e-ISSN. 2685-4066
Jurnal BITE
Vol.1 No.1 (Juni) 2019, Hal 51-59

PERANCANGAN KEAMANAN JARINGAN AUTHENTICATION LOGIN HOTSPOT MENGGUNAKAN RADIUS SERVER DAN PROTOKOL EAP-TTLS PADA MIKROTIK DI IDOOP HOTEL

I Wayan Sukartayasa[1], I Putu Hariyadi[2]
[1]Mahasiswa [2]Dosen Program Studi Teknik Informatika STMIK Bumigora Mataram
Jl. Ismail Marzuki Mataram 83127
[1]sukartayasa29491@gmail.com, [2]putu.hariyadi@gmail.com

ABSTRAK

Idoop Hotel merupakan salah satu hotel yang terletak di kawasan Kota Mataram, Jalan Swaramahardika No.883, 83121. Idoop Hotel mulai beroperasi pada bulan Juni 2014. Idoop Hotel memiliki total 9 *departement* yang tergabung dalam jaringan *back office* dan operasional. Keseluruhan *department* berada dalam satu jaringan lokal yang dikelola oleh *administrator* jaringan pada hotel tersebut. *Protocol Extensible Authentication Protocol-Tunelled Transport Layer Security (EAP-TTLS)* melihat dari segi implementasi *EAP-TTLS* dirancang untuk memberikan kemudahan implementasi otentikasi dibandingkan dengan *protocol EAP* yang berbasis sertifikat digital. Implementasi *EAP-TTLS* hanya memerlukan sertifikat digital pada sisi *authentication server*, sedangkan sertifikat digital pada sisi *client* akan digantikan dengan menggunakan kombinasi *username* dan *password*. Kesimpulan yang diperoleh berdasarkan hasil pengujian yang dilakukan yaitu Penggunaan kombinasi *username* dan *password* untuk menggantikan sertifikat *digital* pada *Extensible Authentication Protocol-Tunelled Transport Layer Security (EAP-TTLS)* juga dapat meningkatkan mobilitas pengguna, karena pengguna tidak perlu menambahkan sertifikat *digital* untuk melakukan login ke *hotspot*. Authentikasi *EAP-TTLS* memiliki kemampuan yang lebih baik yang ditambahkan dengan *enkripsi* MD5 pada *hotspot MikroTIK* sehingga pengguna nyaman untuk melakukan *login* ke *hotspot* dan mempermudah karyawan *IT* dari Idoop Hotel untuk memanajemen pengguna dalam jumlah banyak.

Kata Kunci : *Idoop Hotel, EAP-TTLS, Hotspot, Protocol, MikroTIK, Kemanan jaringan*

ABSTRACT

Idoop Hotel is one of the hotels located in the Mataram City area, Jalan Swaramahardika No.883, 83121. Hotel Idoop began operations in June 2014. Idoop Hotel has a total of 9 departments incorporated in the back office and operational networks. The entire department is in a local network managed by the network administrator at the hotel. The Protocol-Tunneled Transport Layer Security (EAP-TTLS) Extensible Authentication protocol sees in terms of EAP-TTLS implementation designed to provide easy implementation comparing with digital certificate-based EAP protocols. The EAP-TTLS implementation only requires a digital certificate on the authentication server side, while the digital certificate on the client side will be replaced by using a combination of username and password. Conclusions obtained based on the results of tests carried out using a combination of user names and passwords to obtain digital certificates on the Extended Authentication Protocol - Tunelled Transport Layer Security (EAP-TTLS) can also increase user mobility, so users need to add digital certificates to log into hot spot . EAP-TTLS authentication has better capabilities added with MD5 encryption on MikroTIK hotspots allowing convenient users to log in to hotspots and facilitate IT employees from Idoop Hotel to manipulate large numbers of users

Keyword : *Idoop Hotel, EAP-TTLS, Hotspot, Protocol, MikroTIK, Kemanan jaringan*

I. PENDAHULUAN

Seiring perkembangan teknologi informasi dan komunikasi kebutuhan manusia akan mobilitas (mudah berpindah-pindah) dan fleksibilitas yang tinggi menuntut sesuatu yang lebih praktis. Teknologi *wireless* memberikan jawaban akan kebutuhan itu. Teknologi *wireless* memiliki kelebihan yaitu kemudahan dan kebebasan untuk dapat mengakses internet diposisi manapun selama masih dalam jangkauan *wireless*.

Idoop Hotel merupakan salah satu hotel yang terletak di kawasan Kota Mataram, Jalan Swaramahardika No.883, 83121. Idoop Hotel

mulai beroperasi pada bulan Juni 2014. Idoop Hotel memiliki total 9 *departement* yang tergabung dalam jaringan *back office* dan operasional. Keseluruhan department berada dalam satu jaringan lokal yang dikelola oleh administrator jaringan pada hotel tersebut.

