Pengamanan Jaringan *Wireless* LAN Dengan Protokol EAP-TTLS Dan Otentikasi MSCHAPv2 Pada AP Tipe ZTE ZXHN F6093

Kukuh Bagas Permadi [1], Henki Bayu Seta [2], Ria Astriratma [3]
Program Studi Informatika / Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Jl. RS. Fatmawati Raya, Pd. Labu, Kec. Cilandak, Kota Depok, Jawa Barat 12450
bagas.abjay@gmail.com, henkiseta@upnvj.ac.id, astriratma@upnvj.ac.id

Abstrak. Penggunaan pada protokol WPA memiliki dua proses, antara lain adalah otentikasi serta enkripsi. Pada tingkat *network* dengan infrastuktur yang besar serta dengan lalu lintas *network* yang tinggi sama halnya dengan universitas, kantor perusahaan atau tempat umum lainnya yang menggunakan *wireless* LAN, proses otentikasi merupakan proses yang pertama kali yang dilakukan agar pengguna jaringan *wireless* LAN dapat mengakses jaringan *internet*. Maka dari itu, tidak hanya aman namun proses otentikasi bisa beroperasi dengan cepat. Solusi dari penelitian ini adalah dengan menerapkan Protokol IEEE 802.1x EAP dengan *Extensible Authentication Protocol – Tunneled Transport Layer Security* (EAP-TTLS) untuk membuat *secure tunnel* (terowongan keamanan) dalam pertukaran kunci pada jaringan *wireless*, serta dengan *inner authentication Microsoft Challenge Handshake Authentication Protocol Version 2* (MSCHAPv2). Luaran yang dihasilkan pada penelitian ini adalah membangun suatu keamanan pada jaringan *wireless* terpusat pada Fakultas Ilmu Komputer UPN Veteran Jakarta.

Kata Kunci: IEEE 802.1x EAP, EAP-TTLS, MSCHAPv2, RADIUS *Server*, *Wireless* LAN.

1 Pendahuluan

Pada masa globalisasi yang mengandalkan komunikasi dan informasi seperti yang sekarang ini, penggunaan perangkat mobile sering diterapkan dan digunakan. Penggunaan seperti laptop (*notebook*) dan *smartphone* yang menggunakan media nirkabel mampu mempermudah dan mempercepat pekerjaan dengan efektif dan efisien, selain perangkat mobile juga ada teknologi yang dapat mempermudah pekerjaaan manusia salah satunya yaitu jaringan nirkabel (*wireless* LAN). *Wireless* LAN menjadi daya tarik tersendiri bagi penggunanya karena mereka dapat menggunakan jaringan *internet*, dengan keunggulan dalam mengakases jaringan *internet* secara gratis tersebut, *Wireless* LAN juga mudah dijumpai pada beberapa lokasi diantaranya yaitu kampus, kantor, *mall*, kafe serta lokasi lainnya yang memiliki titik *hotspot*. Namun dengan semua kemudahan teknologi tersebut muncul sebuah permasalahan dalam keamanan, karena data yang melewati *wireless* akan sangat mudah untuk dicuri dan dibaca bahkan dapat dimanipulasi oleh pihak-pihak yang tak bertanggung jawab [1].

Penggunaan pada protokol WPA memiliki dua proses, antara lain adalah otentikasi serta enkripsi. Pada tingkat *network* dengan infrastruktur yang besar serta dengan lalu lintas *network* yang tinggi sama halnya dengan kampus, kantor perusahaan atau tempat umum lainnya yang menggunakan *wireless* LAN, proses otentikasi merupakan proses yang pertama kali yang dilakukan agar pengguna jaringan *wireless* LAN dapat mengakses jaringan *internet*. Maka dari itu, tidak hanya aman namun proses otentikasi bisa beroperasi dengan cepat [1].

Pada Universitas Pembangunan Nasional Veteran Jakarta menggunakan keamannan jaringan *wireless* LAN dengan WPA 2 *personal* serta dengan otentikasi PSK (*Pre-Shared Key*). Otentikasi *Pre-Shared Key* sangat rentan dengan adanya tipe penyerangan *dictiornary attack* dengan mencoba banyak kemungkinan dalam mendapatkan *password*. Oleh karena itu, dibutuhkan penerapan protokol otentikasi dan enkripsi yang digunakan pada jaringan *wireless* LAN, salah satunya IEEE 802.1x EAP yang merupakan protokol otentikasi untuk menangani masalah pada kasus ini. IEEE 802.1x EAP mampu menangani kendali pada jaringan *wireless*. EAP *method* yang penulis pilih pada penelitian ini adalah *Extensible Authentication Protocol – Tunneled Transport Layer Security* (EAP-TTLS) untuk membuat *secure tunnel* (terowongan keamanan) dalam pertukaran kunci pada jaringan *wireless*. Keamanan jaringan ini juga menggunakan *inner authentication* yaitu dengan *Microsoft Challenge Handshake Authentication Protocol Version 2* (MSCHAPv2). MSCHAP memiliki protokol keamanan yang dikembangkan oleh tim *Microsoft* agar dapat melakukan *Mutual Authentication* atau otentikasi dua arah dengan menggunakan kombinasi *username* serta *password* [1]. Selain menggunakan protokol otentikasi tersebut. Penulis juga menggunakan *Remote Dial-in User Service* (RADIUS) untuk menangani proses otentikasi secara terpusat. Sehingga menjadikan protokol keamanan jaringan wireless LAN pada lingkungan Fakultas Ilmu Komputer UPN VETERAN Jakarta secara terpusat, sehingga pada penelitian ini penulis memberi judul "**Pengamanan Jaringan *Wireless* LAN Dengan Protokol EAP-TTLS Dan Otentikasi MSCHAPV2 Pada Fakultas Ilmu Komputer UPN Veteran Jakarta**". Dengan harapan hasil penelitian ini dapat meningkatkan keamanan data bagi pengguna jaringan *Quality of Service* di lingkungan Fakultas Ilmu Komputer UPN Veteran Jakarta.

