SISTEM KEAMANAN JARINGAN HOTSPOT PADA STIE LAMAPPAPOLEONRO SOPPENG

Irma
Dosen STMIK Lamappapoleonro Soppeng
Sistem Informasi, STMIK Lamappapoleonro Soppeng
e-mail : Irma@stmik.ypls.ac.id

Abstrak

Jaringan *wireless (hotspot)* yang tidak mempunyai server yang dapat melakukan autentikasi, tentunya tidak menjamin keamanan baik dari *user* maupun administrator pada jaringan *wireless* di kampus STIE Lamappapoleonro Soppeng, sebab seorang *administrator* tidak dapat mengetahui *user-user* yang login dan berinternet pada jaringan. Untuk melakukan system keamanan jaringan hotspot di kampus STIE Lamappapoleonro dibutuhkan suatu autentikasi. Metode sistem keamanan menggunakan radius server. Dengan adanya system kemanan jaringan Hotspot membuat autentikasi pengguna jaringan *wireless (hotspot)* serta meningkatkan keamanan jaringan hotspot kampus STIE Lamappapoleonro Soppeng, dan memberi kenyamanan terhadap pada pengguna jaringan *wireless.*

Kata Kunci : Sistem, Keamanan, Jaringan, Hotspot.

Abstract

Wireless networks (hotspots) that do not have servers that can authenticate, certainly do not guarantee the security of both users and administrators on wireless networks on the STIE Lamappapoleonro Soppeng campus, because an administrator cannot know the users who are logged in and surf the network. To perform a security system for network hotspots on the STIE Lamappapoleonro campus, an authentication is required. The security system method uses a radius server. With the security system the Hotspot network authenticates wireless network users (hotspots) and increases the security of the STIE Lamappapoleonro Soppeng campus hotspot network, and provides convenience to wireless network users.

Keywords: System, Security, Network, Hotspot..

1. PENDAHULUAN

1.1. Latar Belakang Masalah

Salah satu perubahan utama di bidang telekomunikasi adalah penggunaan teknologi jaringan *wireless*. Dimana Jaringan *wireless* atau sering disebut *hotspot* ini menjadi daya tarik tersendiri bagi para pengguna komputer yang menggunakan teknologi ini untuk mengakses suatu jaringan komputer atau internet, dikarenakan kemudahan-kemudahan yang ditawarkan oleh teknologi jaringan *wireless*. Pada beberapa tahun terakhir ini pengguna jaringan *wireless* mengalami peningkatan yang pesat. Peningkatan dari pengguna teknologi ini juga diimbangi dengan peningkatan jumlah *hotspot* di tempat-tempat umum, seperti pusat perbelanjaan, Kafe, Bandara, di perkantoran, di Kampus bahkan juga di Sekolah-sekolah. Dengan menggunakan teknologi *wireless* (*hotspot)* kita dapat menikmati akses internet dimanapun kita berada selama di area *hotspot* tanpa harus menggunakan kabel.

Di lingkungan kampus STIE Lamappapoleonro Soppeng saat ini juga sudah menyediakan layanan internet yang berbasis *wireless (hotspot).* Layanan Telkom Speedy yang berkecepatan hingga 2 Mbps pun digunakan untuk membuat jaringan *wireless (hotspot)* di kampus STIE Lamappapoleonro

Soppeng, dan terdapat dua buah *access point* TP-LINK, sehingga *hotspot* pada kampus STIE Lamappapoleonro Soppeng dapat diakses pada dua area, seperti pada ruangan dosen, dan area ruangan kelas, jumlah *user* yang mengakses jaringan *wireless* di kampus STIE Lamappapoleonro Soppeng berkisar antara 1 sampai dengan 50 *user*, namun didalam jaringan yang tidak mempunyai server yang bertindak sebagai *authentication*, *authorization*, *and* a*ccounting* membuat administrator tidak bisa mengetahui identitas yang jelas dari *user*.

