IMPLEMENTASI MONITORING JARINGAN MENGGUNAKAN CACTI DAN WEB AUTHENTICATION MENGGUNAKAN KERBEROS PADA MAN 1 BOJONEGORO

Dwi Risza Budi Raharja[1] **Periyadi[2]** **Anang Sularsa[3]**

[1,2,3]Fakultas Ilmu Terapan - Universitas Telkom
[1]dwirisza14@gmail.com [2]periyadi@tass.telkomuniversity.ac.id[3]anang@tass.telkomuniversity.ac.id

Abstrak

Di dalam dunia pendidikan, hampir semua sekolah sudah menggunakan jaringan internet untuk setiap proses dari belajar mengajar mereka. Tetapi banyak dari sekolah tersebut kurang memperdulikan tentang *bandwidth* dan keamanan pada jaringan. Selain itu masih banyaknya siswa yang membolos pada jam pelajaran yang berlangsung. Untuk mengatasi beberapa masalah tersebut maka akan dibangun jaringan internet untuk memudahkan siswa dalam belajar mengajar, selain itu akan dilengkapi juga dengan HTB *Tools, web authentication* dengan kerberos 5 pada zeroshell, monitoring dengan menggunakan *cacti* untuk memudahkan admin dalam mengawasi *performance* dari server, dan sistem *sms gateway* yang terintegrasi dengan kehadiran didalam web portal. Dari beberapa sistem yang dibangun dapat memberikan solusi dari Madrasah Aliyah Negeri 1 Model Bojonegoro. Sehingga dapat disimpulkan bahwa Madrasah Aliyah Negeri 1 Bojonegoro memiliki sistem baru yang di dalamnya terdapat server authentikasi dan server utama yang didalamnya terdapat web authentikasi dengan kerberos, manajemen bandwith, monitoring server dengan cacti, dan web portal yang terintegrasi dengan sistem sms gateway.

Kata Kunci: ***Kerberos5, web authentication, zeroshell, HTB tools,SMS gateway.***

Abstract

In education, nearly all scholls are already using internet to get the process of learning. But amoung of schools are less care about bandwith and netwokr seurity. In addition there are many students who are absent during the lesson. To overcome some of these problems, so that it will be built the internet network to facilitate students in learning, otherwise it will be equipped with *HTB tools, web authentication* with *kerberos5* on *zeroshell*, monitoring the performance from server by cacti to make admin easier in monitoring, and the *SMS gateway* system are integrated with presence web portal. Most of the systems that have been built, it hopes that could provide a solution to Madrasah Aliyah Negeri 1 Model Bojonegoro. It can be concluded that Madrasah Aliyah Negeri 1 Bojonegoro have a new system, there is authentication server and the main server in which there is information with kerberos authentication, bandwith management, server monitoring with cacti, and a web portal that is integrated with system sms gateway.

Keywords: Kerberos5, web authentication, zeroshell, HTB Tools, Sms Gateway.

1. Pendahuluan

Di dalam dunia pendidikan hampir semua sekolah sudah menggunakan jaringan internet untuk setiap proses belajar mengajar mereka. Tetapi hampir dari semua sekolah yang memakai jaringan internet tidak memperdulikan kuota yang mereka ambil dengan jumlah siswa yang memakai pada suatu sekolah tersebut. Sehingga itu mengakibatkan kurang nyamannya siswa dalam kegiatan belajar mengajar. Oleh sebab itu diperlukannya sistem monitoring pada jaringan suatu sekolah untuk memonitor per kbps jaringan yang dapat dikelola oleh setiap user yang ada pada Madrasah aliyah Negeri 1 Bojonegoro. Serta untuk proses pengamanan jaringan dibuatlah yang disebut *web authentication* dengan menggunakan *kerberos5* pada *zeroshell* sehingga menjadikan lebih aman jaringan yang dipakai pada sekolah tersebut dan hanya guru dan siswa lah yang namanya tercantum di dalam data base *kerberos* yang bisa mengakses jaringan tersebut.

Selain itu juga untuk mengurangi banyaknya siswa yang membolos pada jam pelajaran, maka dibangunlah sms gateway yang terintegrasi dengan kehadiran pada web portal yang akan mengirimkan sms kepada orang tua siswa berdasarkan kehadiran mereka yang di masukkan oleh guru.

2. Tinjauan Pustaka

1.1 Monitoring Jaringan Komputer

Monitoring jaringan komputer adalah merupakan proses untuk pengumpulan data dan melakukan sebuah analisis terhadap sebuah data-data pada lalu lintas jaringan dengan tujuan untuk memaksimalkan seluruh data yang dimiliki oleh jaringan komputer tersebut. Monitoring data merupakan bagian dari

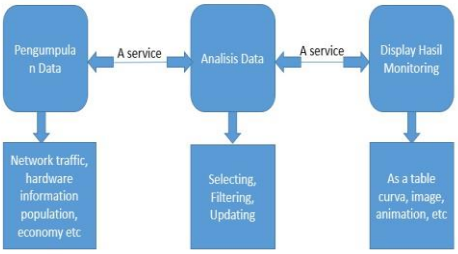
sebuah manajemen jaringan yang dapat dibagi menjadi 2 bagian yaitu :

a. *Connection Monitoring*
   Connection Monitoring adalah sebuah teknik monitoring dengan melakukan *test ping* antara *monitoring station* dan *device target*, sehingga akan diketahui secara langsung apabila koneksi terputus.
b. *Traffic Monitoring*
   Traffic monitoring merupakan sebuah teknik jaringan yang melihat dari sebuah lalu lintas dari data itu sendiri atau melihat dari aktual *paket traffic* pada jaringan dan nantinya akan menghasilkan sebuah laporan berdasarkan *traffic* jaringan itu sendiri.

Monitoring jaringan tersebut mempunyai peranan penting dalam dunia jaringan mereka berfungsi untuk menjaga stabilitas dari jaringan dan mempermudah untuk admin mengecek ketika terjadi kesalahan pada jaringan gateway, *server* , maupun, user. Dan juga berfungsi untuk memberitahukan kepada administrator ketika ada trouble jaringan dan juga mempermudah untuk menganalisi troubleshooting pada sebuah jaringan.