Penggunaan kombinasi *username* dan *password* untuk menggantikan sertifikat digital juga dapat meningkatkan mobilitas pengguna, karena pengguna tidak dibatasi pada perangkat tertentu. Sehingga untuk kondisi jaringan yang ada pada Idoop hotel sesuai dengan data yang tertera diatas maka untuk proses autentikasi yang cocok adalah menggunakan *protocol EAP-TTLS* dan proses implementasinya dilakukan pada penelitian ini dengan judul: "PERANCANGAN KEAMANAN JARINGAN *AUTHENTICATION LOGIN HOTSPOT* MENGGUNAKAN RADIUS *SERVER* DAN PROTOKOL *EAP-TTLS* PADA *MIKROTIK* DI IDOOP HOTEL". Untuk selanjutnya sangat diharapkan hasil penelitian yang dirancang bisa bermanfaat untuk keamanan dan kenyamanan dalam penggunaan jaringan *internet hotspot* pada Idoop Hotel.

Berdasarkan latar belakang diatas dapat dirumuskan suatu permasalahan yang ada di Idoop hotel yakni : "Bagaimana penerapan *Extensible Authentication Protocol-Tunelled Transport Layer Security (EAP-TTLS)* untuk menangani proses otentikasi puluhan pengguna jaringan *hotspot* di Idoop hotel pada router *MikroTIK*".

Tujuan-tujuan yang ingin dicapai dalam melakukan penelitian ini berdasarkan atas permasalahan yang dibahas adalah :

a. Dapat menerapkan teknik autentikasi menggunakan *Extensible Authentication Protocol-Tunelled Transport Layer Security (EAP-TTLS)* pada jaringan hotspot di Idoop Hotel.
b. Dapat memudahkan administrator dalam hal memantau dan mengontrol *user* yang terhubung dalam jaringan *hotspot* di Idoop hotel.
c. Dapat membandingkan kemampuan teknik autentikasi *Extensible Authentication Protocol-Tunelled Transport Layer Security (EAP-TTLS)* dengan teknik keamanan *Extensible Authentication Protocol-Transport Layer Security (EAP-TLS).*

II. METODOLOGI

1. **Identifikasi**

A. Observasi

Tahapan observasi adalah metode pengumpulan data yang dilakukan dengan cara mengamati dan memantau secara langsung kegiatan yang dilakukan pada tempat penelitian. Pengamatan yang dilakukan yaitu mengamati perangkat - perangkat apa yang digunakan,bagaimana kondisi dari jaringan yang telah ada saat ini ,*security* apa yang digunakan pada jaringan *hotspot* Hotel Idoop, dan sistem kerja dari *hotspot* Hotel Idoop. Berikut hasil dari kegiatan observasi yang dilakukan pada Hotel Idoop:

1. *Router* yang digunakan untuk melakukan manajemen jaringan pada Hotel Idoop yaitu *Router MikroTIK*.
2. Idoop Hotel menggunakan 3 *line* koneksi *internet*, diantaranya 2 *line* koneksi Indihome *shared* dengan kecepatan *bandwidth* 50 Mbps dan 1 *line* koneksi *dedicated* Astinet dengan kecepatan 1 *Mbps*.
3. Pengalamatan *IP* pada jaringan Hotel Idoop menggunakan pengalamatan *IP Address* Versi 4 dengan *IP Address* kelas C.
4. Server hotspot yang digunakan pada Hotel Idoop menggunakan fitur router MikroTIK dan pengguna melakukan akses internet dengan menggunakan *SmartPhone*, PC dan laptop.
5. Perangkat *access point* untuk jaringan hotspot diletakkan di banyak titik dan di manajemen secara terpusat oleh administrator jaringan Hotel Idoop dan dapat menjangkau seluruh area hotel.

B. Wawancara

Pada tahapan wawancara penulis melakukan pengambilan data dan informasi dengan melakukan wawancara secara langsung ke sumber data yaitu teknisi *IT* dari Hotel Idoop, agar mendapat data dan informasi yang diinginkan. Penulis melakukan sesi wawancara pada teknisi *IT* hotel idoop dan berikut hasil dari wawancara yang dilakukan penulis pada :