Dengan sistem keamanan yang menggunakan WEP (*Wired Equivalent Privacy*) dimana WEP ini menggunakan satu kunci enkripsi yang digunakan bersama-sama oleh para pengguna *wireless* untuk dapat beriternet pada jaringan *wireless* kampus STIE Lamappapoleonro Soppeng, seorang *user* juga harus meminta key kepada seorang *administrator*, dan setiap *user* yang ingin berpindah ke *hotspot* yang lain, *user* pun di minta untuk kembali memasukan key, karena setiap titik mempunyai *network* key yang berbeda, tentunya cara yang seperti ini sangat menyulitkan baik bagi *user* maupun *administrator*.
Jaringan *wireless (hotspot)* yang tidak mempunyai server yang dapat melakukan autentikasi, tentunya tidak menjamin keamanan baik dari *user* maupun administrator pada jaringan *wireless* di kampus STIE Lamappapoleonro Soppeng, sebab seorang *administrator* tidak dapat mengetahui *user-user* yang login dan berinternet pada jaringan, juga tentunya menyulitkan administrator karena tidak dapat memantau serta mengontrol *user* di dalam jaringan *wireless* (*hotspot*) di kampus STIE Lamappapoleonro Soppeng.

Untuk dapat membuat autentikasi pengguna jaringan *wireless (hotspot)* serta meningkatkan keamanan jaringan hotspot kampus STIE Lamappapoleonro Soppeng, dan memberi kenyamanan terhadap pada pengguna jaringan *wireless*, maka dapat dilakukan penelitian Analisis Sistem Keamanan Jaringan Hot-spot pada STIE Lamappapoleonro Soppeng**.**

1.2. Rumusan Masalah

Berdasarkan latar belakang, maka yang menjadi pokok permasalahan adalah sebagai berikut :

1. Bagaimana menganalisa Sistem keamana jaringan Hotspot pada kampus STIE lamappapoleonro soppeng agar nantinya bisa memberikan metode pengamanan jaringan ?.
2. Bagaimana bisa memberikan pelayanan jaringan internet yang bagus dan aman ?

1.3. Tujuan Penelitian

Adapun Tujuan Penelitian yang diharapkan adalah sebagai berikut :

1. Untuk menganalisa Sistem keamana jaringan Hotspot pada kampus STIE lamappapoleonro soppeng agar nantinya bisa memberikan metode pengamanan jaringan.
2. Untuk memberikan pelayanan jaringan internet yang bagus dan aman.

1.4. Manfaat Penelitian

Hasil penelitian ini diharapkan mempunyai manfaat antara lain:

1. Untuk memberikan pelayanan akses internet yang baik dan aman
2. Sebagai bahan referensi dan sumber informasi bagi pelajar dalam mengembangkan ilmu pengetahuan tentang Analisis Sistem Keamanan Jaringan Hot-spot .
3. Memperkaya wawasan peneliti dalam hal bagaimana menganalisa Sistem Keamanan Jaringan Hot-spot.

2. LANDASAN TEORI

2.1. Radius Server

Remote Access Dial-in User Service (RADIUS), merupakan suatu mekanisme akses kontrol yang mengecek dan mengautentikasi (*authentication*) *user* atau pengguna berdasarkan pada mekanisme authentikasi yang sudah banyak digunakan sebelumnya, yaitu menggunakan metode *challenge / response*. *Remote Access Dial In User Service* (RADIUS) dikembangkan di pertengahan tahun 1990 oleh *Livingstone Enterprise* (sekarang *Lucent Technologies*).

Server RADIUS menyediakan mekanisme keamanan dengan menangani autentikasi dan autorisasi koneksi yang dilakukan pengguna. Pada saat computer *client* akan menghubungkan diri dengan jaringan maka server RADIUS akan meminta identitas pengguna (*username* dan *password*) untuk kemudian dicocokkan dengan data yang ada dalam *database server* RADIUS untuk kemudian ditentukan apakah pengguna diijinkan untuk menggunakan layanan dalam jaringan komputer. Jika proses autentikasi dan autorisasi berhasil maka proses pelaporan dilakukan, yakni dengan mencatat semua aktivitas koneksi pengguna, menghitung durasi waktu dan jumlah transfer data yang dilakukan oleh pengguna. Proses pelaporan yang dilakukan server RADIUS bisa dalam bentuk waktu (detik, menit, jam) maupun dalam bentuk besar transfer data (*Byte, KByte, Mbyte*) (Yunus, Amak, 2010).