Selain itu secara garis besar tahapan dari sistem monitoring jaringan terbagi dalam 3 proses yaitu :

a. Proses di dalam pengumpulan data monitoring.
b. Proses d dalam analisis data monitoring.
c. Proses di dalam menampilkan sebuah data hasil monitoring.



Gambar 2 - 1 Diagram Monitoring

Pengumpulan data atau sumber data dapat berupa sebuah *network traffic*, informasi mengenai hardware atau sumber-sumber lain yang berkaitan dengan informasi dari sebuah data. Sedangkan analisis data diperoleh dari pemilihan data yang terkumpul atau yang sudah masuk di dalam pengumpulan data. Data ini bisa saja menggunakan manipulasi data sehingga akan diperoleh informasi yang akan diharapkan. Sedangkan untuk tahapan *display* hasil monitoring data biasanya berupa pemunculan tabel atau kurva yang didalamnya sudah terisi oleh banyaknya data dari proses pengumpulan data dan analisis data.
Untuk proses-proses di atas biasa disebut dengan sistem monitoring yang mempunyai arti sistem yang berbentuk service dari suatu proses-prose yang secara terus menerus berjalan pada sebuah interval waktu tertentu. Pada proses ini pengumpulan yang dijalankan biasanya dapat berupa pengumpulan data dari objek yang telah berhasil dimonitor atau dapat saja dilakukan dengan melakukan sebuah analisis data yang telah diperoleh dan menampilkanny a. Proses tersbut biasa dikenal dengan proses interval yang berbeda.

1.2 Cacti

Cacti adalah aplikasi monitoring *open source* dan berbasiskan web. Cacti pada umumnya dibuat untuk membuat data grafik seperti kinerja CPU dan bandwidth. Cacti khususnya digunakan pada antar muka switch dan router jaringan lewat snmp untuk memonitor trafik jaringan. Cacti sendiri merupakan complete network graphing solution yang didesain dengan memanfaatkan PRD tool untuk data storage dan fungsi dari graphing tersebut. Di dalam cacti terdapat beberapa fitur yang digunakan untuk proses monitoring dari cacti tersebut. Fitur dari cacti tersebut adalah :

a. Memory Usage berfungsi untuk mengetahui memory yang dipakai oleh server, seberapa besar memory dari server tersebut terpakai.

b. Logged in user berfungsi untuk mengetahui dari user yang terhubung kepada server tersebut.

c. Processor berfungsi untuk mengetahui processor dari server tersebut.

1.3 Kerberos

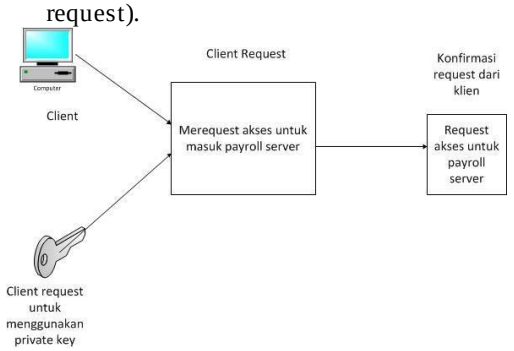
Kerberos merupakan sebuah sistem yang menyediakan strong authentication untuk aplikasi client/server yang nantinya dikombinasikan dengan menggunakan secret key dan public key. Karberos ini menggunakan sebuah server yang terpusat yang berfungsi untuk mengotentikasi user dan mengendalikan akses terhadap sumber data jaringan. Protokol karberos mempunyai 3 cara protokol di antaranya adalah sebagai berikut :

a. *Authentication service* (AS) : yang berfungsi oleh *key distribution center (*KDC*)* untuk menyediakan tiket kepada client.
b. *Ticket Granting Service* (TGS) : digunakan oleh *key distribution center* untuk mendistribusikan kunci sesi layanan dan tiket yang diasosiasikan dengannya.
c. *Client/server* : yang digunakan oleh klien untuk mengirimkan sebuah tiket sebagai pendaftaran kepada sebuah layanan.

Cara kerja kerberos adalah sebagai berikut :

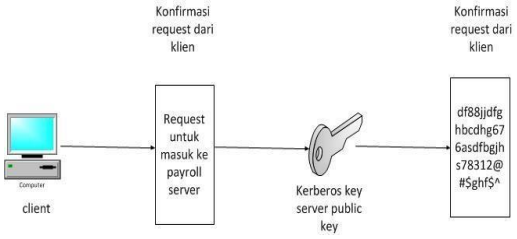
a. Client membuat request kepada authentication server, dan meminta untuk

mengotentikasi dirinya terhadap server, lalu kemudian request tersebut diberi digital signature dengan menggunakan private key client (digitally signed client request).



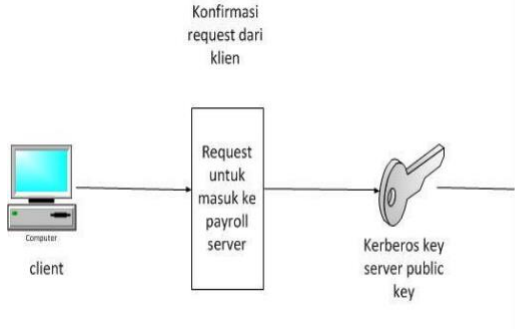
Gambar 2 - 2 Client Request Payroll

b. Client mengenkripsi *digitally signed request* menggunakan public key dari server kerberos.