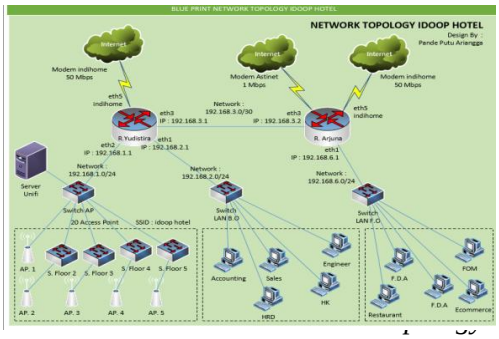
1. Pada Idoop Hotel menggunakan koneksi *internet ISP* dengan Telkom, dengan produk yang digunakan yaitu *Indihome* dan *Astinet.*
2. Besar *bandwidth* yang digunakan untuk *line Indihome* ada 2 koneksi jalur keluar masing-

masing *50Mbps shared*, dan untuk *Astinet 1Mbps dedicated*

3. Pengguna atau *client* dapat melakukan akses *internet* melalui media komputer (*PC*), *Handphone*, *Tablet*, dan Laptop pada saat berada di hotel.
4. Mekanisme agar tamu/*client* dapat menikmati akses *internet via WIFI* yaitu dengan melakukan proses *login hotspot*, dimana *user* akan inputkan *user* dan *password* pada halaman *login hotspot*, yang nanti akan *redirect* secara otomatis ketika memiilih koneksi ke *ssid* Hotel Idoop. *User* dan *password* akan diberikan ke tamu pada saat proses *check-in* dalam bentuk *voucher*. Data *user* dan password di simpan di *server* radius *MikroTIK* dengan proses *generate* secara *batch* pada *management user manager*.
5. Hotel Idoop menggunakan proses *authentikasi* pada saat *login* untuk dapat menikmati akses *internet*, maka untuk keamanan authentikasi perlu ditingkatkan sehingga keamanan bisa lebih baik lagi demi keamanan tamu dalam melakukan proses login ke *system login* page *MikroTIK*. Sebagai informasi proses *authentikasi* masih menggunakan standar keamanan yang disedikan oleh *MikroTIK* belum menggunakan fitur tambahan yang dapat meningkatkan keamanan user. Proses *authentikasi login* MikroTIK bisa lebih aman lagi dengan menambahkan beberapa fitur tertentu, sehingga user dapat lebih aman lagi ketika melakukan proses *login* ke halaman *login hotspot*.

C. Dokumentasi

Pada tahapan ini penulis mendapatkan beberapa arsip dokumentasi berupa foto – foto dari kegiatan yang dilakukan penulis dalam melakukan observasi, dan wawancara. berikut hasil dari kegiatan dokumentasi yang dilakukan oleh penulis:



IDOOP HOTEL

2. Analisa

Analisa Kebutuhan

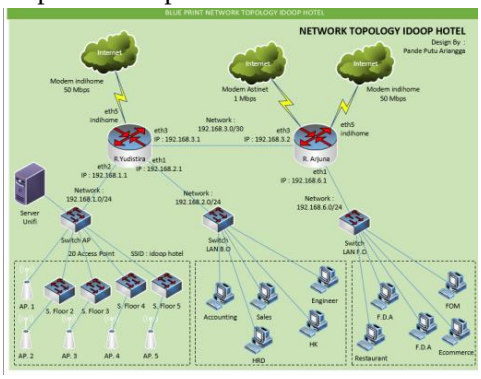
Analisis kebutuhan diperlukan untuk menentukan apa saja yang dibutuhkan untuk membangun jaringan pada Hotel Idoop baik kebutuhan perangkat keras (*hardware*) dan perangkat lunak (*software*). Adapun kebutuhan ini terdiri dari kebutuhan perangkat lunak (*software*) dan kebutuhan perangkat keras (*hardware*).

3. Perancangan

Pada tahapan desain perancangan, dilakukan perancangan – perancangan yang meliputi rancangan jaringan yang berjalan, rancangan jaringan yang baru dan rancangan pengalamatan *IP address.*

A. Desain Jaringan

Dari tahapan identifikasi awal berdasarkan hasil dokumentasi yang dilakukan pada bagian *IT*, didapatkan infrastruktur jaringan yang terdapat di Idoop Hotel.



Gambar 3.2 Desain Jaringan Idoop Hotel

Pada gambar 3.2 menunjukkan *topology* dari Hotel Idoop dan berikut keterangan dari gambar 3.2;

a. Pada gambar 3.2 terdapat 3 Line Koneksi *Internet* yaitu modem *Indihome* dengan kecepatan 50 Mbps , modem Astinet dengan kecepatan 1 *Mbps Dedicated* dan modem indihome dengan kecepatan 50 *Mbps*.
b. Menggunakan 2 *Router MikroTIK* yang diberi pengenal R. Yudistira dan R. Arjuna. Dimana setiap *Router MikroTIK* memanajemen masing – masing perangkat di ruangan tertentu.