2.2. Chili Spot

Chilli Spot, merupakan *open source captive portal* atau *Wireless LAN access point controller*. Digunakan untuk mengautentikasi *user* dari sebuah jaringan *Wireless LAN*. Mensupport login berbasis web yang merupakan standar untuk public *hotspot* dewasa ini. ChilliSpot juga dapat sebagai media autentikasi, autorisasi dan *accounting* (AAA) yang merupakan framework atau arsitektur kerja dari sebuah RADIUS server (http://www.chillicpot.info/).

Chilli men-*support* dua jenis metode authentikasi, yaitu :

1. Universal Access Method (UAM); dengan UAM, *wireless client* me- *request* sebuah IP address, dan dialokasikan oleh Chilli. Ketika seorang *user* membuka sebuah *web browser*, Chilli akan menangkap koneksi TCP tersebut dan me*redirect* browser tersebut ke autentikasi web server. Web server meminta *user* untuk *user*name dan *password*, *password* di enkripsi dan dikirim kembali ke Chilli.
2. *Wireless Protected Access (WPA)*; dengan WPA, metode autentikasi di*handle* oleh *access point* dan *subsequently* di *forward* dari *access point* ke Chilli. Jika WPA digunakan, maka koneksi yang terjadi antara *access point* dan *user* di enkripsi.

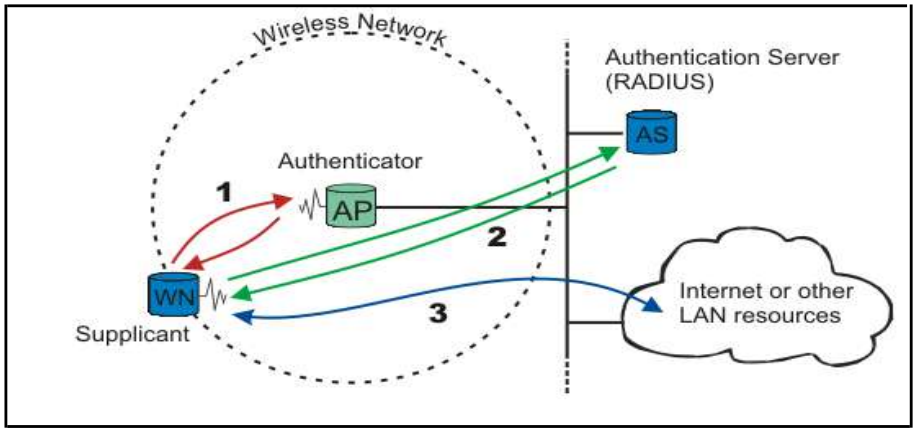
2.3. Autentikasi

Menurut (J, Hassel, 2002), autentikasi adalah proses pengesahan identitas pengguna (*end user*) untuk mengakses jaringan. Proses ini diawali dengan pengiriman kode unik misalnya, *username*, *password*, *pin*, sidik jari oleh pengguna kepada server. Di sisi server, sistem akan menerima kode unik tersebut, selanjutnya membandingkan dengan kode unik yang disimpan dalam *database* server. Jika hasilnya sama, maka server akan mengirimkan hak akses kepada pengguna. Namun jika hasilnya tidak sama, maka server akan mengirimkan pesan kegagalan dan menolak hak akses pengguna.

2.4. Mekanisme Autentikasi

Tujuan standar 802.1x IEEE adalah untuk menghasilkan kontrol akses, autentikasi, dan manajemen kunci untuk *wireless* LANs. Standar ini berdasarkan pada *Internet Engineering Task Force* (IETF) *Extensible Authentication Protocol* (EAP), yang ditetapkan dalam RFC 2284. Standar 802.1x IEEE juga mendukung beberapa metode autentikasi, seperti *smart cards*, *password* yang hanya bisa digunakan oleh satu pengguna pada satu waktu, dan yang lebih baik lagi adalah *biometrics*.(Agung,S ,2008). 802.1x terdiri dari tiga bagian, yaitu *wireless node* (*supplicant*), *access point* (autentikator), autentikasi server.

Autentikasi server yang digunakan adalah *Remote Authentication Dial-In Service* (RADIUS) server dan digunakan untuk autentikasi pengguna yang akan mengakses *wireless* LAN. EAP adalah protocol layer 2 yang menggantikan PAP dan CHAP.