Gambar 2 - 3 Masuk Public Key

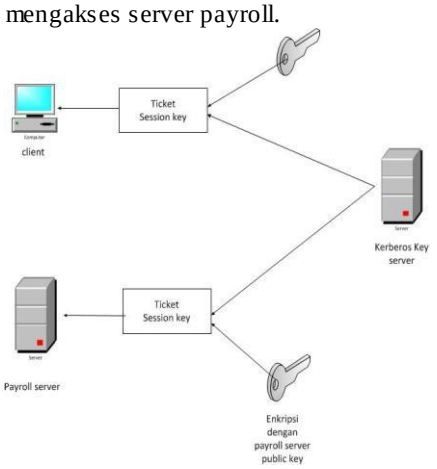
c. Client mengirimkan *digitally signed* and *encrypted* request ke server kerberos, lalu server kerberos mendeskripsikan request menggunakan private key dan meng-otentikasi pengirim request dengan cara memverifikasi digital signature perngirim menggunakna public key pengirim request. Dan jika server kerberos memiliki seluruh database public key dari authorized maka tidak perlu mengandalkan pengirim untuk memverifikasi public key pengirim.



Gambar 2 - 4 Request ke Kerberos Server

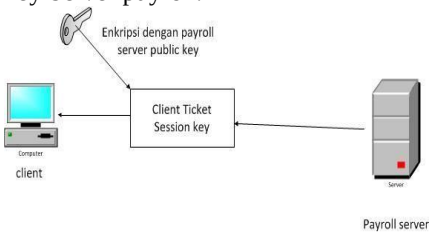
d. Jika server kerberos telah menerima request

dan mengotentikasi identitas dari pengirim request, maka server memverifikasi bahwa client memiliki otorisasi untuk mengakses sumber daya jaringan yang diminta. Dan jika server kerberos sudah menentukan bahwa client bisa mengakses maka akan mengirimkan session ticket untuk mengakses server payroll.



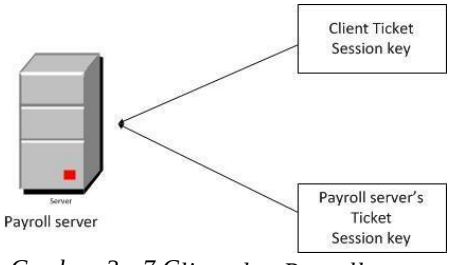
Gambar 2 - 5 Enkripsi Tiket

e. Client kemudian mengirimkan copy dari ticketnya ke server payroll lalu kemudian sebelum client mengirimkan tiket, client mengenkripsi ticket menggunakan public key server payroll.



Gambar 2 - 6 Payroll Server

f. Ketika menerima tiket yang dienkripsi dari client, maka server akan mendeskripsi ticket menggunakan private key server, lalu server paryroll kemudian membandingkan ticket yang diterima dari client dengan ticket yang berasal dari server kerberos server. Dan disaat itu jika ticket sesuai maka client akan diperbolehkan untuk terhubung kepa da server, dan jika ticket tidak sesuai maka client akan ditolak.



Gambar 2 - 7 Client dan Payroll

1.4 Database

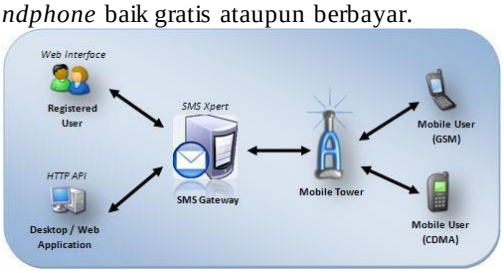
Basis data adalah kumpulan dari suatu data-data yang saling berhubungan secara logika yang isinya didesain untuk memenuhi kebutuhan informasi dari suatu perusahaan. Beberapa istilah umum yang sering dipakai dalam *database* adalah sebagai berikut :

a. *Field* yaitu sekumpulan kecil dari kata atau sebuah deretan dari angka-angka.
b. *Record* yaitu sekumpulan dari field yang berelasi secara logis.
c. *File* yaiut sekumpulan dari record yang berelasi secara logis.
d. *Entity* yaiut orang, tempat, benda, atau kejadian yang berkaitan dengan informasi yang disimpan.
e. *Attribute* yaitu setiap karakteristk yang menjelaskan suatu *entity*.
f. *Primary key* yaitu sebuah field yang nilainya berguna untu menghubungkan primary keu yang berada pada tabel yang berbeda.

Database merupakan salah satu bagian yang penting dalam sistem informasi ini. Apabila orang yang menyebut *database*, biasanya dikaitkan dengan *sofware*/perangkat lunak yang dapat menyimpan data dalam suatu sistem dan dapat diambil kembali kapan saja dan darimana saja. Padahal biasanya *database* tidak hanya merupakan perangkat lunak, tetapi jauh sebelum digunakan teknologi dalam pembuatan *database*, orang telah melakukan dokumentasi secara manual dan semuanya berupa hardcopy/material.

1.5 Sms Gateway

SMS (*Short messages services*) merupakan salah satu layanan dari berbagai macam operator seperti gsm dan cdma. Teknologi sms memungkinkan untuk mengirim pesan alphanumerik singkat dari sebuah ponsel ke ponsel yang lainnya. Dan dari situlah akhirnya berkembang untuk menciptakan sebuah portal yang besar yang didalamnya tersedia layanan pengiriman SMS dari website ke sebuah nomor *handphone* baik gratis ataupun berbayar.



Gambar 2 - 8 Struktur SMS Gateway

1.6 Gammu

Gammu adalah sebuah aplikasi platform yang berfungsi untuk menjembatani antara database pada sms gateway dengan database pada sms devices. Aplikasi gammu berupa daemon yang berjalan secara background. Pada setiap saat gammu memonitoring sms devices dan sms gateway. Ketika ada sms pada inbox sms devices maka gammu akan memindahkannya kedalam database sms gateway begitupun juga sebaliknya ketika mengirim pesan pada sent item maka akan dipindahkan ke dalam database.

1.7 PHP

Gambar 2 - 9 PHP

PHP adalah kependekan dari "*hypertext preprocessor*", jadi *PHP* adalah bahasa sripting web *HTML-embedded*. Ini berati kode *PHP* dapat disispkan kedalam HTML halaman web. Ketikas ebuah halaman *PHP* diakses, kode *PHP* dibaca oleh *server*/output dari fungsi *PHP* pada halaman biasanya dikembalikan sebagai kode *HTML*, yang dapat dibaca oleh browser karena kode *PHP* diubah menjadi HTML sebelum halaman dibuka, jadi pengguna tidak akan dapat melihat kode *PHP* pada halam ini. Ini membuat halam *PHP* cukup aman utnuk mengakses *database* dan informasi aman lainnya.