Berikut desain pengalamatan yang ada pada jaringan Hotel Idoop berdasarkan gambar 3.2:

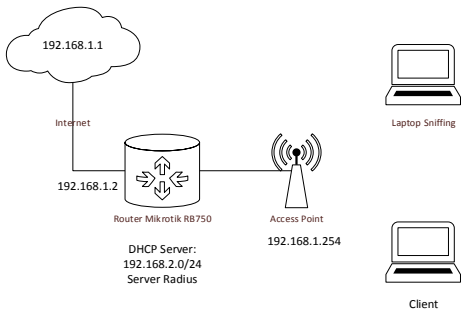
IP Address	Network
192.168.3.1	192.168.3.0/24
192.168.3.2	192.168.3.0/24
192.168.1.1	192.168.1.0/24
192.168.6.1	192.168.6.0/24
192.168.2.1	192.168.2.0/24

Tabel 3.1 Tabel Pengalamatan jaringan pada hotel Idoop

Dalam desain topologi jaringan yang sedang berjalan saat ini penerapan sistem autentikasi *Extensible Authentication Protocol-Tunelled Transport Layer Security (EAP-TTLS)* blm dilakukan pada router *MikroTIK* sehingga perlu di tambahkan untuk mencegah terjadi serangan dalam jaringan *wireless hotspot*, sehingga pengguna jaringan jadi aman dan nyaman.

b. Desain Jaringan Ujicoba

Pada desain jaringan ini akan dilakukan ujicoba *Extensible Authentication Protocol-Tunelled Transport Layer Security (EAP-TTLS)* pada router *MikroTIK* dan berikut adalah gambar topologi jaringan ujicoba:



Gambar 3.3 topologi jaringan ujicoba

4. Konfigurasi

Pada tahapan ini akan dilakukan tahapan – tahapan untuk melakukan konfigurasi pada router *MikroTIK* dan perangkat *client* yang digunakan. Berikut tahapan – tahapan yang akan dilakukan:

a. Konfigurasi *Router MikroTIK*

- Pengalamatan pada Router *MikroTIK*
- *IP Route* pada Router *MikroTIK*
- *IP Firewall NAT* pada router *MikroTIK*
- Konfigurasi *IP Hotspot Setup* pada *router MikroTIK*
- Menambahkan *user* pada *hotspot router MikroTIK*
- *Authentikasi* pada *Hotspot MikroTIK*
- *Radius Server* pada *Hotspot MikroTIK*
- Konfigurasi *User Manager* pada *Hotspot MikroTIK*
- Menambahkan *User* melalui *User Manager* untuk *Hotspot* user

b. Konfigurasi Laptop *Client*

Melakukan verifikasi koneksi dari laptop *client* ke *hotspot MikroTIK*

c. Konfigurasi Laptop *Sniffing*

- Melakukan verifikasi koneksi ke *server Hotspot MikroTIK*.
- Konfigurasi Aplikasi *Wireshark* untuk melakukan *Sniffing*

d. Ujicoba

Berikut adalah sekenario pengujian yang akan dilakukan pada jaringan *hotspot* dengan sistem authentikasi *EAP-TTLS*:

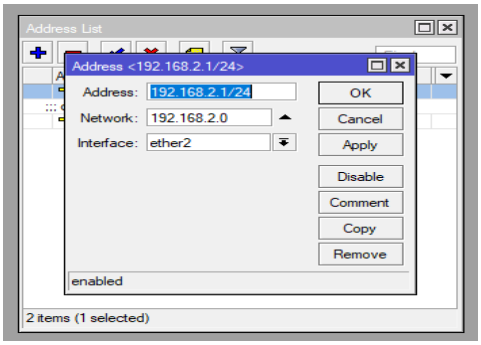
1. Mengkoneksikan laptop *sniffing* ke dalam jaringan *hotspot* dengan menggunakan *user* yang telah dibuat menggunakan fitur authentikasi *EAP-TTLS hotspot MikroTIK*.
2. Melakukan *sniffing* dengan menggunakan *wireshark* pada jaringan hotspot melalui laptop *sniffing* pada *hotspot MikroTIK*.
3. Mengkoneksikan laptop *client* ke jaringan *hotspot* dengan menggunakan *user* yang telah dibuat menggunakan fitur authentikasi *EAP-TTLS hotspot MikroTIK*.

III. HASIL DAN PEMBAHASAN

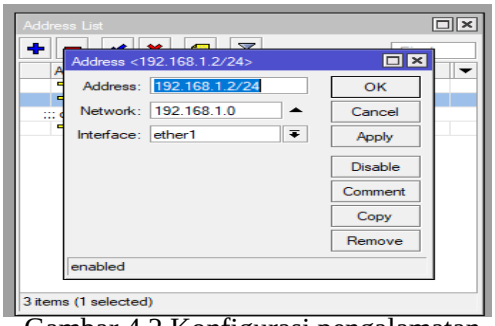
1. Konfigurasi

a. Konfigurasi pada *Router mikrotik*

1. Konfigurasi pengalamatan pada *router MikoTIK*



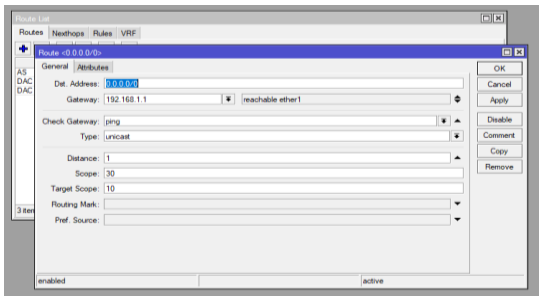
Gambar 4.1 Konfigurasi pengalamatan pada *interface ether* 2



