IMPLEMENTASI JARINGAN HOTSPOT DENGAN *CAPTIVE PORTAL* ZEROSHELL DAN *USER MANAGEMENT* LDAP

Rofiatul Laily Siregar
D3 Manajemen Informatika, Fakultas Teknik, Universitas Negeri Surabaya,
rofiatulsiregar16050623015@mhs.unesa.ac.id

Agus Prihanto
Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya,
agusprihanto@unesa.ac.id

Abstrak

Pemanfaatan teknologi di lingkungan kerja atau perkantoran tentu sangat menunjang pekerjaan dalam mengakses data, informasi, dan lain banyak hal. Dalam memfasilitasi pegawai, maka layanan *wireless* menjadi pilihan tepat untuk diterapkan. Fasilitas koneksi *wireless* bisa membuat ruangan jadi lebih rapi karena tidak perlu mengatur banyak kabel, mudah untuk diakses banyak perangkat seperti *smartphone*, laptop, printer dan komputer personal pegawai itu sendiri. Layanan *wireless* ini yang sering kita sebut dengan *Wi-Fi (Wireless Fidelity)* Memang cukup banyak keuntungan dari layanan *Wi-Fi* namun tentunya ada kekurangan, diantaranya mengingat *SSID* serta *password* yang banyak dan rumit, dimana suatu kantor umumnya terdapat beberapa ruangan berbeda untuk setiap bidangnya terlebih lagi instansi tersebut memiliki gedung yang besar. Hal itu menyebabkan kesulitan dalam mengingat *SSID* serta *password* setiap ruangan. Selain itu, pengguna yang berasal dari luar lingkungan kantor asal mengatahui *password* maka dapat mengakses dengan bebas. Melihat dari permasalahan tersebut, hotspot dapat menjadi solusi yang dapat diimplementasikan pada instansi terkait. Hotspot memberi kemudahan, keamanan dan pembatasan *user* dalam hak akses. Pada penelitian ini menggunakan zeroshell sebagai *captive portal* yang akan memblok web HTTP dan HTTPS untuk meminta autentikasi terlebih dahulu sebelum diberi hak akses ke internet serta OpenLDAP merupakan salah satu *software* yang menerapkan protokol LDAP berfungsi sebagai *backend database* jaringan yang menyimpan profil *users*. Dari hasil pengujian menunjukan bahwa *captive portal* dapat memblok web HTTP dan HTTPS hanya saja di perangkat tertentu dan penngujian *users* autentikasi, autorisasi, dan akunting di LDAP dapat terpenuhi.

Abstract

Utilizing technology in work or office environments certainly supports work in accessing data, information, and many other things. In facilitating employees, wireless services became the best option for implementation. Wireless connection facilities can make the room neater because there is no need to set up many cables and easy to access many devices such as smartphones, laptops, printers and personal computers of the employees themselves. This wireless service is what we often call Wi-Fi (Wireless Fidelity). It is quite a lot of advantages of Wi-Fi services but of course there are disadvantages, including remembering SSIDs and passwords that are many and complicated, where an office generally has several different rooms for each field. Moreover, the agency has a large building. This causes difficulties in remembering the SSID and password for each room. In addition, users who come from outside the office environment as long as they know the password can access freely. Looking from these problems, hotspots can be a solution that can be implemented in related institutions. Hotspots provide convenience, security and restrictions on user access rights. In this research using zeroshell as a captive portal that will block HTTP and HTTPS webs to request authentication before being given the access to the internet and OpenLDAP is one of the software that applies the LDAP protocol to function as a backend of network databases that store users' profiles. From the test results of the test show that captive portals can block HTTP and HTTPS web only on certain devices and testing users of authentication, authorization, and accounting in LDAP can be fulfilled.

Keywords: *Hotspot, Zeroshell, Captive Portal, Authentication, Authorization, Accounting.*

PENDAHULUAN

Pemanfaatan teknologi di lingkungan kerja atau perkantoran tentu sangat menunjang pekerjaan dalam mengakses data, informasi, dan lain banyak hal. Dalam memfasilitasi pegawai, maka layanan *wireless* menjadi pilihan tepat untuk diterapkan. Fasilitas koneksi *wireless* bisa membuat ruangan jadi lebih rapi karena tidak perlu mengatur banyak kabel, mudah untuk diakses banyak perangkat seperti *smartphone*, laptop, printer dan komputer personal pegawai itu sendiri. Layanan *wireless*

ini yang sering kita sebut dengan *Wi-Fi (Wireless Fidelity).*

Memang cukup banyak keuntungan dari layanan *Wi-Fi* namun tentunya ada kekurangan, diantaranya mengingat *SSID* serta *password* yang banyak dan rumit, dimana suatu kantor umumnya terdapat beberapa ruangan berbeda untuk setiap bidangnya terlebih lagi instansi tersebut memiliki gedung yang besar. Hal itu menyebabkan kesulitan dalam mengingat *SSID* serta *password* setiap ruangan. Selain itu, pengguna yang berasal dari luar lingkungan kantor asal tahu *password* maka dapat mengakses dengan bebas.

LPP TVRI Stasiun Jawa Timur mempunyai gedung yang luas dan lima seksi bidang yang memiliki ruangan sendiri – sendri. Setiap ruang bidang juga memiliki fasilitas *Wi-Fi*, dimana koneksi internet, LAN, dan WAN (VPN-IP) baru diintegrasikan tahun 2017. Pegawai yang bekerja disana juga dapat dikatakan yang umurnya sudah tidak muda lebih banyak daripada yang masih muda, jadi dalam hal mengingat *SSID* serta *password* yang banyak dirasa sedikit menyulitkan. Dalam hal ini penerapan layanan *wireless* dengan penerapan sistem autentikasi terpusat *Single Sign-On* akan memudahkan pegawai mengingat satu akun saja untuk dapat terkoneksi internet di ruang mana pun selama di areal kantor yang tercakup sinyal *Wi-Fi*. Ini juga memudahkan administrator jaringan dalam mengubahh maupun menonaktifkan akun.