Contoh program *PHP* :

```
<?php
Echo "hello world";
?>
```

1.8 XAMPP

Gambar 2 - 10 XAMPP

Xampp merupakan singkatan dari (empat sistem operasi apapun), *apache*, *mysql*, *PHP*, *perl*. Xampp merupakan tool yang dibuat untuk menyediakan paket perangkat lunak kedalam satu buah paket. Sedangkan pada dalam paketnya sudah terdapat apache (web *server*), mysql (*database*), *PHP* (*server* side scripting). *Perl*, *FTP server*, *PHPMyadmin* dan berbagai pustaka bantu lainnya. Bagian XAMPP yang biasa digunakan pada umumnya.

1.9 DNS (Domain Name Server)

DNS(*Domain Name Server*) adalah sebuah server yang berfungsi untuk mengetahui dari ip address server. Fungsi yang paling penting dan utama dari DNS adalah untuk menerjemahkan nama dari host yang menjadi alamat IP ataupun sebaliknya sehingga itu akan mempermudah pengguna untuk mengingat nama host dari masing-masing client. DNS dibedakan menjadi dua, ada yang disebut sebagai *Primary Name Server* yaitu sebuah DNS yang bertanggung jawab dalam hal mengingat IP address

dari sebuah komputer. Ada juga yang biasa disebut dengan *Secondary Name Server* adalah sebuah DNS server yang memperoleh datanya berdasakan data-data domain dan *sub domain primary*.

*1.10 DHCP (*Dynamic Host Configuration Protocol*)*

DHCP merupakan sebuah layanan yang berfungsi sebagai memberikan alamat ip secara otomatis kepada client ketika client terhubung dengan server. Komputer yang meminta alamat IP biasa disebut dengan DHCP Client sedangkan yang memberi disebut dengan DHCP server. DHCP sangat membantu admin ketika membangun sebuah jaringan karena admin tidak perlu mensetting secara manual tetapi cukup dengan menkonfigurasi DHCP server, sehingga client yang terhubung pada jaringan tidak perlu untuk mengkonfigurasi ulang secara manual.

1.11 WEB SERVER

Web server adalah sebuah aplikasi yang berfungsi untuk memberikan layanan data yang nantinya berfungsi menerima HTTP atau HTTPS dari klien lalu kemudian mengirimkan kembali pada web browser yang datanya berbentuk HTML.

*1.12 SNMP (*Simple Network Protocol*)*

SNMP (*Simple Network Protocol*) adalah sebuah protocol yang bekerja pada layer aplikasi pada OSI layer. Snmp menyedakan komunikasi yang biasa disebut dengan agent dan manager yang berfungsi untuk melakukan monitoring atau mengatur perangkat-perangkat network seperti switch, router, pc, printer dan perangkat network yang lainnya. SNMP manager merupakan aplikasi network management yang berjalan pada PC dan agent adalah sofware yang berjalan pada device yang akan di atur prosesnya.

*1.13 HTB Tools (*Hierarchical Token Bucket*)*

HTB (*Hierarchical Token Bucket*) merupakan aplikasi yang berfungsi untuk mengatur pembagian bandwidth, pembagian bandwtih yang dibuat merupakan secara hirarki yang dibagi-bagi kedalam kelas sehingga mempermudah pengaturan bandwidth. Sedangkan HTB Tools merupakan aplikasi yang dipakai untuk manajemen bandwidth. Hierarchical Token Bandwidth (HTB) menggunakan Token Bucket Filter (TBF) sebagai estimator untuk menentukan apakah suatu kelas/prioritas berada dalam keadaan underlimit, atlimit atau overlimit. TBF bekerja dengan dasar algoritma ember *token*, setiap paket yang akan dikirimkan harus memiliki token yang berada dalam ember token, jika token tak tersedia di dalam ember maka paket-paket yang akan dikirimkan harus menunggu sampai tersedia token yang cukup untuk mengirimkan paket yang sedang menunggu. Implementasi TBF terdiri dari sebuah *buffer (bucket)*, yang secara konstan diisi oleh beberapa informasi virtuak yang dinamakan *token*, pada *link* yang spesifik. Parameter paling penting dari bucket adalah ukurannya, yaitu banyaknya token yang dapat disimpan. Setiap token yangmasuk mengumpulkan satu paket yang datang dari antrian data dan kemudian dihapus dari bucket. Dengan menghubungkan algoritma ini dengan dua aliran token dan data, akan didapati tiga buah kemungkinan skenario :

1. Data yang datan pada TBF memiliki *link* yang sama dengan masuknya *token*. Dalam hal ini, setiap paket yang masuk memiliki token-nya masing-masing dan akan melewati antrian tanpa adanya *delay*.

2. Data yang datang pada TBF memiliki *link* yang lebih kecil daripada *link* token. Hanya sebagian token yang dihapus pada output pada tiap paket data yang dikirim ke antrian, dan token akan menumpuk, memenuhi ukuran bucket. Token yang tidak digunakan kemudian akan dapat digunakan untuk mengirimkan data pada kecepatan yang melampau *link token* standar, ini terjadi jika ada ledakan data yang pendek.

3. Data yang datang pada TBF memilik *link* yang lebih besar daripada *link* token. Hal ini berarti bucket akan segera kosong dari token, yang menyebabkan TBF akan menutup alirannya untuk sementara. Hal inilah yang dinamakan situasi overlimit. Jika paket-paket tetap datang, maka paket-paket akan segera dibuang (--, Penjelasan Hierarchical Token Bucket, 2007).

