untuk mendukung program tersebut maka Universitas Prof. Dr. Hazairin,SH Bengkulu menyediakan layanan *hotspot* yaitu sebuah area dimana pada area tersebut tersedia koneksi *internet wireless* yang dapat diakses melalui *Notebook*, *PDA* maupun perangkat lainnya yang mendukung teknologi tersebut. Dengan *hotspot* di Universitas Prof. Dr. Hazairin, SH Bengkulu, maka mahasiswa, dosen dan karyawan bisa menikmati akses *internet* dimanapun kita berada selama di area *hotspot* tanpa harus menggunakan kabel. Layanan inilah yang nanti diharapkan akan mempercepat akses informasi bagi mahasiswa, dosen maupun karyawan, khususnya di dunia pendidikan yang mana diketahui sebagai *barometer* kemajuan teknologi informasi.

Hotspot adalah sebuah area dimana pada area tersebut tersedia koneksi internet wireless yang dapat diakses oleh siapapun. Universitas Prof. Dr. Hazairin, SH Bengkulu sudah terdapat area Hotspot. Peneliti merasa bahwa sistem *hotspot* seperti ini harus dikelola dengan baik. Oleh sebab itu peneliti mencoba menerapkan sistem autentifikasi pada Hotspot Universitas Prof. Dr. Hazairin, SH Bengkulu dikarenakan pada saat ini terdapat permasalahan yaitu :

1. Mudahnya orang umum terhubung dengan jaringan Hotspot di Universitas Prof. Dr. Hazairin, SH Bengkulu.
2. Kurangnya keamanan pada jaringan di Universitas Prof. Dr. Hazairin, SH

Sistem kerja pada *Captive Portal* adalah ketika pada saat seorang pengguna berusaha untuk

melakukan *browsing* ke *Internet, captive portal* pengguna akan terlebih dahulu masuk menuju ke *Authentication web* dan akan di beri *prompt login* termasuk informasi tentang *hotspot* yang sedang dia gunakan. Jika *Linux Router/wireless gateway* mempunyai mekanisme untuk menghubungi sebuah *Authentication server* dan mengetahui identitas dari pengguna *wireless* yang tersambung. *wireless gateway* akan membuka aturan *firewall*-nya untuk pengguna tertentu.

Pada penelitian permasalahannya adalah bagaimana implementasi sistem autentifikasi dan pengamanan pada jaringan hostpot pada Universitas Prof. Dr. Hazairin, SH Bengkulu menggunakan captive portal sehingga orang umum tidak dapat terhubung dengan jaringan Hotspot di Universitas Prof. Dr. Hazairin, SH Bengkulu dan upaya meningkatkan keamanan pada jaringan Hotspot di Universitas Prof. Dr. Hazairin, SH Bengkulu.

Tujuan dari penelitian ini adalah :

1. Dengan adanya *Captive Portal* diharapkan dapat mempermudah dalam *memanagement* dan *memonitoring user* di area *hotspot* di Universitas Prof. Dr. Hazairin, SH Bengkulu.
2. Menerapkan sistem *Captive Portal* ke dalam jaringan *Hotspot* Universitas Prof. Dr. Hazairin, SH Bengkulu ke *internet.*
3. Peningkatan keamanan dengan manajemen user pada jaringan Hotspot Universitas Prof. Dr. Hazairin, SH Bengkulu.

II. PENELITIAN YANG TERKAIT

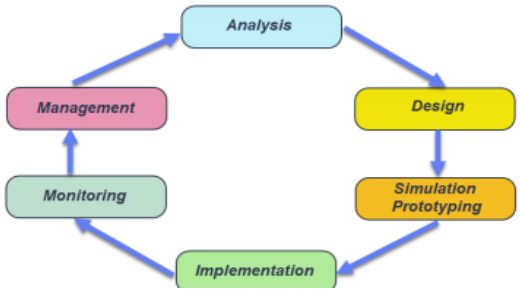
Ada beberapa penelitian terkait pada Captive Portal yaitu yang dilakukan oleh Novrianda(2017*)* pada penelitian ini, dilakukan beberapa konfigurasi untuk membangun *authentication Captive Portal* dengan menggunakan MikroTik routerBOARD serta keseluruhan konfigurasi diproses memanfaatkan program Winbox v3.11. Hasil penelitian diperoleh bahwa keamanan WLAN pada PT. Rikku Mitra Sriwijaya telah berhasil ditingkatkan dengan mengimplementasikan *authentication Captive Portal*. Dengan begitu, *user* yang ingin memanfaatkan *hotspot* PT. Rikku Mitra Sriwijaya terlebih dahulu harus melakukan registrasi dengan mengisikan data-data lengkap *user* termasuk *username* dan *password* masing-masing *user*, sehingga untuk 1 *user* hanya memiliki 1 *username* dan *password* untuk dapat mengakses *internet* pada WLAN PT. Rikku Mitra Sriwijaya. Tidak hanya sebatas itu, pada penelitian ini juga dapat melakukan *monitoring* seluruh *user* yang terhubung dengan WLAN PT. Rikku Mitra Sriwijaya dengan bantuan program Winbox v3.11.

dengan penyedia jaringan wireless yang berfungsi untuk melakukan autentifikasi, sebelum user atau klien mengakses sunihazerdaya jaringan atau jaringan internet.