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

1.1 Rumusan Masalah

1. Bagaimana implementasi RADIUS *server* dalam mengamankan jaringan *wireless* LAN pada AP tipe ZTE ZXHN F6093?
2. Bagaimana cara metode MSCHAPv2 mengotentikasi dalam mengamankan jaringan *wireless* pada AP tipe ZTE ZXHN F6093?
3. Apakah protokol EAP-TTLS dan otentikasi MSCHAPv2 mampu mengamankan jaringan *wireless* LAN dari serangan *dictionary attack* pada AP tipe ZTE ZXHN F6093?

2 Kajian Pustaka

2.1 Jaringan Wireless Local Area Network (WLAN)

Wireless LAN atau biasa dikenal dengan jaringan tanpa kabel (nirkabel), merupakan sebuah media transmisi yang memanfaatkan gelombang radio dalam penggunaannya, dengan mentransmisikan informasi berupa data-data digital melalui *wireless* yang kemudian terjadi proses *modulation* pada aliran *electromagnetic* yang tersebar diudara. Wi-Fi *Alliance* dapat memapaparkan buatan *Wireless Local Area Network* (WLAN) dengan menamainya *Wireless Fidelity* (Wi-Fi) dengan berlandaskan standar *Institute of Electrical and Electronics Engineers* (IEEE) 802.11. Berbeda halnya mengenai *network* yang masih *wired*, pada *network* nirkabel terdapat dua model agar bisa dimanfaatkan tergantung kebutuh antara lain model *Ad-Hoc* dan model infrastruktur. Pada model *Ad-Hoc* merupakan korespondemsi dengan spontan/langsung antara per-komputer melalui nirkabel (WLAN), sedangkan pada model infrastruktur memiliki komponen penting yang dibutuhkan pada model ini yaitu *access point*, karena pada komunikasi antara tiap masing-masing komputer akan melewati *access point* pada kabel (LAN) ataupun tanpa kabel (WLAN) [1].

Jaringan *wireless* LAN merupakan teknologi yang menggunakan media transmisi yang mentransmisikan informasi berupa data-data dengan penggunaan gelombang radio tanpa penggunaan kabel. *Institute for Electrical and Electronics Engineers* (IEEE 802.11) ialah suatu standar *wireless* LAN, dibutuhkannya suatu standar karena meski terdapat banyak ragam barang dari nirkabel dan semua bermula dari penjual yang berbeda-beda, tetapi masih tetap saling bekerja sama pada jaringan [2].

2.2 Komponen Otentikasi Pada 802.1x

Terdapat 3 entitas pada komponen otentikasi 802.1x [3], berikut penjelasannya:
1. *Supplicant* atau pengakses jaringan yang berupa perangkat pengguna, sebagaimana layaknya komputer, laptop, ataupun *handphone* agar dapat terhubung pada *network* WLAN/LAN dengan cara mengirim *request* berbentuk otentikasi ke *authenticator* melewati *access point* yang nantinya dilanjutkan ke *authentication server* agar dapat mengakses jaringan *internet.*
2. *Authenticator*, berfungsi sebagai *filter* antara *supplicant* dengan *authentication server*. Apabila *supplicant* diperiksa dan tidak divalidasi pada tahap *identity* maka *supplicant* tidak dapat mengakses jaringan. Cara kerja *authenticatior* adalah dengan menerima request dari *supplicant* yang nantinya diteruskan lagi menuju otentikasi *server* agar dapat memastikan jika perangkat tadi otentik/tidaknya. Pengotentikasi sering dikenal sebagai *Network Access Server* (NAS), pada jaringan *wireless authenticator* pada umumnya merupakan sebuah *access point*.
3. *Authentication Server,* pada umumnya *authentication server* berfungsi sebagai pemeriksa suatu entitas yang ingin mencoba masuk ke dalam suatu jaringan *wireless*, *authentication server* kemudian menentukan apakah entitas tersebut berhak mengakses jaringan atau tidaknya. *Authentication server* pada dasarnya merupakan *server* yang mendukung protokol keamanan jaringan *wireless* seperti RADIUS dan EAP.

2.3 *Authentication, Authorization, and Accounting* (AAA)

Ada tiga fitur utama dari AAA [4], model AAA (*authentication, authorization, dan accounting*) yaitu:
1. *Authentication,* otentikasi merupakan metode konfirmasi *identity* pengguna (*end-user*) agar dapat terhubung ke *network*.
2. *Authorization*, otoritas merupakan metode pembuktian kewenangan pada *client* pengguna *network computer* yang mereka punyai.
3. *Accounting*, pendaftaran akun merupakan metode penjumlahan yang dilaksanakan pada *system,* setelah itu dilakukan pendataan pada penggunaan jaringan *internet* yang sudah digunakan bagi *user network wireless*.

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

2.4 *Remote Dial-In Users Service* (RADIUS)

RADIUS merupakan suatu protokol security pada computer agar mendukung dalam hal *authentication*, otoritas, serta *accounting* secara terpusat dalam mengakases suatu jaringan wireless LAN. Selain diimplementasikan sebagai protokol keamanan terpusat, RADIUS sekarang sudah digunakan sebagai otentikasi akan jalan masuk network dengan penggunaan jarak jauh, yaitu salah satu pengimplementasian kaitan dial-up, sebagaimana halnya Virtual Private Networking (VPN) [5].