RADIUS (Remote Access Dial-In User Service) merupakan protocol keamanan komputer digunakan untuk keamanan AAA (Authentication, Autorization, and Accounting) yang diterapkan dengan model *client-server* dalam jaringan. Adapun suatu bentuk protocol *client-server* digunakan untuk mengakses direktori aktif yang terdistribusi ke dalam banyak server. Dalam perancangan sistem autentikasi dengan menerapkan keduanya akan menghasilkan kemudahan bagi pengguna yang cukup memiliki satu akun saja yang datanya disimpan secara terpusat, menjadi solusi supaya fasilitas internet hanya dinikmati oleh pengguna tertentu yang punya hak dan tanpa menyampingkan aspek keamanan yang ada.

Melihat dari permasalahan tersebut, maka pada penelitian ini akan dibuat *Implementasi Jaringan Hotspot Dengan Captive Portal Zeroshell dan User Management LDAP*.

KAJIAN PUSTAKA

Penelitian Terdahulu

Penelitian sebelumnya yang digunakan sebagai referensi dalam pembuatan Tugas Akhir yang berjudul "Implementasi Jaringan Hotspot Menggunakan *Captive Portal* Zeroshell dan *User Management* LDAP" sebagai berikut:

Judul : Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer.

Hasil : Server RADIUS berhasil melakukan binding ke server LDAP pusat yang ada di Universitas Diponegoro untuk bisa melakukan autentikasi menggunakan akun Sistem Informasi Akademik melauli perantara portal SSO (*Single Sign On)* Universitas Diponegoro. Penelitian ini diangkat untuk skripsi oleh Ahmad Herdinal Muttaqin pada tahun 2016.

Judul : Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius di SMK Negeri 1 Wanareja.

Hasil : Membangun sistem autentikasi hotspot dapat menggunakan otentikasi berbasis *captive portal* menggunakan RADIUS dan LDAP yang diinstall pada sistem operasi ubuntu sever. Penelitian ini diangkat untuk skripsi oleh Fachrizal Fahmy pada tahun 2017.

Judul : Perancangan Sistem Single Sign-On Terintegerasi pada Jaringan Universitas Multimedia Nusantara.

Hasil :Dengan pengaplikasian sistem *Single Sign On* maka setiap perubahan akan tersinkronisasi secara otomatis pada semua system karena menggunakan database kredensial. Penelitian ini diangkat untuk skripsi oleh Anthony Leonard pada tahun 2012.

Hotspot

Hotspot adalah istilah sebuah area yang bisa akses jaringan internet dengan fitur *Wi-Fi* (*Wireless Fidelity*) maka *PC*, laptop maupun perangkat *mobile* dapat mengakses internet tanpa media kabel. Jangkauan radius hotspot area kurang lebih beberapa ratus meteran tergantung dari kekuatan frekuensi atau sinyalnya.

Pengguna bisa bebas masuk dan terhubung ke *Access Point* tersebut dengan menggunakan berbagai perangkat yang dilengkapi dengan perangkat *wi-fi* sebagai penangkap sinyal. Fungsi Hotspot yaitu bisa melakukan koneksi internet seperti browsing, berkirim email, chatting, *download* dan *upload*, dan lain-lain. Hotspot biasanya terdapat di beberapa tempat umum, seperti kafe, mall, sekolah, kampus, dan bahkan alun-alun kota.

AAA

AAA merupakan program server yang menangani akses ke suatu computer/ layanan dengan menyediakan proses *Authentication, Authorization, Accounting* (AAA), ini merupakan proses validasi keaslian pengguna, memberikan hak akses dan perhitungan pengguna mengenai bandwith dana waktu layanan pengguna pada sebuah jaringan

Authentication yaitu proses identifikasi pengguna dengan mencocokan identitas yang dimasukkan seperti *username* dan password yang telah disimpan pada database jaringan yang berada di server, jika data yang dimasukkan sesuai dengan database maka proses otentikasi berhasil dan sebaliknya jika tidak sesuai maka proses otentikasi gagal.

Authorization yaitu pemeberian hak akses pada pengguna yang terdaftar pada layanan dengan memberi detail khusus sumber daya yang tersedia dan batasan yang boleh diakses.

Accounting yaitu pencatatan aktivitas *client* seperti waktu dan *bandwith.* Informasi ini disimpan pada server yang dapat digunakan sebagai kebijakan manajemen. Jadi pencatatan ini yaitu semacam *log* yang dimiliki oleh tiap pengguna.

LDAP (Light Directory Access Protokol)

LDAP adalah standar protocol dasar yang mendukung mekanisme untuk pengaksesan direktori server serta berguna untuk mengautentikasi dan menyimpan informasi umum mengenai user yang dapat digunakan untuk berbagai macam aplikasi. Informasi umum ini contohnya yaitu nama, alamat, email, nomor induk pegawai, nomor telepon, maupun akun login dan banyak data lainnya. LDAP ini juga memperbolehkan klien untuk meakukan beberapa operasi searching informasi dengan fitur filter, akses terhadap informasi spesifik di direktori server.

LDAP terlihat sama fungsinya seperti database pada umumnya yang berguna untuk menyimpan data. Namun berbeda dengan database relasional yang menggunakan tabel, kolom, dan relasi karena LDAP lebih seperti database tipe NoSql walaupun direktori server jauh lebih dulu ada. (LDAP, n.d.)

LDAP menggunakan model *client-server*, dimana *client* mengirimkan *identifier* data pada *server* menggunakan protocol TCP/IP dan s*erver* mencarinya pada DIT (Directory Information Tree) yang tersimpan di Server (Leonard, 2016). Jadi direktori server ini adalah sebuah tipe database jaringan yang menyimpan informasi yang berhirarki seperti entri pohon.