Dalam penelitiannya Haryadi (2016) yaitu teknik media otentikasi Captive Portal dan keamanan data yang melintas dari jaringan eksternal ke jaringan internal. Captive Portal adalah perangkat router atau gateway untuk melindungi atau tidak membiarkan lalu lintas apapun, sampai pengguna melakukan registrasi ke sistem sebelumnya. Captive Portal biasanya digunakan di infrastruktur nirkabel seperti area hotspot, namun tidak berlaku untuk jaringan kabel.

III. METODE PENELITIAN

Metode Network Development Life Cycle (NDLC) digunakandengan melakukan pendekatan terhadap proses komunikasi data berorientasi network yang memiliki suatu lingkaran tahapan yang tidak memiliki awal maupun akhir proses. Tahapan pada metode NDLC adalah analysis, design, simulation prototyping, implementation, monitoring serta tahapan terakhir adalah management (Novrianda, 2017). Berikut ini pada Gambar 1 memperlihatkan lingkaran tahapan metode NDLC, sebagai berikut:



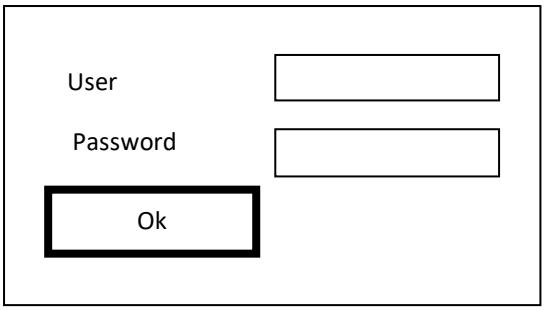
Gbr. 1 Metode Network Development Life Cycle (NDLC)

Captive Portal merupakan suatu teknik autentifikasi dan pengamanan data yang lewat dari network internal ke network eksternal. Captive Portal sebenarnya merupakan mesin router atau gateway yang memproteksi atau tidak mengizinkan adanya trafik, sampai user melakukan registrasi terlebih dahulu ke dalam sistem. Biasaanya Captive Portal ini digunakan pada infrastruktur wireless seperti hotspot area, tapi tidak menutup kemungkinan diterapkan pada jaringan kabel.

3.1 Perancangan

Captive portal bekerja dengan cara mengalihkan semua permintaan akses http dari klien menuju ke sebuah halaman khusus yang biasanya berupa halaman autentifikasi pengguna atau halaman kesepakatan antara pengguna

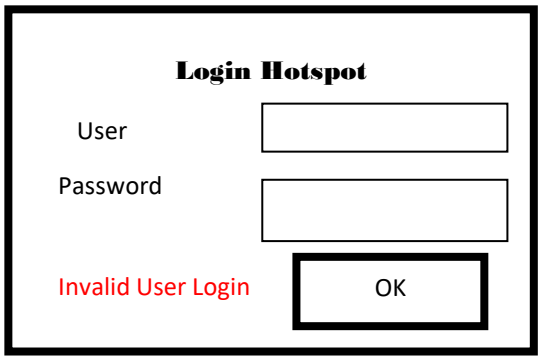
Perancangan Autentifikasi Login User



Gbr. 2 Rancangan Layar Login

Layar login terdiri atas logo, tulisan Login Hotspot (label), Tulisan User, password, text field, button login dan alamat. Apabila login gagal maka akan ditampilkan layar invalid login dan program akan meminta login ulang. Apabila login berhasil maka akan melakukan ridirect ke site : http://www.unihaz.ac.id/v2.

Rancangan Layar Invalid Login



Gbr. 3 Rancangan Layar Invalid Login

Layar login terdiri atas logo, tulisan Login Hotspot (label), Tulisan User, password, text field, button login dan alamat. Layar ini akan terus tampil selama login belum berhasil. Apabila login berhasil maka akan melakukan ridirect ke site : http://www.unihaz.ac.id/v2.