Cara membangun RADIUS *server* adalah dengan melakukan beberapa tahapan konfigurasi dari awal yaitu konfigurasi Mikrotik RB951, konfigurasi firewall NAT, konfigurasi *access point* hingga konfigurasi *hotspot* maka setelah itu RADIUS *server* akan terbangun [6].

RADIUS merupakan *security protocol* jaringan computer secara terpusat agar difungsikan dalam membangun access management dengan terpusat pada suatu *network* dengan skala yang cukup banyak dan pertama kali dikembangkan oleh Livingston Enterprise. RADIUS biasa digunakan pada perusahaan atau universitas atau tempat-tempat lainnya yang memiliki trafik tinggi serta memimiliki skala yang cukup besar dalam mengatur akses ke internet ataupun internet bagi pengguna [7].

2.5 *Extensible Authentication Protocol* (EAP)

Pada umumnya EAP merupakan suatu kerangka otentikasi perolehan pertumbuhan dari standar IEEE agar berguna dan tetap flexible. Lebih jelasnya EAP cukup memberikan peran "mengangkut" dalam mengirim data otentikasi, agar nantinya diberikan pada metode EAP sehingga pada konsep ini EAP bukanlah mekanisme otentikasi secara specific. Oleh karena itu, jika misalkan terdapat metode otentikasi (*new method*), maka sistem tidak melaksanakan dengan meningkatkan terhadap perangkat komponen *network*. ditemukan lebih dari 30 metode EAP, tetapi hanya ada 7 dengan mendapati standar dalam beroperasi pada *network wireless* seperti yang dicantumkan dalam dokumen *Request For Comments* (RFC 4017) serta sudah diakui dengan *Wi-Fi Alliance* hanya ada 7, yang salah satu EAP Method nya yaitu EAP-TTLS [8].

2.6 *Extensible Authentication Protocol – Tunneled Transport Layer Security* (EAP-TTLS)

Tentang standar RFC 5281 " *Extensible Authentication Protocol Tunneled Layer Security Authenticated Protocol Version 0* (EAP-TTLSv0)" EAP TTLS adalah metode otentikasi dengan cara membuat *secure tunneling* yang terdiri dari dua langkah: Langkah satu tujuannya adalah untuk membuat *secure tunnel* (terowongan keamanan) enkripsi simetris berdasarkan sertifikat digital server yang memungkinkan verifikasi *server* klien. Sementara langkah kedua memungkinkan *server* untuk memverifikasi klien identitas dengan metode internal lain melalui terowongan yang dibuat. TTLS mendukung beberapa protokol untuk otentikasi bagian dalam tersebut seperti EAP-MD5, PAP, CHAP, MSCHAP, MSCHAPv2, dll [9].

2.7 *Microsoft Challenge Handshake Authentication Protocol Version 2* (MSCHAPv2)

Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) adalah hasil perkembangan dari sistem protokol keamanan *authentication Challenge Handshake Authentication Protocol* (CHAP) dimodifikasi dengan tim *microsoft*. MSCHAPv2 mempunyai kesamaan dengan protokol versi sebelumnya yaitu MSCHAPv1 dan juga dengan protokol CHAP standardnya. Terdapat perbedaan yang mendasar dari protokol MSCHAPv1 dan protokol MSCHAPv2 yaitu, pada versi ke 2 telah ditambahkan fitur *mutual authentication* antara *authenticator* (*access point*) dengan *supplicant* (pengguna jaringan) [10].

3 Identifikasi Masalah

Pada bagian ini dijalankan untuk melihat permasalahan terkait topik yang ingin diteliti. Ruang lingkup permasalahan kemudian dipersempit menjadi lebih spesifik terhadap akar permasalahan. Dalam penelitian ini terdapat permasalahan yang ditemukan pada wireless LAN Fakultas Ilmu Komputer UPN Veteran Jakarta yaitu masalah pada keamanan otentikasi pengguna jaringan *wireless* LAN. Karena pada umumnya jaringan *wireless* LAN digunakan sebagai *hotspot* untuk mendapatkan akses *internet*, sehingga hal tersebut rentan terhadap penyerangan bila kurangnya keamanan pada jaringan *wireless* LAN. Sebelumnya penulis juga sudah melakukan pengamatan yaitu dengan datang langsung ke lokasi untuk mengumpulkan data serta informasi yang dibutuhkan. Penulis juga melakukan survei dengan mencoba terhubung

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

ke jaringan *wireless* pada Selasar Fakultas Ilmu Komputer, dan menemukan bahwa Fakultas Ilmu Komputer menggunakan WPA2 *Personal* dengan otentikasi PSK (*Pre-Shared Key*).

3.1 Pengumpulan Data

Tahap ini merupakan metode yang berguna untuk menjalankan suatu analisa data serta menjadikannya suatu informasi, yang nantinya dijalankan agar dapat melihat persoalan yang dibahas. Langkah ini dibagi menjadi dua hal, dapat dijabarkan dibawah ini:

3.2 Studi Literatur

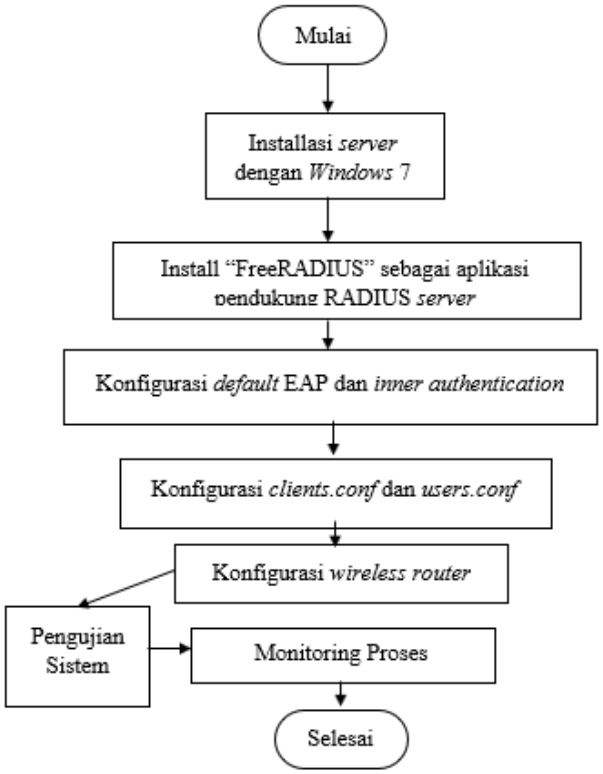
Tahap ini merupakan teknik penggabungan data menggunakan artikulasi, jurnal, dan skripsi yang sesuai dengan pembahasan serta juga memilih data dari *internet* agar dapat digunakan sebagai tumpuan pada penelitian yang akan dilaksanakan.

3.3 Studi Lapangan

Pada tahap ini dilakukannya penggabungan data melalui cara melaksanakan pengamatan dengan datang ke lapangan secara langsung sebagai tujuan penelitian.

3.4 Tahapan Konfigurasi

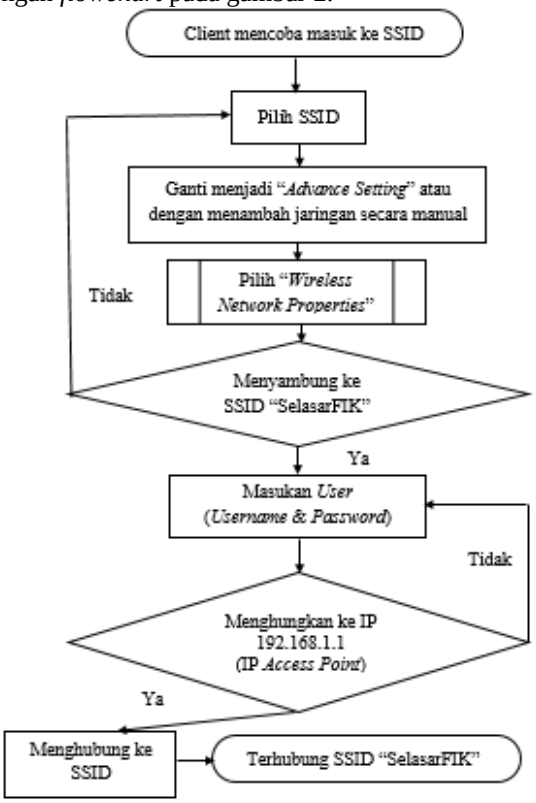
Dalam Tahap ini dilakuakan konfigurasi pada sistem yang akan digunakan. Rancangan penelitian ini terdapat 7 tahapan di dalamnya pada gambar 1 di bawah ini.



Gambar. 1. *Flowchart* Tahapan Konfigurasi

3.5 Pengujian Sistem

Dalam pengetesan sistem, pengguna agar dapat terhubung kedalam jaringan, berikut tahap-tahap pada pengguna agar dapat terhubung dan terlindungi dalal *authentication* nya ke dalam jaringan *wireless* sampai bisa mengakses jaringan *internet* yang akan digambarkan dengan *flowchart* pada gambar 2.

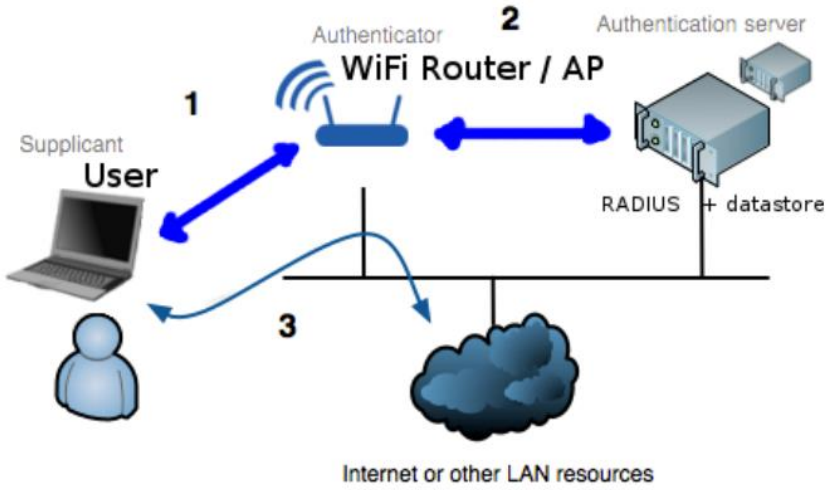


Gambar. 2. *Flowchart* Pengujian Sistem

Pengujian sistem dimulai dilakukan dengan *client* mencoba masuk ke SSID, pengujian sistem dikatakan selesai dan berhasil hingga *client* dapat terhubunga ke jaringan dan gagal bila tidak dapat terhubung ke jaringan. Pada penelitian ini penulis membuat SSID baru beranama "SelasarFIK" dengan IP *access point* yang digunakan yaitu 192.168.1.1

3.6 Topologi Jaringan

Topologi jaringan pada *Free*RADIUS memiliki 3 komponen didalamnya yaitu *supplicant*, *authenticator*,serta *authentication server*, dapat digambarkan pada gambar 3 dibawah ini.