1.14 Zeroshell

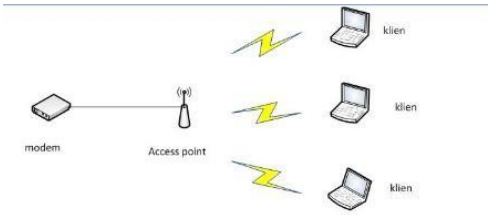
Zeroshell merupakan distro Linux untuk Network Appliance, baik di server maupun di perangkat embedded. Didalamnya terdapat beberapa aplikasi di dalamnya antara lain : LDAP, RADIUS, VPN, Qos, Router, DNS, Firewall, HTTP Poxy. Zeroshell merupakan distro linux independen sehingga zeroshell tidak dapat ditambahkan service dengan secara manual.

3. Analisis dan Perancangan

3.1 Gambaran Sistem Saat Ini

Gambaran umum sistem pada madrasah aliyah negeri 1 bojonegoro, pihak sekolah sudah mempunyai jaringan internet dengan berakseskan melalui satu modem yang diakses oleh siswa, itu sangat tidak efisien dan kurang menjangkau untuk jangkauan seluruh sekolah. Selain itu madrasah

aliyah negeri 1 bojonegoro juga belum memiliki aplikasi yang memumpuni untuk kegiatan belajar mengajar siswa.

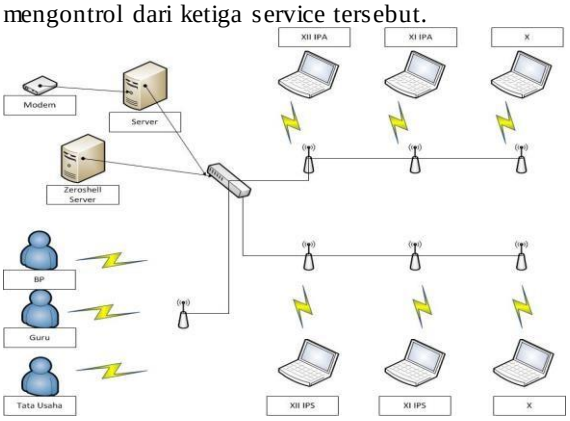


Gambar 3 - 1 Topologi Awal

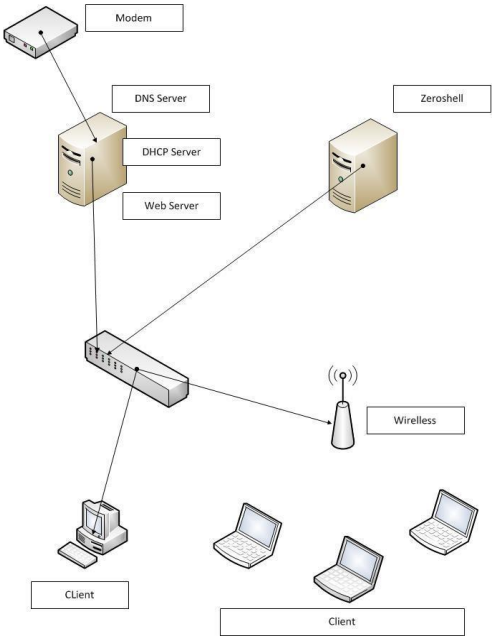
1.15 Analisis Kebutuhan Sistem

3.2.1 Sistem Usulan

Kerberos sebagai authentikasi dari web akan di instal pada sistem operasi Zeroshell, sedangkan monitoring pada cacti, manajemen bandwidth HTB tools, sms gateway dengan gammu akan di instal dalam satu sistem operasi ubuntu. Dimaksudkan untuk memudahkan admin untuk mengawasi dan mengontrol dari ketiga service tersebut.

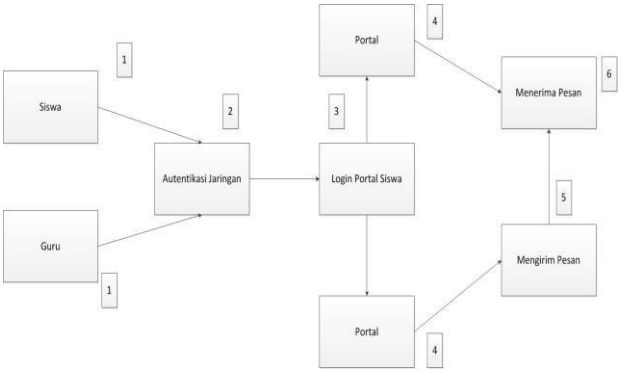


Gambar 3 - 2 Topologi Usulan



Gambar 3 - 3 Sistem Usulan

3.2.2 Alur Kerja Sistem



Gambar 3 - 4 Alur Kerja Sistem

1. Siswa dan guru merupakan dua pengguna dari sistem yang dibangun.

2. Ketika siswa dan guru terhubung kedalam jaringan Man 1 Bojonegoro maka mereka akan masuk pada proses autentikasi kerberos5 menggunakan zeroshell, di sini mereka harus melakukan login jaringan man 1 bojonegoro.

3. Ketika nama user benar-benar ada maka user dapat mengakses jaringan yang ada pada man 1 bojonegoro, kemudian user akan *redirect* secara otomatis oleh sistem masuk pada halaman portal informasi siswa. Ketika user ingin masuk pada portal informasi maka mereka harus login terlebih dahulu.

4. Lalu kemudian siswa dan guru mempunyai beberapa hak akses yang berbeda.

5. Guru dapat menginputkan pengumuman dan absensi siswa, pada bagian absensi jika siswa tidak masuk maka sistem akan secara otomatis mengirimkan data tersebut kepada orang tua siswa.

6. Siswa hanya bisa melihat pengumuman yang diberikan oleh guru dan orang tua mereka akan menerima sms dari sistem ketika mereka tidak masuk sekolah.