1. Success Login (redirect to unihaz.ac.idv2)

Gbr. 4 Redirect to unihaz.ac.id/v2

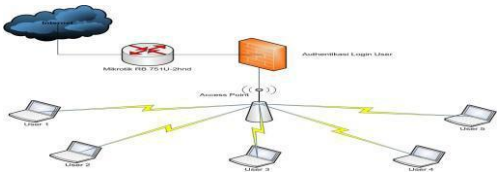
IV. HASIL DAN PEMBAHASAN

4.1. Konsep Captive Portal

Salah satu masalah terbesar bagi infrastruktur WiFi, terutama yang membuka akses untuk umum, seperti hotspot, adalah authentikasi pengguna. Captive portal menjadi mekanisme populer bagi infrastruktur komunitas WiFi dan operator hotspot yang memberikan authentikasi bagi penguna infrastruktrur maupun manajemen flow IP, seperti, *traffic shaping* dan kontrol bandwidth, tanpa perlu menginstalasi aplikasi khusus di komputer pengguna. Proses authentication secara aman dapat dilakukan melalui sebuah web browser biasa di sisi pengguna.

Captive portal juga mempunyai potensi untuk mengijinkan kita untuk melakukan berbagai hal secara aman melalui SSL & IPSec dan mengset rule quality of service (QoS) per user, tapi tetap mempertahankan jaringan yang sifatnya terbuka di infrastruktur WiFi. Jadi ide dasar captive portal sebetulnya cukup sederhana. Daripada kita tergantung pada mekanisme keamanan built-in di peralatan WiFi 802.11b untuk mengontrol siapa saja yang dapat berasosiasi ke Access Point, menggunakan Captive portal kita mengkonfigurasi agar Access Point bekerja tanpa WEP dan merupakan network yang terbuka. Access Point bekerja pada mode bridge (bukan router), dan tersambung melalui kabel LAN ke sebuah router Mikrotik. Router Mikrotik yang akan memberikan IP melalui DHCP bagi semua wireless node yang tergabung, termasuk mengatur bandwidth dari masing-masing wireless node selain mengatur siapa yang boleh bergabung siapa yang tidak. Router Mikrotik disini berfungsi sebagai wireless gateway yang menjadi perantara antara infrastruktur wirelesss dengan Internet.

4.2. Sistem Authentikasi



Gbr. 5 Sistem Authentikasi

Pada gambar diatas dijelaskan bahwa user yang sedang roaming akan berasosiasi dengan Access Point. Kemudian, pengguna Wireless tersebut meminta IP address dari gateway menggunakan protokol DHCP. Gateway (atau Access Point) akan segera memberikan penyewaan DHCP dan alokasi IP address. Semua IP address yang belum terauthentikasi akan terkena firewall sehingga mereka hanya dapat digunakan di segmen wireless

saja. Semua akses melewati gateway akan di blokir.

Pada saat pengguna membuka browser untuk mengakses Web, browser mereka akan di re-direct ke gateway. Gateway kemudian akan me-redirect permohonan akses Web ke halaman login Authentication system menggunakan SSL sesudah menambahkan token random dan beberapa informasi lainnya ke kalimat URL yang digunakan.

4.3. Login User

Pembuatan aplikasi login user dengan menggunakan bahasa pemrograman html. Dimana tampilannya berbentuk website yang menggunakan *deface* hotspot unihaz. Berikut tampilan login user :

Gbr. 6 Tampilan Login User

User yang terkoneksi harus login terlebih dahulu sebelum bisa menggunakan internet. Dimana setiap id dan password user harus didaftarkan terlebih dahulu oleh admin. (koding terlampir)

4.4. Ridirect Url

Setelah login sukses maka link akan melakukan akses kesitus yang sudah dikonfigurasikan. Hal ini bisa langsung mengarah ke situs yang sudah dikonfigurasikan di browsernya sendiri maupun langsung dari *deface* yang dibuat. Konfigurasi yang dilakukan yaitu untuk mengarahkan akses setelah login ke situs resmi UNIHAZ yaitu unihaz.ac.id.

Gbr. 7 Akses Ke situs UNIHAZ

4.5. Add User

User yang akan menggunakan internet terlebih dahulu harus didaftarkan oleh admin sehingga id dan password user diberikan oleh admin.