Gambar. 3. Topologi Jaringan menggunakan *Free*RADIUS

3.6 Alat Bantu Penelitian

Komponen yang difungsikan terhadap penelitian ini ada dua macam yaitu peralatan lunak (*software*) serta peralatan keras (*hardware*) dapat dijabarkan sebagai berikut:

1. Peralatan Lunak (*Software*)

Peralatan lunak (*software*) yang digunakan dalam penelitian ini antaralain adalah sebagai berikut:
1. *Free*Radius versi 1.1.7-r0.0.2
2. *Wireshark* versi 3.2.6
3. *Airmon-ng* versi 1.6
4. *Airodump-ng* versi 1.6
5. *Aireplay-ng* versi 1.6
6. *Aircrack-ng* versi 1.6

2. Peralatan Keras (*Hardware*) *Access Point*

Peralatan keras (*hardware*) *access point* yang digunakan dalam penelitian ini sebagai berikut:
1. Model : ZTE ZXHN F6093
2. MAC : 24-58-6E-D0-7C-EC
3. Product : GPON ONT

3. Peralatan Keras *(Hardware*) PC *Server*

Peralatan keras (*hardware*) pada PC *server* yang digunakan dalam penelitian ini antara lain sebagai berikut:
1. Processor : *Intel®Core™*i3-2370M CPU @ 2.40 GHz, ~2.40GHz
2. RAM : 4GB
3. Type : DDR 3
4. Hard Disk : 500GB
5. VGA : *Intel®* HD *Graphic* 3000
6. *Operating System* (OS) *Windows 7*

4. Peralatan Keras (*Hardware*) PC *Client*

Peralatan keras (*hardware*) pada PC *client* yang digunakan dalam penelitian ini antara lain sebagai berikut:
1. Processor : *Intel®Core™*i7-8750H CPU @ 2.20 GHz (12 CPUs), ~ 2.2GHz
2. RAM : 16GB
3. Type : DDR 4
4. Hard Disk : 1TB
5. VGA : NVIDIA *GeForce* GTX 1060
6. *Operating System* (OS) *Windows 10*

4 Pengujian Sistem

4.1 Perbandingan Sistem Yang Digunakan

Perbandingan sitem yang digunakan dapat dipaparkan pada tabel 1 berikut ini:

Tabel 1. Perbandingan Sistem yang digunakan

No	Perbandingan	Keamanan Sebelumnya	Keamanan Yang Digunakan	Perbandingan
1	Tipe keamanan	Menggunakan WPA2-*personal.*	Menggunakan WPA2-*enterprise.*	Tipe keamanan
2	Otentikasi yang digunakan	Menggunakan jenis otentikasi PSK (Pre-Shared Key).	Menggunakan EAP-TTLS serta *inner authentication* MSCHAPv2.	Otentikasi yang digunakan
3	Kegunaan	WPA2-*personal* sangat efektif untuk	WPA2-*enterprise* dapat	Kegunaan

keamanan jaringan wireless rumahan (dengan trafik data rendah serta dengan jumlah pengguna jaringan yang sedikit).	diimplementasikan pada trafik data tinggi dan pengguna jaringan yang banyak.

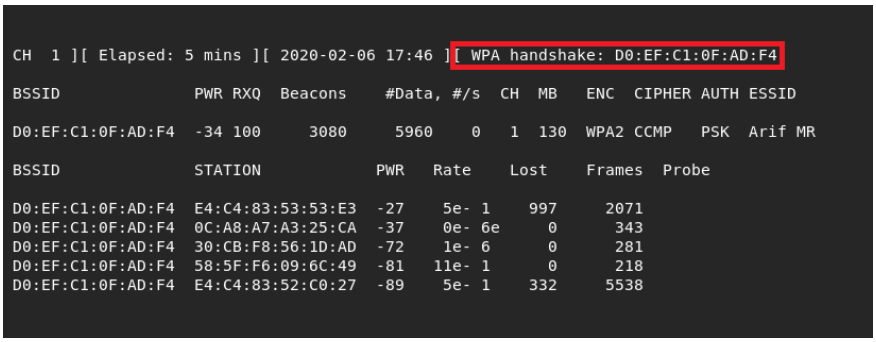
4.2 Pengujian Efektifitas Sistem Sebelumnya

Pengujian efektifitas sistem dilakukan dengan menggunakan *dictionary attack* menggunakan *tools airmon-ng*, *airodump-ng*, *aireplay-ng*, dan *aircrack-ng* pada keamanan jaringan *wireless* WPA2-*Personal* dengan otentikasi PSK. Pertama-tama gunakan *tools airmon-ng* untuk mengubah mode *wireless* dari "*Manage*" ke mode "*Monitor*", dalam mode *Manage* fungsi ini menangkap paket data dari perangkat pengguna ke *access point* dan *access point* ke perangkat pengguna. Sedangkan pada mode *Monitor* dapat menangkap dan membaca paket yang tersebar melalui udara.

Selanjutnya menangkap paket yang dikirimkan melalui udara dengan tools *airodump-ng* untuk monitoring trafik jaringan, lalu fokuskan ke MAC *address* dan *channel* pada *access point* target. Kemudian menggunakan *tools aireplay-ng*, *tools* ini berfungsi untuk melakukan *deauthentication attack* untuk mengeluarkan pengguna jaringan secara paksa. Kemudian ketika pengguna jaringan itu masuk ke jaringan kembali, *airodump-ng* mendeteksi dan mendapatkan *handshake*, kemudian menyimpannya dalam *file* "*pcap*" serperti pada gambar 4. Pengujian dilakukan sebanyak sepuluh kali dengan menggunakan *stopwatch* dalam mengukur waktu untuk *airodump-ng* mendapatkan *handshake* ditunjukkan pada tabel 2.