Berdasarkan penjelasan yang terdapat di *Basic Concepts* website LDAP (LDAP, n.d.), entri LDAP adalah sekumpulan dari informasi tentang sebuah entitas dimana tiap masukan terdiri dari 3 komponen utama yaitu *distuingished names* (DNs), *attribute*, dan *object class.* Berikut penjabarannya:

1. DNs

   DNs yaitu *distuingished names* atau dalam Bahasa berarti nama tidak beraturan yang maksudnya yaitu diidentifikasi unik dalam hirarki Directory Information Tree. DN yang memiliki lebih dari 1 elemen maka disebut RDNs *(Rellative DNs).* Misalnya, "uid = john.doe" mewakili RDN yang terdiri dari atribut bernama "uid" dengan nilai "john.doe". Jika RDN memiliki beberapa pasangan nilai atribut, mereka dipisahkan oleh tanda plus, seperti "givenName = John + sn = Doe". Nama dibedakan khusus terdiri dari nol RDNs (dan karena itu memiliki representasi string yang hanya string kosong) kadang-kadang disebut "null DN" dan referensi jenis entri khusus yang disebut DSE root yang menyediakan informasi tentang konten dan kemampuan server direktori.

2. *Attribute*

   Attribute dalam Bahasa yaitu atribut, menahan data untuk sebuah masukan dimana tiap atribut mempunyai tipe. Tipe atribut adalah skema elemen yang menspesifikasi bagaimana atribut harus diperlakukan oleh klien LDAP dan *server*. Semua atribut mempunyai identifier objek (OID) dan nol atau lebih nama yang dapat digunakan untuk menunjuk atribut dari tipenya.

3. *Object Class*

   Object Class dalam Bahasa yaitu kelas objek merupakan elemen skema yang menentukan koleksi tipe atribut yang mungkin terkait dengan jenis objek tertentu, proses, ataupun entitas lainnya. Setiap masukan memiliki sebuah struktur kelas objek yang mengindikasi macam dari objek dari masukan.

OpenLDAP

OpenLDAP merupakan salah satu *software* yang menerapkan protokol LDAP (Light Weight Directory Access Protocol) yang bersifat OpenSource dan tersedia diseluruh sistem operasi Linux. OpenLDAP memiliki bentuk struktur yang berhirarki (sistem pohon seperti pada file sistem linux), bukannya berformat kolom dan baris, seperti halnya database normal, sehingga memudahkan untuk memasukkan sejumlah besar detail yang mirip dalam bentuk yang terorganisir.

Di dalam OpenLDAP terdapat 2 service utama yaitu : slapd dan slurp. Slapd merupakan OpenLDAP daemon yang melayani permintaan dari klien, query dan berkomunikasi dengan backend database. Sedangkan slurp merupakan replication daemon yang berfungsi melayani replikasi data agar terus terjadi sinkronisasi data antara klien dan server (Leonard, 2016).

Dengan penggunaan OpenLDAP dalam suatu sistem, maka akan memudahkan sistem tersebut dalam melakukan manajemen pengguna, karena data pengguna terpusat pada satu sistem.

UNESA Universitas Negeri Surabaya

Captive Portal

Captive Portal merupakan suatu bentuk teknik autentikasi dan pengamanan data terhadap jaringan *network* internal ke *network* eksternal. *Captive Portal* dapat diartikan sebagai mesin r*outer* atau g*ateway* yang membatasi atau tidak mengizinkan adanya trafik sampai *user* melakukan registrasi terlebih dahulu ke dalam sistem. Ketika pengguna telah terkoneksi dengan jaringan tersebut maka terdapat halaman web yang akan memblok untuk diminta registrasi. Mekanisme yang diterapkan *Captive Portal* biasanya digunakan pada infrastruktur *wireless* seperti *hotspot* area (Walt, 2010).

Zeroshell

Berdasarkan pengertian dari website zeroshell.org (Ricciardi, n.d.), zeroshell adalah distribusi berbasis Linux yang didedikasikan untuk implementasi Router dan Firewall yang sepenuhnya dapat diatur melalui antarmuka web. Fitur yang disediakan antara lain Load Balancing dan Failover untuk beberapa koneksi internet, VPN Site to Site dan VPN Host to Site, captive portal untuk hotspot, firewall, quality of service, otentikasi dan akuntansi RADIUS, hingga pelacakan dan pencatatan koneksi jaringan.

Seperti namanya zero yang berarti nol dan shell yaitu berupa layar hitam, terminal, untuk menuliskan sintaks dalam mengelola dan konfigurasi. Jadi Zeroshell ini administrasinya bergantung pada antarmuka grafis berbasis web dengan demikian tidak perlu menggunakan shell.

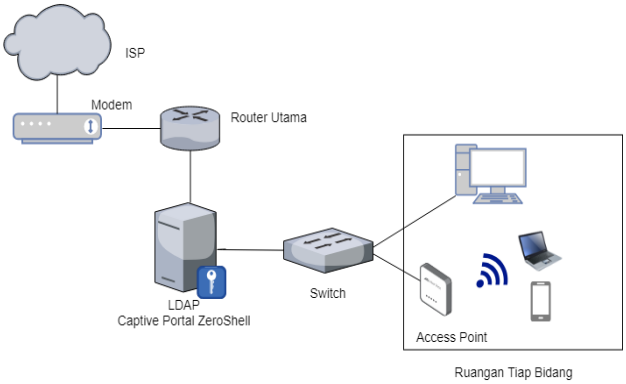
Zeroshell memiliki minimum persyaratan perangkat keras yang sederhana yaitu CPU Pentium 233 Mhz, RAM 96 MB, ATA CD-ROM atau flashdrive. Zeroshell juga dapat digunakan sebagai self-router maupun sebagai tambahan dari router utama.

METODE REKAYASA

Analisis

Dalam tahap perancangan sistem ini dimulai dengan analisis masalah yang diangkat. Dalam analisis masalah tersebut yaitu mengenai perancangan sistem hotspot di LPP TVRI Stasiun Jawa Timur. Implementasi jaringan hotspot ini menerapkan layanan *captive portal* serta *authentication, authorization, accounting* untuk mengatur terkait penggunanya. Tahap ini merupakan tahap memahami sistem yang telah berjalan, identifikasi masalah dan kebutuhan, studi literatur, dan survei lapangan. Persiapan kebutuhan masuk dalam tahap ini pula. Tahap ini mempersiapkan kebutuhan perangkat yang ada di instansi untuk menyesuaikan kelancaran tahap selanjutnya.