4.6. Konfigurasi sistem

Langkah Seting Hotspot Pada Mikrotik RB 751-2HND

a. Langkah pertama, buka aplikasi winbox untuk dapat meremote mikrotik RouterOS pada RB 751-2HND
b. Kemudian klik mac-address yang muncul
c. Klik Connect untuk masuk ke mikrotik
d. Pilih IP Addres dengan cara klik internet Protokol (IP) pilih Addres kemudian klik tanda + kemudian masukan IP yang terhubung ke Access ponit atau RB 751-2HND contoh :192.168.1.1/24 kemudian klik ok
e. Kemudian Setting IP ROUTES GATEWAY dengan cara klik IP pilih Routes kemudia pilih tanda + isi Gateway contoh : 192.168.1.1 klik ok
f. Setting DNS SERVER dengan cara klik IP pilih DNS kemudian isi Servers contoh : 192.168.1.1 klik Ok
g. CHEK PING, klik New Terminal setelah itu ketik ping 192.168.1.1
h. setting IP *FIREWALL*, klik IP klik Firewall, pilih NAT kemudian advance pilih out interface, pilih Action, masqurade klik ok
i. Setting IP Addres Untuk Ether 2 dengan cara klik IP, Addres pilih tanda tambah, klik Address isi contoh : 192.168.2.1/24, interface pilih ether 2 klik ok
j. Setting IP Hotspot, klik IP, Hostpot, servers klik Hotspot Setup kemudian lanjutkan dengan Next sampai selesai
k. setelah itu klik Radius pilih tanda + kemudian pilih General, contreng Hotspot, isi Address Contoh : 127.0.0.1, secret contoh 1234 klik ok
l. Menghubungkan Radius server pada Hospot, klik IP Hospot, Server Profil klik 2 kali, checklist Radius Server klik ok
m. klik New Terminal kemudian kemudian melakukan pengaturan login dan password utuk masuk ke user manager
n. Rubah Port Dengan cara klik IP, Services, pilih www, pada port awalnya 80 di ganti dengan 8080, klik ok
o. Setelah semua pengaturan selesai mulai melakukan tes dengan cara membuka mozilla kemudian pada Address Bar ketik googel.com, setelah itu hotspot akan meminta Login dan Passwoard, isi dengan data yang dimasukan pada IP Addres Ether 2 tadi contoh: Login : admin passwoard : admin
p. setelah Login berhasil maka kita langsung bisah masuk ke googel dan menggunakan jaringan
q. Kemudian kita mulai membuat Usermanager, pada Address bar ketik 192.168.1.1:8080/Userman kemudian Enter

r. kemudian Masukan Login dan password suda benar yang mana suda kita buat di mikrotik pada tool User manager, maka akan tampil pada gambar dibawah ini
s. Pilih Profil, klik tanda tambah (+) kemudian isi nama Profil contoh Dosen, setelah semua data sudah di isi klik save.
t. Langkah terakhir membuat User, klik usre, add pilih one isi username contoh : surya, password : surya, klik caller Id setelah itu klik add
u. Kemudian kita keluar dari radius dengan cara ketik IP : 192.168.2.1 maka akan tampil, tampilan seperti gambar dibawa, maka klik log off, keluar dari google.
v. lakukan pengujian dengan cara buka kembali Googel kembali maka akan akan tampil seperti gambar dibawa, maka isi Login dan Password yang sudah kita buat di User manager tadi

V. KESIMPULAN

Berdasarkan pembahasan diatas, peneliti menarik kesimpulan sebagai berikut :

a. Dengan adanya sistem pengaman data menggunakan captive portal ini yang dikembangkan memudahkan administrator dalam memantau dan mengontrol user-user yang terhubung ke jaringan serta dapat membatasi penggunaan bandwidth.
b. Dari sisi keamanan penggunaan sistem pengaman data menggunakan captive portal ini juga relatif aman bagi data pengguna, karena memanfaatkan sistem tunelling dengan SSL yang akan mengenkrip semua data yang dikirim client maupun server hotspot.
c. Di sisi kenyamanan pengguna juga sistem pengaman data menggunakan captive portal yang dibuat memudahkan bagi mahasiswa untuk terkoneksi ke hotspot tanpa adanya prosedur yang berbelit-belit seperti meminta password WEP KEY (seperti pada sistem sebelumnya). Mahasiswa tidak perlu mendaftar untuk bisa menggunakan layanan hotspot. Karena mahasiswa yang sudah registrasi secara otomatis akan dimasukan sebagai user.

DAFTAR PUSTAKA

[1] Andi 2008 : *"Kamus Lengkap Dunia Komputer"* Yogyakarta Penerbit komputer Semarang
[2] Didik Prasetio 2005: "*Solusi Menjadi Web Master melalui Manejemen web*
[3] *dengan php*" Jakarta Penerbit: Elex Meddia Komputindo
[4] Iwan Safana 2011: "*Teori dan modul praktikum jaringan komputer*" Bandung
[5] Onno W. Purbo 2006: " *Internet Wireles dan Hostpot*" Jakarta Penerbit: Elex
[6] Meddia Komputindo
[7] Rahim Taufik 2008 : *"Sistem informasi"* Bandung *Penerbit : FTI_ITB*
[8] Salemba Infotek :2005:"*Konsep jaringan komputer dan pengembangannya*" Jakarta
[9] Haryadi, M.A., 2016. Perancangan media otentikasi menggunakan captive portal pada jaringan wireless laboratorium komputer Teknik Elektro Universitas Diponegoro. Transient 5 (2), 1-8.
[10] Novrianda, R. (2017). Rancang bangun keamanan jaringan wireless pada STIPER Sriwigama Palembang dengan radius server. Jurnal Maklumatika, 4(1), 19-29.