Gambar 4.2 Konfigurasi pengalamatan pada *interface ether* 1

Pada konfigurasi ini dilakukan penambahan pengalamatan pada *router MikroTIK* pada masing masing *interface* yang ada pada router *MikroTIK*. Pada gambar 4.1 menerangkan tentang menambahkah alamat pada *interface ether2* yang bertindak sebagai *interface* yang terhubung untuk *hotspot* dan pada gambar 4.2 menerangkan tentang menambahkan alamat pada *interface ether1* untuk terhubung ke *internet* atau *ISP*.

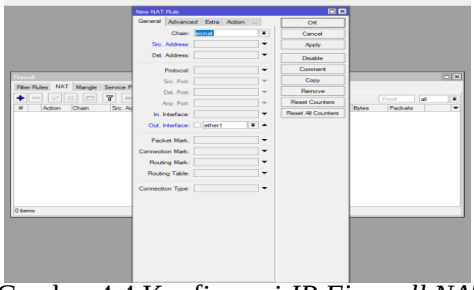
2. Konfigurasi *IP Route* pada *router MikroTIK*



Gambar 4.3 Konfigurasi *IP Ro*ute pada *Router MikroTIK*

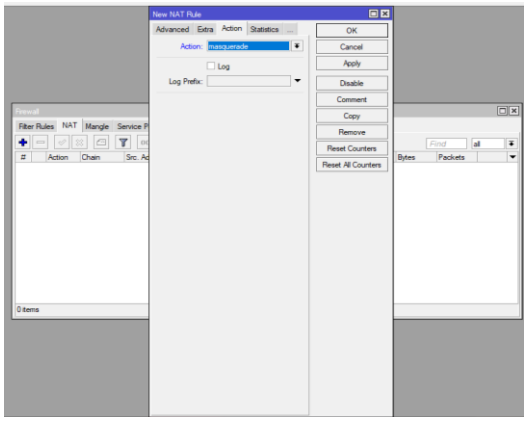
Pada gambar 4.3 konfigurasi ini dilakukan penambahan alamat *gateway* agar *router* dapat terhubung ke modem yang bertindak sebagai *ISP* agar *router* dapat terkoneksi ke jaringan *internet*.

3. Konfigurasi *IP Firwall NAT* pada *router MikroTIK*.



Gambar 4.4 Konfigurasi *IP Firewall NAT* pada *Router MikroTIK tab general*

Pada gambar 4.4 dilakukan konfigurasi *Firewall NAT* pada *router MikroTIK* dimana dilakukan pengaturan pada *tab general* dan *chain* di isikan *srcnat* untuk *out interface* di isikan *ether 1* yang mengarah ke *internet*.



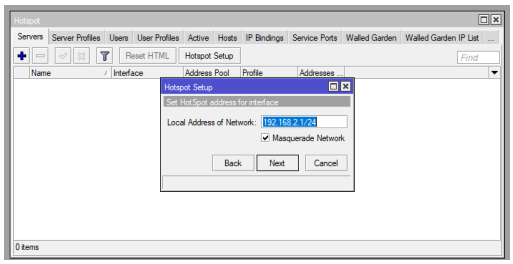
Gambar 4.5 Konfigurasi *IP Firewall NAT* pada *Router MikroTIK tab Action*

Pada gambar 4.5 dilakukan pengaturan *firewall nat* pada *tab action* yang diisi dengan *masquerade* agar setiap *client* yang terhubung ke jaringan *hotspot* dapat terkoneksi ke *Internet*.