Perancangan Sistem



Gambar 1. Rancangan Topologi Hotspot

Tahap selanjutnya yaitu perancangan sistem. Dalam tahap ini memberi gambaran kebutuhan dan bagaimana sistem hotspot ini akan dibagun. Pada tahapan ini terdapat *design* topologi yang dirancang sebagai berikut:

1. Kebutuhan Perangkat
   a) Perangkat Keras
      1) Laptop untuk simulasi dalam perancangan sistem hotspot.
      2) PC server untuk LDAP server dan *captive portal.*
      3) PC dan *mobile client* untuk uji coba koneksi autentikasi hotspot.
      4) Router sebagai sumber internet.
      5) *Access Point* menyebarkan koneksi internet ke tiap ruang.
      6) Kabel UTP sebagai penghubung PC Server dengan *access point* dan *Router.*

   b) Perangkat Lunak
      1) Iso Zeroshell 3.8.2 untuk server.
      2) Windows XP untuk *remote.*

   c) Spesfikasi Komputer Server

Berikut spesifikasi perangkat yang digunakan simulasi dalam tabel 1, implementasi dalam tabel 2 dan *access point* dalam tabel 3:

Tabel 1. Spesifikasi PC untuk server simulasi

Sistem Operasi	Windows 10 Home 64-bit
Prosessor	Intel Core i5
RAM	8 GB
HDD	1 TB
VGA	NVIDIA GeForce 930MX

Tabel 2. Spesifikasi PC Server untuk Implemenntasi

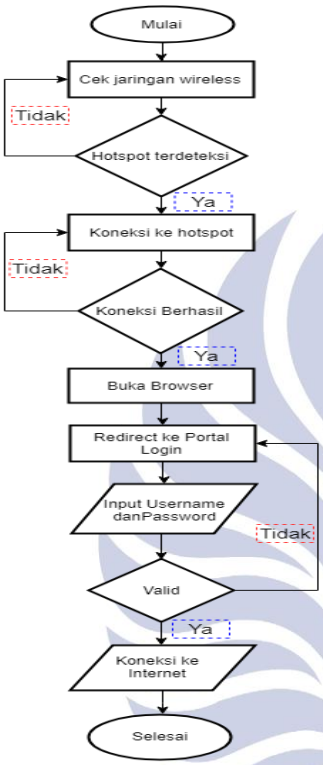
Sistem Operasi	Zeroshell 3.8.2
Prosessor	Pentium IV
RAM	512 MB

UNESA Universitas Negeri Surabaya

Tabel 3. Spesifikasi *Access Point*

Nama Router	TP Link-WR840N
Tipe Router	Wireless
Frekuensi Wi-Fi	2.4 GHz
Kecepatan Wi-Fi	Up to 300 Mbps
Mode Router	*Access Point*

Berikut ini adalah diagram alur koneksi hotspot :

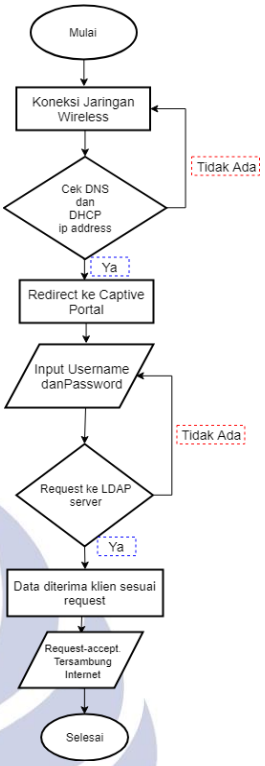


Gambar 2. Diagram Alur Koneksi ke Hotspot

Pada gambar 2 merupakan alur untuk konek ke hotspot:

1. Pertama dimulai dengan cek jaringan *wireless* yang tersedia.
2. Jika hotspot yang akan kita koneksikan terdeteksi, maka sambungkan. Jika tidak maka cek ulang pada menu wi-fi di pada perangkat yang digunakan.
3. Setelah berhasil menyambung ke hotspot, selanjutnya buka browser
4. Ketika membuka browser maka akan *redirect* ke portal login.
5. Masukkan *username* dan *password* pada kolom yang telah disediakan.
6. Setelah itu tunggu proses validasi oleh system
7. Jika *username* dan *password* sesuai maka pengguna mendapat layanan koneksi internet. Jika tida, maka aka membuka ulang portal login.

Beriku ini adalah diagram alur kerja system hotspot :



Gambar 3. Diagram Alur Kerja Sistem

Pada gambar 3 merupakan alur kerja system ketika terdapat permintaan konek ke hotspot:

1. Pertama terdapat permintaan koneksi jaringan *wireless.*
2. Sistem mengecek apakah DNS dan IP *address* tersedia, jika yam aka akan mengarahkan ke portal login, jika tidak meminta untuk koneksi kembali.
3. Pada portal login diminta untuk mengisi *username* dan *password.*
4. Ketika data telah terisi maka dilakukan permintaan di LDAP server apakah pengguna tersebut tersedia.
5. Jika yam aka data diterima *client* sesuai *request,* jika tidak maka input *username* dan *password* ulang.
6. Ketika permintaan diterima maka layanan internet tersambung dan bisa untuk digunakan.m aka akan diberi hotspot yang akan kita koneksikan terdeteksi, maka sambungkan. Jika tidak maka cek ulang pada menu wi-fi di pada perangkat yang digunakan.

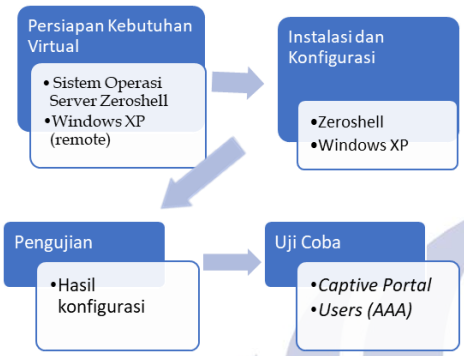
Prototipe Simulasi

Perancangan hotspot dengan *captive portal* ini akan dibuat prototipe simulasi terlebih dahulu. Dalam simulasi ini akan digunakan perangkat lunak virtualisasi *Virtualbox*. Hal ini dilakukan untuk mengetahui bagaimana sistem akan dibangun dan berjalan selain itu juga meminimalisir kesalahan pada tahap implementasi *real.* Jadi pada tahap ini merupakan tahap mencari solusi

UNESA Universitas Negeri Surabaya

kemungkinan masalah yang terjadi ketika membangun sistem.