1.15.2 Rencana Pengujian

Rencana pengujian dengan menggunakan simulasi yang memakai beberapa client sebagai parameter pengukuran terhadap sample yang diambil pada sekolah madrasah aliyah negeri 1 bojonegoro. Dan beberapa parameter keberhasilan pada saat simulasi pengujian adalah sebagai berikut :

1. Client dapat memasuki web authentication yang telah dibuat dengan menggunakan kerberos5 pada zeroshell.

2. Memonitoring jaringan dengan menggunakan cacti.

3. Berjalannya sms gateway pada web portal informasi MAN 1 Bojonegoro.

4. Admin dapat mengatur bandwidth pada penggunaan client dengan menggunakan HTB.
5. Pengujian daripada kinerja dari server yang telah dibuat pada MAN 1 Bojonegoro.

1.16 Kebutuhan Perangkat Keras dan Perangkat Lunak

Perangkast keras dan perangkat lunak yang dibutuhkan untuk sistem adalah sebagai berikut :

1. Perangkat Keras

   a. 1 buah komputer sebagai server zeroshell
   b. 2 buah laptop, 1 sebagai server utama, 1 sebagai client yang nantinya akan dipakai di pengujian.
   c. Access Point yang berfungsi menghubungkan dari kedua server sekaligus akses wifi untuk client.

2. Perangkat Lunak

   a. Ubuntu 14.04 sebagai operasi sistem dari server.

   b. Zeroshell 3.3 sebagai operation sistem dari web authentication.

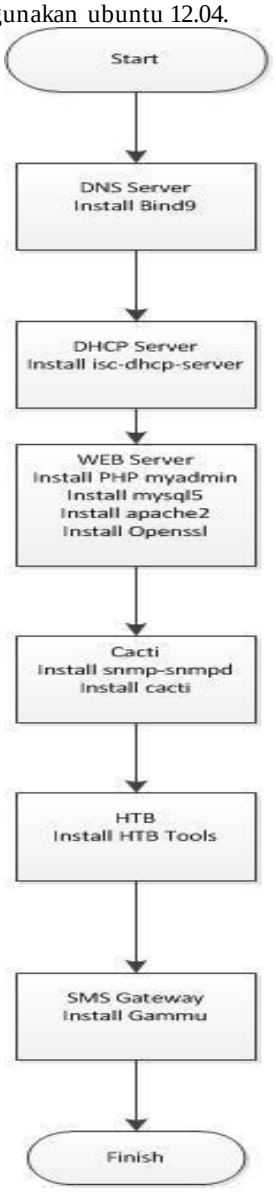
4. Implementasi dan Pengujian

4.1 Implementasi

Implementasi pada sistem monitoring menggunakan cacti dan authentikasi menggunakan kerberos akan dijelaskan pada sub bab berikut terdapat juga langkah-langkah dalam pembangunan sistemnya.

4.1.1Pembangunan server

Berikut adalah tahapan tahapan installasi dari server menggunakan ubuntu 12.04.

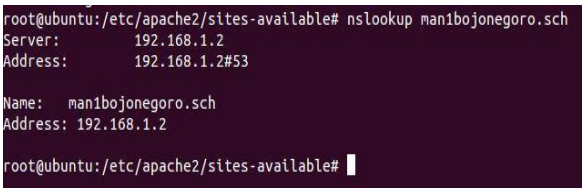


4.2 Pengujian

4.2.1 Pengujian Server

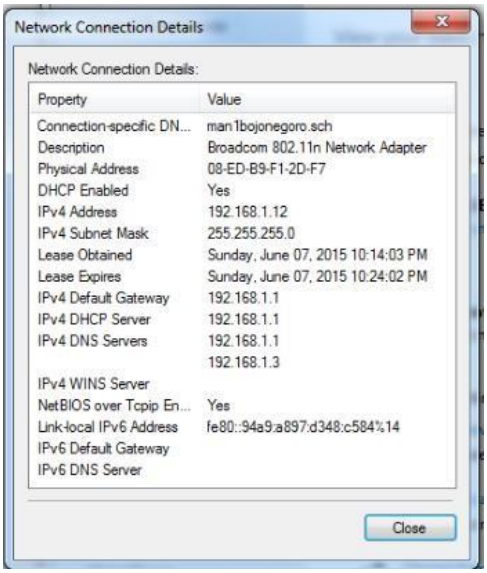
Pengujian server dilakukan karena untuk mengetest apakah server yang telah dikonfigurasi sudah bias berjalan. Untuk pengujian yang pertama penulis melakukan pengujian terhadap dns, dhcp dan web server yang ada pada server utama.

a. Pada gambar di bawah ini merupakan pengujian dns pada server.



Gambar 4 - 1 Pengujian DNS Server

b. Selanjutnya penulis melakukan pengujian dns dan dhcp, dalam pengujian ini penulis melakukan dengan pc server utama dan server zeroshell sudah berada pada satu jaringan dan sudah terhubung kedalam access point, lalu selanjutnya di sharing kepada client dengan wireless.

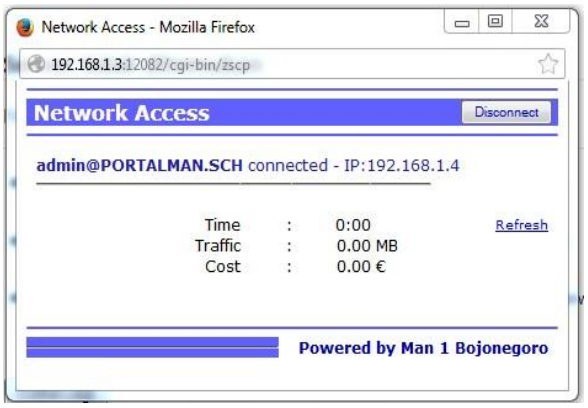


Gambar 4 - 2 Pengujian DHCP dengan acces point

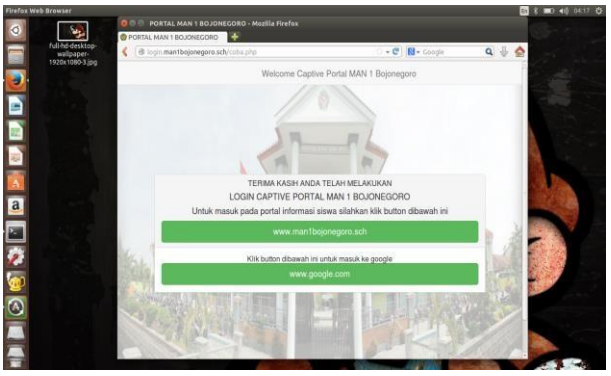
c. Lalu selanjutnya user akan masuk pada jaringan yang sudah terhubung, ketika user akan melakukan koneksi ke internet dengan melalui web browser maka secara langsung user akan masuk pada server authentikasi dengan kerberos5 pada zeroshell, seperti pada gambar di bawah ini.