4. Konfigurasi *IP Hotspot Setup* pada *router MikroTIK*.

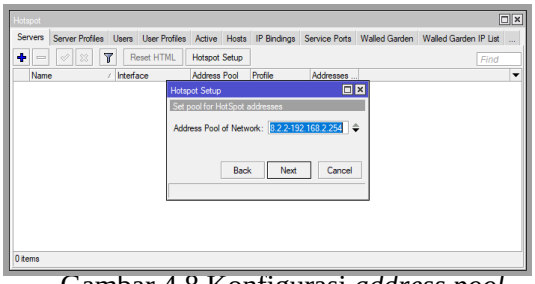
Gambar 4.6 Konfigurasi *interface* untuk *hotspot* melalui *hotspot setup*

Gambar 4.6 menunjukkan konfigurasi *interface* yang akan digunakan untuk jaringan *hotspot* pada langkah setup *hotspot* di *router MikroTIK.*



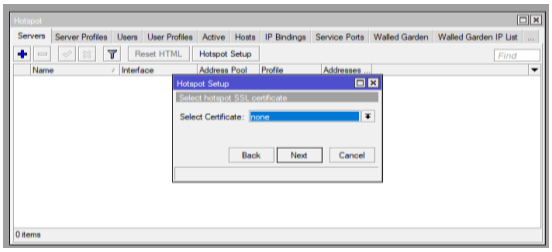
Gambar 4.7 Konfigurasi *local network address* melalui *hotspot setup*

Pada gambar 4.7 menerangkan tentang konfigurasi *network address* untuk jaringan *hotspot* yang akan dibuat.



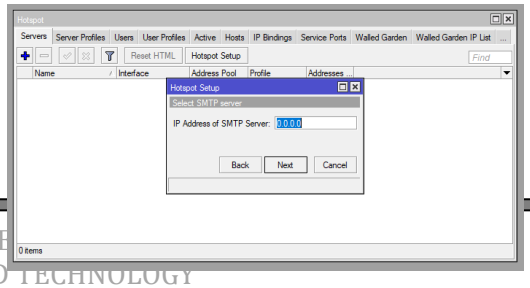
Gambar 4.8 Konfigurasi *address pool* melalui *hotspot setup*

Pada gambar 4.8 menerangkan tentang konfigurasi *address pool* untuk jaringan *hotspot* yang akan dibuat.



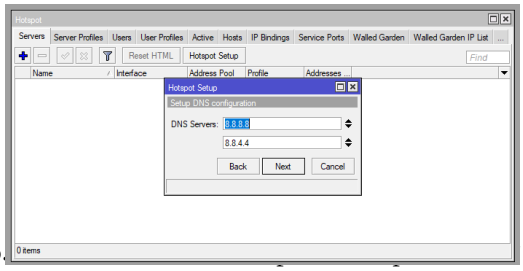
Gambar 4.9 Konfigurasi *certificate* untuk *hotspot* melalui *hotspot setup*

Pada gambar 4.9 menunjukan pemilihan sertifikat elektronik untuk jaringan *hotspot* dan penulis memilih none karena tidak menggunakan sertifikat elektronik.

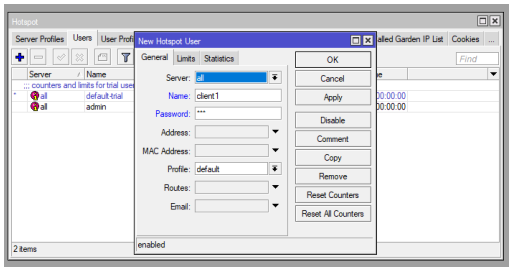


Gambar 4.10 Konfigurasi *SMTP Server* untuk *hotspot* melalui *hotspot* setiup

Pada gambar 4.10 menunjukkan konfigurasi alamat untuk *SMTP server* dan pada pilihan ini karena tidak menggunakan *SMPT server* maka penulis tidak mengisi dan secara *default* terisi 0.0.0.0.

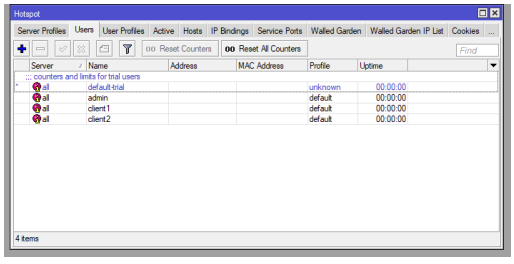


5. *MikroTIK*



Gambar 4.15 Menambahkan *user* pada *hotspot router MikroTIK*

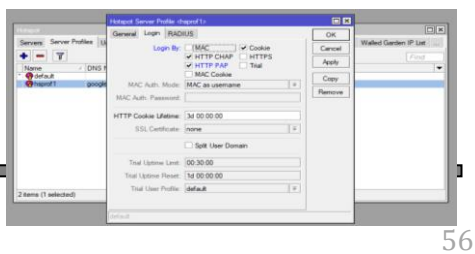
Pada gambar 4.15 akan dilakukan penambahan user hotspot yang akan digunakan untuk *client* hotspot.