Prototipe yang dibangun sesuai dengan bab perancangan sistem yang telah dituliskan pada poin sebelumnya hanya saja tanpa ada *access point* untuk layanan *wi-fi*. Untuk jumlah *user* yang diuji cobakan sebanyak lima akun. Alur pengerjaan prototipe yang dirancang dalam virtualbox sebagai berikut gambar 4:



Gambar 4. Alur Rancangan Prototipe

Tahap pertama menyiapkan segala kebutuhan yang akan dirancang secara virtual seperti iso zeroshell untuk server dan Windows XP untuk *remote*. Setelah mempersiapkan iso yaitu menginstall dan konfigurasi sesuai kebutuhan. Hasil konfigurasi diuji kesesuaian dengan system yang akan dirancang. Tahap terakhir dalam perancangan prototipe ini yaitu uji coba *captive portal* dan *users* (AAA). Autentikasi untuk pengecekan kesesuaian data yang dimasukkan dengan data yang diterima, autorisasi penggunaan akun secara bersamaan, dan akunting batas kuota yang telah ditetapkan dan terdapat informasi *start/stop time* serta IP *address* yang didapatkan.

Implementasi

Dalam tahap implementasi di penelitian ini dimulai dari tahap persiapan *hardware* dan *software* yang telah dirancang pada tahap desain. Tahap selanjutnya yaitu *install* Server Zeroshell, mengatur *IP Manager* untuk web remote, mengatur *setting* melalui antar muka web, ketika telah masuk dalam menu setting nya maka seluruh kebutuhan yang akan diatur dilakukan tanpa menggunakan *shell*. Fitur *captive portal* diaktifkan, setelah itu diuji terlebih dahulu apakah sudah sesuai seperti yang direncanakan, setelah sesuai maka selanjutnya *entry data users*. Jika semua tahap sudah tidak ada masalah maka tahap selanjutnya adalah pengujian sistem jaringan secara keseluruhan dan memastikan siap untuk diuji untuk beberapa *user*.

Uji Coba Sistem

Skenario pengujian system hotspot ini dilakukan sebagai tahap analisa uji coba system. Berikut adalah skenario uji coba system:

1. Pengujian Captive Portal

Pengujian ini mengharuskan *captive portal* dapat memblok semua paket data dan koneksi ke internet karena *client* harus memasukkan *username* dan *password* agar mendapat hak akses untuk menikmati layanan. Akses yang diuji yaitu web HTTP dan HTTPS. Tahap ini dilakukan untuk mengetahui dapatkah Zeroshell sebagai *captive portal* untuk memblok akses HTTP dan HTTPS ketika pengguna belum melakukan autentikasi.

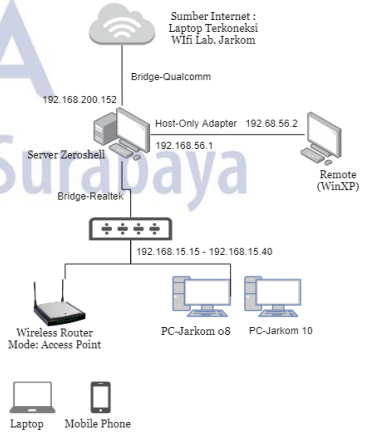
2. Pengujian Users

Pengujian ini untuk menguji terhubungnya *captive portal* ke LDAP server. Pengujian yang dilakukan yaitu autentikasi, autorisasi, dan akunting. Autentikasi yaitu identifikasi saat login memasukkan *username* dan *password*. Autorisasi yaitu akses beberapa perangkat untuk satu user atau biasa disebut *shared users*. Perangkat yang digunakan untuk uji coba diantaranya komputer kabel, laptop, dan *mobile* dengan total *user* uji coba 10 akun pegawai. Akunting yaitu mengenai besar *bandwith*, *traffic*, yang didapat oleh *user*, dan *speedtest*.

HASIL DAN PEMBAHASAN

Pada bab ini akan dijelaskan hasil dan pembahasan terkait sistem yang dibangun secara prototipe pada virtualbox dan implementasi pada perangkat fisik yang berada di Ruang Bidang Teknik LPP TVRI Jawa Timur. Adapun topologi jaringan yang telah dibuat dalam membangun hotspot ini versi prototipe dan implementas real sebagai berikut:

1. Topologi Virtual



Gambar 5. Topologi dalam Virtualbox

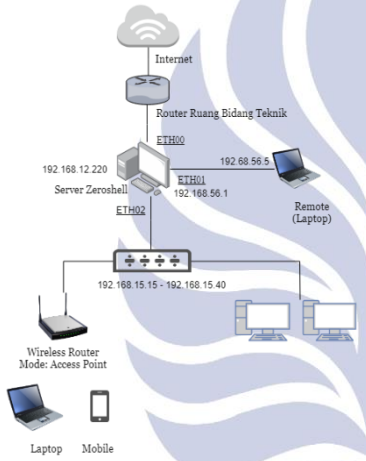
Berikut adalah penjelasan dari gambar topologi 5:

1. Dalam pengerjaan di virtualbox sumber internet berasal dari wi-fi Lab Jarkom, dimana laptop yang digunakan telah terkoneksi wi-fi tersebut.