Gambar 2.1 : Mekanisme Autentikasi menggunakan RADIUS server.

2.5. Jaringan *Wireless*

Sinyal *Wireless* merupakan sinyal gelombang elektromagnetis yang dapat berjalan tanpa media tetapi melalui ruang hampa atau media seperti udara. Karena tidak dibutuhkan media fisik sebagai perantara, maka hal ini akan sangat menguntungkan pada saat membangun jaringan pada daerah atau area yang luas.

WI-FI (*Wireless Fidelity*) atau jaringan tanpa kabel, yang sering, maka disebut degan jaringan 802.11 karena standar yang biasanya digunakan adalah IEEE 802.11. Keuntungan menggunakan jenis jaringan seperti ini adalah tanpa menggunakan medium seperti kabel,kita sudah dapat membangun atau melakukan koneksi ke jaringan.Penggunaan angka 802.11 *(standard wireless network)* dibuat oleh IEEE *(Institute of Electrical and Electronics Engineers).*

Penggunaan notasi a,b,dan g, adalah menunjukan versi yang berbeda dalam standar 802.11. versi yang pertama diluncurkan adalah 802.11b beroperasi pada 2,4GHz dan kecepatan 11 Mbps. Kemudian dilanjutkan dengan versi 802.11a dengan beroperasi pada 5GHz dan kecepatan 54Mbps. Versi yang terakhir adalah 802.11g adalah campuran dari kedua versi sebelumnya, beroperasi pada 2,4 GHz dan kecepatan 54Mbps.

Pada dasarnya sistem yang diggunakan pada jaringan WI-FI adalah analogi dengan HT(*Handie-talkie*). Alat ini dapat mengirim dan menerima sinyal radio. Suara yang dikirim akan diterima oleh microphone dan di enkodekan menjadi frekuensi radio dan di transmisikan melalui antana. (Utomo,Eko.2011:74).

3. METODE PENELITIAN

3.1. Metode Pengumpulan Data

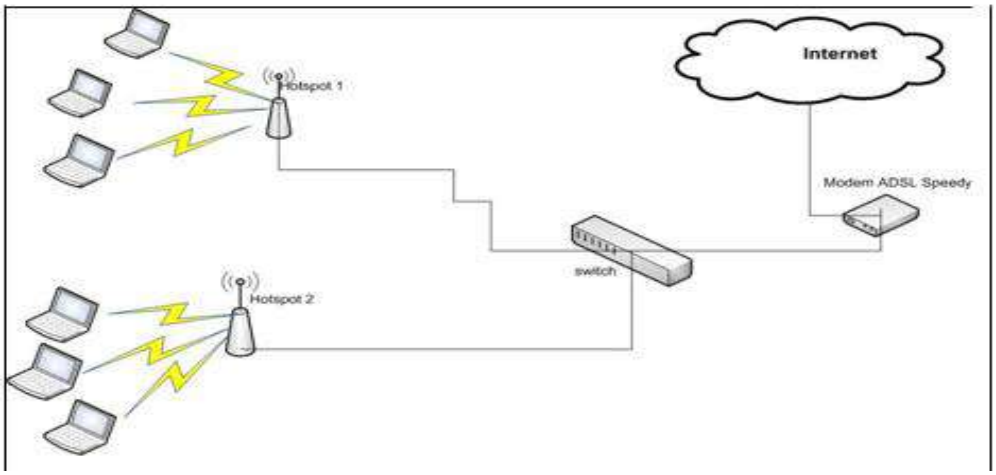
Untuk memperoleh data yang diperlukan dalam penelitian ini, digunakan tiga metode yaitu :

1. Teknik Observasi
   Metode pengamatan merupakan metode pengumpulan data dimana peneliti mengamati peristiwa-peristiwa dengan melihat, mendengar, yang kemudian dicatat dengan sebaik mungkin sesuai dengan kondisi tempat penelitian.

2. Teknik Wawancara
   Metode wawancara merupakan bentuk komunikasi langsung antara peneliti dan orang yang terlibat langsung pada masalah yang dibahas sehingga gerak dan mimik responden dapat melengkapi kondisi dan perasaan yang menggambarkan tentang keadaan ditempat penelitian.
3. Metode Dokumentasi
   Metode dokumentasi merupakan catatan atau berkas tertulis tentang berbagai kegiatan atau peristiwa pada waktu yang lalu.