Tabel 2. Pengujian *Airodump-ng* Dalam Mendapatkan *Handshake*

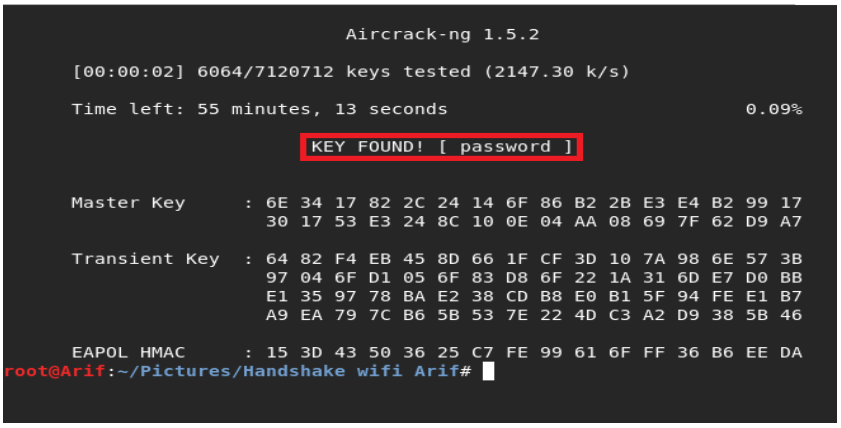
Percobaan	Waktu (detik)
1	1.57
2	1.08
3	1.77
4	2.01
5	1.55
6	1.81
7	0.91
8	1.20
9	1.80
10	0.50



Gambar. 4. *Airodump-ng* mendapatkan *handshake*

Dan langkah terakhir penyerang adalah *file* "pcap" dilakukan *dictionary attack* dengan mencoba semua kemungkinan yang ada pada *wordlist* dengan menggunakan *tools aircrack-ng*, dan mendapatkan kata sandi berdasarkan *handshake* yang telah didapat sebelumnya. Sehingga didapatkan kata sandi pada keamanan tersebut adalah "*password*" dapat ditunjukkan seperti pada gambar 5.

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)



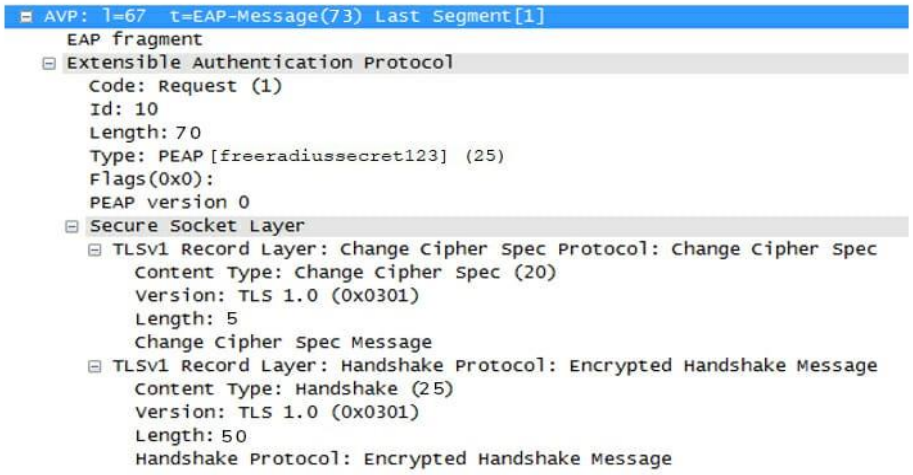
Gambar. 5. *Aircrack-ng* mendapatkan kata sandi.

4.3 Analisa Cara Kerja Protokol EAP-TTLS dan MSCHAPv2

Proses otentikasi pada protokol EAP-TTLS MSCHAPv2 yaitu dengan membentuk jalur komunikasi dengan menggunakan *Transport Layer Security* (TLS) antara pengguna jaringan *wireless*, *wireless access point*, dan *authentication server* atau RADIUS *server*. Terdapat 2 tahapan didalamnya, tahap awal, TTLS membentuk suatu terowongan yang nantinya digunakan sebagai jalur komunikasi, pada tahap ini rangkaian pesan EAP dikirim di antara pengguna *wireless* dan RADIUS *server* secara terenkripsi. Tahap ini dikatakan selesai bila RADIUS *server* mengotentikasi ke pengguna jaringan (*client*) dan kedua nya sudah saling memastikan *encrpytion key* pada terowongan TLS agar memanfaatkan *public key* dengan cara rangkaian pesan berupa EAP-*Message* dapat dilihat dengan *tool wireshark* seperti pada gambar 6. Pengujian dilakukan sebanyak sepuluh kali menggunakan *stopwatch* dalam mengukur waktu untuk EAP-TTLS membuat jalur TLS ditunjukkan pada tabel 3.

Tabel 3. Pengujian EAP-TTLS Untuk Membuat Jalur TLS

Percobaan	Waktu (detik)
1	3.19
2	2.92
3	3.57
4	3.01
5	2.71
6	3.45
7	3.20
8	3.11
9	2.87
10	3.49

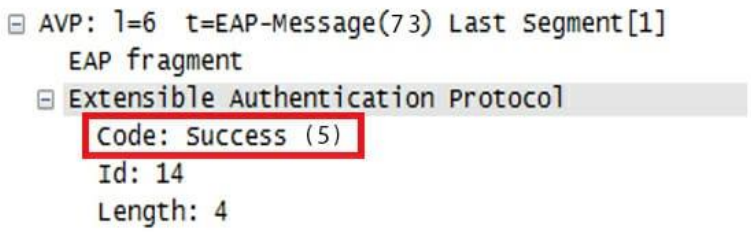


Gambar. 6. Hasil pada *wireshark* dalam membuat jalus TLS

Setelah tahap pembuatan jalur TTLS-TLS selesai, tahapan yang terakhir merupakan pengguna jenis EAP lain dalam melakukan *access authentication* terhadap *wireless network* dengan menggunakan MSCHAPv2. Pada tahap ini akan dikatakan berhasil apabila pengguna jaringan (*client*) dan RADIUS *server* sudah saling mengotentikasi dengan membuktikan *password* yang digunakan dan pertukaran dilakukan dalam terowongan sudah *encrypted* pada terowongan TLS setelah itu *client* dapat mengakses sumber daya jaringan dapat dilihat dengan *tool wireshark* seperti pada gambar 7. Pengujian dilakukan sebanyak sepuluh kali menggunakan *stopwatch* untuk mengukur waktu pada MSCHAPv2 dalam mengotentikasi *client* dengan RADIUS *server* ditunjukkan pada tabel 4.