UNESA Universitas Negeri Surabaya

2. Server zeroshell diinstal di dalam virtualbox yang berada pada laptop dan diaktifkan 3 adapter.
   a) Adapter 1 diatu *bridge* ke wi-fi Lab. Jarkom.
   b) Adapter 2 diatur *host-only* ke WinXP untuk *remote*.
   c) Adapter 3 *bridge*-realtek menggunakan kabel LAN yang dihubungkan ke switch.
3. WinXP digunakan sebagai komputer *remote* yang telah diinstal di dalam virtualbox dan terhubung ke server zeroshell. WinXP ini untuk mengkonfigurasi zeroshell menggunakan web interface yang dibuka melalui browser.
4. Switch untuk menghubungkan koneksi ke komputer kabel dan *access point.*
5. *Access point* digunakan untuk membagikan koneksi *wireless.*

2. Topologi Real



Gambar 6. Topologi Implementasi

Berikut adalah penjelasan dari gambar topologi 6:

1. Router Bidang Teknik yang telah diatur dan dikonfigurasi oleh instansi dan memberi IP address 192.168.12.220 secara DHCP melalui kabel LAN yang dihubungkan ke komputer server.
2. Komputer yang berperan sebagai server, diinstall server zeroshell dan memiliki 3 NIC (*Network Interface Card*), ETH00 mengarah ke sumber internet, ETH01 mengarah ke laptop yang berperan sebagai komputer *remote* untuk konfigurasi awal, ETH02 mengarah ke *access point*.
3. Laptop berfungsi sebagai *remote*.
4. Switch untuk menghubungkan koneksi ke komputer kabel dan *access point.*
5. Access *point* TL-WR840N diatur sebagai mode *access point* yang mendapat IP DHCP dari zeroshell.
6. Komputer yang tersambung menggunakan kabel yaitu terhubung ke switch yang telah disambungkan pada port LAN *access point*.
7. *Clients* yang terhubung ke *wireless* dapat mengkoneksikan perangkat *mobile* maupun laptop.

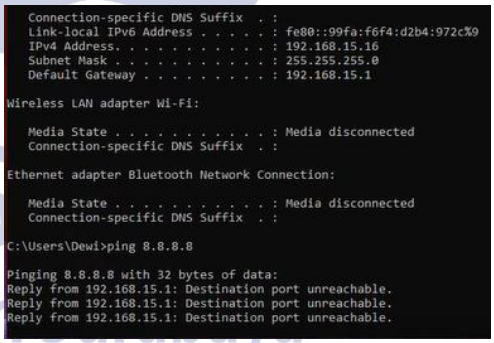
3. Uji Captive Portal

Pengujian ini mengharuskan *captive portal* dapat memblok semua paket data dan koneksi ke internet karena klien harus memasukkan *username* dan *password* agar mendapat hak akses untuk menikmati layanan. Akses yang diuji yaitu web HTTP dan HTTPS. Ketika hotspot yang telah dibuat lalu diuji baik itu simulasi maupun di Ruang Bidang Teknik LPP TVRI Stasiun Jatim memiliki hasil yang beragam. Skenario uji coba yang dirancang dituangkan dalam tabel berikut :

Tabel 4 Hasil Uji *Captive Portal*

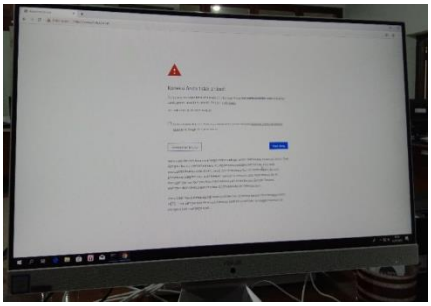
Skenario Uji Captive Portal	Hasil	
	Cable	***Wireless***
Halaman login otomatis terbuka	Tidak	Sebagian
Dapat memblok web HTTP	Ya	Ya
Dapat memblok web HTTPS	Tidak	Sebagian
Mendapat IP dengan range 192.168.15.15 – 192.168.15.40	Ya	Ya

Setelah dilakukan uji coba, perangkat yang telah terkoneksi wi-fi dengan SSID TVRI JATIM, hasilnya yaitu untuk perangkat yang terhubung dengan kabel mendapat notifikasi *no internet access*. Sehingga dilakukan cek ip yang didapat apakah sesuai dengan *range IP* yang telah diatur dan hasilnya sesuai namun ketika coba untuk ping menghasilkan respon "*Destination port unreachable"* seperti pada gambar 7:



Gambar 7. Hasil Ping PC Sebelum Login

Hal itu terjadi karena perangkat belum memasukkan *username* dan *password* pada halaman login. Ketika membuka browser tidak *redirect* otomatis ke *captive portal* sehingga harus dilakukan manual. Sesuai skenario uji yang dirancang yaitu pertama dilakukan untuk membuka web yang HTTPS dan hasilnya menunjukkan bahwa sertifikat tidak resmi seperti pada gambar 9, sehingga tidak bisa membuka laman tersebut karena belum melakukan login namun *captive portal* juga tidak dapat memblok.

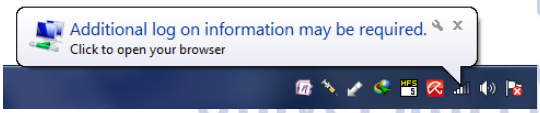


Gambar 8. Hasil Uji *Captive Portal* PC

Untuk hasil uji koneksi *wireless*, halaman login yang otomatis terbuka hanya pada sebagian perangkat *mobile*. Karena tidak semua perangkat *mobile* otomatis *redirect* langsung ke portal login. Dalam uji coba koneksi ke hotspot, merk *mobile phone* yang digunakan diantaranya: Samsung, iphone, Samsung, vivo dan advan. Hasilnya yang dapat *redirect* langsung ke halaman login hanya vivo dan advan. Untuk laptop sama seperti komputer kabel yaitu harus membuka browser terlebih dahulu.

Uji selanjutnya yaitu dengan membuka web HTTP dan *captive portal* berhasil memblok dengan menampilkan halaman login yang mengharuskan klien yang akan menggunakan layanan internet memasukkan *username* dan *password*.