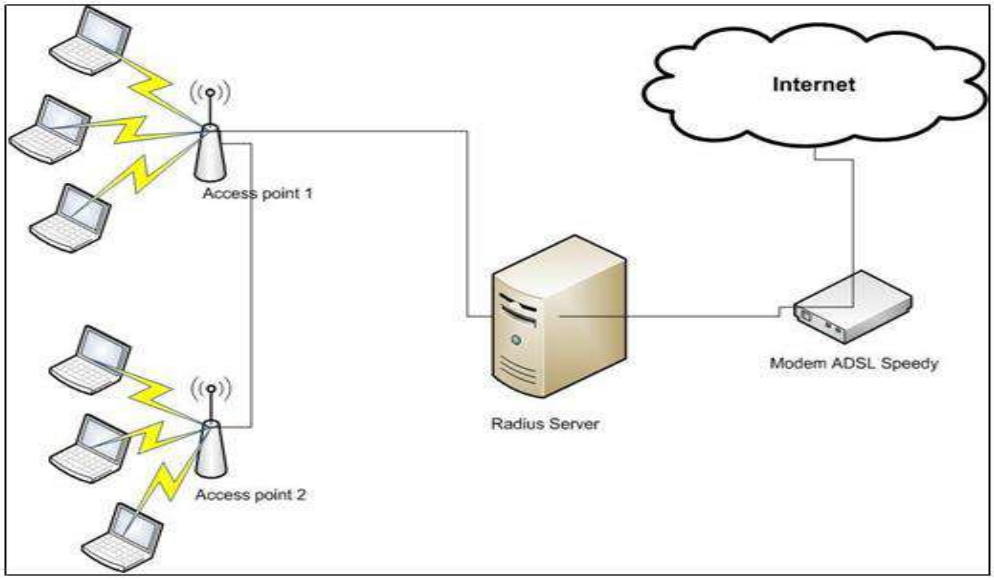
3.2. Analisis Sistem Lama

Proses manganalisa terdapat masalah dalam sistem keamanan jaringan dimana sistem akses jaring masih secara langsung tanpa memberikan security jaringan. Berikut ini adalah gambaran arsitektur jaringan hotspot yang ada di Kampus STIE Lamappapoleonro Soppeng :



Gambar 3.1 : Arsitektur Jaringan Sistem Lama.

3.3. Rancangan Sistem Yang Diusulkan



Gambar 3.2 : Rancangan Arsitektur yang diusulkan.

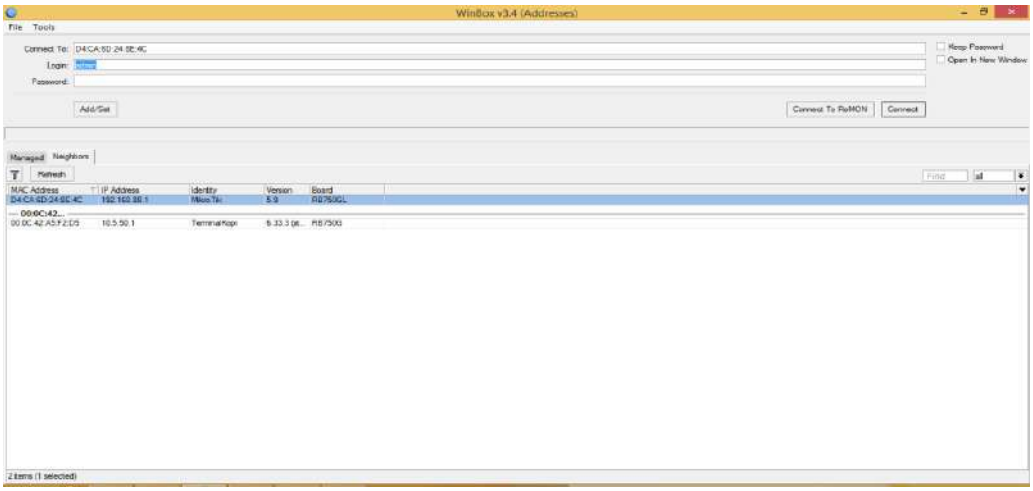
4. HASIL DAN PEMBAHASAN

4.1. Implementasi Sistem

Sistem Keamanan Jaringan Hot-spot pada STIE Lamappapoleonro Soppeng dibangun dengan menggunakan alat mikrotik dan access point