Gambar 4 - 3 Pengujian Captive Portal

d. Lalu kemudian isikanlah password dan username user, ketika user sudah terdaftar dalam database maka user akan secara redirect terhubung pada "login.man1bojonegoro.s ch" dan akan muncul tab internet access seperti pada gambar di bawah ini.



Gambar 4 - 4 Network Access Zeroshell



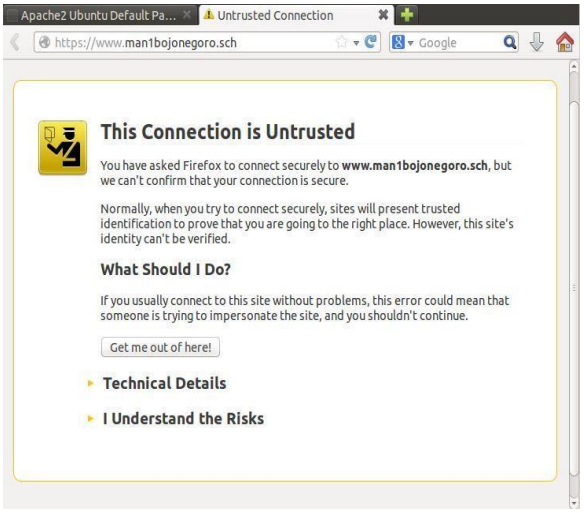
Gambar 4 - 5 Halaman Redirect

Didalam zeroshell admin dapat mengetahui siapa saja yg terhubung dengan masuk pada kolom captive portal. Di bawah adalah contoh bahwa admin masuk dengan menggunakan ip 192.168.1.4

Gambar 4 - 6 Monitoring User Zeroshell

e. Ketika user sudah masuk pada jaringan madrasah aliyah negeri 1 bojonegoro, maka user bisa masuk pada layanan portal

informasi yang disediakan sekolah untuk 3 user : admin, guru dan siswa. Di bawah merupakan hasil pengujian webserver telah dipasang menjadi https.

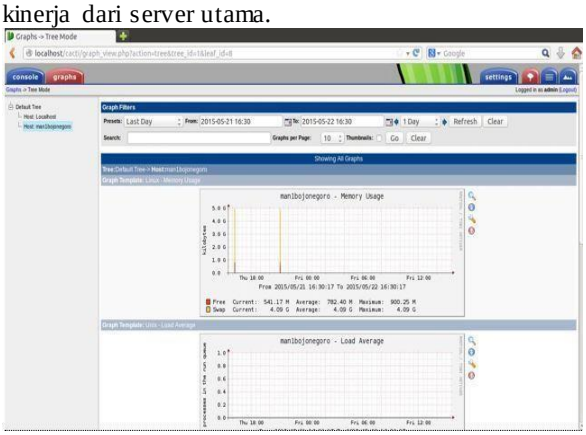


Gambar 4 - 7 Pengujian SSL

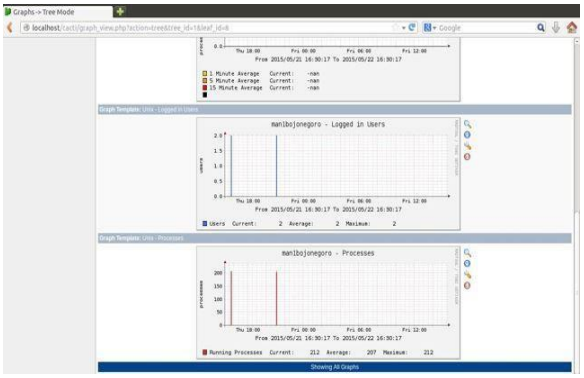
Gambar 4 - 8 Pengujian Web Server

4.2.2 Monitoring Cacti

Pada gambar di bawah ini merupakan tampak hasil pengujian dari monitoring terhadap server utama. Berikut adalah hasil dari grafik yang muncul pada server. Dari monitoring ini kita dapat mengetahui kinerja dari server utama.



Gambar 4 - 9 Pengujian Grafik Cacti



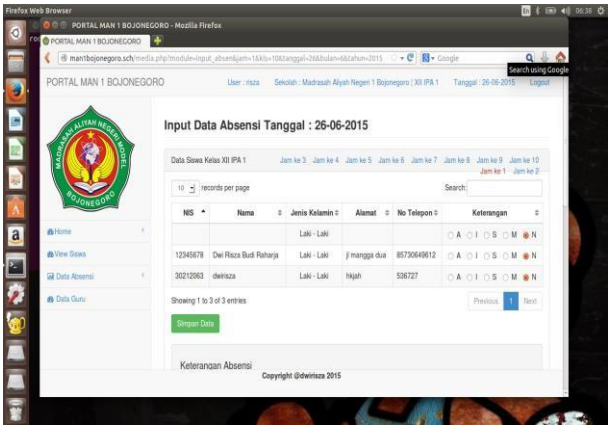
Gambar 4 - 10 Pengujian Grafik Cacti2

4.2.3 Web Portal dan SMS Gateway

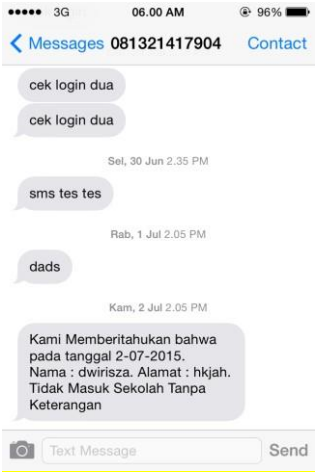
Didalam portal informasi terhadap dua menu yang disediakan menu yang pertama merupakan menu informasi yang berupa pengumuman yang disampaikan oleh guru terhadap siswa dan hanya guru saja yang bisa memberikan informasi tersebut. Ketia guru menginputkan pengumuman maka akan ada 2 pilihan jenis pengumuman yaitu berupa perlombaan dan kegiatan.