Uji captive portal pada perangkat non-cable atau wireless dilakukan menggunakan mobile maupun laptop dan memiliki hasil yang beragam pula. Terdapat perangkat yang otomatis membuka browser dan *redirect* ke *captive portal*. Hasil dari perangkat lain juga terdapat notifikasi bahwa klien harus login sehingga jika notifikasi tersebut di klik maka otomatis membuka browser dan menampilkan halaman login. Pada perangkat mobile notifikasi yang muncul yaitu "*Sign in to* TVRI JATIM*"* dan untuk komputer terdapat notifikasi *"Addition log on information may be required"* seperti gambar 9 :



Gambar 9. Notifikasi Sign-in

Untuk perangkat yang berhasil otomatis membuka halaman login diuji kembali dengan tidak mengisi username dan password namun digunakan untuk membuka halaman web HTTPS dan hasilnya sebagian perangkat selalu *redirect* ke captive portal dan yang lain tidak bisa dengan menampilkan sertifikat tidak resmi maupun dianggap sedang offline.

Perangkat yang berhasil otomatis redirect dan blok web HTTPS dilakukan uji sekali lagi dengan memaksakan membuka web HTTP sebelum login dan hasilnya tetap saja selalu *redirect* ke *captive portal*.

4. Pengujian *Users (*Autentikasi, Autorisasi, Akunting*)*

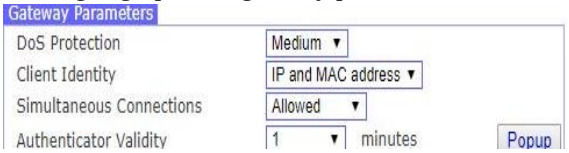
Pengujian ini untuk menguji terhubungnya *captive portal* ke LDAP server. Dalam pembuatan hotspot disini LDAP sebagai database jaringan saja dimana zeroshell telah terintegrasi dengan OpenLDAP sebagai backend. Pengujian yang dilakukan yaitu autentikasi, autorisasi, dan akunting. Ringkasan uji yang dilakukan tertuang pada tabel :

Tabel 5. Hasil Uji *Users*

Point yang Diuji	Keterangan Hasil
Autentikasi	Berjalan sesuai perencanaan dapat mengidentifikasi *username* dan *password* sesuai data pada database.
Autoriasi	Tidak terdapat jumlah pembatasan perangkat yang dapat login secara Bersama. Manajemen bandwith yang berjalan hanya berlaku untuk global bandwith saja.
Akunting	Dapat diberi batasan kredit *traffic* yang telah diatur. Terdapat log *strart* dan *stop time* koneksi, session, *traffic*, *IP* dan *MAC address* perangkat yang sedang maupun pernah terkoneksi.

Pada zeroshell uji users yang didapat untuk autentikasi berjalan seperti yang dirancang yaitu username dan password dapat diidentifikasi sesuai atau tidak dengan data di database jaringan. Ketika salah memasukkan username dan password maka akses ditolak lalu captive portal akan reload dan meminta untuk mengisi ulang.

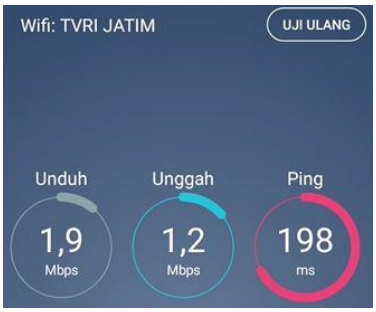
Untuk autoriasi pada zeroshell yaitu pembatasan perangkat yang dapat terkoneksi secara bersamaan hanya bisa dipilih '*allowed*' atau '*not allowed*'. Dalam perencanaan uji sebelumnya akan diatur pembatasan koneksi beberapa perangkat berdasarkan grup user namun fitur itu tidak terdapat di zeroshell. Fitur untuk penggunaan perangkat saat koneksi secara bersamaan yaitu *Simultaneous Connections* berada pada menu captive portal dengan grup menu gateway parameter.



Gambar 10. Fitur Perangkat Koneksi Bersama

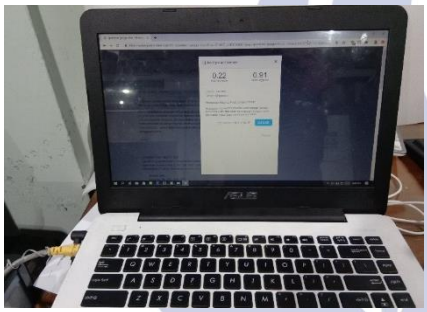
Selain pengaturan perangkat unttuk konek bersama, pembatasan bandwith juga terdapat pada fitur zeroshell. Limitasi bandwith dapat diatur melalui menu QOS. Dalam membatasi bandwith yang didapat oleh user ini hanya bisa

diatur secara global saja yaitu diatur batas maksimal 2 Mbps dan *guaranteed* 100kbps. Sehingga hasil yang di dapat dari beberapa user yang konek ke wi-fi TVRI JATIM lalu melakukan *speedtest*, sebagai berikut :



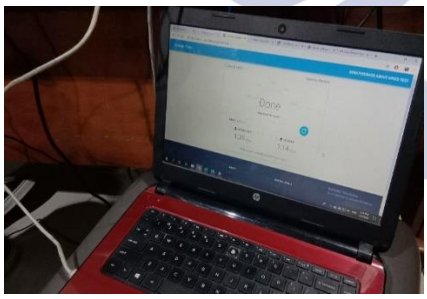
Gambar 11. *Speedtest* Akun VIP

Gambar 11 menunjukkan hasil *speedtest* tersebut berdasarkan akun direksi yang konek internet dengan *mobile phone*.



Gambar 12. *Speedtest* Akun Harian

Hasil *speedtest* tersebut berdasarkan akun harian yang terdapat pada gambar 12 dengan konek internet melalui *PC*, hasilnya yaitu *download* 0,22 Mbps dan *upload* 0,91 Mbps.

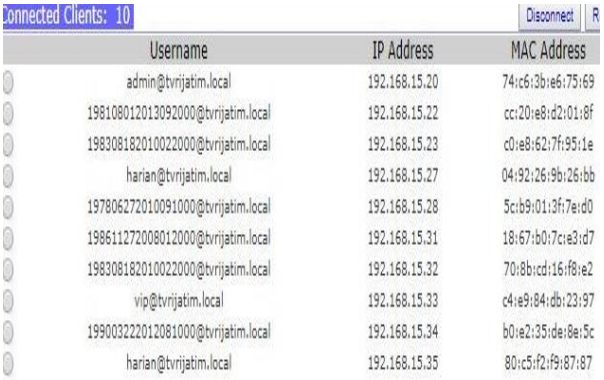


Gambar 13. *Speedtest* Akun Karyawan

Hasil *speedtest* gambar 13 tersebut berdasarkan akun karyawan yang konek internet dengan *PC*, hasilnya yaitu downlaod 1,39 Mbps dan *upload* 1,34 Mbps.