Tabel 4. Percobaan MSCHAPv2 Dalam Mengotentikasi

Percobaan	Waktu (detik)
1	2.15
2	1.59
3	1.71
4	2.29
5	1.75
6	1.89
7	2.06
8	1.99
9	2.38
10	2.00



Gambar. 7. Hasil pada *wireshark* paket EAP telah berhasil

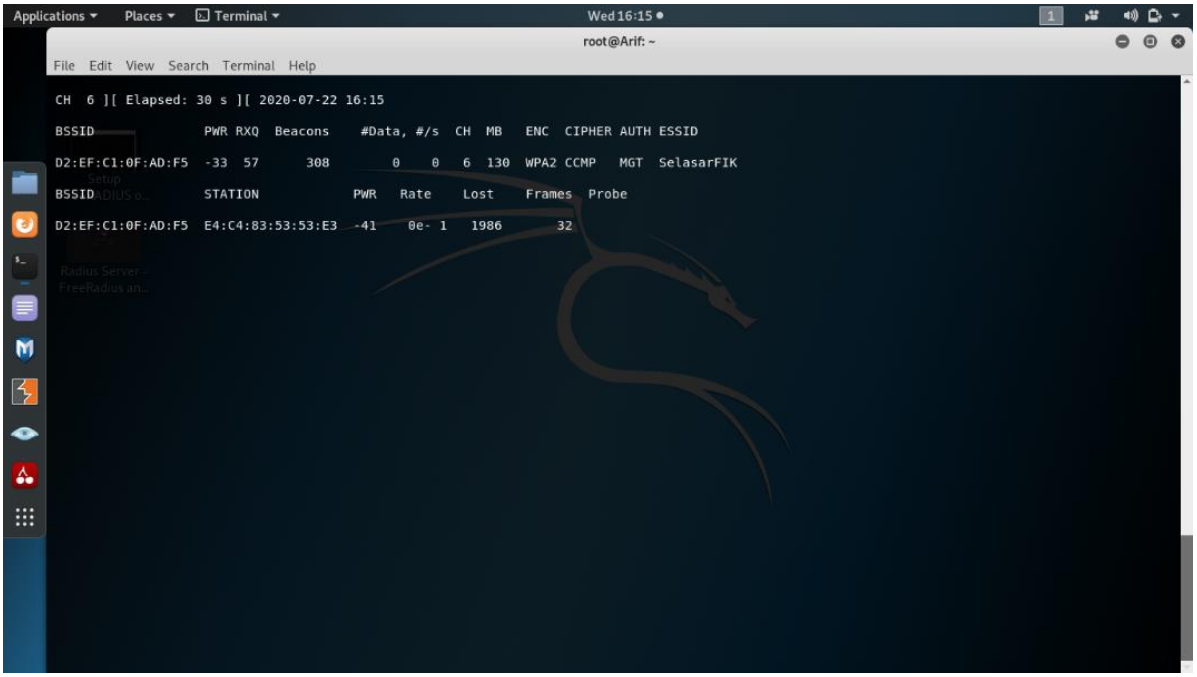
4.4 Pengujian Efektifitas Sistem Yang Digunakan

Pengujian efektifitas sistem pada keamanan WPA2-*Enterprise* dengan otentikasi EAP-TTLS dan MSCHAPv2 dengan *tools* yang sama saat menguji WPA2-*Personal* yaitu dengan *tools airmon-ng*, *airodump-ng*, *aireplay-ng*, dan *aircrack-ng*. Namun berbeda dengan keamanan WPA2-*Personal* dengan otentikasi PSK, WPA2-*Enterprise* dengan otentikasi EAP-TTLS dan MSCHAPv2 membuat *tools airodump-ng* tidak dapat menemukan *handshake*, sehingga tidak dapat dilanjutkan dengan *tool aircrack-ng* dapat diperlihatkan pada gambar 8. Pengujian keamanan yang digunakan dilakukan sebanyak 10 kali dengan menggunakan *stopwatch* dalam mengukur waktu pada *airodump-ng* mencoba mendapatkan *handshake* ditunjukan pada tabel 5.