Gambar 4 - 11 Input Pengumuman

Kemudian dalam portal informasi terdapat sms gateway yang telah terintegrasi dengan kehadiran siswa, ketika guru menginputkan kehadiran siswa dan siswa dinyatakan tidak masuk maka systemakan secara langsung mengirimkan sms kepada orang tua mereka.



Gambar 4 - 12 Halaman Input Absensi



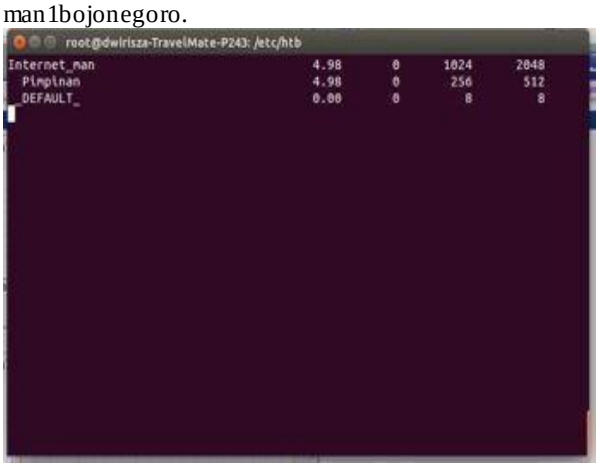
Gambar 4 - 13 Pengujian SMS

Berikut adalah skrip dari sms gateway yang terintegrasi dengan web portal.

```
if($_POST[$ra]=="A"){
$noTujuan = "+62$rs[tlp]";
$message = "Kami Memberitahukan bahwa pada tanggal $rsa[tgl]. Nama : $rs[nama]. Alamat : $rs[alamat]. Tidak Masuk Sekolah Tanpa Keterangan";
$query = "INSERT INTO outbox(DestinationNumber, TextDecoded, CreatorID, Class)
VALUES ('$noTujuan','$message','Gammu','1')";
mysql_query($query);
}
```

4.2.4 Manajemen Bandwidth (HTB Tools)

Htb akan secara otomatis menampilkan bahwa siapa saja yang terhubung didalam jaringan man1bojonegoro.



Gambar 4 - 14 Manajemen Bandwith.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Adapun kesimpulan yang dapat diambil berdasarkan hasil dari *implementasi monitoring jaringan menggunakan cacti dan web authentikasi menggunakan kerberos pada MAN 1 Bojonegoro* adalah sebagai berikut :

1) Server yang dibangun berupa 1 server utama dan 1 server web authentikasi berhasil dilakukan, itu terbukti pada pengujian yang dilakukan.

2) SMS Gateway tentang kehadiran siswa yang terintegrasi dengan web portal informasi siswa sudah berjalan dengan baik, itu terbukti dengan dilakukannya pengujian pada pengerjaan proyek akhir ini.

3) Monitoring sistem yang dilakukan untuk memudahkan admin dalam mengontrol server berjalan dengan baik.

4) Manajemen Bandwith menggunakan HTB Tools berjalan pada server dan sudah dapat dipakai dan sudah melalui pengujian pada proyek akhir ini.

5.2 Saran

Adapun saran yang ingin disampaikan dalam pembuatan proyek akhir ini adalah :

1) Download versi terbaru pada zeroshell untuk pengembangan sistem yang lebih baik.

2) Mengembangkan web portal yang ada, misalnya dengan melakukan penambahan module didalamnya, seperti penambahan input nilai untuk siswa itu akan memudahkan siswa untuk melihat nilai mereka secara online.

3) Untuk penyusunan selanjutnya kembangkan kembali sistem-sistem yang telah dibangun dan belum ada pada server.

4) Untuk penggunaan sistem dari zeroshell sudah diatur, sehingga penggun a tidak bisa menambahkan fitur-fitur diluar sistem.

Daftar Pustaka

[1] Mekanisme sistem otentikasi pada protokol kerberos. [*Online*]. HYPERLINK " http://www.blognazcules .com/2014/06/ mekanisme-otentikasi-pada-protokol-kerberos.html"

http://www.blognazcules .com/2014/06/ mekanisme-otentikasi-pada-protokol-kerberos.html

[2] APA ITU *JQUERY* DAN PENGERTIAN *JQUERY*.[*Online*].

HYPERLINK"http://s eputarti.com/*Jquery*/ap a-itu-*Jquery*-dan-pengertian-*Jquery*.html". http://seputarti.com/*Jquery*/apa-itu-*Jquery*-dan-pengertian-*Jquery*.html

[3] SMS gateway menggunakan gammu dan mysql. [*Online*]. HYPERLINK " http://www.ubaya.ac.id/ubaya/articles_detail/33/SMS-Gateway-menggunakan-Ga mmu-dan-MySQL.html"

http://www.ubaya.ac.id/ubaya/articles_detail/33/SMS-Gateway-menggunakan-Ga mmu-dan-MySQL.html

[4] Tantra, Eno, 2012, *Implementasi Bandwidth Management Dengan Menggunak an Metode HTB (Hierarchical Token Bucket) Pada Clearos Di SMP Islam Terpadu Raudhatul Jannah Cilegon*. Bandung : Politeknik Telkom

[5] Zeroshell net service.Zers hell guide.[online].http://www.zeros hell.net.[6 juni 2015 09.20]

[6] Datty Putri, Karina, 2012, *Implementasi Layanan SMS Gateway Berbasis Online Dengan Memanfaatk an Jaringan Interkoneksi Dalam Dukungan Media Koneksi Dosen-Mahasiswa*.Bandung : Politeknik Telkom