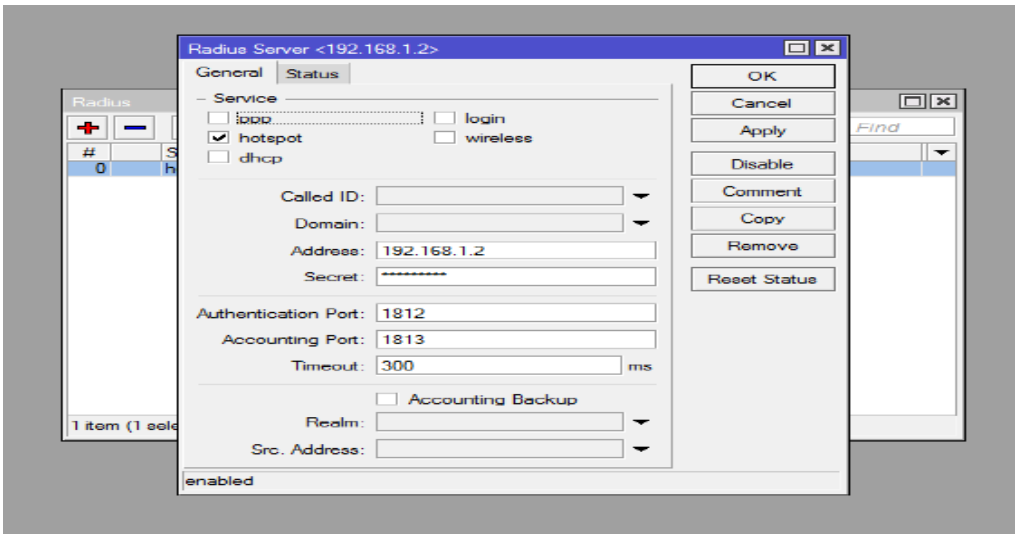
4.1.1. Client Login Mikrotik

Client login dengan winbox adalah tampilan dimana user setting konfigurasi untuk memberikan alamat IP. Berikut gambar konfigurasi mikrotik Client login dengan winbox.



Gambar 4.1 : Login Mikrotik dengan Winbox

4.1.2. Tampilan Server Radius



Gambar 4.2 : Tampiln Server Radius

5. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan pada bab-bab sebelumnya, maka dapat ditarik kesimpulan bahwa Dengan diimplementasikannya sistem keamanan jaringan dapat memberikan pelayanan akses internet yang baik dan aman pada kampus STIE lamappapoleonro soppeng.

DAFTAR PUSTAKA

Agung S., "*Remote Authentication Dial In User Service (RADIUS) untuk Autentikasi Pengguna Wireless LAN*", Laporan Akhir EC-5010 Institut Teknologi Bandung, 2005,

Febyatmoko, dkk. 2006. *Otentikasi, Otorisasi & Pelaporan Koneksi UserWirelessChillispot Dan Server RADIUS.*

Kunang,Yesi Novaria dan Zuhri,YadiIlman.*"Autentikasi Pengguna Wireless Lan Berbasis Radius Server (Studi Kasus WLAN Universitas Bina Darma)"*,

Sudiarta,Pande Ketut, *"Implementasi Sistem Autentikasi Jaringan Hotspot Universitas Udayana Dengan Menggunakan Open Source Freeradius"*.

Utomo,Eko Priyo.2011.*Membangun Jaringan Komputer dan Server Ïnternet*, Yokyakarta : MediaKom.

Yunus,Amak *"Implementasi Sistem Otentikasi Pada Pengguna Jaringan Hotspot Di Universitas Kanjuruhan Malang Guna Meningkatkan Keamanan Jaringan Komputer"*.

C. Rigney, S. Willens, A. Rubens, W. Simpson, "*Remote Authentication DialIn UserService* (RADIUS)",RFC2138,1997