Gambar 4.16 Menambahkan *user* pada *hotspot router MikroTIK*

Pada gambar 4.16 menunjukkan hasil pembuatan *user* untuk *client hotspot.*

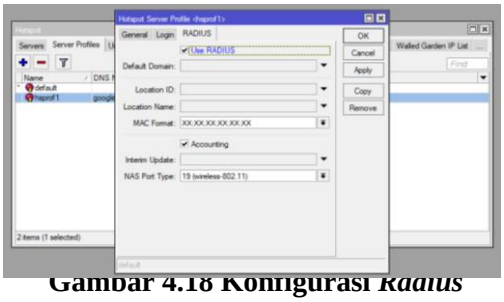
6. Konfigurasi *Authentikasi* pada *Hotspot MikroTIK*



Gambar 4.17 Konfigurasi *Authentikasi* pada *hotspot MikroTIK*

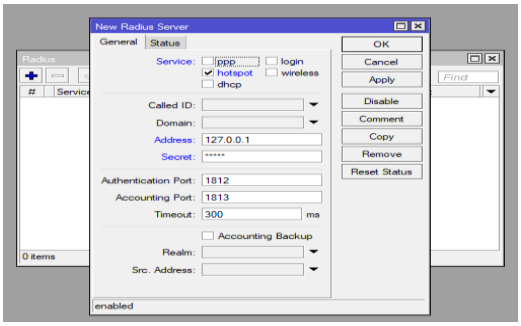
Pada pada gambar 4.17 akan dilakukan konfigurasi authentikasi *EAP-TTLS* pada *hotspot MikroTIK* yaitu *HTTP-CHAP* dan *HTTP-PAP*.

7. Konfigurasi *Radius Server* pada *Hotspot MikroTIK*



Gambar 4.18 Konfigurasi *Radius Server* pada *hotspot MikroTIK*

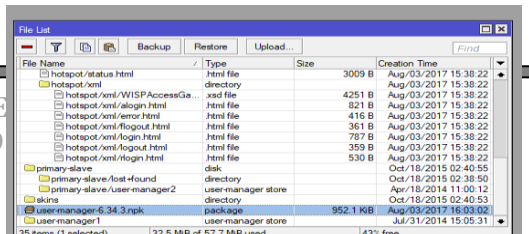
Pada gambar 4.18 menerangkan cara mengaktifkan radius *server* pada *server hotspot MikroTIK*.



Gambar 4.19 Konfigurasi *Radius Server* pada *hotspot MikroTIK*

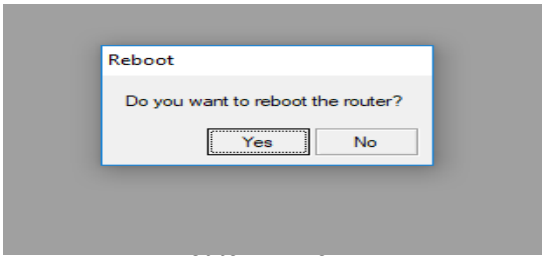
Pada gambar 4.19 menerangkan membuat *server radius* untuk jaringan *hotspot* yang sudah dibuat dan agar *username* dan *password* untuk *client hotspot* dapat dibuat menggunakan *usermanager* dan dapat disimpan secara terpusat dimana untuk konfigurasi pada address ditambahkan *IP Address* dari *MikroTIK* dan *secret* adalah *password* agar *usermanager* dapat terhubung dengan *server radius*.

8. Melakukan instalasi *Usermanager* pada *router MikroTIK*.

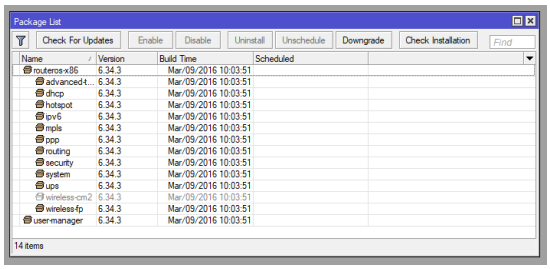


Gambar 4.20 instalasi *User Manager* pada *router MikroTIK*

Pada gambar 4.20 menerangkan cara instalasi *usermanager* pada *router MikroTI* yang mana mengcopykan aplikasi *usermanager* pada *router MikroTIK* pada *menu filelist*.



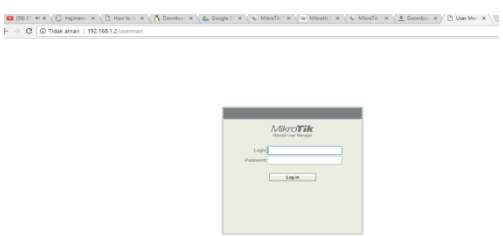
Pada gambar 4.21 menerangkan untuk melakukan *restart* router *MikroTIK* untuk melakukan proses instalasi *usermanager* pada *router MikroTIK*.



Gambar 4.22 hasil instalasi *Usermanager* pada *router MikroTIK*

Pada gambar 4.22 menerangkan hasil instalasi aplikasi *usermanager* yang pada *package list* di *router MikroTIK*.