Gambar 14. *Speedtest* Akun Harian

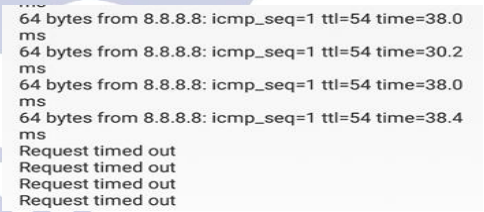
Hasil *speedtest* pada gambar 14 tersebut berdasarkan akun harian yang konek internet dengan *mobile*, hasilnya yaitu downlaod 0,17 Mbps dan *upload* 1,39 Mbps. Berikut gambar 15 adalah cuplikan zeroshell ketika terdapat *users* sedang terhubung :



Gambar 15. *Connected Clients*

Selain manajemen bandwith terdapat limitasi traffic yang masuk dalam point akunting yang fiturnya tersedia di zeroshell. Hasil dari uji coba limitasi *traffic* yaitu akun tamu diberi batasan traffic 200 Mb dan ketika akun tersebut terkoneksi dan telah mencapai maksimal maka saat itu juga akun tersebut akan dipaksa *disconnect* dan tidak dapat menggunakan layanan internet lagi seperti pada gambar 16 dari log yang ada di zeroshell dan gambar 17 berdasarkan ping yang dilakukan *client.*

Gambar 16. Log *Accounting* Zeroshell



Gambar 17. Hasil Ping Akun Tamu

PENUTUP

Simpulan

Kesimpulan yang diperoleh dari penelitian "Implementasi Jaringan Hotspot Dengan *Captive Portal* Zeroshell dan *User Management* LDAP" adalah sebagai berikut:

1. Captive portal zeroshell dapat memblok web HTTP dan HTTPS hanya saja di perangkat tertentu.
   a) Fitur captive portal zeroshell dapat berjalan dengan baik dengan bantuan Kerberos 5 yang mengautentikasi, RADIUS sebagai jembatan ketika proses autentikasi dari halaman login dan cek data pada database LDAP.

b) Tampilan halaman login yang disediakan pada fitur *captive portal* yaitu *default* dan *customize*. Namun halaman yang kustom tidak sepenuhnya dapat dirubah.

2. OpenLDAP hanya sebagai database jaringan yang berguna sebagai database menyimpan data *users.*
   a) Autentikasi berjalan dengan baik.
   b) Autorisasi dapat digunakan untuk koneksi secara bersamaan namun tidak ada batasan perangkat.
   c) Fitur akunting yang diterapkan berupa limit bandwith dan *traffic* namun setelah diuji yang berjalan hanya *traffic* saja dan bandwith manajemen yang dibuat di kelas akunting berdasarkan grup belum terlalu stabil. Limit bandwith yang didapat berdasarkan *global bandwith* yang diatur.

Saran

Agar fitur captive portal dapat diterapkan sepenuhnya untuk hotspot suatu instansi, adapun saran untuk menjadikan penelitian ini menjadi lebih baik yaitu :

1. Mengatur sertifikat resmi X.509 sebagai sertifikat resmi terpercaya yang dapat menyempurnakan fitur *captive portal*.
2. Mengintegrasikan zerotruth untuk tampilan *captive portal* yang lebih fleksibel untuk dikonfigurasi.
3. Menerapkan auotorisasi dengan limitasi bandwith berdasarkan grup pengguna.

DAFTAR PUSTAKA

BPS Statistics Indonesia. (2015). Statistik Telekomunikasi Indonesia. In *Katalog 8305002.*

Fahmy, F. (2017). Sistem Autentikasi Hotspot Menggunakan LDAP dan RADIUS di SMK Negeri 1 Wanareja. *Skripsi Teknik Komputer Universitas AMIKOM Yogyakarta*.

Fauzi, M. I. (2011). *MANAJEMEN BANDWITH MENGGUNAKAN ROUTER MIKROTIK*. Retrieved April 8, 2019, from Pengajuan Tugas Akhir: http://m-ihsan-fauzi.blogspot.com/p/manajemen-bandwith-menggunakan-router.html

LDAP. (n.d.). *Basic of LDAP Concepts*. Retrieved Februari 2019, from LDAP.com: https://ldap.com/basic-ldap-concepts/

LDAP. (n.d.). *Why Choose LDAP?* Retrieved Februari 2019, from LDAP.com: https://ldap.com/why-choose-ldap/

Leonard, A. (2016). Perancangan Single Sign-On Terintegerasi Pada Jaringan Universitas Multimedia Nusantara. *Skripsi Sistem Komputer Universitas Multimedia Nusantara Tangerang*.

Mikrotik Id. (2008). TCP/IP (Bagian -1) : Pengenalan OSI Layer. *Tips dan trik*. Retrieved Februari 2019

Muttaqin, A. H. (2016). Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer. *Skripsi Sistem Komputer Universitas Diponegoro*.

Ricciardi, F. (n.d.). *Homepage*. Retrieved Februari 2019, from Zeroshell Linux Router: https://zeroshell.org/

Sukaridhoto, S. (2014). *Buku Jaringan Komputer 1*. Politeknik Negeri Surabaya.

Talasila, S. a. (2016). *RADIUS Protocol*. Retrieved Februari 2019, from slideplayer: https://slideplayer.com/slide/9072353/

TVRI, B. S. (Ed.). (2010). Company Profile TVRI Jatim. Surabaya, Jawa Timur.

VirtualBox. (n.d.). Retrieved Februari 2019, from Wikipedia: https://id.wikipedia.org/wiki/VirtualBox

Walt, D. v. (2010). *Manage your network resources with freeradius*. Birmingham: Packt Publishing Ltd.

UNESA Universitas Negeri Surabaya