Tabel 5. Percobaan *Airodump-ng* Mencoba Mendapatkan *Handshake*

Percobaan	Waktu (detik)
1	1.75
2	1.51
3	2.03
4	2.11
5	1.90
6	1.79
7	2.20
8	1.82
9	1.88
10	1.79

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)



Gambar. 8. *Airodump-ng* tidak mendapatkan *handshake* pada jaringan SelasarFIK

4.5 Analisa Hasil Kinerja Kedua Keamanan

Dari hasil pengujian sistem yang lama serta pengujian sistem yang digunakan pada sub-bab sebelumnya, penulis menganalisa bahwa keamanan jaringan *wireless* LAN dengan WPA2-*Personal* dengan otentikasi PSK tidak mampu mengamankan dari penyerangan *dictionary attack* karena *tool airodump-ng* mendapatkan *handshake* dengan pengukuran waktu tercepat 0.50 detik, lalu diproses dengan *aircrack-ng* untuk mencoba segala kemungkinan dalam menemukan kata sandi dari *wordlist* sehingga dampak yang dihasilkan penyerang mendapatkan kata sandi pengamanan. Sedangkan pada keamanan dengan menggunakan Protokol keamanan EAP dengan jenis EAP yaitu TTLS dan dengan otentikasi MSCHAPv2 mampu mengatasi penyerangan *dictionary attack* karena pada *tool airodump-ng* tidak mendapatkan *handshake* dengan pengukuran waktu tercepat 1.51 detik, begitu juga pada *tool wireshark* dalam merekam aktifitas jaringan ketika dilakukan penyerangan *deauthentication* pada *tool aireplay-ng* sehingga tidak dapat dilanjutkan dengan *tool aircrack-ng*.

Hasil pada keamanan protokol EAP-TTLS berperan untuk membuat terowongan keamanan pada jalur TLS dengan pengukuran waktu tercepat 2.71 detik, sehingga membuatnya menjadi jalur yang terenkripsi antara *client* dengan RADIUS *server* dengan menggunakan serangkaian pesan berupa EAP-*Message*, TTLS hanya membuat keamanan tambahan pada jalur TLS yang nantinya digunakan untuk jenis EAP lain seperti MSCHAPv2. Sedangkan pada MSCHAPv2 berperan dalam otentikasi yang dilakukan antara *client* dengan RADIUS *server* yang nantinya terjadi didalam terowongan keamanan yang telah dibuat oleh TTLS pada jalur TLS untuk pertukaran informasi yang nantinya *client* saling terotentikasi dengan RADIUS *server* dengan pengukuran waktu tercepat 1.59, setelah itu *client* dapat mengakses sumber daya jaringan.

5 Kesimpulan Dan Saran

5.1 Kesimpulan

Dari semua jabaran bab dahulu, bahwa penulis menentukan suatu pendapat yang dapat dijabarkan dibawah ini :

1. Penerapan aplikasi *Free*RADIUS diimplementasikan pada pengamanan jaringan *wireless* ini sebagai RADIUS *server* yaitu penggunaan AAA (*Authentication, Authorization, Accounting*), penerapan tersebut mendukung dalam penggunaan protokol EAP-TTLS dan otentikasi MSCHAPv2 pada jaringan *wireless* AP tipe ZTE ZXHN F6093.
2. Penerapan pada MSCHAPv2 dalam mengotentikasi *client* dan RADIUS *server* dengan waktu rata-rata 1.981 detik. MSCHAPv2 ini dapat digunakan dengan baik serta diimplementasikan dalam menangani proses keamanan otentikasi pada jaringan *wireless* AP tipe ZTE ZXHN F6093.

3. Berdasarkan pengujian efektifitas kedua sistem keamanan, protokol keamanan jaringan *wireless* LAN dengan menggunakan EAP-TTLS dan otentikasi MSCHAPv2 mampu menangani tipe penyerangan *dictionary attack* dengan waktu rata-rata 1.878 detik.

5.2 Saran

Dalam penelitian lebih lanjut, yang berkaitan dengan pengamanan otentikasi terpusat dengan menggunakan protokol EAP-TTLS dan MSCHAPv2 penulis memberikan saran sebagai berikut:

1. Pada penerapan protokol keamanan EAP-TTLS dan MSCHAPv2 ini dipengaruhi oleh spesifikasi *hardware* yang digunakan, sehingga akan lebih bagus bila PC *server* memiliki spesifikasi *hardware* yang tinggi agar dapat menjaga kualitas kinerja.
2. Untuk pengembangan berikutnya pada proses otentikasi dengan menggunakan EAP-TTLS dan MSCHAPv2 ini tidak hanya diterapkan pada jaringan *wireless* LAN atau nirkabel, namun juga diterapkan pada jaringan LAN atau dengan kabel.

Referensi

[1] Nurmawanti, N. C., Soegiarto, D., & Faruq, U. A. (2013). Pengamanan Jaringan *Wireless* Menggunakan PEAP Ms CHAP V2, 214-219.

[2] Rumalutur, S. (2014). Analisis Keamanan Jaringan *Wireless* LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong, 48-60.

[3] Arifin, Z. (2008). Sistem Pengamanan Jaringan *Wireless* LAN. Yogyakarta: Andi Offset.

[4] Samsumar, L. D., & Gunawan, K. (2017). Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (*Wireless* LAN); Studi Kasus Di Kampus STMIK Mataram, 73-82.

[5] Darmadi, E. A. (2018). Perancangan Sistem Otentikasi RADIUS Pada Pengguna Jaringan *Wireless* Untuk Meningkatkan Keamanan Jaringan Komputer, 9-16.

[6] Novrianda, R. (2017). Rancang Bangun Keamanan Jaringan *Wireless* Pada STIPER Sriwigama Palembang Dengan RADIUS *SERVER*. 19-29.

[7] Hassel, J. (2002). RADIUS *Cambridge Massachusetts* . O'Reilly Media.

[8] Harahap, A. (2011). Perbandingan Kinerja EAP-TLS, EAP-TTLS Dan EAP-PEAP Sebagai Protokol Autentikasi Pada Jaringan Nirkabel, 1-32.

[9] Funk, P., & Blake-Wilson, S. (2008). *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version* 0 (EAPTTLSv0).

[10] Rahman, H. (2011). Implementasi *Hotspot Authentication* Dengan Menggunakan RADIUS *Server* Dan Protokol EAP-TTLS. (Studi Kasus: Sekolah Islam Fitrah Al Fikri Depok Jawa Barat).

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)