9. Konfigurasi *Usermanager* pada *Hotspot MikroTIK*



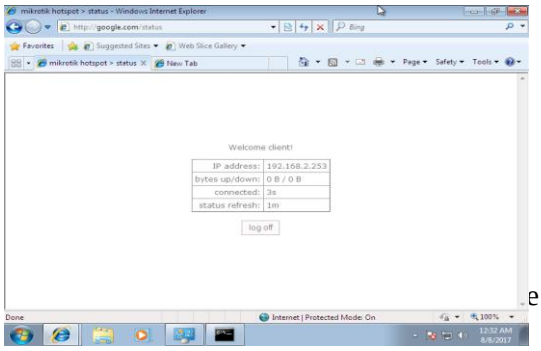
Gambar 4.23 *Login Form User Manager* pada *hotspot MikroTIK*

Pada gambar 4.23 melakukan akses ke *Usermanager* yang beralamatkan 192.168.1.2/*userman* dan melakukan *login* dengan *default username admin* tanpa menggunakan *password*.

2. Pengujian

Pada sub bab ini akan dilakukan pengujian berdasarkan dari sekenario pengujian yang telah dibuat sebelumnya dan membuat kesimpulan berdasarkan hasil pengujian yang didapatkan. Berikut langkah – langkah pengujian yang akan dilakukan :

1. Mengkoneksikan laptop *sniffing* ke dalam jaringan *hotspot* dengan *hotspot MikroTIK* dan melakukan *login* dengan menggunakan *user* yang telah dibuat.



Pada gambar 4.32 menerangkan bahwa *client sniffing* sudah melakukan *login* ke jaringan *hotspot* dengan menggunakan *user client*.

3. Hasil Pengujian

Pada analisa hasil pengujian akan disimpulkan hasil dari pengujian yang dilakukan pada hasil pengujian. Adapun analisa hasil pengujian yang penulis lakukan sebagai berikut:

1. Berdasarkan hasil tanggapan kuisioner pada *table* 4.1, dapat disimpulkan bahwa authentikasi *EAP-TTLS* memiliki kemampuan yang lebih baik dan mudah untuk diterapkan pada *router MikroTIK* dan dapat mempermudah kinerja teknisi *IT* Hotel Idoop dalam melakukan manejemen *client* dalam jumlah yang banyak.
2. Berdasarkan pengujian yang dilakukan penulis tipe authentikasi *EAP-TTLS* sangat mudah untuk diterapkan yang ditambah dengan dukungan fitur dari *hotspot MikroTIK* yang memiliki kemampuan dalam melakukan enkripsi *password* menggunakan *MD5*, membuat tipe atuhentikasi ini lebih aman untuk diterapkan. Penggunaaan *username* dan *password* yang bertidak sebagai pengganti sertifikat digital membuat tipe authentikasi ini lebih mudah untuk digunakan pada jaringan *hotspot*.

IV. SIMPULAN DAN SARAN

1. **Kesimpulan**

Adapun kesimpulan yang dapat diambil dari pengujian yang dilakukan adalah sebagai berikut:

1. Authentikasi *EAP-TTLS* memiliki kemampuan yang lebih baik yang ditambahkan enkripsi *MD5* pada *hotspot MikroTIK*
2. Mudah untuk diterapkan pada *router MikroTIK*.
3. Mempermudah kinerja teknisi *IT* HOTEL IDOOP dalam melakukan manejemen *client* dalam jumlah yang banyak.
4. Penggunaaan *Username* dan *Password* yang bertidak sebagai pengganti sertifikat digital membuat tipe authentikasi ini lebih mudah untuk digunakan pada jaringan *Hotspot*.

2. **Saran**

Adapun saran-saran untuk pengembangan penelitian ini lebih lanjut adalah sebagai berikut:

1. Perlunya pengembangan dalam penerapan authentikasi *EAP-TTLS* di sisi keamanan karena *password* dan *username* yang masih belum dienkripsi.
2. Perlunya dilakukan pengujian pada *system* yang berbeda untuk mengetahui lebih jauh tentang performa dari authentikasi *EAP-TTLS*.
3. Perlunya eksplorasi yang lebih dalam mencoba tipe authentikasi *EAP-TTLS* selain *HTTP-CHAP* dan *HTTP-PAP* pada jaringan *hotspot.*

REFRENSI

[1.] *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)*.(2017).diakses pada tanggal 10 agustus 2017 dari: https://tools.ietf.org/html/rfc5281
[2.] Idoop Hotel.(2017).topology jaringan idoop hotel .it *departement* idoop hotel.
[3.] Mikrotik routeros.(2017). diakses pada tanggal 2 agustus 2017 dari:http://www.mikrotik.co.id.